UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION

Diseño y configuración de un nodo de internet con servidores tipo PC usando Zimbra como herramienta de colaboración en grupo, servicio DNS, servicio Web, servicio DHCP, servidor Proxy y una Central Telefónica Virtual utilizando Elastix en el Colegio Cristo Rey de la ciudad de Managua.

Elaborado por:

Br. David Cárdenas García.

Br. Gisselle Obando López.

Br. Roberto Ocampo Benavides.

Tutor:

Msc. Ing. Álvaro Noel Segovia Aguirre.

Managua, 01 de Diciembre de 2014.

AGRADECIMIENTO.

De manera especial agradecemos al Msc. Ing. Álvaro Segovia; nuestro asesor de tesis, por sus consejos, por compartir con nosotros sus conocimientos, por guiarnos y ayudarnos en la realización de esta tesis, con un interés que ha sobrepasado todas las expectativas que como alumnos depositamos en su persona.

A la Dirección Administrativa y Secretaría del Colegio Cristo Rey Managua por abrirnos las puertas del centro, facilitarnos la información y los medios para la realización del presente trabajo.

A nuestras familias y amistades que nos sirvieron como fuente de apoyo constante e incondicional a lo largo de este proceso.

Al grupo de profesores que contribuyeron en nuestra formación como futuros profesionales.

Un agradecimiento especial merece la comprensión, paciencia y ánimo recibido de todos aquellos que de una u otra manera formaron parte de nuestro crecimiento y desarrollo profesional.

A todos ellos, **¡MUCHAS GRACIAS!**

DEDICATORIA

A mi madre y mi padre, que con este trabajo ven coronado su gran sueño, por ser tan especiales y creer en mí.

A toda mi familia, mis amigos y todos los que me estiman y me son fieles tanto en los buenos momentos como en los malos.

Br. David Cárdenas G.

DEDICATORIA.

A Dios por haberme dado salud, inteligencia, sabiduría y la paciencia necesaria para seguir adelante día a día, para lograr mis objetivos y poder culminar exitosamente esta etapa.

A mi madre, por haberme apoyado en todo momento, por darme la mejor educación y enseñarme que todas las cosas hay que valorarlas, trabajarlas y luchar para lograr los objetivos de la vida, por sus consejos, comprensión, sacrificio, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su incondicional amor.

A mis hermanos Liz y Carlos, mi hermosa sobrina Brianna, a quienes adoro y quienes llenan mi vida de alegrías.

A mi familia y amigos que siempre me han apoyado y motivado a salir adelante, a mi novio, amigo y colega, por ser alguien especial en mi vida, por enseñarme y ayudarme a encontrarle el lado positivo a cada momento de frustración durante la elaboración de este documento.

Br. Gisselle Obando L.

DEDICATORIA.

Primeramente a Dios por su amor incondicional, por darme la paciencia para seguir mi camino y poder cumplir mis sueños y sobre todo por regalarme la vida.

A mis padres por apoyarme cada día con abnegación y empeño, por ser mis amigos en todo momento, enseñarme el valor de la vida, la unión familiar, la importancia de la toma de decisiones y por su formación, aquella que sobrepone la humildad ante todo.

A mis profesores por guiarme en el camino de la educación y ser parte de mi crecimiento personal y profesional.

A mis amigos y familiares por su apoyo y finalmente a mi mejor amiga, compañera y colega que se convirtió en un pilar importante en mi vida y en todo este duro proceso de trabajo, por compartir sus sueños y por depositar su amor y confianza en mí.

"Así pues por más difícil que pueda parecer tú debes luchar por cada sueño porque no sabes si lo que dejaste ir pudo haber sido lo que te habría completado".

Br. Roberto Ocampo B.

RESUMEN.

Este trabajo consistió en la propuesta de diseño y configuración de un nodo de internet en el colegio Cristo rey de la ciudad de Managua. En el que se estructuro una red acorde a las necesidades del colegio, tomando en cuenta la cantidad de docentes y estudiantes, infraestructura, áreas administrativas, laboratorios, ubicación geográfica y recursos económicos.

Esta investigación tiene un enfoque cuantitativo, el método utilizado fue el descriptivo, ya que en este estudio se examinó el sitio definiendo sus características, se aplicaron las técnicas de recolección de datos y se procesaron los resultados a fin de verificar si son o no eficientes, se analizaron las ventajas y desventajas que provee la red de servicios a los usuarios. De esta manera se obtuvieron los datos necesarios para seguir desarrollando esta investigación que contiene un elemento de investigación aplicada y a la vez de evaluación tecnológica.

El instrumento utilizado fue la encuesta como herramienta principal del método descriptivo, la cual fue aplicada de manera personal a la población estudiada. El procesamiento de datos se realizó a través de internet haciendo uso de la herramienta estadística SurveyMonkey.

Producto de este trabajo se configuraron los siguientes servidores:

- Servidor de Correo electrónico bajo la suite de colaboración Zimbra (Zimbra Collaboration Suite o ZCS).
- Servidor de alojamiento de sitio web que se identifica como www.colegiocristorey.edu.ni.
- Servidor de nombre de dominio DNS para la resolución de zonas.
- Proxy-Squid, el cual permite el control de acceso a sitios web no deseados, control de descarga de contenido, control de horarios de acceso a internet de la red de área local (LAN), etc.
- Servidor Elastix para central telefónica virtual y servicio DHCP que mejorará la comunicación interna y asigna dinámicamente direcciones IPs.

Con la implementación de estos servidores el centro se verá beneficiado con incorporación de nuevas aplicaciones de comunicación en grupo, permitiendo a los usuarios acceder de forma eficiente y segura a todos los recursos del centro, así como mejorar y fortalecer el sistema de enseñanza-aprendizaje haciendo uso de las nuevas tecnologías de información y comunicación que la era actual demanda.

CONTENIDO

1. INTRODUCCIÓN. 1
2. OBJETIVOS. 3
2.1. Objetivo General. 3
2.2. Objetivos Específicos. 3
3. JUSTIFICACIÓN. 4
4. MARCO TEóRICO. 5
4.1. SERVIDOR DNS. 5
4.1.1. Jerarquía de Dominios. 6
4.1.2. Consulta recursiva e iterativa. 8
4.1.3. Diagrama de Funcionamiento DNS. 11
4.1.4. Resolución de Zonas. 12
4.2. SERVIDOR WEB. 15
4.2.1. Tipos de página web. 18
4.3. SERVIDOR DHCP 20
4.4. SERVIDOR PROXY. 23
4.5. SERVIDOR DE CORREO (ZIMBRA). 26
4.5.1. DNS Y EL ENCAMINAMIENTO DEL CORREO ELECTRONICO. 28
4.5.2. POSTFIX. 30
4.5.3. FUNCIONAMIENTO Y ARQUITECTURA DE POSTFIX. 31
4.5.4. ZIMBRA. 33
4.5.4.1. ARQUITECTURA DE ZIMBRA. 35
4.6. CENTRAL TELEFÓNICA VIRTUAL (ELASTIX). 39
5. Metodología. 43
5.1. Tipo de estudio 43
5.2. El contexto 43
5.3. Los sujetos 43
5.4. Instrumentos de recolección de datos 45
6. ANÁLIsIS DE RESULTADOS. 46
6.1. Requerimientos. 48
6.1.1. Diagnóstico. 48

6.1.1. Factores de éxito. 49
6.1.2. Valoración sobre la implementación de los servicios. 50
6.2. Diseño. 52
6.2.1. Requerimientos de hardware. 52
6.2.2. Descripción general de la red. 53
6.2.3. Presupuesto. 57
6.3. Configuración de los servicios. 57
6.3.1. Configuración e instalación de los servicios. 57
6.3.1.1. DNS 58
6.3.1.2. Servidor Web. 66
6.3.1.3. DHCP. 69
6.3.1.4. PROXY. 71
6.3.1.5. Servidor de Correo. 74
6.3.1.6. Servidor Elastix. 79
6.4. Pruebas. 88
6.4.1. Validación del funcionamiento de los servicios 88
6.4.2. Resultados de entrevistas y encuestas sobre el funcionamiento de los servicios. 96
7. CONCLUSIONES. 100
8. RECOMENDACIONES. 102
9. BIBLIOGRAFÍA. 103
9.1. Webgrafía 103
ANEXOS i
ANEXO 1: GLOSARIO. i
ANEXO 2: Instrumentos de recolección de información. v
ANEXO 3 ix
ANEXO 4 x
ANEXO 5 xi

Índice de figuras

Figura 1 Jerarquía de dominios..... ……..6
Figura 2 Funcionamiento del Resolver ..... ……..8
Figura 3 Consulta Recursiva ..... ……..9
Figura 4 Consulta Iterativa..... ……10
Figura 5 Diagrama de funcionamiento del DNS ..... ……12
Figura 6 Zona Directa DNS ..... ……13
Figura 7 Zona Inversa DNS ..... ……14
Figura 8 Diagrama de funcionamiento protocolo HTTP ..... ……16
Figura 9 Diagrama de funcionamiento Servidor Web……18
Figura 10 Diagrama de funcionamiento Servidor DHCP..... ……21
Figura 11 Diagrama de funcionamiento Servidor Proxy..... ……24
Figura 12 Ciclo de un correo electrónico ..... ……28
Figura 13 Encaminamiento del correo electrónico ..... ……29
Figura 14 Diagrama de flujo de Postfix……..31
Figura 15 Arquitectura de Zimbra ……36
Figura 16 Servicios de Elastix……...41
Figura 17 Estructura de División del trabajo (EDT)……..…...47
Figura 18 Opinión de docentes y estudiantes sobre la implementación de la propuesta dentro del centro…….....50
Figura 19 Opinión de docentes y estudiantes sobre la relevancia de incorporar nuevas tecnologías dentro del centro……51
Figura 20 Estructura general de la red……...53
Figura 21 Especificaciones de las del FORTINET……..……54
Figura 22 Configuración de Firewall……..……55
Figura 23 Tabla de enrutamiento…..……..……56
Figura 24 Contenido del archivo /etc/hosts……..……58
Figura 25 Contenido del archivo /etc/resolv.conf……58
Figura 26 Configuración del archivo /etc/named.conf……59
Figura 27 Configuración del archivo /var/lib/named/colegio.zone…….....63
Figura 28 Uso de los registros IN A……..……64
Figura 29 Archivo /var/lib/named/192.168.0.zone……..…….....65
Figura 30 Configuración de XAMPP……67
Figura 31 Interfaz de ingreso a phpMyAdmin……67

Figura 32 Diagrama estructural de página web…..……68
Figura 33 Interfaz principal de página web……...……69
Figura 34 Interfaz de configuración modo texto de Zeroshell……..……70
Figura 35 Interfaz gráfica de inicio Zeroshell……70
Figura 36 Configuración del DHCP…….……71
Figura 37 Definición de Lista de Control de Acceso……...73
Figura 38 Definición de Reglas de Control de Acceso……...73
Figura 39 Configuración del proxy cache con aceleración……...74
Figura 40 Inicio de instalación de Zimbra……..75
Figura 41 Error DNS……..……..76
Figura 42 Menú principal Zimbra……..76
Figura 43 Submenú Zimbra……...…….77
Figura 44 Servicios de Zimbra corriendo……..…….78
Figura 45 Interfaz gráfica de inicio de Zimbra…….……..……78
Figura 46 Interfaz de inicio de instalación de Elastix…….……79
Figura 47 Selección del Idioma…….....80
Figura 48 Selección del Disco Duro y tipo de particionamiento…….....80
Figura 49 Aviso de Confirmación de borrar particiones de disco duro...……..81
Figura 50 Configuración de Red...……81
Figura 51 Configuración de red para cada interfaz. ……...82
Figura 52 Contraseña root. ……82
Figura 53 Particionamiento y copiado en el Disco Duro……83
Figura 54 Inicialización de Elastix……..……83
Figura 55 Login Elastix. ……..84
Figura 56 Certificado de Seguridad..…….……...….84
Figura 57 Interfaz Web Elastix. ……..…...….85
Figura 58 Creación de troncales……...……...…….86
Figura 59 Creación de extensiones.…….……...….87
Figura 60 Campos para agregar extensión…..…….....….87
Figura 61 Extensiones telefónicas del centro. ..……...….88
Figura 62 Acceso a Blog dentro del sitio web...……...89
Figura 63 Menú de ingreso a docentes para publicación de información...…….89
Figura 64 Comentarios de usuarios registrados. ..……90
Figura 65 Biblioteca Virtual...……..…….....91

Figura 66 Reglamento Institucional.....92
Figura 67 Interfaz de correo electrónico Zimbra.....92
Figura 68 Crear nueva cuenta.....93
Figura 69 Mensajería instantánea.....93
Figura 70 Prueba de softphone Elastix.....94
Figura 71 Interfaz de configuración de teléfonos IP.....95
Figura 72 Opinión sobre la funcionalidad de la página web.....96
Figura 73 Aspectos más interesantes dentro de la página web.....97
Figura 74 Opinión sobre servicio de correo electrónico.....98
Figura 75 Opinión de efectos positivos con la migración a propuesta.....99

Índice de Tablas

Tabla 1 Ventajas y desventajas de Zimbra……..…..…39
Tabla 2 Condiciones técnicas de los equipo del centro……..…..48
Tabla 3 Diagnóstico de las condiciones del sitio…..……..…..…49
Tabla 4 Factores de éxito……..……....…49
Tabla 5 Direcciones de servidores…….…….…....55
Tabla 6 Direcciones de subredes…….……..56
Tabla 7 Presupuesto……..……..…….……...…57

1. INTRODUCCIÓN.

El colegio Cristo Rey se encuentra ubicado en el distrito I de la ciudad de Managua, con una población estudiantil de 318 alumnas, un cuerpo docente conformado por 20 maestros y 5 colaboradores más del área administrativa.

Desde el año 2008 la institución no cuenta con un proveedor que brinde el servicio de internet, siendo el Operador Claro quien anteriormente proveía este servicio.

En la actualidad, el centro posee un blog público en blogspot donde se brinda información general sobre la misión y visión del centro, sin embargo, esta información no se actualiza desde 2009 debido a que no existe una persona encargada para realizar dicha función.

Para dar respuesta a las situaciones antes mencionadas se ha propuesto la elaboración del diseño de un nodo de internet que incluye los servicios DNS, Web, DHCP, Proxy, Correo electrónico y una central telefónica virtual, utilizando como sistema operativo Suse Linux Enterprise Server 11.

Con el propósito de conocer la situación actual del centro, se realizó un análisis completo de la infraestructura de red, esto permitió realizar el diseño de red propuesto en este documento.

La implementación de un medio tecnológico, como es una página web, permite abrir un espacio de comunicación en la red, generando nuevas posibilidades comunicativas, mayor y más fácil cobertura. Además desde el punto de vista académico se convierte en otro recurso para estimular el desarrollo del colegio. De esta manera este proyecto permitirá divulgar la información de las actividades académicas, culturales y religiosas relacionadas con el que hacer del colegio.

El servidor de correo electrónico que se propone es Zimbra, por la seguridad y estabilidad que brinda, permite una comunicación efectiva, es posible crear grupos de trabajo y mantener un mayor control sobre las comunicaciones del personal.

ZIMBRA es un completo programa de mensajería y colaboración de código libre que ofrece herramientas complementarias como libretas de direcciones, agendas y tareas, funciona bajo cualquier sistema operativo con acceso a internet.

Elastix es un software libre que permite la configuración de una central telefónica que viene a reemplazar a las PBX convencionales. En este documento se realizan las configuraciones necesarias para la implementación de una central telefónica virtual dentro del colegio Cristo Rey Managua.

El presente trabajo se encuentra estructurado en 3 partes. La primera etapa contempla la introducción, objetivos y justificación del tema. La segunda etapa corresponde al marco teórico donde se desarrollan los conceptos básicos, funcionamiento y archivos de configuración de los servicios propuestos.

Finalmente en la tercera y última etapa se desarrolla la metodología utilizada, los análisis de resultados, implementación, pruebas, conclusiones y recomendaciones a tomar en cuenta.

2. OBJETIVOS.

2.1. Objetivo General.

Diseñar un nodo de internet con servidor WEB, DHCP, DNS, PROXY y Servidor de correo ZIMBRA como herramienta de colaboración en grupo y una Central Telefónica Virtual utilizando Elastix en el Colegio Cristo Rey de la ciudad de Managua.

2.2. Objetivos Específicos.

- ✓ Realizar un análisis de la infraestructura del colegio Cristo Rey Managua.
- ✓ Realizar el diseño de la red en base a los requerimientos obtenidos.
- ✓ Configurar los servicios DNS, EMAIL, WEB, DHCP y Proxy SQUID en servidores tipo PC.
- ✓ Configurar cada uno de los servicios en la red de área local cableada e inalámbrica con tecnología WIFI.
- ✓ Realizar pruebas de funcionamiento de cada uno de los servicios del nodo de la institución.
- ✓ Configurar el servicio de la Central Telefónica Virtual utilizando ELASTIX.

3. JUSTIFICACIÓN.

En la actualidad, implementar soluciones a nivel de servidor es costoso sobre todo por las licencias a adquirir, aparte de la compra del software y programas que se instalarán en el servidor, como corta fuegos, antivirus, antispam etc. Al trabajar con Linux el costo es mínimo debido a la licencia pública general (GPL) que este sistema operativo utiliza.

Llevar a cabo esta propuesta dentro del centro traerá muchas ventajas, dentro de las más relevantes está el hecho de tener acceso a internet, adquirir un nombre de dominio y tener su propia página web, poseer un correo electrónico corporativo y contar con una central telefónica virtual.

Al contar con un nombre de dominio y su propio sitio web el centro podrá dar a conocer con una correcta presentación su oferta académica, con el conocimiento general del manejo del software tendrá acceso a modificar, actualizar y editar la información en el momento que desee. De igual forma, desde la web podrá atender solicitudes y consultas realizadas por los interesados.

Un correo electrónico gratuito a como es Zimbra es en la actualidad una herramienta básica y necesaria en los diferentes ámbitos de empresas, universidades, colegios, etc., para el uso personal o institucional.

Elastix no solo brinda un medio de comunicación más económico que las comunicaciones tradicionales, sino que además ofrece una gran variedad de funcionalidades que jamás podrán ser utilizadas con los sistemas convencionales.

La incorporación de esta propuesta y el aprovechamiento de los recursos planteados en ella dentro del centro, permitirán mantener una estructura realmente mucho más eficaz por menores costos.

4. MARCO TEÓRICO.

En los siguientes capítulos se realiza una breve descripción del funcionamiento de cada uno de los servicios que fueron instalados y configurados, se aborda de manera general las bases teóricas y archivos de configuración de estos servicios, lo que permite la comprensión y ejecución del diseño propuesto.

4.1. SERVIDOR DNS.

El Sistema de nombres de dominio (DNS, Domain Name System)[1] es un servicio de directorio que traduce los nombres de host en direcciones IP.

DNS es una base de datos distribuida e implementada en una jerarquía de servidores DNS y un protocolo de la capa de aplicación que permite a los host consultar la base de datos distribuida. Además de la traducción de nombres de host en direcciones IP, DNS proporciona otros servicios importantes como: alias de host, alias del servidor de correo y distribución de carga.

Un servidor DNS proporciona resolución de nombres para redes basadas en TCP/IP. Es decir, hace posible que los usuarios de equipos cliente utilicen nombres en lugar de direcciones IP numéricas para identificar hosts remotos. A su vez permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan todas las direcciones IP y todos los nombres de los PCs pertenecientes a su dominio.
Este servicio cumple las siguientes funciones:

a) Resolución de nombres: convierte el nombre de un host en la dirección IP que corresponde.

b) Resolución inversa de direcciones: realiza el mecanismo inverso, de una dirección IP obtiene el nombre del host correspondiente.

[1] **J.A. Berná, M. Pérez, L.M. Crespo, "Redes de Computadores para Ingenieros en Informática". Publicaciones Universidad de Alicante, Alicante, 2002.**

c) Resolución de servidores de correo: de un nombre de dominio obtiene el servidor a través del cual debe realizarse la entrega del correo electrónico.

El DNS utiliza comúnmente el software llamado BIND ("Berkeley Internet Name Domain") que funciona como una base de datos distribuida que mantiene información sobre las direcciones textuales de una Red y la información sobre direcciones lógicas.

La resolución de nombres utiliza una estructura en árbol, mediante la cual los diferentes servidores DNS de las zonas de autoridad se encargan de resolver las direcciones de su zona, y si no se lo solicitan a otro servidor que creen que conoce la dirección.

4.1.1. Jerarquía de Dominios.

DNS utiliza servidores organizados de forma jerárquica y distribuida alrededor de todo el mundo. Podemos decir que existen 3 clases de servidores DNS: servidores DNS de raíz, servidores DNS de dominio superior (TLD, Top-Level Domain) y los servidores de segundo nivel o DNS Autoritativos. Adicional están los subdominios que son creados por organizaciones y se derivan del servidor de segundo nivel. En la figura 1 se muestra como se encuentran organizados una jerarquía de dominios:

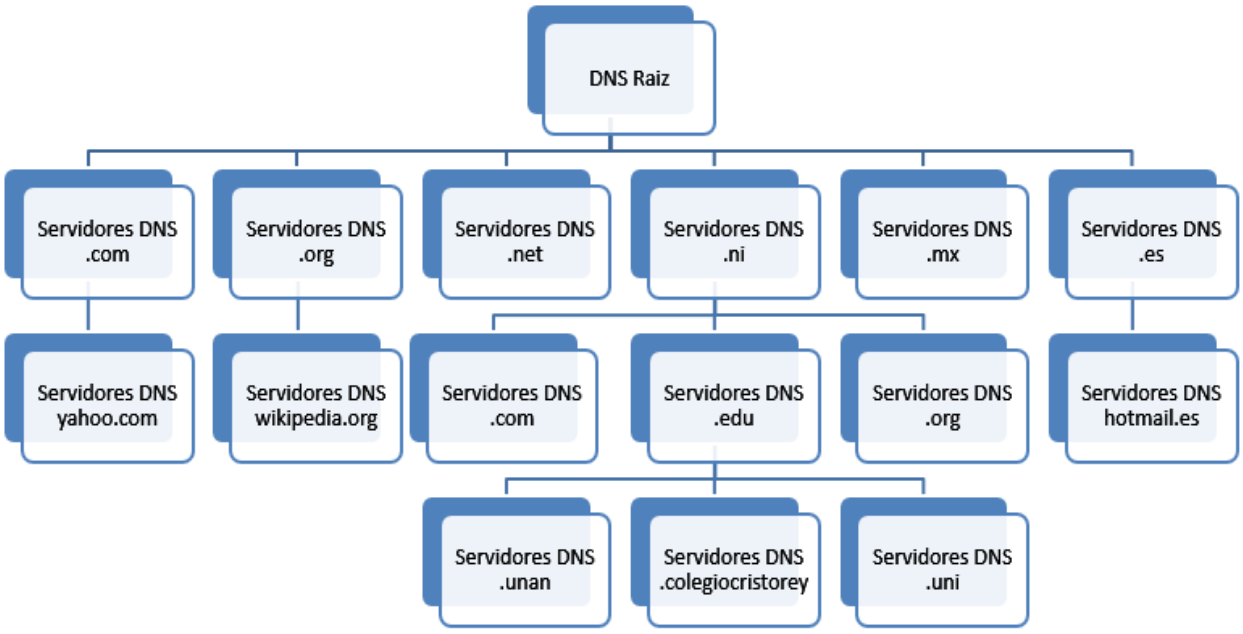


Fig.1. Jerarquía de dominios.

- **Dominio Raíz:** gestionado por la Corporación de Internet para la Asignación de Nombres y Números (ICANN, Internet Corporation for Assigned Named and Number) del que derivan todos. Cuando se utiliza un nombre de dominio DNS, empieza con un punto (.) para designar que el nombre se encuentra en la raíz o en el nivel más alto de la jerarquía del dominio. En este caso, el nombre de dominio DNS se considera completo e indica una ubicación exacta en el árbol de nombres. Los nombres indicados de esta forma se llaman nombres de dominio completos (FQDN, Fully Qualified Domain Names).
- **Dominio de nivel superior:** Un nombre de dos o tres letras que se utilizan para indicar un país o región, o el tipo de organización que usa un nombre.
- **Dominio de segundo nivel:** Nombres de longitud variable registrados que un individuo u organización utiliza en Internet. Estos nombres siempre se basan en un dominio de nivel superior apropiado, según el tipo de organización o ubicación geográfica donde se utiliza el nombre.
- **Subdominios:** Nombres adicionales que puede crear una organización y se derivan del nombre de dominio registrado de segundo nivel. Incluyen los nombres agregados para desarrollar el árbol de nombres de DNS en una organización y que la dividen en departamentos o ubicaciones geográficas.

Toda computadora ya sea Servidor, PC de escritorio o Laptop utilizando Linux, Microsoft Windows o cualquier sistema operativo, utiliza un “Resolver” (Ver figura 2). Este “resolver” es el encargado de encontrar la resolución de nombres para todos los programas que soliciten una resolución, esto es cuando de un navegador web se visita un sitio, el navegador web se comunica con el “Resolver”, cuando se envía un correo electrónico el "Mailer", se comunica con el “Resolver”, al realizar un telnet se utiliza el “Resolver”, y es este mismo “Resolver” es quien regresa los resultados al programa que está solicitando la información.

Esta información es precisamente la resolución de nombres de dominios a direcciones IP.

La resolución de un nombre de dominio es la traducción del nombre a su correspondiente dirección IP. Para este proceso de traducción los "resolvers" pueden formular dos tipos de preguntas, recursivas e iterativas.

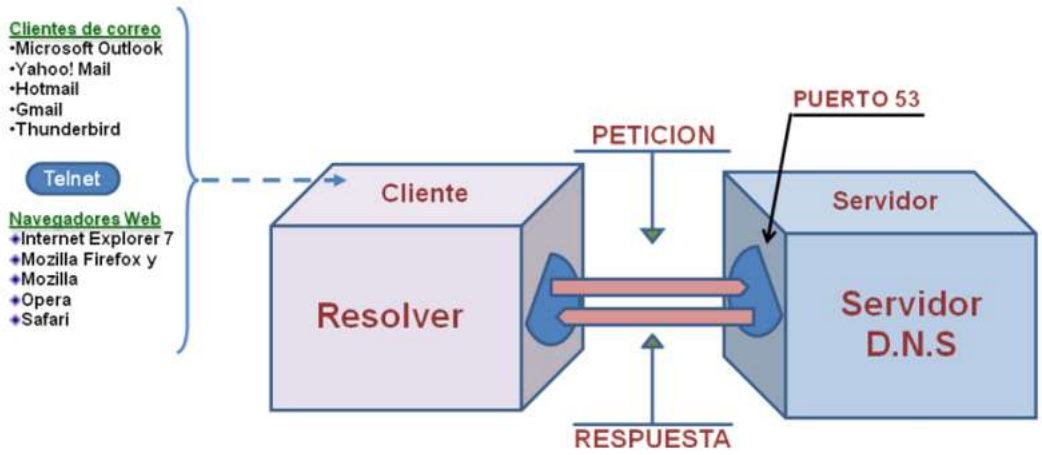


Fig. 2. Funcionamiento del "Resolver".

4.1.2. Consulta recursiva e iterativa.

Una consulta es una solicitud de resolución de nombres que se envía a un servidor DNS. Para la resolución de una solicitud se ejecuta una consulta recursiva o iterativa. La diferencia entre los dos es la decisión de si la resolución del servidor DNS evita o no todos los servidores DNS en el mundo para encontrar la correspondencia entre el nombre de dominio y la dirección IP de su servidor web.

Todas las consultas DNS se realizan a través del puerto 53. En los dos casos, cuando a un servidor DNS le llega una consulta lo primero que hace es comprobar si existe el dominio en su zona o en su caché y, en caso de no tenerla, consulta al servidor superior en jerarquía, devuelve el resultado (según el tipo de consulta) y guarda la resolución en caché.

Una consulta recursiva ocurre cuando el servidor DNS local no contiene la información en sus datos locales y realiza todo un proceso para entregar al cliente la mejor respuesta. En la figura 3 se ejemplifica el camino que sigue una resolución recursiva:

1. El cliente realiza la consulta a su servidor DNS local de www.google.com
2. El servidor DNS local envía la consulta al servidor DNS raíz.
3. El DNS raíz observa el .com y consulta al servidor TLD.
4. El servidor TLD pregunta al servidor DNS autoritativo la IP solicitada.
5. El servidor autoritario del dominio responde con la IP correspondiente.
6. El servidor TLD envía la IP al servidor raíz.
7. El servidor raíz envía la IP al servidor DNS local.
8. El servidor DNS local le comunica al cliente que www.google.com es igual a 74.125.230.224.
9. El cliente accede a la web.

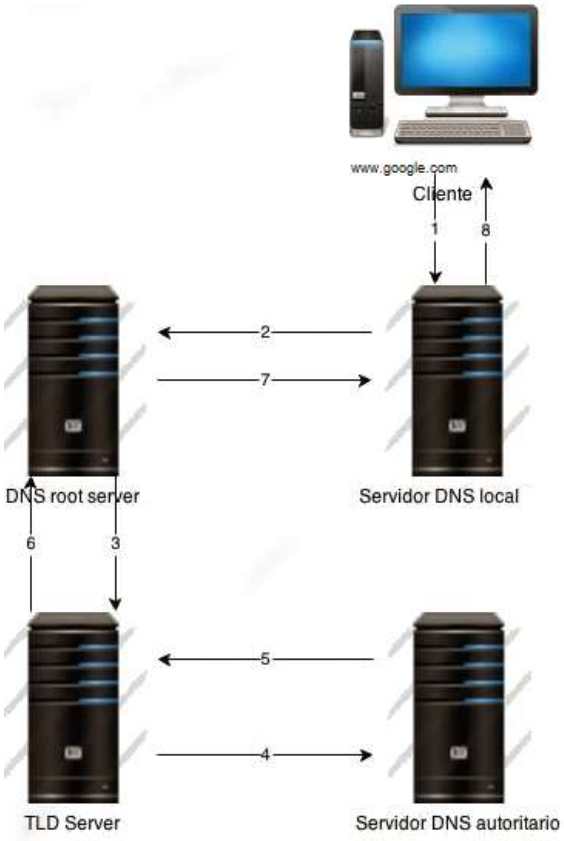


Fig. 3. Consulta Recursiva.

Las consultas iterativas consisten en la respuesta completa que el servidor de nombres pueda dar en función del contenido de su caché. Este proceso es demostrado en la figura 4.

1. El cliente realiza la consulta a su servidor DNS local la IP de www.google.com
2. El servidor DNS envía la consulta al servidor DNS raíz.
3. El DNS raíz contesta con una lista de los servidores TLD .com para www.google.com
4. El servidor DNS local pregunta al servidor TLD la IP de www.google.com
5. El servidor TLD responde con la IP del servidor DNS autoritario del dominio www.google.com.
6. El servidor DNS local pregunta al servidor DNS autoritario del dominio google.com la IP de www.google.com.
7. El servidor DNS autoritario responde que la dirección IP de www.google.com es 74.125.230.224.
8. El servidor DNS local le comunica al cliente que www.google.com es igual a 74.125.230.224.
9. El cliente accede a la web.

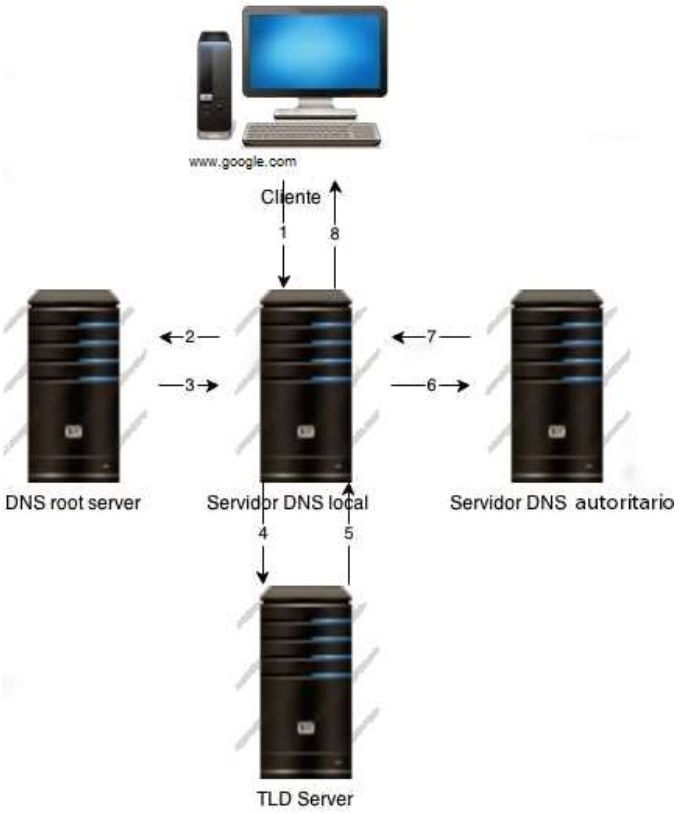


Fig. 4. Consulta Iterativa.

4.1.3. Diagrama de Funcionamiento DNS.

Cuando se desea acceder a una dirección web se teclea en la barra de direcciones el nombre de la página, automáticamente el sistema operativo comprueba la petición realizada, si no lo encuentra en su registro realiza la petición al servidor DNS que se tiene configurado manualmente, en caso de que este tampoco tenga almacenada la dirección IP de ese domino, se escala la petición al servidor encargado de la zona de autoridad quien tiene una tabla donde se almacenan las direcciones IP y sus dominios, busca y responde a la solicitud con la dirección del sitio. El DNS configurado en la PC manualmente realiza la petición a la dirección obtenida para conocer donde se encuentra alojada la página, cuando se recibe respuesta a la solicitud hecha se realiza el intercambio de paquetes.

Cuando un cliente necesita resolver una solicitud envía un requerimiento al servidor DNS local, a partir de entonces se desencadena el proceso de resolución del nombre mostrado en la figura número 5.

1. El usuario realiza una petición de acceso, ejemplo: www.google.com.ni.
2. El servidor local recibe la petición y busca en su base de datos dicha dirección.
3. El servidor local interroga al servidor raíz.
4. El servidor raíz envía la dirección IP de www.google.com.ni al servidor local.
5. El servidor local hace una petición al servidor TLD preguntando por www.google.com.
6. El servidor TLD envía la dirección.
7. El servidor local recibe la dirección y se la envía al host usuario.
8. El host usuario solicita la información directamente al host autoritario.
9. El host autoritario envía la información solicitada por el host usuario.
10. La página web es mostrada en el navegador y se logra establecer la conexión.

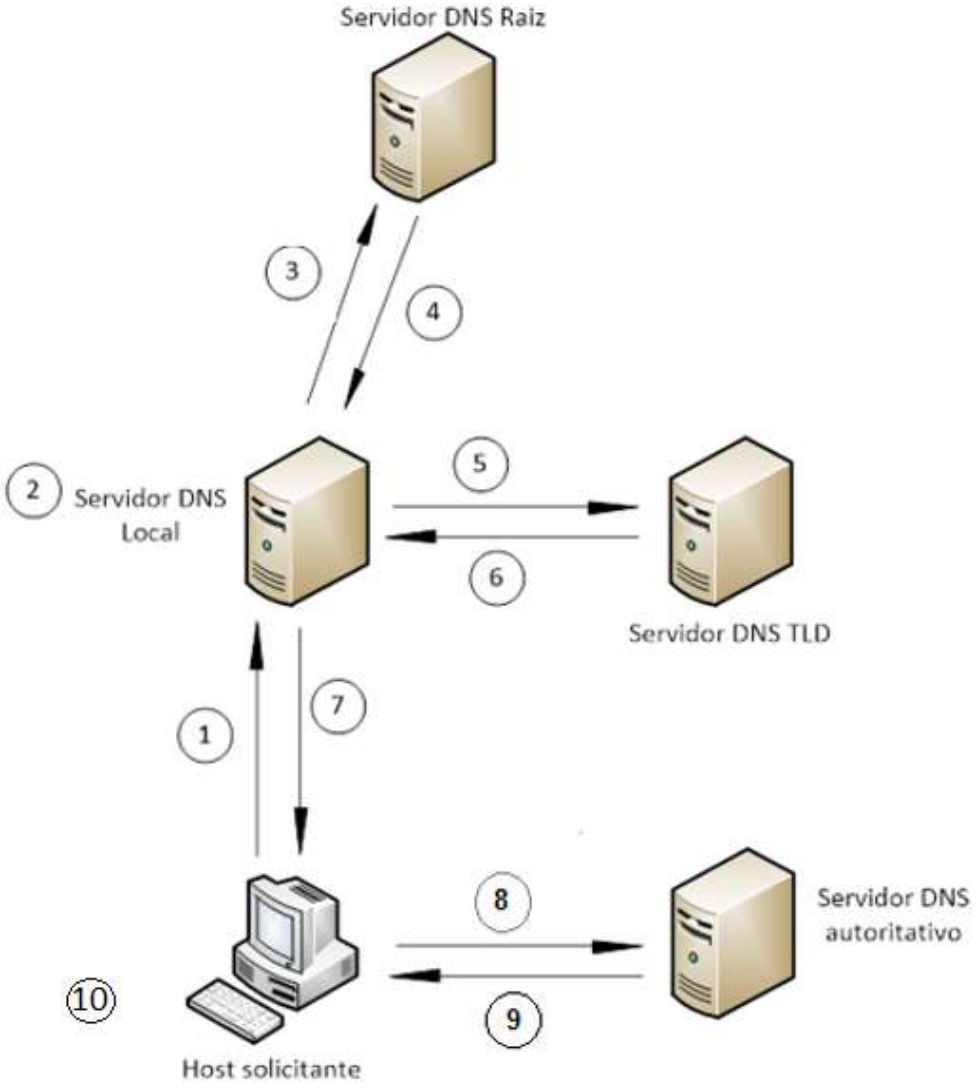


Fig. 5. Diagrama de funcionamiento del DNS.

4.1.4. Resolución de Zonas.

Una zona es el origen de autoridad de la información sobre cada uno de los nombres de dominio DNS incluidos en la zona, cada zona almacena información de nombre sobre uno o más dominios DNS.

- **Zona Directa**

La Zona Directa es la zona que usa el DNS para poder resolver las IPs de los nombres de dominio.

En la mayor parte de las conexiones hechas a través de Internet se utiliza el nombre de los host en vez de sus direcciones IP ya que los nombres son más fáciles de

memorizar que los números. Antes de iniciarse la conexión el protocolo DNS traduce el nombre de host en una dirección IP. Este proceso se llama Resolución de zona directa, o sea, conversión del nombre en dirección IP y está representado en la figura 6.

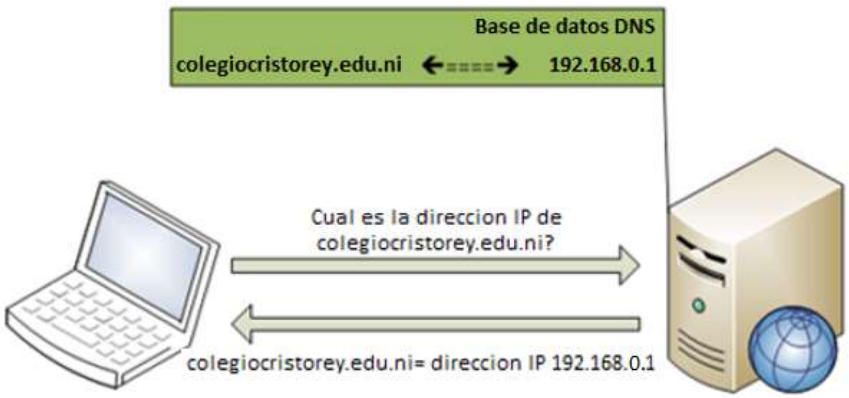


Fig. 6. Zona Directa DNS.

- **Zona Inversa**

La búsqueda DNS inversa es la determinación de un nombre de dominio que está asociado a una determinada dirección IP utilizando el DNS de Internet.

Aunque la función más común de DNS es proporcionar asignaciones de nombres a direcciones IP, hay muchas circunstancias en que se requiere la traducción inversa. Por ejemplo, un servidor que recibe una solicitud de conexión TCP/IP entrante es capaz de determinar la dirección IP de origen de la conexión desde el datagrama IP entrante, pero el nombre (n) correspondiente a la dirección no se realiza en la propia conexión; tal nombre (n) debe ser consultado de alguna otra forma. El uso inteligente del DNS puede proporcionar esta capacidad utilizando el registro PTR RR[2].

Para dar solución a esta problemática, el estándar DNS adoptó un dominio especial, el dominio "`in-addr.arpa`" con el fin de proporcionar una forma práctica y confiable para realizar las consultas inversas.

[2] **El registro PTR es el registro de recurso (RR) de un dominio que define las direcciones IP de todos los sistemas en una notación invertida.**

El dominio `in-addr.arpa` es el dominio estándar del que cuelgan las inversas, se usa en todas las redes TCP/IP que se basan en el direccionamiento del Protocolo de Internet versión 4 (IPv4). El Asistente para crear zona nueva supone de forma automática que se usa este dominio cuando se crea una zona de búsqueda inversa nueva tal y como se muestra en la figura siguiente:

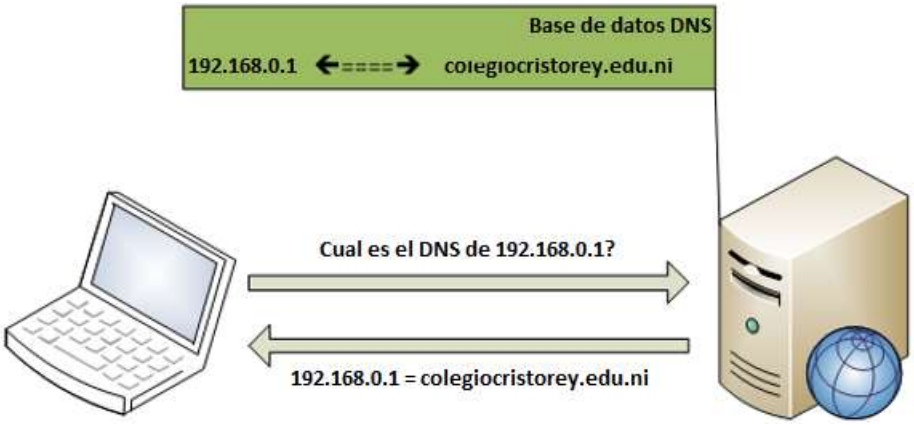


Fig. 7. Zona Inversa DNS.

Ejemplo: inicialmente el cliente consulta al servidor DNS un registro de recursos de puntero (PTR) que asigna la dirección IP 192.168.0.1

Ya que esta consulta se realiza en los registros de puntero, el solucionador invierte la dirección y agrega el dominio `in-addr.arpa` al final de la dirección inversa. De esta manera, forma el nombre de dominio completo ("`1.0.168.192.in-addr.arpa`.") que se va a buscar en una zona de búsqueda inversa. Una vez localizado, el servidor DNS con autoridad en "`1.0.168.192.in-addr.arpa`" puede responder con la información del registro de puntero PTR. Esto incluye el nombre de dominio DNS lo que completa el proceso de búsqueda inversa.

4.2. SERVIDOR WEB.

Los servidores web son aquellos cuya tarea es alojar sitios y/o aplicaciones, las cuales son accedidas por los clientes utilizando un navegador que se comunica con el servidor utilizando el protocolo de transferencia de hipertextos (HTTP, Hypertext Transfer Protocol) el cual se mantiene a la espera de peticiones de clientes y le responde con el contenido según sea solicitado.[3]

El protocolo HTTP es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP, atendiendo a las necesidades de un sistema global de distribución de información como la red global mundial (WWW, World Wide Web), este protocolo fue diseñado originalmente como un protocolo de transferencia de documentos de texto. El proceso es más o menos el mostrado en la siguiente figura:

HTTP es un protocolo de solicitud/respuesta. Cuando un cliente, por lo general un explorador Web, envía una solicitud a un servidor Web, HTTP especifica los tipos de mensaje que se utilizan para esa comunicación. Los tres tipos de mensajes comunes son:

- GET es una solicitud de datos por parte del cliente. Un cliente (explorador Web) envía el mensaje GET al servidor Web para solicitar las páginas HTML. Cuando el servidor recibe la solicitud GET, este responde con una línea de estado, como HTTP/1.1 200 OK, y un mensaje propio. El mensaje del servidor puede incluir el archivo HTML solicitado, si está disponible, o puede contener un mensaje de error o de información, como “Se modificó la ubicación del archivo solicitado”.
- Los mensajes POST y PUT se utilizan para subir datos al servidor Web. Por ejemplo, cuando el usuario introduce datos en un formulario que está integrado en una página Web, el mensaje POST se envía al servidor Web. En el mensaje POST, se incluyen los datos que el usuario introdujo en el

[3] Rodriguez, P. (23 de enero de 2009). *Estudio Seijo*. Recuperado el 21 de agosto de 2014, de http://www.estudioseijo.com/noticias/tipo-de-sitios-web.html

formulario. PUT carga los recursos o el contenido en el servidor Web. Por ejemplo, si un usuario intenta subir un archivo o una imagen a un sitio Web, el cliente envía un mensaje PUT al servidor con la imagen o el archivo adjunto.

Para una comunicación segura a través de Internet, se utiliza el protocolo HTTP seguro (HTTPS) para acceder o subir información al servidor Web. El HTTPS puede utilizar autenticación y encriptación para asegurar los datos mientras viajan entre el cliente y el servidor, a su vez especifica reglas adicionales para pasar datos entre la capa de aplicación y la capa de transporte. El protocolo HTTPS utiliza el mismo proceso de solicitud del cliente-respuesta del servidor que HTTP, pero el stream de datos se encripta con capa de sockets seguros (SSL) antes de transportarse a través de la red. El HTTPS crea una carga y un tiempo de procesamiento adicionales en el servidor debido a la encriptación y el descifrado de tráfico. La figura 8 muestra el diagrama de funcionamiento del protocolo HTTP:

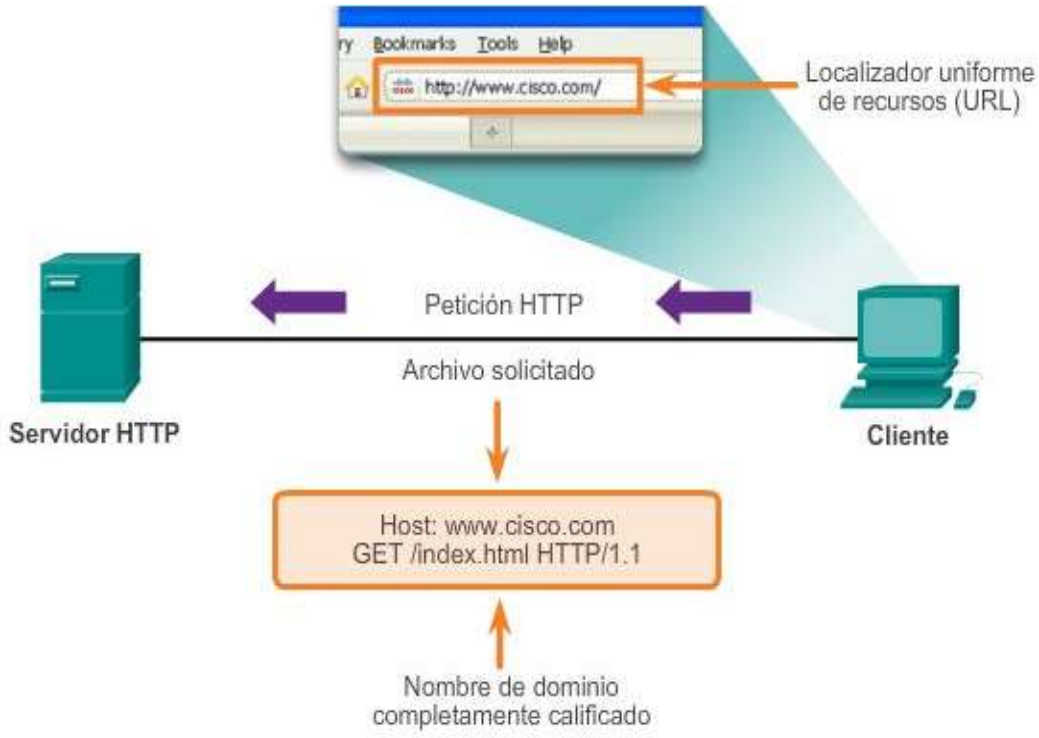


Fig. 8. Diagrama de funcionamiento del protocolo HTTP.

Ejemplo: cuando en el lado del cliente se ingresa una URL en el navegador, se establece una comunicación con el puerto 80 del Servidor Web y se establece el HTTP. La conexión durará durante el tiempo de transferencia de la información para cargar la página web, luego procederá a cerrar la conexión automáticamente y volverá a establecer conexión cuando se vuelva a solicitar una petición.

La figura número 9 muestra el proceso mediante el cual un cliente realiza una solicitud y recibe una respuesta de parte del servidor web:

1. El cliente envía la petición de solicitud de página web, accede a una URL y selecciona un enlace de un documento HTML

2. El servidor recibe una petición, descodifica la URL, identifica el protocolo de acceso, la dirección DNS o IP del servidor, el posible puerto opcional (el valor por defecto es 80) y el objeto requerido del cliente.

3. El servidor busca el recurso, abre una conexión TCP/IP llamando al puerto TCP correspondiente.

   Se realiza la petición. Para ello, se envía el comando necesario (GET, POST, HEAD), la dirección del objeto requerido (el contenido de la URL que sigue a la dirección del servidor), la versión del protocolo HTTP empleada y un conjunto variable de información, que incluye datos sobre las capacidades del browser, datos opcionales para el servidor, etc. Si se solicitaron datos de la base de datos, esta resuelve las consultas que llegan a ella y responde con un resultado.

4. El servidor envía el recurso solicitado utilizando la misma conexión por la que recibió petición, envía el archivo con lenguaje de marcas de hipertexto (HTML, Hyper Text Markup Language) a la conexión TCP.

5. Se cierra la conexión TCP y el cliente recibe la información de la página solicitada.

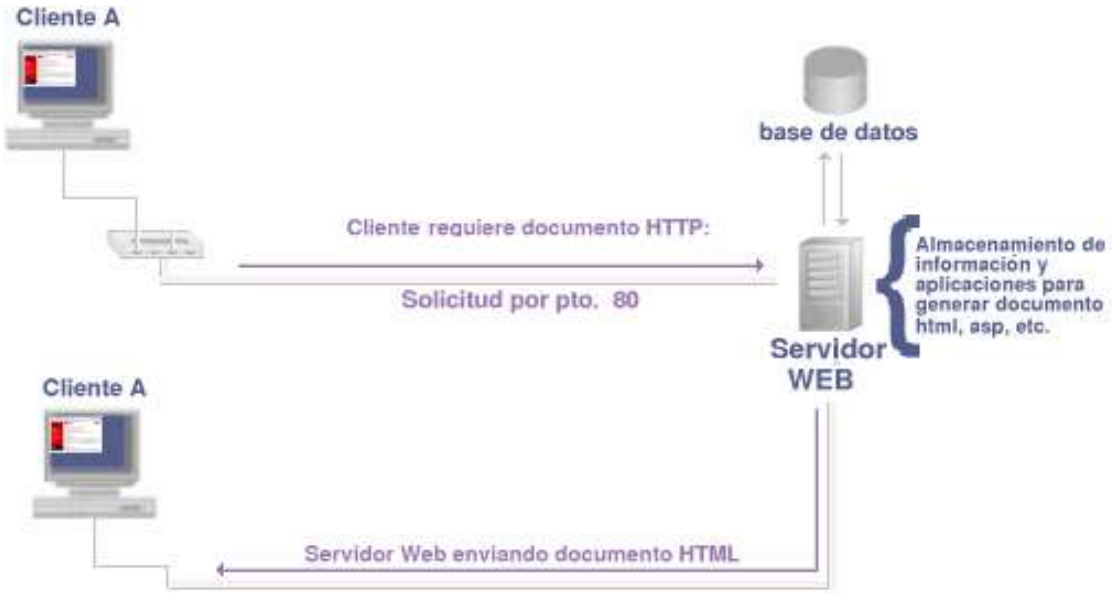


Fig. 9. Diagrama de funcionamiento de servidor WEB.

4.2.1. Tipos de página web.

Las páginas web son documentos o información que se crean en formato HTML, estos son adaptados a WWW y se puede acceder a ellos por medio de un navegador. Al conjunto de páginas web enlazadas se las conoce bajo el nombre de sitio web.

Existen distintos tipos páginas web, dentro de las principales se destacan:

- **Estáticas:** este tipo de páginas web están compuestas por archivos que contienen código HTML, es por medio de este que se pueden mostrar las imágenes, textos, videos y todos aquellos contenidos que componen a la página en sí. Los archivos que constituyen a la página web son almacenados en el servidor de Hosting, cuyo formato es también en HTML.

  Las páginas web estáticas pueden ser editadas por medio de diferentes programas. Para esto, los archivos deben ser descargados del servidor con algún software, editarlos, guardarlos y subirlos nuevamente.

- **Dinámicas:** son aquellas cuya información que presentan se genera a partir de alguna acción o petición del usuario en la página. Contrariamente a las páginas estáticas, en las que su contenido se encuentra predeterminado, en las dinámicas la información aparece inmediatamente después de una solicitud hecha por el usuario. Para la creación de este tipo de páginas, además de etiquetas HTML es necesaria la utilización de algún lenguaje de programación que se ejecute del lado del servidor, así como la existencia de una base de datos. Los lenguajes utilizados para la generación de este tipo de páginas son PHP y ASP.
- **Animada.** Las páginas web animadas son aquellas que se realizan con la tecnología Flash, ésta permite que una página web presente el contenido con ciertos efectos animados. El uso de esta tecnología permite diseños más vanguardistas, modernos y creativos.

También, se pueden incluir clasificaciones como las siguientes:

- Blog.
- Sitios de comunidades virtuales.
- Sitios de descargas.
- Tiendas virtuales o comercio electrónico.
- Portales, etc.

Según la forma en que los usuarios utilizan el sitio web, estos pueden ser:

· **Informativos**: cuando el flujo de información solamente se da desde el sitio web a los usuarios (no en sentido contrario).

· **Interactivos**: cuando el flujo de información es en ambos sentidos, es decir, los usuarios no solamente reciben información del sitio web, sino que también pueden enviar su propia información al sitio web o a otros usuarios.

4.3. SERVIDOR DHCP.

El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol)[4], es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP y las va asignando dinámicamente a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

El servicio de DHCP es el que se encarga de proporcionar dirección IP a los equipos que lo necesiten para conectarse a la red loca mediante el puerto 67. Por tanto, el equipo que proporcionará este servicio se convertirá en el servidor de DHCP o en uno de los servidores de este servicio en la red. La secuencia de eventos del servicio DHCP se muestra en el diagrama siguiente.

[4](2010). Oracle Solaris. Recuperado el 20 de julio de 2014 de http://www.oracle.com/cd/E19957-01/820-2981/dhcp-overview-3/index.html

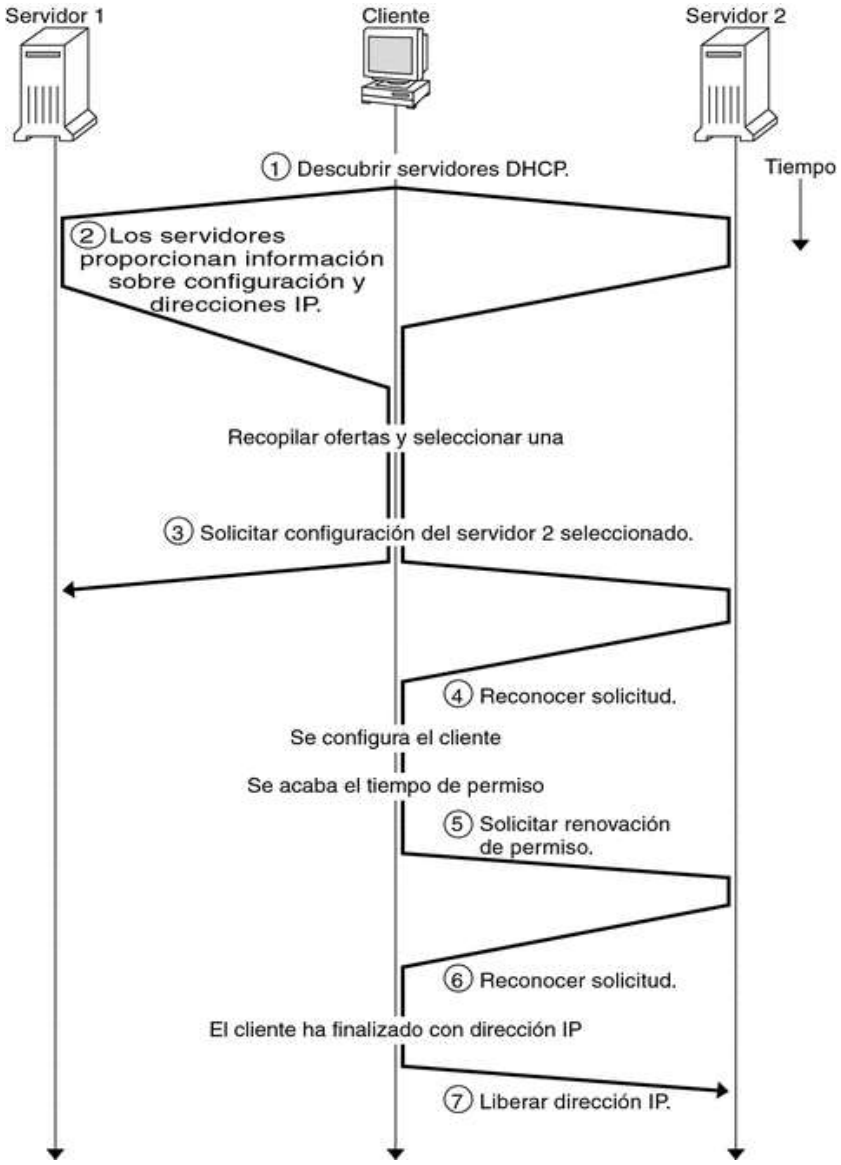


Fig. 10. Diagrama de funcionamiento del Servidor DHCP.

Inicialmente el cliente descubre un servidor DHCP emitiendo un mensaje de descubrimiento a la dirección de emisión limitada (255.255.255.255) de la subred local.

Si hay un enrutador y está configurado para hacer de agente de reenvío de BOOTP, la solicitud se transfiere a otros servidores DHCP de diferentes subredes. La emisión incluye su ID exclusivo que se obtiene de la dirección de control de acceso de soportes (MAC) del cliente. En una red Ethernet, la dirección MAC es la misma que la dirección Ethernet.

Los servidores DHCP que reciben el mensaje de descubrimiento pueden determinar la red del cliente con la información siguiente:

a) El servidor determina si el cliente se encuentra en la red a la que está conectada la interfaz o si está utilizando un agente de reenvío de BOOTP conectado a dicha red.

b) Cuando una solicitud pasa por un agente de reenvío, éste inserta su dirección en el encabezado de la solicitud. Cuando el servidor detecta una dirección de agente de reenvío, el servidor sabe que la parte de red de la dirección indica la dirección de red del cliente porque el agente de reenvío debe estar conectado a la red del cliente.

c) El servidor consulta la tabla netmasks (máscara de red) para encontrar la máscara de subred que se utiliza en la red que indica la dirección del agente de reenvío o la dirección de la interfaz de red que recibió la solicitud. Cuando el servidor conoce la máscara de subred que se utiliza, puede determinar qué parte de la dirección de red es la parte del host, y a continuación seleccionar una dirección IP adecuada para el cliente.

d) Cuando los servidores DHCP determinan la red del cliente, seleccionan una dirección IP adecuada y verifican que no esté en uso. A continuación, los servidores DHCP responden al cliente emitiendo un mensaje de oferta. El mensaje de oferta incluye la dirección IP seleccionada e información sobre los servicios que se pueden configurar para el cliente. Cada servidor reserva temporalmente la dirección IP ofrecida hasta que el cliente determina si utilizará la dirección IP.

e) El cliente selecciona la mejor oferta basándose en el número y el tipo de servicios ofrecidos. El cliente emite una solicitud que especifica la dirección IP del servidor que realizó la mejor oferta. La emisión garantiza que todos los servidores DHCP de respuesta sepan que el cliente ha seleccionado un servidor. Los servidores que no se eligen pueden cancelar las reservas de las direcciones IP que habían ofrecido.

f) El servidor seleccionado asigna la dirección IP para el cliente y almacena la información en el almacén de datos DHCP. El servidor también envía un mensaje de reconocimiento (ACK) al cliente. El mensaje de reconocimiento contiene los parámetros de configuración de red para el cliente. La utilidad ping permite al cliente probar la dirección IP para asegurarse de que no la esté utilizando otro sistema. A continuación, el cliente sigue iniciándose para unirse a la red.

g) El cliente supervisa el tiempo de permiso. Una vez transcurrido un periodo determinado, el cliente envía un nuevo mensaje al servidor seleccionado para aumentar el tiempo de permiso.

h) El servidor DHCP que recibe la solicitud amplía el tiempo de permiso si el permiso sigue cumpliendo la directiva de permiso local que ha fijado el administrador. Si el servidor no responde en 20 segundos, el cliente emite una solicitud para que uno de los demás servidores DHCP pueda ampliar el permiso.

i) Cuando el cliente ya no necesita la dirección IP, notifica al servidor que la dirección IP está libre. Esta notificación puede tener lugar durante un cierre ordenado y también se puede realizar manualmente.

4.4. SERVIDOR PROXY.

Un proxy de conexión a Internet es un servidor que hace de intermediario entre los PCs de la red y el router de conexión a Internet, de forma que cuando un usuario quiere acceder a Internet, su PC realiza la petición al servidor Proxy y es el quien realmente accede a Internet. Posteriormente, el Proxy enviará los datos al PC del usuario para que los muestre en su pantalla. El PC del usuario no tendrá conexión directa con el router, sino que accederá a Internet por medio del proxy. En la figura 11 se muestra el funcionamiento del servicio proxy en una red.[5]

[5]S. Bibillier (2009). Linux, Administración del Sistema y explotación de los servicios de red (2da edición). Barcelona: Ediciones ENI.

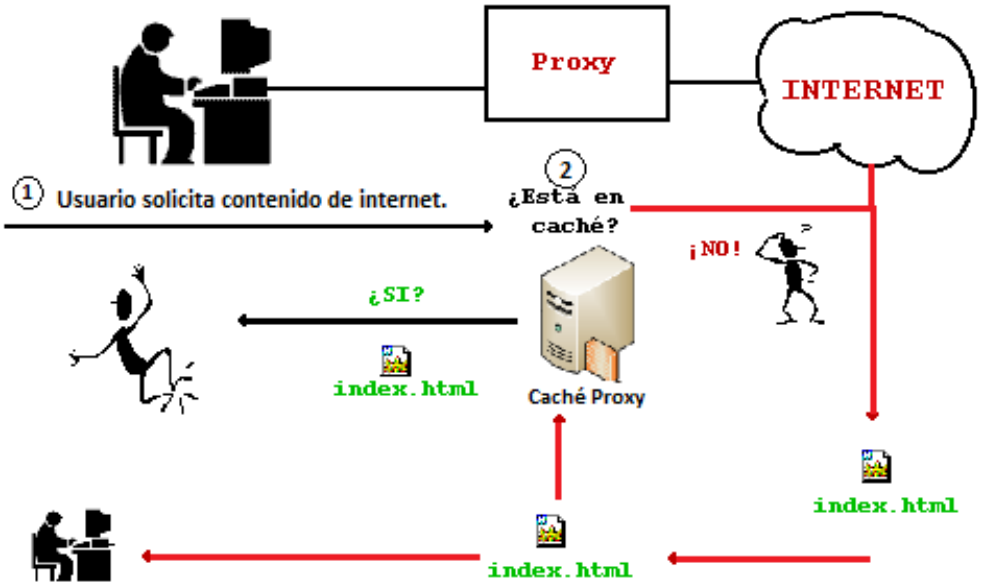


Fig. 11. Diagrama de funcionamiento del servidor Proxy.

Cuando se recibe una petición para un recurso de red, el proxy busca el resultado dentro de la caché. Si este es encontrado responde automáticamente la petición del cliente, si el contenido estuviera ausente en la caché el servidor intermediario lo traerá desde un servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en la caché.

Como las peticiones de los equipos de la red local hacia Internet son interceptadas por el servidor proxy, éste puede realizar una tarea de filtrado de accesos, impidiendo aquellos destinos que estén prohibidos en los archivos de configuración del servicio. Squid es un servidor proxy para web con caché y es una de las aplicaciones más populares y de referencia para esta función, es un software libre publicado bajo licencia pública general (GPL, General Public Licence).

Entre sus utilidades está la de mejorar el rendimiento de las conexiones, guardando en caché peticiones recurrentes a servidores Web y DNS, acelerar el acceso a un servidor web determinado o añadir seguridad realizando filtrados de tráfico.Sus principales funciones son:

a) Permite el acceso web a máquinas privadas (IP privada) que no están conectadas directamente a Internet.

b) Controla el acceso web aplicando reglas.

c) Registra el tráfico web desde la red local hacia el exterior.

d) Controla el contenido web visitado y descargado.

e) Controla la seguridad de la red local ante posibles ataques, intrusiones en el sistema, etc.

f) Funciona como una caché de páginas web.

De modo predefinido Proxy Squid utiliza el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.

Denegar el acceso a ciertos en ciertos horarios, contenidos y descargas permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso en horarios y días de la semana, de acuerdo a su extensión o bien restringir el acceso a contenido en horarios específicos.

Para poder controlar el tráfico de los clientes hacia Internet, es necesario establecer Listas de Control de Acceso (ACL, Access Control List) que definan una red o bien ciertos hosts en particular.

A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Proxy Squid. Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red.

Existen diferentes tipos restricciones que pueden ser configuradas mediante el servidor Proxy Squid utilizando las siguientes reglas de control de acceso:

- **Tipo src:** especifican una o varias direcciones IP de origen o un segmento de red con su máscara. Dentro de este se encuentran las direcciones IP que se encuentran en una red local, limitar permisos por rango de IPs o por políticas de seguridad.

- **Tipo time:** establece límites relacionados con franjas horarias dentro de una semana, de esta forma se puede habilitar o deshabilitar la navegación externa a como se desee.

- **Tipo url_regex:** permite especificar expresiones regulares para comprobar una URL, de esta forma se podrá deshabilitar páginas con un contenido temático.

- **Tipo urlpath_regex:** permite la administración de descargas por extensiones de ficheros.

4.5. SERVIDOR DE CORREO (ZIMBRA).

El correo electrónico es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos mediante sistemas de comunicación electrónicos.

Un correo electrónico durante su recorrido desde el origen hacia su destino final es procesado por tres agentes, estos son[6]:

El agente de usuario de correo (MUA, Mail User Agent): este específicamente maneja las cabeceras del correo electrónico y el usuario usa el editor de texto dentro del MUA para componer el cuerpo del mensaje y luego enviarlo, una vez que es enviado, el mensaje es entregado al servidor de correo saliente MTA o por medio del protocolo para la transferencia simple de correo electrónico (SMTP, Simple Mail Transfer Protocol) predeterminado en la configuración inicial del agente.

El agente de transporte de correo (MTA, Mail Transport Agent) no es más que el servidor de correo saliente. MTA es un término técnico utilizado para referirse a un servidor SMTP de Internet. El servidor de correo se encarga de determinar si el destinatario de correo se encuentra en el servidor local o en uno remoto, en este último caso el servidor iniciará una conexión SMTP con el servidor destino. Esta comunicación servidor a servidor continuará hasta que el mensaje de correo electrónico alcance el servidor que almacena el buzón del destinatario final.

[6] **(2012). MTI. Recuperado el 28 de septiembre de 2014 de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-email.html**

El agente de entrega de correo (MDA, Mail Delivery Agent) una vez que el servidor final de correo electrónico recibe el mensaje, este es manipulado por el agente de entrega de correo (MDA) también llamado agente de entrega local (LDA), es el término técnico para el mecanismo que entrega los mensajes de correo a los buzones finales.

Cuando el mensaje de correo es entregado al destino final, el destinatario puede acceder a los mensajes de distintas maneras.

Una de las formas más utilizadas para descargar el correo es a través del protocolo de oficina de correos versión 3 (POP3), el propósito original de este protocolo es muy simple, proporciona amplias operaciones en el servidor; con POP3 el MUA transfiere el correo desde el servidor y después se borra. El servicio POP3 se encuentra disponible de forma estándar en el puerto TCP 110.

Sin embargo un método más robusto es brindado por el protocolo de acceso a mensajes de Internet IMAP, donde los mensajes de correo se mantienen en el servidor y los usuarios pueden leerlos o borrarlos, IMAP se encuentra disponible en el de forma estándar en el puerto número 143.

POP e IMAP son completamente independientes uno del otro, pero ambos servicios pueden ser ofrecidos desde un mismo Servidor, brindando la flexibilidad al usuario final de escoger el protocolo que más se adapte a sus necesidades.

En la figura 12 se muestra el ciclo completo de un mensaje de correo electrónico, desde que sale de la aplicación cliente del usuario, hasta su llegada al destinatario final.

Para recibir e-mails el Agente de Usuario de Correo (MUA) puede utilizar POP e IMAP, al enviar un e-mail utiliza formatos de mensajes y cadenas de comandos definidas por el protocolo SMTP.
El proceso Agente de transferencia de correo (MTA) se utiliza para enviar correos electrónicos. Como se muestra en la figura 12, el MTA recibe mensajes desde el MUA. Según el encabezado del mensaje, determina como debe reenviarse un

mensaje para llegar a destino. Si el correo está dirigido a un usuario cuyo buzón está en el servidor local, el correo se pasa al MDA.

Si el correo es para un usuario que no está en el servidor local, el MTA enruta el e-mail al MTA en el servidor correspondiente. El protocolo simple de transferencia de correo (SMTP), rige la transferencia de e-mails salientes desde el cliente emisor al servidor de e-mails (MDA), como así también el transporte de e-mails entre servidores de e-mails (MTA).

SMTP permite transportar e-mails por las redes de datos entre diferentes tipos cliente y servidor, y hace posible el intercambio de e-mails en internet. En la siguiente figura se muestra el proceso descrito anteriormente:

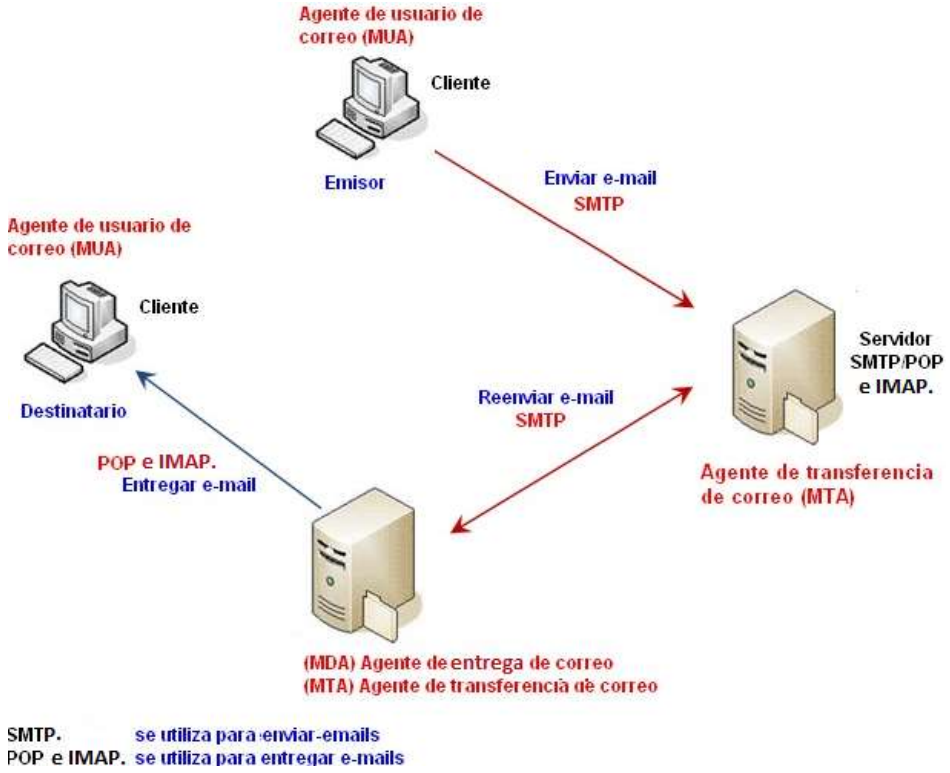


Fig. 12. Ciclo de un correo electrónico.

4.5.1. DNS Y EL ENCAMINAMIENTO DEL CORREO ELECTRONICO.

Existe una relación muy estrecha entre el Sistema de Nombre de Dominio (DNS) y el correo electrónico. Los sistemas de correo encaminan los mensajes basándose en la información brindada por el DNS, es por eso que su buen funcionamiento está en total dependencia de la correcta configuración del DNS.

Los programas gestores de correo electrónico (Servidores SMTP) requieren la información brindada por el servicio DNS para el encaminamiento de los mensajes, esta información solo indica como debe ser enrutado el mensaje y no la manera en como hacen los servidores para realizar la entrega fina de los mensajes al buzón de usuario, es decir el DNS mantiene información en el registro MX (Mail Xchanger) de cual o cuales son los servidores encargados de gestionar el correo electrónico para el dominio sobre el cual se tiene la autoridad de la zona, sin embargo la entrega al buzón de correo destino es tarea del protocolo SMTP.

Una vez que el servidor SMTP origen conoce cuál es el MX del dominio, nuevamente realiza una consulta al servidor DNS, preguntándole en esta ocasión cual es la dirección IP del MX devuelto. En este momento el servidor ya es capaz de abrir la conexión SMTP con el servidor destino y llevar a cabo las tareas de intercambio de mensajes. La figura 13 muestra este proceso:

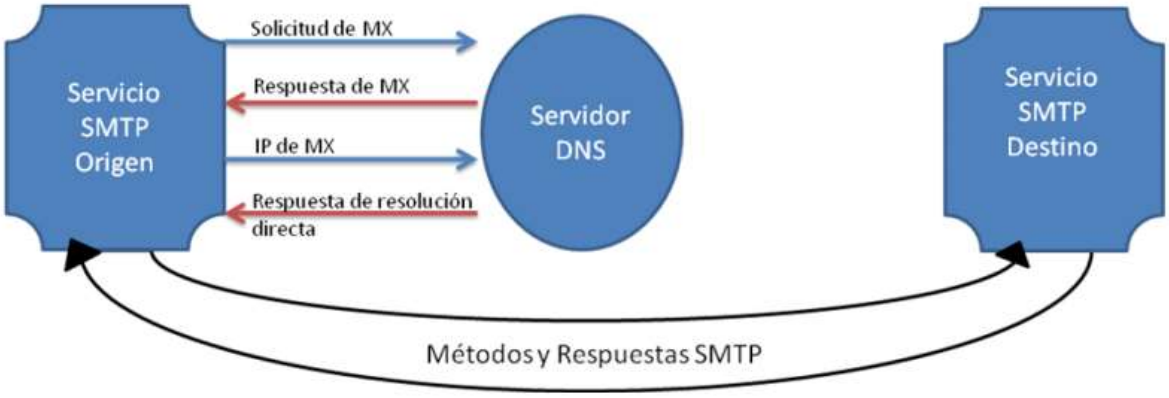


Fig. 13 Encaminamiento de Correo Electrónico.

Los servidores DNS guardan la información en una serie de Registros de Recursos (RR), cada uno de los cuales contiene información particular acerca de un nombre de dominio dado (por lo general un host). El sistema dispone de un registro MX, cada MX asocia un nombre de dominio con dos datos, un número de preferencia (un entero de 16 bits sin signo) y el nombre de un host.

4.5.2. POSTFIX.

Entre los servidores SMTP más populares en la actualidad están: Sendmail, Postfix, Qmail, Exim, Microsoft Exchange Server etc. La suite de colaboración ZIMBRA se basa en proyectos de código abierto y utiliza Postfix y actúa como servidor IMAP y POP3 de correo electrónico.

Postfix fue creado como una alternativa más rápida, segura y fácil de administrar. Las configuraciones de Postfix por defecto son lo suficientemente seguras como para poner al servidor en producción. Su diseño es modular, de tal forma que cada módulo corre con los privilegios mínimos para realizar la tarea para la que está hecho.

El rendimiento de Postfix es admirablemente alto porque está centrado fundamentalmente en las tareas de transporte de correo, lo que se hizo fue tratar de no reinventar lo que ya estaba creado, sino tomando funcionalidades implementadas en otras aplicaciones MTA.

Postfix brinda los medios para conectar aplicaciones externas cuando una tarea compartida está fuera del área de transporte del mensaje. Postfix utiliza todo el poder ofrecido por los sistemas Unix para realizar su trabajo, ésta estrecha relación con el sistema operativo no solo hace más fácil el acceso a las aplicaciones externas, sino también mejora el rendimiento.

La raíz de cualquier sistema de correo electrónico es el servicio SMTP. En muchas distribuciones Linux, como por ejemplo, CentOS, Fedora, Redhat y Open SUSE incorporan como nuevo servicio SMTP por defecto a Postfix.

4.5.3. FUNCIONAMIENTO Y ARQUITECTURA DE POSTFIX.

Recibe los mensajes, los encola y finalmente los entrega. Cada una de estas etapas, es realizada por componentes diferentes de Postfix, lo que permite una configuración por separado en cada una de ellas. Después de que el mensaje es recibido y encolado, el administrador de la cola de mensajes invoca al agente de entrega adecuado para la fase final.

Los mensajes llegan al servidor con Postfix de la siguiente manera: Un mensaje puede ser aceptado por Postfix localmente, es decir, aquel que ha sido enviado por un usuario en el host local y puede ser aceptado por Postfix desde la red. Un mensaje que ya ha sido aceptado por Postfix a través de los métodos ya mencionados, es preparado para su reenvío a otra dirección. Un mensaje puede ser generado por el mismo Postfix, cuando sea necesario entregar una notificación**.**

La arquitectura de Postfix se encarga de delegar su funcionamiento en pequeños módulos que realizan una tarea específica. La mayoría de ellos son demonios, los cuales son procesos informáticos que se ejecutan en segundo plano en vez de ser controlado directamente por el usuario y que corren en background en el sistema.

El camino que sigue un mensaje local al entrar a Postfix se muestra en la figura que a continuación se muestra:

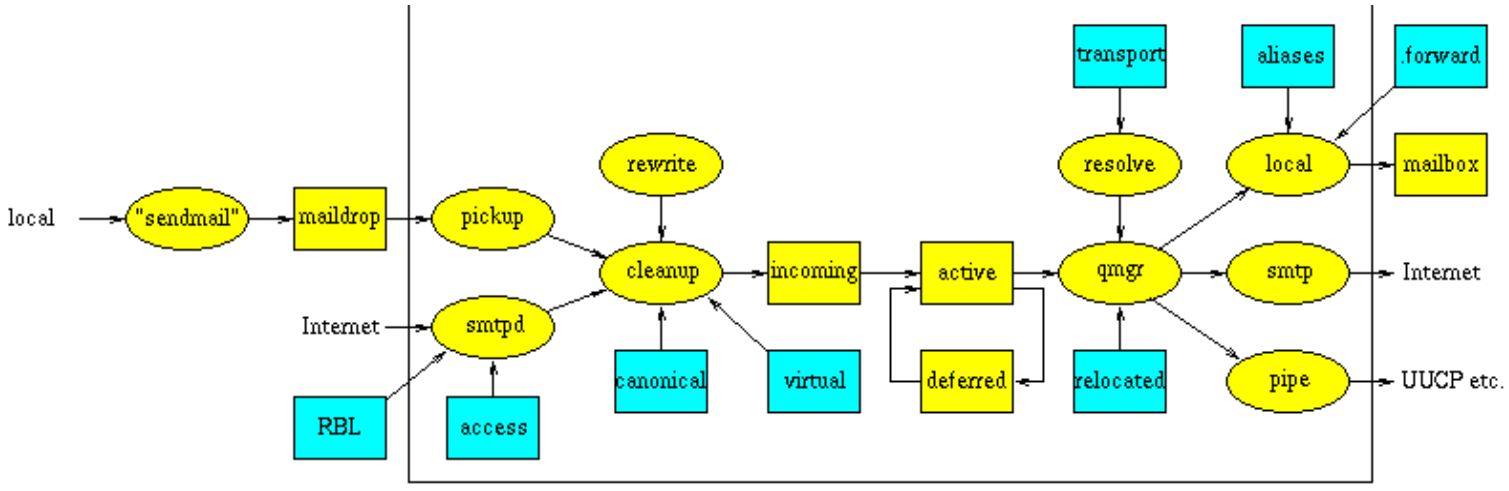


Fig. 14. Diagrama de flujo de Postfix.

- ✓ Las elipses son programas de correo.
- ✓ Las cajas cuadradas son colas de correo o archivos.
- ✓ Las cajas rectángulo son tablas lookup.

Los correos pueden proceder desde el propio servidor llamado local o desde Internet. En el caso que provenga de Internet es procesado por el demonio smtpd el cual verifica a través de las tablas de listas negras (RBL) las cuales contienen las direcciones de posibles spam, además procesa todo el correo verificando que sea descartado, aceptado verificado en las tablas de acceso.

Cuando se inicia una conexión local al servidor de correo, se inicia un proceso de compatibilidad con Sendmail, el cual por defecto lee un mensaje de la entrada Standard hasta un EOF (end-of-file, es decir, fin de fichero, es un indicador o marca de que no hay más información que recuperar de una fuente de datos) o hasta que exista una línea con un . (Punto) y lo arregla para su envío. Sendmail trata de crear un archivo de cola, pasándolo al directorio maildrop. Si ese directorio no tiene permisos de ejecución para todos, el mensaje es pipeado a través del comando postdrop, que se espera se ejecute con privilegios apropiados.

La mayoría de los casos los mensajes locales son depositados en el directorio maildrop de la cola de Postfix por el comando postdrop.
Los programas que están en la caja grande son programas que controla el demonio maestro de Postfix, también llamado master.

El proceso master es el proceso residente que ejecuta los demonios de Postfix cuando se necesitan demonios para enviar o recibir mensajes localmente, etc. Los demonios de Postfix voluntariamente terminan después de estar inactivos por una cierta cantidad de tiempo o después de haber hecho una cierta cantidad de peticiones. La excepción de esta regla es el administrador de colas de mensajes (qmgr).

- **Pickup**: lee el mensaje de la cola y lo pasa al demonio cleanup.
- **Cleanup:** procesa el correo entrante, lo inserta en la cola de correo entrante e informa a qmgr que el mensaje ha sido procesado, adicional inserta las cabeceras From:, To:, Message-Id: y Date, extrae las direcciones desde To:, Cc: y Bcc, transforma el mensaje y las cabeceras al formato usuario@full-dominio que es la forma que otros programas de Postfix entiendan.
- **Rewrite:** procesa dos tipos de petición de cliente: reescribe una dirección a su formato estándar y resuelve una dirección y obtiene información de transporte, nexthp y recipiente. Además distingue si el correo es local o no local.
- **Active:** crea las direcciones SMTP para los destinatarios.
- **Deferred:** En esta cola van a parar los mensajes que no se han podido enviar alguno de los destinatarios y por ello Postfix tiene que volver a reintentar él envío.
- **qmgr :** espera la llegada de correo entrante y se preocupa de su entrega vía proceso de entrega Postfix.
- **Local:** procesa las peticiones de entrega desde qmgr para entregar correo a recipientes locales.
- **Pipe:** procesa peticiones desde qmgr para ejecutar comandos externos.
- **SMTP:** procesa las entregas de mensaje desde qmgr. Funciona exactamente igual que local y pipe. La diferencia está que SMTP busca una lista de direcciones de hosts para intercambio de correo. Ordena la lista por preferencia y se conecta a cada una hasta que encuentra un servidor que responda.

4.5.4. ZIMBRA.

Zimbra es un servidor de correo que además de correo electrónico y calendario, ofrece el intercambio de archivos, tareas, contactos, integración con las Redes Sociales, gestión de documentos y simplifica los controles administrativos desde una interfaz de usuario de correo web.[7]

[7] L. Hurtado, H. Taleno. (2010). Propuesta para la implementación de un servidor de correo electrónico Zimbra en SUSE Linux Enterprise Server 11 en la UNAN – MANAGUA RURD (Recinto Universitario Rubén Darío). [versión impresa]. Nicaragua: Universidad Iberoamericana de ciencia y tecnología (UNICIT).

Zimbra es un completo programa de mensajería y colaboración de código libre que ofrece herramientas complementarias como libretas de direcciones, agendas y tareas, funciona bajo cualquier sistema operativo (Linux, Windows o Mac), ya sea también vía web mail pudiendo consultarse desde cualquier lugar con conexión a internet o un simple cliente de correo tradicional como Outlook.

El servidor de Zimbra empaqueta todos los componentes principales en un simple instalador y utiliza, entre otras, tecnologías como: Jetty, Postfix, MySQL, OpenLDAP, Lucene y soporta, entre otros, protocolos tales como SMTP, LMTP, SOAP, XML, IMAP, POP, iCal y CalDAV. Este es un servidor muy rápido y eficiente que, además, permite escalar de manera horizontal, pues cada host incluye su propio almacén de buzones de correo y de datos de configuración. Zimbra puede crecer añadiendo más máquinas con subdominios diferentes y mantener una gestión centralizada dentro del mismo dominio principal.

Zimbra soporta múltiples dominios y también perfiles de usuarios, que denomina clase de servicio (COS, Class Of Service). En estas clases de servicio se pueden definir las cuotas de almacenamiento y las características a las cuales tendrán acceso los usuarios, entre las más destacadas en su versión actual, están:

- ✓ Correo electrónico.
- ✓ Libreta de direcciones.
- ✓ Calendario de citas.
- ✓ Tareas.
- ✓ Documentos.
- ✓ Maletín.
- ✓ Mensajería instantánea.
- ✓ Preferencias.
- ✓ Etiquetado.
- ✓ Compartición.
- ✓ Cambio de contraseña.
- ✓ Redacción de correos en formato HTML.
- ✓ Atajos de teclado, etc.

- ✓ Escalabilidad hasta millones de buzones.
- ✓ Administración simple y configuración muy extensible.
- ✓ Accesible desde cualquier lugar, independientemente del sistema operativo.
- ✓ Optimización de almacenamiento.
- ✓ Menor costo de inversión.
- ✓ Herramientas de respaldo integrado.

4.5.4.1. ARQUITECTURA DE ZIMBRA.

ZCS o Zimbra Colaboration Suite, está formada por un conjunto de componentes que trabajan juntos para formar una solución completa. El núcleo del servidor está escrito en Java, utilizándose Jetty como servidor de aplicaciones. El servidor se integra con otros sistemas como el MTA, la base de datos y los paquetes de seguridad.

El agente de transferencia de correos (MTA) enruta los mensajes de correo al servidor de ZIMBRA. Este servicio está basado en el popular Postfix. Integrado a través de ZIMBRA-POSTFIX el cual incorpora varios filtros de seguridad, como antivirus y antispam, entre otros. Asimismo, el MTA puede integrarse con otras tecnologías, como Postgrey para el control de listas de spam (greylisting) o Spamhaus para la lista negra (DNSBL), u otras soluciones de seguridad comerciales, como los AV/AS (Anti-Virus, Anti-Spyware) de Barracuda Networks.

En ZCS se incluyen diversos almacenes de datos para la información de los usuarios:

OpenLDAP: proporciona la autenticación.

MySQL: guarda las preferencias y metadatos de los mensajes, es decir, el sistema de ficheros guarda directamente los mensajes de correo.

Lucene: Otro componente integrado en ZIMBRA, un potente motor de indexación y búsquedas que permite a los usuarios y administradores buscar mensajes

a través de múltiples carpetas de correo, tanto metadatos como contenidos en el cuerpo del mensaje.

A continuación en la figura 15 se muestra la arquitectura de Zimbra:

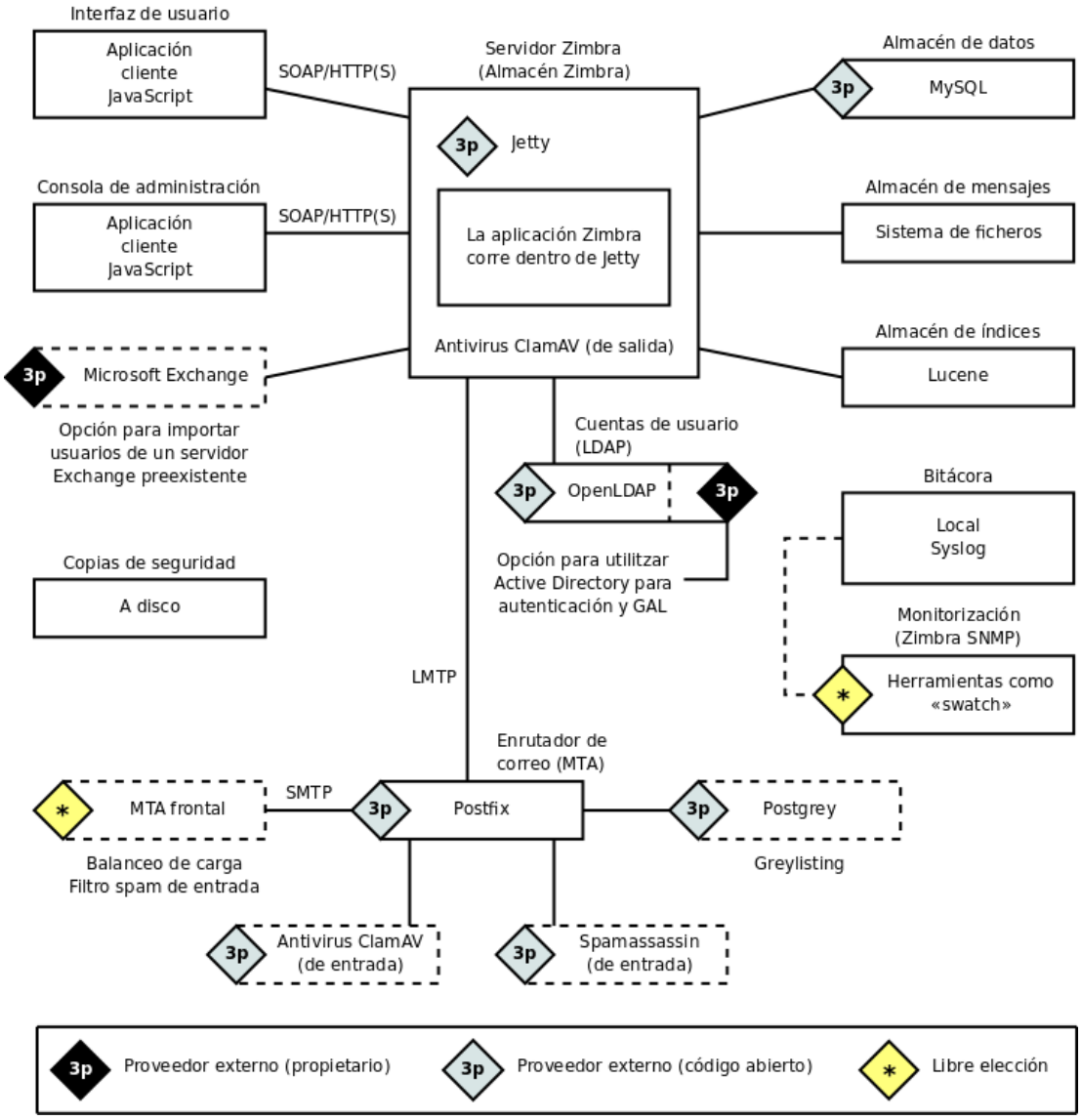


Fig. 15. Arquitectura de Zimbra.

En términos generales, las funcionalidades ofrecidas por Zimbra son muy similares a las de Microsoft Exchange, aunque está mejor preparado para ser utilizado por proveedores de alojamiento web (hosting) y tiene algunas características de colaboración que Exchange no tiene. Además, una gran

diferencia la marcan los bindings de SOAP (Simple Object Access Protocol) que permiten integraciones de terceros que amplíen las funcionalidades de Zimbra.

Los principales componentes de la arquitectura de Zimbra son:

- **Zimbra Core:** incluye las librerías, utilidades, herramientas de monitorización y ficheros básicos de configuración

- **Zimbra LDAP**: un protocolo ligero de acceso directorio (LDAP, Lightweight Directory Access Protocol) es cada vez más una necesidad. ZCS utiliza por defecto OpenLDAP para almacenar y gestionar el almacén de usuarios, integrando de serie el soporte para la replicación.

- **ZimbraMTA:** está formado como es habitual de diversas partes:

✓ Un almacén de buzones de correo accesible por IMAP4 y POP3, con soporte para cifrado del canal mediante una capa de conexión segura (SSL, Secure Sockets Layer).

✓ Unos filtros de contenidos (antivirus y antispam). ZIMBRA utiliza Amavis como filtro de contenidos y por defecto, Spam Assassin y ClamAV como filtros antispam y antivirus respectivamente. De todos modos, es posible configurarlo para que utilice cualquier otro filtro antispam o antivirus.

El correo se recibe mediante SMTP, se enruta mediante una tabla de transportes y se entrega al almacén de correo haciendo uso del protocolo de transporte local de correo (LMTP, Local Mail Transfer Protocol).

- **ZIMBRA Store**: ofrece contenido dinámico desde un servidor web utilizando jetty y almacena el correo electrónico. Cada cuenta se configura en un servidor, y esta cuenta está asociada con un buzón de correo que contiene todos los mensajes y ficheros adjuntos. El servidor de buzones está formado por:

✓ El almacén de datos: es una base de datos MySQL en la cual los identificadores de mensajes son enlazados con las cuentas de usuario

- ✓ El almacén de mensajes: guarda todos los mensajes y sus adjuntos en formato de extensión multipropósito de correos de internet (MIME, Multipurpose Internet Mail ExtensionsEncoding).
- ✓ El almacén de índices: mediante Lucene proporcionan la tecnología necesaria para indexar y buscar.
- ✓ Las utilidades de conversión de adjuntos a HTML.

- **Zimbra SNMP y Zimbra Logger:** ZIMBRA SNMP recoge información periódica del estado del sistema. Además, utiliza Swatch (archivo activo de la herramienta de registro de seguimiento) para analizar la salida del syslog (un estándar de facto para el envío de mensajes de registro en una red informática IP) y generar los traps del Protocolo Simple de Administración de Red(SNMP, Simple Network Management Protocol).

  Por su parte, Zimbra Logger instala herramientas de agregación de logs, informes y seguimiento de mensajes. Sin este paquete no se podrán utilizar las funcionalidades de seguimiento de mensajes y estadísticas del servidor de la consola gráfica de administración.

4.5.4.2. VENTAJAS DE ZIMBRA.

Zimbra es una perfecta opción para aquellas empresas o instituciones que desean implementar una robusta suite de colaboración de correo electrónico la cual al ser de código abierto les evita pensar en la compra de licencias para usuarios así como la ardua tarea de su administración ya que al ser 100% gráfica es fácil de comprender.

Zimbra es una solución colaborativa de última generación con todos los añadidos técnicos y funcionales necesarios para satisfacer a los usuarios y administradores más exigentes. Al contrario de otros servidores de correo tales como Exchange, Zimbra puede funcionar con cientos de usuarios a pleno rendimiento en un solo servidor de gama media. La siguiente tabla muestra algunas de las ventajas que Zimbra brinda al usuario y al administrador.

Tabla No.1 Ventajas para Administrador y Usuario de ZIMBRA.

ADMINISTRADOR	USUARIO
Escalabilidad hasta millones de buzones.	Correo Web interactivo e intuitivo.
Menor costo de inversión que las soluciones propietarias.	Agenda de Actividades.
Optimización del almacenamiento.	Calendario interactivo y colaborativo.
Accesible desde cualquier lugar independientemente del sistema operativo.	Herramientas de búsqueda.
Administración de múltiples dominios	Integración con todos los dispositivos Windows Mobile, Android, BlackBerry, Iphone.

4.6. CENTRAL TELEFÓNICA VIRTUAL (ELASTIX).

Una Central Telefónica Virtual es una solución de comunicaciones que posibilita a las pequeñas y medianas empresas, a partir de una conexión de banda ancha, contar con un grupo de líneas VoIP integradas e incorporar las nuevas aplicaciones de comunicación desarrolladas para el ambiente típico IP.[8]

Las Centrales Telefónicas Virtuales se basan en la transmisión de la voz digitalizada sobre la red IP y permite formar su propio grupo de líneas (incluso con aquellas que no se encuentran en la misma ubicación física o geográfica) con la posibilidad de administrar cada una de las líneas, extensiones o servicios según las necesidades.

A través de las diferentes Centrales Virtuales IP, se puede acceder a servicios de grupo, entre ellos llamadas entre usuarios internos, administración de llamadas, bloqueos de líneas, llamadas mediante marcación de usuarios y administración de

[8] (2011). ElastixTech. Recuperado el 21 de agosto de 2014 de: http://elastixtech.com/curso-basico-de-elastix/

grupos. Entre los servicios individuales, pueden contar con llamada en espera, identificación de llamadas, transferencia, resguardo y captura de llamadas, oficina remota y atención o rechazo selectivo de llamadas, entre otros.

Las centrales telefónicas virtuales son soluciones de comunicación que ofrecen tecnología de última generación y que a nivel financiero permiten concentrar en una cuota todas las facilidades y servicios necesarios para disponer de una central telefónica sin necesidad de grandes inversiones o de instalaciones locales complicadas.

Para poner en operación la tecnología VoIP, se necesita un software que nos permita crear, administrar y configurar sistemas de telefonía IP y además que posea las características de una PBX convencional. Para este proyecto se optó por la PBX virtual ELASTIX por su confiabilidad, fácil uso y además porque es un software libre. Elastix es una suite de comunicaciones que integra las mejores herramientas disponibles para VoIP PBX, Fax, Mensajería Instantánea, Email y Colaboración, esta implementa gran parte de su funcionalidad sobre 4 programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postfix.

El objetivo de Elastix es incorporar en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial.

Algunas de las características básicas de Elastix incluyen:

- Correo de Voz.
- Fax-a-email.
- Soporte para softphones.
- Interfase de configuración Web.
- Sala de conferencias virtuales.
- Grabación e identificación de llamadas.
- Least Cost Routing.
- Roaming de extensiones.

Fig. 16. Servicios de Elastix.

Gracias a la estructura del Elastix utilizado para este fin, es posible alcanzar una convergencia casi absoluta en las comunicaciones, ya que es permite transmitir distintos tipos de paquetes digitales de comunicación, tales como la voz.

Debido a las posibilidades que brinda la utilización de Elastix**,** éste reporta una gran cantidad de ventajas para los usuarios que requieren una comunicación constante**,** más allá del lugar donde se encuentren. Sus principales ventajas son:

- Menores costos**,** es posible establecer comunicación a través de reducidos anchos de banda.
- Aprovechamiento de tecnología IP sin grandes inversiones.
- Permite un gran despliegue y capacidad de expansión.
- Fácil de integrar con otros aplicaciones.

Elastix tiene también algunas desventajas, sin embargo, las ventajas que puede aportar superan claramente a éstas. A continuación vamos a nombrar algunas de las desventajas asociadas al uso de Elastix:

- Retrasos y/o cortes durante una comunicación, puede llegar a producir retraso en la llegada de los paquetes o incluso cortes de información.
- Posible deterioro de la comunicación al ser recibida por el usuario**.** En general esto sucede cuando se produce una congestión importante en la red, o bien cuando se utiliza un ancho de banda escaso que no permite acceder a una velocidad adecuada de conexión.

5. METODOLOGÍA.

El estudio de la presente investigación es de carácter cuantitativo, tuvo como propósito realizar un diseño de una red de área local con servidores tipo pc que brinden diferentes servicios a los usuarios del colegio Cristo Rey Managua, encontrándose dentro de los servicios más significativos el correo electrónico, la página web y la central telefónica virtual.

5.1. Tipo de estudio

Este estudio tiene un alcance descriptivo ya que inicialmente se examinó el sitio definiendo sus características, se aplicaron las técnicas de recolección de datos (ver instrumentos 1 y 2 en anexos) y se procesaron los resultados a fin de verificar si son o no eficientes, se analizaron las ventajas y desventajas que provee la red de servicios a los usuarios. De esta manera se obtuvieron los datos necesarios para seguir desarrollando esta investigación que contiene un elemento de investigación aplicada y a la vez de evaluación tecnológica.

5.2. El contexto

El diseño de la red y nodo de internet se llevó a cabo en las instalaciones del colegio Cristo Rey de la ciudad de Managua. En el proceso de desarrollo de este proyecto se tomó en cuenta la opinión de docentes, trabajadores administrativos, estudiantes y personal de dirección del colegio quienes son los beneficiarios directos con la implementación de estos servicios.

5.3. Los sujetos

El colegio Cristo Rey tiene una población estudiantil total o universo de 343 personas distribuidas en 318 alumnas con un cuerpo docente conformado por 20 maestros y 5 personas administrativas.

Para determinar el tamaño de la muestra, se utilizó la siguiente fórmula[9]:

$$n= \frac{k^{\wedge 2}*p*q*N}{(e^{\wedge 2}*(N-1))+k^{\wedge 2}*p*q}$$

$$n: \frac{(1.96)^2(0.25)(343)}{(0.05)^2(342)+(1.96)^2\,(0.25)}$$

$$n: \frac{(1.96)^2(0.25)(343)}{(0.025)(342)+(1.96)^2\,(0.25)}$$

$$n: \frac{329}{9.5} = 34.6$$

Donde:

N: Es el tamaño de la población o universo.

k:Es una constante que depende del nivel de confianza que se asigne.

e: Es el error muestral deseado,

p: Es la proporción de individuos que poseen en la población la característica de estudio.

q: Es la proporción de individuos que no poseen esa característica.

n: Es el tamaño de la muestra (número de encuestas que se van a realizar).

Aplicando la fórmula con 343 como universo, un nivel de confianza de 95 % (k=1.96) y la proporción de individuos p=q=0.5, se obtuvo una muestra de 34.6, o sea 35 personas.

[9] **http://www.monografias.com/tamano-muestra-archivistica/tamano-muestra-archivistica2.shtml, M. (s.f.).**

5.4. Instrumentos de recolección de datos

La información necesaria para la investigación se adquirió directamente de los docentes, administrativos y personal del equipo de dirección. Para la recolección de información se utilizó como instrumento de apoyo la aplicación de encuesta a estudiantes de diferentes niveles, las encuestas se procesaron a través de internet haciendo uso de la herramienta estadística SurveyMonkey, permitiendo de esta manera analizar los resultados obtenidos.

Para la elaboración del marco teórico se recurrió a fuentes bibliográficas disponibles en Internet, libros y trabajos monográficos relacionados con el tema de redes.

6. ANÁLISIS DE RESULTADOS.

Para estructurar el presente estudio se utilizó el método de división del trabajo, segmentando en cuatro etapas la propuesta. Los pasos a seguir fueron: requerimientos, diseño, configuración y pruebas. (Ver Fig.17).

Para la elaboración de la propuesta presentada se analizaron varias alternativas, tomando como criterios el costo, la disponibilidad, calidad y capacidad de usuarios.

A continuación se define paso a paso la instalación y configuración de cada uno de los servicios propuestos.

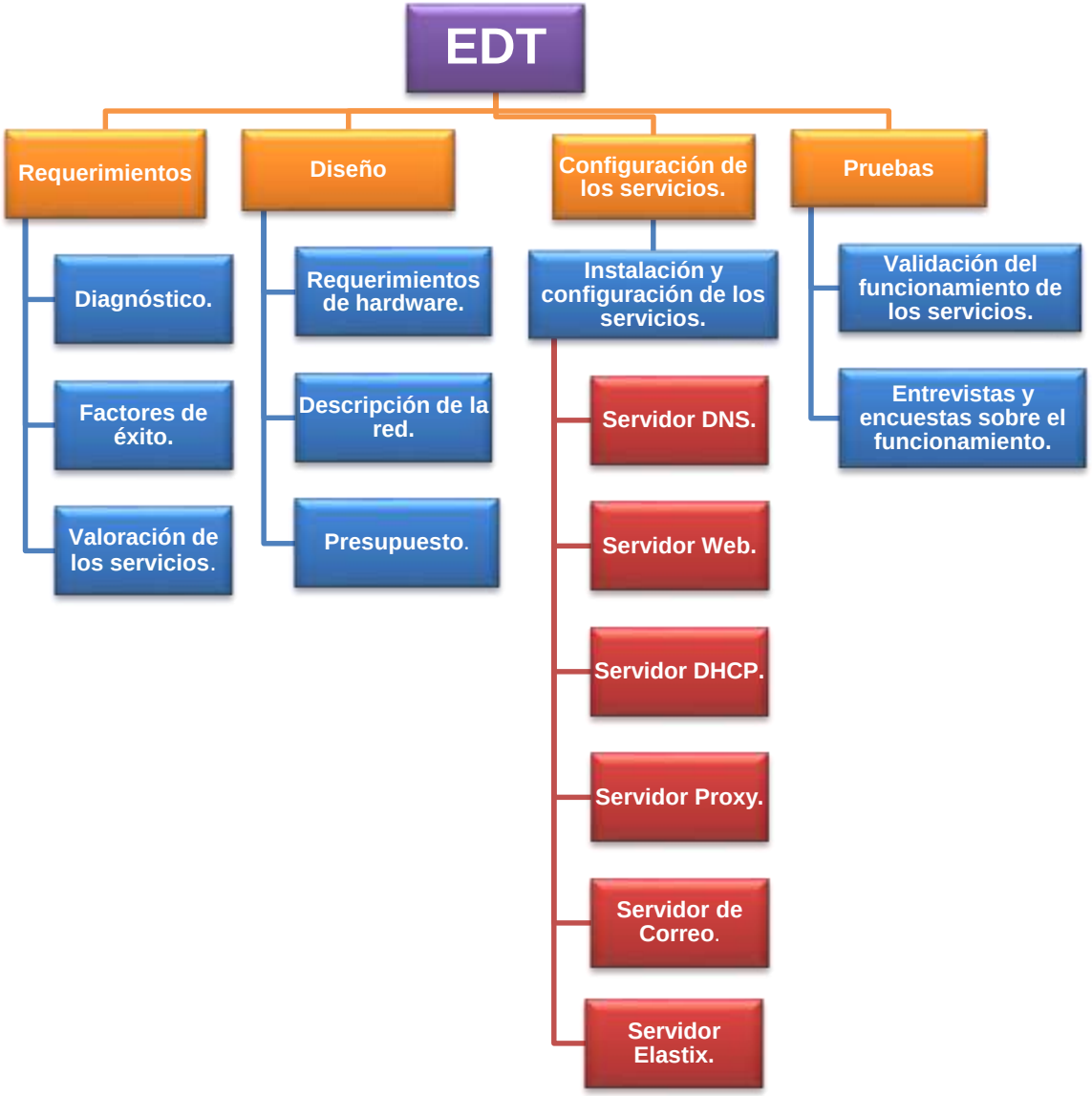


Fig. 17. Estructura de División del Trabajo (EDT).

6.1. Requerimientos.

El levantamiento de requerimientos técnicos permitió contabilizar los equipos disponibles haciendo una valoración del estado funcional de cada uno de ellos; se evaluaron las condiciones físicas del local donde se ubicó el nodo, ubicación geográfica del laboratorio y del área administrativa, donde se realizó el análisis de las distancias lo que permitió el cálculo de cables que fueron utilizados.

6.1.1. Diagnóstico.

La propuesta que se plantea de la instalación y configuración de los servicios surge ante la necesidad que tienen las estudiantes y docentes del Colegio Cristo Rey para el desarrollo tecnológico y ante la inexistencia de una infraestructura LAN dentro del centro educativo, lo que ha llevado a que las alumnas, docentes y personal administrativo se vean limitados en cuanto al acceso a compartir información y aprovechamiento de los recursos que ofrecen las nuevas tecnologías de información. Frente a esta situación la Administración General del Centro aceptó se realizara el levantamiento de requerimientos técnicos de las condiciones actuales del Centro (Ver Anexo 3).

Al momento de hacer levantamiento de requerimientos para el funcionamiento de los servicios propuestos se logró constatar lo descrito en la Tabla 2 y Tabla 3 que se detallan a continuación:

Tabla No.2 Condiciones Técnicas de los equipos del centro.

EQUIPOS	CARACTERÍSTICAS	EVALUACIÓN Y OBSERVACIONES
Computadoras	**Cantidad:** 32, 24 en el laboratorio de computación y 8 de personal administrativo. **Sistema Operativo** Windows 7 Professional. **Procesador:** Intel Pentium de 3 GHZ. **Memoria RAM:** 2 GB. **Disco Duro**: 250 GB.	Todas las maquina se encuentran en estado funcional y con buen mantenimiento.

Tabla No.3 Diagnóstico de las Condiciones del sitio.

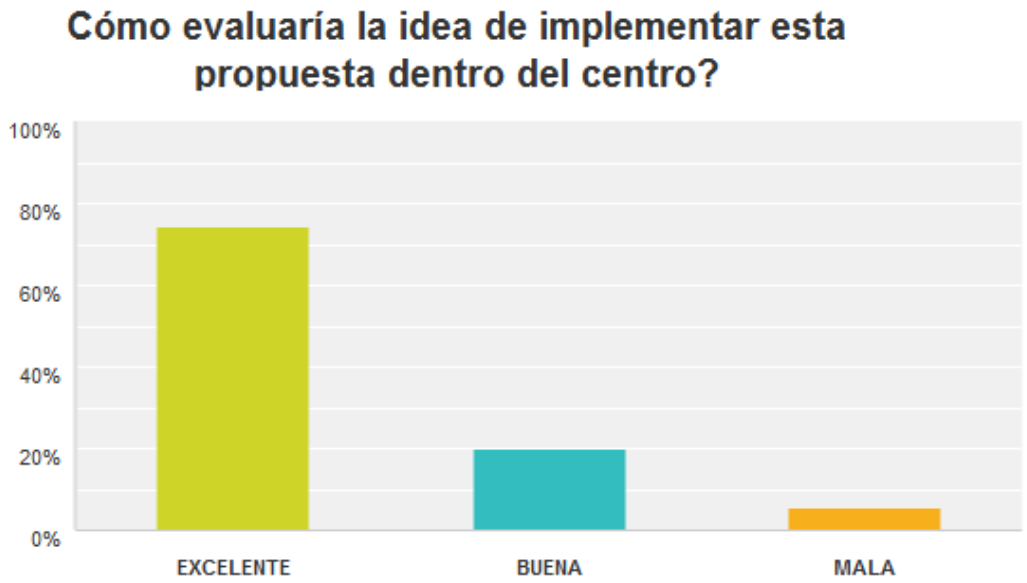
PARTE	CARACTERÍSTICAS	EVALUACIÓN Y OBSERVACIONES
Local	Laboratorio de computación. Dimensiones: 4.5 mts de ancho x 5.20 mts de fondo.	El local presta las condiciones adecuadas. Es necesario realizar una pequeña división para la instalación de los servidores.
Ventilación.	Aire acondicionado marca Samsung. Capacidad: 18,000 BTU.	Buen estado.
Energía	**Tomacorrientes:** 10 tomacorrientes dobles. **Lámparas**: 6. **Sistema de respaldo**: 6 baterías.	2 tomacorrientes deben ser reemplazados ya que se encuentran con desperfecto.
Línea telefónica dedicada.	No existe una red telefónica interna, solo una línea convencional tradicional.	Utilizando Elastix se realizó un diseño de red telefónica que permite la comunicación entre las principales áreas del centro.

6.1.1. Factores de éxito.

Tabla No.4 Factores de Éxito.

FACTOR	DESCRIPCIÓN
Apoyo Institucional.	Se cuenta con el interés y apoyo de la administración del centro en relación a la propuesta presentada.
Responsable del proyecto.	La Directora Administrativa del centro es la persona encargada de gestionar con la Directora General los requerimientos para el seguimiento del proyecto.
Personal Técnico.	El soporte técnico de los equipos de cómputos es un servicio subcontratado ya establecido por el centro. Se deberá coordinar la contratación de un recurso encargado de velar por el buen funcionamiento de los Servidores.
Equipos y local.	Se cuenta con un local ya designado para el funcionamiento de los servicios.

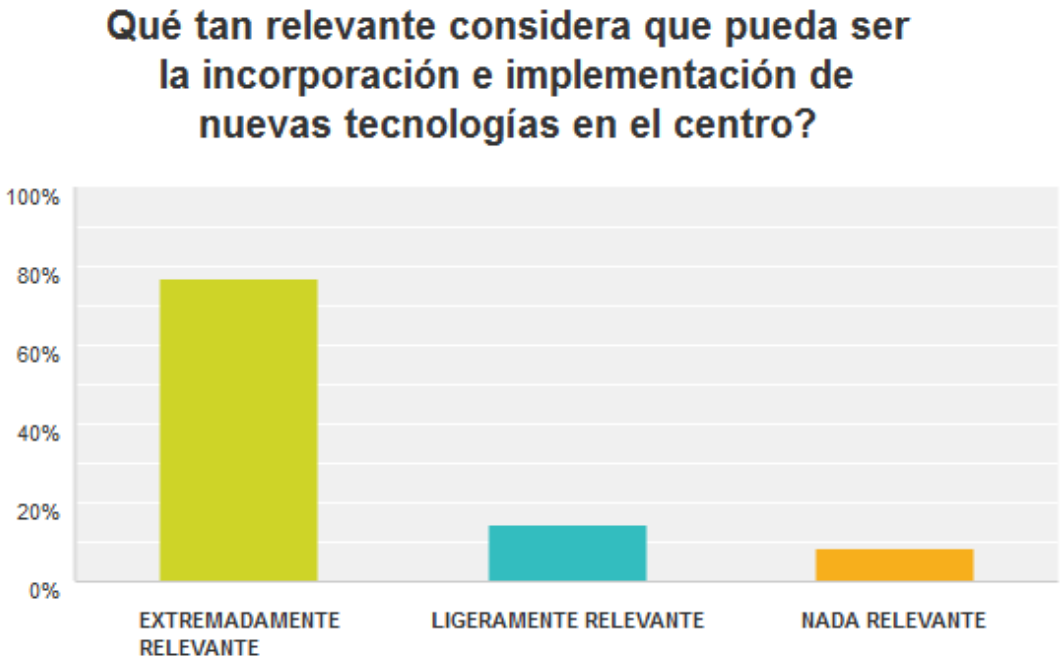
6.1.2. Valoración sobre la implementación de los servicios.



Opciones de respuesta	Respuestas	
EXCELENTE	74,29%	26
BUENA	20,00%	7
MALA	5,71%	2
Total		35

Fig. 18. Opinión de docentes y estudiantes sobre la implementación de la propuesta dentro del colegio.

En la Figura 18, se aprecia que el 74.29% de los estudiantes y docentes encuestados consideran una excelente idea la implementación de la propuesta dentro del centro, seguido por un 20% que la valora una buena idea y apenas un 5.71% que indica es una mala idea.



Opciones de respuesta	Respuestas	
EXTREMADAMENTE RELEVANTE	77,14%	27
LIGERAMENTE RELEVANTE	14,29%	5
NADA RELEVANTE	8,57%	3
Total		35

Fig. 19. Opinión de docentes y estudiantes sobre la relevancia de incorporar e implementar nuevas tecnologías dentro del centro.

La figura 19 resume las opiniones de los estudiantes y docentes encuestados en lo referente a la importancia y relevancia que tiene la implementación de nuevas tecnologías dentro del centro. Puede notarse que una mayoría (77.14%), señala que es extremadamente relevante incorporar y aprovechar las herramientas que ofrecen las nuevas tecnologías. Un 14.29% expresa que es ligeramente relevante y una minoría (9%) opina que no es relevante.

6.2. Diseño.

El aspecto más importante del diseño fue la elaboración del diagrama completo de la red donde se muestra la ubicación de los servidores y la distribución de cada una de las subredes en la red de área local, ubicación del enrutador y los puntos de acceso para la comunicación inalámbrica.

6.2.1. Requerimientos de hardware.

Los presentes son los requerimientos mínimos recomendados para los servidores instalados. Algunas de las razones que pueden hacer variar estos valores son: aumento en la cantidad de usuarios, otras aplicaciones que corran en el servidor y el tamaño y cantidad de los documentos.

- **Servidor de servicios DNS, Correo y Proxy:**
  - Procesador Intel/AMD 2.0 GHZ+ 64-bit.
  - RAM 2GB (recomendados 4GB).
  - Disco duro: 50 GB.

- **Servidor Web:**
  - Procesador de 2 GHZ.
  - RAM 2GB.
  - Disco Duro: 250 GB.

- **Servidor de servicio VoIP (Elastix) y DHCP:**
  - Cualquier Pentium.
  - RAM 512.
  - Disco duro de 40 GB.

6.2.2. Descripción general de la red.

La estructura general de la red que se propone, está dispuesta en la figura 20, en la cual se expresa con claridad la ubicación de los servidores y la conexión con conmutadores y enrutador.

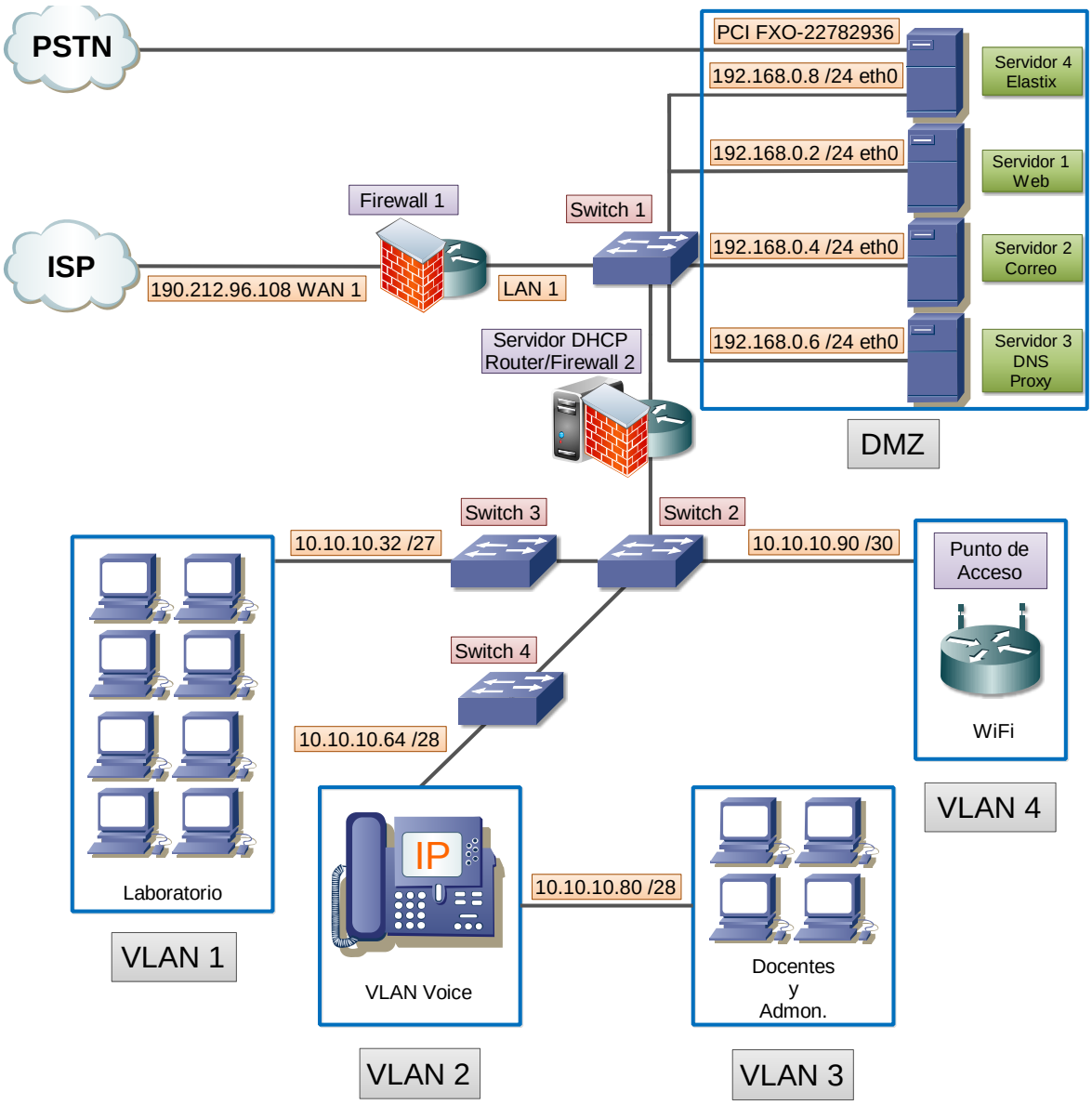


Fig. 20. Estructura general de la red.

A continuación se realiza una breve descripción para cada equipo de la red, detallando la conectividad de los equipos a través de sus interfaces,

Firewall 1: FORTINET 60D, posee 7 puertos de entrada-salida para tecnología Ethernet (cable UTP, conector RJ-45), que son utilizados para las subredes de área local. Tiene 2 puertos Ethernet para red de área extensa denominadas WAN1, puerto Ethernet para zona desmilitarizada (DMZ) y 1 puerto USB para servidor.

El FORTINET 60D puede ser administrado vía consola o a través de una PC vía Web mediante uno de los puertos RJ-45 para acceso desde internet o desde la red local. La figura 21 muestra las especificaciones de las interfaces del FORTINET 60D.

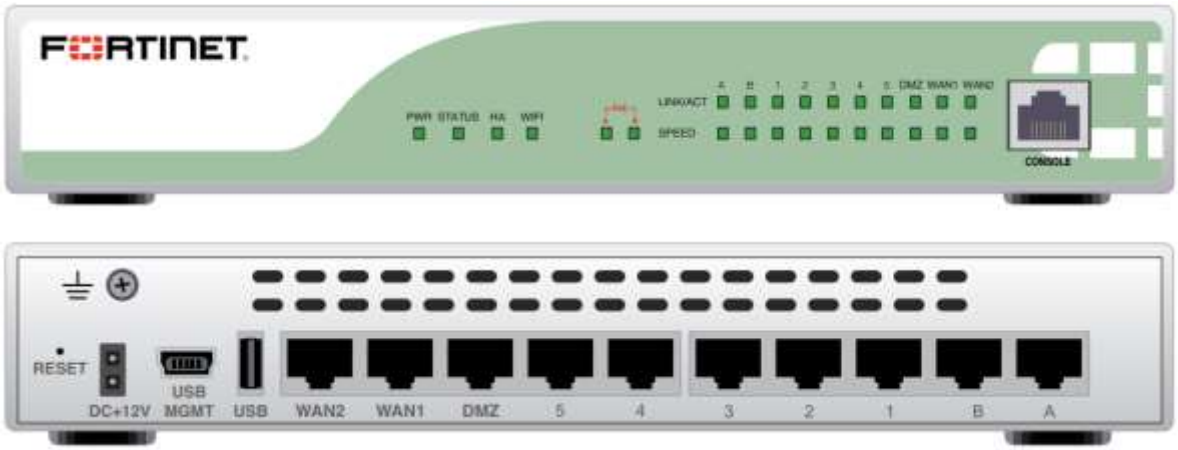


Fig. 21. Especificación de las interfaces del FORTINET.

- **WAN1:** Le es asignada una Dirección IP pública, es la interfaz mediante la cual el FORTINET se conecta al ISP.

- **LAN1:** Tiene asignada la Dirección IP 10.10.10.1 y es la interfaz que conecta al enrutador con el switch 1 al cual se conectan los servidores (web, correo electrónico, proxy y DNS) con las direcciones IP mostradas en la tabla número 5. A esta zona donde están todos los servidores se le llama “Zona Desmilitarizada”. Esta es una red local del administrador del nodo, normalmente es privada, y los clientes no tendrán acceso a ella, solamente para recibir los servicios que ofrece.

Tabla No.5 Direcciones de Servidores.

Servidores	Dirección	Máscara de subred
Servidor Web	192.168.0.2	255.255.255.0
Servidor de Correo	192.168.0.4	255.255.255.0
Servidor DNS y Proxy	192.168.0.6	255.255.255.0
Servidor Elastix y DHCP	192.168.0.8	255.255.0.0

- **Servidor DHCP, Router/Firewall 2**: Se concibió una PC con sistema operativo Zeroshell el cual prestar el servicio de Router/Firewall. Zeroshell es una distribución Linux para servidores y dispositivos embebidos, que provee de servicios de red. Es un Firewall (figura 22) gratuito que tiene las características de los equipos complejos de seguridad, además de funcionar como router y servidor DHCP.

Fig. 22. Configuración de Firewall.

La figura 23 muestra la tabla de enrutamiento de las direcciones IP de la red:

Fig. 23. Tabla de enrutamiento.

Dispone de un interfaz web para su configuración, pero también puede ser administrado desde un terminal remoto. Este servidor interconecta la zona desmilitarizada con todos los clientes de la red local que tendrán como puerta de enlace la dirección del servidor proxy, sin embargo la red de área local está dividida en diferentes subredes como se muestra en la tabla número 6.

En las cuatros subredes los clientes deberán estar previamente identificados para tener acceso a internet.

Tabla No.6 Direcciones de red por subredes.

Subredes	Dirección	Máscara de subred
Laboratorio	10.10.10.32	255.255.255.224
VLAN Voice	10.10.10.64	255.255.255.240
Docentes y Admón.	10.10.10.80	255.255.255.240
Punto de Acceso WiFi	10.10.10.90	255.255.255.252

6.2.3. Presupuesto.

Tomando en cuenta las especificaciones y consideraciones del diseño y la infraestructura del centro (Ver Anexo 4), se elaboró una lista de equipos y materiales requeridos para el funcionamiento correcto de la red, la lista se muestra a continuación en la siguiente tabla:

Tabla 7. Presupuesto de materiales y equipos.

Descripción del artículo	Cantidad	Costo x UND (USD)	Costo total (USD).
FORTINET 60D	1	472.00	472.00
Router Linksys Rv082	1	80.99	80.99
Cisco WS-C2960 24-PT	1	329.00	329.00
TredNet TEG-2248WS 48-PT	1	203.62	203.62
NETGEAR GS108NA ProSafe 8-Port	2	48.45	96.09
Servidor Lenovo ThinkServer TS140 (3.2 GHz Intel Xeon E3-1225 v3 Processor)	2	399.99	799.98
Intel Gigabit ET Dual Port Server Adapter - PCI Express x4 - 2 Port - 10/100/1000Base-T	1	66.71	66.71
Teléfono IP Grandstream GXP1400	6	30.00	180
Cable Ethernet Cat5E 1000ft	2	48.99	97.98
Conectores RJ45 100 pack	2	10.66	21.32
TOTAL:			2347.7

6.3. Configuración de los servicios.

Para efectos de prueba de funcionamiento se utilizó máquinas virtuales VMWare y Virtualbox, lo que permitió la instalación y configuración de cada uno de los servicios tanto en modo texto como en modo gráfico.

6.3.1. Configuración e instalación de los servicios.

La instalación y configuración de los servicios fue realizada bajo ambiente Linux, precisamente utilizando SLES o Suse Linux Enterprise Server 11. A continuación se detallan los archivos de configuración de cada uno de los servicios planteados en el diseño.

6.3.1.1. DNS

El DNS es sin duda es uno de los servicios más importantes de la red. Para la configuración de éste se deben configurar los siguientes archivos:

- ✓ /etc/hosts
- ✓ /etc/resolv.conf
- ✓ /etc/named.conf
- ✓ /var/lib/named/archivos de zona directa.
- ✓ /var/lib/named/archivos de zona inversa.

- **/etc/hosts,** contiene la resolución del equipo servidor definido localmente usando la dirección IP, el FQDN y un Alias (nombre corto del FQDN). El contenido de este archivo puede apreciarse en la figura siguiente:

```
127.0.0.1       localhost
192.168.0.1     server.colegiocristorey.edu.ni server
```

Fig. 24. Contenido del archivo /etc/hosts.

- **etc/resolv.conf,** resuelve los nombres de los servidores de internet, define varios parámetros y tiene la siguiente forma que se muestra en la siguiente figura:

```
search colegiocristorey.edu.ni
domain colegiocristorey.edu.ni
nameserver 192.168.0.1
```

Fig. 25. Contenido del archivo /etc/resolv.conf.

El parámetro `search` es utilizado como un auxiliar para la resolución de nombres, mientra que el parámetro `domain` indica el dominio al cual pertenece el "host", en este caso `colegiocristorey.edu.ni`. El parámetro `nameserver`, indica cuales con las direcciones IP de los servidores DNS que deben ser utilizados.

- **/etc/named.conf,** se puede dividir en dos áreas. Una es la sección `"options"` para los ajustes generales y la otra consiste en entradas de zonas `"zone"` para los dominios individuales. El archivo completo se puede ver en la figura 26.

```
# Copyright (c) 2001-2004 SuSE Linux AG, Nuernberg, Germany.
# All rights reserved.
#
# Author: Frank Bodammer, Lars Mueller <lmuelle@suse.de>
#
# /etc/named.conf
#
# This is a sample configuration file for the name server BIND 9.  It works as
# a caching only name server without modification.
#
# A sample configuration for setting up your own domain can be found in
# /usr/share/doc/packages/bind/sample-config.
#
# A description of all available options can be found in
# /usr/share/doc/packages/bind/misc/options.

options {

        # The directory statement defines the name server's working directory

        directory "/var/lib/named";

        # Write dump and statistics file to the log subdirectory.  The
        # pathenames are relative to the chroot jail.
       dump-file "/var/log/named_dump.db";
       statistics-file "/var/log/named.stats";

       # The forwarders record contains a list of servers to which queries
       # should be forwarded.  Enable this line and modify the IP address to
       # your provider's name server.  Up to three servers may be listed.

       #forwarders { 192.0.2.1; 192.0.2.2; };

       # Enable the next entry to prefer usage of the name server declared in
       # the forwarders section.

       #forward first;

       # The listen-on record contains a list of local network interfaces to
       # listen on.  Optionally the port can be specified.  Default is to
       # listen on all interfaces found on your system.  The default port is
       # 53.

       #listen-on port 53 { 127.0.0.1; };

       # The listen-on-v6 record enables or disables listening on IPv6
       # interfaces.  Allowed values are 'any' and 'none' or a list of
       # addresses.
```

```
        listen-on-v6 { any; };

        # The next three statements may be needed if a firewall stands between
        # the local server and the internet.

        #query-source address * port 53;
        #transfer-source * port 53;
        #notify-source * port 53;

        # The allow-query record contains a list of networks or IP addresses
        # to accept and deny queries from. The default is to allow queries
        # from all hosts.

        #allow-query { 127.0.0.1; };

        # If notify is set to yes (default), notify messages are sent to other
        # name servers when the the zone data is changed.  Instead of setting
        # a global 'notify' statement in the 'options' section, a separate
        # 'notify' can be added to each zone definition.

        notify no;

# To configure named's logging remove the leading '#' characters of the
# following examples.
#logging {
#       # Log queries to a file limited to a size of 100 MB.
#       channel query_logging {
#               file "/var/log/named_querylog"
#                       versions 3 size 100M;
#               print-time yes;                 // timestamp log entries
#       };
#       category queries {
#               query_logging;
#       };
#
#       # Or log this kind alternatively to syslog.
#       channel syslog_queries {
#               syslog user;
#               severity info;
#       };
#       category queries { syslog_queries; };
#
#       # Log general name server errors to syslog.
#       channel syslog_errors {
#               syslog user;
#               severity error;
```

```
#       };
#       category default { syslog_errors;  };
#
#       # Don't log lame server messages.
#       category lame-servers { null; };
#};

# The following zone definitions don't need any modification.  The first one
# is the definition of the root name servers.  The second one defines
# localhost while the third defines the reverse lookup for localhost.

zone "." in {
        type hint;
        file "root.hint";
};

zone "localhost" in {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "colegiocristorey.edu.ni" in {
        type master;
        file "colegio.zone";
};

zone "0.168.192.in-addr.arpa" in {
        type master;
        file "192.168.0.zone";
};

# Include the meta include file generated by createNamedConfInclude.  This
# includes all files as configured in NAMED_CONF_INCLUDE_FILES from
# /etc/sysconfig/named

# include "/etc/named.conf.include";

# You can insert further zone records for your own domains below or create
# single files in /etc/named.d/ and add the file names to
# NAMED_CONF_INCLUDE_FILES.
# See /usr/share/doc/packages/bind/README.SUSE for more details.
```

Fig. 26. Configuración del archivo /etc/named.conf

La sección "options" está definida por defecto y con una breve descripción de su operación. A continuación se describen las opciones que fueron modificadas en el archivo:

```
#allow-query { 127.0.0.1; };
```

Los archivos de zona son consideras como zona de dominio. La zona es directa cuando se especifica el nombre de dominio, por ejemplo:

```
zone "colegiocristorey.edu.ni"
```

La zona es inversa cuando se especifican los primeros 3 octetos de la dirección IP en orden inverso seguido del subdominio: ".in-addr.arpa", por ejemplo:

```
.in-  zone "0.168.192.in-addr.arpa"
```

Al especificar `type master`, significa que este servidor DNS contiene la información principal sobre el dominio. El parámetro "file" indica el nombre del archivo que contiene los parámetros específicos de la zona, este archivo es denominado archivo de zona y se encuentra en la ruta /var/lib/named/.

```
"localhost.zone";
"127.0.0.zone";
"colegio.zone";
"192.168.0.zone";
```

En los archivos de zona se encuentran algunos registros que definen los valores que se pueden consultar, entre los más comunes están:

A (Address):	Dirección IP de un cliente.
MX (Mail Xchange):	Lista priorizada de dónde entregar el correo.
SOA (Start of Authority):	Comienzo de los datos de la zona.
NS (Name Server):	Indica un servidor de nombres.
PTR (Pointer):	Alías para una dirección IP.
CNAME (Canonical Name):	Nombre del dominio (alías).
IN(Internet**):**	Clase que se aplica en internet.

- **Zona Directa:** a continuación se describen cada uno de los archivos de configuración para la resolución de zonas directas.

  Lo primero es copiar el archivo plantilla `localhost.zone` y guardarlo con el nombre de archivo de zona directa a configurar, por ejemplo:

  ```
  Cp localhost.zone colegio.zone
  ```

  La figura 27 muestra lo que contiene este archivo de zona que incluye el servidor DNS, servidor web y servidor de correo (mail):

```
$TTL 1W
@               IN SOA  server.colegiocristorey.edu.ni.  root (
                        42              ; serial (d. adams)
                        2D              ; refresh
                        4H              ; retry
                        6W              ; expiry
                        1W )            ; minimum

                    IN NS           server
                    IN A            127.0.0.1
                    IN A            192.168.0.1
                    IN MX   10      mail
server              IN A            192.168.0.1
mail                IN A            192.168.0.1
web                 IN A            192.168.0.1


www                 IN CNAME        web
```

Fig. 27. Configuración del archivo de zona directa /var/lib/named/colegio.zone.

A continuación se describe el archivo:

Aquí comienza la parte del registro de control SOA (Inicio de autoridad):

```
@               IN SOA  server.colegiocristorey.edu.ni.
```

- El símbolo @ corresponde al nombre de la zona de dominio especificada en el archivos `/etc/named.conf`.
- El parámetro IN SOA define el servidor de nombres que actuará como principal en esta zona.
- A continuación aparece la dirección de correo electrónico de la persona que se encarga de este servidor de nombres. Como el símbolo @ ya tiene un significado

especial, se reemplaza por un punto. Por tanto se debe escribir `server.colegiocristorey.edu.ni.` Debe incluirse un punto al final para impedir que la zona se añada.

- El paréntesis de apertura (incluye todas las líneas que se hayan en el registro SOA hasta el paréntesis de cierre).
- IN NS especifica el servidor de nombres responsable de este dominio. En este caso `IN NS server`.
- El registro MX indica el servidor de correo que acepta, procesa y remite los mensajes de correo electrónico al dominio. En este ejemplo, se trata del host `mail.colegiocristorey.edu.ni`. El número situado delante del nombre del host se corresponde con el valor de preferencia.

```
IN MX   10      mail
```

A través del registro A (address o dirección IP) se utiliza para asignar la dirección IP a los nombres de host. El dominio "`colegiocristorey.edu.ni`" se añadirá a todos ellos automáticamente.

El registro A toma la forma mostrada en la siguiente figura:

```
                    IN NS           server
                    IN A            127.0.0.1
                    IN A            192.168.0.1
                    IN MX   10      mail
server              IN A            192.168.0.1
mail                IN A            192.168.0.1
web                 IN A            192.168.0.1
```

Fig. 28. Uso de los registros IN A.

Nota: En la figura 27 también se puede observar que al utilizar el alias www se puede acceder al servidor "web" (CNAME significa nombre canónico), es decir este registro enviará todas las solicitudes de `www.colegiocristorey.edu.ni` a `web.colegiocristorey.edu.ni`.

- **Zona Inversa:** para la resolución de zona inversa solo se copia el archivo `127.0.0.zone` ubicado en `/var/lib/named`y se le asigna el nombre del archivo de zona a configurar, en este caso `192.168.0.zone` con la orden `cp`:

```
Cp 127.0.0.zone 192.168.0.zone
```

Para la modificación, solamente se reemplaza la palabra localhost por el FQDN (colegiocristorey.edu.ni.):

```
$TTL 1W
@ IN SOA server.colegiocristorey.edu.ni. root.colegiocristorey.edu.ni. (
                                42              ; serial (d. adams)
                                2D              ; refresh
                                4H              ; retry
                                6W              ; expiry
                                1W )            ; minimum

                IN NS           server.colegiocristorey.edu.ni.
1               IN PTR          server.colegiocristorey.edu.ni.
1               IN PTR          web.colegiocristorey.edu.ni.
1               IN PTR          mail.colegiocristorey.edu.ni.
1               IN PTR          proxy.colegiocristorey.edu.ni.
```

Fig. 29. Archivo /var/lib/named/192.168.0.zone.

Para iniciar automáticamente el servidor DNS es necesario iniciar `named` activándolo en el editor de niveles de ejecución. Con el fin de que siempre se inicie al arrancar el sistema, se debe activar para los niveles de ejecución 3, 4 y 5: `chkconfig –level 345 named on`.

En caso de no estar activo, en todos los sistemas Unix existe un script de arranque que puede ser utilizado para arrancar el servidor a través de la orden: `service named restart`. Adicional BIND brinda 3 herramientas para la prueba del servicio: `dig, nslookup y host.`

6.3.1.2. Servidor Web.

El sitio web fue desarrollado con Joomla, una herramienta de administración de Sistema de gestión de contenidos (CMS, Content Management System) que trabaja con entorno Apache y PHP, posee una base de datos controlada mediante MySQL donde se aloja toda la información de la página web (noticias, actividades, publicaciones, comentarios, etc.) y la información de los usuarios registrados. Cabe destacar que todas las herramientas utilizadas para el desarrollo del sitio son Open Source.

Para un mejor manejo de una página web desarrollada en Joomla se requiere tener ciertos servicios instalados, principalmente Apache y MySQL. Se realizó la descarga del paquete XAMPP, que es una distribución de Apache completamente gratuita que contiene MySQL, PHP y Perl.

1. Inicialmente se debe descargar el paquete desde la web http://www.apachefriends.org/en/xampp-linux.html
2. Una vez descargado se descomprime el paquete descargado desde una terminal y se ejecuta la instalación:

   ```
   sudo tar xvfz xampp-linux-1.8.3.tar.gz -C /opt
   sudo ./xampp-linux-1.8.3-5-installer.run
   ```
3. Una vez finalizada la instalación XAMPP ya se encuentra listo en el sistema y se guarda en la carpeta `/opt/lampp`. Se debe arrancar el servicio utilizando la siguiente línea de comando:

   ```
   linux:~ # sudo /opt/lampp/lampp start
   Starting XAMPP for Linux 1.8.3-5...
   XAMPP: Starting Apache...ok.
   XAMPP: Starting MySQL...ok.
   XAMPP: Starting ProFTPD...ok.
   linux:~ #
   ```

En XAMPP se puede configurar la contraseña para aumentar el grado de seguridad del sitio. Tecleando en el navegado `http://localhost/xampp/` nos direcciona a la página principal (ver figura 30):

Fig. 30. Configuración de XAMPP.

Dentro de XAMMP se muestra una ventana de acceso para entrar en `http:/localhost/phpMyAdmin` (ver figura 31):

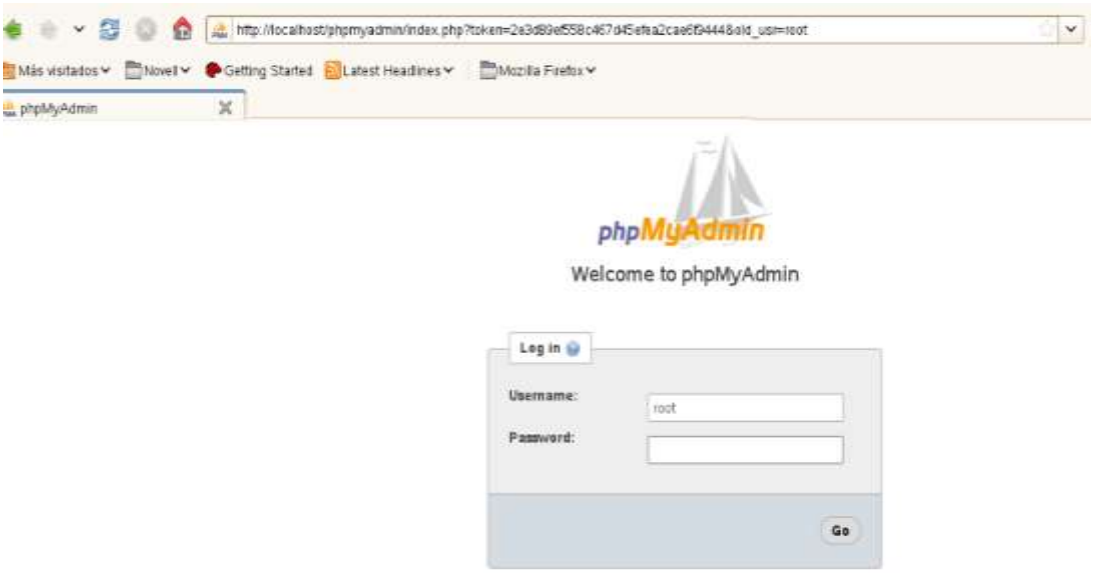


Fig. 31. Interfaz de ingreso a phpMyAdmin.

Siendo una página web dinámica el sitio posee una interfaz cómoda y simple para el usuario ya que consta de un solo menú principal donde están ubicados los controles para acceder a las diferentes secciones de la página, la siguiente figura muestra el diagrama estructural de la página web.

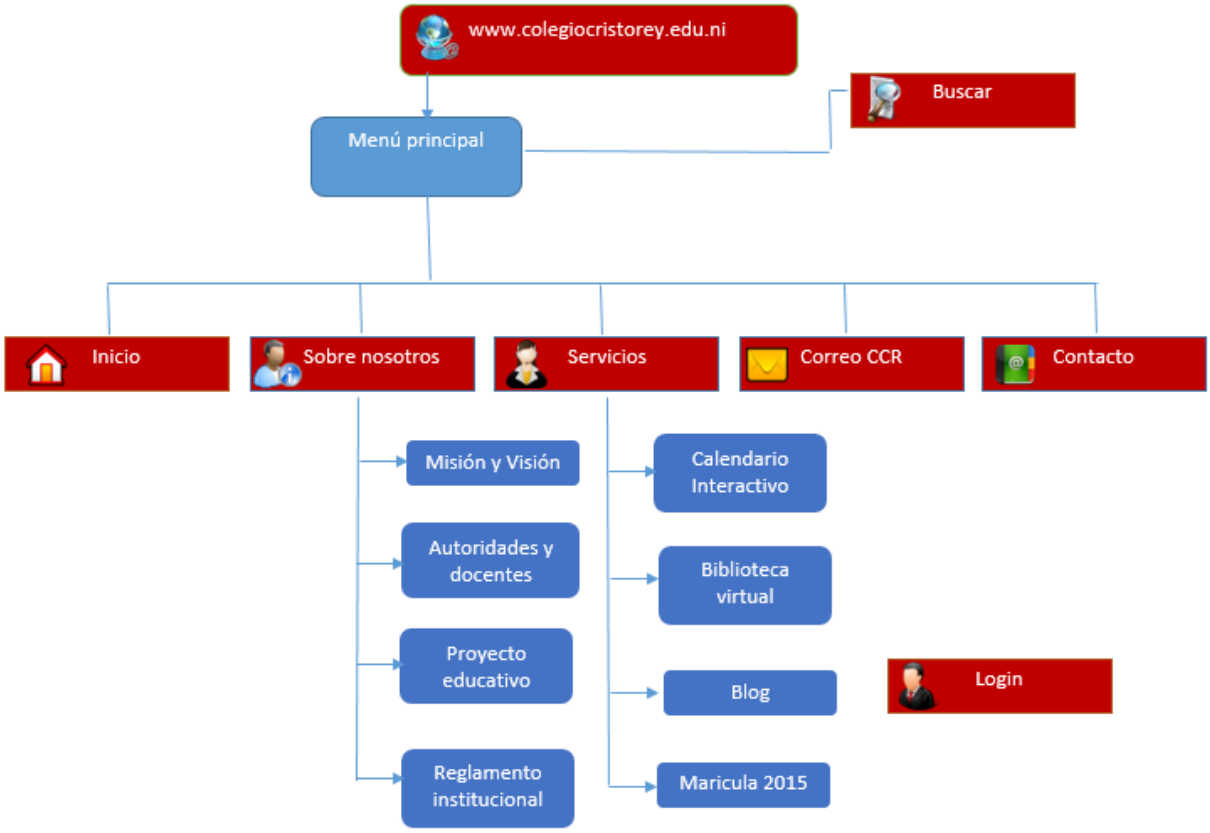


Fig. 32. Diagrama estructural de página web.

En la pantalla principal del sitio se encuentra la vista inicial de la página con una sección de imágenes que se enlazan con actividades o noticias que estarán inactivas hasta que el usuario decida que ver, cuenta con vistas rápidas de artículos publicados del centro educativo así como con artículos multimedia para su visualización. Posee una sección de enlaces externos de páginas de interés social y paginas amigas. La figura 33 muestra la interfaz gráfica principal del sitio web.

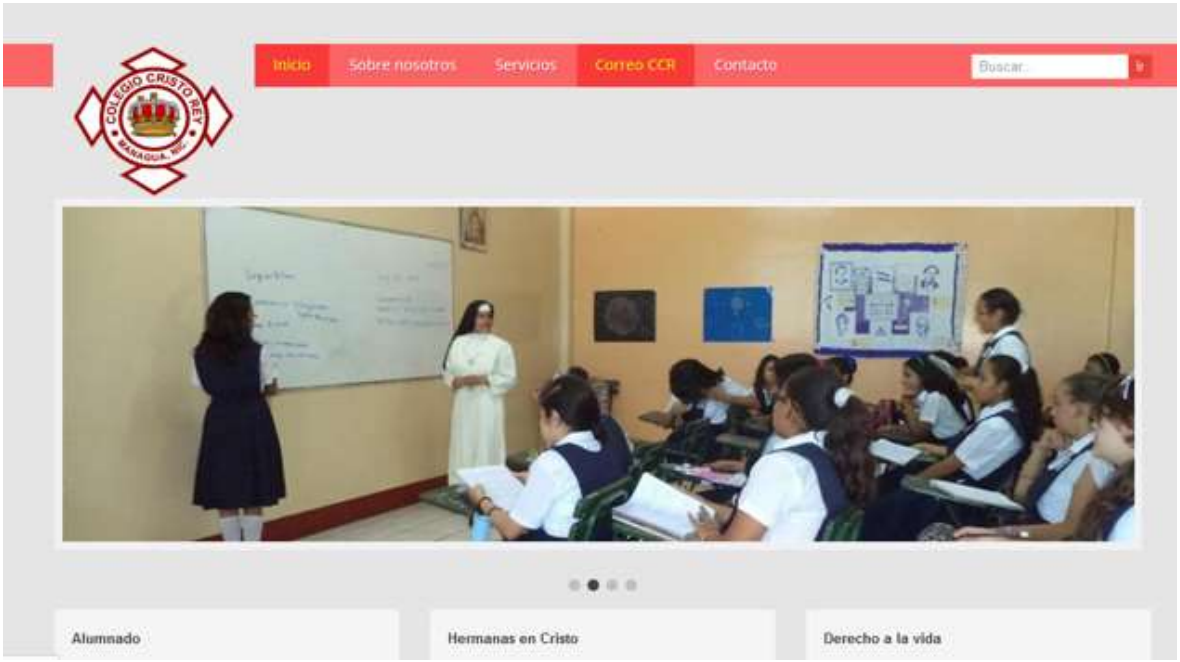


Fig. 33. Interfaz gráfica principal.

6.3.1.3. DHCP.

Este servicio es de vital importancia ya que permitirá asignar de forma automática direcciones a los dispositivos (PC, Teléfonos IP, ATA, etc.) de la red.

Para hacer uso de este servicio se hará uso del Sistema Zeroshell el cual es una distribución Linux para servidores y configurable vía web.

Zeroshell es una distribución “Live”, esto significa que no es necesario de una instalación para que funcione.

La figura 34 muestra su interfaz modo texto, en esta se deben configurar parámetros fundamentales como activación de perfil “Activate Profile” y gestor IP “IP Manager” los cuales son necesarios para ingresar vía Web, aunque el sistema operativo trae por defecto la IP 192.168.0.75.

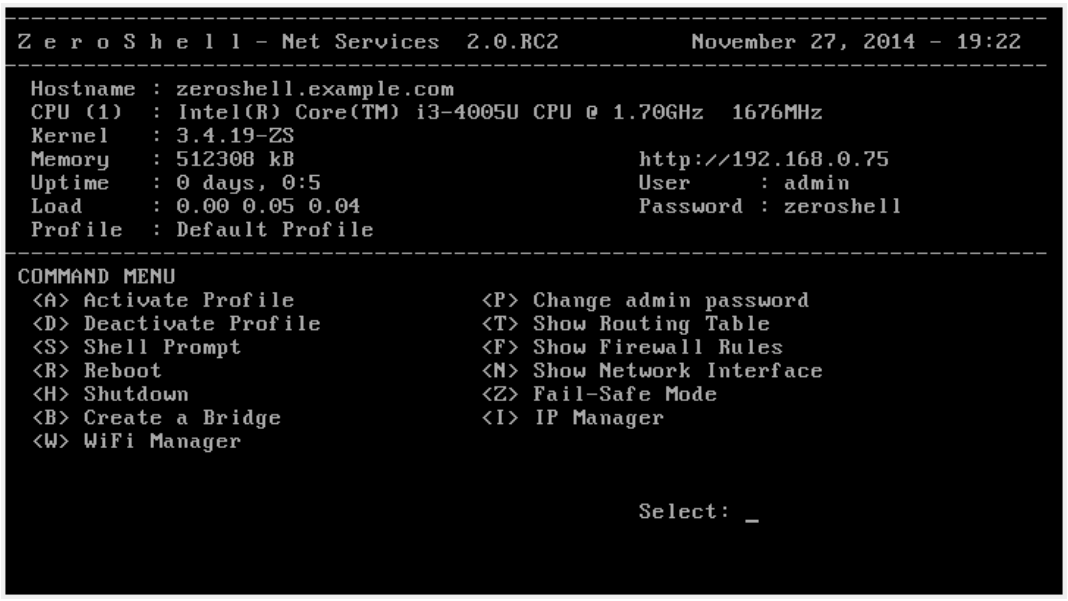


Fig. 34. Interfaz de configuración modo texto de Zeroshell.

Una vez configurado los parámetros antes mencionados se procede a su configuración a través de la interfaz gráfica vía web, para ello se debe ingresar la dirección IP asignada. La figura 35 muestra la pantalla grafica de inicio, donde solicita ingresar el usuario que por defecto es “admin” y la contraseña que es “zerozero”, esta información puede ser modificada

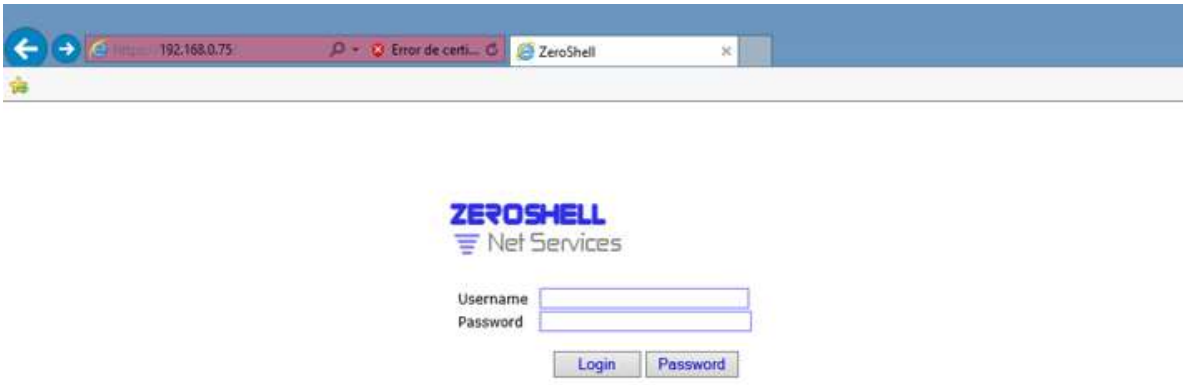


Fig. 35. Interfaz gráfica de incio.

Al ingresar se procede a la configuración del servidor DHCP. En la figura 36 se muestran los parámetros que se deben configurar para habilitar el servicio DHCP.

Para ello se selecciona en la casilla “Subnet” la interfaz a configurar, luego en “Range” se asignan los rangos de direcciones IP y en “Default Gateway” se define la puerta de Enlace.

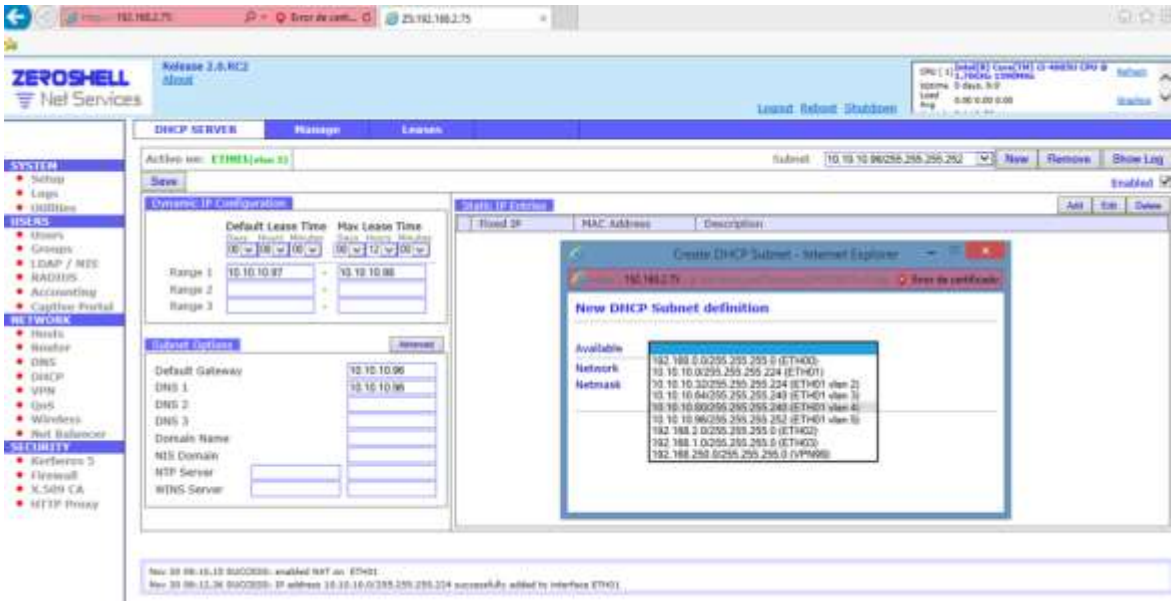


Fig. 36. Configuración del servicio DHCP.

6.3.1.4. PROXY.

Squid utiliza el archivo de configuración localizado en `/etc/squid/squid.conf`. Existe un gran número de parámetros en este archivo, de los cuales se configuran los siguientes:

- **http_port:** los puertos registrados (rango desde 1024 hasta 49151) recomendados para proxies pueden ser el 3128 y 8080 a través de TCP. De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible como el 8080 o bien que lo haga en varios puertos disponibles a la vez.

```
# You may specify multiple socket addresses on multiple lines
# Default: http_port 3128
http_port 3128
http_port 8080
```

Si se desea incrementar la seguridad, se puede vincular el servicio a una dirección IP que solo se pueda acceder desde la red local. En este caso el servidor utilizado posee una IP `192.168.0.1` Puede hacerse lo siguiente:

```
# You may specify multiple socket addresses on multiple
lines
# Default: http_port 3128
http_port 192.168.0.1:3128
http_port 192.168.0.1:8080
```

- **cache_mem:** establece la cantidad ideal de memoria para los objetos en tránsito, los cuales se almacenan en bloques de 4Kb. De modo predefinido se establecen 8Mb, pero se puede especificar más memoria, en este caso se establecieron :

```
cache_mem 64 MB
```

- **caché_dir**: Este parámetro se utiliza para establecer que tamaño desea que tenga el caché en el disco duro para Squid, es decir, cuanto se desea almacenar de internet en el disco duro. De modo predefinido Squid utiliza un caché de100MB, 16 directorios con 256 niveles cada uno.

```
cache_dir ufs /var/spool/Squid 100 16 256
```

- **caché_mgr**: de modo predefinido, si algo ocurre con el caché, como por ejemplo que mueran los procesos, se enviara un mensaje de aviso a la cuenta webmaster del servidor:

```
cache_mgr webmaster@colegiocristorey.edu.ni
```

- **Listas de control de acceso (ACL):** sirven para definir a los usuarios por redes, listas negras, sitios denegados, contenido que se puede bajar de internet, etc.

Generalmente una ACL se establece con la siguiente sintaxis:

```
acl [nombre de la lista] src [lo que compone a la lista]
```

La declaración de ACL en archivo `/etc/squid.conf` es la siguiente:

```
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl redlocal src 192.168.0.0/255.255.0.0
acl sitiosdenegados url_regex "etc/squid/sitios-denegados"
```

Fig. 37. Definición de una Lista de Control de Acceso.

- **Reglas de control de acceso (http_access):** estas definen si se permite o no el acceso a Squid. Se aplican a las ACL y deben colocarse en la sección de reglas de control de acceso definidas por el administrador, a partir de donde se localiza la siguiente leyenda:

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow redlocal
http_access allow localhost
http_access allow  redlocal !sitios denegados
http_access deny all
```

Fig. 38. Definición de Reglas de Control de Acceso.

La sintaxis básica es la siguiente:

`http_access [deny o allow] [lista de control de acceso]`

A continuación una breve descripción de las reglas antes descritas:

- `http_access allow localhost:` permite el acceso total al localhost, es decir al mismo servidor.
- `http_access allow redlocal:` Permite el acceso a Squid a la Lista de Control de acceso denominada redlocal, la cual está conformada por 192.168.0.0/255.255.0.0.
- `http_access allow redlocal !sitios denegados`: permite el acceso a las ACL denominada redlocal pero le niega el acceso a todo lo que coincida con lo especificado en las Listas de Control de Acceso denominadas sitiosdenegados.

- **Proxy Caché con aceleración.**

Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché de Squid. Si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet.

Esta función permite navegar rápidamente cuando los objetos ya están en el caché de Squid y además optimiza enormemente la utilización del ancho de banda.

En la sección `HTTPD ACCELERATOR OPTIONS` deben agregarse los siguientes parámetros:

```
# HTTPD-ACCELERATOR OPTIONS
# -----------------------------------------------------------------------------

#  TAG: httpd_accel_no_pmtu_disc        on|off
#       In many setups of transparently intercepting proxies Path-MTU
#       discovery can not work on traffic towards the clients. This is
#       the case when the intercepting device does not fully track
#       connections and fails to forward ICMP must fragment messages
#       to the cache server.
#
#       If you have such setup and experience that certain clients
#       sporadically hang or never complete requests set this to on.
#
#Default:
httpd_accel_no_pmtu_disc on
```

Fig. 39. Configuración del Proxy cache con aceleración.

6.3.1.5. Servidor de Correo.

Los pasos para la instalación de Zimbra son sencillos y se describen a continuación:

Se debe descomprimir el paquete donde viene el instalador de Zimbra a través de la orden tar:

```
tar –xvzf zcs-6.0.2_GA_1912.SLES11_64.20091020140456.tgz
```

Una vez que el archivo se descomprime, se utiliza la terminal para entrar al directorio donde se descomprimió y se ejecuta el instalador:

```
./install.sh
```

La instalación procede y se muestran todos los paquetes que se instalan de Zimbra, así como los requerimientos de software necesario. En caso de no encontrar un paquete del servidor se detiene la instalación y se procede a instalar el paquete solicitado.

Los paquetes se instalan presionando las teclas Y (Si) o N (No) y luego enter. Al momento de instalar Zimbra Proxy, se presiona la tecla N para evitar conflictos con el servidor Squid y se prosigue con la instalación (Ver fig. 40).

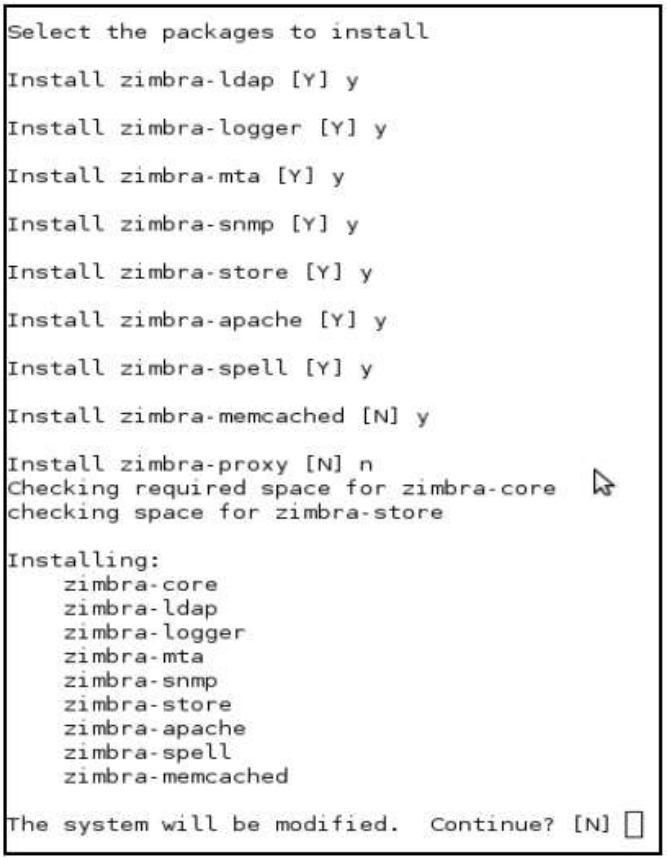


Fig. 40. Inicio de instalación de Zimbra.

En el proceso se muestra si se desea continuar puesto que el programa será modificado y se debe presionar la tecla Y como se muestra en la figura anterior.

Por defecto Zimbra no reconoce el registro MX asociado al servidor mail para resolverlo, por lo tanto se debe poner solamente el nombre del dominio (Ver fig. 41).

```
DNS ERROR - none of the MX records for mail.colegiocristorey.edu.ni
resolve to this host
Change domain name? [Yes] y
Create domain:[mail.colegiocristorey.edu.ni] colegiocristorey.edu.ni
```

Fig. 41. Error DNS.

Si surge algún conflicto de puertos de servicios como el puerto 25 de Postfix u otro servicio se puede abrir otra terminal y detener estos, continuando con la instalación:

```
Service postfix stop
```

En el menú que se muestra a continuación en la figura 42, se observa la configuración de cada paquete de Zimbra. Se elige el número 3 para entrar a las opciones de `Zimbra-store`:

```
Main menu

   1) Common Configuration:
   2) zimbra-ldap:                          Enabled
   3) zimbra-store:                         Enabled
        +Create Admin User:                 yes
        +Admin user to create:              admin@colegiocristorey.edu.ni
******* +Admin Password                     UNSET
        +Enable automated spam training:    yes
        +Spam training user:                spam.yohruh__@colegiocristorey.edu.ni
        +Non-spam(Ham) training user:       ham._jejtv9Opt@colegiocristorey.edu.ni
        +Global Documents Account:          wiki@colegiocristorey.edu.ni
        +SMTP host:                         server.colegiocristorey.edu.ni
        +Web server HTTP port:              80
        +Web server HTTPS port:             443
        +Web server mode:                   http
        +IMAP server port:                  143
        +IMAP server SSL port:              993
        +POP server port:                   110
        +POP server SSL port:               995
        +Use spell check server:            yes
        +Spell server URL:                  http://server.colegiocristorey.edu.ni:7780/aspell.php
        +Configure for use with mail proxy: FALSE
        +Configure for use with web proxy:  FALSE
        +Enable version update checks:      TRUE
        +Enable version update notifications: TRUE
        +Version update notification email: admin@colegiocristorey.edu.ni
        +Version update source email:       admin@colegiocristorey.edu.ni

   4) zimbra-mta:                           Enabled
   5) zimbra-snmp:                          Enabled
   6) zimbra-logger:                        Enabled
   7) zimbra-spell:                         Enabled
   8) Default Class of Service Configuration:
   r) Start servers after configuration     yes
   s) Save config to file
   x) Expand menu
   q) Quit

Address unconfigured (**) items  (? - help)
```

Fig. 42. Menú principal.

Dentro de `Zimbra-store` existen varias opciones, entre las cuales se permite cambiar la contraseña del administrador (Admin), a la vez se cambia el puerto HTTP de 80 a 8080 para evitar conflictos futuros con el servidor Web. En la siguiente figura se muestra que las opciones son 4 para cambiar password y 10 para cambiar el puerto.

```
Store configuration

   1) Status:                                  Enabled
   2) Create Admin User:                       yes
   3) Admin user to create:                    admin@colegiocristorey.edu.ni
   4) Admin Password                           set
   5) Enable automated spam training:          yes
   6) Spam training user:                      spam.yohruh__@colegiocristorey.edu.ni
   7) Non-spam(Ham) training user:             ham._jejtv9Opt@colegiocristorey.edu.ni
   8) Global Documents Account:                wiki@colegiocristorey.edu.ni
   9) SMTP host:                               server.colegiocristorey.edu.ni
  10) Web server HTTP port:                    8080
  11) Web server HTTPS port:                   443
  12) Web server mode:                         http
  13) IMAP server port:                        143
  14) IMAP server SSL port:                    993
  15) POP server port:                         110
  16) POP server SSL port:                     995
  17) Use spell check server:                  yes
  18) Spell server URL:                        http:// server.colegiocristorey.edu.ni:7780/aspell.php
  19) Configure for use with mail proxy:       FALSE
  20) Configure for use with web proxy:        FALSE
  21) Enable version update checks:            TRUE
  22) Enable version update notifications:     TRUE
  23) Version update notification email:       admin@colegiocristorey.edu.ni
  24) Version update source email:             admin@colegiocristorey.edu.ni

Select, or 'r' for previous menu [r] r
```

Fig. 43. Submenú.

El sistema indica que para regresar al menú principal se debe tecla "`r`", luego con la tecla "`a`" se aplican todos los cambios. Cuando lo solicite el sistema, con la tecla "`y`" se permite guardar la configuración, finalizando la instalación de Zimbra.

Al finalizar la instalación se debe registrar como usuario Zimbra para ver si los servicios están corriendo debidamente, en la terminal se ejecuta: `su –zimbra`.

Con el comando `zmcontrol status` se pueden ver si los servicios corren correctamente (ver fig.44).

Fig. 44. Servicios de Zimbra corriendo correctamente.

Para entrar a la interfaz gráfica de ZIMBRA se escoge el navegador y se escribe la ruta de administrador para entrar como administrador:

https://mail.colegiocristorey.edu.ni:7071/zimbraAdmin

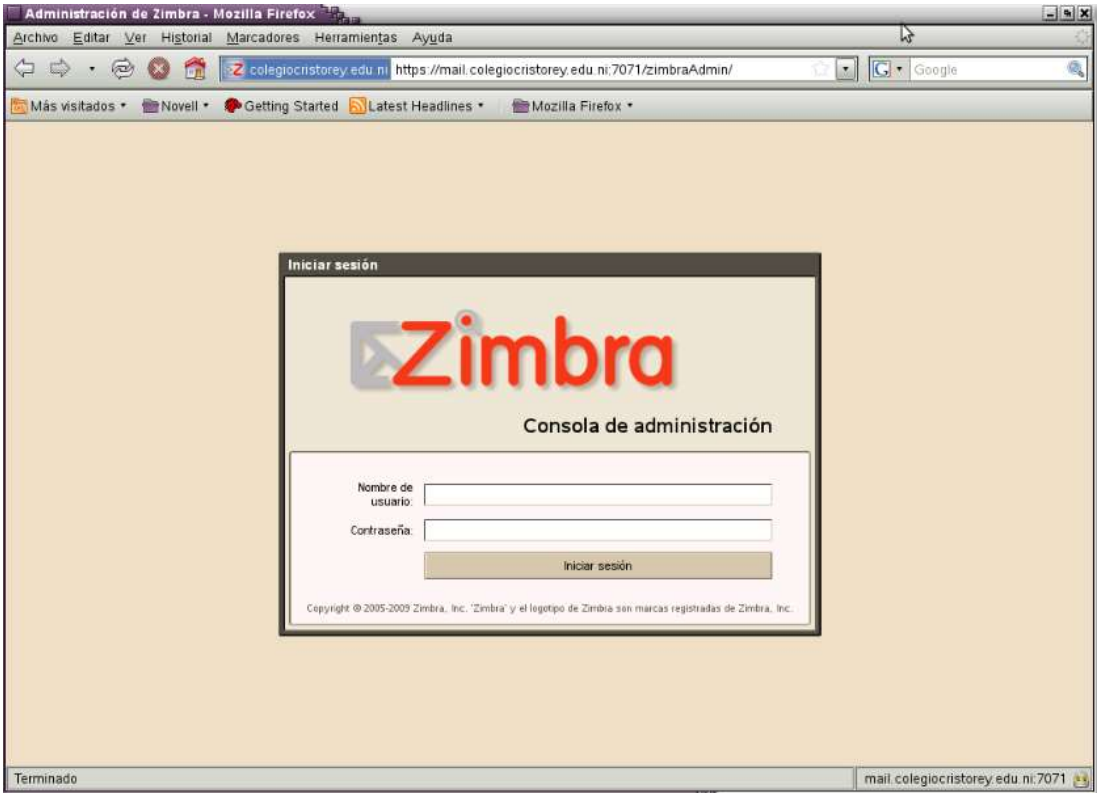


Fig. 45. Interfaz gráfica de inicio.

6.3.1.6. Servidor Elastix.

Para la instalación de Elastix es necesario tener un computador dedicado exclusivamente para estos fines. La descarga de Elastix se distribuye como un archivo de imagen tipo ISO y puede realizarse desde el sitio web www.elastix.org, la versión con la que se trabajó fue la 2.3.

Luego de descargar la imagen que se utilizó, se utilizó el software “iso2usb-v0.7” que permitió grabar la imagen ISO en una memoria de almacenamiento externo.

Una vez grabada la imagen en el dispositivo de almacenamiento, se procedió a la instalación física de Elastix, para esto nos aseguramos que el ordenador arrancara desde “USB Storage”. Lo primero que se muestra en la pantalla es el logo de Elastix con diferentes opciones para seleccionar, esta vez solo le daremos “ENTER”.

Fig. 46. Interfaz de inicio de instalación de Elastix.

Luego de esto, el sistema irá cargando una serie de datos y parámetros hasta que llega a una pantalla donde nos pide seleccionar el lenguaje de nuestra instalación a como se muestra en la siguiente figura.

Fig. 47. Selección del Idioma.

El siguiente paso es seleccionar el tipo de partición del disco duro y como se desea distribuir dichas particiones. Lo recomendable es dejar que el sistema cree sus particiones automáticamente.

Fig. 48. Selección del Disco Duro y tipo de particionamiento.

Luego el programa instalador nos consulta con un cuadro de aviso si se borra toda la información de todas las particiones, a lo que seleccionamos “Si”.

Fig. 49. Aviso de Confirmación de borrar particiones de disco duro.

Continuando con la instalación Elastix consulta si se desea configurar los parámetros de direccionamiento IP en las tarjetas de red con las que cuenta el servidor y seleccionamos “Si”.

Fig. 50. Configuración de Red.

Para cada tarjeta de red que se tenga instalada, Elastix preguntará si quiere que su tarjeta inicie al arrancar el sistema y que tipo de soporte IP se va a habilitar en ella. Para nuestro servidor se habilitaron las casillas “Activar al inicio y Activar soporte IPv4” y luego seleccionamos “Aceptar”.

Fig. 51. Configuración de red para cada interfaz.

Luego aparece un cuadro donde solicita que se asigne una contraseña al usuario root, se especifica la contraseña que será usada por el usuario con privilegios de administrador de Elastix.

Fig. 52. Contraseña root.

Enseguida inicia el proceso de formateo de las particiones ya creadas y los sistemas de archivos. Adicionalmente se copian todos los archivos necesarios para ejecutar Elastix correctamente.

Fig. 53. Particionamiento y copiado en el Disco Duro.

Una vez finalizado el proceso de particionamiento y copiado de archivos del sistema el servidor se reinicia automáticamente.

Fig. 54. Inicialización de Elastix.

Al finalizar el arranque de Elastix, se despliega una ventana de la consola de la PBX que permite acceder al sistema ingresando la contraseña definida anteriormente.

Fig. 55. Login Elastix.

Elastix resalta su grandeza por su interfaz Web, todas las configuraciones necesarias para la red pueden ser realizadas en un entorno gráfico. Para ingresar a la interfaz Web se digita la dirección IP del servidor en el cualquier navegador que se esté utilizando, inmediatamente se emite una advertencia de desconocimiento del certificado de seguridad ya que Elastix se comunica por una capa de conexión segura (SSL, Secure Sockets Layer), omitimos la advertencia y cliqueamos “Vaya a este sitio web (no recomendado)”.

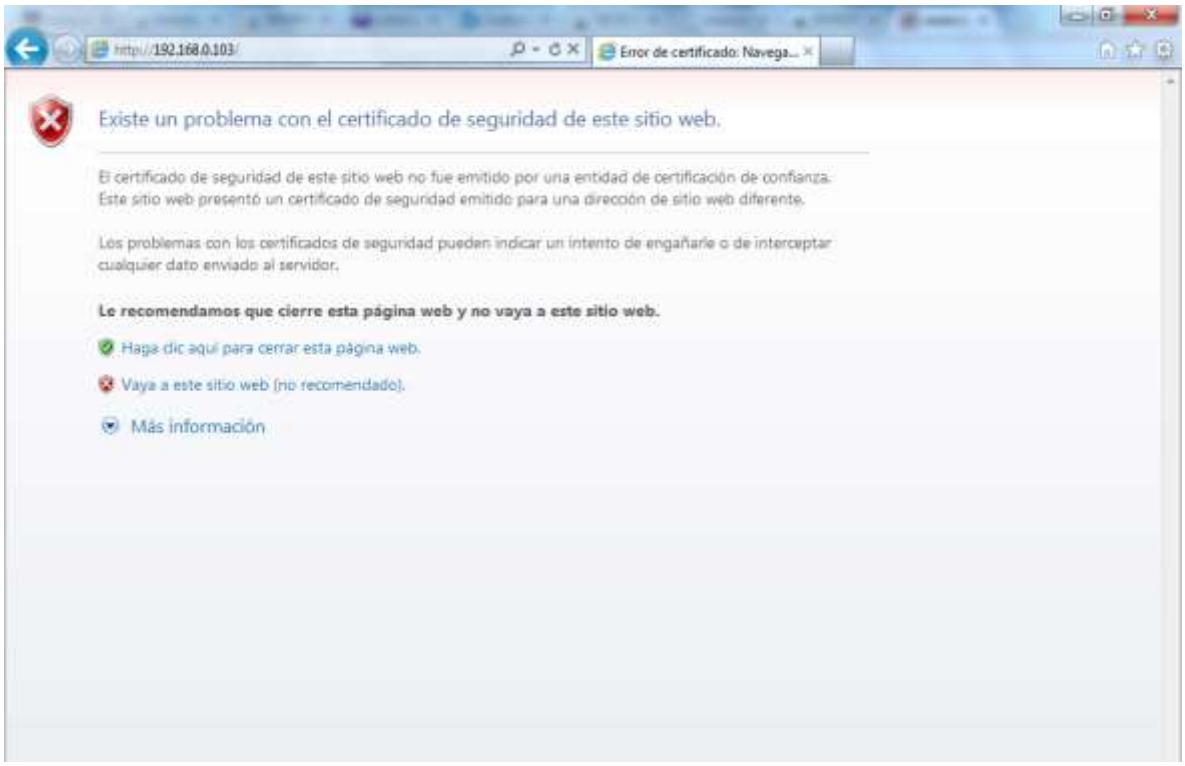


Fig. 56. Certificado de Seguridad.

Para poder acceder a la página de inicio de Elastix, se debe ingresar con el usuario y password correspondiente.

Fig. 57. Interfaz Web Elastix.

- **Creación de troncales.**

Las troncales (Trunks) son el medio que permiten comunicar a la PBX-IP Elastix con el mundo exterior o con la red telefónica pública conmutada (PSTN, Public Switched Telephone Network), son los canales de comunicación de entrada y salida de llamadas, también permiten la comunicación hacia otras PBX, tradicionales o IP.

En las troncales son por donde vamos a sacar y recibir llamadas e interactuar con la Red PSTN. Podemos tener varios troncales de la misma o de diferentes tecnologías.

Para configurar la troncal se debe ir a la pestaña PBX > troncal y se selecciona Agregar troncal Dahdi**.** Se deben llenar los campos: nombre del troncal y el patrón de números de marcado (Ver figura 58).

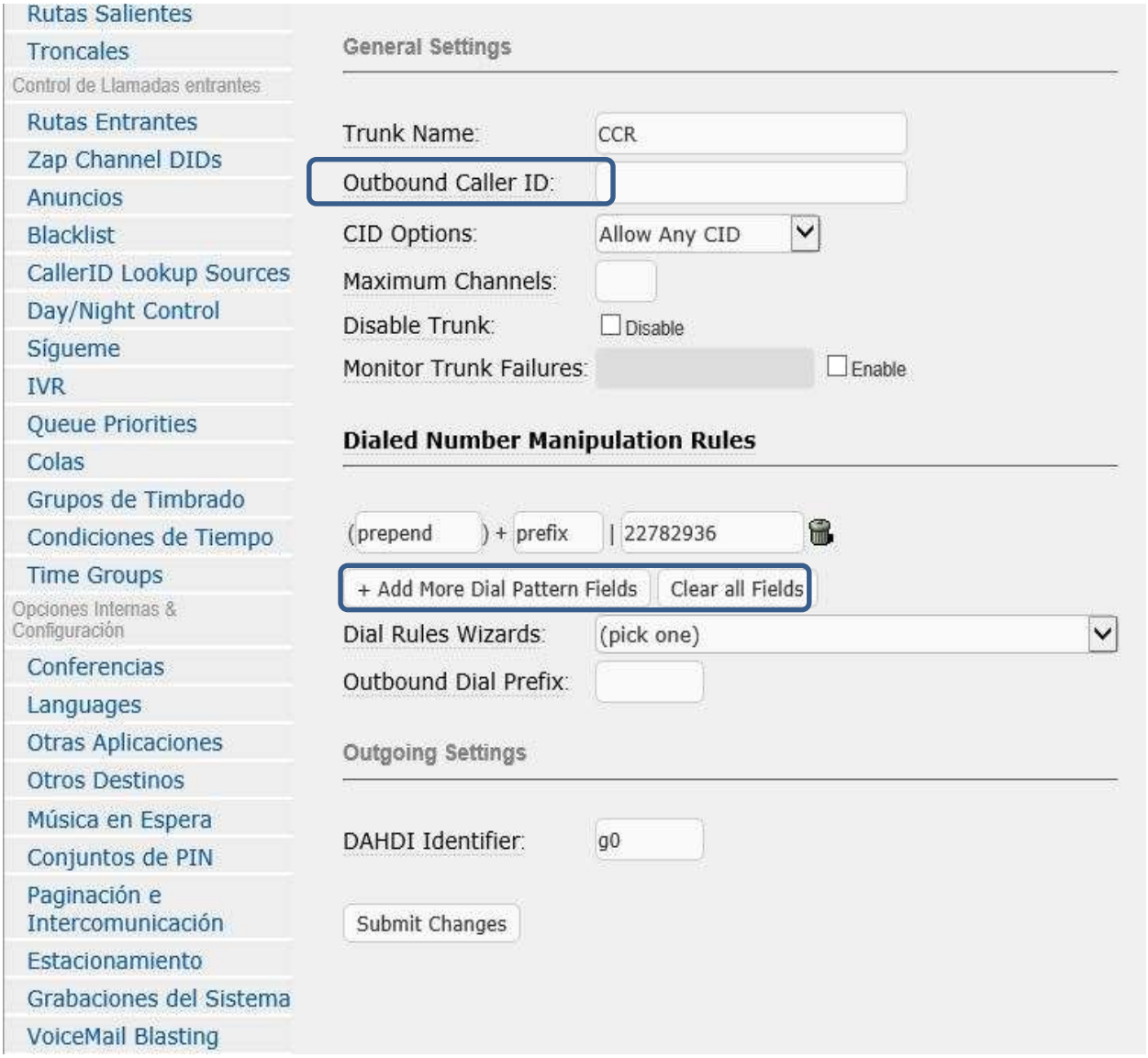


Fig. 58. Creación de troncales.

- **Creación y configuración de extensiones.**

Para crear las extensiones de las áreas administrativas del centro, se hizo uso del Protocolo de Inicio de Sesiones (SIP, Session Initiation Protocol) que es uno de los más difundidos y utilizados en los sistemas de telefonía IP.

Dentro de nuestra interfaz Web ingresamos a "PBX>PBX Configuration>Extensiones", una vez que estemos dentro de la ventana seleccionamos "Device">Generic SIP Device" y cliqueamos "Submit".

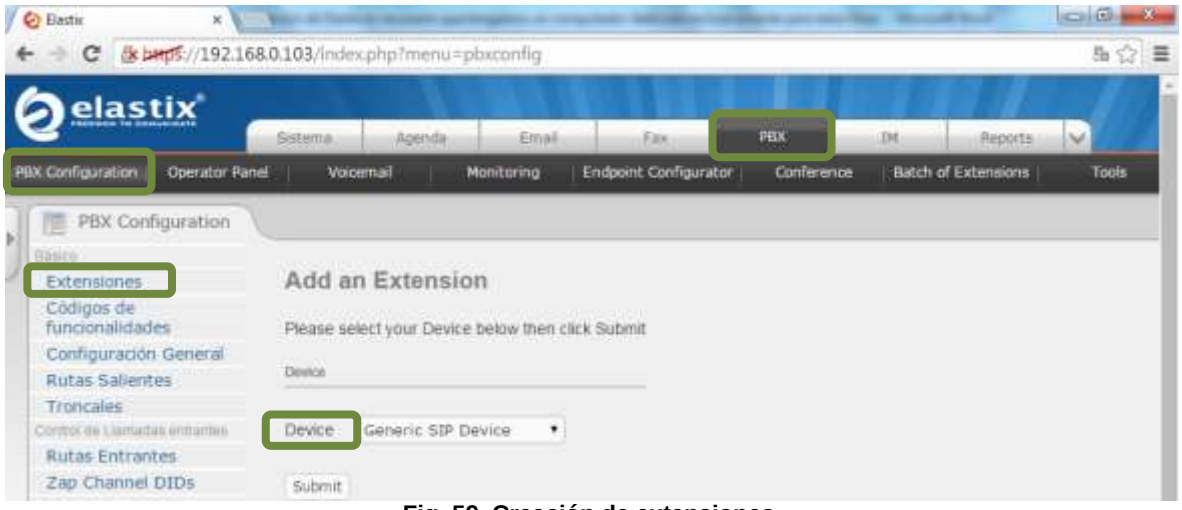


Fig. 59. Creación de extensiones.

Por cada extensión se debe llenar una serie de campos, de los cuales tres son de vital importancia para que la extensión creada funcione correctamente, los campos a completar son los siguientes:

- **UserExtensions:** es el número de la extensión que vamos a asignar.
- **DisplayName:** es el nombre del usuario con que se identificará la extensión al llamar a otra extensión.
- **Secret:** es el campo donde se asigna una contraseña a cada extensión creada.

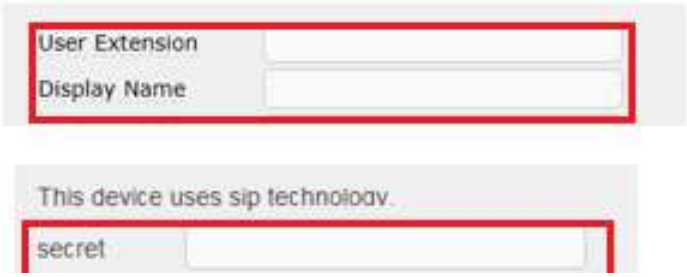


Fig. 60. Campos para agregar extensión

La siguiente figura muestra las 5 extensiones que fueron creadas para la comunicación entre las áreas administrativas del centro.

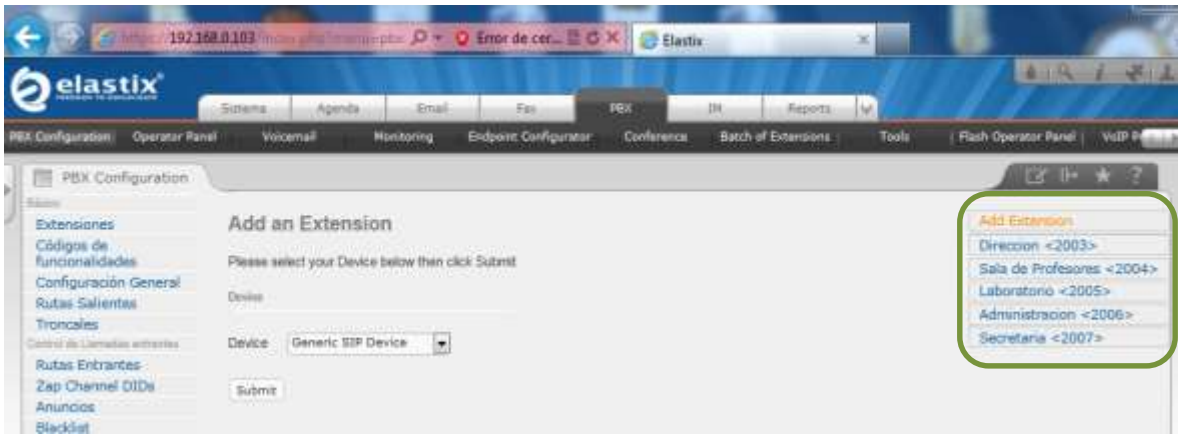


Fig. 61. Extensiones telefónicas del centro.

6.4. Pruebas.

Para realizar la entrega del proyecto fué necesario realizar pruebas para validar el funcionamiento desde el punto de vista técnico y operativo. Las prueba consistieron en verificar el buen funcionamiento de los equipos en un periodo de una semana, con todo el personal haciendo uso de la red, posteriormente fueron aplicadas las entrevistas a directivos y profesores y encuestas a estudiantes para conocer el grado de satisfacción de las pruebas realizadas.

6.4.1. Validación del funcionamiento de los servicios.

Con las pruebas que se realizaron, se logró comprobar que el sitio web permite a los usuarios hacer uso de las herramientas que esta posee.

En cuanto al servicio web, uno de los servicios más vistosos dentro de él, es que ofrece a los docentes y alumnado en general una plataforma de comunicación virtual (blog) donde el docente previamente registrado por el administrado podrá publicar tareas o temas de estudio que estime conveniente el mismo a su vez podrá eliminar, actualizar o editar publicaciones anteriores hechas por ellos.

Fig. 62. Acceso a Blog dentro del sitio web.

Fig. 63. Menú de ingreso a docentes para publicación de información.

Dentro del mismo blog, los usuarios registrados previamente por el administrador pueden comentar las publicaciones hechas por los docentes y de esta manera se puede entablar una comunicación directa en caso de dudas o preguntas, cabe señalar que los comentarios no deseados o con vocabulario inadecuados no podrán ser publicados por las bases de seguridad del sitio. Para poder comentar los

artículos basta con ingresar un correo electrónico valido un nombre de usuario cualquiera y el detalle de su comentario.

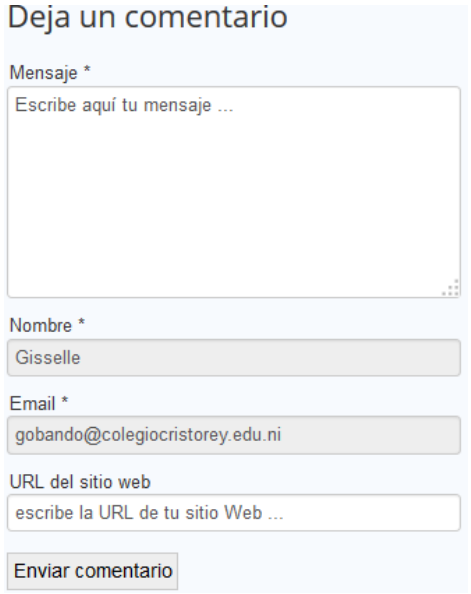


Fig. 64. Comentarios de usuarios registrados.

Dentro del sitio también se cuenta con un espacio llamado Biblioteca Virtual, este servicio muestra una serie de enlaces de categorías que se redireccionan a carpetas guardadas en google drive servicio de alojamiento de archivos en la nube. Estos recursos pueden ser descargados en algunos casos o solo pueden ser visualizados por el usuario en dependencia de las opciones que quiera incluir el administrador del sitio.

Fig. 65. Biblioteca Virtual.

El submenú reglamento institucional muestra una atractiva herramienta donde se puede visualizar las normas y leyes que se deben cumplir internamente en el centro educativo. Para la elaboración de este se utilizó un efecto de libro virtual llamado flippingBook, herramienta interactiva que hace que la lectura no sea aburrida y tediosa. También es posible descargar la información del libro en formato PDF.

Fig. 66. Reglamento Institucional.

Para lograr unificar el servicio web con el servicio de correo se agregó dentro de la página un botón que permitiera a los docentes del centro con solo hacer click en el botón Correo CCR dirigirse hacia su correo electrónico Zimbra.

Fig. 67. Interfaz de correo electrónico Zimbra.

Para agregar nuevas cuentas en Zimbra, se deberá hacer con el usuario de administrador, detallando el nombre de dominio configurado previamente. Los campos con un asterisco son de carácter obligatorio.

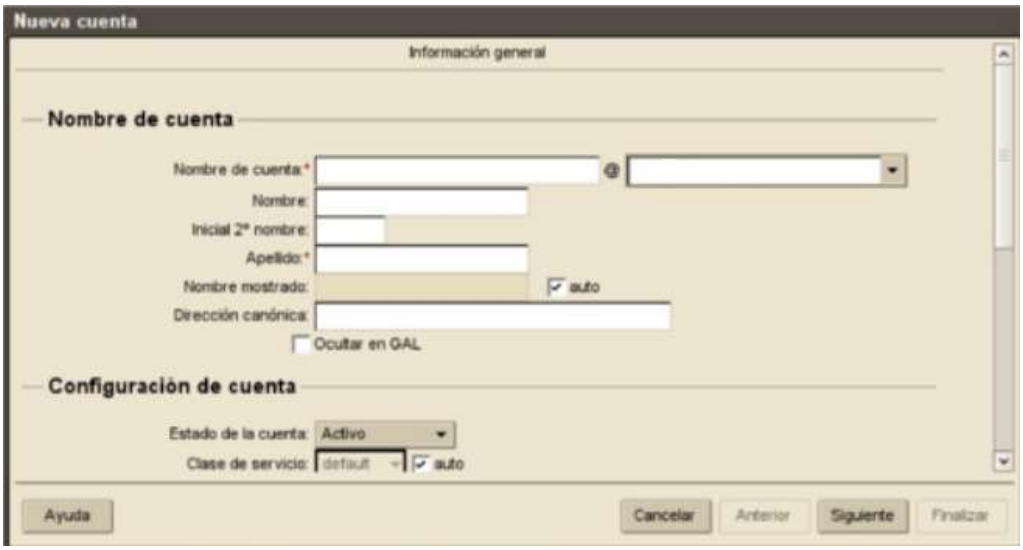


Fig. 68. Crear nueva cuenta.

Una vez se tenga creada la cuenta existen diferentes opciones a las que Zimbra tiene acceso, dentro de ellas está la mensajería instantánea. Esta despliega un cuadro en la parte inferior en el cual se puede mantener una conversación con otro usuario Zimbra.

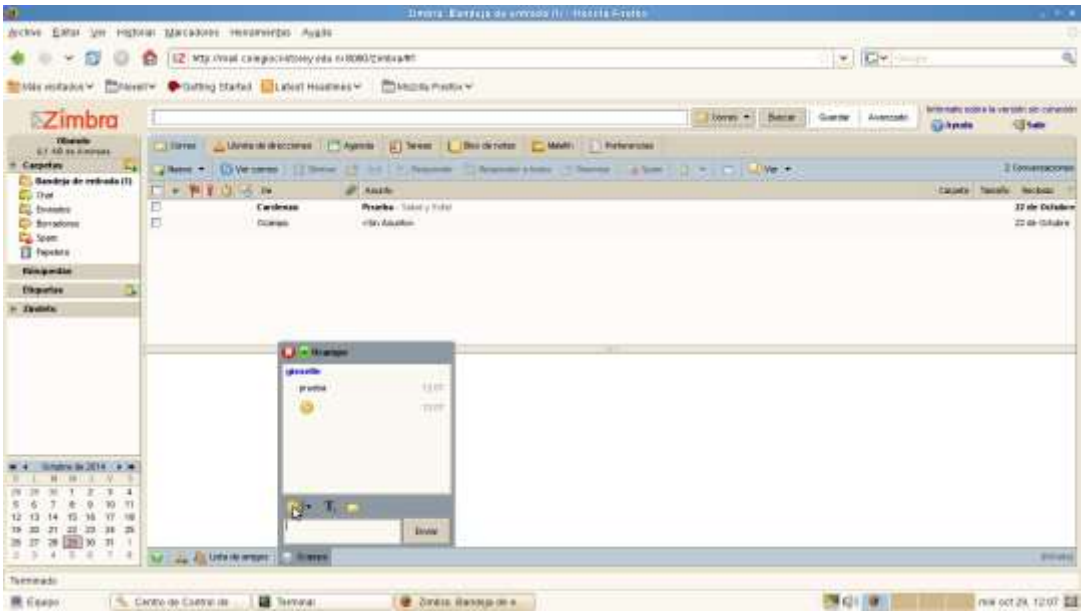


Fig. 69. Mensajería instantánea.

Para la implementación del servicio VoIP, existen diversas formar para lograr la integración del tráfico telefónico a la red de datos. Se puede hacer uso de una tarjeta PCI adaptable a Elastix, un adaptador telefónico análogo (ATA) que permite la integración de teléfonos análogos a la topología de red de datos o bien se pueden utilizar teléfonos IP que disponen de una dirección IP a la que se puede acceder y mediante la que se puede configurar. Existe también la opción de Softphones la cual fue utilizada para hacer pruebas que validan el buen funcionamiento del servidor.

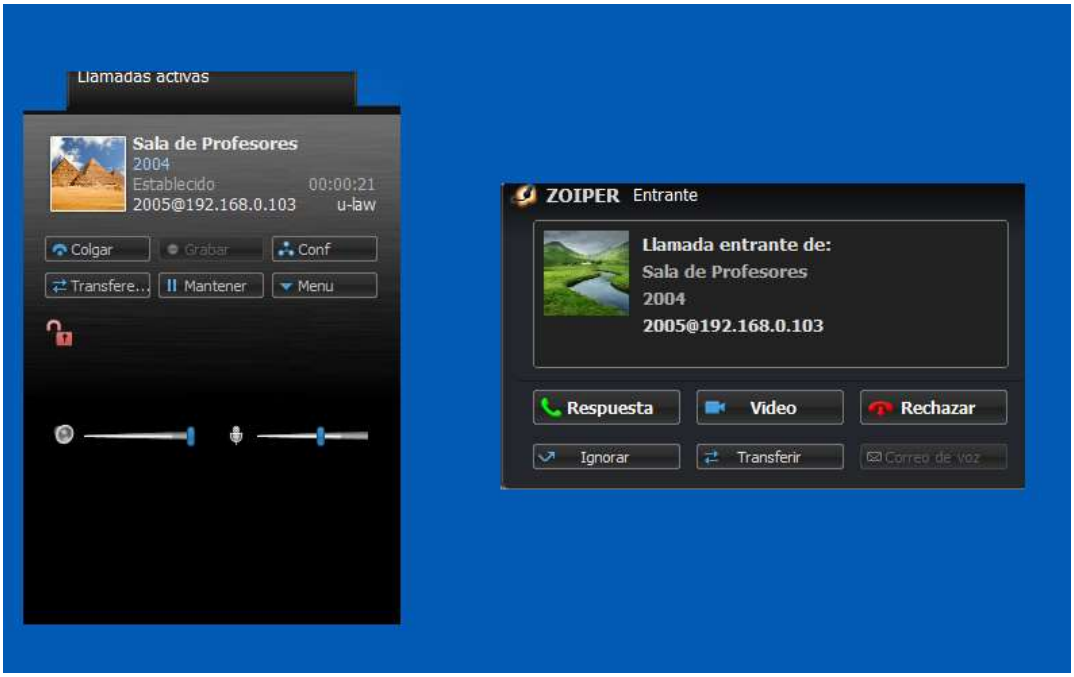


Fig. 70. Prueba de softphone Elastix.

Para el caso de los teléfonos IP, se debe acceder a una herramienta web mediante la dirección IP del teléfono donde se deben llenar los campos correspondientes a la autenticación del teléfono en el servidor y la asociación de la extensión previamente creada. (Ver figura 71).

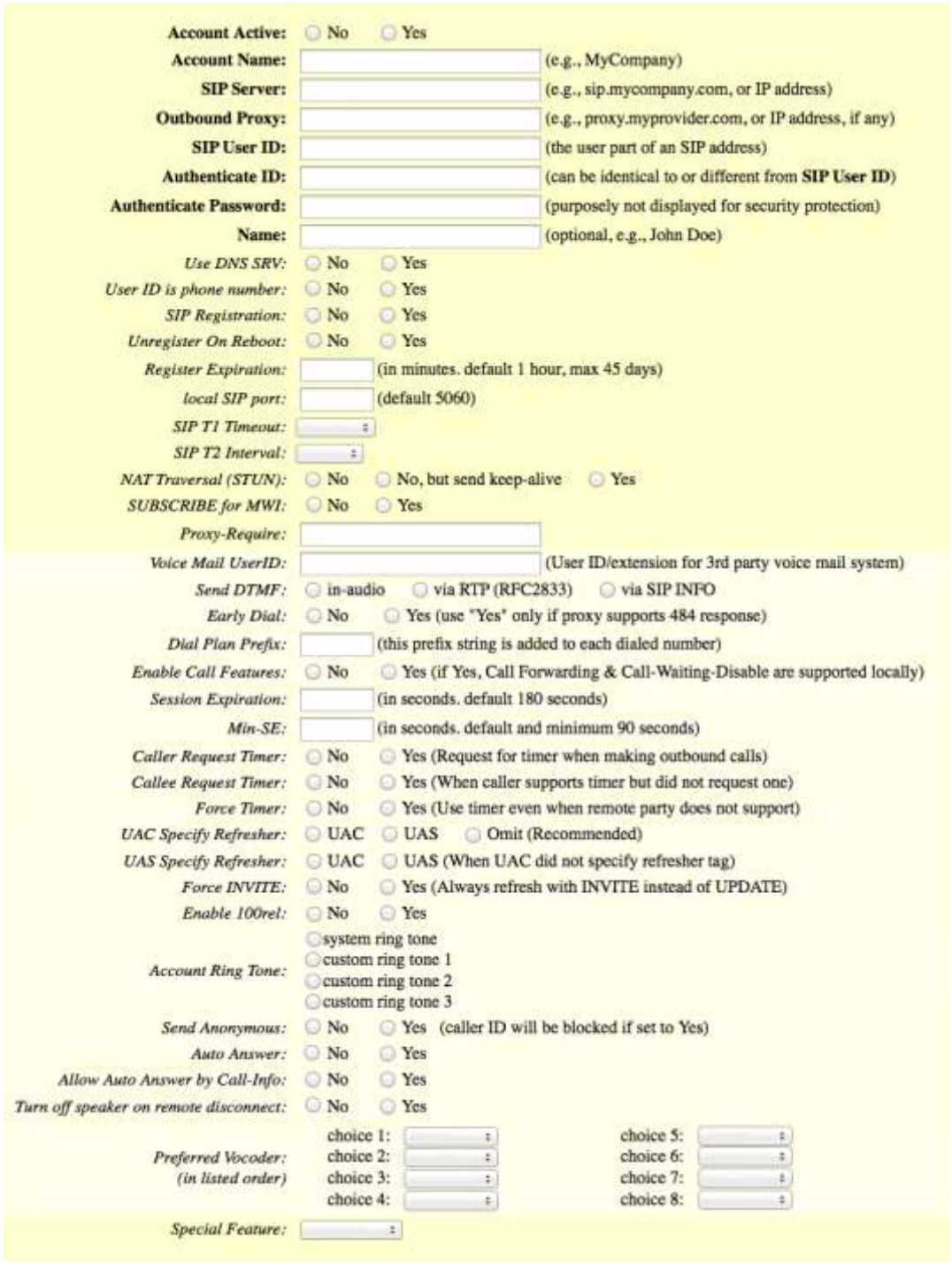
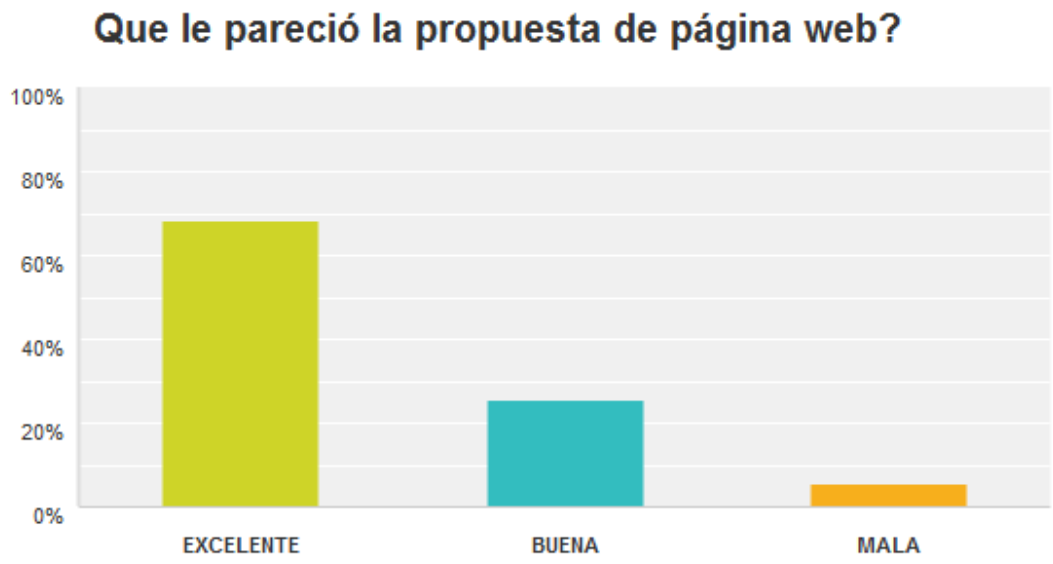


Fig. 71. Interfaz de configuración de teléfonos IP.

6.4.2. Resultados de entrevistas y encuestas sobre el funcionamiento de los servicios.

Luego de haber aplicado los instrumento de recolección de información sobre el correcto funcionamiento de los servicios configurados que son demostrables (página web y correo) se presenta un análisis de los resultados obtenidos.

En la Figura 72 se observa que el 68.57% de los estudiantes y docentes encuestados consideran que la propuesta de página web es excelente, seguido por un 25.71% la apreció buena y un 5.71% como mala. Por los resultados obtenidos podría decirse que más del 60% de los encuestados está satisfecho con la propuesta de página web presentada.



Opciones de respuesta	Respuestas	
EXCELENTE	68,57%	24
BUENA	25,71%	9
MALA	5,71%	2
Total		35

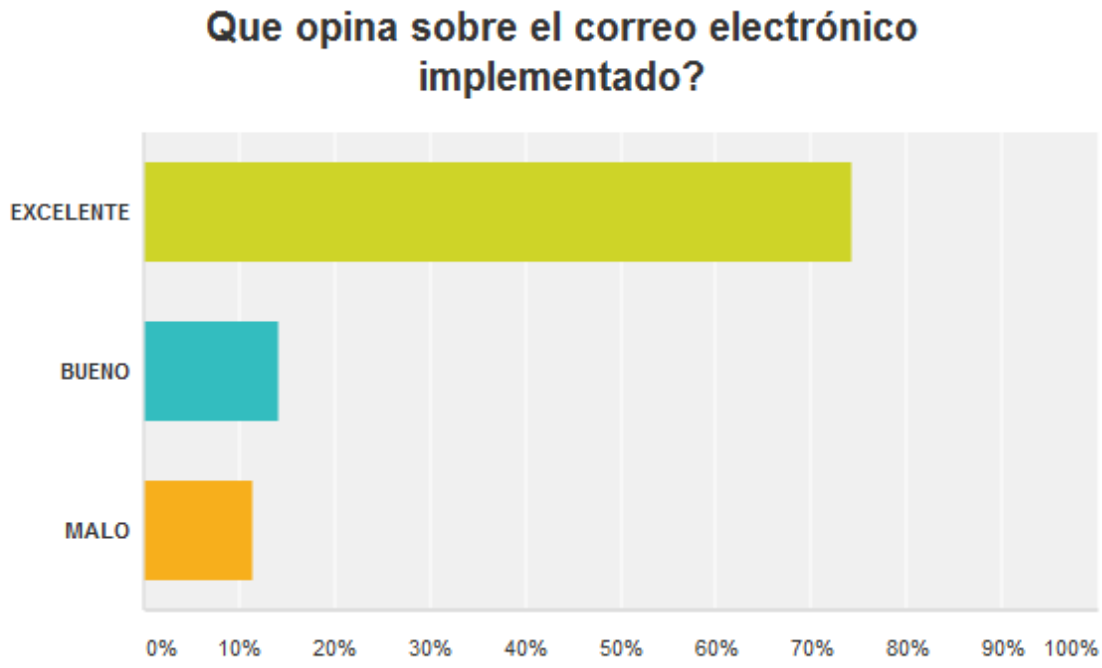
Fig. 72. Opinión sobre la funcionalidad de la página web.

Al momento de solicitar a los encuestados que indicaran cuales de los temas dentro de la página web encontraron más interesantes estos manifestaron lo mostrado en la figura 73. Un 28.57% estimó que el blog interactivo era el aspecto con mayor relevancia dentro del sitio, seguido por un 22.86% que indicó que el acceso a descargas de contenido académico era el aspecto más significativo, un 20% dijo que la publicación de información, la integración con redes sociales y calendario de actividades obtuvieron un 14.29% cada uno.

Opciones de respuesta	Respuestas	
Blog interactivo	28,57%	10
Publicación de información	20,00%	7
Integración con redes sociales	14,29%	5
Calendario de actividades	14,29%	5
Descarga de contenido académico	22,86%	8
Total de encuestados: 35		

Fig. 73. Aspectos más interesantes dentro de la página web.

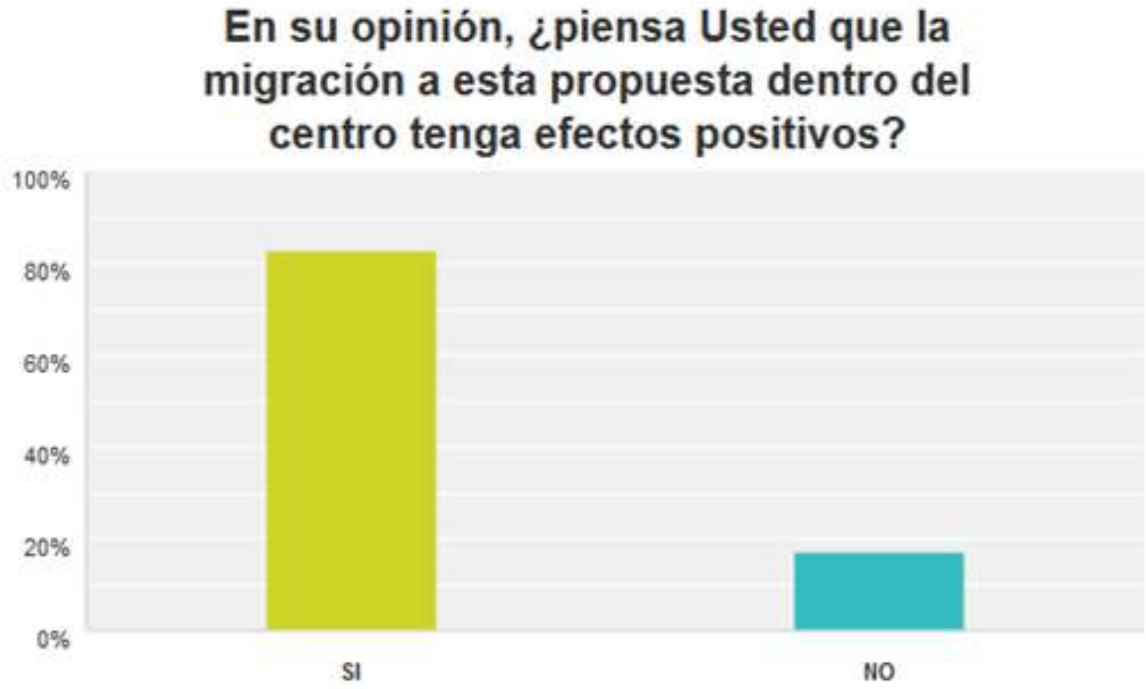
La figura 74 corresponde al resultado de la valoración otorgada al servicio de correo electrónico. Un 74.29% de los encuestados valoraron el servicio como excelente, seguido por un 14.29% que lo consideró bueno y un 11.43% que indicó era malo.



Opciones de respuesta	Respuestas	
EXCELENTE	74,29%	26
BUENO	14,29%	5
MALO	11,43%	4
Total		35

Fig. 74. Opinión sobre servicio de correo electrónico.

Para conocer la opinión y percepción general que tuvieron de la propuesta de implementación del diseño, se consultó si creían que esta tendría beneficios y efectos positivos a lo que la mayoría, representada por un 82.86% respondió que sí y su complemento un 17.14% manifestó lo contrario (ver figura 75).



Opciones de respuesta	Respuestas	
SI	82,86%	29
NO	17,14%	6
Total de encuestados: 35		

Fig. 75. Opinión de efectos positivos con la migración a propuesta.

7. CONCLUSIONES.

Para este trabajo primeramente se realizó un análisis de la infraestructura del centro, y como resultado encontramos que las condiciones de infraestructura educativa y el acceso a los servicios básicos con que cuenta el centro son adecuados, sin embargo, se encontró que el centro no contaba con acceso a internet, ni correo electrónico corporativo, ni un sitio web donde alojar una página informativa sobre la actividad académica del colegio, tampoco existía una red inalámbrica que brindara servicios a los estudiantes para realizar sus investigaciones.

Producto de este hallazgo, se hizo una propuesta a la Administración General del Centro sobre el levantamiento de requerimientos técnicos de las condiciones actuales del Centro. Además, mediante encuestas se consultó a estudiantes y docentes sobre la implementación y configuración de un nodo de internet en el centro, a lo que el 49% de los estudiantes y docentes encuestados consideraron una excelente idea, seguido por un 26% que manifestaron ser muy buena, un 20% la valoró como buena idea y apenas un 6% respondió como mala idea.

Una vez presentada la propuesta al centro, se procedió a realizar el diseño de la red a partir de las condiciones encontradas y algunas pequeñas modificaciones en la infraestructura.

La instalación y configuración de los servicios fue realizada bajo ambiente Linux, configurándose los siguientes servidores:

- Servidor de Correo electrónico bajo la suite de colaboración Zimbra (Zimbra Collaboration Suite o ZCS).
- Servidor de alojamiento de sitio web que se identifica como www.colegiocristorey.edu.ni.
- Servidor de nombre de dominio DNS para la resolución de zonas, y squid-proxy el cual permite el control de acceso a sitios web no deseados, control de descarga de contenido, control de horarios de acceso a internet, administración del ancho de banda y de la red de área local (LAN).

- Servidor Elastix para central telefónica virtual y servicio DHCP que mejorará la comunicación interna y asigna dinámicamente direcciones IPs.

Posterior a la configuración, se procedió a poner en funcionamiento cada uno de los servicios en la red del centro, tanto cableada como inalámbrica haciendo uso para este último, la tecnología WiFi.

Se realizaron pruebas de funcionamiento de cada uno de los servicios del nodo de la institución, los resultados obtenidos de la puesta en marcha fueron satisfactorios, tanto para los ejecutores como para la administración del centro.

Podemos concluir expresando que la adaptación de esta propuesta dentro del centro tendrá un impacto positivo y traerá beneficios al personal administrativo y docentes del centro. Con la implementación de estos servidores el centro se verá beneficiado con la incorporación de nuevas aplicaciones de comunicación en grupo. Así mismo se les facilitará una herramienta a las alumnas y padres de familia para mejorar el proceso de enseñanza-aprendizaje.

8. RECOMENDACIONES.

1. Se recomienda utilizar baterías de alta duración UPS (Sistema de alimentación ininterrumpida, la más recomendable es la Smart-UPS de APC que ofrece protección de energía funcional para servidores, y redes de voz y datos. La serie Smart-UPS de APC protege los datos mediante el suministro de energía confiable, es la opción ideal para proteger servidores, minicomputadoras, hubs y switches de redes.

2. A medida que la cantidad de datos van aumentando es importante ampliar la capacidad de almacenamiento de los servidores, sobre todo del servidor web y el servidor de correo.

3. Es importante contar con un antivirus y un antispam adicional que proteja la red ya que el antivirus amavis y el antispam spamassassin son exclusivamente para correos entrantes en Zimbra.

4. Si en algún momento la cantidad de usuarios excede la capacidad del punto de acceso Wifi, hay baja potencia de la señal y en el peor de los casos no haya cobertura en muchos puntos es importante considerar situar otro punto de acceso que de cobertura a la zona deseada o bien utilizar un repetidor.

5. Realizar mantenimiento preventivo y correctivo, cada 3 meses a los equipos de cómputo, para garantizar un buen funcionamiento y aumentar la vida útil de los mismos.

6. Realizar copia de seguridad de los archivos del sitio web y demás aplicaciones necesarias para tener un respaldo ante posibles daños que sufra el equipo donde están alojadas.

9. BIBLIOGRAFÍA.

- Stallings W. (2004). Comunicaciones y redes de computadoras (7ma ed). Madrid: Pearson Educación, S.A.

- Barceló Ordinas J.M, Íñigo Griera J, Escalé R.M, Peig Olivé E, Perramon Tornil X. (2004). Redes de computadora (1era ed.). Universidad de Cataluña, Barcelona.

- Muñoz, A. (2010). Elastix a Ritmo de Merengue. Republica Dominicana.

- Forouzan B.A (2009). Transmisión de datos y redes de computadoras (2da ed.).

- Kurose J.F. Redes de computadoras un enfoque descendente basado en Internet. Pearson

- Kevin R. Fall, W. Richard Stevens (1993) TCP/IP Illustrated, Vol 1.

- James F. Kurose , Keith W. Ross (2010) Redes de computadoras (5ta ed.).

- Alfio Muñoz (2009). Elastix a ritmo de merengue.

- S. Bibillier (2009). Linux, Administración del Sistema y explotación de los servicios de red (2da ed.). Barcelona: Ediciones ENI.

9.1. WEBGRAFÍA.

- *http://www.zimbra.com/buzz/index.es.html_Recuperado el 20 de Agosto de 2014.*

- *http://www.elastix.org/index.php/es/_Recuperado el 3 de Septiembre de 2014.*

ANEXOS

ANEXO 1: GLOSARIO.

ACK: acknowledgement, en español acuse de recibo o asentimiento. Es un mensaje que el destino de la comunicación envía al origen de ésta para confirmar la recepción de un mensaje, también puede informar si se ha recibido de forma íntegra y sin cambios.

ACL: access control list, en español lista de control de acceso. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, permite controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

ASP: es una tecnología desarrollada por Microsoft para la creación de páginas web dinámicas.

BIND: Berkeley Internet Name Domain, es el servidor DNS más comúnmente usado en Internet, especialmente en sistemas Unix.

Blog: es un sitio web en el que uno o varios autores publican cronológicamente textos o artículos, apareciendo primero el más reciente, y donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente.

BOOTP: Boot strap Protocol. Es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente. Normalmente se realiza en el proceso de arranque de los ordenadores o del sistema operativo. Este protocolo permite a los ordenadores sin disco obtener una dirección IP antes de cargar un sistema operativo avanzado.

Demonio: daemon (de sus siglas en inglés Disk And Execution Monitor), es un tipo especial de proceso informático que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario (es un proceso no interactivo).

Flash: es una tecnología para crear animaciones gráficas vectoriales independientes del navegador y que necesitan poco ancho de banda para mostrarse en los sitios web.

FQDN: fully qualified Domain name es un nombre que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo.

Host: es un ordenador que funciona como el punto de inicio y final de las transferencias de datos.

HTML: Hyper Text Mark up Language, en español lenguaje de marcas de hipertexto, hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que sirve de referencia para la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código.

HTTP: Hypertext Transfer Protocol, en español protocolo de transferencia de hipertexto. Es el protocolo usado en cada transacción de la World Wide Web.

IMAP: Internet Message Access Protocol, en español Protocolo de acceso a mensajes de internet. Es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet

IP: Internet Protocol, en español Protocolo de Internet. Es un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI. Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo dentro de una red que utilice IP.

Java: es una tecnología que se usa para el desarrollo de aplicaciones que convierten a la Web en un elemento más interesante y útil.

Jetty: es un servidor HTTP 100% basado en Java y un contenedor de Servlets escrito en Java. Jetty se publica como un proyecto de software libre bajo la licencia Apache 2.0.

LAN: Local Area Network, en español Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada.

MAC: media access control, en español control de acceso al medio. Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.

MIME: Multipurpose Internet Mail Extensions Encoding, en español extensiones multipropósito de correo de Internet. Es un estándar utilizado en Internet para normalizar el intercambio de todo tipo de archivos (texto, audio, vídeo, etc) en la Red y para acabar con el problema de las transferencias de texto internacional por correo electrónico.

MySQL: es un sistema gestor y de administración de bases de datos.

MX: es aquel que define el nombre del servidor y su nivel de preferencia para recibir mensajes de correo electrónico, es decir, al momento de ser enviado un correo electrónico a nuestro buzón, el equipo emisor pregunta al servidor donde se registra nuestro dominio, quien es el encargado de recibir los correos. Una vez comprobado esto, el enlace se establece entre el servidor saliente y quien recibe el mensaje completándose la operación.

Open Source: 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; permita redistribuirlo, siempre y cuando sea de acuerdo con los términos de la licencia bajo la cual el Software original fué adquirido.

PBX: Private Branch Exchange, en español Central Secundaria Privada. Se encarga de establecer conexiones entre terminales de una misma empresa, o de hacer que se cursen llamadas al exterior. Hace que las extensiones tengan acceso desde el exterior, desde el interior, y ellas a su vez tengan acceso también a otras extensiones y a una línea externa.

PHP: Es un lenguaje de programación interpretado, está diseñado especialmente para desarrollo web y puede ser incrustado dentro de código HTML.

POP: Post Office Protocol, en español protocolo de oficina postal. Es un protocolo estándar de internet de la capa aplicación del modelo OSI. El protocolo POP es utilizado por programas de e-mail locales para recibir e-mails desde un servidor remoto a través de una conexión TCP/IP.

SMTP: Simple Mail Transfer Protocol, en español Protocolo para la transferencia simple de correo electrónico. Es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

SNMP: Simple Network Management Protocol, en español Protocolo Simple de Administración de Red. Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

SOAP: Simple Object Access Protocol. Es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.

TCP: Transmission Control Protocol, en español Protocolo de Control de Transmisión. Es uno de los protocolos fundamentales en Internet. Gracias a él las aplicaciones pueden comunicarse en forma segura e independientemente de las capas inferiores.

VoIP: (Voz sobre Protocolo de Internet) es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite la transmisión de la voz sobre el protocolo IP.

ANEXO 2: Instrumentos de recolección de información.

INSTRUMENTO 1

Estimados (as) docentes y alumnas favor tome unos minutos para responder la siguiente encuesta.

1. **¿Considera necesario el uso de internet dentro del centro?**

   SI ( )
   NO ( )

2. **¿Cómo valora la idea de incorporar el servicio de correo corporativo en el colegio?**

   MALA ( )
   BUENA ( )
   MUY BUENA ( )
   EXCELENTE ( )

3. **¿Qué tan importante es que el colegio cuente con una página web informativa?**

   EXTREMADAMENTE IMPORTANTE ( )
   MUY IMPORTANTE ( )
   LIGERAMENTE IMPORTANTE ( )
   NADA IMPORTANTE ( )

4. **¿Considera Usted que el uso de una página web dentro del centro beneficiaria al centro para dar a conocer la oferta y actividades académicas?**

   SI ( )
   NO ( )

5. **¿Cómo evaluaría la idea de implementar esta propuesta dentro del centro?**

MALA ( )
BUENA ( )
MUY BUENA ( )
EXCELENTE ( )

6. **¿Qué tan relevante considera que pueda ser la incorporación e implementación de nuevas tecnologías en el centro?**

EXTREMADAMENTE RELEVANTE ( )
MUY RELEVANTE ( )
LIGERAMENTE RELEVANTE ( )
NADA RELEVANTE ( )

INSTRUMENTO 2

Estimados (as) docentes y alumnas favor tome unos minutos para responder la siguiente encuesta.

1. **¿Qué opina sobre el servicio de correo electrónico implementado?**

MALO ( )
BUENO ( )
MUY BUENO ( )
EXCELENTE ( )

2. **¿Qué tan amigable le pareció el servicio de correo electrónico?**

NADA AMIGABLE ( )
MUY AMIGABLE ( )
EXTREMADAMENTE AMIGABLE ( )

3. **¿Qué le pareció la propuesta de página web?**

MALA ( )
BUENA ( )
MUY BUENA ( )
EXCELENTE ( )

4. **¿Qué aspectos dentro de la página web le resultaron más interesantes?**

Blog interactivo ( )
Publicación de información ( )
Integración con redes sociales ( )
Calendario de actividades ( )

5. **¿Considera Usted que la tecnología es un factor importante para el sector educativo?**

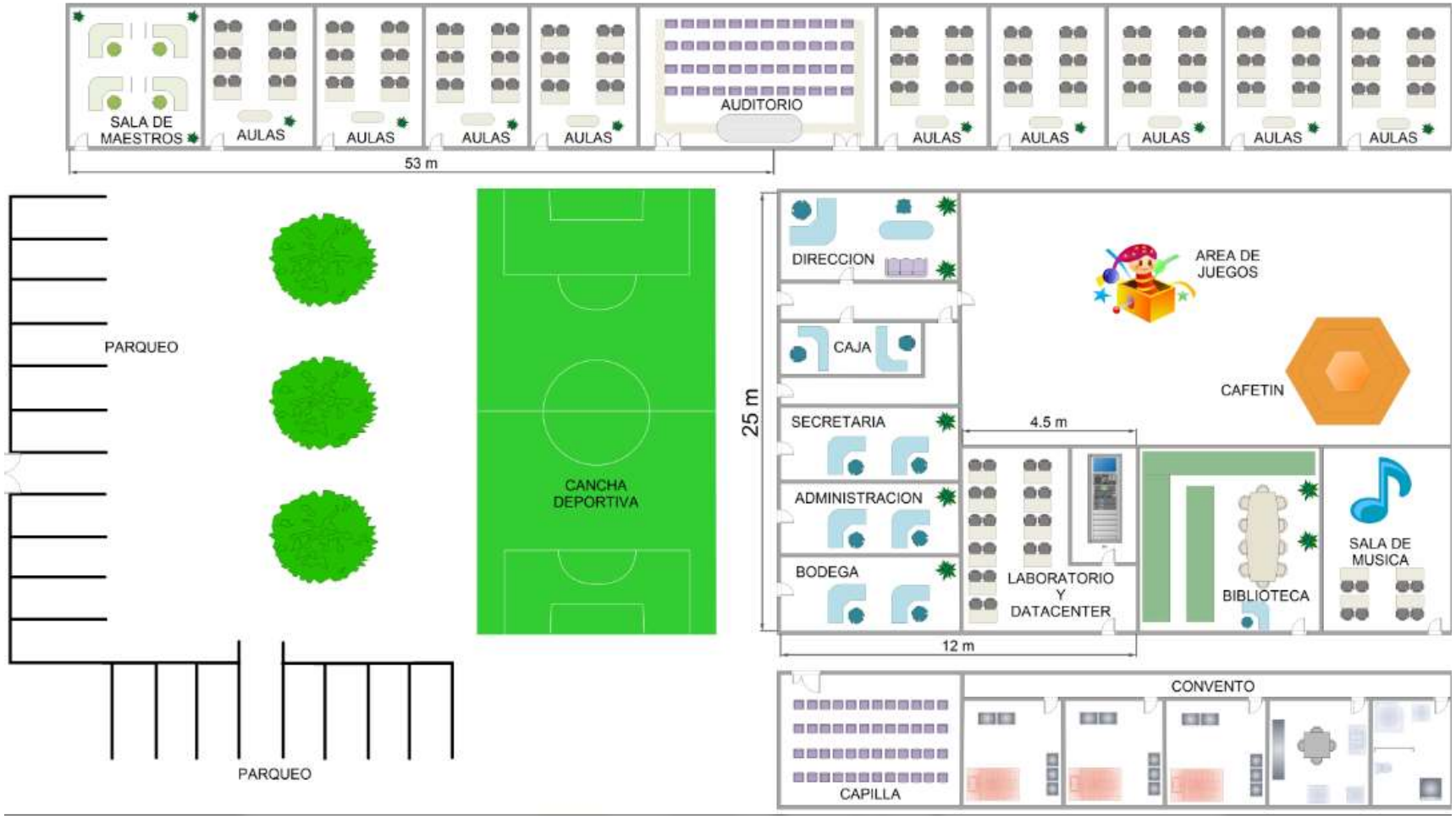
SI ( )
NO ( )

6. **En su opinión, ¿piensa Usted que la migración a esta propuesta dentro del centro tenga efectos positivos?**

SI ( )
NO ( )

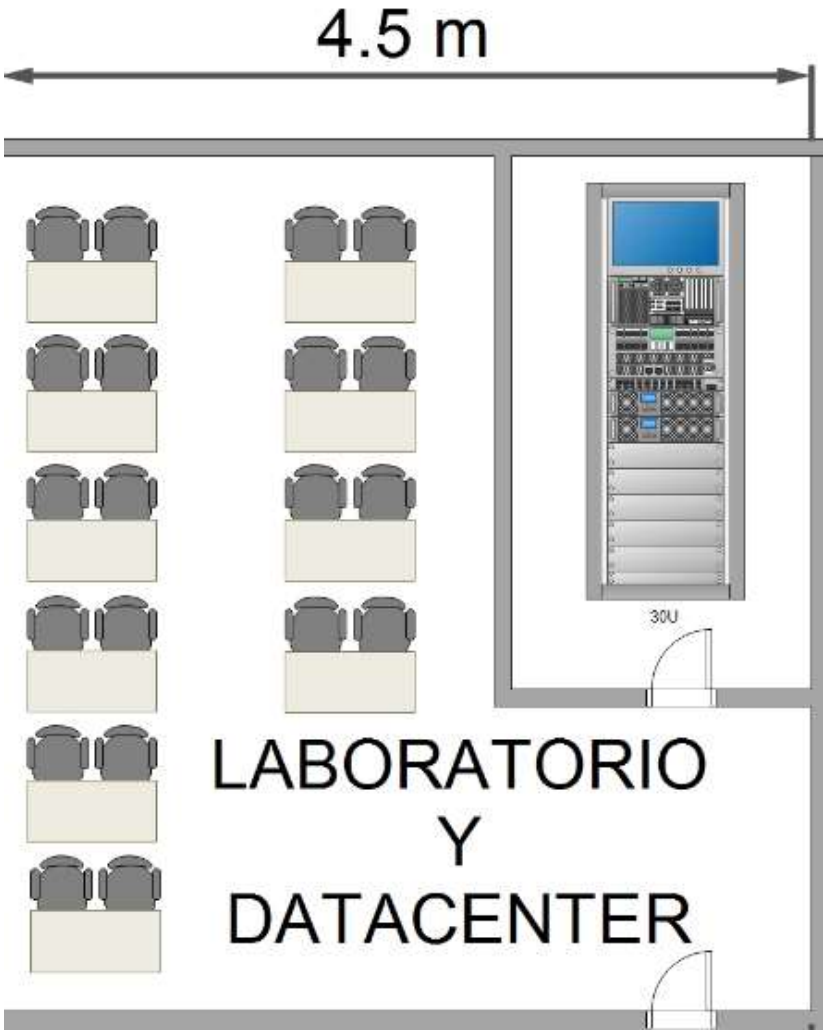
ANEXO 3

Diagrama de la infraestructura del Colegio Cristo Rey Managua.



ANEXO 4

Sitio propuesto para ubicación de los servidores.



ANEXO 5

COLEGIO CRISTO REY
Cristo vence, Cristo Reina, Cristo Impera

Managua, 11 de noviembre de 2014.

A quien concierna.

¡Que Cristo Rey del Universo, este en siempre en sus corazones!

Por medio de la presente y en representación del Colegio Cristo Rey Managua en calidad de Directora Administrativa hago constar; que el Estudio monográfico realizado por los jóvenes David Cárdenas García, Gisselle Gabriela Obando López y Roberto Enrique Ocampo Benavides titulado "Diseño y configuracion de un nodo de internet con servidores tipo PC usando Zimbra como herramienta de colaboración en grupo, servicio web, servicio DNS, servidor DHCP, servidor Proxy y una central telefónica virtual utilizando Elastix en el colegio Cristo Rey de la ciudad de Managua," fue expuesto ante los docentes y personal administrativo vinculados a nuestra institución de manera presencial generando grandes expectativas y considerando a futuro su posible implementación en nuestra institución, no omito manifestar que las dudas sobre este proyecto fueron aclaradas con preguntas realizadas a los expositores durante el foro.

Sin más a que referirme se despide,

Atentamente

Sor Maricela Fajardo
Directora Administrativa

Radial Santo Domingo • Tel.: 2278-2936 / 2278-5419