UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

PROYECTO TÉCNICO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS CON MENCIÓN EN TELEMÁTICA

TEMA:

IMPLEMENTACIÓN DE UN SERVIDOR WEB Y UN DISEÑO DE UNA PÁGINA UTILIZANDO HERRAMIENTAS DE SOFTWARE LIBRE PARA EL DISPENSARIO "SAGRADA FAMILIA" DE LA CIUDAD DE GUAYAQUIL.

AUTORES:

BRUNO CHAVARRIA NEIRA

EDISSON GUDIÑO DE LA A

DIRECTOR:

M.Sc. Ing. OSVALDO PEREIRA BARZAGA

GUAYAQUIL – ECUADOR

2017

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO.

Nosotros; Bruno Alexander Chavarría Neira y Edisson Wilmer Gudiño de la A, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además, declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Bruno Alexander Chavarría Neira
CC: 0927693408

Edisson Wilmer Gudiño de la A
CC: 0922899661

CESIÓN DE DERECHOS DE AUTOR

Yo **EDISSON WILMER GUDIÑO DE LA A,** con documento de identificación N° **0922899661**, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de grado intitulado: "**IMPLEMENTACIÓN DE UN SERVIDOR WEB Y UN DISEÑO DE UNA PÁGINA UTILIZANDO HERRAMIENTAS DE SOFTWARE LIBRE PARA EL DISPENSARIO SAGRADA FAMILIA DE LA CIUDAD DE GUAYAQUIL**", mismo que ha sido desarrollado para optar por el título de: **INGENIERO DE SISTEMAS MENCIÓN TELEMÁTICA**, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....

EDISSON WILMER GUDIÑO DE LA A

0922899661

SEPTIEMBRE 2016

CESIÓN DE DERECHOS DE AUTOR

Yo **BRUNO ALEXANDER CHAVARRIA NEIRA,** con documento de identificación N° **0927693408**, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de grado intitulado: "**IMPLEMENTACIÓN DE UN SERVIDOR WEB Y UN DISEÑO DE UNA PÁGINA UTILIZANDO HERRAMIENTAS DE SOFTWARE LIBRE PARA EL DISPENSARIO SAGRADA FAMILIA DE LA CIUDAD DE GUAYAQUIL**", mismo que ha sido desarrollado para optar por el título de: **INGENIERO DE SISTEMAS MENCIÓN TELEMÁTICA**, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....

BRUNO ALEXANDER CHAVARRÍA NEIRA

0927693408

SEPTIEMBRE 2016

CERTIFICADO DE DIRECCIÓN

El presente trabajo previo a la obtención del título de Ingeniero de Sistemas con mención en Telemática, fue guiado satisfactoriamente por el M.Sc. Ing. Osvaldo Pereira Barzaga, quien autoriza su presentación para continuar los trámites correspondientes.

Guayaquil, noviembre del 2016.

M.Sc. Ing. Osvaldo Pereira Barzaga
DIRECTOR DE TITULACIÓN

DEDICATORIA

Llegué a la meta, el título universitario anhelado por mí y muchas personas, todas las personas pasan por un título, carrera, proyecto en su vida, pero de que hacen lo hacen y lo terminan, al finalizar todo me di cuenta que no fui el mejor de la clase ni terminé tampoco con excelentes calificaciones no fue fácil tuve muchos resbalones en el camino, materias repetidas como un estudiante normal obviamente, como Lavoisier llegó a la conclusión de que la materia, medida por la masa, no se crea ni destruye, sino que sólo se transforma en el curso de las reacciones, y como se dice por los salones la materia no se crea ni se destruye si no que se repite.

Pero lo que si me llena de orgullo es que aprendí y puedo poner todos los conocimientos en práctica, estudié, hice amigos conocí gente pude conocer a las personas, saque una experiencia algo que contar a los demás, lo más importante es que puedo decir con orgullo yo estudie en la Universidad Politécnica Salesiana y llevar eso en alto.

Con todo esto sólo puedo dar gracias a Dios; en primer plano, como dice: ***Juan 15,5.*** "Yo soy la vid; vosotros los sarmientos. El que permanece en mí y yo en él, ése da mucho fruto; porque separados de mí no podéis hacer nada", es verdad por eso agradezco a Dios.

Mis Padres que han hecho un trabajo excelente tantos años aguantándome hasta hacerles sacar canas verdes, pero siempre me han apoyado en todo lo que he hecho ya más de 25 años levantándome y llevándome a casi todos lados atendiéndome, dándome consejos, amor, apoyo. Los méritos son en conjunto les agradezco la vida y todos mis éxitos son éxitos de ustedes (Julio Cesar Chavarria Bimbela y Alexandra del Carmen Neira Alegría).

Mis hermanos también cumplen un rol importante en todo esto sin ellos tampoco hubiera podido hacer las veces que me dieron la mano me hicieron un favor o cuando me dijeron al mal tiempo buena cara una palabra de aliento basta y sobra para que siga adelante en si estoy agradecido a todos los que me apoyaron.

A los maestros gracias totales por el apoyo, desarrollo y progreso en mi vida profesional. El internet, Google, rincón del vago, stackoverFlow, Wikipedia porque sin ellos no hubiera adquirido el conocimiento necesario para desempeñarme mejor en mis clases y vida laboral.

Como todo llega al final entiendo muchas cosas y para poder terminar una meta proyecto básicamente debe de haber 3 partes: **proyecto terminado = Dios + Familia + esfuerzo**. si una de esa falla no hay proyecto. Dios permite hacer todas las cosas posibles, la familia para disfrutar el logro, dar apoyo moral sentimental siempre y por último el esfuerzo que son las ganas, intelecto, ideas para realizar el proyecto.

Bruno Alexander Chavarria Neira (bruchane)

DEDICATORIA

A Dios, por haberme dado la vida y permitirme llegar a este momento importante de mi formación, por darme fuerzas enseñándome a encarar y aprender de las dificultades que se presentaron en el camino.

Al apoyo inconmensurable de mis padres Edisson Gudiño Espinosa y Carmen De La A Escalante pilares fundamentales por tanto amor que me brindan, quienes me han formado con valores, principios, a confiar en mis capacidades y alcanzar mis metas. Gracias por sus consejos y por acompañarme en cada etapa de mi vida, a ustedes dedico mis logros.

A mis hermanos Michael y Sharon, quienes han estado siempre presente acompañándome siendo mi motivación, inspiración y felicidad.

Este nuevo logro es en gran parte gracias a ustedes familiares, amigos, maestros han sido base de mi formación, participes y promotores de este proceso aportando grandes cosas en mi vida.

Gracias totales por tanto y tanto.

Edisson Wilmer Gudiño De La A

AGRADECIMIENTO

De manera muy especial queremos agradecer a la Orden Capuchina del Ecuador (Dispensario Médico “Sagrada Familia”) a su Coordinador el Padre Juan Jima Lalangui, por haber confiado en nuestras capacidades, darnos la oportunidad y las facilidades de llevar a cabo este y otros proyectos, gracias a todo el personal quienes conforman esta noble institución queremos ratificar esa confianza con trabajo y esmero.

RESUMEN

El objetivo de este proyecto es establecer su marca e identidad en línea, promover, ofrecer sus servicios como canal adicional de información hacia el público en general.

Para que el proyecto sea terminado se dividió en tres fases:

Router, se configuró algunas políticas como: la configuración NAT uno a uno crea una relación y asigna una dirección IP de la WAN a una dirección IP de la LAN mediante NAT, de esa forma protegemos nuestro servidor web para que sea detectado y posteriormente vulnerado a ataques, también habilitó la opción DMZ la cual permite redirigir el tráfico que llega al puerto WAN a una dirección IP especificada en el servidor que está ubicado en la red LAN. Esta configuración brinda seguridad si se produce un ataque en alguno de los nodos o reglas aplicadas en la DMZ.

Las políticas configuradas en el firewall fueron inspección de paquetes de estado, denegación de servicio, bloqueo de solicitudes WAN, Https. Para proteger el sitio web se restringió las características Web Java, Cookies, ActiveX o Acceso a servidores proxy HTTP.

Se realizaron los pasos básicos para configurar un servidor web Apache, todas las configuraciones fueron hechas de manera segura, se instalaron algunos módulos de seguridad de apache y varias herramientas para control de puertos, detección de Rootkit, monitoreo de la actividad de usuarios y procesos.

El sitio web es el producto de todos los anteriores, básicamente está diseñado de manera intuitiva para que el usuario no se pierda, si no que la información esté al alcance de él.

ABSTRACT

The target of this Project is to establish a Brand and online identity, promote and offer their services and be an additional Information channel to Public

To finish this Project, we divided in three phases:

Router was configured with several policies: Set up One-to-One NAT creates a relationship that maps a valid WAN IP address to LAN IP addresses that are hidden from the WAN (Internet) by NAT. This protects the Web Server from discovery and attack. Also we enabled DMZ option, this allow redirect the traffic that comes from WAN port to an IP direction specified in the server that is located in the LAN network, this configuration give us security if an attack occurs in one of the nodes or rules applied in the DMZ.

The firewall configuration policies were state full packet inspection, service denied, Wan, Https request blocking. To protect the web site were strict the following characteristics web Java, Cookies, ActiveX, Access to proxy HTTP servers.

It has been made the basic Steps to configure the Apache Web Server, all the configurations were done securely, was installed some apache security modules and many other tools to control ports, Rootkit detection, user and process activity monitoring.

The last point and important one is the web site because is the final product of all steps, basically the web site was designed in an intuitive way so the user cannot lose any page because the Information is reachable to him.

ÍNDICE

ÍNDICE DE ILUSTRACIÓN

INTRODUCCIÓN.

Existe la necesidad de informatizar el proceso de gestión de pacientes; con el fin de brindarle una atención más eficiente a los mismos.

La informatización y/o automatización de este proceso, permitirá a los pacientes y sus familiares (clientes); consultar en el portal web del dispensario consultar el estado de sus trámites y servicios brindados por la institución “SAGRADA FAMILIA”.

La posibilidad de que los pacientes puedan vía online realizar consultas, trámites e informarse; desde cualquier dispositivo electrónico con conexión a internet, aumenta en gran medida la satisfacción de los usuarios del dispensario en relación a la agilidad de los trámites y a la calidad de la información que se les brinda.

El siguiente proyecto describe la puesta en marcha desarrollado en cuatro capítulos donde se detalla el análisis y estudios preliminares previos a la implementación y posterior integración física y lógica de los equipos para el dispensario “SAGRADA FAMILIA” con el fin de presentar como resultado final una página web de tipo informativa que cumpla con los propósitos planteados por la empresa para brindar mayor facilidad a sus usuarios.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 **PROBLEMA**

El dispensario “Sagrada Familia” no cuenta con un sitio web que informe y automatice el proceso de gestión de pacientes; por este motivo los pacientes tienen que asistir al dispensario para realizar trámites de consultas generales, médicas o gestión de trámites.

También cuenta con infraestructura inadecuada de servidores y medios de cómputos para soportar el nivel de información y automatización que requiere el dispensario en su proceso de gestión de pacientes.

1.1.1 ANÁLISIS DEL PROBLEMA

La inexistencia de una herramienta que le permita al usuario estar informado sobre las actividades y servicios ofrecidos por el dispensario médico “SAGRADA FAMILIA” sin acudir físicamente al establecimiento, sumada a la falta de equipos adecuados limita a las empresas a un óptimo desarrollo ocasionando pérdidas en tiempos para el proceso de la información e incluso pérdidas económicas por falta de gestión de las mismas, la implementación y la correcta planificación brindará mayor calidad y eficiencia de las operaciones de las empresas. Se detalla en la ilustración1 el esquema de red con el que contaba el dispensario antes de la intervención

Las limitadas herramientas tecnológicas con las que cuenta el dispensario no son las adecuadas y es uno de los factores principales por el cual se pone en marcha este proyecto dotando de una infraestructura que permita el desarrollo de esta entidad y se dé solución a los principales problemas:

- Falta de acceso e información que tienen los pacientes sobre los servicios y actividad laboral del dispensario.

- Debido al crecimiento de las instalaciones del dispensario la infraestructura actual no está acorde a la demanda, el cual requiere de la inserción de equipos que soporte este crecimiento y gestión los recursos de la red y que a su vez brinde la escalabilidad necesaria de fututos proyectos.

- Una mala arquitectura de los equipos de red actual no establecidos de manera jerárquica que no brinda la confiabilidad necesaria.

- Falta de implantación de un firewall que brinde la seguridad a la red y los servidores internos del dispensario.

- Limitado control y administración de los recursos a nivel de la red LAN.

- Equipo Router no soporta configuraciones avanzadas que permitan de manera correcta gestionar los recursos WAN proporcionados por los dos proveedores ISP.

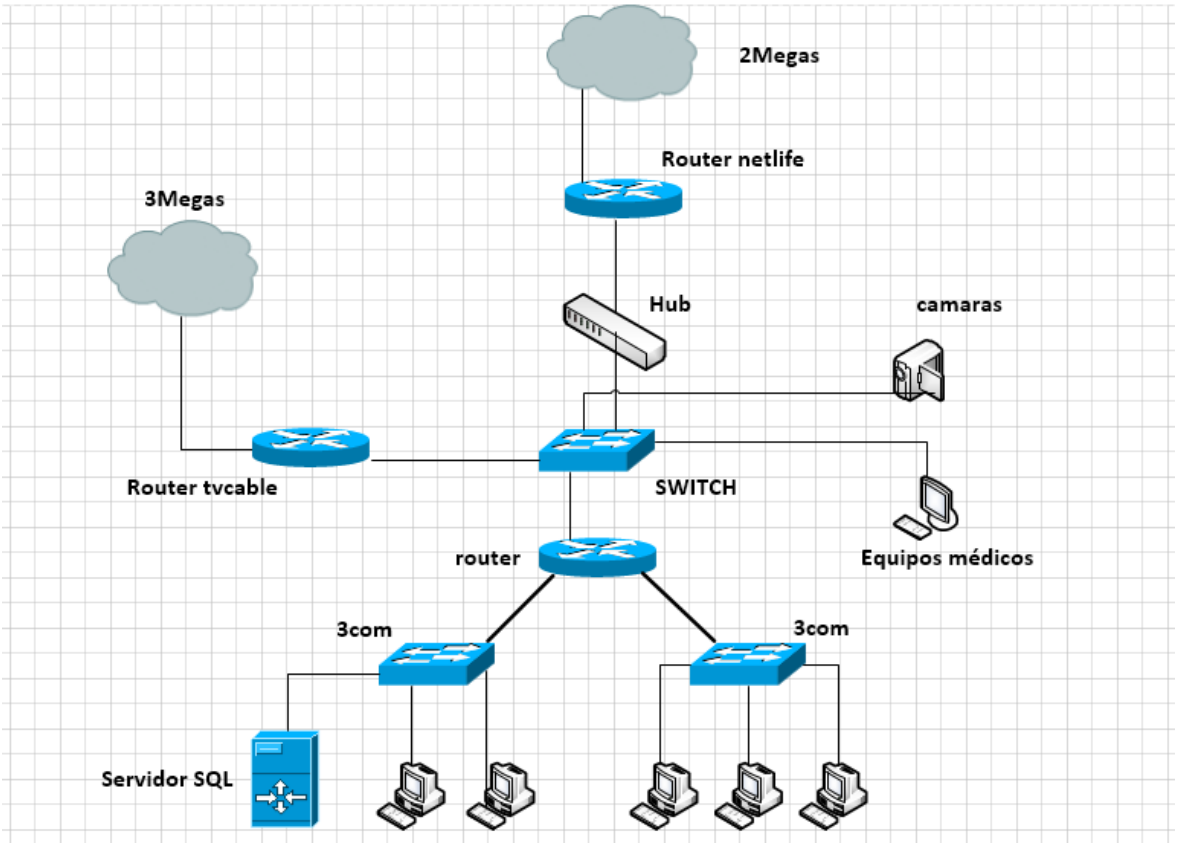


Ilustración 1 Diseño actual de red

Elaborado por: Autores

1.1.2 SISTEMATIZACIÓN DEL PROBLEMA

- ¿Cómo puede mejorar los recursos y la fluidez de la información con inserción de nuevos equipos y el cambio de arquitectura de la red dispensario médico Sagrada Familia de la ciudad de Guayaquil?

- ¿Qué actividades realizadas por el personal médico y administrativo del dispensario médico Sagrada Familia de la ciudad de Guayaquil se ven beneficiadas con la implementación del servidor web?

- ¿De qué manera los pacientes del dispensario médico Sagrada Familia de la ciudad de Guayaquil pueden aprovechar la innovación e implementación de infraestructura tecnológica?

1.1.3 JUSTIFICACIÓN

El proyecto de investigación resulta de gran utilidad por el aporte teórico, práctico y metodológico que se realiza, a continuación, vamos a explicar las tres bases en que se fundamenta el proyecto:

- **Teórico:** El argumento teórico de este proyecto le brinda al lector la teoría básica y complementaria para entender cómo se configura de manera correcta un servidor web, router firewall y además el diseño de una página web.

- **Metodológico:** Los pasos para realizar configuración tanto de servidor web como el router están basados en una metodología porque no fueron tomados directamente de cualquier fuente llámese esta página web, libro, revista, artículo científico si no que se realizó un estudio exhaustivo para determinar cuál es la mejor manera de configurar los equipos y que sea de fácil entendimiento para el lector.

- **Práctico:** En cuanto a la parte tecnológica página web es un canal para mantener informadas a las personas y de fácil acceso a la información ya que el diseño de la misma es intuitivo y las personas no se perderán en buscar la información, toda

página web debe de tener un mecanismo atrás que este controlando y vigilando los intrusos y demás vulnerabilidades que pueda presentar un sitio web por ese motivo configuramos un firewall para que nos brinde esa protección extra y no haya anomalías en el funcionamiento de la página.

- **Relevancia social**: El impacto del proyecto en la sociedad sería que las personas no tienen que llamar al dispensario para obtener información básica como: horarios de atención, especialidades, horarios disponibles de los doctores etc. Podrán acceder desde la comodidad de sus casas o cualquier lugar que tenga habilitada una conexión a internet en si se beneficiarían a los clientes ya que el proyecto es un canal de información verdadera y publicitaria, mediante el cual atraerá más clientes al dispensario aumentando los ingresos. La parte tecnológica se beneficia el dispensario porque se organizará la infraestructura de red y se añadirá protecciones adicionales.

1.2 **ANTECEDENTES**

En 1967 Se Realizó Un Primer Intento De Crear Un Dispensario, Que Tuvo Una Vida Fugaz De Pocos Meses. El Dispensario Sagrada Familia es una institución sin fines de lucro que procura, a partir del evangelio, brindar atención médica digna a aquellas personas carentes del amparo y protección pública. Para el efecto cuentan con un selecto equipo de profesionales en todas las especialidades y el soporte técnico de equipos de última generación.

Al pasar del tiempo el dispensario ha ido adecuando tanto sus instalaciones como equipos tecnológicos implementando equipos de cómputo en cada consultorio y almacenando las fichas medica en unos servidores de base de datos, haciéndose también de un sistema interno con varios módulos de facturación y atención al cliente, gestionado así las consultas de sus pacientes

Antes el Dispensario Sagrada Familia daba a conocer sus servicios mediante llamada telefónica o acudir al dispensario donde se reflejaba información básica del mismo, el dispensario no contaba principalmente con una infraestructura adecuada para implementar los equipos necesarios un servidor y un sitio web, para realizar una solución que le permita darse a conocer.

También es de mucha importancia el que la empresa ofrezca servicio en línea mediante un sitio Web, ya que esto es un escaparate para obtener nuevos clientes si se utilizan estrategias adecuadas de marketing para informar al público en general de las actividades, descuentos, servicios del dispensario.

El proyecto ayudará mejorar la conectividad en todas las áreas, segmentar la red, tarifar el tráfico y agregar seguridades para los proyectos posteriores del dispensario Sagrada Familia ya que no cuentan con una infraestructura tecnológica adecuada para brindar el servicio necesario a los clientes , el proyecto será realizado con soluciones de software libre porque las instituciones, sobre todo las pymes y autónomos, buscan siempre herramientas y

mecanismos que les permitan reducir los gastos del día a día de la empresa. Una forma de hacerlo es mediante el uso de software libre software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software; de modo más preciso.

1.3 **IMPORTANCIA**

El diseño y la implementación de un servidor web tiene como fin facilitar y automatizar el servicio que brinda el dispensario médico “sagrada familia” a sus usuarios que podrán beneficiarse con información de los diferentes servicios médicos que pone a disposición esta institución a la comunidad en general.

La implementación de este nuevo servicio permite al usuario desde la comodidad de su casa ingresar al sitio web en busca de información que brinda la institución beneficiándose de los recursos que se pone a disposición tanto como parte informativa como la posibilidad de que el usuario vea los horarios de los médicos y de las especializaciones en la que atienden pudiendo registrarse y separando un cita optimizando y automatizando el servicio del dispensario, obviando así que este tenga que recurrir al establecimiento por dicha información, facilitando también la administración del personal interno de la institución que integra y pone a disposición esta nueva plataforma tecnológica.

1.4 **ALCANCE:**

1.4.1 DISEÑO DE LA NUEVA INFRAESTRUCTURA

Se realiza un levantamiento de información sobre la arquitectura actual y diseño de red como tal analizando el número de usuarios, espacio físico y consumo de recursos que genera la labor diaria del dispensario. Que como resultado reflejan las necesidades en equipos y espacio las cuales conllevan la implementación de este nuevo servicio.

1.4.2 ADQUISICIÓN DE EQUIPOS

Mediante el análisis de las necesidades se determina la adquisición de ciertos equipos:

- Servidor DELL que se alojara físicamente en un rack de piso con las características necesarias para soportar el servicio y todo lo que demande la implementación de la página web.

- Router cisco de la serie smallbusiness que nos garantizar administrar y gestionar de manera óptima los recursos de la empresa con una amplia gama de parámetros a nivel de administración, brindando también la seguridad necesaria para proteger la red interna.

- Switch cisco de la serie smallbusinesscon una amplia gama de opciones a nivel de gestión que ayudará a distribuir de manera jerárquica los equipos ya existentes siendo intermediario entre el núcleo y el acceso de la red.

Teniendo en cuenta que los equipos adquiridos soportan de manera escalable un futuro crecimiento en la Red.

1.4.3 IMPLEMENTACIÓN DE LOS EQUIPOS A LA RED

Se realiza la integración de los nuevos equipos adquiridos mediante una restructuración física y lógica de la arquitectura de la red de tal manera de que los recursos se distribuyan de manera eficiente, específicamente con los siguientes parámetros:

- Instalación del servidor basado en software libre con sistema operativo Linux Ubuntu server y servidor DNS.

- Configuración lógica de la WAN router cisco donde se levantó un servidor dhcp para el direccionamiento de la red interna, se aplicó parámetros de configuración el FIREWAL y DMZ para garantizar seguridad a los servicios, asignación de NAT UNO A UNO de la IP publica que redirección la página WEB.

- Configuración lógica switch cisco equipo de distribución entre el núcleo y los switch de acceso.

1.4.4 DESARROLLO DEL SITIO WEB

Diseño y maquetado de sitio web informativo responsivedesing que se adapta a cualquier tipo de dispositivo.

1.5 DELIMITACIÓN

1.5.1 DELIMITACIÓN TEMPORAL

El tiempo que se tomó en realizar todo el proyecto fue de seis meses entre las diversas actividades que tuvimos que realizar, el importe de los equipos activos y pasivos demoro aproximadamente dos meses la llegada al país y el desarrollo y puesta a producción del proyecto se demoró cuatro meses para que los equipos queden óptimamente configurados y puesta en marcha.

1.5.2 DELIMITACIÓN EN ESPACIO

Este proyecto fue puesto en marcha en el sur de la ciudad de Guayaquil de la provincia del Guayas orientada a personas que deseen la información necesaria que les acceder a los servicios brindados por el dispensario médico Sagrada Familia de esta ciudad y sitios aledaños en general.

1.6 OBJETIVOS

1.6.1 OBJETIVO GENERAL

Dotar al dispensario de una herramienta que facilite y agilice el proceso y los tiempos entre la entidad y sus pacientes implementando una infraestructura de servidores y medios de cómputo para soportar el nivel de información necesaria permitiendo diseñar un sitio web

que informe y automatice el proceso de gestión de pacientes del Dispensario Médico Sagrada Familia.

1.6.2 OBJETIVOS ESPECÍFICOS

- Analizar las características óptimas de los equipos de cómputo y de red para el levantamiento de la infraestructura estableciendo proformas para la adquisición de los mismos.

- Diseñar el esquema de red para integración y ubicación de cada uno de los componentes que forman parte de la infraestructura.

- Realizar las configuraciones y puesta en marcha de los equipos de cómputo y de red.

- Determinar las mejores opciones de software libre y herramientas de desarrollo para servidores páginas webs.

- Diseñar el sitio web que ofrezca información actualizada al público en general acerca de las actividades y servicios del Dispensario.

MARCO TEÓRICO

2 REDES DE COMPUTADORAS

La definición más clara de una red según (Econ, s.f.)Es que un sistema de comunicaciones, que permite comunicarse con otros usuarios y compartir archivos y periféricos. Es decir, es un sistema de comunicaciones que conecta a varias unidades y que les permite intercambiar información.

Se entiende por red al conjunto interconectado de computadoras autónomas.

Se dice que dos computadoras están interconectadas, si éstas son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación.

2.1 REQUISITOS DE LOS DISEÑOS DE REDES

Para (Zepeda Vega, s.f.) Los requisitos de diseño de redes son los siguientes:

Funcionalidad: La red debe funcionar. Es decir, debe permitir que los usuarios cumplan con sus requisitos laborales. La red debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonables.

Escalabilidad: La red debe poder aumentar de tamaño. Es decir, el diseño original debe aumentar de tamaño sin que se produzcan cambios importantes en el diseño general.

Adaptabilidad: La red debe diseñarse teniendo en cuenta futuras tecnologías. La red no debería incluir elementos que limiten la implementación de nuevas tecnologías a medida que éstas van apareciendo.

Facilidad de administración: La red debe estar diseñada para facilitar su monitoreo y administración, con el objeto de asegurar una estabilidad de funcionamiento constante.

2.2 **OBJETIVOS DE LAS REDES**

Menciona (Econ, s.f.)Que son muchas las organizaciones que cuentan con un número considerable de computadoras en operación y con frecuencia alejadas unas de otras. Por ejemplo, una compañía con varias fábricas puede tener una computadora en cada una de ellas para mantener un seguimiento de inventarios, observar la productividad y llevar la nómina local.

Inicialmente cada uno de estas computadoras puede haber estado trabajando en forma aislada de las demás, pero, en algún momento, la administración puede decidir interconectarlos para tener así la capacidad de extraer y correlacionar información referente a toda la compañía.

Es decir, el objetivo básico es compartir recursos, es decir hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que lo solicite, sin importar la localización del recurso y del usuario.

Un segundo objetivo que plantea (Econ, s.f.)Es proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro.

Todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que, si una no se encuentra disponibles, podría utilizarse algunas de las copias. La presencia de múltiples CPU significa que, si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Las grandes máquinas tienen una rapidez mucho mayor.

Analiza (Econ, s.f.)Que una red de computadoras puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí.

Con el empleo de una red es relativamente fácil para dos personas, que viven en lugares separados, escribir un informe junto.

2.3 TIPOS DE REDES

2.3.1 SEGÚN SU ALCANCE

2.3.1.1 LAN

Una red de área local, red local o LAN (del inglés Local Area Network) es la interconexión de varios ordenadores y periféricos(Casillas Gallegos & Domínguez Ruíz, 2009) Da a conocer que su extensión está limitada físicamente a un edificio o a un entorno de hasta 200 metros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones.

Ilustración 2 RED LAN

Fuente:(LAN, WAN, MAN, WLAN, WMAN, WWMAN, SAN y PAN: Qué significa cada término, 2015)

2.3.1.2 MAN

Como dice (Casillas Gallegos & Domínguez Ruíz, 2009) Una red de área metropolitana (MetropolitanArea Network o MAN, en inglés) es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de

múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica.

Ilustración 3 RED MAN

Fuente: (LAN, WAN, MAN, WLAN, WMAN, WWMAN, SAN y PAN: Qué significa cada término, 2015)

2.3.1.3 WAN

Una Red de Área Amplia (Wide Area Network o WAN, del inglés), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo en el que se basa (Casillas Gallegos & Domínguez Ruíz, 2009) De este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

Ilustración 4 RED WAN

Fuente: (LAN, WAN, MAN, WLAN, WMAN, WWMAN, SAN y PAN: Qué significa cada término, 2015)

2.3.2 SEGÚN SU TOPOLOGÍA

La topología de red o forma lógica de red se define como la cadena de comunicación que los nodos que conforman una red usan para comunicarse. Es la distribución geométrica de las computadoras conectadas.

2.3.2.1 RED BUS

Su topología se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre sí. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente. La ruptura del cable hace que los hosts queden desconectados.

Los extremos del cable se terminan con una resistencia de acople denominada terminador, que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus por medio de un acople de impedancias.

Las estaciones están conectadas por un único segmento de cable. A diferencia de una red en anillo, el bus es pasivo, no se produce generación de señales en cada nodo.

De acuerdo con(Casillas Gallegos & Domínguez Ruíz, 2009) Las ventajas y desventajas de una red tipo bus son las siguientes:

Ventajas

- Facilidad de implementación y crecimiento.
- Económica.
- Simplicidad en la arquitectura.

Desventajas

- Longitudes de canal limitadas.
- Un problema en el canal usualmente degrada toda la red.
- El desempeño se disminuye a medida que la red crece.
- El canal requiere ser correctamente cerrado (caminos cerrados).
- Altas pérdidas en la transmisión debido a colisiones entre mensajes

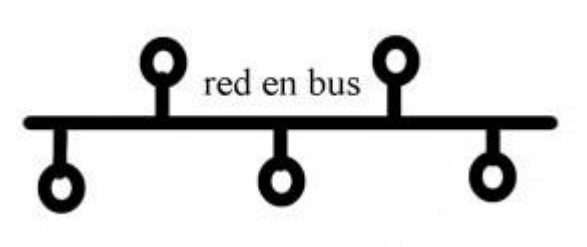


Ilustración 5 RED EN BUS

Fuente: (Juliá, 2015)

2.3.2.2 RED ESTRELLA

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones que han de hacer necesariamente a través de este. Dado su transmisión, una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en éstas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes.

Según (Casillas Gallegos & Domínguez Ruíz, 2009) las ventajas y desventajas son:

Ventajas

- Tiene dos medios para prevenir problemas.
- Permite que todos los nodos se comuniquen entre sí de manera conveniente.

Desventajas

- Si el nodo central falla, toda la red se desconecta.
- Es costosa, ya que requiere más cable que la topología Bus y Ring.
- El cable viaja por separado del hub a cada computadora

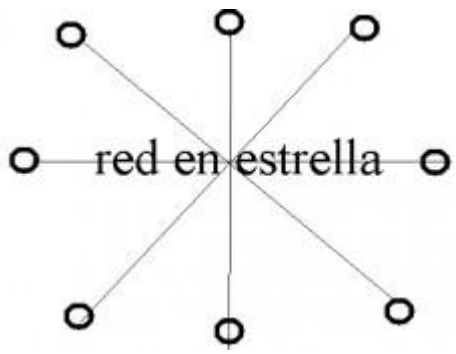


Ilustración 6 RED EN ESTRELLA

Fuente:(Juliá, 2015)

2.3.2.3 RED ANILLO

Topología de red en la que cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

Cabe mencionar que(Casillas Gallegos & Domínguez Ruíz, 2009) Expresa que, si algún nodo de la red deja de funcionar, la comunicación en todo el anillo se pierde.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos), lo que significa que, si uno de los anillos falla, los datos pueden transmitirse por el otro.

Según (Casillas Gallegos & Domínguez Ruíz, 2009) las ventajas y desventajas son:

Ventajas

- Simplicidad de arquitectura. Fácil implementación y crecimiento.

Desventajas

- Longitudes de canales limitadas.
- El canal usualmente degradará a medida que la red crece.

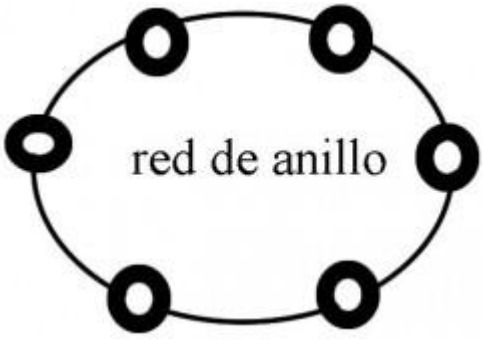


Ilustración 7 RED EN ANILLO

Fuente: (Juliá, 2015)

2.3.2.4 RED EN MALLA

La topología en malla es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos expresa(Casillas Gallegos & Domínguez Ruíz, 2009) Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

El establecimiento de una red de malla es una manera de encaminar datos, voz e instrucciones entre los nodos. Las redes de malla se diferencian de otras redes en que los elementos de la red (nodo) están conectados todos con todos, mediante cables separados. Esta configuración ofrece caminos redundantes por toda la red de modo que, si falla un cable, otro se hará cargo del tráfico.

Dicho con palabras de (Casillas Gallegos & Domínguez Ruíz, 2009)Esta topología, a diferencia de otras (como la topología en árbol y la topología en estrella), no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento (un error en un nodo, sea importante o no, no implica la caída de toda la red).

Las redes de malla son autoruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable. Es una opción aplicable a las redes sin hilos (Wireless), a las redes cableadas (Wired) y a la interacción del software de los nodos.

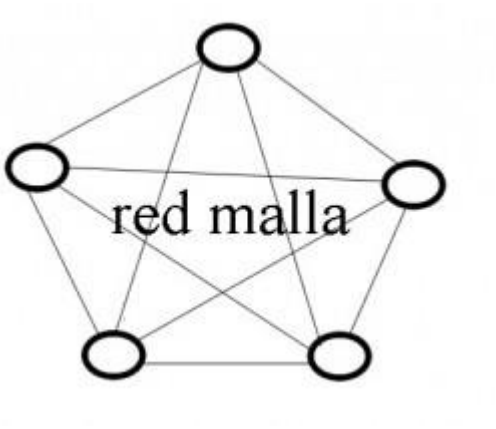


Ilustración 8 RED EN MALLA

Fuente:(Juliá, 2015)

2.3.2.5 RED EN ÁRBOL

Según (Casillas Gallegos & Domínguez Ruíz, 2009) la topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

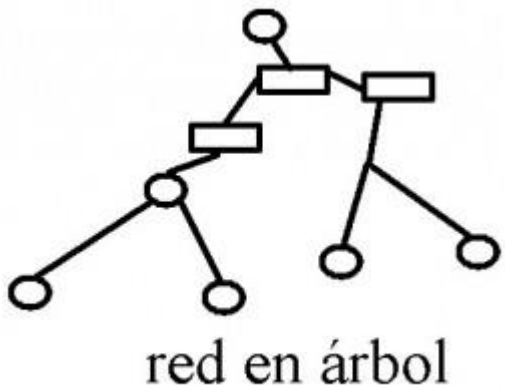


Ilustración 9 RED EN ÁRBOL

Fuente:(Juliá, 2015)

2.3.3 SEGÚN SU MEDIO DE PROPAGACIÓN

El medio de comunicación es el canal o enlace físico entre los nodos de una red a través del cual es transmitida la información expresa (Méndez Hernández). Existen medios de comunicación.

2.3.3.1 MEDIOS DE COMUNICACIÓN INALÁMBRICOS

De acuerdo con (Méndez Hernández), los medios de comunicación alámbricos es el espacio libre por donde se propaga un tipo particular de ondas electromagnéticas: ondas de radiofrecuencia que son portadoras de señales de datos. En la actualidad existen redes cuya señal no es transmitida por un medio físico como el cable, sino que es radiada de una antena a través de espacio (radiomódems).

2.3.3.2 MEDIOS DE COMUNICACIÓN ALÁMBRICOS

Un medio de comunicación alámbrico lo define como un cable y quizá otros dispositivos electrónicos que conectan físicamente adaptadores de comunicación entre sí expresa (Méndez Hernández). Sí el medio de comunicación consta solamente de cable, el medio de comunicación es llamado pasivo. Sí el medio de comunicación además de cable, consta de algún dispositivo que: amplifique, regenere o module la señal, el medio es llamado activo. Estos cables tienen entre sí, dependiendo de su principio de operación y aplicaciones, diversas configuraciones, componentes y materiales.

2.4 SISTEMA DE CABLEADO ESTRUCTURADO

2.4.1 QUÉ ES EL CABLEADO ESTRUCTURADO

Es el conjunto de elementos pasivos, flexible, genérico e independiente, que sirve para interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes sistemas de control, comunicación y manejo de la información, sean estos de voz, datos, video, así como equipos de conmutación y otros sistemas de administración señala (Proyectos Curso Cableado Estructurado:Universidad del Azuay, 2006).

En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central, facilitando la interconexión y la administración del sistema, esta disposición permite la comunicación virtualmente con cualquier dispositivo, en cualquier lugar y en cualquier momento afirma (Proyectos Curso Cableado Estructurado:Universidad del Azuay, 2006).

2.4.2 INTRODUCCIÓN

Según (Sistema de cableado estructurado : Gobierno del Estado de Chiapas) un sistema de cableado estructurado consiste de una infraestructura flexible de cables que puede aceptar y soportar múltiples sistemas.

La necesidad de contar con mayor robustez y prestaciones en las plataformas de comunicaciones ha impulsado la utilización de mayores velocidades de transmisión de información en el hardware activo (electrónica) de las redes.

Esta situación necesariamente implica mayor capacidad de transmisión de información en el hardware pasivo de la red, entendiéndose éste como la infraestructura de cableado estructurado, cuyo diseño e instalación están reglamentados internacionalmente desde 1991.

El 20 de junio del 2002 TIA publicó la categoría 6 que tiene el número del documento oficial de ANSI/TIA/EIA-568-B.2-1, incrementado el ancho de banda a 250 Mhz. La norma satisface todos los objetivos originales establecidos por TR-42.1 (anteriormente TR-41.8.1).

2.4.3 OBJETIVO

Establecer las especificaciones necesarias para el diseño, construcción, instalación, administración y mantenimiento de redes de cableado estructurado de telecomunicaciones, que garanticen la correcta operación de los servicios de telecomunicaciones con tecnología de vanguardia indica (Sistema de cableado estructurado : Gobierno del Estado de Chiapas).

2.4.4 ALCANCE

Según (Sistema de cableado estructurado : Gobierno del Estado de Chiapas), esta norma específica una red de cableado estructurado de telecomunicaciones, estableciendo los siguientes aspectos:

- Diseño y especificaciones de una red de cableado estructurado genérica para servicios de voz, datos y video, en edificios administrativos y Campus.

- Diseño, construcción e instalación de las canalizaciones para el soporte e instalación de los diversos cables de la red de cableado estructurado de telecomunicaciones, en el interior de un edificio administrativo y en un Campus.

- Diseño y construcción de los espacios o áreas para la instalación de los equipos de telecomunicaciones, sistemas auxiliares y distribuidores de las redes de cableado estructurado.

- Esquema de administración uniforme para las redes de cableado estructurado de telecomunicaciones.

- Pruebas para la aceptación de las redes de cableado estructurado de telecomunicaciones.

2.4.5 NORMAS ANSI PARA CABLEADO ESTRUCTURADO VIGENTE

De acuerdo con (Sistema de cableado estructurado : Gobierno del Estado de Chiapas) Las normas ANSI para el cableado estructurado vigente son:

- ANSI/NECA/BICSI-568 Standard for Installing CommercialBuilding Telecommunications.

- ANSI/TIA/EIA-568-B.1 Commercial Building TelecommunicationsCabling Standard Part 1 General Requirements.

- ANSI/TIA/EIA-568-B.2 Commercial Building TelecommunicationsCabling Standard Part 2 Balanced Twisted Pair CablingComponents.

- ANSI/TIA/EIA-568-B.3 Optical Fiber Cabling ComponentsStandard.

- ANSI/TIA/EIA-569-B Commercial Building Standard forTelecommunications Pathways and Spaces.

- ANSI/TIA/EIA-606-(A) The Administration Standard forTelecommunications Infrastructure of Commercial Building.

- ANSI/TIA/EIA-607-(A) Commercial Building Grounding and Bonding Requirements for Telecommunications.

- ANSI/TIA/EIA-526-7 Measurement of Optical Power Loss ofinstaled Single Mode Fiber Cable Plant.

- ANSI/TIA/EIA-526-14. A Measurement of Optical Power Loss ofinstaled Multimode Fiber Cable Plant.
- ANSI/TIA/EIA-758-A Customer Owned Outside PlantTelecommunications Cabling Standard.

- ANSI/TIA-854 1000BASE-TX Standard for Gigabit Ethernet overCategory 6 Cabling.

- CENELEC-EN-50173 SecondEdition

2.4.6 TIPOS DE CABLES

Desde el punto de vista de (Armendáriz, 2009), las principales diferencias de rendimiento entre los distintos tipos de cables radican en la anchura de banda permitida (y consecuentemente en el rendimiento máximo de transmisión), su grado de inmunidad frente a interferencias electromagnéticas y la relación entre la pérdida de la señal y la distancia recorrida (atenuación).

Dicho con palabras de (Armendáriz, 2009), existen en la actualidad básicamente tres tipos de cables factibles de ser utilizados para el cableado en el interior de edificios o entre edificios:

- Par Trenzado
- Coaxial (No se recomienda para instalaciones nuevas, excepto redes de TV y CATV)
- Fibra Óptica

2.4.6.1 PAR TRENZADO

Dice(Armendáriz, 2009) que actualmente el tipo de cable más común en redes de área local y se originó como solución para conectar redes de comunicaciones reutilizando el cableado existente de redes telefónicas, Cada cable de este tipo está compuesto por una serie de pares de cables trenzados. Los pares se trenzan para reducir la diafonía -interferencia o crosstalk entre pares adyacentes-. El cable histórico de telefonía disponía de 2 pares, pero ya no se instala. En Europa además los pares no iban trenzados.

El cable típico en las redes de área local y en la conexión final de equipos es el de 4 pares. Los cables llamados multipar pueden tener 25, 50, 100, 200 y 300 pares.

Dice (Armendáriz, 2009) que las normativas de cableado estructurado clasifican los diferentes tipos de cable de pares trenzados en las siguientes categorías:

- **Categoría 3:** Aplica a cables UTP de 100 Ù y sus componentes de conexión, para aplicaciones de hasta 16 MHz de ancho de banda.

- **Categoría 4:** Aplicaba a cables UTP de 100 Ù y sus componentes de conexión, para aplicaciones de hasta 20 MHz de ancho de banda. Sin embargo, esta categoría ya no es reconocida en el estándar.

- **Categoría 5:** Aplicaba a cables UTP de 100 Ù y sus componentes de conexión, para aplicaciones de hasta 100 MHz de ancho de banda. Sin embargo, esta categoría ha sido sustituida por la 5e, y ya no es reconocida en el estándar.

- **Categoría 5e:** Aplica a cables UTP de 100 Ù y sus componentes de conexión, para aplicaciones de hasta 100 MHz de ancho de banda. Se especifica para esta categoría parámetros de transmisión más exigentes que los que aplicaban a la categoría 5.

- **Categoría 6:** Aplica a cables UTP de 100 Ù y sus componentes de conexión, para aplicaciones de hasta 200 MHz de ancho de banda. Se especifica para esta categoría parámetros de transmisión hasta los 250 MHz.

- **Categoría 6A:** La categoría 6A está en proceso de estandarización. Estará definida en la recomendación TIA 568-B.2-10, pensada para ambientes de hasta 10 Giga bit Ethernet, sobre cables UTP, soportando aplicaciones de hasta 500 MHz de ancho de banda.

2.4.6.2 CABLE COAXIAL

El cable coaxial está formado por un núcleo de cobre (llamado “vivo”) rodeado de un material aislante (dieléctrico); el aislante está cubierto por una pantalla de material

conductor, que según el tipo de cable y su calidad puede estar formada por una o dos mallas de cobre, un papel de aluminio, o ambos. Señala (Armendáriz, 2009) que este material de pantalla está recubierto a su vez por otra capa de material aislante. Por su construcción el cable coaxial tiene una alta inmunidad electromagnética frente al ruido, poca atenuación de la señal y puede llegar a tener unos anchos de banda considerables; siendo adecuado para grandes distancias y/o capacidades.

El cable coaxial más utilizado en la actualidad es el de 75 Ω de impedancia también llamado cable coaxial de banda ancha, que no es ni más ni menos que el cable coaxial utilizado para televisión y redes de cable (CATV).

Originalmente fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive. Su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos, además de que debe manipularse con cuidado.

Menciona (Armendáriz, 2009) que para redes de datos se han utilizado dos tipos de cable coaxial:

- Grueso (Coaxial amarillo de 50 Ω). Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Utilizado en la norma Ethernet 10Base-5.

- Fino (Coaxial RG58 de 50 Ω) con terminaciones BNC. Es más barato y fino y, por tanto, solventa algunas de las desventajas del cable grueso; aunque obtiene peores rendimientos que el cable amarillo. Utilizado en la norma Ethernet 10Base-2.

2.4.6.3 FIBRA ÓPTICA

La fibra óptica es un medio excelente para la transmisión de información por sus características: gran ancho de banda, baja atenuación de la señal que permite cubrir grandes distancias sin repetidores, integridad -proporción de errores baja (BER: Bit Error Rate)-,

inmunidad a interferencias electromagnéticas, alta seguridad y larga duración -resistente a la corrosión y altas temperaturas dice (Armendáriz, 2009).Sus mayores desventajas son su coste de producción -superior al resto de los tipos de cable- y su fragilidad durante el manejo en producción.

La terminación de los cables de fibra óptica requiere un tratamiento especial para convertir la señal óptica en eléctrica que ocasiona un aumento de los costes de instalación ("optoelectrónica").

Argumenta (Armendáriz, 2009) que el medio de transmisión la fibra óptica es un conductor de ondas en forma de filamento recubierto por una funda óptica o cubierta. La fibra interior, llamada núcleo, transporta el haz luminoso a lo largo de su longitud gracias a su propiedad de reflexión total interna (TIR: Total InternalReflection) y la fibra exterior -con un índice de refracción menor- actúa como 'jaula' para evitar que ésta escape.

La relación entre los índices de refracción del núcleo y de la cubierta depende también del radio del núcleo y se conoce como apertura numérica. Las fibras con una baja apertura solo permiten un único modo de propagación, o camino delhaz luminoso, (fibras "monomodo"), las fibras con una apertura mayor permiten varios modos (fibras "multimodo").

2.5 **MODELO DE RED JERÁRQUICAS**

Las redes jerárquicas se administran y se expanden con más facilidad (escalabilidad) que otras arquitecturas. Además, los problemas se resuelven con mayor rapidez da a conocer(Lopez, 2009).

El modelo de diseño jerárquico típico se separa en tres capas con funciones específicas: capa de acceso, capa de distribución y capa núcleo.

2.5.1 CAPA DE ACCESO

La Capa de Acceso aporta un medio de conexión de los dispositivos finales (PCs, impresoras y teléfonos IP) a la red, controla qué dispositivos pueden comunicarse y puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos.

Según (Lopez, 2009)Hoy en día los dispositivos más comunes en esta capa son los switches y los puntos de acceso inalámbricos.

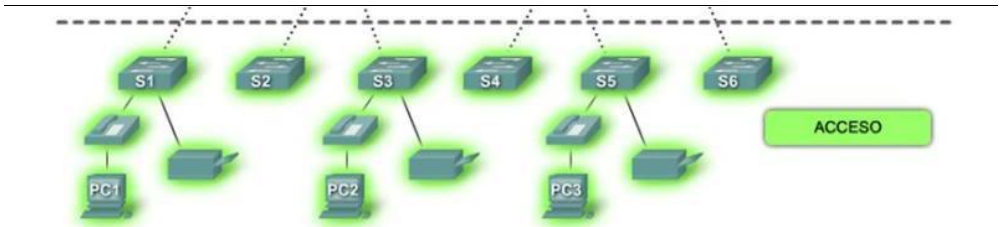


Ilustración 10 CAPA DE ACCESO

Fuente: (Lopez, 2009)

2.5.2 CAPA DE DISTRIBUCIÓN

De acuerdo con (Lopez, 2009)las principales características de la capa de distribución son las siguientes:

- La Capa de Distribución agrega los datos recibidos de los switches de la Capa de Acceso antes de que se transmitan a la Capa Núcleo para el enrutamiento hacia su destino final.
- La Capa de Distribución controla el flujo de tráfico de la red mediante el uso de políticas y segmenta la red en dominios de broadcast mediante el uso de LAN virtuales (VLAN).

- Las VLAN permiten al usuario segmentar el tráfico sobre un switch en subredes separadas (muchas veces de acuerdo a grupos de usuarios en una empresa).

- Los switches de la Capa de Distribución normalmente trabajan en las Capas 2 y 3 del Modelo OSI.

- A veces se usan switches de Capa 2 asistidos por routers para distribuir los datos entre las VLAN.

- Los switches de la Capa de Distribución son dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad.

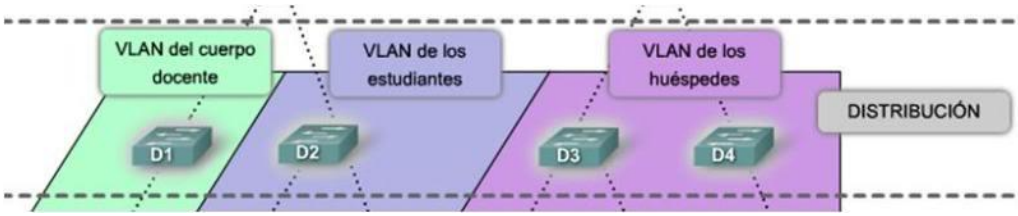


Ilustración 11 CAPA DE DISTRIBUCIÓN

Fuente:(Lopez, 2009)

2.5.3 CAPA NÚCLEO

- La Capa Núcleo es la espina dorsal (backbone) de alta velocidad de la red.

- La Capa Núcleo permite la interconectividad entre los dispositivos de la capa de distribución y la conexión a los recursos de Internet.

- Aquí se encuentran switches de capa 3 y routers.

Según (Lopez, 2009) en redes más pequeñas no es inusual que se implemente un modelo de núcleo colapsado en el que se combinan la Capa de Distribución y la Capa Núcleo en una sola capa.

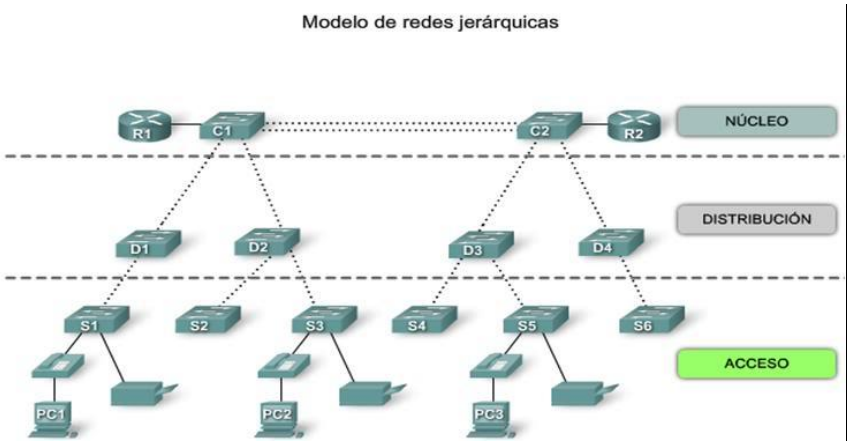


Ilustración 12MODELO JERARQUICO-NÚCLEO

Fuente:(Lopez, 2009)

2.5.4 BENEFICIOS DE UN MODELO DE RED JERÁRQUICO

Según (sistemasumma, 2012) los beneficios que se obtienen de una red jerárquica son:

- **Capacidad de mantenimiento** Debido a la segmentación física que mantienen las redes jerárquicas es fácil aislar y encontrar la fuente de los problemas de comunicación o cuellos de botella

- **Facilidad de administración** Debido a que cada capa de la red cumple con funciones específicas es fácil determinar en donde se deben de llevar a cabo las modificaciones o que reglas y configuraciones implementar en un router o switch nuevo.

- **Seguridad** Dada la misma naturaleza de la red jerárquica y su segmentación es fácil definir políticas de acceso entre los segmentos de la red, de forma que solo puedan tener acceso a un determinado segmento los equipos o segmentos autorizados o implementar restricciones basadas en protocolos para ciertas áreas.

- **Rendimiento** El rendimiento de la red se ve incrementada al emplear switch de alto rendimiento en secciones donde el flujo de datos es más intenso, además de que las mismas restricciones o políticas de seguridad permiten controlar los flujos de datos.

- **Redundancia** Para asegurar el funcionamiento de la red se pueden emplear enlaces redundantes a través de switch alternos o de respaldos que permitan mantener la comunicación en caso de algún fallo.

- **Escalabilidad** Al ser una estructura modular es fácil agregar nuevos nodos a la red o nuevos segmentos a través de los switch, o incluso en caso de un incremento en el tráfico es fácil descargarlo añadiendo switchs de mayor rendimiento.

2.6 DISPOSITIVOS DE INTERCONEXIÓN DE REDES

De acuerdo con (Unidad III Dispositivos de Red: Tecnológico Nacional de México), son dispositivos electrónicos que distribuye banda ancha a determinada cantidad de equipos (Computadores) de una red. (Switch, router) Son los equipos que se encargan de distribuir en forma activa la información a través de la red, como concentradores, redes inalámbricas, switches.

2.6.1 HUB

Es denominado concentrador. Cuando se transmiten señales eléctricas por un cable, se produce una degeneración proporcional a la longitud del cable, lo que se denomina Atenuación. Un hub es un simple dispositivo que se añade para reforzar la señal del cable y para servir de bus o anillo activo.

Normalmente, un repetidor no modifica de ningún modo la señal, excepto amplificándola para la transmisión por el segmento de cable extendido. Describe(Unidad III Dispositivos de Red: Tecnológico Nacional de México) que básicamente las características de un repetidor son las siguientes:

- Define la topología lógica de la red Sirve para definir la topología física estrella dentro de un cableado estructurado, cuando se utiliza cable de cobre trenzado.

- Regenera las señales de red para que puedan viajar más lejos.

- Se usa principalmente en sistemas de cables lineales como Ethernet.

- Opera en el nivel más bajo de la pila de un protocolo: el nivel físico. No se usa en protocolos de más alto nivel. Dos segmentos conectados por un repetidor deben usar el mismo método de acceso a la comunicación. Los segmentos conectados mediante un repetidor forman parte de la misma red y tienen la misma dirección de red.

Ilustración 13 HUB

Fuente: (Imagen: HW GROUP)

2.6.2 BRIDGE (PUENTE)

Es el dispositivo que interconecta las redes y proporciona un camino de comunicación entre dos o más segmentos de red o subredes explica (Unidad III Dispositivos de Red: Tecnológico Nacional de México). El Bridge permite extender el dominio de broadcast, pero limitándole dominio de colisión. Algunas razones que plantea (Unidad III Dispositivos de Red: Tecnológico Nacional de México) para utilizar un puente son las siguientes:

- Para ampliar la extensión de la red o el número de nodos que la constituyen.

- Para reducir el cuello de botella del tráfico causado por un número excesivo de nodos.

- Para unir redes distintas y enviar paquetes entre ellas, asume que ejecutan el mismo protocolo de red.

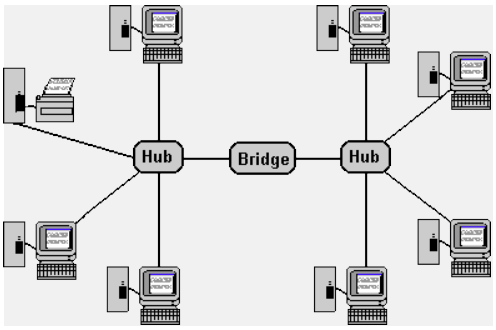


Ilustración 14BRIDGE

Fuente: (Switch image: Bucaro TecHelp)

2.6.3 GATEWAY (COMPUERTA PASARELA)

Una pasarela consiste en una computadora u otro dispositivo que actúa como traductor entre dos sistemas que no utilizan los mismos protocolos de comunicaciones, formatos de estructura de datos, lenguajes y/o arquitecturas. Una pasarela no es como un puente, que simplemente transfiere la información entre dos sistemas sin realizar conversión. Una pasarela modifica el empaquetamiento de la información o su sintaxis para acomodarse al sistema destino manifiesta (Unidad III Dispositivos de Red: Tecnológico Nacional de México). Su trabajo está dirigido al nivel más alto de la referencia OSI, el de aplicación.

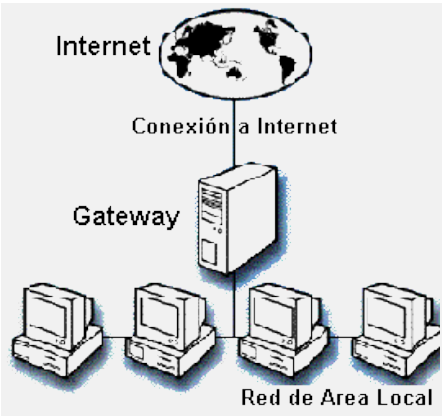


Ilustración 15 GATEWAY

Fuente: (Image Gateway :Hardware y Software de redes)

2.6.4 ROUTER

Un router es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Cuando un usuario accede a una URL, el cliente web (navegador) consulta al servidor de nombre de dominio, el cual le indica la dirección IP del equipo deseado.

La estación de trabajo envía la solicitud al router más cercano, es decir, a la pasarela predeterminada de la red en la que se encuentra. Este router determinará así el siguiente equipo al que se le enviarán los datos para poder escoger la mejor ruta posible. Para hacerlo, el router cuenta con tablas de enrutamiento actualizadas, que son verdaderos mapas de los itinerarios que pueden seguirse para llegar a la dirección de destino expresa (CCM, CCM). Existen numerosos protocolos dedicados a esta tarea.

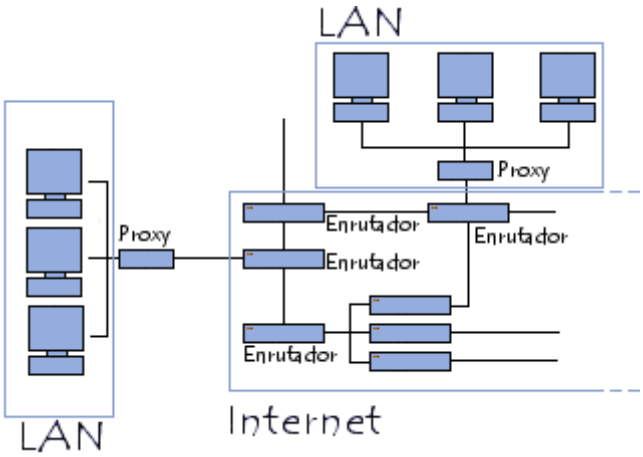


Ilustración 16 Esquema Router

Fuente: (CCM, CCM)

Dice(CCM, CCM), el router además de su función de enrutar, los routers también se utilizan para manipular los datos que circulan en forma de datagramas, para que puedan pasar de un tipo de red a otra. Como no todas las redes pueden manejar el mismo tamaño de paquetes de datos, los routers deben fragmentar los paquetes de datos para que puedan viajar libremente.

2.6.5 SUICHES (SWITCH)

Son dispositivos utilizados para entregar todo el ancho de banda a un segmento de red en una fracción de tiempo. Un switch en su presentación es muy parecido al hub, sólo difiere en su función lógica y en la adición de unos puertos para funciones adicionales. El switch

realiza transferencia de tráfico de broadcast y de multicast, pero disminuye el dominio de colisión al mínimo.

Algunas características especiales que describe (Unidad III Dispositivos de Red: Tecnológico Nacional de México) de los switch son las siguientes:

- Número de puertos. Se consiguen de 12 o 24 puertos. Además de los puertos nominales (12 o 24), tienen otros puertos adicionales que sirven para conectar un equipo a una velocidad mayor o para unirlo a otro switch.

- También se le pueden conectar opcionalmente, módulos para interconexión por fibra óptica.

Ilustración17 SWITCH

Fuente: (Image Switch: BroadBand Buyer)

2.6.6 EL MODEM

Es un dispositivo que sirve para enviar una señal llamada modulada y mediante otra señal llamada portadora ella envía señales o recibe datos digitales que vienen siendo ceros y unos o llamado binario describe (Unidad III Dispositivos de Red: Tecnológico Nacional de México) y los trasforma a datos analógicos para mandar la información.

Ilustración 18 MODEM

Fuente: (Router Image: C.A. Combustibles Equipos de Computo y Accesorios)

2.6.7 TARJETA DE RED

Según (Unidad III Dispositivos de Red: Tecnológico Nacional de México),una tarjeta de red es el dispositivo que nos permite conectar la estación (ordenador u otro equipo de red) con el medio físico de transmisión (cable). Se le llama tarjeta porque normalmente se coloca en uno delos slots libres del PC, pero cada vez son más los equipos que la llevan incorporada en la placa base.

Las tarjetas de red pueden disponer de varios tipos de conectores. Los más habituales son el tipo BNC y el RJ-45, para conectar con cableado de tipo coaxial o UTP respectivamente.

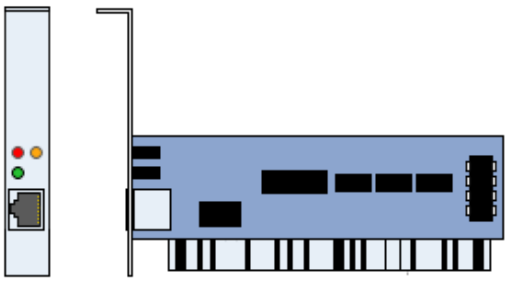


Ilustración 19TARJETA DE RED

Fuente:(CCM, CCM)

2.7 SOFTWARE LIBRE

«Software libre» es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir,

estudiar, modificar y mejorar el software describe (Free Software Foundation, 2016). Es decir, el «software libre» es una cuestión de libertad, no de precio. Para entender el concepto, piense en «libre» como en «libre expresión», no como en «barra libre» enfatiza (Free Software Foundation, 2016). En inglés a veces decimos «libre software», en lugar de «free software», para mostrar que no queremos decir que es gratuito.

Promovemos estas libertades porque todos merecen tenerlas. Con estas libertades, los usuarios (tanto individualmente como en forma colectiva) controlan el programa y lo que este hace. Cuando los usuarios no controlan el programa, decimos que dicho programa «no es libre», o que es «privativo». Un programa que no es libre controla a los usuarios, y el programador controla el programa, con lo cual el programa resulta ser un instrumento de poder injusto.

Según la (Free Software Foundation, 2016), un programa es software libre si los usuarios tienen las cuatro libertades esenciales:

- La libertad de ejecutar el programa como se desea, con cualquier propósito (libertad 0).

- La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera (libertad 1). El acceso al código fuente es una condición necesaria para ello.

- La libertad de redistribuir copias para ayudar a su prójimo (libertad 2).

- La libertad de distribuir copias de sus versiones modificadas a terceros (libertad 3). Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.

De acuerdo con (Free Software Foundation, 2016), un programa es software libre si otorga a los usuarios todas estas libertades de manera adecuada. De lo contrario no es libre. Existen

diversos esquemas de distribución que no son libres, y si bien podemos distinguirlos en base a cuánto les falta para llegar a ser libres, nosotros los consideramos contrarios a la ética a todos por igual.

2.7.1 LICENCIA DE SOFTWARE LIBRE

Como expresa (Siguencia Siguencia, Dscape.ups.edu.ec, 2011), una licencia de software es una autorización formal, o permisos que un autor de software da a quienes lo vayan a utilizar para la distribución, modificación, uso.

Principalmente en este contrato se acuerdan: la instalación, alcances de uso, reproducción, copias, etc.

2.7.2 LICENCIA GNU GPL (GENERAL PUBLIC LICENSE)

La licencia pública general (GPL) es la licencia que acompaña los paquetes distribuidos por el proyecto GNU y fue creada por Free Software Foundation en el año de 1989, brinda al usuario el derecho a usar un programa licenciado bajo GPL, modificarlo y distribuir las versiones modificadas de éste.

Según (Siguencia Siguencia, Dscape.ups.edu.ec, 2011) nadie debería ser restringido por el software que usan. Hay 4 libertades que cada usuario debe tener:

- La libertad de usar el software para cualquier propósito
- la libertad de cambiar el software para satisfacer sus necesidades
- La libertad de compartir el software con amigos vecinos.
- La libertad de compartir los cambios que haces.

2.7.3 LICENCIA CON COPYLEFT

El software protegido con Copyleft autoriza al usuario la libertad de la ejecución, copia, modificación y la distribución de las versiones modificadas, pero sin que se añada ninguna restricción para su utilización como dice (Siguencia Siguencia, Dscape.ups.edu.ec, 2011).

2.7.4 LICENCIA DE SOFTWARE CON DOMINIO PÚBLICO

Según (Siguencia Siguencia, Dscape.ups.edu.ec, 2011), el software de dominio público no está protegido por las leyes del derecho de autor, y pueden ser copiados sin costo, es un caso especial de software libre no protegido con copyleft, que significa que algunas copias o versiones modificadas no pueden ser libres completamente

2.7.5 LICENCIA OPEN SOURCE

Open Source o Código Abierto es un término que se aplica al Software distribuido bajo una licencia que le permita al usuario acceso al código fuente del Software, y además le permita estudiar y modificarlo con toda libertad, sin restricciones en el uso del mismo; y además le permita redistribuir, siempre y cuando sea de acuerdo con los términos de la licencia bajo la cual el Software original fue adquirido enfatiza (Siguencia Siguencia, Dscape.ups.edu.ec, 2011).

2.7.6 COPYRIGHT

El copyright es un derecho que tiene el autor de una obra de arte; es el medio por el que se establecen las condiciones de uso y comercialización de esta obra. El copyright es solo una parte (la parte “patrimonial”) del derecho de autor menciona (Siguencia Siguencia, Dscape.ups.edu.ec, 2011).

2.7.7 VENTAJAS DEL SOFTWARE LIBRE

Empleando las palabras de (Medina, 2012), las ventajas del software libre son:

- Libre Uso. Cualquier persona puede disponer del software libre bajo las condiciones de la licencia.

- Bajo Costo. Es gratuito.

- Existe Libertad de Conocimiento y trabajo cooperativo entre sus usuarios lo que permite una mayor innovación tecnológica.

- Rápida corrección de errores facilitado por el trabajo comunitario a través de Internet y de su libre acceso al código fuente.

- Total, independencia de un proveedor. El usuario puede administrar libremente su crecimiento y operación con total autonomía.
- Independencia de las condiciones del mercado. A salvo de cambios drásticos por parte del proveedor o modificaciones que realice por las condiciones del mercado o baja rentabilidad.

- Contribuye a la formación de profesionales y el desarrollo de la industria local, generando conocimiento y trabajo).

- Facilidad para personalizar el software de acuerdo a las necesidades del usuario.
- Posibilidad de traducir el mismo a cualquier idioma, inclusive a una lengua regional o indígena.

- Independencia tecnológica de los Estados con respecto a grandes grupos económicos.

- Fácil acceso por parte del sector educativo público y privado.

- Mayor seguridad y privacidad de los datos. Disminuye los riesgos de filtración, aumenta la imposibilidad de acceso y manipulación de los datos críticos del Estado.

- Asegura la durabilidad de la información y su migración, gracias al acceso al código fuente.

- Disminuye los riesgos de "puertas traseras" que introduzcan códigos maliciosos o de espionaje.

- El conocimiento de códigos fuente permite la rápida solución a funcionamientos erróneos.

- Elimina el sistema operativo mono usuario. Ya que permite el uso y trabajo de varios usuarios al mismo tiempo.

- Elimina el derecho exclusivo de la innovación.
- Abre la posibilidad del trabajo compartido entre diferentes empresas o dependencias de gobierno.

- Elimina la inseguridad ante cierre de compañías de provisión o discontinuidad del producto.

- No depende de prácticas monopólicas.

2.7.8 DESVENTAJAS DEL SOFTWARE LIBRE

Empleando las palabras de(Medina, 2012) las desventajas del software libre son:

- Dificultad en el intercambio de archivos (doc. de texto), dan errores o se pierden datos.

- Mayor dificultad en la instalación y migración de datos para el usuario común.

- Desconocimiento. El usuario común está muy familiarizado con los soportes de Microsoft, lo que hace elevar el costo de aprendizaje.

- Ausencia de garantía. El software libre no se hace responsable por los daños.

- Para su configuración se requieren conocimientos previos de funcionamiento del sistema operativo.

- Por lo general para su implementación se necesitan conocimiento previo de programación.

- Se debe monitorear en forma constante la corrección de errores por Internet.

- No existe un control de calidad previo.

- Hay aplicaciones específicas que no se encuentran en el software libre.
- Baja expansión de su uso en centros educativos.

- Baja difusión en publicaciones.

- En ambientes de red todavía hay software propietario con mejores desempeños

2.8 **SERVIDOR WEB**

De acuerdo con (Cases, 2014), un servidor Es un programa especialmente diseñado para transferir datos de hipertexto, es decir, páginas web con todos sus elementos (textos, widgets, banners, etc). Estos servidores web utilizan el protocolo http.

Expresa (Cases, 2014) que los servidores web están alojados en un ordenador que cuenta con conexión a Internet. El web Server, se encuentra a la espera de que algún navegador le haga alguna petición, como, por ejemplo, acceder a una página web y responde a la petición, enviando código HTML mediante una transferencia de datos en red.

Un servidor web recibe peticiones de clientes y responde con el envío de ficheros solicitados, texto plano (html, php) o binarios (gif, jpeg).

Permanentemente escucha las peticiones de conexión de los clientes en determinados puertos: 80 para HTTP, 443 para el HTTPS.(Eduard)

La atención a la petición del cliente consiste en buscar el archivo solicitado. Si lo encuentra, lo transmite; sino envía un mensaje de error. (Eduard)

El servidor web comprueba si el usuario tiene acceso a los documentos.(Eduard)

2.8.1 FUNCIONALIDADES DE UN SERVIDOR WEB

En la opinión de (Cases, 2014) las funcionalidades de un servidor Web son:

- Atender de manera eficiente, ya que puede recibir un gran número de peticiones HTTP, incluyendo una ejecución multitarea ya que pueden darse peticiones simultáneas. Cualquier petición compleja (por ejemplo, con acceso a base de datos) dejaría colapsado el servicio.

- Restricciones de acceso a los ficheros que no se quieran 'exponer', gestión de autenticaciones de usuarios o filtrado de peticiones según el origen de éstas.

- Manejar los errores por páginas no encontradas, informando al visitante y/o redirigiendo a páginas predeterminadas.

- Gestión de la información a transmitir en función de su formato e informar adecuadamente al navegador que está solicitando dicho recurso.

- Gestión de logs, es decir almacenar las peticiones recibidas, errores que se han producido y en general toda aquella información que puede ser registrada y analizada posteriormente para obtener las estadísticas de acceso al sitio web.

2.8.2 SERVIDORES WEB MÁS USADOS

Los servidores web más utilizados según (LÓPEZ PINO, 2010) son los siguientes:

- **Apache**: Es el servidor más utilizado, aunque ha vivido tiempos mejores. Parte de su éxito se debe a que es multiplataforma y a su estructura modular, que permite emplear diversos lenguajes en el lado del servidor (PHP, Python y Perl principalmente), así como incorporar características como la compresión de datos, las conexiones seguras y la utilización de URLs amigables.

- **Microsoft IIS**: A pesar de haber superado los momentos en que era más conocido por sus vulnerabilidades que por sus características, IIS ha perdido mercado en los últimos años. Es el segundo servidor web más usado y cuenta con un buen número de módulos, pero también con el gran handicap de funcionar únicamente en Windows.

- **Google Web Server**: El tercero más utilizado, conocido como GWS, es una gran incógnita. Google no publica apenas información sobre él y se rumorea que puede ser una versión adaptada de Apache. Obviamente, la gran cantidad de dominios que emplean este servidor no pertenecen todos a Google, sino que la mayoría son de compañías que emplean sus servicios como Blogger o App Engine.

- **Nginx**: Es un servidor web ligero que funciona en múltiples plataformas (entre las que se encuentran Windows Linux y Mac OS X). Es usado por algunos sitios importantes como Wordpress.com o Hulu.

- **Lighttpd**: Es el otro gran servidor ligero, que permite usar menos cantidad de memoria y CPU. También es empleado por sitios con mucho tráfico como YouTube, Wikimedia, ThePirateBay, etc.

2.8.3 PROTOCOLO HTTP

El protocolo de transferencia de hipertexto HTTP (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW).

Detalla (Profesorado, s.f.)Cuandose escribe una URL, por ejemplo, como ésta "http://www.prueba.com/index.html", el navegador interpreta tres partes:

- HTTP (protocolo).
- www.prueba.com (nombre del servidor).
- index.html (nombre del archivo especificado).

Una vez analizadas estas partes, el navegador comunica con un servidor de nombres (DNS) y se conecta con el servidor.

Normalmente, para este proceso utilizamos el protocolo HTTP, que pasamos a detallar a continuación.

Comenzaremos por decir que HTTP significa "Protocolo de trasferencia de hipertexto", además pertenece al grupo TCP/IP y se creó fundamentalmente para publicar páginas HTML. Es uno de los protocolos más utilizados actualmente.

Define (Profesorado, s.f.) Que Su funcionamiento básico es el siguiente: Un navegador manda una solicitud GET al servidor y pide un archivo, el servidor responde enviando al navegador el código de ese archivo, que posteriormente es descifrado por el navegador.

Expresa (Profesorado, s.f.)QueHTTP utiliza tres tipos de mensajes para enviar la información y recibirla del navegador.

- GET
- POST
- PUT

GET: se trata de un mensaje con solicitud de datos por parte del cliente, es decir, un navegador web envía el mensaje GET para solicitar páginas al servidor.

POST y PUT: estos dos tipos de mensajes son utilizados por el servidor para enviar información al navegador web. En concreto, "Post" incluye la información en el mensaje enviado al servidor y "Put" carga el contenido en el servidor.

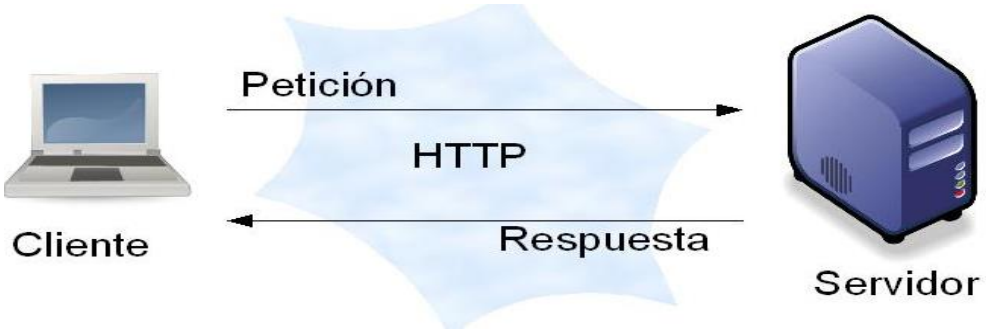


Ilustración 20 Protocolo HTTP

Fuente:(Profesorado, s.f.)

2.9 FUNCIONAMIENTO DE LA ARQUITECTURA CLIENTE/SERVIDOR

Ilustración 21 Arquitectura Cliente Servidor

Elaborado por: Autores

Según (Profesorado, s.f.) El funcionamiento de la Arquitectura cliente servidor es el siguiente:

- El usuario especifica en el cliente web la URL de la página que desea consultar.
- El cliente establece la conexión con el servidor web mediante internet y solicita la página deseada.
- El servidor busca la página solicitada en su sistema de ficheros. Si la encuentra la transfiere, sino devuelve un código de error.
- El cliente interpreta el código HTML y muestra la página al usuario.
- Se cierra la conexión.
- La conexión siempre se libera al terminar la transmisión de la página.

2.10 **SITIO WEB**

2.10.1 DEFINICIÓN

Un sitio web es un conjunto de páginas web desarrolladas en código html, relacionadas a un dominio de Internet el cual se puede visualizar en la World Wide Web (www) mediante los navegadores web o también llamados browser como ser Chrome, Firefox, Edge, Opera entre otros define (Pairuna, 2016).

Cada página web perteneciente al sitio web tiene como objetivo publicar contenido, y este contenido podrá ser visible o no al público.

2.10.2 CLASIFICACIÓN DE SITIOS WEB

Según (Pairuna, 2016) clasifica los sitios web de dos tipos:

Sitios Web Estáticos: Se denomina sitio web estático a aquellos que no acceden a una base de datos para obtener el contenido. Por lo general un sitio web estático es utilizado cuando el propietario del sitio no requiere realizar un continuo cambio en la información que contiene cada página.

Sitios Web Dinámicos: Por el contrario, los sitios web dinámicos son aquellos que acceden a una base de datos para obtener los contenidos y reflejar los resultados obtenidos de la base de datos, en las páginas del sitio web. El propietario del sitio web podrá agregar, modificar y eliminar contenidos del sitio web a través de un "sistema web", generalmente con acceso restringido al público mediante usuario y contraseña, el cual se denomina BACK END.

Se asume que, a la hora de contratar el desarrollo de un sitio web, el propietario, especificará al desarrollador web, la cantidad de páginas que contendrá el sitio, discriminando si son dinámicas o estáticas.

2.10.3 NECESIDAD DE UN SITIO WEB

Internet es la Red de Información y Publicidad más grande del mundo. Usted, sus emprendimientos o su empresa deben lograr presencia en internet, y para pertenecer a esta red de información, deben hacerlo a través de un sitio web, pero no todo lo que brilla es oro enfatiza (Pairuna, 2016). Para lograr con éxito el desarrollo de un sitio web, se debe considerar un profundo análisis de los objetivos del sitio, en el caso que se trate de una empresa, analizar la competencia y los clientes, y de esta manera determinar cómo imponerse en este mega entorno que no para de crecer, llamado Internet.

2.11 LENGUAJES DE DESARROLLO WEB

Desde los inicios del internet, surgieron diferentes demandas por los usuarios y se dieron soluciones mediante lenguajes estáticos. A medida que pasa el tiempo, las tecnologías de desarrollo han evolucionado y evolucionarán para dar solución a los nuevos problemas. Por

este motivo se desarrollaron nuevos lenguajes de programación para el desarrollo de web dinámicos que permitan interactuar con los usuarios.

2.11.1 LENGUAJE HTML

Lenguaje base porque desde los inicios del internet se han publicado sitios web gracias a este lenguaje, es un lenguaje estático para desarrollo de sitios web, donde los archivos pueden tener extensiones (HTML, HTML) da a conocer (Pérez Valdés, 2007). Desarrollado por World Wide Web Consorcium (W3C). Mediante un gráfico explicaremos la sintaxis de un documento HTML.

```
<html> (Inicio del documento HTML)
<head>
( Cabecera )
</head>
<body>
( Cuerpo )
</body>
</html>

<b>  </b> Negrita
<p>  </p> Definir parrafo
<etiqueta> Apertura de la etiqueta
</etiqueta> Cierre de la etiqueta
```

Ilustración 22 Sintaxis documento HTML

Elaborado por: Autores

2.11.2 LENGUAJE JAVASCRIPT

Según (Pérez Valdés, 2007) es un lenguaje interpretado y no necesita compilación, utilizado principalmente en páginas web. Similar a Java, pero no es orientado a objetos ni permite herencia, la mayoría de los navegadores en sus últimas versiones permiten interpretar código JavaScript.

El código JavaScript puede ser integrado dentro de nuestras páginas web o proyectos que vayamos a realizar. Para evitar incompatibilidades el W3C diseñó un estándar denominado

DOM. A continuación, vamos a detallar con un ejemplo la sintaxis JavaScript con la siguiente imagen:

```
<script type="text/javascript"> ... </script>
```

Ilustración 23 Sintaxis JavaScript

Elaborado por: Autores

2.11.3 LENGUAJE PHP

De acuerdo con (Pérez Valdés, 2007), PHP es un lenguaje Script interpretado del lado del servidor para la generación de páginas web Dinámicas, embebidas en páginas HTML y ejecutadas en el servidor. Este lenguaje no necesita ser compilado para ejecutarse. Necesita tener instalado un servidor web como Apache, Nginx o IIS con librerías de PHP para poder funcionar señala (Pérez Valdés, 2007).

A continuación, se detalla mediante un gráfico la sintaxis básica del lenguaje:

```
<?php
$mensaje = “Hola”;
echo $mensaje;
?>
```

Ilustración 24 Sintaxis básica del lenguaje PHP

Elaborado por: Autores

2.11.4 LENGUAJE ASP.

Es una tecnología del lado de servidor desarrollada por Microsoft para el desarrollo de sitio web dinámicos. ASP significa en inglés (Active Server Pages), fue liberado por Microsoft en 1996. Las páginas web desarrolladas bajo este lenguaje es necesario tener instalado Internet Information Server (IIS) expresa (Pérez Valdés, 2007).

2.11.5 LENGUAJE JSP.

Es un lenguaje para la creación de sitios web dinámicos, acrónimo de Java Server Pages. Está orientado a desarrollar páginas web en Java. JSP es un lenguaje multiplataforma. Creado para ejecutarse del lado del servidor.

Desarrollado para la creación de aplicaciones web potentes enfatiza (Pérez Valdés, 2007). Posee un motor de páginas basado en los servlets de Java. Para su funcionamiento se necesita tener instalado un servidor Tomcat.

```
<%= new java.util.Date() %>
```

Ilustración 25Sintaxis básica del lenguaje JSP

Elaborado por: Autores

2.11.6 LENGUAJE PYTHON

Es un lenguaje de programación creado en el año 1990 por Guido Van Rossum, es el sucesor del lenguaje de programación ABC. Python es comparado habitualmente con Perl. Los usuarios lo consideran como un lenguaje más limpio para programar. Permite la creación de todo tipo de programas incluyendo los sitios web.

(Pérez Valdés, 2007)Dice que su código no necesita ser compilado, por lo que se llama que el código es interpretado. Es un lenguaje de programación multiparadigma, lo cual fuerza a que los programadores adopten por un estilo de programación particular, a continuación (Pérez Valdés, 2007) detalla características básicas del lenguaje:

- Programación orientada a objetos.
- Programación estructurada.
- Programación funcional.
- Programación orientada a aspectos.

```
def dibujar_muneco(opcion):
    if opcion == 1:
        C.create_line(580, 150, 580, 320, width=4, fill="blue")
        C.create_oval(510, 150, 560, 200, width=2, fill='PeachPuff')
```

Ilustración 26Sintaxis básica del lenguaje Python

Elaborado por: Autores

2.11.7 LENGUAJE RUBY

Es un lenguaje interpretado de muy alto nivel y orientado a objetos. Desarrollado en el 1993 por el programador japonés Yukihiro "Matz" Matsumoto. Su sintaxis está inspirada en Phyton, Perl. Es distribuido bajo licencia de software libre.

(Pérez Valdés, 2007) Dice que Ruby es un lenguaje dinámico para una programación orientada a objetos rápida y sencilla. Para los que deseen iniciarse en este lenguaje pueden encontrar un tutorial interactivo de ruby. Se encuentra también a disposición de estos usuarios un sitio con informaciones y cursos en español.

```
puts "hola"
```

Ilustración 27 Sintaxis básica del lenguaje Ruby

Elaborado por: Autores

3 MARCO METODOLÓGICO

3.1 CONFIGURACIONES DE LA RED

Luego del estudio realizo en la red del dispensario “SAGRADA FAMILIA” se reestructura la misma con la integración de los equipos adquiridos cambiando el funcionamiento lógico al ser administrado el núcleo de la red por un router administrativo gestionado a la necesidad y requerimientos de los usuarios de la red interna

3.1.1 CONFIGURACIÓN ROUTER CISCO

Pantalla de ingreso principal al router cisco

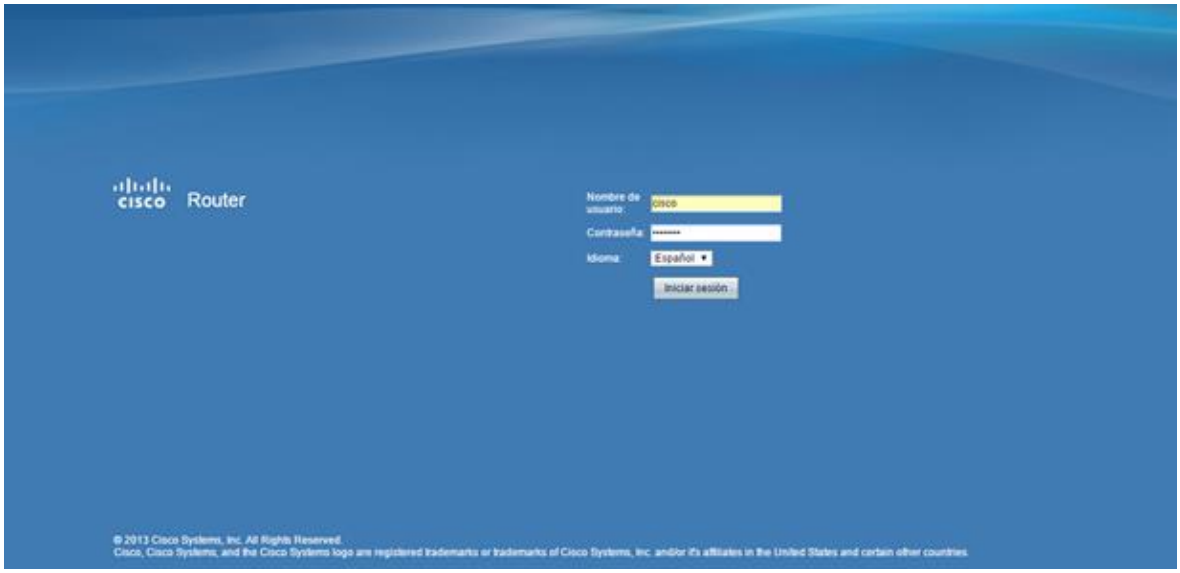


Ilustración 28 Pantalla loginRouter Cisco

Elaborado por: Autores

Menú principal de configuración router cisco

Ilustración 29 Menú Principal Router

Elaborado por: Autores

3.1.2 CONFIGURACIÓN DE LA INTERFAZ WAN

Como podemos ver las opciones del ajuste WAN existen 4 interfaces con las que se puede configurar, en el este caso solo se va a configurar una interfaz que es estática, la que va a tener salida mediante el proveedor de internet corporativo.

A continuación, se aprecia detalladamente los ajustes de la conexión WAN, en el tipo de conexión WAN se elige Ip estática, Se especifica la dirección IP de la interface WAN, Mascara de subred (IPv4), Dirección de Gateway predeterminada, direcciones DNS (DomainNameSystem) primarias y secundarias. Toda esta información proporcionada por el ISP, definimos de manera automática el tamaño de la MTU (MaximumTransmissionUnit, unidad de transmisión máxima).

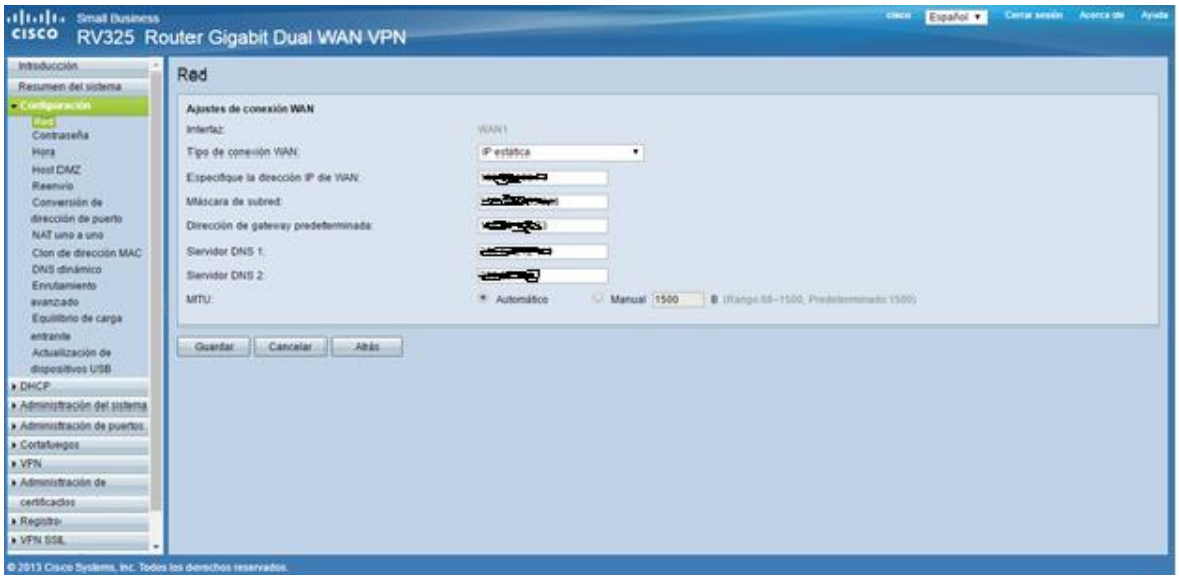


Ilustración 30 Configuración de la WAN

Elaborado por: Autores

3.1.3 CONFIGURACIÓN DE DHCP PARA LA RED INTERNA

En el menú lateral de las configuraciones del router donde se elige La opción configuración de DHCP (Dynamic Host Configuration Protocol)

Para configurar DHCP para IPv4 se debe de realizar lo siguiente:

- **Elegir la opción VLAN (virtual LAN)**.
  Crear un ID de la VLAN correspondiente donde se especifica la dirección IP del dispositivo que es la dirección IP de administración del equipo y la máscara de subred de la IP de administración del dispositivo.

- **Modo de operación del DHCP:**
  Servidor DHCP: transmite las solicitudes DHCP del cliente al servidor DHCP del dispositivo.

- **Tiempo de cesión de cliente**: El periodo de tiempo que los usuarios con una dirección IP asignada pueda permanecer conectado al router con la misma IP antes de ser reasignada, el valor predeterminado es de 1440 minutos es decir 24h.

- **Inicio de rango y Fin de rango:** Direcciones IP de inicio y de finalización generando un rango de direcciones IP que se pueden asignar dinámicamente de acuerdo al número y orden en el que los equipos se vayan conectando.

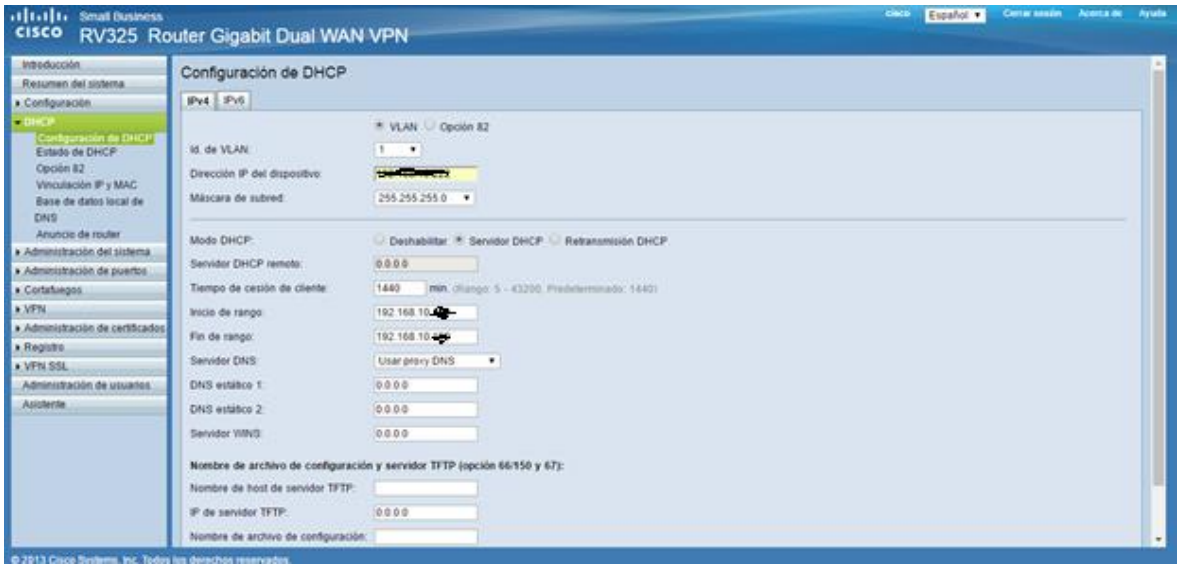


Ilustración 31 Configuración de la LAN DHCP

Elaborado por: Autores

3.1.4 CONFIGURACIÓN DE NAT UNO A UNO

La configuración de NAT uno a uno crea y asigna una dirección IP de WAN válida a las direcciones IP LAN mediante NAT. En este caso protegiendo a nuestro servidor LAN para evitar que sea detectado y posteriormente sea vulnerable a ataques.

Mediante esta configuración se reserva las direcciones IP interna a los que se desee llegar mediante NAT uno a uno.

Configuración- **NAT** uno a uno en el panel de navegación.
Para habilitar la función, se aplica la opción **Habilitar.**

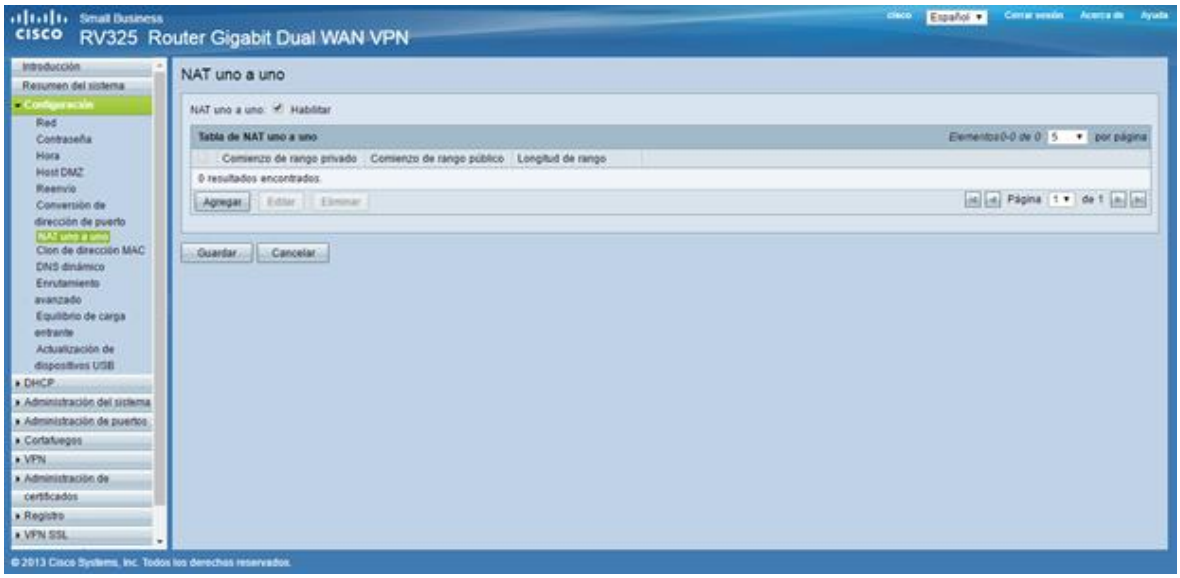


Ilustración 32 Habilitar NAT

Elaborado por: Autores

Para agregar una regla a la lista se debe especificar:

- **Comienzo de rango privado:** la dirección IP internas que se desea asignar al rango público.

- **Comienzo de rango público:** IP públicas que proporciona el ISP asignada para el servidor web.

- **Longitud de rango: se** asigna un rango único, de una dirección ubicando el número correspondiente.

Guardar, después de la configuración realizada.

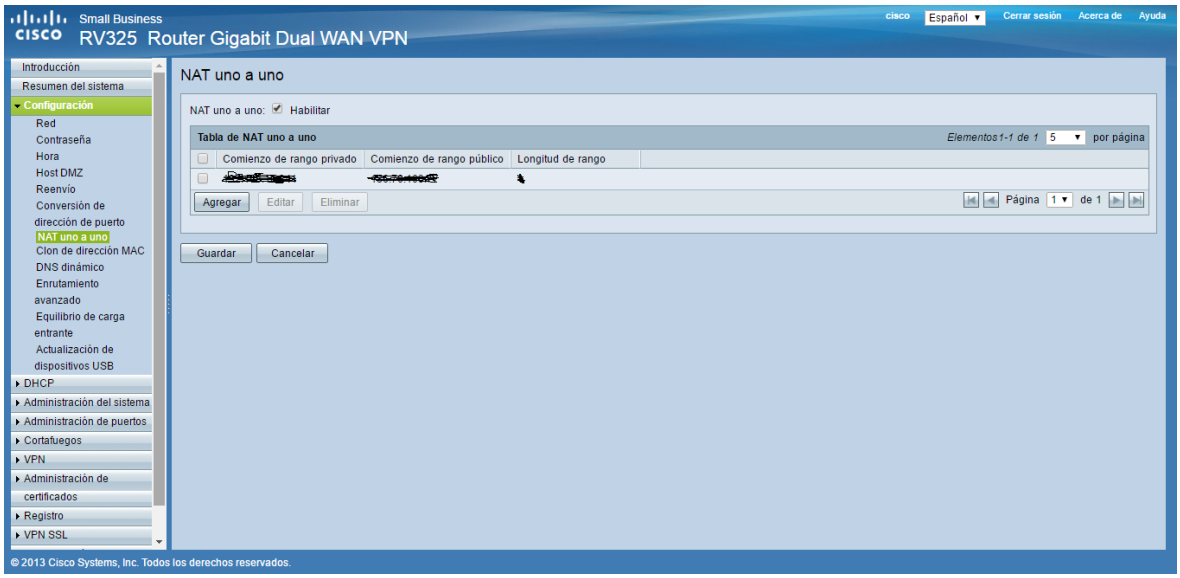


Ilustración 33 Configuración NAT uno a uno

Elaborado por: Autores

3.1.5 HABILITAR DMZ

Una dirección asignada a una DMZ es una subred que como característica está abierta al público, pero protegida tras un firewall. Una DMZ permite redirigir el tráfico que llega al puerto WAN a una dirección IP especificada en el servidor de la LAN. (Cisco C.)

Brindando seguridad si se produce un ataque en alguno de los nodos o reglas aplicadas en la DMZ, no tiene por qué afectar necesariamente a la red interna.

Para Configurar DMZ se realiza los siguientes pasos:

- Elija en Configuración> Red y seleccione la opción Habilitar DMZ.
- Aceptar los cambios.
- Seleccionar la interfaz de DMZ en los Ajustes de DMZ. Se despliega la ventana de edición de la conexión DMZ.
- Se especifica dirección interna del servidor web.
- Guardar cambios

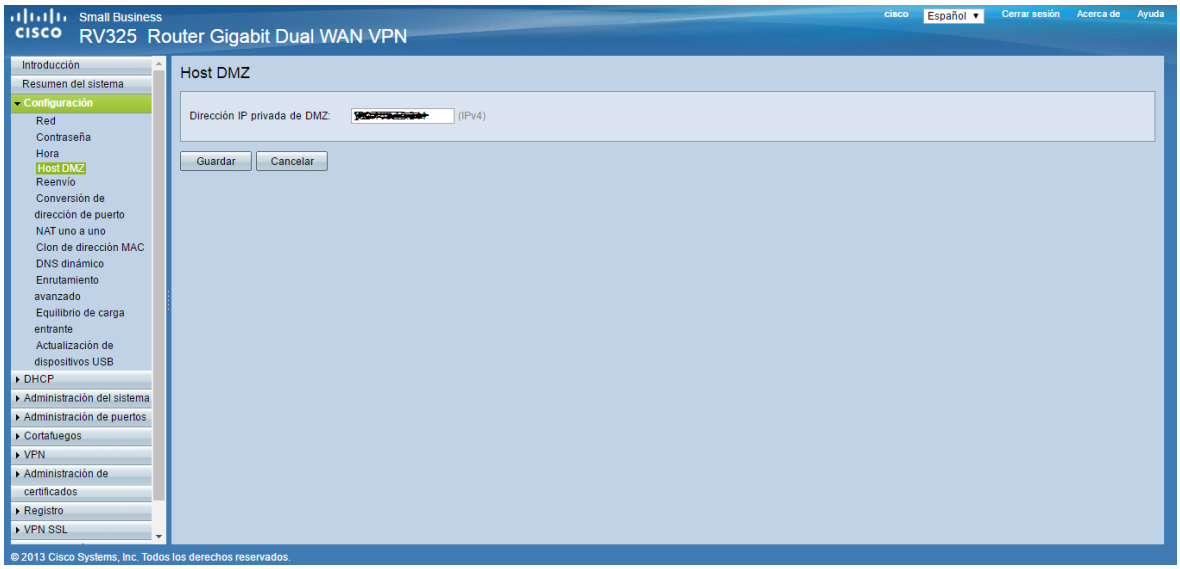


Ilustración 34 Configuración DMZ

Elaborado por: Autores

3.1.6 CONFIGURACIÓN DEL FIREWALL

El principal objetivo de la implementación de la configuración del firewall es controlar y filtrar el tráfico de llegada de la WAN y saliente mediante el análisis de los paquetes y la determinación de si se deben filtrar o no, mediante un conjunto de reglas o Access list.

Un firewall de red construye un puente entre una red interna que se considera segura y de confianza y otra red que suele ser externa y no se considera segura ni de confianza.

3.1.6.1 CONFIGURACIÓN GENERAL

La configuración general del firewall administra las funciones en seguridad que usan normalmente los navegadores y las aplicaciones.(Cisco C.)

Cortafuegos> **General** para desplegar el árbol de opciones.

3.1.6.2 ACTIVACIÓN DE LAS FUNCIONES DEL FIREWALL

Para activar el firewall, opción **Habilitar.** Las siguientes funciones:

- **SPI (inspección de paquetes con estado):** inspecciona el estado de las conexiones de red tanto el tráfico TCP y UDP que fluyen por la misma. El firewall actúa como un filtro de paquetes para los distintos tipos de conexiones. Son rechazados los paquetes que no coincidan con una conexión segura y conocida, especificadas en la red.

- **DoS (Denegación de servicio):** detecta intentos de saturar el servidor. Generalmente los ataques de denegación de servicio fuerzan el reinicio de los equipos propensos a ataque, consumiendo sus recursos de forma que no puedan cumplir de manera normal su funcionamiento.

- **Bloquear solicitud de WAN:** bloquea las solicitudes TCP y los paquetes ICMP, para evitar saturación de peticiones en nuestra red

- **HTTPS (Hypertext Transfer ProtocolSecure, protocolo seguro de transferencia de hipertexto):** es un protocolo de comunicaciones que garantiza la seguridad de las comunicaciones la versión segura de http que nos va a brindar la seguridad en funciones futuras de nuestro servidor web. En Internet se usa con mucha frecuencia.

3.1.7 RESTRICCIÓN DE LAS CARACTERÍSTICAS WEB

Se va restringir las características Web Java, Cookies, ActiveX o Acceso a servidores proxy HTTP, active la casilla correspondiente. Para permitir únicamente las características seleccionadas (Java, Cookies, ActiveX o Acceso a servidores proxy HTTP)(Cisco C.)

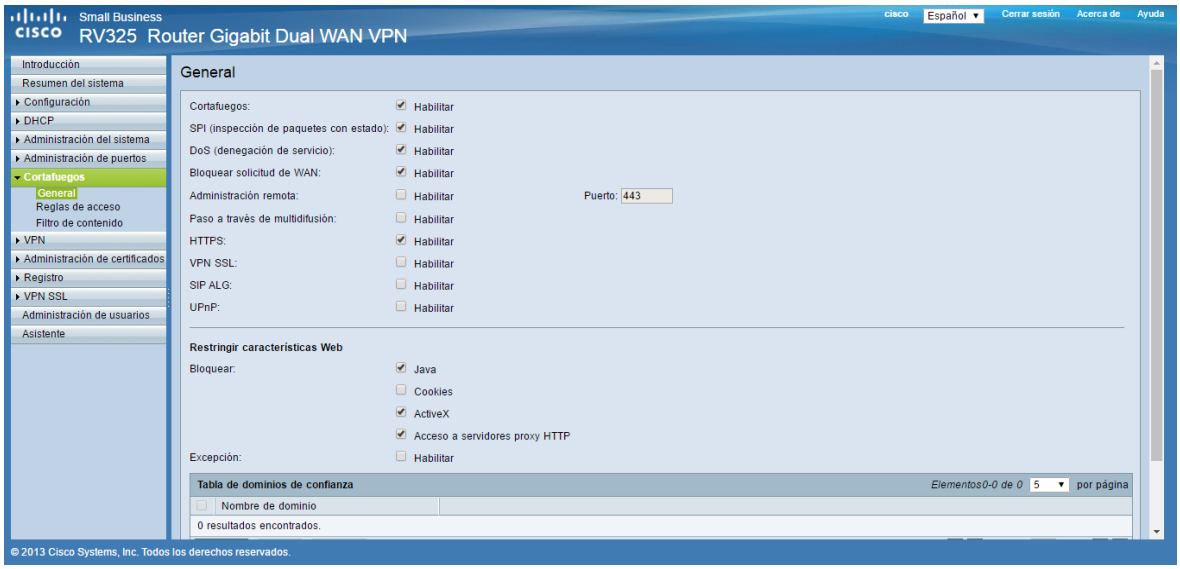


Ilustración 35 Configuración de Firewall

Elaborado por: Autores

3.2 INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR WEB

3.2.1 CONFIGURAR INTERFAZ DE RED ESTÁTICA

Para configurar la interfaz de red se especifica la ruta y se editar el archivo de configuración con el siguiente comando como detalla en la Ilustración 36.

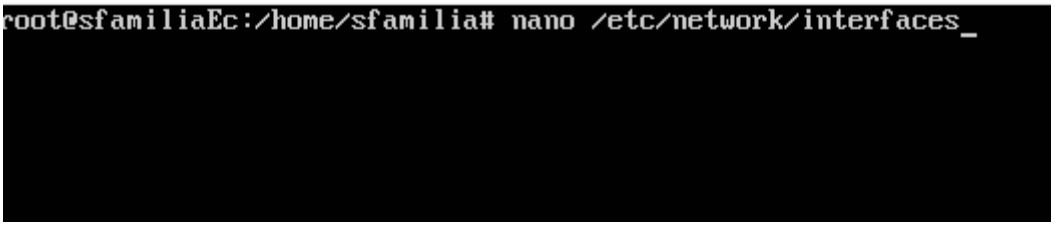


Ilustración 36 Configuración Interfaz de Red

Elaborado por: Autores

En la imagen se cambia la configuración de la interfaz DHCP de modo dinámico a estático, hay muchas opciones que pueden ser añadidas y personalizadas de acuerdo a la red donde vaya ser ubicado el servidor se abre el archivo ubicado en **/etc/network/interfaces**
yse añade las siguientes líneas que detalla la ilustración 37.

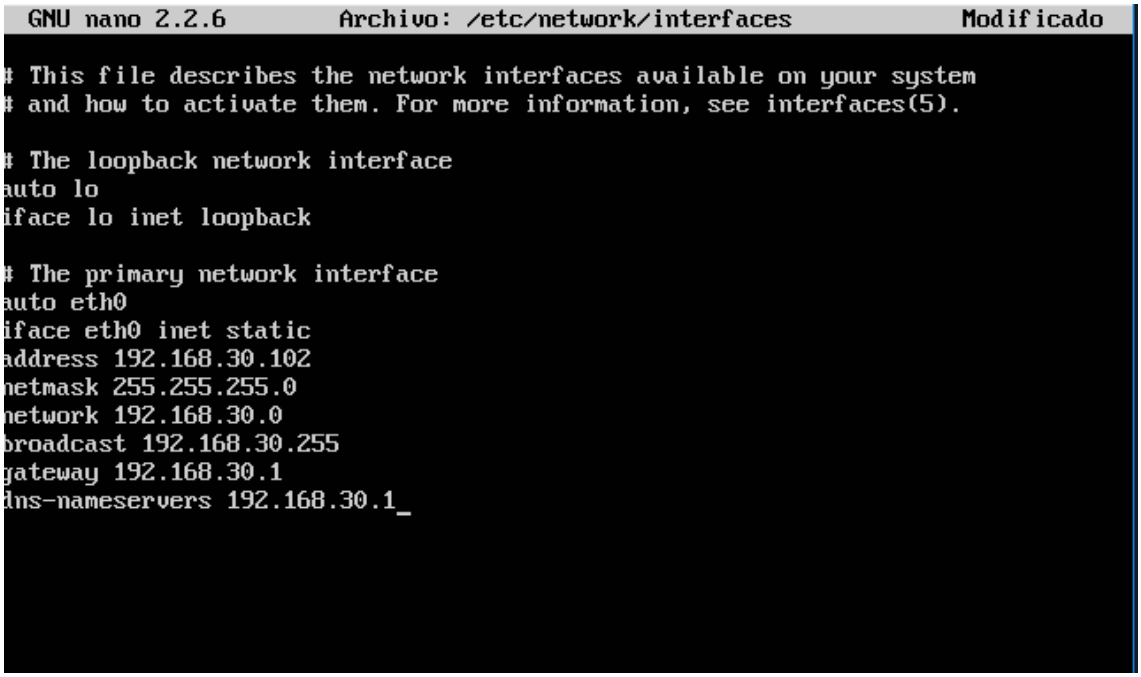


Ilustración 37 Configuración de interfaz de Red DHCP

Elaborado por: Autores

Una vez configurada la interfaz de red se añade las configuraciones DNS en el archivo ubicado en **/etc/resolv.conf** como detalla la ilustración 38.

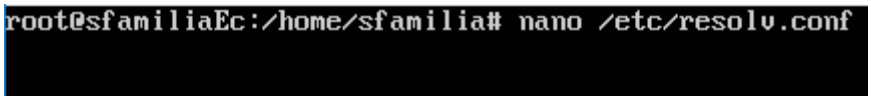


Ilustración 38 configuración /etc/resolv.conf

Elaborado por: Autores

En la Ilustración 39 que es la siguiente muestra el texto que se debe de ubicar en el archivo de configuración **resolv.conf.**

Ilustración 39 Configuración del DNS

Elaborado por: Autores

Después de configurar el nameserveres necesario reiniciar el servicio de red con el siguiente comando **/etc/init-d/networkingrestart.**

3.2.2 ACTUALIZAR SISTEMA:

Como prioridad se debe actualizar todo el sistema, es recomendable realizarlo frecuentemente ya que a diario se presentan fallas de seguridad y uno de los paquetes del sistema desactualizado puede convertirse en una amenaza.

Para actualizar se debe ejecutar dos comandos:

- **apt-getUpdate**
- **apt-getupgrade**

Primero se debe de actualizar los repositorios con el comando que detalla en la ilustración 40.

Ilustración 40 Actualización del Sistema

Elaborado por: Autores

En la ilustración 41 comparará las versiones instaladas con las disponibles y actualizará aquellas que estén obsoletas.

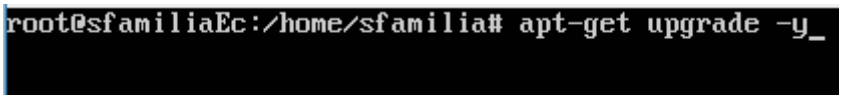


Ilustración 41 Versiones Instaladas Upgrade

Elaborado por: Autores

3.2.3 SECURIZADO DE LA CARPETA TEMPORAL

En este paso se crea y monta un sistema de archivos /tmppor separado con algunas restricciones. ¿Pero por qué se realiza esto? El directorio /tmpes donde se alojan los archivos temporales de las aplicaciones. Es posible que pueda ser usado para alojar ejecutables maliciosos para comprometer el servidor. De no asegurarse se pueden darse ataques como, por ejemplo:

- Procesos Maliciosos
- Ataques de Denegación de servicio
- Ejecución de scripts maliciosos

Lo que se consigue es montar la partición **/tmp** con **nosuid y noexec** que permite el bloqueo de la configuración de **SUID/SGID** y la posibilidad de ejecutar algún script malicioso, además crea la entrada correspondiente en **/etc/fstab**para montarlo en el booteo.

Para realizar esto se ejecutan los siguientes comandos en el siguiente orden:

- **dd if=/dev/zero of=/usr/tmpDISKbs=1024 count=2048000**

En la ilustración 42 muestra el comando que permite asegurar la carpeta temporal del sistema de operativo.

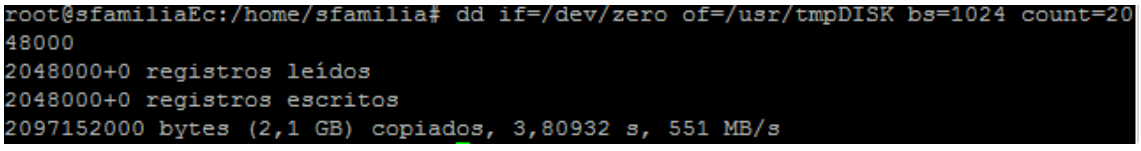


Ilustración 42 Seguridad Carpeta Temporal

Elaborado por: Autores

- **mkdir /tmpbackup**
- **cp -Rpf /tmp /tmpbackup**
- **mount -t tmpfs -o loop,noexec,nosuid,rw /usr/tmpDISK /tmp**
- **chmod 1777 /tmp**
- **cp -Rpf /tmpbackup/* /tmp/**
- **rm -rf /tmpbackup**
- **echo "/usr/tmpDISK /tmptmpfsloop,nosuid,noexec,rw 0 0" >> /etc/fstab**
- **sudo mount -o remount /tmp**
- **rm -rf /var/tmp**
- **ln -s /tmp /var/tmp**

3.2.4 SECURIZAR SSH

Para realizar una configuración segura del archivo de configuración **sshd_config** y proteger los accesos remotos al servidor, se edita las siguientes líneas del archivo ubicado en: **/etc/ssh/sshd_config,** como lo dice la ilustración 43.

Ilustración 43 Seguridad SSH

Elaborado por: Autores

Las siguientes líneas:

- Port 885
- Protocol 2
- ServerKeyBits 768
- LoginGraceTime 30
- PermitRootLogin no
- MaxAuthTries 4
- AllowUserssfamilia
- ClientAliveInterval 300
- ClientAliveCountMax 0
- HostbasedAuthentication no
- Banner /etc/issue
- UsePrivilegeSeparation yes
- KeyRegenerationInterval 3600

- SyslogFacility AUTH
- LogLevel INFO
- StrictModes yes
- RSAAuthentication yes
- PubkeyAuthentication yes
- IgnoreRhosts yes
- RhostsRSAAuthentication no
- HostbasedAuthentication no
- PermitEmptyPasswords no
- ChallengeResponseAuthentication no
- X11Forwarding no
- AllowTcpForwarding no
- PermitUserEnvironment no
- X11DisplayOffset 10
- PrintMotd no
- PrintLastLog yes
- TCPKeepAlive yes
- AcceptEnv LANG LC_*
- Subsystem sftp /usr/lib/openssh/sftp-server
- UsePAM yes
- MaxStartups 2

Algunas de las opciones:

- **Port 885:** Aquí se configura el puerto donde se va a realizar las conexiones remotas. Muchos de los ataques de fuerza bruta van dirigidos al puerto por defecto que es el 22.

- **Protocol2:** Permite al servidor que solo use este protocolo ya que la versión 1 es vulnerable a diversos ataques.

- **PermitRootLogin:**no le permitirá al usuario root hacer login remoto a este servidor.

- **PasswordAuthentication:** Elimina la autenticación por contraseñas convencionales.

- **LoginGraceTime 30:** El tiempo de gracia de inicio de sesión es un periodo de tiempo en el que un usuario puede estar conectado, pero no ha comenzado el proceso de autenticación. De forma predeterminada, sshd permitirá a un usuario conectado a esperar 120 segundos (2 minutos) antes de empezar a autenticar. Al acortar este tiempo, puede disminuir las posibilidades de que alguien intente un ataque de fuerza bruta contra el servidor SSH de ser exitoso.

- **MaxAuthTries 4:** Se fija la cantidad máxima de intentos de login.

- **AllowUsersUsername:** Los usuarios pueden hacer login al servidor vía ssh y se puede setear un intervalo de tiempo de espera, se ha seteado el valor de (300 seg = 5 minutos), después de que el intervalo pase el usuario va a salir de sesión.

- **ClientAliveInterval 300:** El usuario puede iniciar sesión con el servidor a través de SSH y se puede establecer un intervalo de tiempo de espera para evitar la sesión ssh sin vigilancia.

Las demás opciones ponen ciertas restricciones en lo que se puede hacer con ssh.

3.2.5 INSTALAR FAIL2BAN

Es una herramienta que actúa bloqueando las conexiones remotas que hacen intento de acceso por fuerza bruta. Al momento de generarse una incidencia o posible ataque, esta crea reglas en el iptables para bloquear la ip atacante.(Soto, 2015)

En la línea de comandos se digita lo siguiente:

- **apt-getinstallsendmail.**
- **Apt-getinstall fail2ban**

```
root@sfamiliaEc:/home/sfamilia# apt-get install fail2ban
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  python-pyinotify whois
Paquetes sugeridos:
  python-gamin mailx python-pyinotify-doc
Se instalarán los siguientes paquetes NUEVOS:
  fail2ban python-pyinotify whois
0 actualizados, 3 se instalarán, 0 para eliminar y 3 no actualizados.
Necesito descargar 184 kB de archivos.
Se utilizarán 927 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://ec.archive.ubuntu.com/ubuntu/ trusty/universe fail2ban all 0.8.11-1
 [129 kB]
Des:2 http://ec.archive.ubuntu.com/ubuntu/ trusty/main python-pyinotify all 0.9.
4-1build1 [24,5 kB]
Des:3 http://ec.archive.ubuntu.com/ubuntu/ trusty/main whois amd64 5.1.1 [30,2 k
B]
Descargados 184 kB en 1seg. (123 kB/s)
```

Ilustración 44apt-getinstall fail2ban

Elaborado por: Autores

3.2.6 INSTALAR APACHE

Para instalar el servidor web apache se debe escribir en la línea de comandos lo siguiente

- **apt-getinstall apache2**

La ilustración 45 muestra la ejecución del comando y el proceso de instalación de manera breve.

```
root@sfamiliaEc:/home/sfamilia# apt-get install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  apache2-bin apache2-data libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap ssl-cert
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine apache2-suexec-custom apache2-utils
  openssl-blacklist
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap ssl-cert
0 actualizados, 8 se instalarán, 0 para eliminar y 3 no actualizados.
Necesito descargar 1.283 kB de archivos.
Se utilizarán 5.348 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Ilustración 45Install Apache

Elaborado por: Autores

Al reiniciar el servidor apache se refleja en la consola un Warning AH00558 como lo detalla la ilustración 46.

```
 * Starting web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified doma
in name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress th
is message
 *
```

Ilustración 46Warming Apache AH00558

Elaborado por: Autores

Para solucionar el Warningse busca el archivo de configuración de apache ubicado en: **/etc/apache2/apache.conf.**y se añade la siguiente línea al final del documento como se describe en la ilustración 47.

```
  GNU nano 2.2.6       Archivo: /etc/apache2/apache2.conf          Modificado


# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

ServerName localhost
```

Ilustración 47 Solución Warming

Elaborado por: Autores

Se reinicia el servicio de apache2 con el comando service apache2 restart, como se ve en la ilustración 48 el mensaje de error ha desaparecido.

```
root@sfamiliaEc:/home/sfamilia# service apache2 restart
 * Restarting web server apache2                                      [ OK ]
root@sfamiliaEc:/home/sfamilia#
```

Ilustración 48RestartService Apache

Elaborado por: Autores

Una vez reiniciado el servicio de apache se verifica si el servicio está funcionando consultamos la dirección ip del servidor web en el navegador ej. 192.168.50.102 y se podrá visualizar la página de inicio de apache2 como lo muestra la ilustración 49.

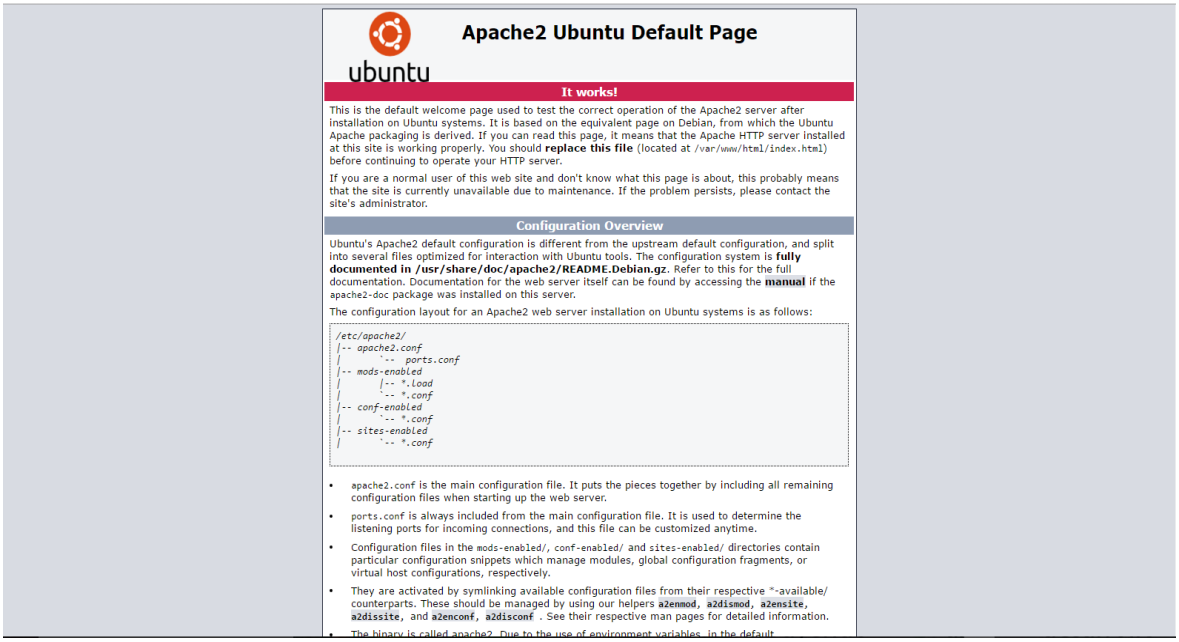


Ilustración 49 Página de inicio Apache

Elaborado por: Autores

3.2.7 CONFIGURAR Y OPTIMIZAR PHP

La mejor manera de configurar y optimizar PHP es cambiando el archivo de configuración PHP.ini por una segura ejecuta el comando **apt-getinstall php5 php5-cli php-pear,** Como lo demuestra la ilustración 50.

```
root@sfamiliaEc:/home/sfamilia# apt-get install php5 php5-cli php-pear
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  libapache2-mod-php5 php5-common php5-json php5-readline
```

Ilustración 50 Configuración PHP Instalación

Elaborado por: Autores

Adicional a eso se ejecuta el comando **apt-getinstall php5-mysql python-mysqldb** Comose muestra en la ilustración 51.

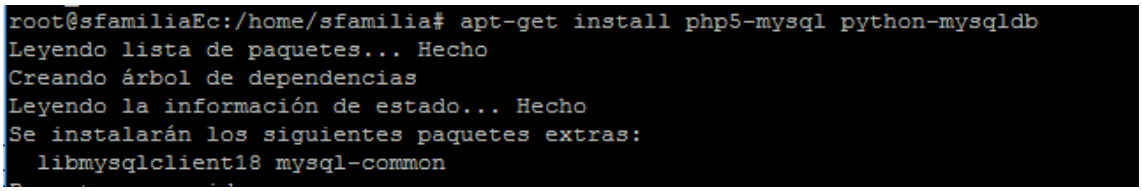


Ilustración 51 Instalación PHP-MySql

Elaborado por: Autores

En esta configuración quedan deshabilitadas algunas funciones que pueden llevar a php a mostrar **información sensible** tanto de la configuración del lenguaje php como del servidor. La más importante es la directiva **disable_functions**, donde se deshabilitan todas las funciones consideradas como peligrosas en PHP y que pueden llevar a ejecutar algún ataque y comprometer el servidor.

disable_functions = proc_open, popen, disk_free_space, diskfreespace, set_time_limit, leak, tmpfile, exec, system, shell_exec, passthru, show_source, system, phpinfo, pcntl_alarm, pcntl_fork, pcntl_waitpid, pcntl_wait, pcntl_wifexited, pcntl_wifstopped, pcntl_wifsignaled, pcntl_wexitstatus, pcntl_wtermsig, pcntl_wstopsig, pcntl_signal, pcntl_signal_dispatch, pcntl_get_last_error, pcntl_strerror, pcntl_sigprocmask, pcntl_sigwaitinfo, pcntl_sigtimedwait, pcntl_exec, pcntl_getpriority, pcntl_setpriority

Ilustración 52Disable_Functions

Elaborado por: Autores

Según su aplicación es posible que requieran hacer uso de algunas de estas funciones, pero se recomienda que se busque una alternativa o se habiliten en caso de ser estrictamente necesario.

Por último, se reinicia el servicio apache2 mediante el siguiente comando.

- **service apache2 restart**

3.2.8 SECURIZAR Y OPTIMIZAR APACHE

Según (Soto, 2015), se debe reemplazar la configuración por defecto de apache por una configuración más segura, el contenido del archivo imagen 53,54,55:

```
Mutex file:${APACHE_LOCK_DIR} default
PidFile ${APACHE_PID_FILE}
Timeout 300
KeepAlive On
MaxKeepAliveRequests 1000
KeepAliveTimeout 2

<IfModule mpm_prefork_module>
    StartServers 1
    MinSpareServers 3
    MaxSpareServers 6
    MaxClients 24
    MaxRequestsPerChild 3000
</IfModule>

<IfModule mpm_worker_module>
    StartServers 2
    MinSpareThreads 25
    MaxSpareThreads 75
    ThreadLimit 64
    ThreadsPerChild 25
    MaxClients 150
    MaxRequestsPerChild 0
</IfModule>

<IfModule mpm_event_module>
    StartServers 2
    MinSpareThreads 25
    MaxSpareThreads 75
    ThreadLimit 64
    ThreadsPerChild 25
    MaxClients 150
    MaxRequestsPerChild 0
</IfModule>
```

Ilustración 53Configuración securizar y optimizar Apache

Elaborado por: Autores

```
User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}
AccessFileName .htaccess
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
    Satisfy all
</Files>

<Directory />
    Options -Indexes -Includes -ExecCGI
<LimitExcept GET POST HEAD>
      deny from all
    </LimitExcept>
</Directory>

HostnameLookups Off
ErrorLog ${APACHE_LOG_DIR}/error.log
LogLevel warn

# Include module configuration:
Include mods-enabled/*.load
Include mods-enabled/*.conf

# Include ports listing
Include ports.conf

LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
```

Ilustración 54 Configuración securizar y optimizar Apache

Elaborado por: Autores

```
<IfModule security2_module>
    Include /usr/share/modsecurity-crs/*.conf
    Include /usr/share/modsecurity-crs/base_rules/*.conf
</IfModule>

LogFormat "%{User-agent}i" agent

IncludeOptional conf-enabled/*.conf
IncludeOptional sites-enabled/*.conf

ServerSignature Off
ServerTokens Prod

ErrorDocument 404 "Archivo no encontrado"
ErrorDocument 500 "Tareas de mantenimiento en curso. Disculpe las molestias"
FileETag None
TraceEnable off
ServerName localhost
```

Ilustración 55 Configuración securizar y optimizar Apache

Elaborado por: Autores

Según (Soto, 2015), se debe de agregar algunas directivas de seguridad como, por ejemplo:

ServerSignature Off

ServerTokensProd

Con estas directivas se protege de divulgar informaciones sensibles del servidor apache que luego pueden ser utilizadas para crear un vector de ataque.

<Files ~ "^\.ht">
Order allow, deny
Deny from all
Satisfyall
</Files>

Aquí se protege el archivo .htaccess en caso de que se esté utilizando.

Options -Indexes -Includes –ExecCGI
deny from all

Con esta sección se controla que se puede hacer desde el directorio raíz y limitando los accesos exclusivamente a GET, POST y HEAD.

FileETagNone
TraceEnable off

Estas directivas protegen contra ataques para conseguir información sensible o ataques para robar información de cookies.

-Se Inicia el mod_rewrite de apache: a2enmod rewrite
-Reiniciar el servidor ejecutando el siguiente comando
-service apache2 restart

3.2.9 MOD EVASIVE DE APACHE

-apt-get install libapache2-mod-evasive
-mkdir /var/log/mod_evasive
-chownwww-data:www-data /var/log/mod_evasive/

-sed s/MAILTO/$inbox/g templates/mod-evasive > /etc/apache2/mods-available/mod-evasive.conf

-service apache2 restart

3.2.10 MOD_QOS / MOD_SPAM_HAUS

Se instala los módulos de apache **Mod_Qos y Mod_Spam_Haus** que protegen el servidor de ataques **DOS** como el **Slowroris(qos)**, y contra ataques de **Inyección DNS** usados por los Spammers. (Soto, 2015)

Se ejecuta los siguientes comandos:

-apt-get -y install libapache2-mod-qos

-se debe de editar el archivo de configuración qos ubicado en **/etc/apache2/mods-available/qos.conf**. Como se aprecia en la ilustración 56:

```
<IfModule qos_module.so>
  # minimum request rate (bytes/sec at request reading):
  QS_SrvRequestRate                                120

  # limits the connections for this virtual host:
  QS_SrvMaxConn                                    100

  # allows keep-alive support till the server reaches 600 connections:
  QS_SrvMaxConnClose                               600

  # allows max 50 connections from a single ip address:
  QS_SrvMaxConnPerIP                                50

  #Maximum Number of active TCP connections
  MaxClients                    192

  #Disable keep-alive when 70% of the TCP connections are occupied
  QS_SrvMaxConnClose            70%

  #Minimum request/response speed
  QS_SrvMinDataRate             150     1200

  # block clients violating some basic rules frequently (don't allows more than 20
  # violations within 5 minutes):
  QS_ClientEventBlockCount 20 300
  QS_SetEnvIfStatus 400 QS_Block
  QS_SetEnvIfStatus 401 QS_Block
  QS_SetEnvIfStatus 403 QS_Block
  QS_SetEnvIfStatus 404 QS_Block
  QS_SetEnvIfStatus 405 QS_Block
  QS_SetEnvIfStatus 406 QS_Block
  QS_SetEnvIfStatus 408 QS_Block
  QS_SetEnvIfStatus 411 QS_Block
  QS_SetEnvIfStatus 413 QS_Block
  QS_SetEnvIfStatus 414 QS_Block
  QS_SetEnvIfStatus 417 QS_Block
  QS_SetEnvIfStatus 500 QS_Block
  QS_SetEnvIfStatus 503 QS_Block
  QS_SetEnvIfStatus 505 QS_Block
  QS_SetEnvIfStatus QS_SrvMinDataRate QS_Block
  QS_SetEnvIfStatus NullConnection QS_Block

</IfModule>
```

Elaborado por: Autores

*Ilustración 56 Instalación módulos de apache **Mod_Qos***

- Al editar el archivo de configuración Spamhaus ubicado en **/etc/apache2/mods-available/spamhaus.conf**quedandocomo se detalla en la ilustración 57:

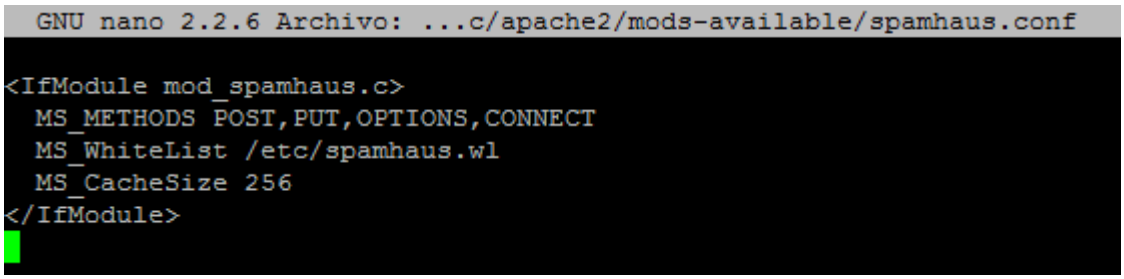


Ilustración 57 Módulo Mod_Spamhaus

Elaborado por: Autores

Se reinicia el servicio de apache con el siguiente comando **service apache2 restart**

3.2.11 CONFIGURAR FAIL2BAN

Se reemplaza la configuración por defecto de fail2ban, donde contiene configuraciones para servicios como SSH, apache, entre otros. Veamos el contenido del archivo:

- sed s/MAILTO/$inbox/g templates/fail2ban > /etc/fail2ban/jail.local
- cp /etc/fail2ban/jail.local /etc/fail2ban/jail.conf

La configuración final debe de ser como se muestra en las imágenes siguientes:

```
[DEFAULT]
ignoreip = 127.0.0.1/8
bantime  = 3600
maxretry = 2
findtime = 600
usedns = warn
backend = auto
destemail = MAILTO
banaction = iptables-multiport
mta = sendmail
protocol = tcp
chain = INPUT
action_ = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s", chain="%(chain)s"]
action_mw = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s", chain="%(chain)s"]
%(mta)s-whois[name=%(__name__)s, dest="%(destemail)s", protocol="%(protocol)s", chain="%(chain)s"]
action_mwl = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s", chain="%(chain)s"]
%(mta)s-whois-lines[name=%(__name__)s, dest="%(destemail)s", logpath=%(logpath)s, chain="%(chain)s"]
action = %(action_mw)s

[ssh]
enabled = true
port = 372
filter = sshd
logpath = /var/log/auth.log
maxretry = 3

[dropbear]
enabled  = false
port = ssh
filter = sshd
logpath = /var/log/dropbear
maxretry = 6
```

Ilustración 58Configuración Fail2ban

Elaborado por: Autores

```
[pam-generic]
enabled = false
filter = pam-generic
port = all
banaction = iptables-allports
port = anyport
logpath = /var/log/auth.log
maxretry = 6

[xinetd-fail]
enabled   = false
filter    = xinetd-fail
port      = all
banaction = iptables-multiport-log
logpath   = /var/log/daemon.log
maxretry  = 2


[ssh-ddos]
enabled  = false
port     = 372
filter   = sshd-ddos
logpath  = /var/log/auth.log
maxretry = 6

[apache]
enabled  = false
port     = http,https
filter   = apache-auth
logpath  = /var/log/apache*/*error.log
maxretry = 6

[apache-multiport]
enabled   = false
port      = http,https
filter    = apache-auth
logpath   = /var/log/apache*/*error.log
maxretry  = 6
```

Ilustración 59Configuración Fail2ban

Elaborado por: Autores

```
[apache-noscript]
enabled  = false
port     = http,https
filter   = apache-noscript
logpath  = /var/log/apache*/*error.log
maxretry = 6

[apache-overflows]
enabled  = false
port     = http,https
filter   = apache-overflows
logpath  = /var/log/apache*/*error.log
maxretry = 2

[vsftpd]

enabled  = false
port     = ftp,ftp-data,ftps,ftps-data
filter   = vsftpd
logpath  = /var/log/vsftpd.log
maxretry = 6


[proftpd]
enabled  = false
port     = ftp,ftp-data,ftps,ftps-data
filter   = proftpd
logpath  = /var/log/proftpd/proftpd.log
maxretry = 6


[pure-ftpd]

enabled  = false
port     = ftp,ftp-data,ftps,ftps-data
filter   = pure-ftpd
logpath  = /var/log/auth.log
maxretry = 6
```

Ilustración 60 Configuración Fail2ban

Elaborado por: Autores

```
[sasl]

enabled  = false
port     = smtp,ssmtp,imap2,imap3,imaps,pop3,pop3s
filter   = sasl
logpath  = /var/log/mail.log
[dovecot]
enabled = false
port    = smtp,ssmtp,imap2,imap3,imaps,pop3,pop3s
filter  = dovecot
logpath = /var/log/mail.log

# DNS Servers
[named-refused-tcp]
enabled  = false
port     = domain,953
protocol = tcp
filter   = named-refused
logpath  = /var/log/named/security.log
```

Ilustración 61Configuración Fail2ban

Elaborado por: Autores

```
[wuftpd]

enabled  = false
port     = ftp,ftp-data,ftps,ftps-data
filter   = wuftpd
logpath  = /var/log/auth.log
maxretry = 6

[postfix]

enabled  = false
port     = smtp,ssmtp
filter   = postfix
logpath  = /var/log/mail.log

[couriersmtp]

enabled  = false
port     = smtp,ssmtp
filter   = couriersmtp
logpath  = /var/log/mail.log

[courierauth]

enabled  = false
port     = smtp,ssmtp,imap2,imap3,imaps,pop3,pop3s
filter   = courierlogin
logpath  = /var/log/mail.log

[sasl]
```

Ilustración 62Configuración Fail2ban

Elaborado por: Autores

Para reiniciar el servicio Fail2ban mediante el siguiente comando

- /etc/init.d/fail2ban restart

3.2.12 PAQUETES ADICIONALES

(Soto, 2015)Recomienda instalar algunos paquetes adicionales que pueden ser de utilidad tanto para el desarrollador como el administrador de sistemas, otros son para cuestiones de seguridad. Se detalla cada uno:

- **apt-getinstalltree**

Da una visión estructurada de los archivos y directorios.

- apt-get install libapache2-mod-wsgi
- **apt-getinstallpython-pip**

Para la instalación de módulos de Python

- apt-getinstall nano
- **apt-getinstallphp-pear**

Framework y sistema de distribución para componentes de PHP reutilizables.

- **apt-getinstalldebsums**

Revisa el checksum de paquetes instalados

- **apt-get install apt-show-versions**

Muestra las versiones de los paquetes.

- **PHPUnit** es un framework de pruebas para detector fallas.
- pear config-set auto_discover 1
- mv phpunit-patched /usr/share/phpunit
- echo include_path = ".:/usr/share/phpunit:/usr/share/phpunit/PHPUnit" >> /etc/php5/apache2/php.ini
- echo include_path = ".:/usr/share/phpunit:/usr/share/phpunit/PHPUnit" >> /etc/php5/cli/php.ini

- **service apache2 restart**

3.2.13 SECURIZAR EL KERNEL

Agrega directivas a **sysctl.conf** para pasarle a kernel configuración en tiempo de ejecución. Estas directivas aumentan el nivel de seguridad del servidor ya que controlan ciertos aspectos de funcionamiento directamente en el kernel. Veamos en las siguientes imágenes que contienen el archivo, las descripciones indican el objetivo de las directivas.(Soto, 2015)

```
# Kernel sysctl configuration file for Ubuntu
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 0

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1

# Controls the use of TCP syncookies
net.ipv4.tcp_syncookies = 1

# Disable netfilter on bridges.
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0

# Controls the default maxmimum size of a mesage queue
kernel.msgmnb = 65536

# Controls the maximum size of a message, in bytes
kernel.msgmax = 65536

# Controls the maximum shared segment size, in bytes
kernel.shmmax = 68719476736
```

Ilustración 63Configuración para securizar el Kernel

Elaborado por: Autores

```
# Controls the maximum number of shared memory segments, in pages
kernel.shmall = 4294967296

######### GENERAL SECURITY OPTIONS ################

# Automatically Reboot Server in 30 Seconds after a Kernel Panic
vm.panic_on_oom = 1
kernel.panic = 30
kernel.panic_on_oops = 30

# Enable ExecShield
kernel.exec-shield = 1
kernel.randomize_va_space = 1

########## COMMUNICATIONS SECURITY ##############
# No Redirections
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Do not Accept Packets with SRR
net.ipv4.conf.all.accept_source_route = 0

# Do not accept Redirections
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.all.secure_redirects = 0

# Disable Packets Forwarding
net.ipv4.ip_forward = 0
net.ipv4.conf.all.forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.default.forwarding = 0
```

Ilustración 64Configuración para securizar el Kernel

Elaborado por: Autores

```
# Log Suspicious Packets
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Ignore ICMP ECHO or TIMESTAMP sent by broadcast/multicast
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.tcp_timestamps = 0

# Protect Against 'syn flood attack'
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_syn_retries = 5
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_max_syn_backlog = 4096

# Enable Reverse Source Validation (Protects Against IP Spoofing)
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Ignore Bogus Error Response
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Reduce KeepAlive
net.ipv4.tcp_keepalive_time = 300
net.ipv4.tcp_keepalive_probes = 5
net.ipv4.tcp_keepalive_intvl = 15

# Disable IPv6
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Ilustración 65Configuración para securizar el Kernel

Elaborado por: Autores

- cptemplates/sysctl.conf /etc/sysctl.conf;echo" OK"
- cptemplates/ufw /etc/default/ufw
- sysctl -e –p

3.2.14 ROOTKIT HUNTER

Es una herramienta que escanea el servidor en busca de **Rootkits, Backdoors o Exploits** locales, nosotros vamos a instalar la herramienta y a realizar un escaneo inicial del servidor.

Para instalarlo se ejecuta el siguiente comando:

- **apt-getinstallrkhunter**

Actualizarlo se ejecutan los siguientes comandos:

- **rkhunter –update**
- **rkhunter –propupd**

Si se desea iniciar la herramienta se ejecuta lo siguiente:

Rkhunter –c –enable all –disable none

3.2.15 INSTALAR PORTSENTRY

Es un sistema de detección que ayuda a proteger el servidor de escaneos de puertos (Soto, 2015)

- Se instala ejecutando el comando**apt-getinstallportsentry**como lo detalla la siguiente figura:

```
root@sfamiliaEc:/home/sfamilia# apt-get install portsentry
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  logcheck
Se instalarán los siguientes paquetes NUEVOS:
  portsentry
0 actualizados, 1 se instalarán, 0 para eliminar y 3 no actualizados.
Necesito descargar 69,5 kB de archivos.
```

Ilustración 66 Instalación PortSentry

Elaborado por: Autores

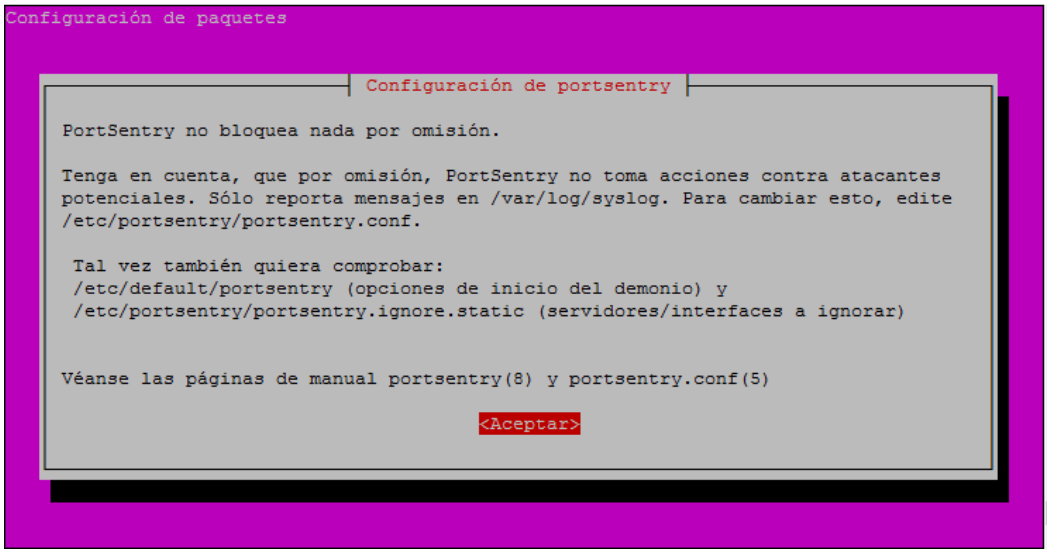


Ilustración 67 Configuración de PortSentry

Elaborado por: Autores

Para evitar cualquier equivocación o error es recomendable realizar una copia del archivo de configuración portsentry mediante el siguiente comando:

- **mv /etc/portsentry/portsentry.conf /etc/portsentry/portsentry.conf-original**

Se cambia la configuración del archivo **portsentry. conf** por la siguiente:

```
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337
,32771,32772,32773,32774,40421,49724,54320"
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774
,31337,54321"

ADVANCED_PORTS_TCP="1024"
ADVANCED_PORTS_UDP="1024"
ADVANCED_EXCLUDE_TCP="113,139"
ADVANCED_EXCLUDE_UDP="520,138,137,67"

IGNORE_FILE="/etc/portsentry/portsentry.ignore"
HISTORY_FILE="/var/lib/portsentry/portsentry.history"
BLOCKED_FILE="/var/lib/portsentry/portsentry.blocked"

RESOLVE_HOST = "0"

BLOCK_UDP="1"
BLOCK_TCP="1"

KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"
KILL_RUN_CMD_FIRST = "0"
KILL_RUN_CMD="/sbin/blockip $TARGET$"

SCAN_TRIGGER="0"

# EOF
```

Ilustración 68Configuración del archivo portsentry.conf

Elaborado por: Autores

- sed s/tcp/atcp/g /etc/default/portsentry> salida.tmp
- mv salida.tmp /etc/default/portsentry

Se reinicia el servicio mediante el comando**/etc/init.d/portsentryrestart**

```
root@sfamiliaEc:/home/sfamilia# service portsentry restart
Stopping anti portscan daemon: portsentry.
Starting anti portscan daemon: portsentry in atcp & udp mode.
```

Ilustración 69 Reinicio PortSentry

Elaborado por: Autores

3.2.16 PASOS ADICIONALES DE SEGURIDAD DEL SERVIDOR

En este punto se va a mejorar el nivel de seguridad del servidor, como en el detalle:

- **echo tty1 > /etc/securetty**
- #ProtectAgainst IP Spoofing
- echo nospoof on >> /etc/host.conf
- #Remove AT and Restrict Cron
- apt-getpurge at
- echo " Securing Cron "
- touch /etc/cron.allow
- chmod 600 /etc/cron.allow

3.2.17 INSTALAR UNHIDER

Según.(Soto, 2015)**Unhide** es una herramienta desarrollada por Yago Jesús y Patrick Gouinenfocada a identificar anomalías inicialmente para sistemas Unix/Linux, pero según vi en la página del proyecto hay una versión para sistemas Windows. Estas anomalías son detectadas por la herramienta identificando procesos y puertos TCP/UDP ocultos, que son, sin duda síntomas de un Rootkit en el sistema

Unhide para Linux emplea las siguientes técnicas para la detección.

Unhide(ps)

- Detecta procesos ocultos y a su vez emplea seis técnicas.

- Compara la salida de /proc contra /bin/ps.
- Compara la información obtenida de /bin/ps con la info obtenida recorriendo el filesystem de /proc.
- Compara la información obtenida de /bin/ps con la obtenida de syscalls o llamadas del sistema (syscallscanning).
- Búsqueda por fuerza bruta de todos los PIDs del sistema (PIDsbruteforcing).
- Búsqueda al reverso, verifica que todos los hilos visto por ps también sean vistos por el Kernel (/bin/ps vs /proc, procfs, syscall).
- Rápida comparación /proc, recorrido procfs y syscall vs salida /bin/ps.

Unhide-TCP

Identifica puertos TCP/UDP en escucha que no se muestran en /bin/nestat haciendo un bruteforcing de todos los puertos TCP/UDP disponibles.

Ejemplos de uso:

- **Unhideproc**

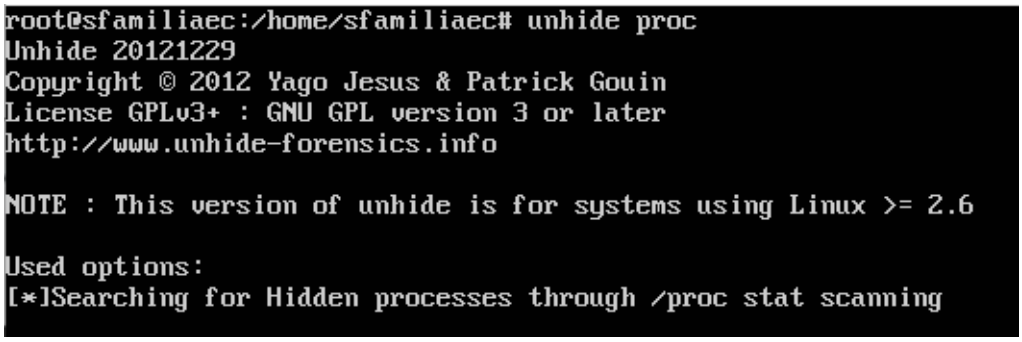


Ilustración 70Unhideproc

Elaborado por: Autores

- **Unhidebrute**

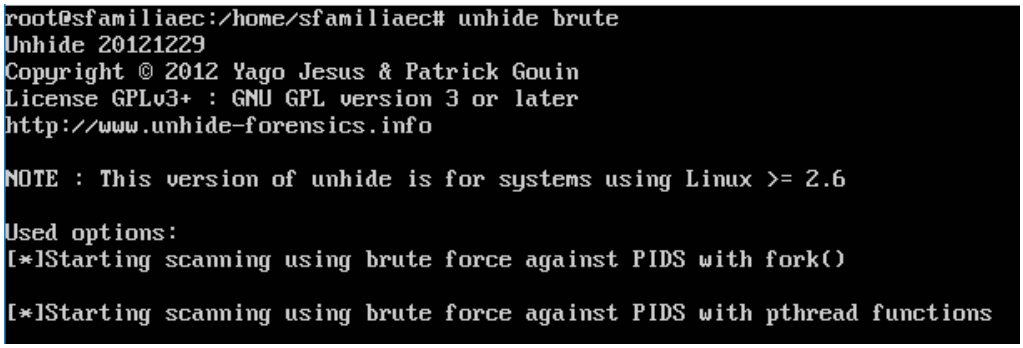


Ilustración 71UnhideBrute

Elaborado por: Autores

- **Unhidesys**

```
root@sfamiliaec:/home/sfamiliaec# unhide sys
Unhide 20121229
Copyright © 2012 Yago Jesus & Patrick Gouin
License GPLv3+ : GNU GPL version 3 or later
http://www.unhide-forensics.info

NOTE : This version of unhide is for systems using Linux >= 2.6

Used options:
[*]Searching for Hidden processes through getpriority() scanning

[*]Searching for Hidden processes through getpgid() scanning

[*]Searching for Hidden processes through getsid() scanning

[*]Searching for Hidden processes through sched_getaffinity() scanning

[*]Searching for Hidden processes through sched_getparam() scanning

[*]Searching for Hidden processes through sched_getscheduler() scanning

[*]Searching for Hidden processes through sched_rr_get_interval() scanning

[*]Searching for Hidden processes through kill(..,0) scanning

[*]Searching for Hidden processes through  comparison of results of system calls
```

Ilustración 72UnhideSys

Elaborado por: Autores

Para instalar Unhidese ejecuta el siguiente comando:

- **apt-get install Unhide –y**

```
root@sfamiliaEc:/etc# apt-get  install unhide -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  unhide
0 actualizados, 1 se instalarán, 0 para eliminar y 3 no actualizados.
Necesito descargar 1.460 kB de archivos.
```

Ilustración 73 Instalación Unhide

Elaborado por: Autores

3.2.18 INSTALAR TIGER

Tiger puede ser usado como un auditor de seguridad y sistema de detección de intrusos. Durante la instalación deben configurar los passphrases, que deben recordarlas para aceptar cambios en el sistema de archivos. Como lo expresa (Soto, 2015)

Para instalarlo se ejecuta el siguiente comando:**apt-getinstalltiger –y.** En la ilustración se observa el progreso de la instalación del paquete y la ejecución del comando.

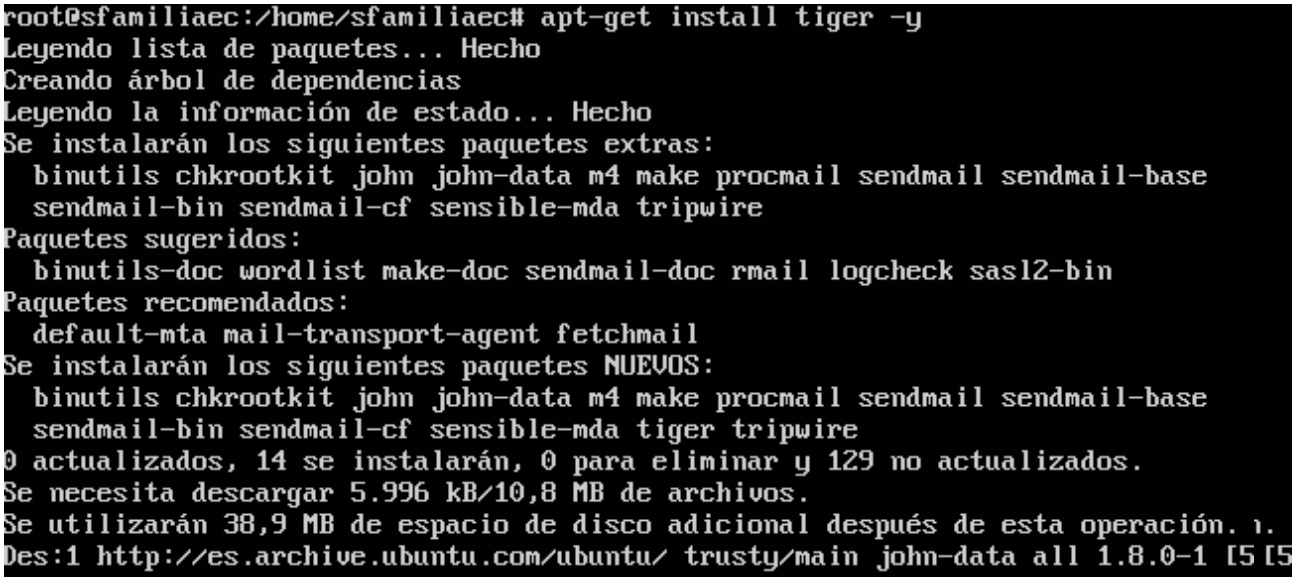


Ilustración 74 Instalación de Tiger

Elaborado por: Autores

3.2.19 RESTRINGIR EL ACCESO A LOS ARCHIVOS DE CONFIGURACIÓN DE APACHE

Colocar permisos más restrictivos a los archivos de configuración de apache, se ejecutan los siguientes comandos:

- **chmod 750 /etc/apache2/conf* >/dev/null 2>&1**
- **chmod 511 /usr/sbin/apache2 >/dev/null 2>&1**
- **chmod 750 /var/log/apache2/ >/dev/null 2>&1**
- **chmod 640 /etc/apache2/conf-available/* >/dev/null 2>&1**
- **chmod 640 /etc/apache2/conf-enabled/* >/dev/null 2>&1**
- **chmod 640 /etc/apache2/apache2.conf >/dev/null 2>&1**

3.2.20 DESCARGAR ACTUALIZACIONES DE VERSIONES ESTABLES

Ejecutando el comando: **dpkg-reconfigure -plowunattended-upgrades,** se va a lograr activar las actualizaciones para mantener al sistema siempre actualizado sin la iteración del administrador de sistemas, ejemplo del comando detallado en la siguiente ilustración.

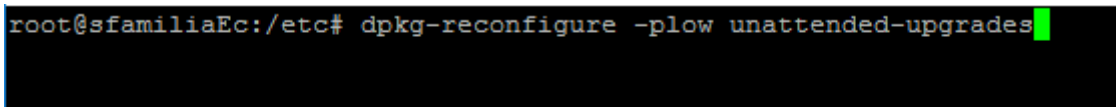


Ilustración 75 Instalar Versiones Estables

Elaborado por: Autores

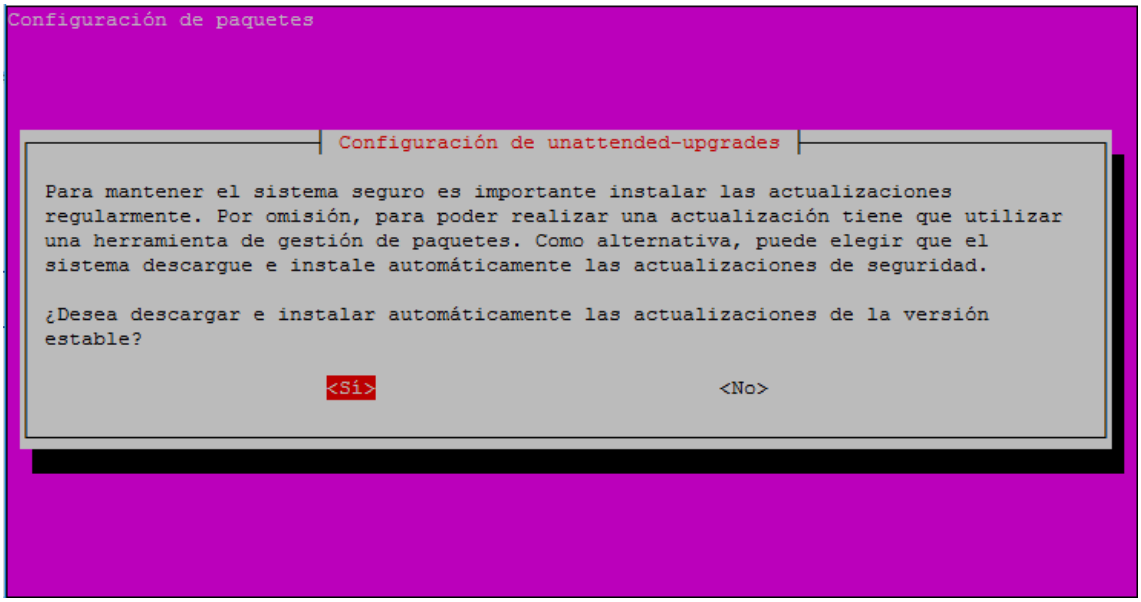


Ilustración 76 Configuración Paquete Unattended-Upgrades

Elaborado por: Autores

3.2.21 HABILITAR PROCESS ACCOUNTING

ACCT: es una herramienta que monitorea la actividad de los usuarios y procesos en el sistema. Nos provee de diversas herramientas para monitorear las actividades de los procesos, según lo expresa (Soto, 2015)

- **ac,** muestra las estadísticas de las conexiones y desconexiones de los usuarios en horas.
- **lastcomm,** muestra la información de comandos ejecutados
- **accton,** activa y desactiva la contabilidad
- **sa.**Sumariza la información de comandos ejecutados
- **last y lastb,** muestra un listado de los últimos usuarios conectados

Para instalar se ejecuta el siguiente comando:

- **apt-getinstallacct**
- Touch /var/log/wtmp

```
root@sfamiliaEc:/etc# apt-get install acct
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  acct
0 actualizados, 1 se instalarán, 0 para eliminar y 3 no actualizados.
Necesito descargar 80,6 kB de archivos.
Se utilizarán 340 kB de espacio de disco adicional después de esta operación.
```

Ilustración 77 Habilitar ProcessAccounting

Elaborado por: Autores

3.2.22 DOMINIOS VIRTUALES O VIRTUAL

El servidor web de Apache es una herramienta para servir aplicaciones web, ofrece muchas posibilidades de configuración, a continuación, se detalla cómo crear distintos servidores virtuales para diferentes dominios. Esto quiere decir que, en una misma máquina con una instancia de Apache(Pérez Esteso, 2016), es posible tener los diferentes dominios ejemplo: **dispensariosagradafamilia.com.ec y dispensariosagradafamilia.com** sin la necesidad de tener dos servidores diferentes.

Para editar el virtual host de apache se usa la siguiente ruta y usando uno de los editores de texto como nano: nano **/etc/apache2/sites-available/000-default.conf,** en la siguiente ilustración se puede apreciar cómo está configurado el archivo 000-default.conf**.**

```
<VirtualHost *:80>
  ServerAlias dispensariosagradafamilia.com.ec
  ServerName  dispensariosagradafamilia.com.ec
  DocumentRoot /var/www/html/sfamilia
   <Directory /var/www/html/sfamilia>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
   </Directory>
</VirtualHost>
```

Ilustración 78 Dominios Virtuales

Elaborado por: Autores

Para habilitar el nuevo Virtual Host se utiliza la herramienta **a2ensite** de Apache, para habilitarlo se especifica en la línea de comandos lo siguiente: **a2ensite 000-default.conf**

Configurar el archivo Host

Según (Denker, 2014), si se tiene un servidor DNS apuntando a nuestro servidor se omite la configuración del archivo hosts debido a que el servidor DNS se encargaría de resolver la dirección. En caso de que no se tenga un servidor DNS abrimos el archivo hosts que está ubicado en **/etc/hosts**, el paso a ejecutar sería el siguiente:

- **nano /etc/hosts**

En este archivo se ubica el nombre de dominio del dispensario que sería el siguiente **dispensariosagradafamilia.com.ec**, como se observa en la siguiente ilustración.

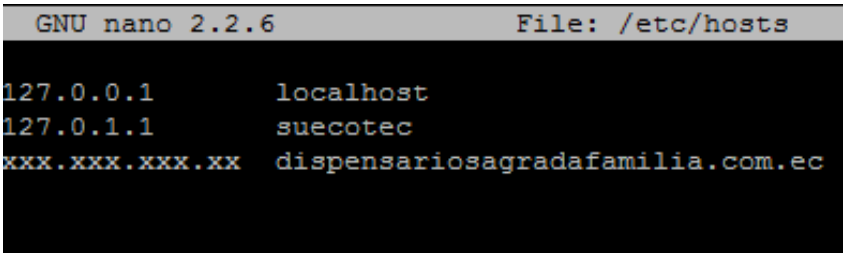


Ilustración 79 Configuración Archivo Host

Elaborado por: Autores

Si se coloca la dirección del sitio web dispensariosagradafamilia.com.ec en el navegador se observa el sitio como lo describe la siguiente ilustración:

Ilustración 80 Pantalla Inicial de la Página

Elaborado por: Autores

3.3 DISEÑO DEL SITIO WEB

En esta sección se describe el funcionamiento del sitio web del Dispensario Sagrada familia y se detalla con imágenes la estructura básica.

El sitio del dispensario es una página tipo parallax donde todo el contenido e información se despliega en una sola página, el usuario no se va a confundir al buscar cualquier información ya que consta de un menú, como se observa en la siguiente imagen, la página principal del dispensario sagrada familia, se utiliza una gama de colores que hacen referencia al logo del dispensario.

A continúan se detalla cada una de las opciones que conforman el menú de la página web:

3.3.1 NOSOTROS

Breve introducción al origen del dispensario la hora de atención del dispensario.

Ilustración 81 PESTAÑA NOSOTROS

Elaborado por: Autores

3.3.2 SERVICIOS

Muestra una breve reseña de los servicios principales del dispensario.

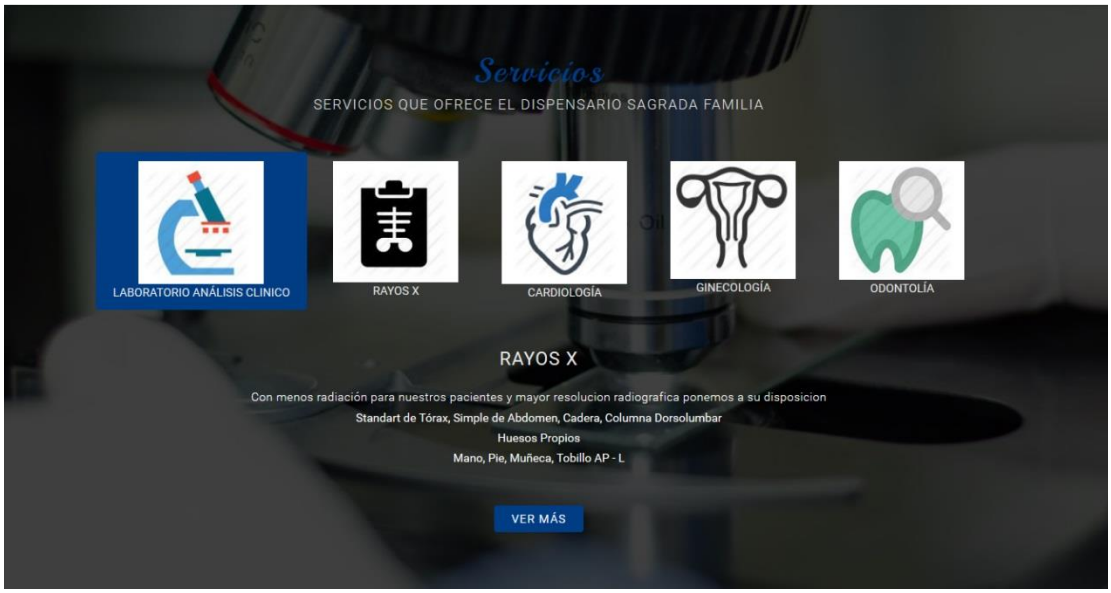


Ilustración 82 PESTAÑA SERVICIOS

Elaborado por: Autores

3.3.3 GALERÍA

Ilustración 83 GALERIA

Elaborado por: Autores

3.3.4 EVENTOS

Eventos recientes del dispensario

Ilustración 84 EVENTOS

Elaborado por: Autores

3.3.5 EXPERIENCIAS

Ilustración 85 EXPERIENCIAS

Elaborado por: Autores

3.3.6 SERVICIOS MÉDICOS

Muestra un listado de los servicios médicos existentes en el Dispensario, así como el respectivo horario

Ilustración 86 SERVICIOS MEDICOS

Elaborado por: Autores

Se puede buscar el servicio médico por cualquiera de los elementos de la tabla tanto especialidad como hora

3.3.7 DIRECTORIO MÉDICO

Muestra un listado de todos los Doctores con su respectiva especialidad y horario, para buscar un doctor específico solo debemos escribir en el cuadro buscar tanto el nombre del doctor como especialidad y busca por cualquier elemento de la tabla.

Ilustración 87DIRECTORIO MEDICO

Elaborado por: Autores

3.3.8 CONTÁCTENOS

Formulario donde pueden enviar todas las inquietudes que tengan sobre el dispensario.

Ilustración 88CONTACTENOS

Elaborado por: Autores

4 RESULTADOS

Como se muestra en la ilustración donde de detalla el resultado de la arquitectura y el diseño de la red con la integración de los equipos, reestructurando de manera lógica los recursos físicos del dispensario “SAGRADA FAMILIA” basados en los principios básico de implementación de redes sistematizando un modelo jerárquico para mayor gestión y administración de la misma brindado alta disponibilidad en los servicios de la siguiente manera.

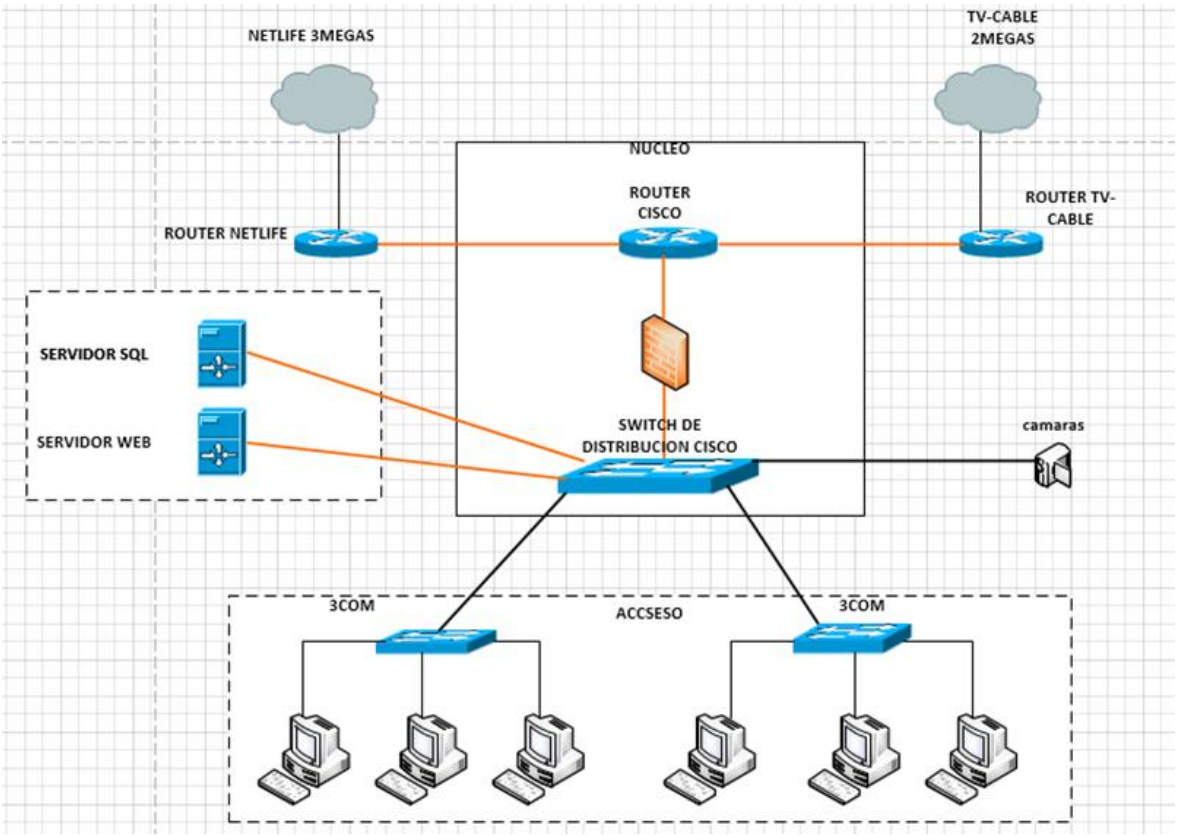


Ilustración 89 Diseño Final

Elaborado por: Autores

1. En el núcleo o conmutador de la red se integra:

- De tal manera gestione y administre el tráfico de entrada y salida a la LAN.
- Filtrar puertos garantizando la seguridad del servicio brindado.
- Inspeccionar los paquetes que salen de la red interna a internet.
- Configurar las DMZ para nuestro servidor web.
- Conectar los dos proveedores de internet a las 2 interfaces WAN del dispositivo.
- Balanceo de carga en las dos interfaces WAN del dispositivo.

2. Capa de distribución

- Administrar la distribución entre los switch de acceso y el núcleo de la red.
- Amplia gama de configuraciones a nivel de administración de red.

3. Capa de acceso

- Switch al cual se conectan usuarios finales del dispensario.

4. Servidor.

- Sistema operativo Linux Ubuntu server 16.04 LTS
- Servidor http apache.

5. Página web.

- Desarrollada en HTML con material design con información facilitada por el dispensario.

4.1.1 HARDWARE

Marca	**Modelo**	**Precio**
DELL	PowerEdge R430: PowerEdge R430 Server	$4.928,00
Cisco	Cisco SG200-26P Gigabit Ethernet Smart Switch, 24 10/100/1000 Ports, PoE	$651,28
Cisco	Cisco RV325 Gigabit Dual WAN VPN Router	$435,32
Subtotal		**$6.014,60**

Elaborado por: Autores

4.1.2 SOFTWARE

Sistema Operativo	Distribución	Precio
Linux	Ubuntu Server 16.04 LTS	0,00

Elaborado por: Autores

4.1.3 DOMINIO /HOSTING

Empresa	Descripción	Precio
Godaddy	Redireccionamiento DNS	
Nic.ec	dispensariosagradafamilia.com.ec	

Elaborado por: Autores

4.2 **CONCLUSIONES**

Se analizó las características óptimas de los equipos, debido al alza de los precios en el país se optó por exportar todos los equipos de cómputo y de red abaratando los precios y se realizó la respectiva proforma con los valores para la adquisición de los mismos.

Se diseñó un esquema de red ya que el Dispensario contaba con una red plana, este esquema de red es el óptimo para integración y ubicación de cada uno de los componentes que forman parte de la infraestructura.

Se realizó las configuraciones tanto del servidor web como de los equipos necesarios para la red habilitando en cada uno las funcionalidades más importantes para un correcto desempeño.

Se diseñó el sitio web del dispensario utilizando html5, JavaScript, responsiveDesingn y lenguaje de programación, este mismo es una herramienta empleada para difundir y promocionar actividades, servicios y eventos permitiendo de forma más sencilla y ágil puedan consultarlo todas las personas.

Se determinó que la mejor opción de acuerdo al presupuesto del Dispensario es utilizar para el sistema operativo Ubuntu Server como el servidor web Apache dada que estas tecnologías son software libre y consta de abundante documentación en internet para realizar las respectivas configuraciones.

4.3 **RECOMENDACIONES**

El servidor tiene muy buenas características, para ser utilizado no solo para instalar un servidor web, se utilizaría tecnologías de virtualización como **Citrix, Hyper-V o VMWare** para virtualizar algunos de los servicios que cuenta en Dispensario como por ejemplo el de Base de datos, servidor de archivos y el servidor Web aprovechando las características del servidor, pero por motivos de trabajo de investigación utilizamos para instalar solo el servidor web.

El sitio web es un canal para generar información y contenido para que las personas estén informados de las actividades, servicios, horarios de atención y médicos del Dispensario, en un principio fue una excelente idea implementar, pero conforme avanza la tecnología y la manera de separar citas médicas creemos que un futuro se podría poner a disposición un portal donde los clientes puedan separar su cita médica desde la comodidad de su casa evitando largas filas.

El internet se ha convertido en el principal mecanismo del comercio a nivel internacional, pero en Ecuador lastimosamente los niveles de transaccionalidad electrónica son bajos, la falta de facilidad para realizar pagos mediante diferentes formas es una de las barreras más grandes para el e-commerce a nivel local, en un futuro los clientes podrán realizar pagos mediante el sistema web otorgándoles un usuario y clave para consultar historial médico y realizar pagos en línea mediante uno o varios botones de pagos de los bancos y tarjetas más conocidas que el dispensario realice contrato.

La situación actual algunos de los equipos médicos necesitan conectarse a internet para que el fabricante del equipo pueda dar soporte, pero el fabricante del equipo se conecta manera directa a la red mediante una IP pública al percatarnos de eso nos dimos cuenta que sigue así la red puede ser comprometida ya que no cuenta con un tipo de seguridad, pueden alterar los datos del dispensario. Por este motivo se recomienda el uso de una **Vpn** para conectarse de forma segura a una red remota a través de Internet para que los proveedores puedan acceder a los equipos médicos y otros recursos de la red del dispensario sin comprometer la seguridad.

En cuanto a la organización de los equipos de red y computadores proponemos que se instale un Directorio activo porque de forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.
Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

También se pretende virtualizar un servidor VOIP con una central Asterisk ya que se ha implementado cableado estructurado con puertos de voz con un aproximado de 35 a 40 extensiones internas, se pretende configurar 2 troncales SIP con las líneas externas que posee el dispensario y un IVR para llamadas entrantes de tal manera que se gestione de mejor manera la telefonía interna

Se recomienda la implementación de un servidor **WSUS** que este únicamente destinado a la distribución de paquetes oficiales y estables de Microsoft, por tanto, en la actualización no se podrá incluir aplicaciones de terceros como, por ejemplo: Java, Abode Flash player o la actualización de las bases de datos y firmas de virus de ningún antivirus.

A nivel de seguridad de las estaciones de trabajo se recomienda la implementación de una consola antivirus que ayudaría a optimizar la administración del antivirus en la red, monitoreo de amenazas, mejor control del producto final llamado endpoint.

REFERENCIAS BIBLIOGRÁFICAS

Andrés, R. (16 de Diciembre de 2015). *http://computerhoy.com*. Obtenido de http://computerhoy.com/noticias/internet/que-es-que-sirve-dominio-tu-pagina-web-22007

Armendáriz, L. M. (Abril de 2009). *Cableado Estructurado: Guimi.* Obtenido de Guimi Web site: http://guimi.net/monograficos/G-Cableado_estructurado/G-Cableado_estructurado.pdf

Cases, E. F. (11 de Junio de 2014). *www.ibrugor.com*. Obtenido de http://www.ibrugor.com/blog/apache-http-server-que-es-como-funciona-y-para-que-sirve/

Casillas Gallegos, M. A., & Domínguez Ruíz, R. (1 de Marzo de 2009). *Redes de Computadoras, Tipos y Topologías*. Obtenido de Redes de Computadoras, Tipos y Topologías: http://redestipostopologias.blogspot.com/

CCM. (Marzo de 2016). *http://es.ccm.net/*. Obtenido de http://es.ccm.net/contents/264-el-protocolo-http

CCM. (s.f.). *CCM*. Obtenido de CCM: http://es.ccm.net/contents/299-equipos-de-red-router

CISCO. (23 de Junio de 2014). *CISCO*. Obtenido de CISCO: http://www.cisco.com/c/en/us/products/collateral/switches/small-business-220-series-smart-plus-switches/datasheet-c78-731284.html

CISCO. (24 de Junio de 2016). *CISCO*. Obtenido de CISCO: http://www.cisco.com/c/en/us/products/collateral/routers/rv325-dual-gigabit-wan-vpn-router/datasheet-c78-729726.html

Cisco, S. (s.f.). *CISCO*. Obtenido de CISCO: http: // www.cisco.com/go/findit

Cuenca, C. L. (20 de Marzo de 2003). *desarrolloweb.com*. Obtenido de desarrolloweb.com: http://www.desarrolloweb.com/articulos/1112.php

DELL. (2015). *DELL*. Obtenido de DELL: http://www1.la.dell.com/ec/es/corp/Servidores/poweredge-r430/pd.aspx?refid=poweredge-r430&s=corp

Denker. (23 de Agosto de 2014). *Codedrinks*. Obtenido de Codedrinks: http://www.codedrinks.com/configurar-host-virtuales-de-apache-en-ubuntu-server-14-04/

Diana. (Julio de 2009). *Modelo de redes jerárquicas: Blog de Tecnologia*. Obtenido de Blog de Tecnologia Web site: http://blogxdextecnologia.blogspot.com/2009/07/modelo-de-redes-jerarquicas.html

Econ. (s.f.). *econ*. Obtenido de econ: http://www.econ.uba.ar/www/departamentos/sistemas/plan97/tecn_informac/briano/seoane/tp/yquiro/redes.htm

Eduard, L. (s.f.). *Departament d'Arquitectura de Computadors.* Obtenido de Departament d'Arquitectura de Computadors: http://personals.ac.upc.edu/elara/documentacion/INTERNET%20-%20UD8%20-%20Protocolo%20HTTP%20y%20servidores%20WEB.pdf

Fernandez, E. (13 de Septiembre de 2014). *http://www.neoteo.com*. Obtenido de http://www.neoteo.com/servidor-http-apache-los-mejores-desarrolladores#prettyPhoto

Free Software Foundation, I. (2016). *http://www.gnu.org/philosophy/*. Obtenido de http://www.gnu.org/philosophy/free-sw.es.html

HOY, I. (s.f.). *INFORMATICA HOY*. Obtenido de INFORMATICA HOY: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-DMZ.php

Image Gateway :Hardware y Software de redes.(s.f.). Obtenido de Hardware y Software de redes Web site: http://www.abcnet.es/wp-content/uploads/2013/02/GATEWAY1.gif

Image Switch: BroadBand Buyer. (s.f.). Obtenido de BroadBand Buyer Web site: http://www.broadbandbuyer.com/images/features/2032/ciscoswitch-img1.jpg

Imagen: HW GROUP. (s.f.). Obtenido de HW GROUP Web site: http://www.hwgroup.cz/products/poseidon/images/S-Hub_800.jpg

Joskowicz, J. (Septiembre de 2006). *http://bibdigital.epn.edu.ec.* Obtenido de http://bibdigital.epn.edu.ec: http://bibdigital.epn.edu.ec/bitstream/15000/10009/1/Cableado%20Estructurado.pdf

Juliá, S. (26 de Agosto de 2015). *Tipos de redes informáticas según su topología: GADAE NETWEB.* Obtenido de GADAE NETWEB: http://www.gadae.com/blog/tipos-de-redes-informaticas-topologia/

LAN, WAN, MAN, WLAN, WMAN, WWMAN, SAN y PAN: Qué significa cada término. (6 de Mayo de 2015). Obtenido de LAN, WAN, MAN, WLAN, WMAN, WWMAN,

SAN y PAN: Qué significa cada término: http://www.informatica-hoy.com.ar/redes/LAN-WAN-MAN-WLAN-WMAN-WWMAN-SAN-PAN.php

LÓPEZ PINO, J. L. (30 de JULIO de 2010). *SERVIDORES WEB MAS USADOS: JOSE LUIS DEL PINO*. Obtenido de JOSE LUIS DEL PINO WEB SITE : : http://lopezpino.es/2010/07/30/servidores-web-mas-usados/

Maldonado, D. M. (20 de Abril de 2008). *http://empresayeconomia.republica.com*. Obtenido de http://empresayeconomia.republica.com/aplicaciones-para-empresas/apache-el-servidor-web-mas-reconocido.html

MASADELANTE. (s.f.). *MAS ADELANTE*. Obtenido de MAS ADELANTE: https://www.masadelante.com/faqs/dominio

Medina, A. (6 de Abril de 2012). *http://andreitamedina.blogspot.com/*. Obtenido de http://andreitamedina.blogspot.com/2012/04/ventajas-y-desventajas-del-software.html

Méndez Hernández, E. (s.f.). *Redes Alámbricas e Inalámbricas: Scribd.* Obtenido de Scribd: https://es.scribd.com/doc/28842240/REDES-ALAMBRICAS-E-INALAMBRICAS

Pairuna, L. (13 de Abril de 2016). *codedimension*. Obtenido de codedimension: http://www.codedimension.com.ar/noticias-sobre-tecnologia/noticias/-que-es-y-para-que-sirve-un-sitio-web-/1

pepito. (1 de noviembre de 2010). *desarrollo*. Obtenido de desarrollo: http://www.desarrolloweb.com/articulos/protocolo-http-ftp.html

Pérez Esteso, M. (08 de Enero de 2016). *geekytheory*. Obtenido de geekytheory: https://geekytheory.com/como-configurar-un-virtual-host-de-apache-en-linux/

Pérez Valdés, D. (2 de Noviembre de 2007). *Los diferentes lenguajes de programación par ala web: Maestros del Web*. Obtenido de Maestros del Web Werb site: http://www.maestrosdelweb.com/los-diferentes-lenguajes-de-programacion-para-la-web/

Profesorado, I. N. (s.f.). *Instituto Nacional de Tecnologías Educativas y de formación del Profesorado*. Obtenido de Instituto Nacional de Tecnologías Educativas y de formación del Profesorado: http://roble.pntic.mec.es/jprp0006/tecnologia/bachillerato_tic/unidad01_navegadores/navegadores3.htm

Proyectos Curso Cableado Estructurado:Universidad del Azuay. (Junio de 2006). Obtenido de Universidad del Azuay Web site:

https://www.uazuay.edu.ec/estudios/electronica/proyectos/cableado_estructurado.pdf

Router Image: C.A. Combustibles Equipos de Computo y Accesorios. (s.f.). Obtenido de C.A. Combustibles Equipos de Computo y Accesorios Web site: http://www.caconsumibles.com/blog/wp-content/uploads/2015/09/modem-and-router-units.jpg

Sara, A. (19 de Septiembre de 2012). *Desarrollo web*. Obtenido de http://www.desarrolloweb.com/articulos/protocolo-http-ftp.html

Siguencia Siguencia, M. (2011). *Dscape.ups.edu.ec*. Obtenido de Dscape.ups.edu.ec: http://dspace.ups.edu.ec/bitstream/123456789/1604/17/UPS-CT002147.pdf

Siguencia Siguencia, M. (s.f.). *D.* Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/1604/17/UPS-CT002147.pdf

Sistema de cableado estructurado : Gobierno del Estado de Chiapas. (s.f.). Obtenido de Gobierno del Estado de Chiapas Web site: http://www.dnit.chiapas.gob.mx/pdfs/infra/anexo2.pdf

sistemasumma. (19 de Febrero de 2012). *Redes Jerárquicas: Sistemas umma*. Obtenido de Sistemas umma Web site: https://sistemasumma.com/2012/02/19/redes-jerarquicas/

Solusan. (29 de Marzo de 2007). *http://www.solusan.com*. Obtenido de http://www.solusan.com/que-es-una-dmz.html

Soto, J. (2015). *jsitech - Linux Hardening Script Guide.*Obtenido de jsitech: https://www.gitbook.com/book/jsitech1/jshielder-linux-server-hardening-script/details

Switch image: Bucaro TecHelp. (s.f.). Obtenido de Bucaro TecHelp Web site: http://bucarotechelp.com/networking/images/bridge.gif

Systems, C. (s.f.). *Software Cisco*. Obtenido de Software Cisco: https://software.cisco.com/download/navigator.html

systems, I. (s.f.). *ISOCRON SYSTEMS*. Obtenido de ISOCRON SYSTEMS: https://www.isocron.net/node/35

Unidad III Dispositivos de Red: Tecnológico Nacional de México. (s.f.). Obtenido de Tecnológico Nacional de México Web site: http://itpn.mx/recursosisc/6semestre/redesdecomputadoras/Unidad%20III.pdf

Vallejos, I. O. (s.f.). *UNIVERISDAD NACIONAL DEL NORDESTE*. Obtenido de UNIVERISDAD NACIONAL DEL NORDESTE: http://ing.unne.edu.ar/pub/internet.pdf

web-gdl. (s.f.). *http://web-gdl.com/*. Obtenido de http://web-gdl.com/: http://web-gdl.com/servicios/dominios/que-es-un-dominio/

Zepeda Vega, D. (s.f.). *Programa para el fortalecimiento de la información para la investigación*. Obtenido de http://www.peri.net.ni/pdf/docLAN/PresentacionII.pdfv

ANEXOS

Cisco Small Business RV320 and RV325 Dual Gigabit WAN WF VPN Routers Data Sheet

Ficha técnica

Router Cisco VPN con WAN Gigabit dual RV320

Descripción general de productos

La conectividad de red es el centro de cada pequeña empresa y el acceso seguro, la protección de firewall y el alto rendimiento son los pilares de cada router Cisco® Small Business de la serie R. El router Cisco VPN con WAN Gigabit dual RV320 no es la excepción. Con una interfaz de usuario intuitiva, el router Cisco RV320 está listo para funcionar en minutos. El router Cisco RV320 ofrece acceso confiable y altamente seguro para usted y sus empleados, tan transparente que no sabrá que está allí.

Figura 1. Router Cisco VPN con WAN Gigabit dual RV320

Funciones y ventajas

- Los puertos WAN Gigabit Ethernet dobles facilitan el equilibrio de carga y la continuidad comercial.
- Los puertos Gigabit Ethernet asequibles y de alto rendimiento permiten la transferencia rápida de archivos grandes y admiten varios usuarios.
- Los puertos USB dobles admiten un módem 3G/4G o una unidad flash. La red WAN también tiene conmutación por falla con el módem 3G/4G conectado a un puerto USB.
- Las plataformas VPN con SSL y VPN de sitio a sitio permiten una conectividad altamente segura, por lo que el router Cisco RV320 es perfecto para empleados remotos y diversas oficinas.
- El firewall con inspección activa de estado de paquetes (SPI) y el cifrado de hardware ofrecen una sólida seguridad.
- Las herramientas de configuración fáciles de utilizar, de acuerdo con asistentes, pueden utilizarse para establecer la conectividad de red y administrar la seguridad.

En un entorno comercial en constante cambio, su pequeña red empresarial debe ser potente, flexible, accesible y altamente confiable, en especial cuando el crecimiento es la mayor prioridad. Su red debe poder adaptarse de manera rentable a este crecimiento.

Ilustración 90 FICHA TÉCNICA CISCO RV325

Elaborado por: Autores

El router Cisco VPN con WAN Gigabit dual RV320 es la elección de todas las redes para las que el rendimiento, la seguridad, la confiabilidad y la adaptabilidad encabezan la lista de requisitos. El router Cisco RV320 ofrece dos conexiones a un proveedor de servicios mediante el equilibrio de carga para obtener un alto rendimiento o a dos proveedores diferentes para garantizar la continuidad comercial. Las redes privadas virtuales (VPN) de alta capacidad conectan diversas oficinas y permiten a una gran cantidad de empleados acceder a la información que necesitan desde cualquier lugar con la misma seguridad que desde la oficina principal.

Especificaciones del producto

En la tabla 1, se enumeran las especificaciones del producto Cisco RV320.

Tabla 1. Especificaciones del producto

Descripción	Especificación
WAN dual	• Puertos Gigabit Ethernet duales • Falla • Equilibrio de carga
Estándares	• 802.3, 802.3u • IPv4 (RFC 791) • IPv6 (RFC 2460)
Conectividad WAN	• Servidor de protocolo de configuración dinámica de host (DHCP), cliente DHCP, agente de retransmisión DHCP • IP estática • Protocolo punto a punto sobre Ethernet (PPPoE) • Protocolo de túnel punto a punto (PPTP) • Puente transparente • Relé de DNS, DNS dinámico (DynDNS.org, 3322.org), base de datos local de DNS • IPv6
Protocolos de routing	• Protocolo de información de routing (RIP) v1, v2 y RIP para IPv6 (RIPng) • Routing entre VLAN • Routing estático • VLAN admitidas: 7
Traducción de direcciones de red (NAT)	• Traducción de direcciones de puertos (PAT) • NAT uno a uno • NAT transversal
Vinculación de protocolos	Los protocolos se pueden vincular a un puerto WAN específico para equilibrar la carga.
Perímetro de la red (DMZ)	• Puerto DMZ • Host DMZ
Dos puertos USB 2.0	Almacenamiento y soporte de módem 3G/4G
Seguridad	
Firewall	• Firewall SPI • Prevención de denegación de servicio (DoS): ping de la muerte, inundación SYN, falsificación de IP, WinNuke
Reglas de acceso	• Reglas de acceso según cronogramas • Hasta 50 entradas
Reenvío de puerto	Hasta 30 entradas
Activación de puerto	Hasta 30 entradas
Bloqueo	Java, cookies, ActiveX, proxy HTTP
Filtrado de contenido	Bloqueo estático de dirección URL o bloqueo de palabras clave
Administración segura	• Acceso web HTTPS al administrador de dispositivos • Aplicación de complejidad de nombre de usuario/contraseña
VLAN	802.1Q (VLAN) 7 VLAN admitidas

Ilustración 91 FICHA TÉCNICA CISCO RV325

Elaborado por: Autores

Descripción	Especificación
VPN	
Seguridad IP (IPsec)	• 36 túneles IPsec de sitio a sitio para conectividad de sucursales • 25 túneles VPN IPsec a través del cliente VPN de Cisco y clientes de terceros como "The GreenBow"para la conectividad VPN de acceso remoto
VPN con SSL	10 túneles VPN con SSL para acceso remoto de clientes
PPTP	10 túneles PPTP para acceso remoto
Cifrado	• Estándar de cifrado de datos (DES) • Estándar de triple cifrado de datos (3DES) • Cifrado con norma de cifrado avanzado (AES): AES-128, AES-192, AES-256
Autenticación	MD5/SHA1
IPsec NAT transversal	Compatible con túneles gateway a gateway y túneles cliente a gateway
Transferencia de VPN	PPTP, Protocolo de túnel de capa 2 (L2TP), IPsec
VPN avanzada	• Detección de punto muerto (DPD) • DNS dividido • Respaldo de VPN • Intercambio de claves por Internet (IKE) con certificado
Calidad de servicio (QoS)	
QoS basada en el servicio	Prioridad o control de velocidad
Control de tráfico	Ancho de banda de carga y descarga por servicio
Tipos de priorización	Prioridad basada en la aplicación en el puerto WAN
Prioridad	Servicios asignados a uno o dos niveles de prioridad
Rendimiento	
Rendimiento de NAT	900 Mbps
Rendimiento de VPN con IPsec	100 Mbps
Rendimiento de VPN con SSL	20 Mbps
Conexiones simultáneas	20.000
Configuración	
Interfaz de usuario web	Administrador de dispositivos de acuerdo con el navegador (HTTP/HTTPS)
Administración	
Protocolos de administración	• Navegador web (HTTP/HTTPS) • Protocolo simple de administración de redes (SNMP) v1, v2c y v3 • Bonjour
Registro de eventos	• Registro local • Syslog • Alerta por correo electrónico • Servicio de mensajes cortos (SMS)
Capacidad de actualización	• Firmware que se puede actualizar mediante el navegador web • Importación o exportación de archivos de configuración de o a una unidad flash USB

Especificaciones del sistema

En la tabla 2, se enumeran las especificaciones del sistema de Cisco RV320.

Tabla 2. Especificaciones del sistema

Descripción	Especificación
Dimensiones del producto (ancho x alto x profundidad)	208 x 132 x 44 mm (8,1 x 5,2 x 1,7 pulgadas)
Puertos	Cuatro puertos RJ-45 Gigabit Ethernet 10/100/1000 Un puerto RJ-45 Gigabit Ethernet (WAN) 10/100/1000 Un puerto RJ-45 Gigabit Ethernet 10/100/1000 DMZ/Internet (WAN)
Fuente de alimentación	12 V 1,5 A

Ilustración 92FICHA TÉCNICA CISCO RV325

Elaborado por: Autores

Descripción	Especificación
Certificación	FCC clase B, CE clase B, UL, cUL, CB, CCC, BSMI, KC, Anatel
Temperatura de funcionamiento	De 0° a 40 °C (32° a 104 °F)
Temperatura de almacenamiento	0° a 70 °C (32° a 158 °F)
Humedad de funcionamiento	De 10 a 85%, sin condensación
Humedad de almacenamiento	De 5 a 90%, sin condensación

Información sobre la garantía

Obtenga información sobre la garantía en la página Product Warranties (Garantías de productos) de Cisco.com.

Información para realizar pedidos

Ofrezca ayuda a los clientes para que comprendan cuáles son los componentes y las piezas que necesitan comprar para instalar y utilizar el producto. En la Tabla 3, se ofrece información para realizar pedidos de Cisco RV320. En esta sección, también se ofrece un vínculo directo a la herramienta de Cisco para realizar pedidos y enumera los números de piezas para la comodidad de los clientes.

Para hacer un pedido, visite la página principal de pedidos de Cisco. Para descargar software, visite el centro de software de Cisco.

Tabla 3. Información para realizar pedidos

Nombre del producto	Número de pieza
Router VPN con WAN dual RV320	RV320-K9-NA
Router VPN con WAN dual RV320	RV320-K9-G5
Router VPN con WAN dual RV320	RV320-K9-AU
Router VPN con WAN dual RV320	RV320-K9-CN
Router VPN con WAN dual RV320	RV320-K9-AR

Garantía limitada de por vida de Cisco para productos Cisco Small Business

Este producto Cisco Small Business incluye una garantía de hardware limitada de por vida. Los términos de la garantía del producto y otra información aplicable a los productos de Cisco están disponibles en www.cisco.com/go/warranty.

Servicio de soporte técnico de Cisco Small Business

Este servicio opcional ofrece cobertura asequible de tres años para su tranquilidad. Este servicio por suscripción a nivel del dispositivo lo ayuda a proteger su inversión y a obtener el máximo valor de los productos Cisco Small Business. Proporcionado por Cisco y respaldado por su partner de confianza, este servicio integral ofrece acceso extendido a Cisco Small Business Support Center y reemplazo de hardware acelerado, de ser necesario.

Más información

Para obtener más información sobre el Router Cisco VPN con WAN Gigabit dual RV320, visite www.cisco.com/go/rv320.

Para obtener más información sobre los productos y soluciones de Cisco Small Business, visite www.cisco.com/smallbusiness.

Ilustración 93FICHA TÉCNICA CISCO RV325

Elaborado por: Autores

CISCO 200 SERIES SWITCHES HOJA DE DATOS

Switches inteligentes Cisco de la serie 200 Cisco Small Business

Construya una red empresarial básica potente y fácil de usar a un precio asequible

La clave del éxito en el competitivo entorno empresarial actual es invertir los recursos con sabiduría, saber cómo separar lo esencial de lo superfluo y aprovechar al máximo su dinero. Como la columna vertebral de sus aplicaciones empresariales y de productividad, la red de una pequeña o mediana empresa se enmarca claramente en la categoría "esencial". Pero eso no significa que usted necesita el conjunto de funciones más avanzadas del mercado.

Con los switches inteligentes Cisco® de la serie 200, puede lograr seguridad y rendimiento en una red de clase empresarial sin pagar por las funciones avanzadas de administración de red que no necesitará. Cuando necesite una solución confiable para compartir recursos de red y conectar computadoras, impresoras y servidores, pero su prioridad principal sea mantener el bajo costo, los switches inteligentes Cisco de la serie 200 son la solución ideal.

Figura 1. Switches inteligentes Cisco de la serie 200

Switches inteligentes Cisco de la serie 200

La serie 200 de Cisco (Figura 1) es un conjunto de switches inteligentes y asequibles que combinan un potente rendimiento y confiabilidad de red con las funciones esenciales de administración de red que usted necesita para una red empresarial sólida. Estos switches Fast Ethernet o Gigabit Ethernet expandibles ofrecen funciones básicas de administración, seguridad y calidad de servicio (QoS) superiores a las que ofrece un switch no administrado o para uso de consumidores, a un costo menor que los switches administrados. Gracias a una interfaz de usuario web fácil de usar, el protocolo de detección de Cisco y Cisco Smartports, usted puede implementar y configurar una red empresarial sumamente sólida en pocos minutos.

Aplicaciones empresariales

Ya sea que necesite conectividad básica de alta velocidad para sus computadoras y servidores o una solución integral de voz, datos y tecnología inalámbrica, los switches Cisco de la serie 200 pueden satisfacer las necesidades de su empresa. Entre las posibles situaciones de implementación, podemos mencionar:

- **Conectividad de alta velocidad para equipos de escritorio.** Los switches Cisco de la serie 200 pueden conectar, de manera rápida y segura, los empleados que trabajan en pequeñas oficinas entre sí y con todos los servidores, las impresoras y demás dispositivos que utilicen. La conectividad confiable de alto

Ilustración 94 FICHA TÉCNICA SWITCH CISCO

Elaborado por: Autores

rendimiento acelera la transferencia de archivos y el procesamiento de datos, aumenta el tiempo de actividad de la red y mantiene a los empleados conectados y productivos.

- **Conectividad inalámbrica altamente segura.** Los switches Cisco de la serie 200 funcionan con soluciones inalámbricas de Cisco y de terceros para extender el alcance de su red. Los empleados pueden trabajar de manera productiva desde salas de conferencias y áreas comunes, colaborar en cualquier oficina y acceder a aplicaciones empresariales desde cualquier lugar en que se encuentren. Con sus funciones de seguridad, alimentación por Ethernet (PoE), Auto Smartports, VLAN y QoS, estos switches son la base perfecta para añadir conectividad inalámbrica de nivel empresarial a una red.
- **Comunicaciones unificadas.** La serie 200 de Cisco ofrece funciones de calidad de servicio (QoS) para que pueda dar prioridad al tráfico sensible a retardos en la red y permitir la convergencia de todas las soluciones de comunicación, como telefonía IP y videovigilancia, en una sola red Ethernet. Cisco ofrece una cartera completa de telefonía IP y otros productos de comunicaciones unificadas diseñados para pequeñas y medianas empresas y los switches Cisco de la serie 200 han sido probados rigurosamente para ayudar a garantizar una integración fácil y compatibilidad total con productos de Cisco y de otros proveedores.

Funciones y ventajas

Los switches inteligentes Cisco de la serie 200 ofrecen todas las funciones que necesita para crear una red de clase empresarial básica a un precio asequible. Estas funciones incluyen:

- **Fácil configuración y administración:** los switches Cisco de la serie 200 están diseñados para facilitar la implementación y el uso por parte de las pequeñas y medianas empresas o los partners que les prestan servicios. Las interfaces web fáciles de usar reducen el tiempo de implementación, administración y solución de problemas en la red. Entre las funciones clave se encuentran:
  - Protocolo de detección de Cisco y protocolo de detección de capa de enlace (LLDP-MED) detectan automáticamente todos los dispositivos conectados a la red y se configuran de forma automática para la conectividad adecuada e indican a los dispositivos que utilicen los parámetros adecuados de QoS o VLAN de voz.
  - Tecnología Cisco Smartports: proporciona capacidades más avanzadas y un control práctico mediante la configuración automática de los puertos con niveles específicos de seguridad, QoS y disponibilidad de acuerdo con el tipo de dispositivo conectado, según las configuraciones probadas previamente y las mejores prácticas de Cisco. La función Auto Smartports aplica automáticamente la inteligencia proporcionada a través de las funciones de Smartports al puerto basado en los dispositivos detectados en el protocolo de detección de Cisco o LLDP-MED. Esta capacidad facilita las implementaciones sin intervención.
  - Utilidad de detección de red Cisco FindIT: funciona mediante una simple barra de herramientas en el navegador web del usuario a fin de detectar dispositivos Cisco en la red y mostrar información básica, como números de serie y direcciones IP, para contribuir a la configuración y agilizar la implementación de los productos Cisco Small Business. Para obtener más información y descargar la utilidad, visite www.cisco.com/go/findit.
- **Rendimiento y escalabilidad:** los switches Cisco de la serie 200 han sido probados para ofrecer la alta disponibilidad y el rendimiento que espera de un switch Cisco, lo que lo ayudará a evitar costosos tiempos de inactividad. Los switches aceleran los tiempos de transferencia de archivos, mejoran las redes lentas e inactivas, mantienen la disponibilidad de las aplicaciones empresariales vitales y permiten que los empleados respondan con mayor rapidez a los clientes y a otros empleados. Gracias a una red basada en switches Cisco de la serie 200, puede abordar todas las necesidades de conectividad y de comunicaciones empresariales y reducir el costo total de propiedad de su infraestructura tecnológica.

Ilustración 95TÉCNICA SWITCH CISCO

Elaborado por: Autores

- **Alimentación por Ethernet (PoE):** los switches Cisco de la serie 200 se encuentran disponibles con PoE en modelos Fast Ethernet y Gigabit Ethernet. Esta capacidad simplifica la implementación de telefonía IP, tecnología inalámbrica, videovigilancia y otras soluciones dado que le permite enviar datos y alimentación a los terminales de la red a través del mismo cable de red. Sin necesidad de contar con fuentes de alimentación por separado o tomacorrientes para teléfonos IP, cámaras IP o puntos de acceso inalámbricos, puede agilizar la implementación y la instalación, además de aprovechar las tecnologías de comunicación avanzadas en forma rápida y a un menor costo.
- **Seguridad de red:** los switches Cisco de la serie 200 ofrecen las funciones de seguridad y administración de red que necesita para mantener un alto nivel de seguridad para su empresa, evitar que usuarios no autorizados accedan a la red y proteger la información empresarial. Los switches ofrecen seguridad de red integrada para reducir el riesgo de violación a la seguridad, con seguridad de puertos IEEE 802.1X para controlar el acceso a la red. La prevención de ataques de denegación de servicio (DOS) aumenta el tiempo de actividad de la red en presencia de un ataque.
- **Compatibilidad con telefonía IP:** los switches Cisco de la serie 200 incluyen funciones de calidad de servicio (QoS) para dar prioridad a los servicios sensibles a retardos, como voz y video, simplificar las implementaciones de comunicaciones unificadas y garantizar un rendimiento uniforme de red para todos los servicios.
- **Implementación automática de voz en toda la red:** mediante una combinación de protocolo de detección de Cisco, LLDP-MED, Auto Smartports y el protocolo VSDP (Protocolo de descubrimiento de servicios), un protocolo único de Cisco cuya patente está en trámite, los clientes pueden implementar una red de voz de punta a punta en forma dinámica. Los switches de la red convergen automáticamente en una sola VLAN de voz y un conjunto de parámetros de QoS, y luego los propagan a los teléfonos en los puertos donde se descubran. Por ejemplo, las funciones automáticas de VLAN de voz le permiten conectar cualquier teléfono IP (incluso teléfonos de terceros) en su red de telefonía IP y obtener tono de marcación de inmediato. El switch configura el dispositivo automáticamente con los parámetros adecuados de QoS y VLAN para priorizar el tráfico de voz.
- **Compatibilidad con IPv6:** a medida que el esquema de asignación de direcciones IP de la red evoluciona para utilizar más dispositivos, tendrá la seguridad de que su red está preparada. Los switches Cisco de la serie 200 ofrecen compatibilidad nativa con IPv6, además del tradicional IPv4. Esto significa que podrá aprovechar al máximo los sistemas operativos y las aplicaciones compatibles con IPv6 en el futuro, sin necesidad de actualizar sus equipos de red.
- **Una solución de óptimo rendimiento energético:** los switches Cisco de la serie 200 están diseñados para lograr un óptimo rendimiento energético y ecológico sin perjudicar su rendimiento. Permiten conservar la energía mediante la optimización de su consumo, lo que contribuye a la protección del medio ambiente y reduce los costos de energía. Las funciones de ahorro de energía comprenden:
  - Ethernet de ahorro de energía (EEE, el IEEE estándar 802.3az), compatible con todos los modelos de switches Gigabit Ethernet Cisco de la serie 200. EEE mejora la eficacia de los equipos de red y proporciona mecanismos de señalización estandarizados que pueden habilitar las transiciones rápidas entre el funcionamiento normal y los estados de inactividad de bajo consumo (LPI) en los sistemas en cualquier extremo del enlace de la capa física.
  - Apagado automático en puertos Gigabit Ethernet cuando un enlace no está activo.
  - Inteligencia integrada para ajustar la energía según la longitud de los cables en modelos Gigabit Ethernet.

Ilustración 96TÉCNICA SWITCH CISCO

Elaborado por: Autores

- Diseño sin ventilador en la mayoría de los modelos, que reduce el consumo de energía, aumenta la confiabilidad y brinda un funcionamiento más silencioso.

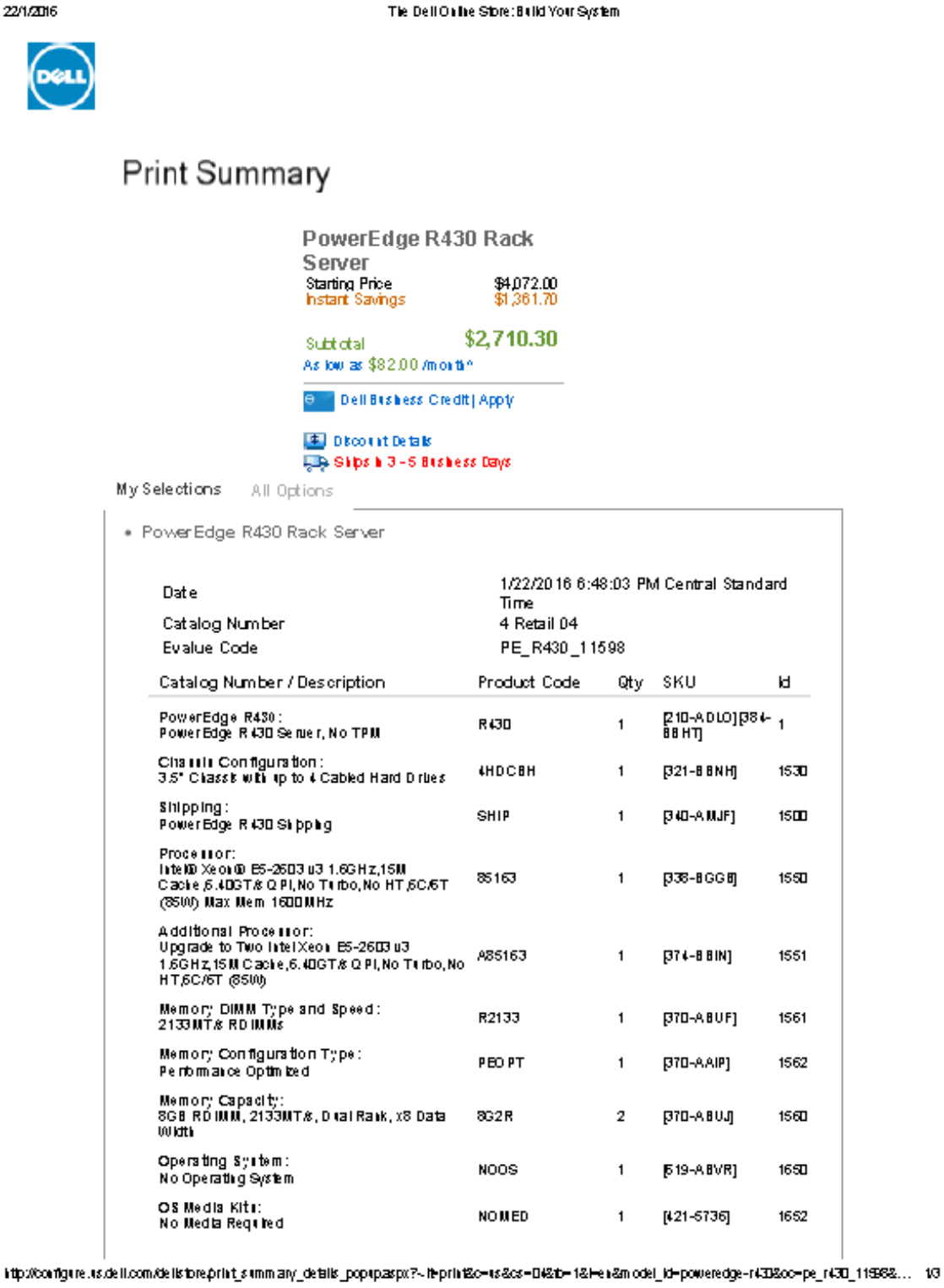
- **Puertos Gigabit Ethernet adicionales:** la serie 200 de Cisco ofrece más puertos por switch que otros switches en el mercado. Esto le brinda mayor flexibilidad para conectar y fortalecer su empresa. Los modelos Gigabit Ethernet incluyen switches de 26 y 50 puertos, en comparación con los dispositivos tradicionales que ofrecen 20 o 44 puertos con 4 puertos compartidos. La serie 200 de Cisco ofrece también ranuras de expansión mini convertidor de interfaz Gigabit (mini-GBIC) que le permiten agregar conectividad uplink Gigabit Ethernet o por fibra óptica al switch. La capacidad de aumentar la variedad de opciones de conectividad de los switches le brinda una mayor flexibilidad de diseño de red en su entorno empresarial específico y la facilidad de conexión de switches en los diferentes pisos o en toda la empresa.
- **Tranquilidad y protección de la inversión:** los switches Cisco de la serie 200 ofrecen el rendimiento confiable, la protección de la inversión y la tranquilidad que espera de un switch Cisco. Si invierte en la serie 200 de Cisco, obtendrá las siguientes ventajas:
  - Garantía limitada de por vida de Cisco para proteger su inversión.
  - Pruebas rigurosas para garantizar una fácil integración y compatibilidad con otros productos de redes y comunicaciones de Cisco, como la cartera completa de Cisco Small Business.
- **Garantía limitada de por vida:** los switches Cisco de la serie 200 vienen con la garantía de hardware limitada de por vida de Cisco, con reemplazo por devolución al fabricante, 1 año de garantía limitada para ventiladores y fuentes de alimentación y una garantía de software limitada de 90 días. Además, Cisco ofrece actualizaciones de software con corrección de errores durante el plazo de la garantía y soporte técnico por teléfono sin costo alguno durante los primeros 12 meses a partir de la fecha de compra. Para descargar actualizaciones de software, visite www.cisco.com/cisco/web/download/index.html.
- **Compatibilidad de primera clase:** para ampliar la cobertura de soporte más allá de las disposiciones de la garantía, elija el servicio de soporte de Cisco Small Business, que le permite obtener el mayor valor de las soluciones de Cisco Small Business y a su vez le proporcionará tranquilidad a un precio asequible. Este servicio por suscripción ofrece actualizaciones de software, acceso al centro de soporte para pequeñas y medianas empresas Cisco Small Business Support Center, reemplazo de hardware el siguiente día hábil (si fuese necesario) y soporte telefónico y vía chat en línea. Para obtener más información, visite www.cisco.com/go/smbservices.

  Para saber dónde se encuentra disponible el servicio de soporte técnico de Cisco Small Business, visite https://supportforums.cisco.com/community/netpro/small-business/sbcountrysupport.
- Varias opciones de idioma: la serie 200 de Cisco está disponible en siete idiomas: inglés, francés, alemán, italiano, español, japonés y chino simplificado. Toda la documentación de los productos y la mayoría de las interfaces de usuario están traducidas, lo que le permite seleccionar su idioma preferido.

Ilustración 97TÉCNICA SWITCH CISCO

Elaborado por: Autores

SERVIDOR DELL POWER EDGW R430



22/1/2016 The Dell Online Store: Build Your System

Print Summary

PowerEdge R430 Rack Server

Starting Price $4,072.00
Instant Savings $1,361.70

Subtotal $2,710.30
As low as $82.00 /month*

Dell Business Credit | Apply

Discount Details
Ships in 3 - 5 Business Days

My Selections All Options

- PowerEdge R430 Rack Server

Date	1/22/2016 6:48:03 PM Central Standard Time
Catalog Number	4 Retail 04
Evalue Code	PE_R430_11598

Catalog Number / Description	Product Code	Qty	SKU	Id
PowerEdge R430: PowerEdge R430 Server, No TPM	R430	1	[210-ADLO][384-BBHT]	1
Chassis Configuration: 3.5" Chassis with up to 4 Cabled Hard Drives	4HDCBH	1	[321-BBNH]	1530
Shipping: PowerEdge R430 Shipping	SHIP	1	[340-AMJF]	1500
Processor: Intel® Xeon® E5-2603 v3 1.6GHz,15M Cache,6.4GT/s QPI,No Turbo,No HT,6C/6T (85W) Max Mem 1600MHz	E5163	1	[338-BGGB]	1550
Additional Processor: Upgrade to Two Intel Xeon E5-2603 v3 1.6GHz,15M Cache,6.4GT/s QPI,No Turbo,No HT,6C/6T (85W)	A85163	1	[374-BBIN]	1551
Memory DIMM Type and Speed: 2133MT/s RDIMMs	R2133	1	[370-ABUF]	1561
Memory Configuration Type: Performance Optimized	PEOPT	1	[370-AAIP]	1562
Memory Capacity: 8GB RDIMM, 2133MT/s, Dual Rank, x8 Data Width	8G2R	2	[370-ABUJ]	1560
Operating System: No Operating System	NOOS	1	[619-ABVR]	1650
OS Media Kits: No Media Required	NOMED	1	[421-5736]	1652

http://configure.us.dell.com/dellstore/print_summary_details_popup.aspx?~ltr=print2c=us&cs=04&b=1&l=en&model_id=poweredge-r430&oc=pe_r430_11598&... 1/3

Ilustración 98 Proforma Adquisición Del Servidor Hoja 1

Elaborado por: Autores

RAID Configuration: RAID 5 for H330/H730/H730P (3-4 HDDs) with Cabled Chassis	R5HC	1	[780-BBQI]	1540
RAID Controller: PERC H330 RAID Controller	H330	1	[405-AAEF]	1541
Hard Drive: 1TB 7.2K RPM SATA 6Gbps 3.5in Cabled Hard Drive	1TB6CB	3	[400-AFXX]	1570
PCIe Riser: No Riser - (No add-on PCIe card allowed)	NOPCIE	1	[330-BBED]	1510
Additional Network Card: On-Board Broadcom 5720 Quad Port 1Gb LOM	OBNICQ	1	[542-BBCO]	1514
Power Supply: Dual, Hot-plug, Redundant Power Supply (1+1), 550W	550R	1	[450-AEGZ]	1620
Power Cord: NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m), Power Cord, North America	125V10	2	[450-AALV]	1621
Power Management BIOS Settings: Power Saving DellActive Power Controller	DAPC	1	[750-AABF]	1533
Rack Rails: ReadyRails™ Sliding Rails With Cable Management Arm	RRCMA	1	[770-BBBL]	1610
Bezel: No Bezel	NOBEZL	1	[350-BBBW]	1532
Internal Optical Drive: DVD, SATA, Internal for 4 HD Chassis	DVD12	1	[429-AAAN]	1600
System Documentation: Electronic System Documentation and OpenManage DVD Kit for R430	EDOCS	1	[343-BBDT]	1590
Processor Thermal Configuration: 2 CPU Standard	2CPU	1	[370-ABXP] [370-ABXV] [374-BBIJ] [374-BBIJ]	1697
Embedded Systems Management: IDRAC8, Basic	IBAS	1	[385-BBIJ]	1520
Shipping Information: US No Canada Ship Charge	USNONE	1	[332-1286]	111
Hardware Support Services: 3 Year Basic Hardware Warranty Repair, 5X10 HW-Only, 5X10 NBD On-site	U3OS	1	[996-8029] [997-2924] [997-2926]	29
Deployment Services: No Installation	NOINSTL	1	[900-9997]	714
Remote Consulting Services: Declined Remote Consulting Service	NORCS	1	[973-2426]	735
Proactive Systems Management: Dell Proactive Systems Management - Declined	NOPSM	1	[909-0259]	30

Print

Ilustración 99 Proforma Adquisición Del Servidor Hoja 2

Elaborado por: Autores

FOTOGRAFÍAS

Ilustración 100 INFRAESTRUCTURA ANTES DE INTERVENCIÓN

Elaborado por: Autores

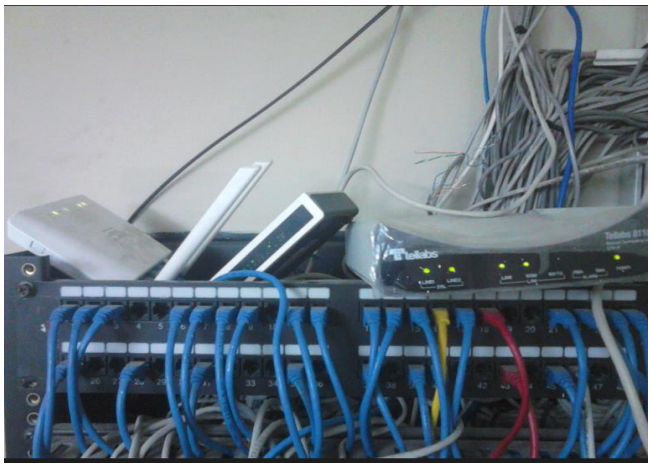


Ilustración 101 CONEXIÓN DE PROVEEDORES DE INTERNET

Elaborado por: Autores

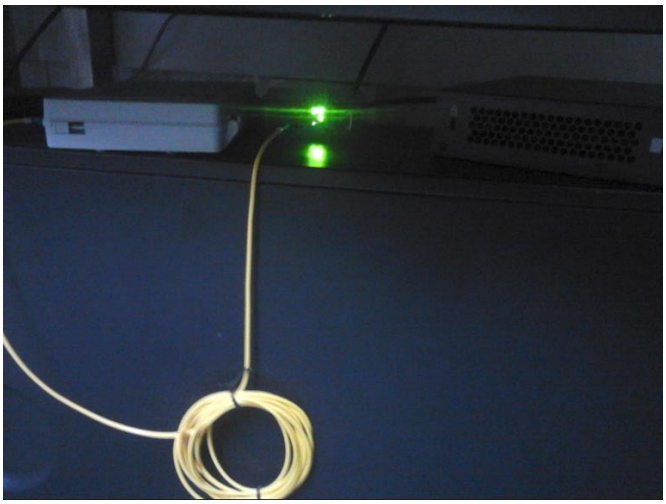


Ilustración 102CONEXIÓN DE PROVEEDORES DE INTERNET

Elaborado por: Autores

Ilustración 103RACK ACTUAL ESTADO

Elaborado por: Autores

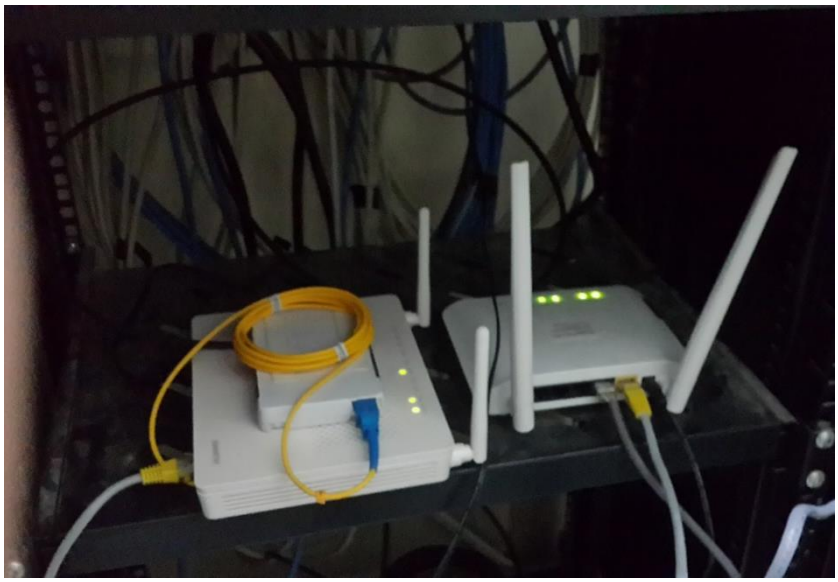


Ilustración 104CONEXION DE PROVEEDORES DE INTERNET FINAL

Elaborado por: Autores