UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

MAESTRÍA EN TELEMÁTICA

"Diseño de una red telemática con VPN e internet para la Dirección Provincial de Salud de Loja"

Proyecto de graduación previo a la obtención del grado de**:**

MAGÍSTER EN TELEMÁTICA

Presentada por:

ING. GABRIELA VIÑÁN RUEDA

Director:

Diego Ávila P. Ing. MsC.

CUENCA-ECUADOR

2010-2011

CERTIFICACIÓN

ING. DIEGO ÁVILA P. , CATEDRÁTICO DE LA UNIVERSIDAD DE CUENCA, DIRECTOR DE LA TESIS DE MAESTRÍA EN TELEMÁTICA.

CERTIFICA:

Que la presente tesis ha sido realizada por la Ing. Gabriela Viñán Rueda, además de haber sido dirigida, orientada y revisada, observando las disposiciones emanadas por las autoridades de la Universidad de Cuenca, a través de la Facultad de Ingeniería y la Maestría en Telemática, considerando también las normas que la Metodología de la Investigación Científica sugiere.

…….

Diego Ávila P. Ing. MsC.

OBSERVACIÓN

EL CONTENIDO DE ESTA TESIS ES DE ABSOLUTA RESPONSABILIDAD DEL AUTOR.

…….

Ing. Gabriela Viñán Rueda.

AGRADECIMIENTOS

A DIOS

Porque sin Él nada se mueve,

A MIS PADRES

Por su apoyo,

A MIS HERMANOS

Por su comprensión,

A LA DPSL

Por su ayuda y colaboración,

A TODOS LOS PROFESORES

Por sus enseñanzas.

DEDICATORIA

A DIOS

A MIS PADRES

Y FAMILIARES.

RESUMEN

El presente trabajo trata sobre implementar una VPN para conectar las áreas de salud a la Dirección Provincial de Salud de Loja, que se ajuste a sus requerimientos y necesidades ya que existen en el mercado gran variedad de alternativas tecnológicas tanto software como hardware que sirven para implementar la VPN, de entre estas tecnologías se escoge una y se la presenta como alternativa para el intercambio de información entre estos sitios, además se ha diseñado una intranet para poder realizar este intercambio de comunicación, previo a una recopilación de información, investigación, se determinó la situación y se plantea la solución.

CAPÍTULO 1:

Se presenta la introducción, alcance, objetivos del proyecto, la metodología utilizada para desarrollarlo.

CAPÍTULO 2:

Luego de la introducción, se establece el marco teórico para indicar conceptos acerca de las VPN, tipos de VPN y conexiones.

CAPÍTULO 3:

En este capítulo se hace el diseño de la red donde se describe el modelo, la arquitectura del diseño, tipos de servidores, y se hace el direccionamiento IP para la red.

CAPÍTULO 4:

Especificado el diseño, se plantea diferentes alternativas tecnológicas especificando sus principales características, y seleccionando una que se ajuste a los requerimientos de la institución.

CAPÍTULO 5:

Se presenta una alternativa tecnología para el diseño de la red VOIP, considerando los equipos actuales, costos y mantenimiento.

CAPÍTULO 6:

Aquí se hace el análisis de requerimientos, diseño de bases de datos y finalizando con el desarrollo de la aplicación de red, para brindar servicios tales como noticias, documentos, chat, webmail, y el servicio de inspecciones necesario para la emisión de los permisos de funcionamiento a toda la provincia de Loja.

ABSTRACT

This paper deals with implementing a VPN to connect the areas of Health to the DPSL (Direccion Provincial de Salud de Loja) that fits your needs and requirements as they exist in the market a veriety of technologies alternatives that both software and hardware are used to implement VPN, among these technologies is selected and presents an alternative for the exchange of information between these sites, plus an intranet is designed to perform this exchange of communication prior to a collection of information, research, was determined the situation and considers the solution.

CHAPTER 1:

We present the introduction, scope, project objectives, the methodology used to develop it.

CHAPTER 2:

After the introduction, it begins to indicate the theoretical concepts about the VPNs, types and connections.

CHAPTER 3:

This chapter makes the design of the network which describes the model, architecture design, server types, and becomes the IP address for the network.

CHAPTER 4:

Then Specified design, it raises different technological alternatives specifying its main characteristics, and selecting one that meets the requirements of the institution.

CHAPTER 5:

It present an alternative technology for the VOIP network design, considering the current equipment and maintenance costs.

CHAPTER 6:

Here is the requirements analysis, database design and finishing with the development of network application, to provide services such as news, documents, chat, webmail, service and inspections for the issuance of operating permits to all the province of Loja.

ÍNDICE DE CONTENIDOS:

DISEÑO DE UNA RED TELEMÁTICA CON VPN E INTERNET PARA LA DIRECCIÓN PROVINCIAL DE SALUD DE LOJA

1. INTRODUCCIÓN

El uso del Internet actualmente se ha convertido en una necesidad que no debe faltar en las empresas, negocios, hogares, etc. Especialmente cuando estas entidades tienen el papel principal de prestar servicios públicos. Con esta gran tecnología como es el Internet, podemos hacer esta comunicación a través de la creación de redes privadas que no necesitan grandes costos especialmente para entidades públicas donde el capital disponible debe ser controlado.

Además, otra de las necesidades vitales de las empresas o entidades públicas, es la de compartir información, especialmente en aquellas que se encuentran distribuidas en zonas diferentes y que están bajo administración de una central como es el caso de la Dirección Provincial de Salud de Loja.

En este proyecto, se expone el diseño de una red telemática capaz de conectar todos los centros de salud de la Dirección Provincial de Loja, cuya finalidad es además de compartir información, la de prestar diferentes servicios y herramientas al personal administrativo, y así poder brindar una mejor atención a la ciudadanía de la provincia de Loja.

Con el uso de protocolos apropiados y encriptación, se mantendrá la integridad de los datos y privacidad de las conexiones para que estas sean seguras.

Con esta red se podrá dar seguimiento a las actividades que realizan los inspectores en cada centro de salud, así como recopilar, publicar y recuperar información que se genera en la Dirección Provincial de Salud.

La Dirección Provincial de Salud de Loja (DPSL) tiene su sede en la ciudad de Loja, y controla 13 Áreas o Centros de Salud en toda la provincia, tres áreas en la ciudad de Loja y diez en cada uno de los cantones, la función de esta institución es:

- Promover la Salud, incidir en la calidad de vida de la población de la Provincia de Loja y actuar en coherencia con el Sistema de Nacional de Salud.
- Proceso de Control y Vigilancia sanitaria.
- Registro de títulos de profesionales de la Salud.
- Controlar la promoción de medicamentos de uso y consumo humano.
- Etc.

Con la creación de la Intranet se podrán realizar, habrá mayor control y comunicación con todas estas Áreas para poder dar un servicio óptimo a toda la provincia, y mediante VPN se creará una red privada y segura que funcione sobre la red Internet ya que esta es la más apropiada para llegar a sitios remotos donde la tecnología es insipiente.

1.1 Descripción del problema y/o necesidad

Uno de los mayores problemas que se ha detectado es la falta de control y administración de todas las Áreas de Salud de la provincia, la DPSL tiene bajo su control 13 centros que deben suministrar información especialmente relacionada con los permisos sanitarios de todas las tiendas o comercios, los inspectores que son los encargados de revisarlos, deben enviar la información en papel cada vez a la ciudad de Loja donde se encuentra funcionando el sistema informático que ingresa estas inspecciones, toda esta tarea se la puede ahorrar y economizar gastos si ellos registraran esta información al sistema pero a través de una intranet.

En el futuro esta red servirá para implementar otros sistemas, proporcionar acceso remoto, VoIP para unificar todas las áreas y trabajar en mejores condiciones, entregar nuevos servicios a la ciudadanía como son la implementación de sistemas de Telemedicina, teletrabajo, etc; por lo que es muy importante desarrollarla y además la DPSL ya tiene tecnología que no es aprovechada en este momento por carecer de la intranet.

Con la implementación de la intranet, se podrán realizar las siguientes funciones:

- Registro, control y administración de las inspecciones que se realizan a los diferentes establecimientos de la provincia de Loja, por parte de los inspectores designados en cada Área, para poder emitir los permisos de funcionamiento.
- Control e informe de los inspectores ubicados en cada Área de funcionamiento en toda la provincia de Loja.
- Manejo de información interna en toda la DPSL.
- Ofertar servicios adicionales como webmail, chat.

1.2 Justificación del proyecto de tesis

1.2.1 Justificación académica

El presente proyecto involucra tecnología y aplicación de los conocimientos adquiridos en los cursos de la Maestría en Telemática como: Diseño de Redes, Gestión de Red, Seguridad, entre otros, los que me sirvieron para afianzar los conocimientos de mi especialidad y tener la seguridad de proponerlos en este proyecto.

1.2.2 Justificación Tecnológica

Dada la necesidad de comunicación entre los diferentes centros de la Dirección Provincial de Salud de Loja, se plantea la red telemática a través de internet, con lo cual la DPSL ya cuenta con equipos y tecnología especializada como un servidor web, computadores en todas las oficinas, una red y servicio de internet a toda la red de la provincia, para poder llevar a efecto este proyecto.

Los datos ingresados en cada centro, se almacenaran en el centro de cómputo de la DPSL porque es el único centro encargado de su administración y permitirá una comunicación eficiente entre toda la Institución.

1.2.3 Justificación Legal

La Dirección Provincial de Salud en cada provincia, es la encargada de velar, administrar, controlar, promover la salud, siendo su sede en la ciudad de Loja y bajo su administración están todas las áreas o centros de salud de cada cantón.

1.2.4 Justificación Económica

La DPSL cuenta con los recursos necesarios para adquirir tecnología, sistemas o software para ser implementados e inclusive posee equipos que no son aprovechadas toda su capacidad y tecnología.

1.3 Objetivos de la tesis de grado

1.3.1 Objetivo general

DISEÑAR UNA RED TELEMÁTICA PARA LA DPSL CON VPN E INTERNET QUE PERMITA EL INTERCAMBIO DE INFORMACIÓN Y SERVICIOS EN TODOS LOS CENTROS DE SALUD.

1.3.2 Objetivos específicos

- Recolectar y seleccionar la información obtenida en la Dirección Provincial de Salud de Loja que permita identificar las necesidades y requerimientos para la caracterización de la red.
- Diseñar la red telemática utilizando VPN que conecte todos los centros de salud de la DPSL con el nodo central especificando los recursos, medios y protocolos.
- Realizar la instalación y configuración de las VPN cliente y servidor en Linux para tener una conexión segura y confiable a bajo costo con servicios de webmail, Chat.
- Desarrollar la interfaz gráfica de la intranet para proporcionar el servicio de webmail, chat y el registro de las inspecciones de los centros de salud.
- Realizar pruebas y correcciones del prototipo implementado en el servidor Linux.

1.4 Alcance del proyecto

Se hará el análisis y diseño de una red telemática para conectar todas las Áreas de salud con la Dirección Provincial de Salud de Loja, esta conexión será mediante la plataforma internet y con el uso de VPN para dar mayor seguridad a la red, para demostrar su efectividad, se desarrollará un prototipo entre el Área de salud N3 y el centro de cómputo de la DPSL.

Para el desarrollo de este proyecto, se hace uso de software libre por ser la DPSL una institución pública y el Estado promueve este tipo de software.

1.5 Desarrollo del método de trabajo

El método de trabajo para realizar el presente proyecto, es a partir de la información recolectada en la DPSL, a través de entrevistas y observaciones realizadas al personal técnico y administrativo se logro conocer sus necesidades que actualmente tiene la institución, luego de analizar la información necesaria se hará el diseño de la red lógica de la misma que incluya todos los centros de salud y que satisfaga los requerimientos de la DPSL, finalizado el diseño lógico programaré un prototipo de la intranet que contenga los servicios más importantes, desarrollado el prototipo se procederá a configurar las VPNs tanto servidor como cliente para realizar las pruebas y correcciones de la red.

1.5.1 Metodología

Para el diseño de la red y el prototipo, se usa la **metodología XP (Programación Extrema)**, esta es adecuada para este tipo de proyecto porque mantiene el diseño simple y claro, con XP se puede añadir funcionalidad con retroalimentación contínua en caso de cambio de

requerimientos cuando el cliente no los tiene definidos con claridad, es útil para proyectos de riesgo y apto para proyectos que no requieren mucho personal pueden ser uno o dos programadores, además me permite tener una correcta planificación para desarrollarlo a tiempo y al final obtener mayor productividad en el proyecto y un software de calidad.

1.5.2 Características de XP:

- Pruebas
- Programación en pares
- Integración contínua
- Versiones frecuentes
- Etc.

1.5.3 Fases:

Las fases a seguir de esta metodología son:

Planificación.-que contiene el cronograma, información recolectada de la DPSL y de sus necesidades.

Diseño.- teniendo claro los requerimientos, se realiza el diseño de la red pero que sea simple y sencillo, determinando la funcionalidad y riesgos.

Codificación.- definido el diseño, se desarrolla el software respectivo.

Pruebas.-se hace uso de test para comprobar la funcionalidad del prototipo y optimizar su rendimiento, luego el código será implantado cuando supere los respectivos tests.

Figura 1.1. Fases metodológicas del proyecto con el uso de XP.

CAPÍTULO 2

2. MARCO TEÓRICO

2.1 VPN

Como las redes LAN de los Centros de Salud están ubicadas en cada cantón de la provincia y con el tiempo es necesario acceder a la Dirección Central de manera que puedan compartir información y no se encuentren aisladas sin ningún control, al establecer la red telemática con VPN e internet, se ahorrará recursos y la inversión será inferior para este tipo de instituciones públicas que no cuentan con capital propio.

El internet no es seguro, por esto las VPN usan protocolos especiales que encriptan la información, y solo las personas que tengan la llave de desencriptación y acceso de su equipo al servidor VPN pueden tener una comunicación confiable. Con el diseño de la red telemática se podrá conectar todas las filiales de la Institución y debe ser implementada sobre una plataforma segura a todo tipo de ataques o permisos no autorizados.

RED PRIVADA VIRTUAL (VPN).- Una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, tal como Internet, en un túnel privado que simula una conexión punto a punto. Un acceso VPN habilita a todos los usuarios acceder a una organización de una localidad remota, el usuario usa software en su computadora para conectarse con la Dirección Central, luego de ingresar el login, el servidor acepta la sesión del usuario y establece el túnel y el software empieza a transportar paquetes por el internet de forma segura.

La forma de comunicación entre el VPN servidor y las VPNs clientes es a través de túneles entre estos puntos, los cuales negocian la comunicación para que esta sea segura, ya que la información requiere ser privada.

Para esta conexión, se requieren recursos elevados tanto en el servidor como en los clientes para ello se necesitará un equipo servidor potente para que la transmisión de la comunicación no sea lenta.

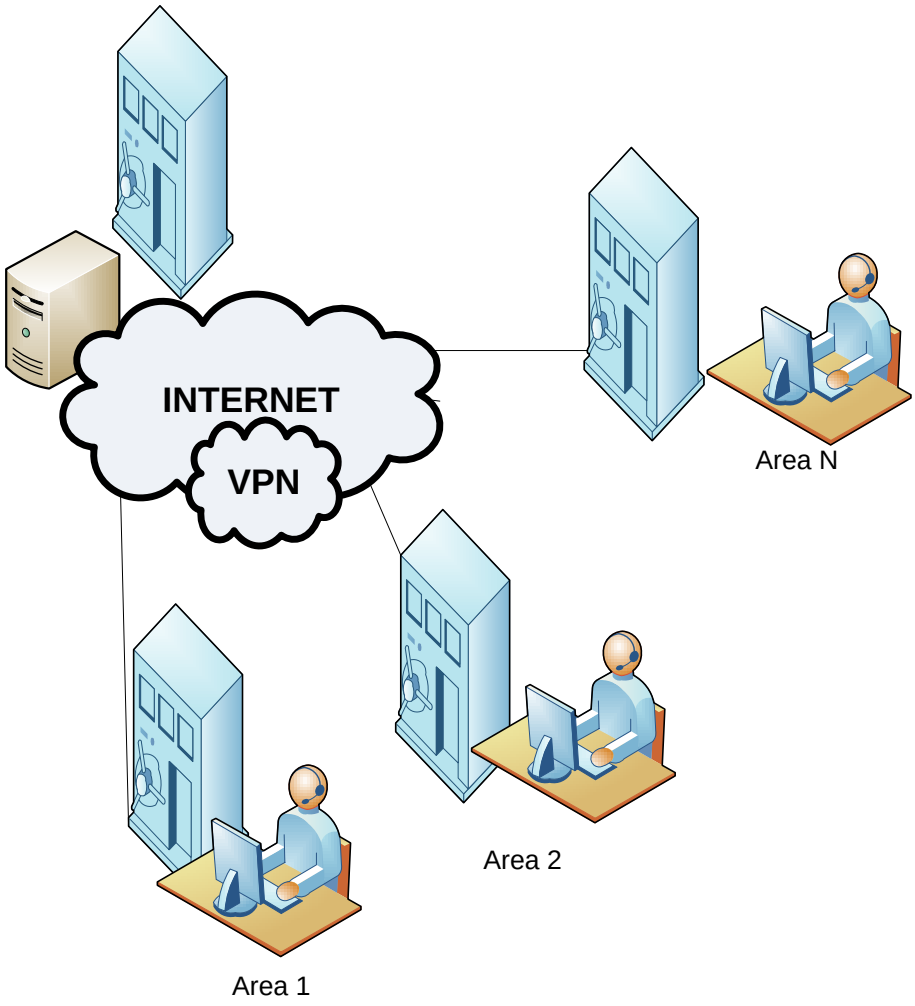


Figura 2.1. VPN.

Para el presente proyecto la VPN forma parte del sistema operativo Linux, Fedora 12 pero se puede adaptar a cualquier sistema operativo Linux.

Mediante las VPN's se obtiene:

- La administración de la red a bajo costo.
- Seguridad para conectarse vía Internet.
- Confidencialidad, integridad de los datos.
- Permite conexión de cualquier equipo que tenga autorización.

- Son sencillas de manejar, etc.

No sólo es necesario mencionar las ventajas de las VPN sino que se debe presentar sus desventajas para cuidar el rendimiento de la intranet y optimizar sus recursos, las desventajas más conocidas son:

- Se deben establecer correctamente las políticas de seguridad y de acceso.
- No se garantiza disponibilidad ya que si no hay internet no hay intranet.
- Mayor carga en el cliente VPN porque debe encapsular los paquetes de datos y encriptarlos.
- Fallo en seguridad debido a la conexión por internet o debido a los usuarios que accesan remotamente pueden utilizar las computadoras para abrir otras aplicaciones que amenazan la red.

2.1.1 CREACIÓN DE TÚNELES.

El túnel es el camino lógico o sentido que los paquetes encapsulados viajan a través de la red interna de tránsito, se pueden crear muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura, el tunneling tiene implicaciones notorias para las VPN's.

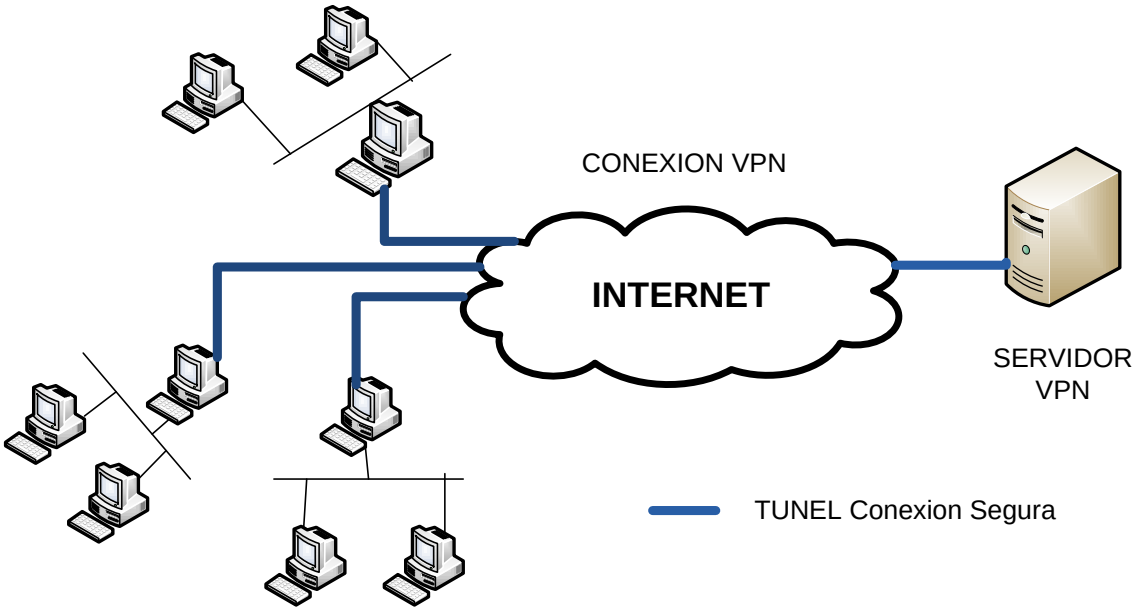


Figura 2.2. Creación de túneles.

Tunneling.- es un método que consiste en utilizar la infraestructura de una interred, en este caso el Internet, para transportar datos de una red a otra, además hace el proceso de colocación de cada paquete de información que se envía dentro de otro encapsulado, lo que permite que los usuarios se conecten de forma segura estén donde estén a la organización.
Los componentes básicos de un túnel son:

- Un iniciador de túnel
- Dispositivos de enrutamiento
- Terminadores de túneles.

Tipos de túneles:

Túneles Voluntarios: Un usuario o cliente puede emitir una petición VPN para configurar y crear un túnel voluntario. En este caso, el usuario es un terminal del túnel y actúa como el cliente del mismo.

Túneles Compulsivos: Una VPN con servidor con capacidad de acceso por llamada, configura y crea un túnel, Otro dispositivo, el RAS (Servidor de

Acceso Remoto), entre la computadora usuario y el servidor de túnel es la terminal del túnel y actuará como cliente.

El tipo de túnel empleado para la VPN de la DPSL es túnel Voluntario, en donde un usuario conectado de cualquier PC o estación de trabajo se conectará con el servidor VPN de la Dirección ubicado en la ciudad de Loja.

2.1.2 ELEMENTOS DE UNA VPN

- Un servidor VPN para aceptar las conexiones cliente.
- Un cliente VPN que hace las peticiones al servidor, puede ser una PC o router.
- Un túnel, parte de la conexión en que los datos están cifrados.
- Protocolos de tunneling para hacer la gestión del túnel y cifrar los datos.
- Red de tránsito, es la red pública para transportar los datos, en este proyecto se considera como red pública al internet.

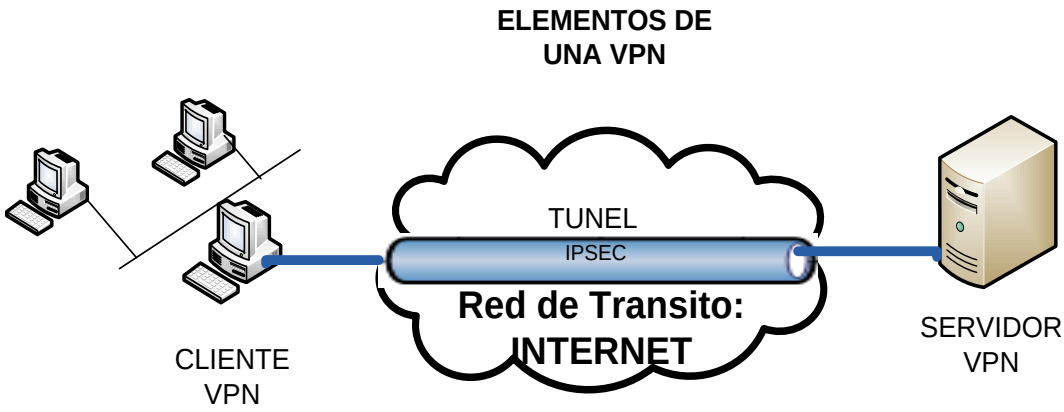


Figura 2.3. Elementos de una VPN.

2.1.3 TIPOS DE VPN

Existen varias clasificaciones de VPN, la clasificación más común o detallada de Vpn es la siguiente:

- **VPN DE ACCESO REMOTO.-**consisten en usuarios y computadoras que se conectan a la empresa desde sitios remotos a través de internet.
- **TUNNELING.-**establece un túnel VPN dando mayor seguridad para conectarse por el internet, desde las oficinas remotas hasta la Dirección Central y requiere tener cuenta en la Central para poder acceder.
- **VPN SITIO A SITIO.-**conecta oficinas remotas con la central a través del internet, la conexión se realiza entre servidores o enrutadores, aquí no será necesario configurar clientes individuales o aplicaciones.
- **VPN INTERNA.-**es similar a la VPN de acceso remoto, pero en vez de utilizar el internet para conectarse, emplea la red LAN de la empresa**.**

Para el diseño de este proyecto se utiliza el tipo de VPN Tunneling de host a Sitio por permitir la encriptación y autenticación de los usuarios que trabajan en todas las Áreas de Salud y solo a través de estos lugares pueden acceder a la intranet.

La conexión encriptada a través de VPn requiere bastantes recursos tanto como en el servidor como del lado del cliente, existen muchas aplicaciones VPN por software o productos hardware que hacen este trabajo, dentro de esta familia tenemos a los productos de Nortel, Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, D-link etc. y dentro de las soluciones software tenemos productos de código abierto (Open Source) que es lo que nos interesa y como ejemplos tenemos: OpenSSH, OpenVPN y FreeS/Wan.

2.1.4 TIPOS DE CONEXIONES:

Las VPN soportan tres modos de uso:

- Conexiones de cliente con acceso remoto
- Interconexiones LAN a LAN.
- Acceso controlado dentro de una Intranet.

2.1.4.1 Conexiones de cliente con acceso remoto:

Puede establecerse con soporte de acceso remoto, utilizado para el teletrabajo, utiliza un diseño cliente/servidor. Los paquetes enviados a través de la conexión se originan en el cliente de acceso remoto, y este se autentica en el servidor de acceso remoto.

2.1.4.2 Interconexiones LAN a LAN:

Se usa para puntear dos redes locales, formando una intranet extendida, esta solución utiliza una conexión de servidor VPN a servidor VPN. También es una conexión de router a router, el router que origina la comunicación se autentica ante el otro router que responde y este a su vez se autentica al router que origina la comunicación, también sirve para la intranet.

2.1.4.3 Acceso controlado dentro de una intranet:

En este modo de operación los clientes se conectan a un servidor VPN que actúa como el Gateway de la red, no involucra a un Proveedor de Servicios de Internet ni al cableado de una red pública. Es realizada por un firewall que se conecta a la red, los paquetes son enviados por cualquier usuario conectado al internet y el firewall se autentica ante el solicitante y viceversa.

El modo de conexión utilizado en este proyecto conexiones de cliente que se conectan remotamente al servidor de la red y su arquitectura de VPN basada en intranet es la siguiente:

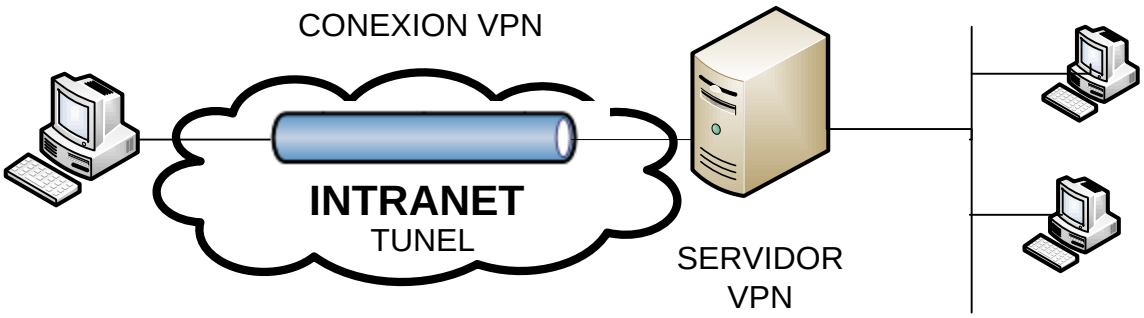


Figura 2.4. Tipo de conexión VPN cliente-servidor.

Los principales beneficios que obtenemos con esta solución son: privacidad (todos los datos transmitidos van encriptados, por lo que se garantiza la confidencialidad de los mismos), integridad (existen mecanismos por los que se garantiza el mensaje no ha sido modificado durante el envío), autenticación (el emisor firma sus mensajes digitalmente, de forma que el receptor puede comprobar que realmente fue enviado por él).

Se trata de una solución para sus comunicaciones, sencilla de implantar y que proporciona beneficios a corto plazo.

CAPÍTULO 3

3. DISEÑO DE LA RED TELEMÁTICA.

3.1 DESCRIPCIÓN DEL MODELO

3.1.1 Situación Actual

Actualmente la red de la DPSL en Loja consta de un servidor de aplicaciones que funciona en el mismo servidor que provee el servicio de internet, se prevé implementar un servidor para la página web de la Dirección en lo posterior; cada Área tiene implementada una LAN y con servicio de internet con diferentes proveedores, solo tienen acceso al servidor principal de la DPSL la red LAN de la misma, las Áreas no están conectadas con la DPSL.

En cada Área hay un switch de 32 puertos para conectar la LAN y un servidor web para el servicio de internet de la red, el número total de equipos se muestran a continuación:

TABLA 3.1. Equipos disponibles en la DPSL.

AREA	CIUDAD	SWITCH	ROUTER	SERVIDOR	EQUIPOS	TOTAL
DPSL	Loja	3	1	1	90	95
1	Loja	1		1	13	14
2	Loja	1		1	18	20
3	Loja	1		1	18	20
4	Catamayo	1		1	15	17
5	Cariamanga	1		1	15	17
6	Amaluza	1		1	18	20
7	Macará	1		1	15	17
8	Catacocha	1		1	12	14
9	Alamor	1		1	15	17
10	Saraguro	1		1	10	12
11	Gonzanamá	1		1	10	12
12	Vilcabamba	1		1	10	12

El diseño de la red como se encuentra estructurada actualmente es la siguiente:

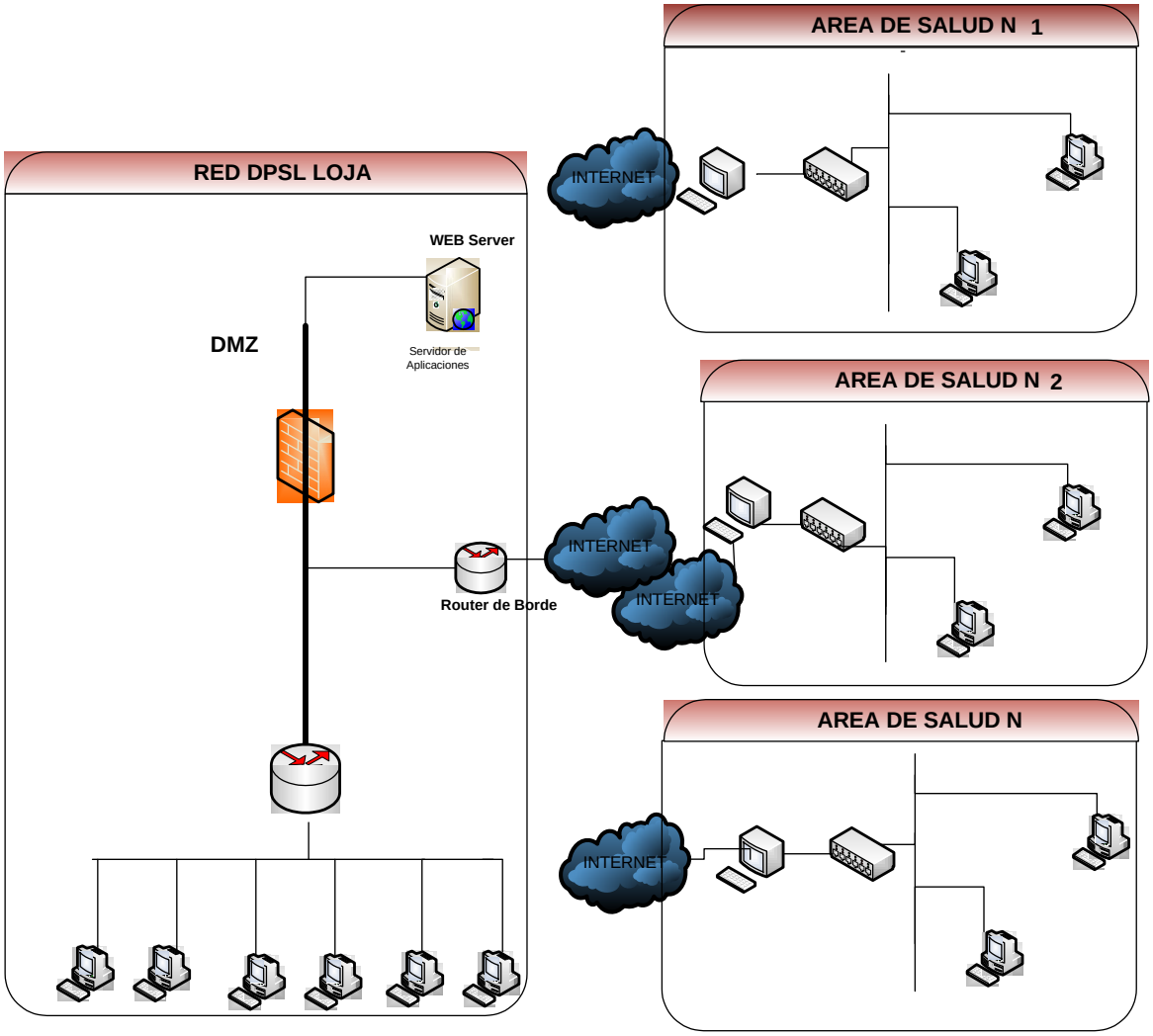


Figura 3.1. Diseño actual de la DPSL.

Este proyecto está planteado sobre la base de la tecnología y arquitectura de red actual existente, para la red VPN se incrementarán unos equipos adicionales para mejorar el rendimiento y tráfico de la red, esta opción se ajusta a la situación económica de la DPSL ya que es una institución del Estado y no es fácil conseguir presupuesto a corto plazo, la red de cada Área tiene cableado estructurado Cat 5.e, no todas tienen el mismo ancho de banda de internet y con diferentes proveedores, el Gobierno prioriza

CNT como proveedor de internet para las entidades públicas porque es una empresa de telecomunicaciones del Estado.

En la siguiente tabla están resumidas las LAN de cada área:

TABLA 3.2 LAN de las Áreas de Salud.

AREA	CIUDAD	INTERNET	VELOCIDAD	LAN
DPSL	Loja	Si	2,5 Mbps	Si
1	Loja	Si	512 Kbps	Si
2	Loja	Si	512 Kbps	Si
3	Loja	Si	512 Kbps	Si
4	Catamayo	Si	512 Kbps	Si
5	Cariamanga	Si	512 Kbps	Si
6	Amaluza	Si	300 Kbps	Si
7	Macará	Si	512 Kbps	Si
8	Catacocha	Si	512 Kbps	Si
9	Alamor	Si	300 Kbps	Si
10	Saraguro	Si	300 Kbps	Si
11	Gonzanamá	Si	256 Kbps	Si
12	Vilcabamba	Si	300 Kbps	Si

3.1.2 Solución propuesta

Se plantea que todas las áreas estén funcionando conjuntamente a través de una red VPN con internet y que todas tengan el acceso y estén bajo el control de la Dirección Central en la ciudad de Loja, lo que se propone aumentar la capacidad del ancho de banda en respuesta a la necesidad presentada y además se rediseña esta red para que proporcione los servicios para los cuales se la ha creado, como son:

- Chat
- Webmail
- Aplicación
- Descarga de archivos y documentos

- Compartición de información y
- Plataforma para servicios futuros como VoIP.

La red de la DPSL es una red de Área Amplia (WAN), dentro de la cual hay un servidor central a través de una Red Virtual Privada (VPN) e internet para la compartición de datos e información relativa a las Áreas conectadas.

Es importante considerar el tipo de aplicaciones que van a correr en la VPN, para lo cual se debe delimitar las aplicaciones como acceso a internet, correo electrónico, consulta a la base de datos, transferencia de archivos, no es recomendable utilizar la VPN para servicios como streaming, videoconferencia ya que consume gran cantidad de recursos de los equipos además del ancho de banda.

También hay que considerar el número de usuarios, cada equipo de cada red LAN representa un usuario, pero no todos tienen las mismas atribuciones o roles, los usuarios de todas las Áreas de salud tendrán acceso a la base de datos del servidor central ubicado en la ciudad de Loja.

EQUIPOS EN LA DPSL.

El proyecto va en función de los equipos y las instalaciones que tiene actualmente la DPSL, solo cuenta con un servidor HP Proliant que reúne las características técnicas necesarias, todo el equipamiento y la red se encuentra funcionando y está en buenas condiciones ya que se la implementó en menos de 2 años.

En el centro de cómputo de la DPSL para dar mayor escalabilidad y rendimiento a la VPN, el software será todo bajo Linux para los servidores

y se proyecta implementar en este centro, en la zona desmilitarizada los siguientes servidores:

- Un servidor de autenticación para la emisión de las claves públicas y privadas de todos los usuarios conectados a la red.
- Un servidor web para alojar el sitio de internet de la DPSL.
- Un servidor de correo para proveer el servicio de emails a todos los usuarios.

Además implementar los siguientes equipos:

- Un servidor de base de datos que contenga la información de las aplicaciones manejadas por todas las áreas.
- Un servidor de aplicaciones para compartir los sistemas y archivos entre toda la DPSL.
- Un servidor VPN para integrar toda la red.
- Un router de borde para proveerse del servicio de internet (este no necesariamente puede pertenecer a la DPSL sino al ISP).
- Un router para conectar toda la LAN de la Dirección central.

A continuación se muestra un esquema general de toda la red:

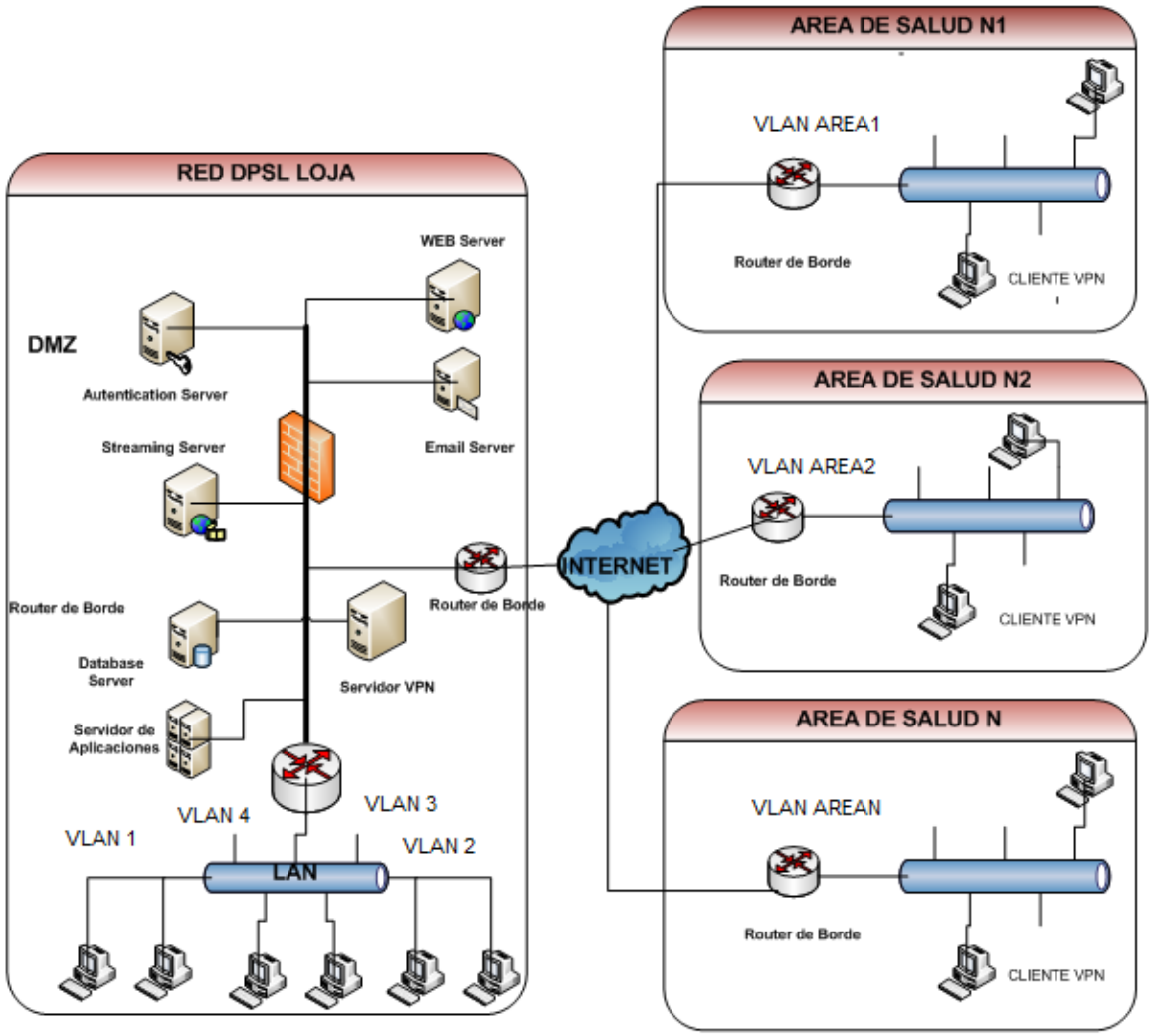


Figura 3.2. Arquitectura de la red.

3.2 CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS.

3.2.1 REDES LAN

3.2.1.1 Switch

Las LAN de todas las áreas tienen cableado estructurado categoría 5e, y se emplea para conectarse al servidor un switch capa 2 no administrable. Para optimizar la red se propone adquirir un switch administrable para cada Área, que reúna las siguientes características:

- Switch con firewall
- Encriptación.
- Mínimo 32 puertos.
- Configuración de vlan.
- Etc.

Existen muchas opiniones sobre hardware que se deben utilizar, como referencia se recomienda utilizar el siguiente switch:

TABLA 3.3. Características de los switch LAN.

Marca	3COM
Serie	2226
Ethernet LAN (RJ-45) cantidad de puertos	24
Administrable	SI

El switch actual que tiene cada Área será utilizado para segmentar cada subred para propósitos de escalabilidad.

3.2.1.2 PC

Los clientes deben cumplir los requerimientos mínimos de hardware, pueden ser de cualquier configuración de software o hardware que no implica incompatibilidad, con la única condición de estar conectados al internet y configurados lógicamente con la respectiva dirección IP, con configuración VPN, y tener acceso al servidor Vpn, la intranet es compatible con cualquier sistema operativo que tengan.

Para mayor velocidad de la vpn e instalación de programas como firewall para seguridad del equipo, como recomendación debe tener los requisitos mínimos de hardware que son:

- Procesador 3 Ghz.
- Memoria 3 Gb.
- Videocámara
- Capacidad para procesar imágenes.
- Almacenamiento 120 Gb.
- Capacidad para transmitir videos.
- Etc.

3.2.1.3 Routers

Los ruteadores, deben tener capacidad para manejar las rutas y además brindar seguridad a las subredes, como las Áreas no cuentan con los recursos suficientes para un buen equipo, se requiere un equipo que cumpla las siguientes características mínimas:

- Compatible con dispositivos que operen en el estándar 802.11b
- Compatible con otros productos IPSEC VPN.
- Tenga 4 puertos o más.
- Soporte VPN.
- Soporte encriptación SSL, IPSEC.
- Calidad de servicio QoS.
- Firewall

- Soporte de hasta 32 túneles simultáneos.
- Configuración remota, NAT, etc.

El ruteador puede ser de cualquier marca que se ajuste las características, el equipo que se puede utilizar se lo propone a continuación:

TABLA 3.4. Características de los ruteadores

Marca	LYNKSYS
Serie	Cable/DSL VPN Router
Modelo	BEFVP41
Ethernet LAN (RJ-45) cantidad de puertos	5
Tuneles	50

3.2.1.4 Servidores

Los servidores para cada Área con las características:

- Mínimo 2 Ghz de memoria.
- Memoria mínimo 2 Gb.
- Configuración Linux.
- Tenga 6 puertos o más.

El servidor puede ser de cualquier marca, tipo pero que reúna las características mínimas requeridas, el equipo que se puede utilizar se lo propone a continuación:

TABLA 3.5. Características de los servidores para las Áreas de Salud

Marca	Servidor HEWLETT-PACKARD ProLiant ML115 G5
Sistema Operativo	Linux
Velocidad	2.2 GHz
Memoria	512 MB (instalados) / 8 GB (máxima)
Procesador	1 x AMD Athlon 3500+ / 2.2 GHz

HARDWARE Y SOFTWARE DE SERVIDORES REDES LAN

TABLA 3.6. Hardware y software de servidores para las Áreas de Salud.

AREA	CIUDAD	MARCA	MODELO	SISTEMA OPERATIVO	USO
1	Loja	HEWLETT-PACKARD	ML115 G5	LINUX	Firewall, Seguridad
2	Loja	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
3	Loja	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
4	Catamayo	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
5	Cariamanga	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
6	Amaluza	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
7	Macará	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
8	Catacocha	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
9	Alamor	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
10	Saraguro	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
11	Gonzanamá	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones
12	Vilcabamba	HEWLETT-PACKARD	ML115 G5	LINUX	BBDD, Archivos y aplicaciones

DISPOSITIVOS INTERCONECTANTES PARA LAS LAN

TABLA 3.7. Dispositivos interconectantes para las Áreas de Salud.

AREA	CIUDAD	MARCA	MODELO	APLICACION
DPSL	Loja	LYNKSYS	BEFVP41	router
1	Loja	LYNKSYS	BEFVP41	router
2	Loja	LYNKSYS	BEFVP41	router
3	Loja	LYNKSYS	BEFVP41	router
4	Catamayo	LYNKSYS	BEFVP41	router
5	Cariamanga	LYNKSYS	BEFVP41	router
6	Amaluza	LYNKSYS	BEFVP41	router
7	Macará	LYNKSYS	BEFVP41	router
8	Catacocha	LYNKSYS	BEFVP41	router
9	Alamor	LYNKSYS	BEFVP41	router
10	Saraguro	LYNKSYS	BEFVP41	router
11	Gonzanamá	LYNKSYS	BEFVP41	router
12	Vilcabamba	LYNKSYS	BEFVP41	router

3.2.2 CENTRO DE COMPUTO DPSL

3.2.2.1 SERVIDORES

Este componente contiene elementos de hardware y software que permite centralizar la información que proviene de los clientes de todas las Áreas de Salud de Loja, estos servidores estarán ubicados en el centro de cómputo de la DPSL, la Dirección ya dispone de Ups de alta capacidad para proveer de energía eléctrica de reserva para los servidores.

Para el presente proyecto se plantea el uso de siete servidores que son:

- Servidor de Autenticación
- Web Server
- Streaming Server
- Servidor de Bases de datos
- Servidor de aplicaciones
- Servidor VPN.
- Servidor Email.

Servidor de Autenticación.-permite autenticar a los usuarios en forma centralizada para proporcionar acceso a uno o más servicios, ayuda a controlar la seguridad de la red.

Web Server.- la DPSL tendrá su propio dominio y alojará su sitio web en este servidor.

Streaming Server.- para audio/video que añaden contenido dinámico con multimedia a los sitios web.

Servidor de Bases de Datos.- provee servicios de bases de datos a los clientes, en este proyecto nos basamos en el modelo cliente-servidor y la base de datos MySql, aquí se alojará las bases de datos de la DPSL actuales que desean compartir con los usuarios de las demás Áreas.

Servidor de Aplicaciones.-proporciona el servicio de aplicaciones a los clientes para qué accesen a los datos a través de internet, se puede

implementar a la intranet de la DPSL en un futuro, servicios adicionales como wiki, blogs.

Servidor VPN.-permite autenticar a los usuarios en forma centralizada para proveerles acceso a uno o más servicios y que mediante el internet accedan en forma segura a través de túneles vpn a la intranet de la DPSL.

Servidor Email.-permite almacenar correo electrónico y dar este servicio a todos los usuarios.

La implementación de estos servidores se los puede hacer a través de hardware o software, dependiendo de los recursos de la Dirección, sin embargo para ahorrar recursos y equipos solo se planifica el uso de 3 servidores hardware que contenga todos los componentes instalados (software) y que reemplacen a los 7 servidores necesarios, el sistema operativo de estos servidores es Linux con esto se cumple con la política del Estado y se ahorrará recursos por las licencias; las funciones que desempeñaría cada servidor son:

Servidor 1: Servidor de autenticación, Servidor VPN.

Servidor 2: Servidor de Streaming, Servidor de Aplicaciones.

Servidor 3: Servidor de BBDD, Email, web.

La plataforma sobre la cual funciona la intranet está formada por los servidores anteriormente descriptos que pueden ser implementados varios servicios en un solo servidor potente mediante software reemplazaría a los servidores físicos especificados y en el cual se instalen todos los servicios básicos para la red.

Para mantener una alta disponibilidad de los servicios evitando cualquier fallido, se propone un servidor especial para la VPN, para garantizar así el servicio todo el tiempo, para este servidor se recomienda las siguientes características mostradas a continuación:

- El servidor debe tener tamaño máximo de memoria y procesador en toda su arquitectura, esto es, si posee memoria y procesadores distribuidos por interfaces o funcionalidades deben configurarse al máximo.
- Debe contar con alta disponibilidad.
- Calidad de servicio (QoS) extremo a extremo.
- Soporte IPv6.
- Tunneling
- Soporte en protocolos capa 2 y capa 3.
- Este servidor tienes varias tarjetas de red para conectarse a la red pública y a la red privada.

Hay gran variedad de equipos en el mercado y de cualquier precio, teniendo en consideración las características antes mencionadas se presenta 3 tipos de servidores de la marca HP que goza de gran experiencia y popularidad en las empresas, cada uno de ellos servirá para implementar todos los servicios de la red:

Servidor 1: Servidor de autenticación, Servidor VPN.

Este servidor debe tener mayor memoria RAM, mayor velocidad del procesador, porque de aquí se van a conectar todas las redes y controlará la autenticación y va a permitir conectar la red VPN.

TABLA 3.8. Características del servidor principal Vpn.

Marca	Hewlett-Packard
Serie	ML150 G6
Nombre	ProLiant ML150 G6 Server
Procesador	1 x Intel Xeon E5520 Quad-core 2.26 GHz
Cache	8 MB L2
Memoria	4 GB

Servidor 2: Servidor de Streaming, Servidor de Aplicaciones.

Para futuros servicios como VoIP, videoconferencia, sistemas centralizados, este servidor tendrá la capacidad suficiente y proporcionará el acceso a estos servicios.

TABLA 3.9. Caracteristicas del servidor de aplicaciones.

Marca	Hewlett-Packard
Serie	ML150 G6
Nombre	HP ProLiant ML150G6
Procesador	QuadCore Xeon E5504 (2.00 GHz)
Cache	8 MB L2
Memoria	2 GB

Servidor 3: Servidor de BBDD, Email, web.

Este servidor está disponible en la DPSL y es adecuado para el utilizarlo.

TABLA 3.10. Características del servidor de bbdd.

Marca	Hewlett-Packard
Serie	ML150 G6
Nombre	HP ProLiant ML150G6
Procesador	QuadCore Xeon E5504 (4.00 GHz)
Cache	8 MB L2
Memoria	4 GB

3.2.2.2 RUTEADOR

El equipo propuesto a continuación es un ruteador y tiene la ventaja de tener puerto para VoIP, para conectar la centralilla telefónica de la DPSL e implementar el telefonía IP a la red, tiene además las siguientes características técnicas:

- Velocidad mayor a 4 Mbps.
- Compatible con dispositivos que operen en el estándar 802.11b
- Soporte VPN.
- Calidad de servicio QoS.
- Firewall
- Configuración remota, etc.

TABLA 3.11. Características del ruteador

Marca	LYNKSYS
Serie	Linksys RT31P2 EU Router neutro con módulo ATA integrado
Modelo	RT31P2
Protocolo de direccionamiento	RIP-1, RIP-2, direccionamiento IP estático
Protocolo de compression de datos	Ethernet, Fastethernet
Puertos	3
Velocidad de transferencia de datos	100Mbps.

DISPOSITIVOS INTERCONECTANTES DE LA RED WAN Y SERVIDORES DPSL

TABLA 3.12. Dispositivos interconectantes de la red WAN y servidores para la DPSL.

EQUIPO	MARCA	MODELO	SISTEMA OPERATIVO	USO
Servidor	Hewlett-Packard	ProLiant ML150 G6 Server	LINUX	Servidor vpn
Servidor	Hewlett-Packard	HP ProLiant ML150G6 QuadCore Xeon E5504	LINUX	Servidor de Aplicaciones
Servidor	Hewlett-Packard	QuadCore Xeon E5504	LINUX	Servidor de BBDD
Ruteador	LYNKSYS	RT31P2		Red LAN

3.3 TOPOLOGÍA DE LA RED

3.3.1 Topología Física

3.3.1.1 Redes LAN

La topología física de la red LAN de cada área es en estrella extendida utilizando la tecnología Ethernet 802.3, el cableado estructurado seguirá la norma TIA/EIA-568B. Los tendidos horizontales utilizarán un cableado del tipo UTP cat 5e. En caso de que el área tenga más pisos entonces en el cableado vertical se utilizará fibra óptica.

La ventaja de esta topología es que en caso de caída del servidor o nodo central de la LAN pueden comunicarse las estaciones de trabajo que pertenezcan al mismo departamento y hay mayor velocidad en el tráfico así se evita colisiones o cuellos de botella con un solo nodo central que una a todos los equipos, con la topología actual estrella si se cae el servidor central ningún equipo puede comunicarse con otro así pertenezca al mismo departamento.

Para la ubicación de los servidores y la división en plantas tendremos un MDF para las Áreas de Salud en la provincia y para la LAN de la DPSL tendremos un MDF en el centro de cómputo y un IDF por planta, en el MDF tendremos los servidores de los Centros de Salud además de estos las Zonas desmilitarizadas DMZ para los servidores internet, VPn, firewall y DTE o Router para la conexión a internet.

Para la conexión cruzada horizontal a los *patch panels* cumplirá la tecnología 100BaseTX *Fast Ethernet Full Duplex*. Para la conexión cruzada vertical la cual conecta los IDF con los MDF la tecnología empleada será 1000BaseSX *Gigabit Ethernet.*

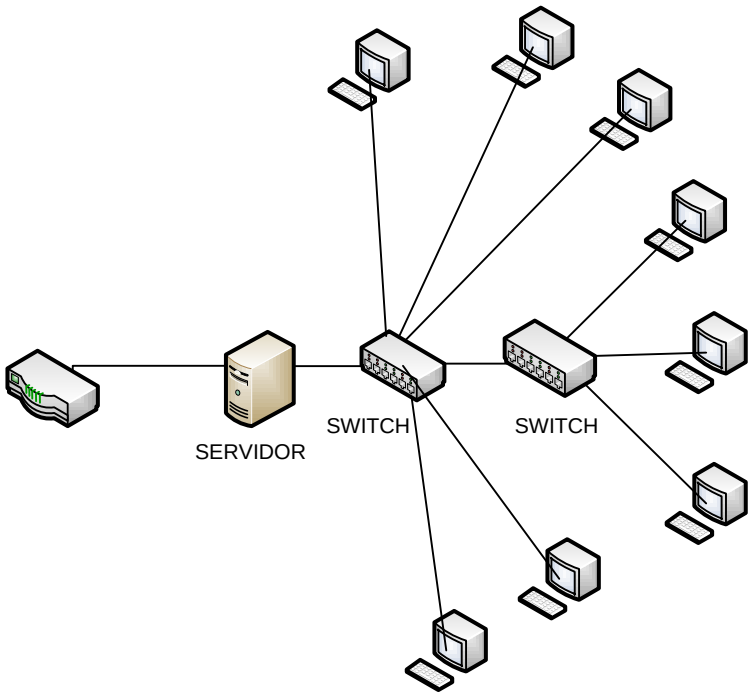


Figura 3.3. Topología Física de las redes LAN.

3.3.1.2 Red WAN/VPN

La red de transporte de datos desde las áreas a la DPSL es una red WAN, la topología física de la red WAN es de malla porque el internet es la plataforma de transporte de los datos desde las áreas que se encuentran en sitios remotos de la provincia hacia la central, sin embargo también en este diseño es centralizado, presenta una topología de estrella porque de cada nodo que sale de las LAN de cada área y estos a su vez se conectan al nodo central para alimentar de información a la DPSL a través de la red internet:

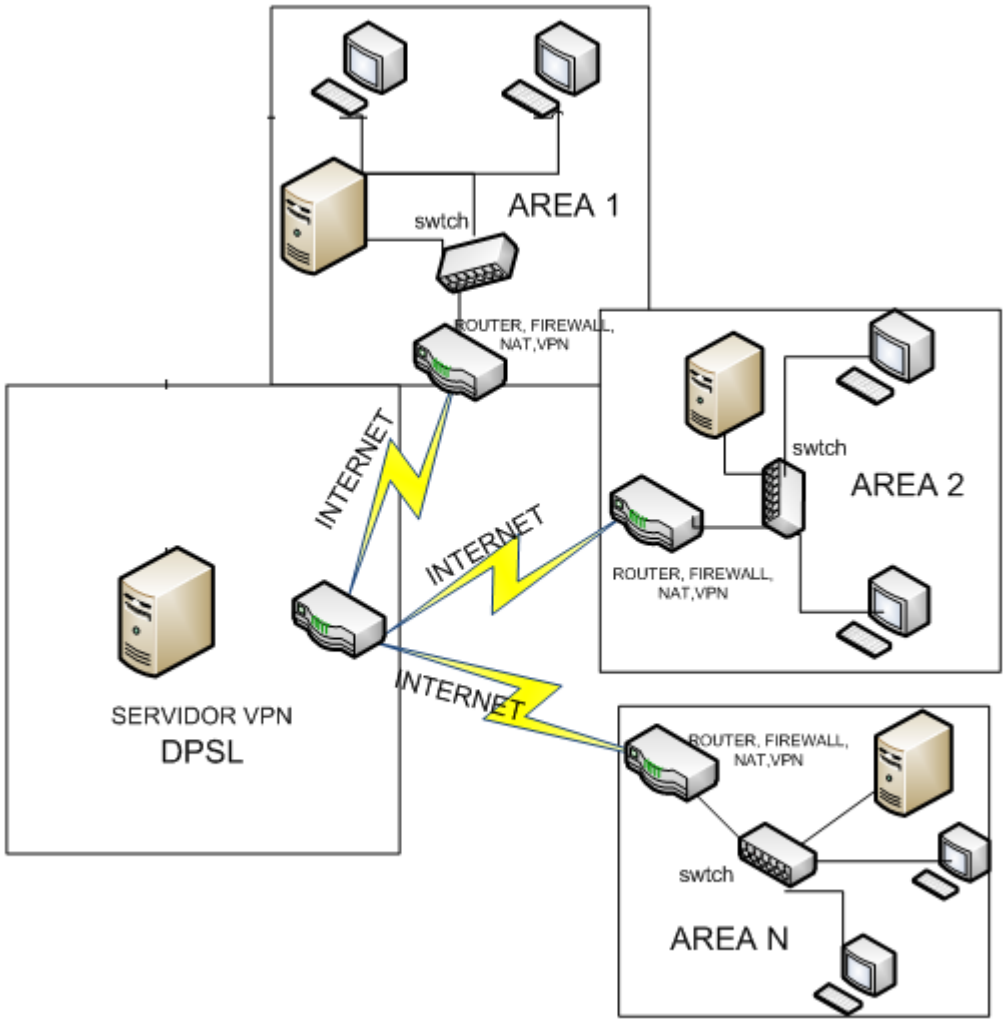


Figura 3.4. Topología Física de la red WAN.

3.3.2 CAPACIDAD DE LOS ENLACES

El tipo de tráfico que va a transportar la red WAN es:

- Datos de transacción.
- Datos de cliente/servidor
- Mensajería (por ejemplo, correo electrónico, chat)
- Transferencias de archivos
- Administración de red
- Voz/fax

En la siguiente tabla se especifica la capacidad de los enlaces para el internet, necesarios para la conexión de la vpn en la red WAN, la tecnología WAN que se ajusta al proyecto de acuerdo con la recolección de datos, como las Áreas están ubicadas en zonas remotas es útil la tecnología DSL (*Digital Subscriber Line*) que maneja velocidades de hasta más 51.84 Mbps es ideal para el tipo de tráfico de la WAN, seleccionando un único proveedor de internet para toda la red, la opción resultante es CNT para el enlace de última milla sea con fibra óptica en la Dirección Central y mediante líneas DSL en todas las Áreas con cobre, no solo tiene preferencia por el servicio económico sino también por ser propiedad del Estado.

Como el ancho de banda proporcionado por las empresas de telecomunicaciones ha aumentado debido a la demanda existente y sus costos han bajado, es por esto que si se implementará el servicio de VoIP se requiere mayor ancho de banda por el tráfico de voz y por la VPN porque la red es centralizada ya que estará bajo la administración de la DPSL; por ende que se ha planteado la capacidad razonable para unir los enlaces en toda la red a través de internet:

TABLA 3.13. Capacidad de los enlaces del Internet

ENLACE	CAPACIDAD (Mbps)	TRÁFICO
DPSL-LAN	3	Voz/Datos
DPSL-AREA1	1	Voz/Datos
DPSL-AREA2	1	Voz/Datos
DPSL-AREA3	1	Voz/Datos
DPSL-AREA4	1	Voz/Datos
DPSL-AREA5	1	Voz/Datos
DPSL-AREA6	1	Voz/Datos
DPSL-AREA7	1	Voz/Datos
DPSL-AREA8	1	Voz/Datos
DPSL-AREA9	1	Voz/Datos
DPSL-AREA10	1	Voz/Datos
DPSL-AREA11	1	Voz/Datos
DPSL-AREA12	1	Voz/Datos

3.4 ARQUITECTURA DEL DISEÑO

3.4.1 DIRECCIONAMIENTO IP

El esquema de direccionamiento para la red es estático y dinámico. Es estático al asignar direcciones IP a los servidores, ruteadores, y estos a su vez mediante DHCP reparten dinámicamente las direcciones IP a todos los equipos de trabajo.

Para el diseño de la red, se necesita direcciones públicas y privadas, a cada Área se le ha asignado equipos extra para la nueva red, tanto la Dirección como las Áreas se estructuran en los siguientes departamentos:

- Financiero.
- RRHH y Administración.
- Epidemiología

- Inspección

Como mencionamos en la tabla 3.1 los equipos con los que cuenta actualmente la DPSL y sus Áreas son:

TABLA 3.14. Equipos disponibles en la DPSL.

AREA	CIUDAD	TOTAL
DPSL	Loja	95
1	Loja	15
2	Loja	20
3	Loja	20
4	Catamayo	17
5	Cariamanga	17
6	Amaluza	20
7	Macará	17
8	Catacocha	14
9	Alamor	17
10	Saraguro	12
11	Gonzanamá	12
12	Vilcabamba	12

Como mencionamos con el diseño de la nueva red se necesitará implementar más equipos ya que la vpn consume recursos: consumo de ancho de banda, nuevas aplicaciones, futuros servicios como VoIP, mayor seguridad, etc.

Para solventar esto, se plantea el siguiente equipamiento, tomando en consideración los costos mínimos y el rendimiento básico para una red eficiente y rápida, además se considera el aumento de 4 equipos por Área que es el aumento durante un periodo de 10 años para la escalabilidad y se toma en cuenta la asignación de las direcciones IP de acuerdo a los

equipos que necesitan IP, el número total de quipos tanto adicionales como los que cuenta la DPSL y sus Áreas se muestra a continuación:

TABLA 3.15. Equipos necesarios para la red en la DPSL.

AREA	CIUDAD	PC's	SWITCH CAPA 2	ROUTER	SERVIDOR	EQUIPOS	TOTAL
DPSL	Loja	91	1	2	3	95	100
1	Loja	18	1	1	1	20	24
2	Loja	18	1	1	1	20	24
3	Loja	18	1	1	1	20	24
4	Catamayo	15	1	1	1	17	21
5	Cariamanga	15	1	1	1	17	21
6	Amaluza	18	1	1	1	20	24
7	Macará	15	1	1	1	17	21
8	Catacocha	14	1	1	1	16	20
9	Alamor	15	1	1	1	17	21
10	Saraguro	12	1	1	1	14	18
11	Gonzanamá	12	1	1	1	14	18
12	Vilcabamba	10	1	1	1	12	16

La intranet debe tener capacidad para futuros equipamientos de VoIP; en el peor de los casos si consideramos teléfonos IP por cada equipo conectado a la red tendremos que adicionar direcciones IP para los teléfonos, con esta nueva estructura el total de equipos por cada Área es la siguiente:

TABLA 3.16. Direcciones IP necesarias

AREA	CIUDAD	TOTAL EQUIPOS	TELEFONOS IP	TOTAL DIRECCIONES
DPSL	Loja	99	90	190
1	Loja	24	18	42
2	Loja	24	18	42
3	Loja	24	18	42
4	Catamayo	21	15	36
5	Cariamanga	21	15	36
6	Amaluza	24	18	42
7	Macará	21	15	36
8	Catacocha	20	14	34
9	Alamor	21	15	36
10	Saraguro	18	12	30
11	Gonzanamá	18	12	30
12	Vilcabamba	16	10	26

Con la estructura física planteada, se solicitarían al ISP por cada Área direcciones públicas de clase C, y se utiliza direcciones privadas para la intranet; el número de direcciones físicas necesarias son las mostradas a continuación:

TABLA 3.17. Direcciones públicas solicitadas al ISP.

ÁREA	TOTAL	CLASE
DPSL	10	C
1	5	C
2	5	C
3	5	C
4	4	C
5	4	C
6	5	C

7	4	C
8	3	C
9	4	C
10	3	C
11	3	C
12	3	C

Para el direccionamiento de la red internamente se presenta el siguiente diseño a continuación:

Numero de subredes=13

Dirección IP = 192.168.0.0/ clase C

2^8-2=254

Mascara=255.255.255.0

TABLA 3.18. Intervalo de direcciones IP por Área.

ÁREA	DIRECCIONES IP	
DPSL	192.168.0.0	192.168.0.255
1	192.168.1.0	192.168.1.255
2	192.168.2.0	192.168.2.255
3	192.168.3.0	192.168.3.255
4	192.168.4.0	192.168.4.255
5	192.168.5.0	192.168.5.255
6	192.168.6.0	192.168.6.255
7	192.168.7.0	192.168.7.255
8	192.168.8.0	192.168.8.255
9	192.168.9.0	192.168.9.255
10	192.168.10.0	192.168.10.255
11	192.168.11.0	192.168.11.255
12	192.168.12.0	192.168.12.255

3.4.2 VLSM

Para mayor aprovechamiento de la dirección IP y para crear subredes dentro la red se especifica de acuerdo al número de host utilizados, y para cada subred tenemos:

TABLA 3.19. Host por Área.

AREA	TOTAL
DPSL	190
1	42
2	42
3	42
4	36
5	36
6	42
7	36
8	34
9	36
10	30
11	30
12	26

TABLA 3.20. VLSM

ÁREA	TOTAL	RANGO DIRECCION IP		
DPSL	190	192.168.0.0	192.168.0.255/24	2^n= 256→n=8
1	42	192.168.1.0	192.168.1.63/26	2^n= 64→n=6
2	42	192.168.1.64	192.168.1.127/26	2^n= 64→n=6
3	42	192.168.1.128	192.168.1.191/26	2^n= 64→n=6
4	36	192.168.1.192	192.168.1.255/26	2^n= 64→n=6
5	36	192.168.2.0	192.168.2.63/26	2^n= 64→n=6
6	42	192.168.2.64	192.168.2.127/26	2^n= 64→n=6
7	36	192.168.2.128	192.168.2.191/26	2^n= 64→n=6
8	34	192.168.2.192	192.168.2.255/26	2^n= 64→n=6
9	36	192.168.3.0	192.168.3.63/26	2^n= 64→n=6
10	30	192.168.3.64	192.168.3.95/27	2^n= 32→n=5
11	30	192.168.3.96	192.168.3.127/27	2^n= 32→n=5
12	26	192.168.3.128	192.168.3.159/27	2^n= 32→n=5

A continuación se muestra el direccionamiento para las LAN, especificando la dirección de red, máscara, el rango, dirección de la puerta de enlace, direcciones para administración:

TABLA 3.21. Direccionamiento IP LANs

AREA	DIRECCION DE RED	MASKARA	GATEWAY INTERFACE SERIAL	DIRECCIONES ADMINISTRIVAS	
DPSL	192.168.0.0	255.255.255.0	192.168.0.1	192.168.0.253	190.168.0.254
1	192.168.1.0	255.255.255.192	192.168.1.1	192.168.1.61	192.168.2.62
2	192.168.1.64	255.255.255.192	192.168.1.65	192.168.1.125	192.168.1.126
3	192.168.1.128	255.255.255.192	192.168.1.129	192.168.1.189	192.168.1.190
4	192.168.1.192	255.255.255.192	192.168.1.193	192.168.1.253	192.168.1.254
5	192.168.2.0	255.255.255.192	192.168.2.1	192.168.2.61	192.168.2.62
6	192.168.2.64	255.255.255.192	192.168.2.65	192.168.2.125	192.168.2.126
7	192.168.2.128	255.255.255.192	192.168.2.129	192.168.2.189	192.168.2.190
8	192.168.2.192	255.255.255.192	192.168.2.193	192.168.2.253	192.168.8.254
9	192.168.3.0	255.255.255.192	192.168.3.1	192.168.3.61	192.168.3.62
10	192.168.3.64	255.255.255.224	192.168.3.65	192.168.3.93	192.168.3.94
11	192.168.3.96	255.255.255.224	192.168.3.97	192.168.3.125	192.168.3.126
12	192.168.3.128	255.255.255.224	192.168.3.129	192.168.3.157	192.168.3.158

3.4.3 VLAN

Dentro de las subredes es necesario la comunicación por departamento, por área, por ejemplo en un área de Salud, el departamento de Inspección es independiente de las otras Áreas, por esta razón y por mayor seguridad se ha segmentado la dirección IP para implementar *vlans basadas en la dirección de red.*

Dirección IP privada = 192.168.0.0 clase C

TABLA 3.22. VLAN.

ÁREA	VLAN	EQUIPOS	RANGO	
DPSL	VLAN Financiero	44	192.168.0.0	192.168.0.63/26
	VLAN RRHH	50	192.168.0.64	192.168.0.127/26
	VLAN Epidemiologia	48	192.168.0.128	192.168.0.191/26
	VLAN Inspección	48	192.168.0.192	192.168.0.255/26
1	VLAN 1	42	192.168.1.0	192.168.1.63/26
2	VLAN 2	42	192.168.1.64	192.168.1.127/26
3	VLAN 3	42	192.168.1.128	192.168.1.191/26
4	VLAN 4	36	192.168.1.192	192.168.1.255/26
5	VLAN 5	36	192.168.2.0	192.168.2.63/26
6	VLAN 6	42	192.168.2.64	192.168.2.127/26
7	VLAN 7	36	192.168.2.128	192.168.2.191/26
8	VLAN 8	34	192.168.2.192	192.168.2.255/26
9	VLAN 9	36	192.168.3.0	192.168.3.63/26
10	VLAN 10	30	192.168.3.64	192.168.3.95/27
11	VLAN 11	30	192.168.3.96	192.168.3.127/27
12	VLAN 12	26	192.1688.3.128	192.168.3.159/27

3.4.4 DIAGRAMA GENERAL DE LA RED.

Para la red VPN se usa la arquitectura sitio a sitio (LAN to LAN), para la VPN es necesario un Gateway VPN que se instale en el borde de cada red para realizar el túnel, el modelo de entunelamiento es END to END (Servidor a Servidor) que se da en las capas superiores, aquí el host inicia el túnel y el servidor VPN se encarga de negociar con el host para iniciar el servicio.

En cada LAN un switch conecta a la red, no se utiliza el protocolo STP (Spanning Tree Protocol) porque no hay conexiones redundantes con otros switchs, el servidor de cada LAN se conecta al switch y pasa al ruteador o Gateway para enviar la señal a través de un modem de la empresa ISP al internet.

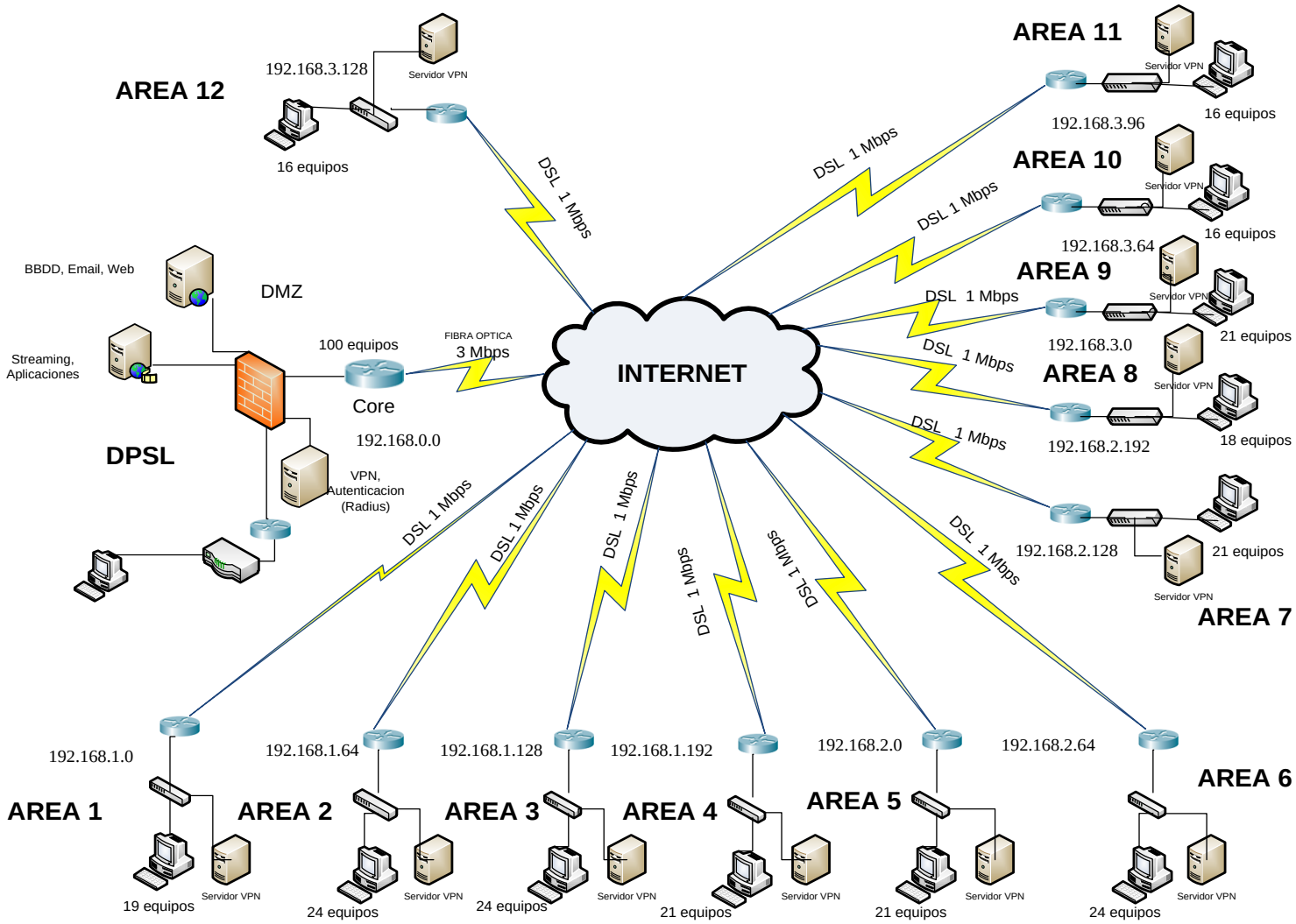


Figura 3.5. Diagrama General de la red.

CAPÍTULO 4

4. ALTERNATIVAS TECNOLÓGICAS VPN.

4.1. TECNOLOGÍAS VPN

Las formas en que pueden implementar las VPNs pueden ser basadas en HARDWARE o a través de SOFTWARE, pero lo más importante es el protocolo que se utilice para la implementación.
Se puede crear VPN's usando tecnologías de la capa 2 y 3 del modelo OSI, es decir, en la capa de enlace y red de datos o combinando ambas capas:

Implementaciones de capa de Enlace.- pueden tunelizar cualquier tipo de paquetes, permite transferencias sobre protocolos no-IP, dentro de esta categoría están: PPTP, L2TP, L2F.

Implementaciones de capa de Red.- IPSec es la tecnología más aceptada en este punto y fue desarrollada como un estándar de seguridad de Internet en esta capa.

Existe además la tecnología MPLS, que esta implementada en las dos capas de enlace y de red.

A continuación se presentan características principales de estos protocolos para seleccionar la mejor tecnología que se ajuste a las necesidades de la DPSL y al presente proyecto:

4.1.1 PPTP (Point to Point Tunneling Protocol):

Es un protocolo de red que permite el tráfico seguro en una red VPN basada en TCP/IP, PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y desencriptados de acuerdo al protocolo de red transmitido.

Soporta múltiples protocolos de red como son: IP, IPX, NETBEUI. PPTP puede ser aplicado de acuerdo al tipo de conexiones, este se basa en conexiones punto a punto. Es un protocolo desarrollado por Microsoft pero en Linux hay soporte para vpns bajo protocolo PPTP gracias al proyecto POPTOP, encargado de la creación del programa PPTPD que es el que se puede usar para crear una vpn.

PPTP ofrece autenticación de usuarios a través de PAP y CHAP, En cuanto a la encriptación de datos, PPTP utiliza el proceso de encriptación de secreto compartido en el cual sólo los extremos de la conexión comparten la clave y puede usar cortafuegos y routers.

4.1.2 L2F (Point to Point Tunneling Protocol):

Protocolo desarrollado por Cisco, a diferencia del PPTP el protocolo L2F no depende de IP con lo cual es capaz de trabajar bajo otros protocolos y en diferentes medios como Frame Relay o ATM, permite que los dispositivos remotos accedan a la red TCP/IP de la organización, a través de internet con seguridad, proporciona un mecanismo de túnel para envía tramas a nivel de enlace, el protocolo que utiliza para la autenticación de usuario remoto es el PPP, además implementa TACAS (Terminal Access Controller Access Control System) y RADIUS (Remote Authentication Dial-In User Service).

4.1.3 L2TP (Point to Point Tunneling Protocolo):

Es una extensión del protocolo Punto a Punto, tiene casi la misma funcionalidad que PPTP, es fundamental para la creación de VPNs. L2TP combina las mejores funciones de los otros dos protocolos tunneling Layer 2 Forwarding (L2F) de Cisco Systems y Point-to-Point Tunneling (PPTP) de Microsoft.

Dado que L2TP es un protocolo de capa 2, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI, y también ofrecen un acceso seguro a su sistema o red cuando las utilice conjuntamente con IPSec.
Un sistema VPN basado en L2TP se basa en una red con tres nodos principales: el nodo de partida donde está el usuario que va a enviar los datos, un nodo final o destino, y un nodo intermedio encargado de transmitir los datos del usuario fuente al nodo de destino,
Esta comunicación es mediante el uso de una o varias redes públicas.

4.1.4. SSL (Secure Socket Layer):

Es un protocolo usado para establecer comunicación segura entre un Servidor y un Cliente porque permite que la información viaje encriptada, es decir, sus comunicaciones en Internet serán transmitidas en formato codificado que no podrá ser propensa a ataques.

Opera en la capa de transporte y en la de sesión del modelo OSI. Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP. Cifra los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA.

4.1.5. SSH (Secure Shell):

Es un protocolo de red y conjunto de estándares, que permite comunicación encriptada entre computadoras. Usa criptografía de clave publica para la autenticación de usuarios, y para la autenticación usa algoritmos RSA y DSA, con SSH se puede acceder a una maquina remota similar a telnet, SSH utiliza un modelo cliente/servidor, tiene una arquitectura de capas.

4.1.6. IPSec (Seguridad IP)

Define la seguridad en la capa de Red del modelo OSI, esta descrito en el RFCs 2401, 2402 y 2406, es un protocolo que tiene simplicidad, es fácil de implementarlo y de gran velocidad. Con este protocolo obtenemos confidencialidad, integridad de los datos y se basa en criptografía simétrica, posee también gran flexibilidad cuando se requiere personalizar las aplicaciones ya que trabaja en la capa de red.

IPSec es un conjunto de protocolos que da varios servicios de seguridad y estos servicios trabajan gracias a dos protocolos, el Authentication Header (AH) y el Encapsulating Security Payload (ESP), y también al uso de protocolos y procedimientos para el manejo de llaves criptográficas tales como IKE (Internet Key Exchange Protocol).

Este protocolo es orientado a la conexión, y opera en dos posibles modos: Modo Transporte o Modo Túnel. En el **modo transporte** se emplea sobre los equipos terminales, sin modificar la cabecera original del paquete.

Y puede utilizarse en el **modo túnel** esto es útil cuando tenemos varias conexiones TCP y se mantiene un flujo cifrado, así se evitaría ataques de hackers ya que no se sabe quien envía y cuantos paquetes, este modo permite definir un túnel entre dos enrutadores, los túneles IPSec se establecen dinámicamente y se liberan cuando no están en uso, Así, mientras que en el

modo transporte sólo se encriptan los datos, en el modo túnel se encripta la cabecera IP original.

La desventaja de este protocolo es el incremento del tamaño de los paquetes porque se agrega un encabezado IP a todo el paquete, es decir su complejidad, ya que contiene demasiadas opciones.

4.1.7. MPLS (Multiprotocol Label Switching):

Conmutación de Etiquetas Multiprotocolo, es una tecnología innovadora a través de la más moderna tecnología disponible en el mercado, el servicio de red MPLS establece túneles VPN dedicados a la comunicación de su empresa entre filiales, socios comerciales y la matriz a bajo costo de propiedad, se usa mas para comunicar grandes zonas geográficas porque utiliza grandes anchos de banda.

Es un método para enviar paquetes a través de una red usando información contenida en etiquetas añadidas a los paquetes. Combinando los beneficios del envío de paquetes basado en conmutación de Nivel 2, con los beneficios del enrutamiento de Nivel 3.
Esta tecnología puede trabajar con Internet, ATM, FRAME RELAY dando como ventaja tener redes mixtas, añadiendo QoS para optimizar los recursos de la red. Permite aprovechar las posibilidades de ingeniería de tráfico para las poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación…), lo que es necesario para un servicio completo VPN.

4.1.8. COMPARATIVA ENTRE TECNOLOGÍAS VPN

TABLA 4.1. Comparativa entre tecnologías de vpn.

TECNOLOGIA	PUNTOS FUERTES	PUNTOS DEBILES
PPTP	- Proporciona una capacidad multiprotocolo. - Integración con IPSec	- Precisa un servidor NT como terminador del túnel. - Esta siendo sustituido por el L2TP, ya no se utiliza porque la IETF no lo reconoció como estándar.
L2F	- Proporciona el tunneling multiprotocolo. - Soportado por la gran mayoría de fabricantes.	- No hay encriptación - No hay control de flujo en el túnel - Seguridad débil.
L2TP	- Combina L2F y PPTP. - Necesidad de únicamente una red de paquetes para operar bajo X.25 y Frame Relay.	- Da problemas la definir una encriptación estándar.
IPSEC	- Subconjunto de Ipv6. - Transparente a aplicaciones (por debajo de la capa de Transporte). - Provee seguridad para usuarios individuales.	- No estandarizado - No hace gestión de usuarios. - Protocolo complejo que requiere una configuración complicada. - Puede afectar el rendimiento en recursos del CPU. - Requiere la instalación de software cliente
SSL	- No es necesario instalar software cliente para la vpn.	- No se usa para conexiones red a red. - Funciona a través de un servidor NAT. - No da seguridad en la

		estación de trabajo. - No se ajusta a unir redes completas sino al modelo negocio/cliente. - No trabaja bien con gateways.
SSH	- Simplicidad de implementación - Todos los datos que se envían en una conexión son cifrados.	- No soporta UDP y solo por TCP tuneliza.
MPLS	- Las capacidades más relevantes son: Calidad de servicio QoS, soporte multiprotocolo. - Permite transportar diferentes tipos de tráfico IP, incluyendo tráfico de voz y datos - fácil de configurar y administrar. - Soporta multicast	- Puede crear tunneles IP a través de la red sin necesidad de encriptación o aplicación en el usuario final lo que es propensa a ataques. - No se pueden mantener los vínculos en Internet entre etiquetas MPLS y los hosts.

4.1.9 Tecnología propuesta

Hemos presentado todas las tecnologías empleadas para las VPN, pero analizando estas tecnologías se ajusta a este proyecto los protocolos SSL/TLS, más populares y flexibles actualmente, posee métodos flexibles de autenticación para los clientes basados en certificados.

Para proteger la comunicación en la capa de transporte se propone el protocolo SSL, la implementación es más flexible y menos compleja que la tecnología IPSec, además es uno de los mecanismos que goza de gran experiencia, una ventaja de usar SSL es la ayuda técnica en línea, capacitación y manuales, porque SSL usa OpenVpn que es un proyecto que se mantiene en desarrollo.

La seguridad de estos protocolos son de doble capa:

- Autenticación basada en certificados x509 SSL/TLS
- Autorización por usuario y contraseña (PAM, LDAP)

Esta tecnología es ideal para conectar dispositivos wifi, móviles a la intranet, no requiere utilizar hardware adicional y su implementación es fácil, además existen gran cantidad de información relacionada a SSL mientras que IPSEC no ha evolucionado rápidamente en software como SSL.
Para este prototipo por motivos de demostración y no implementación se utilizará el software OpenVPN por su facilidad y sencillez, pero por la principal razón que solo conectará la intranet y no afectará el desempeño del software.

4.2. PROTOCOLOS

4.2.1 PROTOCOLOS PARA LAS REDES LAN

4.2.1.1 Protocolo para gestión remota a los ruteadores de las redes LAN

Los ruteadores permiten manejar los protocolos HTTP, SNMP y TELNET, de manera que puede el Administrador de la red configurarlos, diagnosticar problemas de la red, gestionar el control de la red de manera remota, el SNMP es un protocolo sencillo que permite manejar problemas relacionados con la administración de las redes.

4.2.2. PROTOCOLO PARA LA RED WAN

4.2.2.1 PROTOCOLO TCP/IP

La red propuesta está basada en el estándar universal de transporte de red llamado TCP/IP, en el modelo OSI de siete capas de comunicaciones de red, el IP es la tercera capa y el TCP es la cuarta capa. TCP/IP es un protocolo orientado a la conexión para asegurar un flujo de bytes rápido, confiable y garantizado proporcionando una conexión confiable de extremo a extremo en una red no confiable e insegura como es el Internet.

Una parte muy importante de este proyecto es la seguridad ya que el internet está sujeto a múltiples ataques e inseguridades; se pretende conectar el servidor a la red pública mediante un servidor VPN con sus respectivas claves asimétricas y certificados.

Este servidor también permite conectar los VPN basados en clientes, esto significa que los que quieran acceder a la intranet, puedan mantener la seguridad y confidencialidad de la información.

4.2.3 PROTOCOLOS PARA LA VPN

Utilizando el método túnel y considerando las características especificadas en los puntos anteriores la opción más óptima es SSL/TLS

Es un buen protocolo de seguridad especialmente para las VPN's y para acceso de usuarios remotos a redes privadas, este funciona bajo la capa de transporte lo que lo hace transparente a los usuarios, otra fortaleza de este protocolo es su flexibilidad que simplifica su instalación y funcionamiento a través de cualquier red IP.

4.3. SEGURIDAD

Asegurar una red es un reto dinámico y no estático. Toda la seguridad representa un balance que actúa entre la protección contra amenazas de seguridad potenciales y el no saturar la red porque afectaría a su desempeño.

Para este proyecto se plantea la siguiente tecnología para dar mayor seguridad a la intranet y que sea acorde al presupuesto de la DPSL:

4.3.1. TUNNELING

Con la tecnología de túneles (tunneling) los paquetes se encapsulan dentro de un protocolo de comunicaciones y al llegar a su destino, el paquete original es desempaquetado a su estado de origen.

En el traslado a través de Internet, como los paquetes viajan encriptados, por este motivo, las técnicas de autenticación son esenciales para el correcto funcionamiento de las VPNs, ya que se asegura que el emisor y receptor intercambien información con el usuario o dispositivo correcto.

Es tan importante la encriptación como la autenticación, ya que permiten proteger los datos transportados de ser interceptados en el viaje de un extremo a otro de la conexión.

Conexión por Túnel con SSL:

Con este esquema que autentifica y encripta individualmente paquetes IP, la red está segura, el tráfico de la red está protegido por tun/tup se encargan de levantar y encapsular los paquetes solo en una parte del trayecto entre el equipo de origen y el de destino, esto es cuando atraviesa el internet que no es una red de confianza.

Para que el tránsito de información sea seguro, el sistema de red privada virtual actúa a través de dos mecanismos simultáneos de seguridad adicional:

- Certificados
- Encriptación.

4.3.2. CERTIFICADOS

Un certificado permite asociar una clave pública con una entidad (una persona, un equipo, etc.) para garantizar su validez. Mediante un certificado de seguridad cualquier información enviada al servidor es encriptada, imposibilitando su intercepción o robo.

Un certificado VPN se lo instala en un equipo de red para cifrar la comunicación entre los clientes que tienen su certificado y el certificado servidor, el equipo también usa un certificado especial IPSec.

Hay diferentes tipos de certificados como:

- Certificados de Servidor (SSL)
- Microsoft Server Gated Cryptography Certificates

- Certificados Canalizadores.
- Certificados de Correo Electrónico.
- Certificados de Valoración de páginas WEB.
- Certificados de Sello, Fecha y Hora

Y protocolos de certificación así tenemos:

- SET (Secure Electronic Transaction)
- PGP (Enterprice Security)
- SSL (Secure Socket Loyout)

Autoridad Certificadora (CA).- son empresas dedicadas a vender certificados de seguridad, la entidad de certificación es responsable de emitir los certificados, tiene autoridad de poner fecha de validez y de revocarlos antes de esta fecha en caso de que la clave (o su dueño) estén en una situación de riesgo. Ejemplos de estas tenemos: Verisign, Thawte, beTRUSTed o ValiCert, etc., estos ya están presentes en los navegadores.

El Tipo de certificado que se puede utilizar para la intranet es Certificados de servidor SSL utilizando el respectivo protocolo, estos certificados X.509 están para que protejan los datos que viajan por el internet y son previamente firmados por una autoridad certificadora.

La base de esta tecnología reside en los códigos secretos osea en la "encriptación".

4.3.3. ENCRIPTACION

Es el proceso de codificación de datos que sirve para prevenir accesos no autorizados en la transmisión. La encriptación garantiza la confidencialidad, la integridad y la autenticidad de la información que se desea transmitir y que tiene gran importancia, este se lleva a cabo utilizando un algoritmo especial.

*Encriptación Simétrica.-*se basa en una clave secreta que se comparte por dos partes que están en comunicación, la clave se utiliza tanto para encriptar como para desencriptar por lo cual puede crear problemas de seguridad. Ejemplos de algoritmos de encriptación son RSA, IDEA, etc.

*Encriptación Asimétrica.-*llamada también clave pública, usa dos claves que son diferentes para cada usuario, una es la clave privada que solo conoce el usuario y la otra es la clave pública para el que va a acceder. Una clave se utiliza para la encriptación y la otra para la desencriptación. La encriptación de clave pública permite que se coloquen firmas digitales en los mensajes para identificar al emisor. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

ENCRIPTACION PROPUESTA:

En las redes virtuales, la encriptación debe ser realizada en tiempo real, de esta manera, los flujos de información encriptada a través de una red lo son utilizando encriptación de clave secreta con claves que son válidas únicamente para la sesión usada en ese momento.

Mediante OpenVPN la encriptación es asimétrica, envía paquetes encriptados vía TCP, es basado en los protocolos SSL/TLS usando certificados y claves RSA para su cifrado asimétrico, depende de OpenSSL, por lo cual también puede usar cualquiera de los cifrados de algoritmos disponible por esa biblioteca.

4.3.4. AUTENTICACIÓN

Verifica si el emisor es quien dice realmente ser, asegurando la privacidad e integridad de las comunicaciones, es similar al logeo en un sistema como nombre de usuario y contraseña, pero con mayor necesidad de validación de las identidades, se lleva a cabo en un inicio de sesión pero también durante el curso

de la misma para comprobar que no haya ningún usuario extraño metido en la conversación.

Una variedad de métodos de autenticación hay disponibles de acuerdo a las necesidades de las VPN entre estos tenemos: uso de claves o passwords, Radius, LDAP, certificados digitales, incluso aquellos que involucran hardware como son las tarjetas inteligentes.

El método de autenticación empleado en este proyecto es mediante claves o passwords y certificados digitales, aunque no es tan recomendable estos métodos son lo más económico y se ajusta a la tecnología empleada, teniendo en cuenta el costo de adquisición de un servidor Radius extra, o comprar software adicional.

4.3.5. FILTRACIÓN

El administrador otorga permisos a los usuarios y determina que usuarios utilicen los servicios de la intranet. Las reglas del cortafuegos se aseguran de que ambas máquinas tanto cliente como servidor sólo acepten datos provenientes del túnel. Esto significa que los paquetes insertados directamente dentro de la WLAN por algún cracker malintencionado serán inofensivos. Se puede aplicar filtros a las puertas de entrada del servidor VPN o a las puertas de salida de este.

A ambos lados del túnel, OpenVPN recoge los paquetes destinados al otro lado, y usando una clave local encripta los paquetes antes de enviarlos. En el punto de recepción tan solo se aceptarán datos que hayan sido encriptados usando la clave válida. Cualquier otro paquete se ignorará. Con esta solución los datos se transportan en contenedores seguros a través de ambientes hostiles.

4.3.6. FIREWALL

Firewall (cortafuegos).-es un sistema de defensa que protege a la intranet de otros usuarios no autorizados o intrusos. Es un filtro que controla todas las comunicaciones dependiendo de que se autoriza o se niega su paso para entrar a la intranet, puede ser un dispositivo software o hardware.

Colocar el firewall al frente de un servidor VPN sobrecarga al servidor porque tiene que analizar los paquetes, para este proyecto lo ideal es una sola máquina que dirige el tráfico VPN a su destino específico y dirige el resto del tráfico que recibe el servidor al firewall para ser analizado, el firewall va ser instalado en el servidor web, este enfoque es el más económico y se recomienda para la intranet.

Varios firewall que cumplan con las características de software libre, fáciles de instalar, administración remota hay en el mercado de entre estos tenemos:

- CensorNet,
- Devil-Linux,
- Ipcop,
- Endian,
- Smoothwall,
- Etc.

Las máquinas clientes ya vienen incorporado firewall si estas utilizan sistemas operativos Windows así controlan la salida de la información a la intranet, caso contrario se debe instalar cualquiera de estos programas de código abierto, en los sistemas operativos Linux, este proyecto utiliza estos dos tipos de Sistemas operativos.

Cada servidor debe tener herramientas de monitoreo instaladas para monitoreo, herramientas de diagnóstico de red, para que alertas del mantenimiento del sistema puedan ser generadas antes de que las fallas ocurran, por ejemplo tenemos: tcp- wrappers, Netlog, Udploggers, nstat, etc. El servidor principal

contendrá una herramienta de software que proporcione datos sobre la confiabilidad de la red.

Los switch y ruteadores ya tienen incorporado firewall, en estos equipos en pueden filtrar puertos y tráfico en las LAN para todas las estaciones de trabajo mediante configuración de ACL, VLANs, y los protocolos que manejan estos dispositivos.

4.3.7 POLITICAS DE SEGURIDAD

Mantener la red segura requiere de varias estrategias que consiste en políticas empleadas por la Institución, es importante implementar un conjunto de estas políticas que sirvan de guía para todo el personal.

Políticas del uso del internet:

Se debe elaborar un conjunto de políticas para que el usuario use debidamente este servicio y no ponga en riesgo la información de la institución, ejemplos de estas políticas tenemos:

- Acceder solo a la información para con fines laborales.
- Restringir el acceso a ciertas páginas con información prohibida.
- Evitar poner a disposición materiales no permitido a los otros empleados
- Etc.

Políticas del uso del Correo electrónico:

Al no tener políticas establecidas para el uso del correo electrónico desde y hacia la Dirección, el usuario puede enviar correos de cualquier índole, los usuarios deben acatar las disposiciones que implanta la Dirección, dentro de estas políticas tenemos:

- Protección de las claves del correo.
- Evitar la difusión masiva de mensajes, especialmente publicidad no solicitada.
- No enviar envíos de contenidos ilegales.
- Mantenimiento o cambio de la contraseña de la Institución. Etc.

Políticas de Administración de la red:

Para aquí se presenta ejemplos de qué políticas de seguridad puede implementar el Administrador de la red para protegerla:

- Debe conceder los mismos permisos a los usuarios que desempeñan el mismo rol en todas las Áreas, por ejemplo todo el personal de Epidemiologia tiene el mismo privilegio.
- Mantener respaldos periódicos de las bases de datos en función de su importancia y actualización.
- Ofrecer los servicios de la intranet para los que ha sido creada.
- Además de las herramientas criptográficas, debe haber control y vigilancia contínua por parte de los responsables de la red.
- Fijar la política de que usuarios deben poseer correo electrónico, y el tipo de permisos del correo electrónico, tales como correo externo, correo entrante, saliente, tipo de archivos a recibir, tipo de archivos a enviar.
- Limitar el uso de herramientas de mensajera instantánea.
- Limitar el uso de Internet a usuarios que no deben utilizarlo.
- Fijar horarios de uso del Internet para los usuarios que deban utilizarlo.
- Etc.

CAPÍTULO 5

5. DISEÑO DE LA RED VoIP PARA UN ENTORNO LINUX.

En este proyecto se utilizarán las ventajas e infraestructura de las redes privadas de los centros de salud y la intranet para realizar el diseño de la red VoIP, cada teléfono tendrá su propia dirección IP ya establecida anteriormente.

Una alternativa de solución propuesta para VoIP en el siguiente proyecto es utilizar la centralilla telefónica ASTERISK.

Asterisk es una aplicación de software libre que implementa los servicios de una centralita telefónica de VoIP. A la centralita se le pueden conectar teléfonos de VoIP (que también pueden ser programas de ordenador o “softphones”), fax, líneas RDSI, líneas telefónicas analógicas convencionales.

La técnica de conmutación se realiza de paquetes.

Dentro de sus características tenemos:

- Música en espera.
- Buzón de voz.
- Informes de tráfico.
- Clave por anexo.
- Grabado de todas las llamadas, entrantes y salientes.
- Envío de mensajes de voz a correo electrónico.
- Uso de cableado CAT 5 estructurado existente.
- Teléfonos de software.
- Anexos extendidos entre sucursales.
- Condiciones de horario para reproducir mensajes.
- Panel WEB de actividad.
- Colas de llamados, para ventas, soporte u otros departamentos de su compañía.

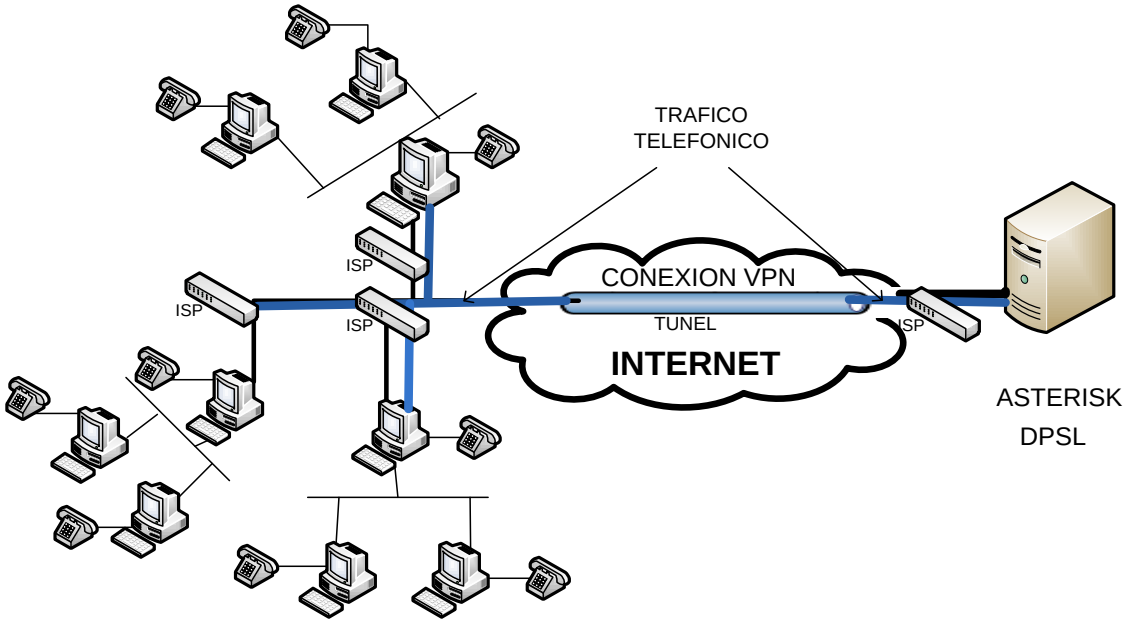


Figura 5.1. Red VoIP

5.1 PROTOCOLO DE VOIP

SIP.- (Session Initiation Protocol) Es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet, la comunicación es entre pares, es parecido al protocolo HTTP, es basado en texto, además muy abierto y flexible. Consecuentemente ha reemplazado el estándar H323. Este protocolo es abierto, porque no está amarrado a ningún proveedor de hardaware ni de software por lo que hoy en día en el mercado existen diversos fabricantes que está produciendo estos productos a precios realmente muy bajos.

5.2 COMPONENTES BASICOS PARA LA RED VoIP.

Entre los componentes especializados para el diseño de la red propuesta mencionamos:

- Servidor
- PBX
- Codecs.
- Gatekeeper
- Gateway
- Teléfono

Los codecs que soporta Asterisk son:

- G.711
- GSM
- G.729
- iLBC
- Speex

SERVIDOR ASTERISK

TABLA 5.1. Características del servidor Asterisk

Marca	Hewlett-Packard
Serie	ML150 G6
Nombre	HP ProLiant ML150G6
Procesador	QuadCore Xeon E5504 (4.00 GHz)
Cache	8 MB L2
Memoria	2 GB

GATEWAY

El gateway permite interconectar la telefonía tradicional con la telefonía por IP, lo que permite integrar con la red telefónica pública con interfaces analógicos o enlaces digitales, el Gateway propuesto servirá para conectar la centralilla existente en la DPSL y esta tiene las siguientes características:

TABLA 5.2. Características del gateway

Marca	CISCO
Serie	SPA3102
Nombre	CISCO SPA3102 VOICE GATEWAY WITH ROUTER
Puertos	1 FXO Y 1 FXS

5.3 EQUIPOS TERMINALES

Los equipos terminales pueden ser teléfonos IP, tarjetas, softphone, por los costos se pueden restringir a teléfonos IP en las áreas de atención al público y los softphones en todos los computadores conectados a la intranet.

Teléfonos IP

Los teléfonos IP son teléfonos muy similares a los tradicionales, aunque no en su precio, son aparatos telefónicos con la misma apariencia física que los teléfonos tradicionales pero utilizan tecnologías VoIP.

En lo que respecta a los teléfonos, en el diseño se implementaría un teléfono por cada PC conectada, debido a los costos y a la estructura actual de la DPSL y

sus Áreas de salud, solo se prevee un teléfono IP por cada departamento ya sea Financiero, RRHH y/o Administración, Epidemiología e Inspección, en los demás equipos la solución optima es el sophone X-lite.

TABLA 5.3. Equipos disponibles en la DPSL.

AREA	CIUDAD	TOTAL	Telefonos IP
DPSL	Loja	95	20
1	Loja	15	4
2	Loja	20	4
3	Loja	20	4
4	Catamayo	17	4
5	Cariamanga	17	4
6	Amaluza	20	4
7	Macará	17	4
8	Catacocha	14	4
9	Alamor	17	4
10	Saraguro	12	4
11	Gonzanamá	12	4
12	Vilcabamba	12	4

TABLA 5.4. Características de los equipos terminales

Marca	LINKSYS
Serie	SPA921
Nombre	Teléfono VoIP - SIP v2
Protocolo	SIP

Softphone

El softphone hace posible que puedas hacer llamadas a teléfonos convencionales a través de Internet, generalmente a un bajo costo, y también hacer conexiones "PC-PC" gratuitamente, que es el tipo más conocido y utilizado con respecto a llamadas VOIP actualmente, el softphone es el software que hace la simulación de teléfono en un ordenador sin necesidad de un teléfono físico lo que tiene la ventaja de ahorrar en costos en las llamadas VOIP.

El softphone que usamos es el X-Lite 2.0 o 4.0 que funciona tanto en Windows como en Linux.

Adaptadores IP

Son dispositivos (hardware) que permiten conectar un teléfono analógico a la red IP utilizando protocolos de VozIP, para reutilizar todos los teléfonos analógicos de la DPSL mediante el uso de estos adaptadores **ATA**: Analog Telephone Adapter, el caso más normal, tienen un conectr FXS para teléfono analógico normal y envían por VozIP a través del conector LAN, soportan SIP normalmente.

TABLA 5.5. Características de los adaptadors ATA.

Marca	LINKSYS
Serie	PAP2
Nombre	Adaptador VoIP
Puertos	2 puertos FXS
Protocolo	SIP

5.3 ESQUEMA DE LA RED

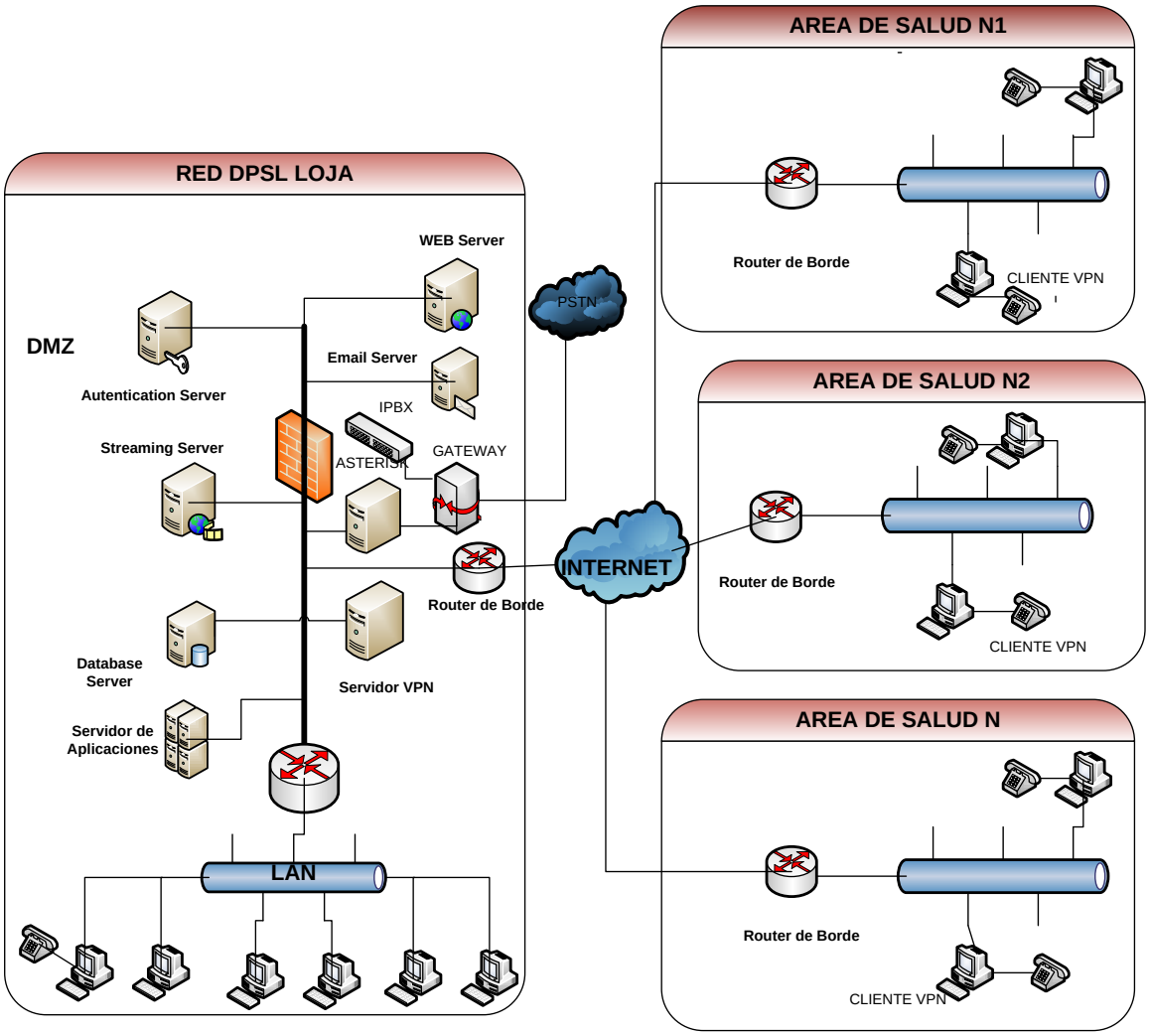


Figura 5.2 Esquema de la red VoIP.

CAPÍTULO 6

6. DESARROLLO DEL SOFTWARE DE RED.

Aquí se describirá la solución propuesta, así como el diseño que se realizó para la intranet, siguiendo las etapas de la ingeniería de software más comúnmente utilizadas iniciando en el análisis de requerimientos, luego se muestra las especificaciones a través de casos de uso, la arquitectura es mostrada mediante el modelo conceptual, la siguiente fase que sigue es la programación en donde se explica el software a utilizar, herramientas de diseño, y finalmente la documentación para hacer el manual de usuario.

6.1. ANÁLISIS DE REQUERIMIENTOS

Terminada la fase de diseño de la red, a continuación se desarrolla el prototipo para hacer pruebas, se diseña el modelo entidad-relación, modelo conceptual para las bases de datos y se especifican los requerimientos principales de los usuarios.

6.1.1 REQUERIMIENTOS DE USUARIO

Se ha realizado el análisis de toda la información que se necesita para el Área Administrativa en cuanto a las inspecciones y los servicios que se han planteado en este proyecto.

Desde el punto de vista de los usuarios tenemos los siguientes requerimientos:

6.1.1.1 Área Administrativa

- Realizar las inspecciones para la emisión de los permisos de funcionamiento.

- Enviar información como documentos, boletines, etc. a todos los empleados y trabajadores de la Dirección de Salud.
- Generar reportes de las inspecciones realizadas por los inspectores.
- Intercambio de información con las diferente Áreas.
- Mayor comunicación entre los diferentes lugares.
- Otorgar correos a todos los empleados y trabajadores.

6.1.1.2 Área Laboral.

- Registrar información de las inspecciones de cada Área.
- Interacción y comunicación entre los miembros de todas las áreas.
- Acceso a los recursos de la red como son: chat, webmail, noticias, etc.
- Mantenerse informados de todos los boletines publicados.
- Rápida localización de sus compañeros.
- Mayor colaboración y asistencia técnica entre sus miembros.
- Etc.

6.2 ESPECIFICACIÓN DE REQUISITOS

6.2.1 DEFINICIÓN DE ACTORES

TABLA 6.1. Actores de los casos de uso.

ACTOR	DESCRIPCIÓN
SERVIDOR	Otorga todos los servicios de la red.
BBDD DPSL	Base de datos perteneciente a la Dirección Provincial de Salud donde consta toda la información necesaria.
Empleado/trabajador	Persona que va a ser uso de la intranet.
Administrador	Usuario o persona que va a administrar o manejar la intranet.
Inspector	Persona encargada de realizar las inspecciones.

6.2.2 CASOS DE USO GENERALES

ADMINISTRADOR

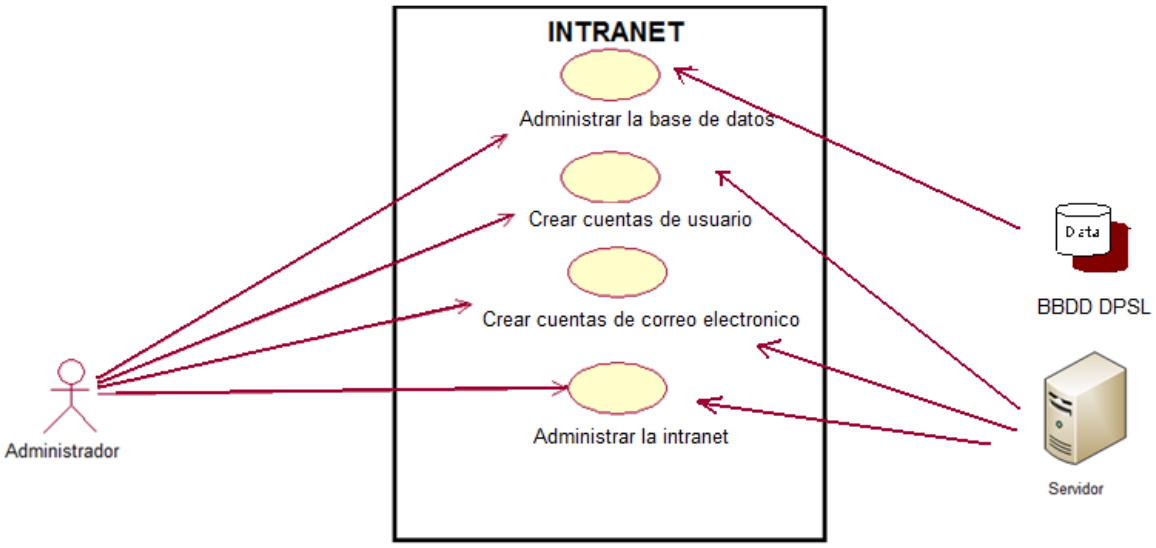


Figura 6.1. Caso de uso general Administración de la Intranet.

INSPECTOR

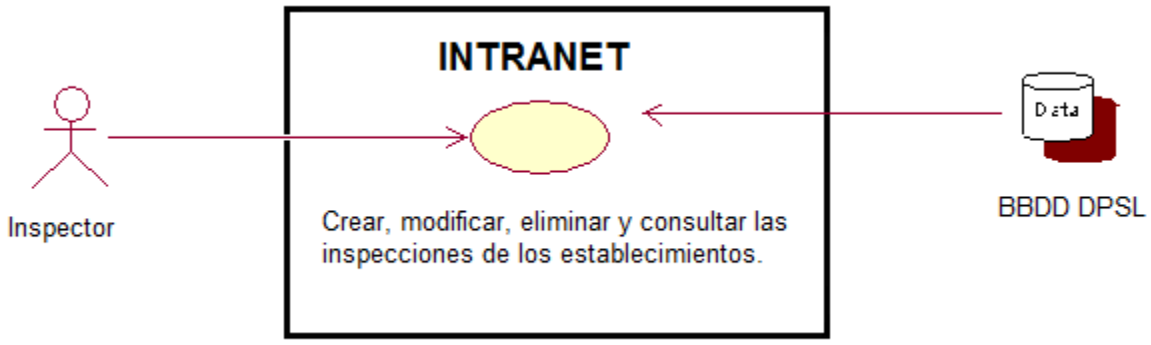


Figura 6.2. Caso de uso general Manejo de las Inspecciones.

USUARIO

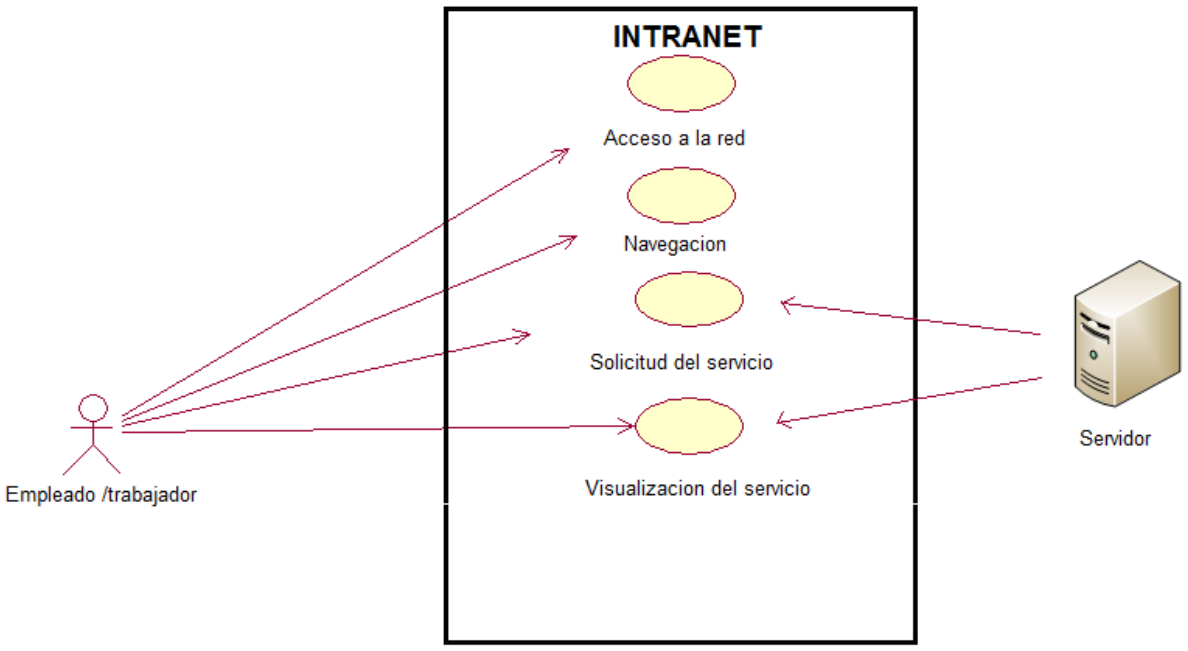


Figura 6.3. Caso de uso general Uso de los Servicios de la Intranet.

6.3 DISEÑO DE LA BASE DE DATOS

Antes de modelar la base de datos se diseñó el siguiente modelo Entidad-Relación:

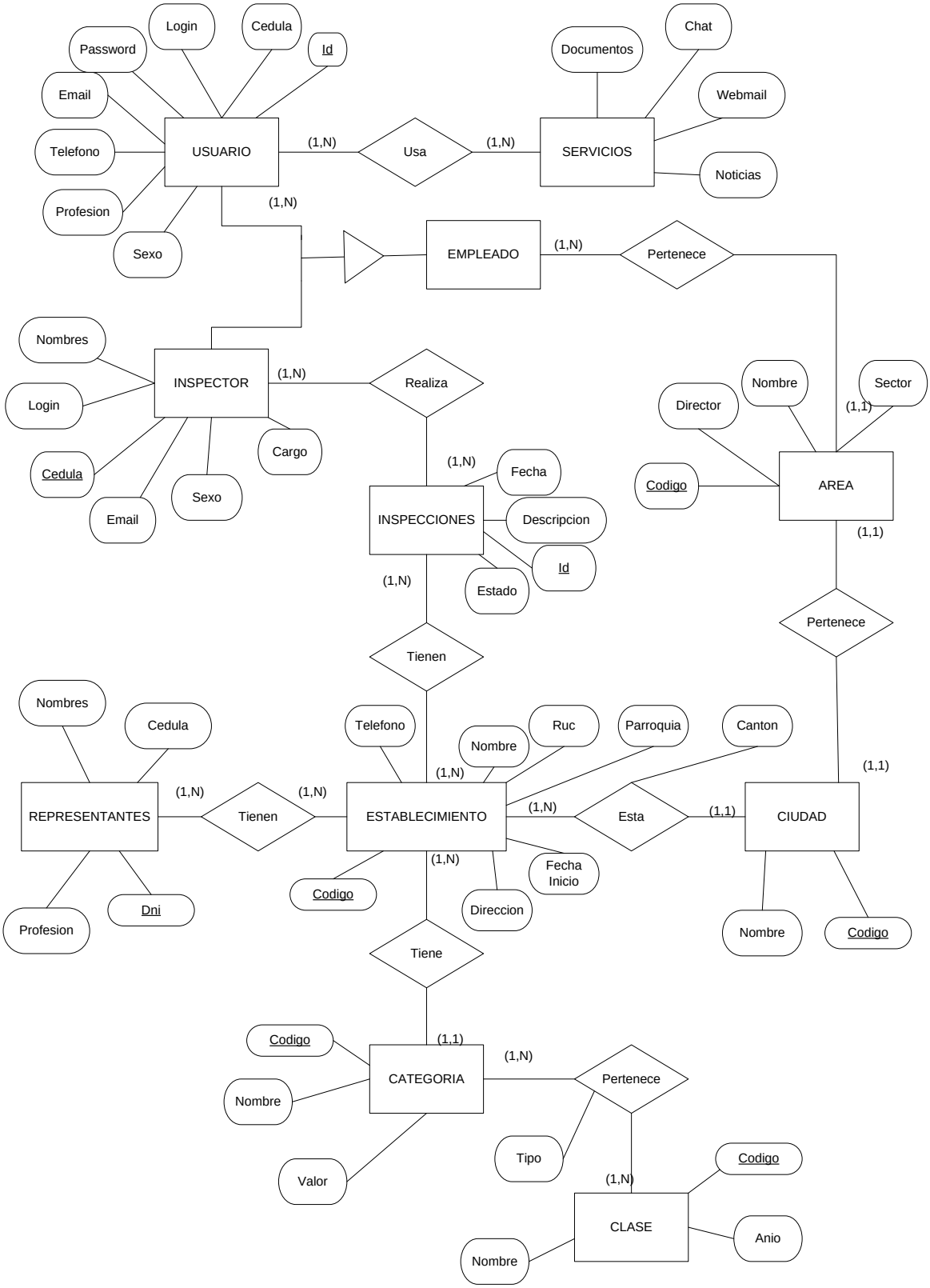


Figura 6.4. Diagrama Entidad Relacion.

Una vez realizado el análisis a través del modelo Entidad/Relacion, mediante normalización se obtuvieron los campos y tablas de la base de datos principal denominada dpsl.

La base de datos dpsl es una base centralizada ubicada en el servidor principal de la Dirección de Salud, esto es porque existe disposición del Gobierno Nacional de que los permisos de funcionamiento solo son emitidos en este lugar, pero los datos de: Inspectores, Inspecciones, Establecimientos y Representantes son propios de cada área, sin embargo no se controlan sino en la DPSL.

En la base de datos principal dpsl se almacena toda la información principal concerniente a la intranet y sus servicios principales, a excepción del servicio de chat que tiene su propia base de datos.

Esta base de datos contiene catorce tablas de las cuales once pertenecen a la base de datos del sistema de permisos de funcionamiento de la DPSL, estas tablas son:

- Actividad
- Áreas
- Categoría
- Ciudad
- Clases
- Sector
- Tipo
- Establecimientos
- Representantes
- Inspecciones
- Inspectores

En la siguiente figura se describen las tablas utilizadas de la base de datos dpsl para la realización de cada consulta:

TABLA 6.2. Tablas de la base de datos dpsl

dpsl
Actividad
Areas
Categoria
Ciudad
Clases
Documentos
Establecimientos
Inspecciones
Inspectores
Noticias
Representantes
Sector
Tipos
usuario

Para el control de usuarios:

USUARIO

Contiene los datos de los usuarios que tienen acceso a todos los servicios de la intranet

TABLA 6.3. Tabla usuario

codigo_usuario	int(10)
login	varchar(15)
password	varchar(15)
Codigo_Area	int(11)
apellidos	varchar(35)
nombres	varchar(35)
cedula	varchar(10)
estado	char(1)
id_sesion	int(11)
Telefono	varchar(9)
Email	varchar(30)
Sexo	varchar(1)
Cargo	varchar(35)
Profesion	varchar(35)
tipo_usuario	varchar(1)

Para las Inspecciones:

ÁREAS

Se registran aquí los datos de todas las Áreas de la DPSL.

TABLA 6.4. Esquema de la tabla Áreas.

Field	Type
Codigo_Area	int(11)
Ciudad_Area	varchar(15)
Descripcion_Area	varchar(35)
Sector_Area	varchar(20)
Director_Area	varchar(55)

SECTOR

Guarda datos de a qué sector pertenece un establecimiento, ya que estos están divididos por sectores.

TABLA 6.5. Esquema de la tabla Sector.

Field	Type
Codigo_Sector	int(11)
Descripcion_Sector	varchar(15)
Codigo_Area	int(11)

CIUDAD

Para almacenar datos de los lugares donde están funcionando los establecimientos.

TABLA 6.6. Esquema de la tabla Ciudad.

Field	Type
Codigo_Ciudad	int(11)
Descripcion_Ciudad	varchar(15)
Codigo_Area	int(11)

ACTIVIDAD

Contiene las actividades que desempeñan los establecimientos.

TABLA 6.7. Esquema de la tabla Actividad.

Field	Type
Codigo_Act	int(11)
Descripcion_Act	varchar(60)

CATEGORÍA

Sirve para guardar a que categoría pertenecen los establecimientos.

TABLA 6.8. Esquema de la tabla Categoría.

Field	Type
Codigo_Categ	varchar(10)
Codigo_Tipo	varchar(8)
Codigo_Clase	varchar(6)
Descripcion_Categ	varchar(60)
Valor	decimal(10,0)
Categoria	varchar(10)
Cat_Anio	varchar(4)

CLASES

Registra la clase del establecimiento

TABLA 6.9. Esquema de la tabla Clases.

Field	Type
Codigo_Clase	varchar(6)
Descripcion_Clase	varchar(60)
Clase_Anio	varchar(4)

TIPOS

Cada establecimiento pertenece a un tipo de categoría que se registra en esta tabla.

TABLA 6.10. Esquema de la tabla Tipos.

Field	Type
Codigo_Tipo	varchar(8)
Codigo_Clase	varchar(6)
Descripcion_Tipo	varchar(60)
Tipo_Anio	varchar(4)

ESTABLECIMIENTOS

Aquí se registran los datos de los establecimientos que tienen que sacar el permiso de funcionamiento.

TABLA 6.11. Esquema de la tabla Establecimientos.

Field	Type
Id_Establ	int(11)
Nombre_Establ	varchar(50)
Ruc	varchar(13)
Codigo_Act	int(11)
Codigo_Area	int(11)
Fecha_Inicio_Establ	date
Estado_Establ	varchar(1)
Telefono_Establ	varchar(9)
Telefono_Establ2	varchar(9)
Fax_Establ	varchar(9)
Email_Establ	varchar(25)
Direccion_Establ	varchar(50)
Id_Rep	int(11)
Codigo_Categ	varchar(10)
Parroquia	varchar(20)
Codigo_Sector	int(11)
Codigo_Ciudad	int(11)
Anio_Establ	int(11)
Exonerado	varchar(1)
Canton	varchar(20)

REPRESENTANTES

Para almacenar datos de los propietarios de los establecimientos.

TABLA 6.12. Esquema de la tabla Representantes.

Field	Type
Id_Rep	int(11)
Nombres_Rep	varchar(35)
Apellidos_Rep	varchar(35)
Cedula_Rep	varchar(10)
Profesion_Rep	varchar(35)

INSPECCIONES

Aquí se registran todas las inspecciones realizadas a los establecimientos.

TABLA 6.13. Esquema de la tabla Inspecciones.

Field	Type
Id_Inspeccion	varchar(13)
Id_Inspector	int(11)
Id_Establ	int(11)
Fecha_Inspec	date
Descripcion_Inspec	varchar(100)
Estado_Inspec	varchar(1)
Codigo_Area	int(11)
Tipo_Inspec	varchar(1)

INSPECTORES

Se almacena los datos personales de los inspectores encargados de realizar las inspecciones.

TABLA 6.14. Esquema de la tabla Inspectores.

Field	Type
Id_Inspector	int(11)
Cedula_Inspector	varchar(10)
Apellidos_Inspector	varchar(35)
login	varchar(10)
clave	varchar(10)
Nombres_Inspector	varchar(35)
Estado_Inspector	varchar(1)
Codigo_Area	int(11)
Telefono_Inspector	varchar(9)
Celular	varchar(9)
Estado_Civil	varchar(1)
Sexo	varchar(1)
Fecha_Ingreso	date
Fecha_Nacimiento	date
Profesion	varchar(25)
Email	varchar(35)
Observacion	varchar(60)
Direccion	varchar(60)

Para los gestión de documentos:

DOCUMENTOS

Para gestionar todos los documentos que se van a exhibir en la intranet.

TABLA 6.15. Esquema de la tabla Documentos.

Field	Type
Id_Documento	int(11)
Titulo	varchar(150)
Descripcion	varchar(250)
Contenido	longblob
Tamanio	int(11)
Tamanio_Unidad	varchar(150)
Nombre_Archivo	text
Autor	varchar(250)
Fecha_Publi	date
Tipo	varchar(150)

Para las Noticias:

NOTICIAS

Para guardar las noticias del blog.

TABLA 6.16. Esquema de la tabla Noticias.

Field	Type
Id_Noticia	int(11)
Titulo	varchar(50)
Cuerpo	text
Codigo_Usuario	int(11)
Fecha_Publicacion	date
Copete	varchar(255)
imagen	text

Conforme se incremente las aplicaciones y servicios de la intranet, es necesario crear bases de datos relacionadas que pueden ser independientes entre sí, un ejemplo de esto es la base de datos Chatty utilizada para el servicio de chat.

Base de datos Chatty: Se utiliza para manejar el chat llamado Chatty, esta base de datos está diseñada en Mysql y está compuesta de dos tablas que son msg y users:

TABLA 6.17. Tablas del chat.

chatty
msg
users

USERS

Almacena la información de todos los usuarios que pueden utilizar el chat.

TABLA 6.18. Campos de la tabla Users.

Field	Type
id	int(10)
username	varchar(255)
password	varchar(255)
email	varchar(255)
active	varchar(1)
sent_on	timestamp

MSG

Guarda la información de los mensajes que se envían entre usuarios.

TABLA 6.18. Campos de la tabla msg.

Field	Type
id	int(10)
username	varchar(255)
msg	varchar(255)
color	varchar(1)
sent_on	timestamp

El modelo conceptual de las bases de datos diseñadas dpsl y Chatty se presentan en el Anexo 1 y 2.

6.4 PROGRAMACIÓN

6.4.1 SOFTWARE DE APLICACIÓN

La DPSL es una institución pública y está regulada por el Estado Ecuatoriano en cuya Constitución se promueve la adquisición de software libre para todas las Instituciones públicas y por esto el prototipo se ha diseñado con el uso de las siguientes herramientas y software:

LINUX FEDORA.- el sistema operativo puede ser de cualquier tipo de sistemas Linux, para el presente proyecto opte por Fedora 12, este sistema operativo es un software de código abierto que permite acceder a las últimas versiones existentes y se actualizan automáticamente a versiones superiores que salen cada seis meses. Fedora es siempre libre para que cualquiera lo puede usar, modificar y distribuir, además existen gran cantidad de documentos y foros que pueden ayudar a usuarios, administradores de servidores a manejarlos adecuadamente.

La intranet puede ser implementada en cualquier sistema operativo Linux, no necesariamente se debe utilizar Linux Fedora, sino que es compatible con cualquier plataforma Linux, se tomo esta opción para hacer demostraciones y pruebas pero en el mercado existen versiones de Sistemas operativos más robustos, estables y populares los mismos que gozan de mayor experiencia y aceptación.

SERVIDOR APACHE.- contiene todas las funcionalidades de un servidor web y es un programa de software libre donde constantemente se está mejorando sus características y funcionalidades de parte de toda la comunidad Linux.

Apache es un servidor web que ha penetrado en el mercado en un 60% de todos los servidores de internet, sus características más sobresalientes son:

- Es un servidor potente, flexible.
- Se ejecuta en diversas plataformas operativas.
- Es una tecnología gratuita de código fuente abierto.
- Soporta varios lenguajes como son Perl, Php, y otros.
- Puede ser extendible a través de módulos para ampliar sus capacidades, etc.

PHP.-HYPERTEXT PREPROCESOR, es un lenguaje interpretado de alto nivel poderoso, fácil de utilizar que esta embebido en código HTML y se procesa o ejecuta en el servidor, lo que nos beneficia ya que así cualquier cliente puede utilizarlo y funcionar correctamente el programa, es decir, su interpretación y ejecución se da en el servidor web, en el cual se encuentra almacenado el script, y el cliente sólo recibe el resultado de la ejecución. PHP es código open source y está disponible de manera gratuita, está diseñado específicamente para trabajar bien con Apache, el servidor web de la aplicación. Entre sus características principales tenemos:

- Soporte para una gran cantidad de bases de datos.
- Ofrece una solución simple y universal para las paginaciones dinámicas del Web de fácil programación.
- Mas fácil de mantener continuamente con mejoras y extensiones para ampliar sus capacidades.
- Tiene la capacidad de ser ejecutado en la mayoría de los sistemas operativos

MYSQL.-es un sistema de administración de bases de datos relacional (RDBMS), que permite el almacenamiento y manejo de gran cantidad de datos. Utiliza el lenguaje SQL para el manipular, recuperar los datos. Este gestor de bases de datos es, probablemente, el gestor más usado en el mundo del software libre, debido a su gran rapidez y facilidad de uso.

Las características más relevantes de este sistema de base de datos son:

- Tiene implementación multihilo lo que lo hace más veloz.
- Gestión de usuarios y passwords, manteniendo un muy buen nivel de seguridad en los datos.
- El servidor está disponible como un programa separado para usar en un entorno de red cliente/servidor.
- Relativamente sencillo de añadir otro sistema de almacenamiento. Esto es útil si desea añadir una interfaz SQL para una base de datos propia, etc.

OpenVPN

OpenVPN.- es un paquete de software que crea un túnel entre dos puntos cifrando los datos que pasan a través de él, permite la autentificación a través de claves privadas, certificados o contraseñas. Utiliza el protocolo SSL para el cifrado de datos.

Adicionalmente, para mantener la confidencialidad de los datos, se cifran todas las comunicaciones realizadas a través de la conexión VPN.

Ventajas:

- Compresión adaptativa dependiendo del tipo de datos, con lo que brinda protección a los usuarios remotos.
- Ethernet Bridge vía VPN.
- VPNs en las que ambos nodos tienen IP dinámica (adsl, dhcp, etc.)
- Simples de configurar y utilizar, ideal para ambientes heterogéneos y en cualquier plataforma.
- Soporte para proxy y firewall.
- Alta flexibilidad y posibilidades de extensión mediante scripts.
- Diseño modular.

Desventajas:

Compresión adaptativa dependiendo del tipo de datos, con lo que brinda protección a los usuarios remotos

6.4.2 SOFTWARE DE DESARROLLO

Utilizando programación libre, si bien existen muchas alternativas, el software que se utilizo para el desarrollo del proyecto es:

PHP.- lenguaje de programación gratuito, que maneja scripts y es uno de los más extendidos y utilizados del internet.

Adicionalmente para el desarrollo del prototipo se utilizaron programas adicionales para programar en PHP, hay gran variedad de editores de código abierto en el mercado y productos comerciales, de entre estos se utilizaron los siguientes programas:

- Eclipse Galileo
- Dreamweaver CS4
- PHP Editor.

TECNOLOGÍA WEB

Para las páginas web, se empleo la siguiente tecnología web:

- HTML
- HOJAS DE ESTILO CSS.
- JAVASCRIPT

HTML (HyperText Markup Lenguaje).- es el lenguaje que se utiliza para crear las páginas web. Este lenguaje indica a los navegadores cómo deben mostrar el contenido de una página, es un lenguaje que permite marcar textos usa una

serie de “tags” o “etiquetas” que funcionan como comandos para especificar con HTML que un texto va en negritas, otro en itálicas, etc.

El HTML se puede crear por medio de un editor de textos, sin embargo existe una gran variedad de programas profesionales gratuitos o comerciales que ayudan y hacen más fácil la tarea de crear páginas web, he utilizado DreamWeaver y FrontPage en Windows para el diseño de las páginas.

HOJAS DE ESTILO CSS.-es una innovación del html, permiten mejorar la apariencia de las páginas web, van incrustadas en las etiquetas html y esta sintaxis CSS permite dar forma y aplicar al documento formato de modo mucho más exacto.

JAVASCRIPT.- es un lenguaje de programación del lado del cliente más utilizado, se utiliza para construir sitios web y hacerlos más interactivos, es decir, con Javascript podemos crear efectos especiales en las páginas y definir interactividades con el usuario. El uso de javascript en este desarrollo es mínimo para evitar retardos en las peticiones de los clientes y en la transmisión de la información.

También se utiliza utilerías y programas extra como Photoshop, Paint, para la manipulación de imágenes y botones que enlazan a las páginas web, si bien son productos de software comerciales, hay versiones o demos que nos pueden servir en un lapso de tiempo determinado y que tienen todas las funciones necesarias para lograr una interfaz amigable y atractiva.

Para el siguiente proyecto se propone optar por software libre sin sacrificar la calidad del producto de software, no solo para minimizar los costos de operación en cuanto a licencias sino porque la DPSL es una institución pública y el Estado Ecuatoriano promulgo una ley de utilizar este tipo de software en todas las instituciones públicas.

Considerando esto, el lenguaje utilizado es el PHP versión 5.2, utilizando la tecnología LAMP lo que se tiene las siguientes ventajas:

- Compatibilidad con varios tipos de Sistemas Operativos Linux.
- Compatibilidad con Hardware.
- Compatibilidad con VPN's Windows para los usuarios finales.
- Existen soluciones de software libre gratuitos, y corren en esta plataforma.
- Mayor seguridad para la red.
- Bajos costos, etc.

Para asegurar la adquisición de las habilidades necesarias por los miembros de la red en el empleo de todas estas aplicaciones informáticas, se ha desarrollado el sistema en forma fácil de manera que posibilita el uso eficiente.
Ahora bien, existe un factor clave para el éxito o el fracaso en el empleo de la red propuesta que es la cultura informática de los miembros de la Institución.

6.4.3 DESARROLLO DE LA INTERFAZ

6.4.3.1 SISTEMA DE AUTENTIFICACIÓN

Para asegurarnos de que el usuario asignado con la contraseña respectiva sea el que ingrese a la red, este se autentica a través de esta pantalla donde debe ingresar el login y su contraseña, caso contrario no puede ingresar a la intranet, mediante autenticación verificamos que la persona que ofrece la contraseña es la autorizada para tener acceso a la red.

Figura 6.5. Pantalla de Inicio de Sesión de la Intranet.

6.4.3.2 PÁGINA PRINCIPAL

Si el usuario se ha autenticado correctamente se accede a la intranet, cuya página principal es la mostrada a continuación, vemos aquí el contenido de todas las noticias, documentos actuales que se presentan dinámicamente, y todas las opciones para acceder a todos los servicios de la red.

Figura 6.6. Pantalla Principal de la Intranet.

6.4.3.3 CORREO ELECTRÓNICO

Existen en el mercado un sinnúmero de programas gratuitos para el servicio de correo electrónico que instalados y configurados correctamente en el servidor proporciona el respectivo servicio, hay dos tipos de acceder al correo electrónico:

1.- Correo POP

2.- Web Mail o Correo web

En ambos tipos se necesita conexión a internet, pero la diferencia está en que en un correo POP requiere cualquier conexión puede ser un ADSL, uso de programas como Outlook Express, es más rápido, no se puede consultar desde el internet u otra PC, mientras que en el webmail se requiere un navegador web y hay que estar permanentemente conectado.

Por esta razón he seleccionado un webmail para el servicio de correo electrónico, hay varios programas que prestan este servicio entre estos tenemos: NuralStorm Webmail Client, Hastymail, Squirrelmail, OpenWebmail, etc.

Para esta red he seleccionado Squirrelmail por ser un webmail potente y de mayor experiencia en el mercado, para utilizar este servicio, debe el administrador tener creadas las cuentas de correo en el servidor.

SQUIRRELMAIL.- es una aplicación webmail que se lo encuentra en la red de fácil instalación y mantenimiento, especialmente en su uso, este software debe tener soporte en un servidor php y es compatible con la mayoría de los servidores web. Entre sus características principales tenemos:

- Es totalmente gratis porque es software libre.
- Está en 40 idiomas, se lo puede ampliar, modificar.
- Se puede acceder desde cualquier sitio.

- Trabaja con plugins lo que hace favorable para trabajar con nuevas características hace que tenga un montón de funciones interesantes.
- Tiene gestión de carpetas.
- No necesita de base de datos para funcionar.
- Interfaz de usuario fácil y potente.
- Es compatible con cualquier navegador.
- Configuración de vistas de mensajes y de temas, etc.

La pantalla que se nos presenta cuando queremos acceder a nuestro correo es la siguiente:

Figura 6.7. Pantalla Principal del correo.

6.4.3.4 CHAT

Un servicio adicional que puede ser implementado en la intranet es el chat, hay muchos programas de software libre para poderlos usarlos tales como: SILC, Xchat, Amsn Messenger, Pidgin, Chatty, etc. Como propósito de ejemplo he seleccionado Chatty un programa básico de chat, fácil de manejar e instalar, su

configuración es sencilla, su interfaz amigable y no se necesita una amplia experiencia para manipularlo.

El programa contiene una base de datos en Mysql para registrar a los usuarios, solo se requiere ingresar el nombre de usuario, su password, y el email del usuario para registrarse y listo ya puede hacer uso del chat.

No es obligatorio utilizar este programa en la red, se puede implementar video conferencia u otro programa de mensajería instantánea, el propósito de chatty es mostrar las posibilidades y utilerías que pueden ser implementadas en la red.

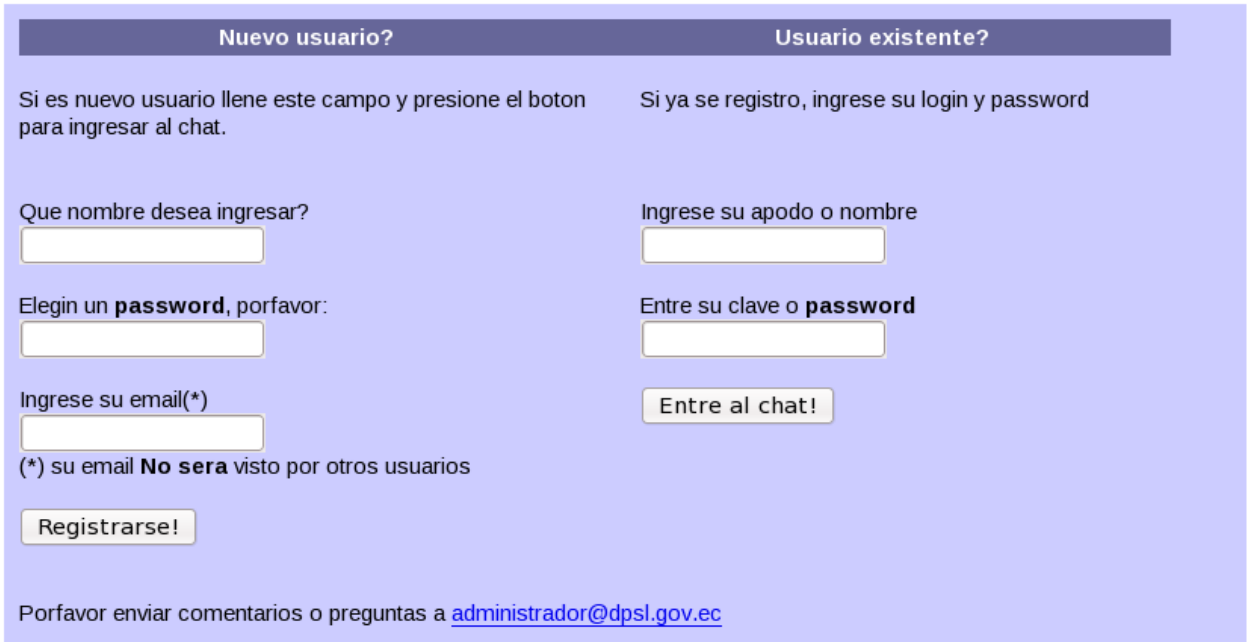


Figura 6.8. Pantalla Principal del Chat.

Una vez que el usuario ingreso aparece la siguiente pantalla para ya utilizar el servicio del chat.

Figura 6.9. Pantalla para utilizar el servicio de Chat.

6.4.3.5 DIRECTORIO

Para realizar búsquedas de datos de los miembros de la Dirección de Salud, como son:

- Características personales
- Identificación de contactos
- Teléfonos
- Etc.

Se plantea este buscador de contactos, cuya información que se mostrará dependerá de la DPSL, parar que funcione tendremos que tener en el directorio tanto los datos por los que serán buscables (por ejemplo, nombre y apellidos), como los datos que queremos mostrar (teléfono, dirección de correo electrónico), es útil para mantener contacto con los compañeros de la Institución.

Figura 6.10. Pantalla para utilizar el servicio de Directorio.

6.4.3.6 DOCUMENTOS

Con la implementación de este servicio, todo tipo de documentación y recursos divulgativos, prácticos, de interés y calidad, estarán disponibles a todos los miembros de la DPSL. Se pueden publicar circulares, documentos de interés general, oficios, volantes, que pertenecen a la información interna de la Dirección.

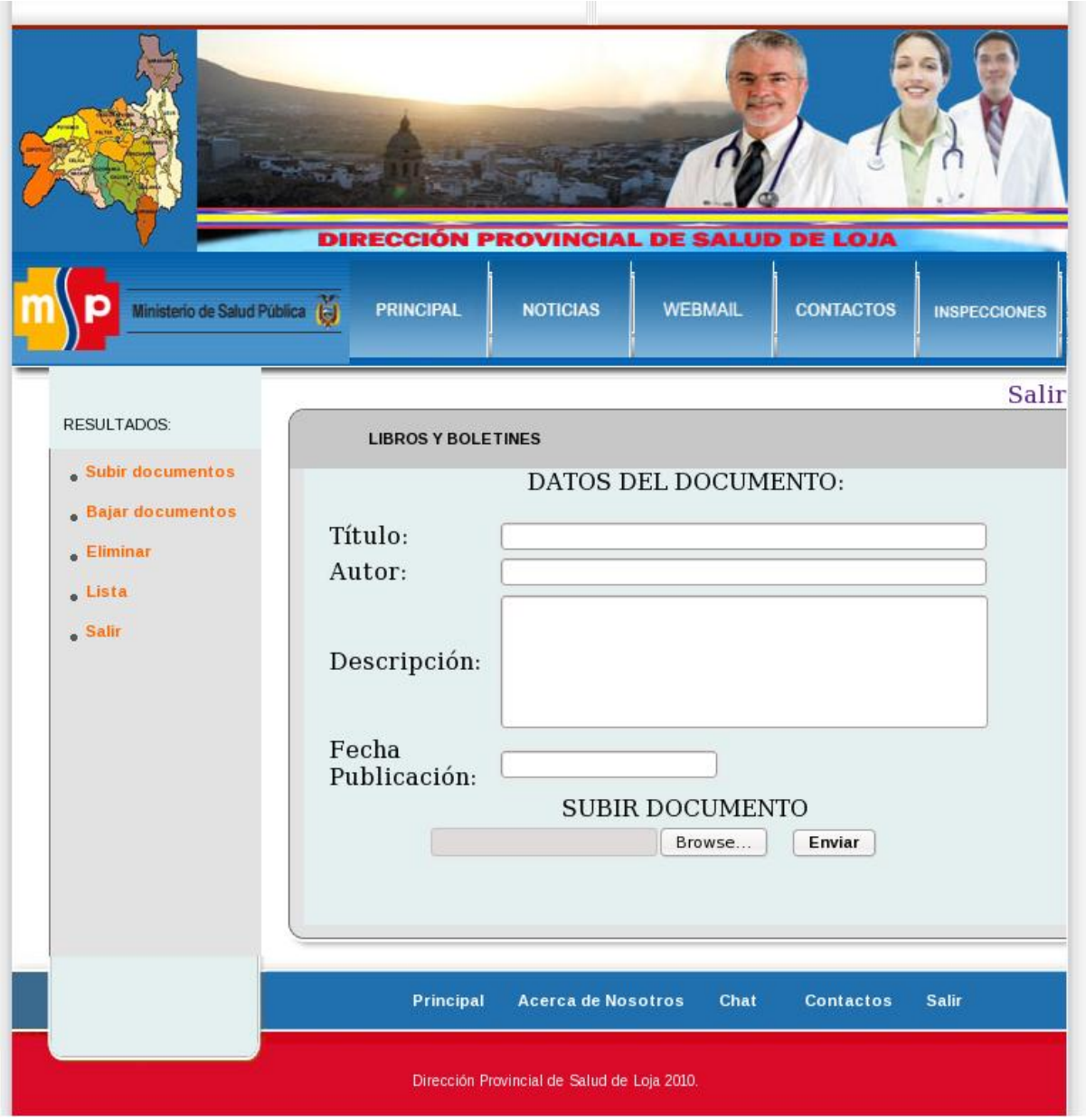


Figura 6.11. Pantalla para la Gestión de documentos.

6.4.3.7 NOTICIAS

Un blog de noticias es un servicio interesante, que nos mantiene informados del acontecer interno de la DPSL, esto nos va a permitir mayor interactividad con el resto de integrantes de todas las áreas de salud. Todos los miembros pueden ver todas las noticias pero el acceso a su edición está restringido. Todas las noticias se presentan de la siguiente manera:

Figura 6.12. Pantalla de Noticias.

6.4.3.8 INSPECCIONES

Para poder acceder a este recurso es necesario ser inspector de salud, en las diferentes áreas hay inspectores encargados de registrar todas las inspecciones realizadas a los establecimientos, sin esta inspección no se puede otorgar los permisos de funcionamiento de los locales comerciales, restaurantes, etc.

Este servicio es fundamental ya que los inspectores no tendrían que viajar a la central para registrar las inspecciones de todos los cantones de la provincia de Loja, sino que automáticamente se ingresan al sistema de gestión de los permisos de funcionamiento.

Figura 6.13. Pantalla para registrar las inspecciones.

6.5 CONFIGURACIÓN E INSTALACIÓN

Todos los programas de la red telemática de la entidad se hospedarán en el servidor principal ubicado en la Dirección principal, al no estar dispersos estos programas, se los podrá manejar, proteger y controlar más fácilmente y en forma eficiente.

En este punto, se explica cómo instalar y configurar todos los servicios necesarios para implantar la intranet.

6.5.1 SERVIDOR

El servidor será entonces configurado para aceptar conexiones desde el cliente (y viceversa).

Necesita tener instalado y configurado los siguientes paquetes de software en el servidor web, que son:

- Linux, el sistema operativo
- Instalar y configurar un servidor completo con httpd, mysqld y php:
- Instalar y configurar un servidor httpd
- Apache, el servidor web
- MySQL, el gestor de bases de datos
- MysqlAdmin para gestionar la base de datos
- PHP el lenguaje de programación.
- Instalar un Mail Server: Postfix
- Servidor DNS: BIND
- Servidor FTP: proftpd
- Servidor POP3/IMAP: Dovecot
- Instalación y configuración de Squirrelmail o servidor de Correo electrónico.

Una vez instalados todos estos paquetes, se graba la carpeta que contiene el software de la intranet en el sitio: var/www/html/ para poder acceder a la aplicación.

6.5.2 CLIENTE

Los requerimientos de software que debe tener los clientes o equipos que van a conectarse a la intranet son:

- Sistema operativo Linux o Windows 9X., NT, XP, Vista, etc.
- Aplicaciones o software para desarrollo de documentos pdf, .doc, etc.
- Software interprete para la intranet (browser o navegador) Internet Explorer, Mozilla Firefox.
- Configuración para acceso VPN.

6.5.3 VPN

Para poder configurar la VPN hace falta al menos un servidor de VPN por red, y un cliente de VPN por cada cliente de acceso remoto que se conecta a la misma. El servidor VPN es el encargado de autenticar la conexión y permitir la comunicación entre la red y el otro extremo de la VPN.

La idea es que todos los usuarios de la red entren desde cualquier ordenador, se validen en el servidor y dispongan siempre su escritorio. El servidor se encargará de validar todos los usuarios y de contener las cuentas y los datos de todos los usuarios.

6.5.4 PRUEBAS

Uno de los inconvenientes de este proyecto es las pruebas, ya que no se puede determinar en tiempo real y con equipos especializados y con varios usuarios concurrentes debido a la falta de disponibilidad de los equipos como servidores, routers y switch, ahora en la Institución no hay la capacidad de hacer estas pruebas debido a la falta de configuración de los equipos que podrían ocasionar caídas a la red LAN que se encuentra actualmente funcionando.

Las pruebas se basan en el manejo del prototipo de software, se utiliza para este fin una computadora configurada con todas las características de servidor, y otra que hace el papel de cliente, para ello se ha instalado y configurado el software en el equipo.

Luego se hace una conexión vpn entre estos dos equipos y se prueba el prototipo, se hizo la prueba con el ingreso de inspecciones, consultas entre otros.
Los errores que se encontraron es que una portátil como servidor no responde a la misma velocidad que un equipo servidor especializado, por lo que se recuerda que el proyecto va dirigido a funcionar bajo los parámetros especificados en todo el plan.

7. CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

- La intranet deberá convertirse en una base de conocimientos para la toma de decisiones de la gerencia y no solo para mejorar el desempeño de sus miembros.
- Se evaluaron los equipos con los que cuenta actualmente disponibles la red, y se observa que tienen las capacidades técnicas requeridas para el proyecto.
- El uso de la intranet beneficia tanto a la organización para optimizar sus recursos, al cliente para dar una mejor atención y a la vez oportuna, además a los miembros para tener información fiable y disponible todo el tiempo.
- Las soluciones basadas en hardware resultan en la mayoría de los casos ser más costosas que las basadas en software pero estas poseen características del manejo de la seguridad más solidas, existiendo en el mercado gran cantidad de productos que se adaptan a esta solución.
- Hoy en día existen gran cantidad de tecnologías que proporcionan calidad sobre servicio, VPN es una tecnología abierta y transparente, que permite tener acceso a lugares remotos de una forma fácil, segura y menos coste que otras tecnologías como ADSL.
- Las VPN’s entre el servidor central y los clientes junto con los protocolos de comunicación seleccionados, es una combinación muy económica, seria y segura para la DPSL.
- La mayoría de proveedores de VPN’s ofrecen productos que solo otorgan autenticación y encriptación lo que es inadecuado para implementar una VPN, para el desarrollo de VPN sobre internet se debe tomar en cuenta la seguridad y rendimiento.
- La facilidad de instalación de OpenVPN y mantenimiento, su alto grado de seguridad, la posibilidad de instalación en la mayoría de las

plataformas, ser código abierto y entre otros, la hacen idónea para ser instalada en la DPSL.

- Hay variedad de equipos en diferentes marcas que brindan la misma solución y mejores prestaciones pero el costo es un gran inconveniente para la entidad de salud sin embargo los equipos seleccionados tienen capacidad suficiente para la red propuesta.
- El software desarrollado tiene una interfaz amigable al usuario lo que beneficiara su uso correcto y rápido.
- Se puede concluir que la Intranet desarrollada es un sistema que puede dar solución a las necesidades actuales de la DPSL y permitirá que toda la información esté organizada y que no existan los problemas que había. En otras palabras, significará una mejora en la calidad de las informaciones y los servicios que se brindan en la Dirección de Salud.

7.2 Recomendaciones

- Tener una conexión a internet de calidad.
- Se recomienda un servidor potente para la red VPN con las características mencionadas, ya que requiere gran consumo de recursos.
- Implementar nuevos servicios, como VoIP, videoconferencia, colaboración de grupos, foros, aulas de aprendizaje virtual, encuestas, etc. para mayor productividad en la automatización de la comunicación y mejoras en la productividad del servicio.
- La seguridad es uno de los factores de éxito de esta tecnología para garantizar la integridad de la información
- Es recomendable utilizar un software que se ejecute en el servidor de firewall para examinar virus, también que utilice filtrado de paquetes, muy parecidos a lo que hacen los enrutadores para filtrar, de esta forma se evita contaminar o dañar la información de la red.
- Asignar los niveles de acceso para garantizar que las personas autorizadas puedan a llegar a consultar y actualizar los datos correspondientes a su perfil.
- Establecer políticas de monitoreo, plan de contingencia para el implemento de la red y garantizar su eficiente servicio.
- Establecer políticas de control de acceso, reglas de control de acceso y utilizar mecanismos de control de acceso.
- Restringir los túneles para que sean solo entre puertos y clientes autorizados.

8. PRESUPUESTO

8.1 Hardware

Descripción	Modelo	Precio Unitario	Cantidad	Valor Total
DPSL				
Servidor Streaming	SATA NHP ML150G6 E5502 2 GB HP	1092,81	1	1092,81
Servidor Vpn	SAS/SATA ML150G6 E5520 4GB HP ProLiant	1862,55	1	1862,55
Router	Linksys RT31P2 EU Router neutro con módulo ATA integrado	176,84	1	74,00
Enlace WAN	DSL	557,55	3 Mbps	557,55
TOTAL				**3590,91**
ÁREAS				
Router	Cisco 4-Port SSL/IPSec VPN Router	$ 222,540	12	2670.48
Enlace WAN	DSL	225,53	12 Mbps	2706,36
TOTAL				**5376,84**
TOTAL HARDWARE				**$ 8967,75**

8.2 Software

Descripción	Cantidad	Valor total
Licencias para sistema operativo de servidor Linux	3	0,00
Software VPN para servidor	1	0,00
Software VPN para clientes		0,00
TOTAL		0,00

8.3 Presupuesto

Número	Detalle	Unidad	Precio Unitario	Total Presupuestado
	Inversión			
1	Costos de licencias para los equipos.		$0,00	$0,00
2	Equipos			$ 5703,84
3	Software especializado			$0,00
4	Desarrollo de software	1		$450,00
	Operación y Mantenimiento			
5	Entrenamiento personal de la empresa	3	$50	$150,00
6	Gastos de publicidad			$120,00
7	Remuneración de personal técnico	3		$1650,00
8	* Servicios Técnicos y de mantenimiento.	1	$500	$500,00
9	*Contrato con la empresa proveedora de internet			3263,91
* Costo mensual TOTAL				$ 11837,75

9. BIBLIOGRAFÍA

- Dueñas Joel Barrios, IMPLEMENTACION DE SERVIDORES CON GNU/LINUX, Edicion Agosto 2009, pags. 600.
- Enrique V. Carrera, Unix Network Administration, University San Francisco of Quito, August 18, 2009. Pags.46.
- Arena, Hector Facundo. LA BIBLIA DE LINUX, MP ediciones Buenos Aires Argentina, pags. 264.
- Cross Michael y otros, SECURITY +, Syngress. Pags. 862.
- Barba Martí Antonio, GESTION DE RED, España , pags 241.
- Salavert Casamor, Antonio. LOS PROTOCOLOS EN LAS REDES DE ORDENADORES, pag. 150.
- Caire, Ramiro MANUAL DE INTRODUCCIÓN A LAS REDES MANUALES PRIVADAS (VPN) BAJO GNU/LINUX.
- Feilner, Marcus; OpenVPN: building and operating virtual private networks, 241 pags, Editorial PACK.

- http://www.iti.upv.es/seguridad/compraseg.html
- http://www.arearh.com/Criterios para construir una Intranet Corporativa- arearh_com
- http://www.redes-linux.com/rfc-es/rfc1591-es.txt
- http://www.ajsabadell.es/cs/tecno/ceres/iniciativa.html
- http://www.webhost.cl/tombrad/ayudaprensapgp.html
- http://www.vpnc.org
- http://www.entarasys.com/la
- http://en.wikipedia.org/wiki/IPsec
- http://openvnp.org
- http://fedoraprojecto.org
- http://www.wikilearning.com/tutorial/introduccion_a_la_administracion_de_una_red_local_basada_en_internet/9763
- http://www.ceta.ufm.edu/cms/es/VPN-windowsVista

10. ÍNDICE DE GRÁFICOS

11. ÍNDICE DE TABLAS

12. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

ADSL: (Asymetric Digital Subscriber Line) Línea de Abonado Digital Asimétrica, son técnicas de modulación de datos a altas velocidades sobre las líneas telefónicas.

AH: (Authentication Header) es un protocolo que provee autenticación de todas o partes del contenido de un datagrama, adicionándole una cabecera que es calculada en base a los valores del datagrama, es utilizada por IPSec.

ATM: (Asynchronous Transfer Mode) Modo de Transferencia Asíncrona, es tecnología de comunicación que usa celdas pequeñas de tamaño fijo.

CHAP: (Challenge Handshake Authenticacion Protocolo) Protocolo de autenticación por intercambio de señales por desafio, es más seguro que PAP ya que ofrece cifrado.

DHCP: (Dynamic Host Configuration Protocol) Protocolo Dinámico de Configuración de puestos, asigna direcciones IP de manera automática sobre una red TCP/IP.

DPSL: Dirección Provincial de Salud de Loja.

DSA: (Digital Signature Algorithm) Un algoritmo efectivo que hace uso de un sistema de clave pública para cifrar sólo la firma osea, sólo sirve para firmar y no para cifrar información.

ESP: (Encapsulating Security Payload) Protocolo utilizado por IPSec para asegurar la integridad y confidencialidad de la información.

IDEA: (International Data Encryption Algorithm) Algoritmo Internacional de cifrado de datos, El IDEA es un cifrador de bloques que opera sobre secuencias de 64 bits en cada ciclo.

IETF: (Internet Engineering Task Force) desarrolla y promueve los estándares internet.

IKE: (Internet Key Exchange) Intercambio de la Llave de Internet, protocolo que permite la creación de conexiones de seguridad, usado por IPSec.

IPSEC: (Internet Protocol Security) es un protocolo de seguridad que protege las comunicaciones sobre las redes IP mediante criptografía y autenticación.

IPSec: (Internet Protocol Security) Protocolo de seguridad internet.

IPX: (Internet Packet Exchange) Intercambio de paquetes de interred, no orientado a la conexión.

L2F:(Layer Two Forwarding)

L2TP: (Layer 2 Tunneling Protocol) auna las características de PPTP y L2F.

MPLS: (Multiprotocol Label Switching)

NETBEUI: (NetBIOS Extended User Interface) Interfaz Extendida de usuario NetBIOS, protocolo de comunicación de Microsoft para LAN mediante el intercambio de sus nombres.

NT: (New Technology) Nueva Tecnología, es una familia de sistemas operativos de Microsoft.

OSI: (Open System Interconnection) es un estándar o modelo desarrollado por ISO para las comunicaciones, formada de siete capas que define las fases que deben pasar los datos sobre una red.

PAP: (Password Authentication Protocol) el protocolo de autenticación de contraseña es un protocolo simple en el que se envían en texto plano el nombre de usuario y contraseña al servidor remoto.

PHP: (Hypertext Preprocessor) Lenguaje de programación interpretado.

PPTP: (Point−to−Point Tunneling Protocol) protocolo que permite a las corporaciones extenderse a través de túneles sobre una red pública como el internet.

PROTOCOLO: conjunto de reglas, normas establecidas para permitir la comunicación.

QoS: (Quality of Service) Calidad de servicio es la tecnología que garantiza el rendimiento o determinado servicio en la transmisión en una red o internet.

RADIUS: (Remote Autenthication Dial-In User Service) es una aplicación que permite la autenticación de un cliente que accede de forma remota a una red.

RAS: (Remote Access Server) Servidor de Acceso Remoto, permite acceso remoto a información que está en una red de dispositivos, este servidor puede ser hardware o software.

RC4: en criptografía es el sistema más utilizado de crifrado de flujo.

RSA: (Rivest, Shamir y Adleman) Sistema de encriptación muy utilizado, cifra información con llaves públicas y privadas.

SSH: (Secure Shell Server)

SSL: (Secure Sockets Layer) Capa de sócalos de seguridad.

TACAS: (Terminal Access Controller Access Crontrol System) programa de autenticacion basado en UNIX/LINUX.

TCP/IP: (Transmission Control Protocol/Internet Protocol) Procolo de Control de Transmisión/Protocolo de Internet, protocolo sobre la cual funciona la red Internet.

TCP:(Transmission Control Protocol) Protocolo de control de transmisión, uno de los protocolos principales de la capa de transporte del modelo OSI.

VoIP: (Voice over Internet Protocol) tecnología que hace posible que la señal de voz viaje por internet.

VPN: (Virtual Private Network) red privada virtual que utiliza un red pública para conectar sitios distantes.

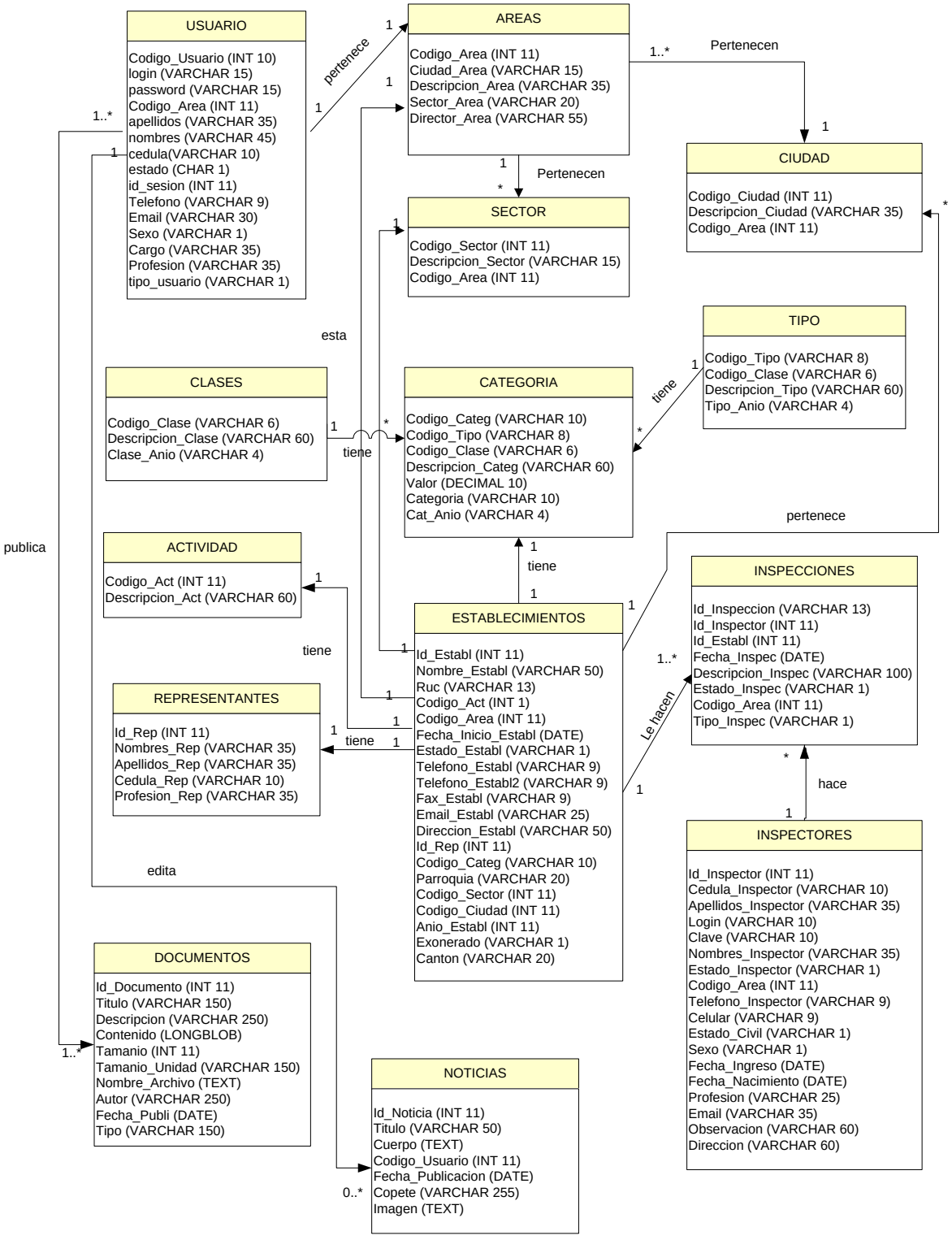
VSLM: (Variable Length subnet mask), mascara de subred de tamaño variable.

X25: Es un estándar para el acceso a redes públicas de conmutación de paquetes.

XP: (Extreme Programming) metodología de Programación Extrema.

13. ANEXOS

ANEXO 1: Base de datos dpsl



ANEXO 2:

Base de datos Chatty