

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**



UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN
ENTRE LOS SERVIDORES PARA APLICACIONES EN TELESALUD
UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA (UCV) Y
TELEMEDICINA (UCAB)**

María G. Camacho R.

gabycr_16@hotmail.com

Mirelly S. Carrillo C.

solangel17_20@hotmail.com

RESUMEN

Cada día se observa como la Telemedicina forma parte importante dentro de la sociedad, debido a que permite a los profesionales de la salud poder monitorizar a los pacientes, sin la necesidad de tener contacto físico con éstos, pudiendo hacer consultas y evaluaciones remotamente desde cualquier lugar en el que se encuentren. Es por esto que los grupos de Física Médica de la UCV y Telemedicina de la UCAB se unen para formar un proyecto, el cual contempla el diseño de una Red Privada Virtual que permita la transmisión de información entre ambos grupos médicos, mediante una interfaz gráfica que pueda sustentar los datos que ambos grupos compartirán.

No obstante, éstos cuentan con servidores propios, los cuales contienen información confidencial, que solo maneja el personal autorizado. Sin embargo, ésta información no está exenta de fallas o errores, ya que los archivos contenidos en los servidores utilizados para aplicaciones de Telemedicina pueden borrarse por distintos motivos, como: virus, fallas mecánicas del disco duro, ataques malintencionados, o incluso por accidentes (robos, incendios, inundaciones). Debido a esto el proyecto lleva a cabo el proceso de sincronización entre ambos grupos, permitiendo un gran nivel de resguardo y disponibilidad en el servicio.

Palabras clave: Telemedicina, red, VPN, sincronización.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Introducción

La telemedicina representa una de las aplicaciones que aprovecha los múltiples servicios ofrecidos por las telecomunicaciones, permitiendo el intercambio de datos, registros, opiniones y demás informaciones médicas a través de medios electrónicos, permitiendo el acceso a esta información desde lugares remotos interconectados, sin la necesidad de la interacción presencial médico-paciente.

En vista de la creciente demanda de atención médica especializada para realizar diagnósticos y estudios de pacientes a distancia, surge la idea de plantear el diseño de una red privada virtual que permita establecer la conexión y sincronización entre los servidores ubicados en los centros de investigación: Física Médica (UCV) y Telemedicina (UCAB), como una solución en el caso de los pacientes ubicados en zonas alejadas de los centros urbanos y con dificultades de acceso a centros hospitalarios y la atención médica adecuada. De manera que los pacientes puedan obtener un diagnóstico oportuno y objetivo de una forma segura, confiable y eficaz, sin necesidad de trasladarse a un centro clínico.

Además, mediante la sincronización de los servidores se podrá contar con un respaldo de toda la información que se maneja entre ambos centros, como medida de prevención en caso de que el servidor principal presente alguna falla.

I. Planteamiento del problema

En la actualidad, uno de los propósitos más importantes de la telemedicina consiste en brindar asistencia remota de personal médico especializado independientemente de la zona geográfica en la que se encuentren.

Por lo que se puede decir, que la telemedicina es un recurso tecnológico que permite optimizar los servicios de atención en salud, ahorrando tiempo y dinero.

En vista de la creciente demanda de atención médica especializada para realizar diagnósticos y estudios de pacientes a distancia, así como de la necesidad de tener un respaldo de toda la información que se maneja entre distintos centros de salud e investigación científica, surge la idea de plantear el diseño de una red privada virtual que permita la conexión y sincronización entre los servidores correspondientes a dos centros de investigación, como lo son el Grupo de Física Médica de la Universidad Central de Venezuela (UCV), y el Grupo de Telemedicina de la Universidad Católica Andrés Bello (UCAB), con el fin de que puedan intercambiar información, para que pueda ser estudiada y evaluada por personal especializado.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

II. Objetivos

II.1 General:

Diseñar una red privada virtual que permita establecer la conexión y sincronización entre los servidores correspondientes a dos centros de investigación en Telesalud, como lo son el Grupo de Física Médica (UCV) y el Grupo de Telemedicina (UCAB).

II.2 Específicos:

- Realizar la revisión y evaluación de los servidores a utilizar en el Trabajo Especial de Grado.
- Diseñar la red empleando VPN (Virtual Private Network).
- Diseñar el esquema para la sincronización entre los servidores ubicados en los centros de investigación: Física Médica (UCV) y Telemedicina (UCAB).
- Elaborar una página web que facilite la visualización de historias médicas y consultas, por parte de las personas autorizadas para acceder a la información.
- Probar la conexión y sincronización respectiva al diseño elaborado.

III. Marco Teórico

Telemedicina

La telemedicina es una aplicación de las telecomunicaciones que se basa en la prestación de soluciones y servicios al sector salud, mediante el uso de tecnologías de información y comunicaciones a larga distancia. Esto permite un gran número de ventajas, como por ejemplo, la intervención indirecta de especialistas a larga distancia mediante teleconferencias o Chat; manejo, almacenamiento y transmisión de datos e imágenes de gran importancia, ya sea en tiempo real o no; entre otras. (Benítez y Méndez, 2010).

Telesalud

Es un sistema computarizado que permite la transmisión y recepción de señales de audio, video y datos utilizando algún medio de telecomunicación como satélite, fibra óptica, línea telefónica digital o red de área local o amplia (LAN/WAN). Es un concepto más amplio que la atención médica a distancia o telemedicina, ya que incluye los elementos necesarios para brindar servicio a médicos, enfermeras, paramédicos y administrativos a través de cursos de capacitación, conferencias, diplomados, asesorías, etc. (Sánchez, 2011)

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Dispositivo BioHarness BioModule

Este dispositivo es una nueva tecnología de sensores inteligentes que trabaja con tecnología Bluetooth, permitiendo así la captura y transmisión de datos fisiológicos de un usuario a través de las redes de datos móviles y fijos. Es decir, este sensor permite el monitoreo y control remoto del rendimiento y la condición humana en el mundo real, evaluando respuestas impulsivas básicas e importantes como: la temperatura de la piel, frecuencia cardíaca y respiratoria, posición y aceleración. (Zephyr Technology Corporation, 2010)

Servidores

Según Sierra (2012), un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al “servicio” de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información.

Sincronización de servidores

La sincronización es el proceso mediante el cual se realiza la actualización de dos o más servidores de forma que contengan exactamente los mismos datos. Si se agrega, modifica o elimina un archivo de una ubicación, el proceso de sincronización agregará, modificará o eliminará el mismo archivo en las otras ubicaciones. (Torres, 2013)

VPN (Virtual Private Network)

Una red privada virtual se basa en un protocolo denominado “protocolo de túnel”, el cual consiste en un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.

Se dice que esta red es virtual porque conecta dos redes "físicas" (redes de área local) a través de una conexión poco fiable (Internet) y privada porque sólo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden "ver" los datos. (Rodríguez, 2012)

Protocolo TCP/IP

Corresponde con la capa de transporte del modelo OSI que se refiere a Open System Interconnection (Modelo de interconexión de sistemas abiertos). Es un protocolo de comunicación orientado a la conexión, creado para la conexión a Internet. Ofrece control de flujo y de congestión. (Universidad Pública de Navarra, s.f.)

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Protocolo UDP

Es un protocolo no orientado a la conexión. Al igual que TCP transporta los mensajes a través del protocolo IP (*Internet Protocol*), sin embargo de forma menos fiable. (Universidad Tecnológica Nacional, s.f.)

SSH (Secure Shell)

Según López (2004), SSH es un protocolo que permite acceder en forma remota y ejecutar comandos desde una máquina a otra en forma segura. Cuenta con una ardua autenticación y encriptación sobre los canales de comunicación entre el cliente y el servidor.

SFTP (Secure File Transfer Protocol)

Es un protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable. Se utiliza comúnmente con SSH para proporcionar la seguridad a los datos, aunque permite ser usado con otros protocolos de seguridad. (Lamana, 2012)

HTML (HiperText Markup Language)

Hace referencia al lenguaje de marcas de hipertexto para la elaboración de páginas web. Es un estándar que, en sus diferentes versiones, define una estructura básica y un código (denominado código HTML) para la definición de contenido de una página web, como texto, imágenes, etc.

El código HTML determina cómo luce el sitio en general, incluyendo dónde se ubica el texto, las fotos y los demás elementos que lo componen. (Gutiérrez, 2012)

Protocolo HTTPS (Protocolo Seguro de Transferencia de Hipertexto)

HTTPS proviene del protocolo HTTP que se refiere a Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto), el cual se encuentra presente cada vez que hay tráfico de información a través de Internet.

El HTTPS, representa una versión más segura de HTTP, ya que es la fusión entre este protocolo y el cifrado SSL (Secure Socket Layer) ó Capa de Conexión Segura. Por ello, es comúnmente utilizado en páginas de Internet que manejan información confidencial como números de tarjetas de crédito, teléfono, dirección, incluso al momento de ingresar una clave o contraseña. (Herrera, 2011)

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Protocolo SSL

Según Ximenez (s.f.), es un protocolo impulsado por Netscape. Es muy utilizado actualmente en Internet, ya que le da mayor confianza al usuario al realizar transacciones de cualquier tipo a través de la Web.

Base de datos

Según Valade (2008), una base de datos es un conjunto de información organizada en registros o tablas, los cuales son guardados en una computadora y se manejan por el usuario a través de una interfaz gráfica. Cada registro constituye una unidad independiente de información que puede estar a su vez estructurada en diferentes campos o tipos de datos que se recogen en dicha base de datos. En cada registro se recogerán determinados datos, como el nombre, la profesión, la dirección o el teléfono, cada uno de los cuales constituye un campo.

MySQL

Es un sistema administrativo relacional de bases de datos. Este tipo de bases de datos puede ejecutar desde acciones tan básicas, como insertar y borrar registros, actualizar información ó hacer consultas simples, hasta realizar tareas tan complejas como la aplicación lo requiera. (Valade, 2008)

PHP (*Hyper Text Processor*)

Es un lenguaje de programación diseñado para ser utilizado en aplicaciones WEB. Su sintaxis es similar a la del código C. Maneja la conexión con la base de datos y la comunicación con ella. (Valade, 2008)

IV. Metodología

Fase 1: Investigación documental.

Tiene como finalidad buscar y recopilar información teórica, como proyectos y artículos que se han desarrollado previamente y que de una u otra forma permiten establecer una base teórica fundamental para el proyecto que se llevará a cabo, lo cual permitirá obtener conocimientos acerca de los tópicos que abarcará el trabajo.

Fase 2. Estudio de Equipos e Infraestructura.

Se realizará una revisión y evaluación de los equipos a utilizar en el Trabajo Especial de Grado, especialmente los servidores, a fin de conocer el estado de los mismos y determinar si

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

es necesario optimizar su funcionamiento o si ya cumplen con los requisitos necesarios para llevar a cabo este proyecto.

Para ello se tomarán en cuenta aspectos como: sistema operativo, espacio de disco duro disponible, entre otros.

Fase 3. Diseño e implementación de una VPN para la conexión y sincronización entre los servidores de la UCV y de la UCAB.

A través de esta fase, se contará con una forma segura y eficiente de conexión entre ambos servidores, así como de la actualización sincronizada entre los mismos, permitiendo tener un respaldo de la información utilizada por el personal especializado del Grupo de Física Médica de la Universidad Central de Venezuela (UCV) y el Grupo de Telemedicina de la Universidad Católica Andrés Bello (UCAB).

Se deben realizar una serie de pruebas de establecimiento de conexión e intercambio de datos entre dos computadoras portátiles conectadas en la misma red a través de Internet, con el propósito de realizar pruebas previas al establecimiento de la conexión entre servidores.

Fase 4. Diseño y desarrollo de la aplicación web.

En esta etapa se busca integrar todos los elementos en una plataforma amigable que facilite la visualización de historias médicas y consultas realizadas por las personas autorizadas para acceder a la información. Buscando la manera de que la misma sea lo suficientemente confiable para quienes la manejarán. El sistema funciona bajo el mismo principio de operación de una página web.

Fase 5. Pruebas y Simulaciones.

En esta etapa se realizarán pruebas y simulaciones utilizando los servidores indicados anteriormente, con el fin de certificar si el diseño de la conexión y la sincronización de dichos servidores se logran de forma exitosa.

Para esto, se debe establecer la conexión entre el servidor y el cliente, una vez diseñada la aplicación, se llenarán cada uno de los campos que se muestran en dicha aplicación, para luego almacenarlas en una base de datos con un historial que contiene información básica del paciente, reduciendo de esta forma el tiempo de duración en la elaboración de un diagnóstico efectivo.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Fase 6. Redacción y Elaboración del Trabajo Especial de Grado.

Una vez concluidas las pruebas y simulaciones en dichos servidores, se procederá a realizar un informe final que contemple los conceptos teóricos utilizados y el desarrollo práctico basado en la metodología.

V. Desarrollo

Luego de conocer la metodología empleada, se procede a su desarrollo, el cual plasma cada una de las fases mencionadas anteriormente, de manera de alcanzar los objetivos propuestos.

V.1 Caracterización del servidor y cliente

Para la realización de esta etapa fue necesaria la obtención de las características de los servidores del Grupo de Física Médica y el Grupo de Telemedicina, además de los servidores propios que se utilizarían para hacer las pruebas necesarias en primer lugar. Es por esto que se elaboraron tablas, que se muestran en Resultados, indicando los aspectos básicos de los servidores tanto para el cliente como para el servidor. De este modo se tendrían las especificaciones necesarias para la realización de la conexión VPN, estableciendo quien sería el servidor y el cliente.

V.2 Diseño y simulación de la conexión cliente-servidor

Se desarrolló el diseño de una red privada virtual (VPN), que conecta los grupos de Física Médica (UCV) y Telemedicina (UCAB), de manera que la información que se envía por el túnel VPN, pueda hacerse de forma práctica y segura.

Para implementar la conexión de red privada virtual, se utilizaron inicialmente dos equipos diferentes como servidores, con la finalidad de simular las pruebas, antes de realizar la configuración en los servidores reales entre los grupos UCAB-UCV.

V.2.1 Configuración del Servidor y Cliente VPN

En la configuración tanto del servidor como del cliente, se instalaron todos los paquetes necesarios para su óptimo funcionamiento, ajustando parámetros precisos, para un correcto desempeño de la red privada virtual. Para esta configuración se utilizaron una serie de comandos, algunos de ellos se pueden observar en el Apéndice A.

V.3 Implementación de la conexión

Luego de realizada la simulación de la conexión VPN en dispositivos ajenos al diseño, se procedió a realizar la conexión entre el servidor de la UCV y el servidor de la UCAB.

Se utilizó el protocolo SSH, para lograr el acceso a ambos servidores en modo remoto, de manera de poder hacer las configuraciones necesarias para que el servidor de la UCV

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

funcione como servidor principal y el servidor de la UCAB se encuentre funcionando como servidor de respaldo.

V.4 Sincronización de los servidores

Al establecer la conexión mediante acceso remoto a los servidores, se procedió a configurar la manera de sincronizar la base de datos de la página Web con el servidor de respaldo. Para esto se ejecutaron los siguientes comandos de manera de sincronizar la base de datos mediante la VPN.

Inicialmente, se deben configurar permisos requeridos en el servidor, para que al momento de que el cliente acceda por SSH, no sea necesario introducir una clave cada vez que se establezca la conexión, permitiendo que la sincronización funcione automáticamente. Es por esto que se debe crear la llave pública y privada en el servidor. Para ello se utilizó el siguiente comando:

```
#ssh-keygen -t rsa (no indicar ninguna clave cuando lo requiera)
```

- Las llaves se crean en el directorio `‘/root/.ssh’`, con los nombres `‘id_rsa’` (privada) e `‘id_rsa.pub’` (pública).
- Se debe agregar en el servidor remoto el contenido del archivo `‘id_rsa’` a la ruta del cliente `‘/root/.ssh/authorized_keys’`, con lo cual el proceso de autenticación del acceso SSH quedaría configurado.
- Una vez que se establece el proceso de autenticación se ejecuta el comando que permite la sincronización desde el servidor que será el encargado de respaldar la información.

```
#rsync -vuArtlpoge 'ssh -p 22' usuario@ip_vpn_servidor:/directorio_local/  
/dir_remoto/
```

Para poder hacer automático el envío de datos en la sincronización, se configura el archivo: `/etc/crontab/`, especificando cada cuanto tiempo se actualizará la información.

Se debe configurar el archivo `crontab` de manera que se actualice la base de datos, asegurando la disponibilidad del servidor de respaldo en caso de que falle el principal.

- Debe colocarse lo siguiente de manera de actualizar la información en el directorio especificado:

```
* 2 * * * root rsync -vuArtlpoge 'ssh -p 22' --delete  
usuario@ip_vpn_servidor:/directorio_local/ /dir_remoto/
```

La Figura 1 muestra la configuración del archivo `crontab`, especificando que cada día a las dos (2) de la mañana la información se actualizará en el directorio indicado.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

```
root@telem1-tesis: /etc
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that some of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
2 * * * * root    /usr/bin/rsync -vuArtlpoge 'ssh -p 22' --delete root@192.168.2.4:/var/lib/mysql/bdtesis/ /var/lib/mysql/db_tesis20136
```

Figura 1. Configuración de la hora de sincronización.

Fuente: Elaboración propia.

V.5 Diseño de la aplicación

El diseño de la aplicación, consistió en la elaboración de una Página Web, mediante la cual los pacientes y especialistas tienen acceso, de manera que puedan consultar o dar seguimiento de una consulta médica. Dicha aplicación fue elaborada en el software de Dreamweaver.

Para que los pacientes y especialistas pudieran acceder a la página Web, fue necesario la elaboración de una base de datos con MySQL.

La base de datos se elaboró sobre la plataforma *PhpMyAdmin*, en la cual se realizó una serie de pasos, para crear la base de datos, tablas y guardar la información correspondiente a cada proceso asociado.

Al realizar la creación de la base de datos, se procedió a investigar acerca de lenguajes necesarios para la creación de una página Web. La documentación obtenida abarcó diferentes lenguajes de programación, sin embargo, los más utilizados para dicho fin, serían el código HTML y PHP.

Primeramente se realizó el diseño de la estructura para definir como se obtendrían los datos de los pacientes y la manera en la que se plasmarían en la aplicación Web, de forma de que la base de datos corresponda con la información alojada en el portal Web.

Cuando el especialista o el paciente ingresa a la página Web, podrá acceder o registrarse si fuese necesario, inmediatamente que se cargan los datos, éstos se verán reflejados en la base de datos de MySQL. Se desarrollaron los códigos *.php* y los códigos *.html*, en un programa diseñado para realizar páginas Web, el cual contiene diversas funcionalidades a modo de lograr que la expectativa del usuario sea cómoda y agradable.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

En el Apéndice B, se muestra la manera en la cual está conformado el sitio Web que representa la aplicación del proyecto.

Para asegurar la confidencialidad de los datos contenidos en la aplicación, el *software* de Apache ofrece la modalidad de seguridad HTTPS, de manera que toda la información sea transmitida y recibida en forma cifrada a través del protocolo SSL. Para activar su funcionamiento en la aplicación, se activó el Protocolo Seguro de Transferencia de Hipertexto en las páginas que ameritan la existencia de dicha medida de seguridad.

VI. Resultados

A continuación, se presentan los resultados obtenidos durante el desarrollo del proyecto:

VI.1 Características de los dispositivos a utilizar.

A continuación se presentan las características básicas de los dispositivos a utilizar para establecer la conexión entre la UCV y la UCAB.

Características

Ubicación del Servidor	UCAB
Fabricante	IBM
Memoria RAM	512.0 MB/8.0 Gb (max)
Espacio de disco	30 Gb
Espacio disponible	10 Gb
¿Utiliza interfaz gráfica?	No
Sistema operativo	Linux
Versión del sistema operativo	Ubuntu
Procesador	Intel Xeon 3.06 GHz
ISP (Modem)	CANTV
Velocidad	533.0 MHz
Función actual del servidor	Almacenamiento.

Tabla 1. Características del dispositivo Nro. 1.

Fuente: Elaboración propia.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Características

Ubicación del Servidor	Física Médica. Facultad de Ciencias, UCV
Fabricante	Compaq
Memoria RAM	1.5 Gb
Espacio de disco	30 Gb
Espacio disponible	25 Gb
¿Utiliza interfaz gráfica?	No
Sistema operativo	CentOS
Versión del sistema operativo	CentOS 5.6
Procesador	2 Xeon Intel 2GHz
ISP (Modem)	CANTV
Rango de direcciones	Clase C
Función actual del servidor	Web y servidor de correo

Tabla 2. Características del dispositivo Nro. 2.

Fuente: Elaboración propia.

Características

Ubicación del Servidor	Portátil
Fabricante	Gateway
Memoria RAM	4 Gb
¿Trabaja en una partición?	Si
Espacio de disco	500 Gb
Espacio disponible	100 Gb
¿Trabaja con máquina virtual?	No
Sistema operativo de la partición:	CentOS
Versión del sistema operativo:	CentOS 5.6
Procesador	Core i3
ISP (Modem)	CANTV
Conexión a Internet	Inalámbrica

Tabla 3. Características del dispositivo Nro. 3.

Fuente: Elaboración propia.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Características

Ubicación del Servidor	Portátil
Fabricante	Gateway
Memoria RAM	4 Gb
¿Trabaja en una partición?	Si
Espacio de disco	300 Gb
Espacio disponible	100 Gb
¿Trabaja con máquina virtual?	No
Sistema operativo de la partición:	CentOS
Versión del sistema operativo:	CentOS 5.6
Procesador	Core i3
ISP (Modem)	CANTV
Conexión a Internet	Inalámbrica

Tabla 4. Características del dispositivo Nro. 4.

Fuente: Elaboración propia.

Una vez obtenida toda la información de los equipos a utilizar, se procedió a evaluar sus características en función de las necesidades de interconexión entre los dos servidores, y se determinó que los dispositivos cumplen con los requisitos básicos necesarios para su utilización a través del proyecto.

Es importante mencionar que cada dispositivo actualmente cumple funciones distintas, que en cierta forma podrían interferir en el funcionamiento del proyecto. En el caso de la UCV, el servidor es compartido con el Centro de Computación de la Facultad de Ciencias, por lo tanto, está subdividido en varias sesiones, limitando la capacidad de almacenamiento y la velocidad de procesamiento.

En cuanto al servidor de la UCAB, por los momentos es administrado por la DTI, siendo usado sólo por la Escuela de Ingeniería de Telecomunicaciones. Actualmente se utiliza para proyectos de Telemedicina, por lo que está subdividido en varias secciones, correspondientes a otros proyectos. A pesar de que en este caso la capacidad de almacenamiento también es limitada, es menos probable que surjan inconvenientes relacionados con la velocidad de procesamiento.

Por otro lado, en la UCV nos ofrecieron la posibilidad de contar con una sala de computadoras, en la cual se encontraba el servidor a utilizar, de manera que pudiéramos

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

acceder directamente a este dispositivo, teniendo así un mayor control del mismo. Es por esto que se decidió que el servidor principal sería el que se encuentra ubicado en la UCV, y el servidor con rol de cliente el que se encuentra ubicado en la UCAB, en este último existirá un respaldo de toda la información colocada en el servidor principal, mediante el proceso de sincronización de ambos servidores.

VI.2 Acceso a los servidores

Para poder acceder al servidor de la UCAB se utilizaron dos programas: VPN Client y Filezilla.

Con los datos proporcionados por el Departamento de Tecnología e Información de la UCAB, se logró configurar una nueva conexión VPN llamada “VPN-UCAB”, entre el servidor ubicado en la UCAB y una computadora personal. Una vez hecho esto, se procedió a la conexión mediante el software de VPN Client, en el cual se debe acceder con un usuario específico, en nuestro caso “tesis20136”, con la clave correspondiente. (Ver Figura 2)

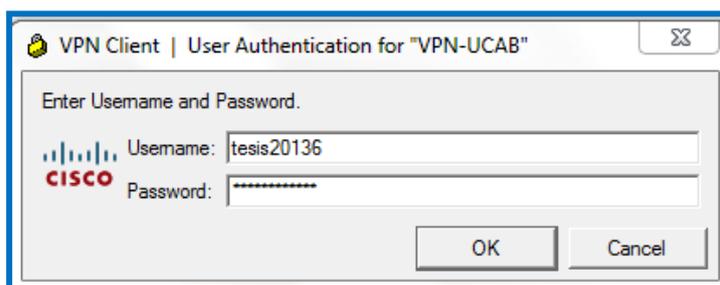


Figura 2. Ventana de configuración de usuario interno.

Fuente: Elaboración propia.

Y finalmente muestra un mensaje de que la conexión se realizó de manera exitosa. (Ver Figura 3)

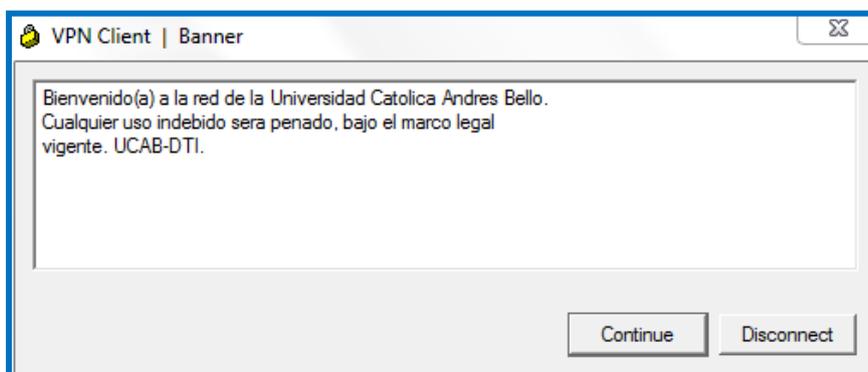


Figura 3. Mensaje de bienvenida al conectar con el servidor remoto.

Fuente: Elaboración propia.

DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA (UCV) Y TELEMEDICINA (UCAB)

Para el proceso de transferencia de archivos desde la PC hacia el servidor, *FILEZILLA* brindó una interfaz amigable con la cual se pudo realizar la subida y bajada de archivos necesarios, este proceso se realizó de manera remota mediante el protocolo SSH, y la transferencia de archivos se realizó mediante SFTP. Para acceder al servidor se colocaron los datos de dirección IP, usuario, clave y puerto de conexión a utilizar, en este caso se colocó directamente la dirección IP del servidor ya que está conectado a la red de la UCAB. El proceso de conexión puede observarse en la Figura 4.

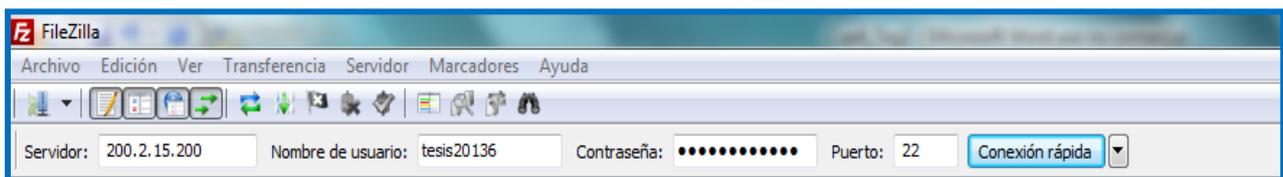


Figura 4. Ventana de conexión al servidor UCAB.

Fuente: Elaboración propia.

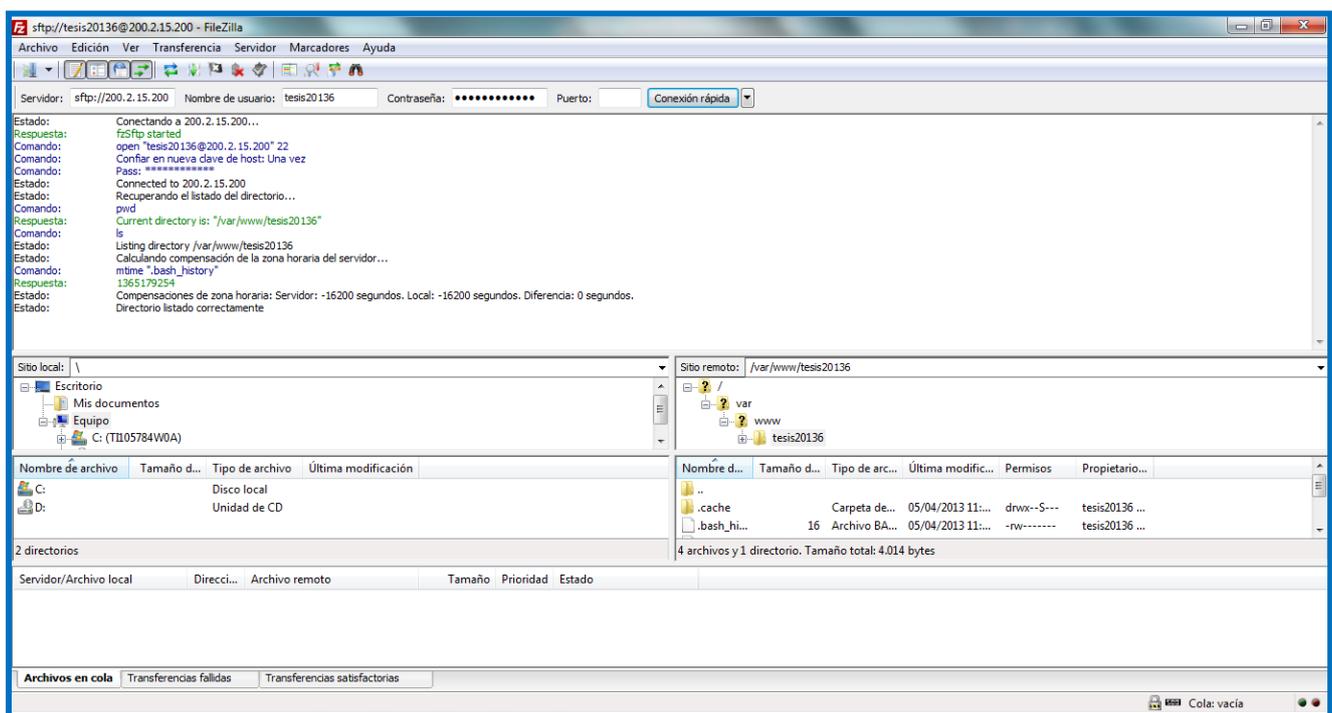


Figura 5. Ventana de conexión Filezilla (UCAB).

Fuente: Elaboración propia.

DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA (UCV) Y TELEMEDICINA (UCAB)

Para poder acceder al servidor de la UCV sólo fue necesario el programa Filezilla, en el cual se siguieron los mismos pasos mencionados anteriormente. En este caso, utilizando los datos proporcionados por el Administrador de Red de la Escuela de Física de la Facultad de ciencias de la UCV.

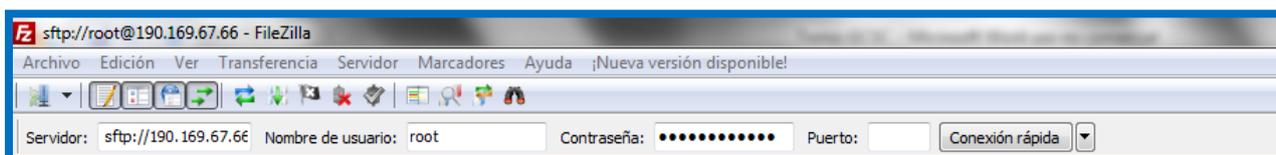


Figura 6. Ventana de conexión Filezilla (UCV).

Fuente: Elaboración propia.

Finalmente, se seleccionaron las carpetas y/o archivos a transferir y se enviaron al servidor, observándose en las carpetas del servidor que los archivos fueron subidos satisfactoriamente.

VI.3 Diseño de la red de interconexión UCV- Física Médica y UCAB - Telemedicina

Una vez consideradas las necesidades del proyecto para la conexión y sincronización de ambos servidores y tomando en cuenta las características de los dispositivos disponibles a utilizar en el proyecto, se procedió a elaborar el diseño de la red de interconexión UCV - Física Médica y UCAB - Telemedicina (Ver Figura 7). De esta manera fue posible definir los protocolos que serían implementados para establecer la conexión. Siendo SSH uno de los protocolos definidos en el diseño, ya que a través de este protocolo se pudo acceder al servidor de la UCV y al de la UCAB de forma remota.

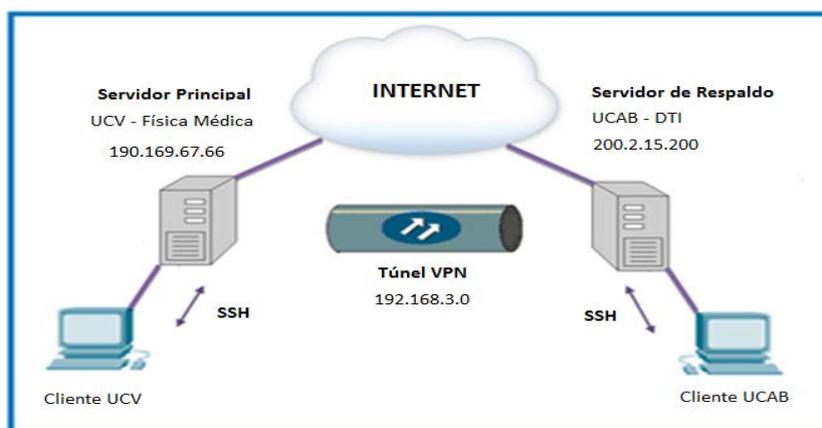


Figura 7. Diseño de la red.

Fuente: Elaboración propia.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Definido el diseño, se procedió entonces a realizar las simulaciones de conexión.

VI.4. Simulación de Conexión VPN

Para esta parte se realizó la implementación de una red privada virtual (VPN) en dos equipos ajenos al diseño, con el fin de simular su funcionamiento a modo de prueba antes de hacerlo en los servidores correspondientes a los Grupos de Física Médica (UCV) y de Telemedicina (UCAB).

Una vez configuradas las dos laptops, una como servidor y otra como cliente, se procedió a establecer la red privada virtual entre los dos dispositivos. Se realizaron pruebas para verificar la creación del túnel VPN, esto se puede apreciar en las Figuras 8 y 9 que aparecen a continuación:

```
[root@servidor1 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:13:D3:13:EE:FC
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60163 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32801 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42284558 (40.3 MiB)  TX bytes:3837126 (3.6 MiB)
          Interrupt:177 Base address:0xa000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1899 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1899 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3001969 (2.8 MiB)  TX bytes:3001969 (2.8 MiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.1  P-t-P:172.16.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:3584 (3.5 KiB)  TX bytes:4072 (3.9 KiB)
```

Figura 8. Establecimiento del túnel desde el servidor VPN.

Fuente: Elaboración propia.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

```
[root@servidor2 openvpn]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:14:2A:27:08:FE
          inet addr:192.168.2.5  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25526 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29811408 (28.4 MiB)  TX bytes:4131822 (3.9 MiB)
          Interrupt:185 Base address:0x6000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:6541 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6541 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3452717 (3.2 MiB)  TX bytes:3452717 (3.2 MiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:172.16.0.6  P-t-P:172.16.0.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:13719 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4784 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:16932312 (16.1 MiB)  TX bytes:589492 (575.6 KiB)
```

Figura 9. Establecimiento del túnel desde el cliente VPN.

Fuente: Elaboración propia.

Luego de verificar el establecimiento del túnel entre el servidor y el cliente, se comprobó la correcta conectividad entre los miembros de la red VPN a través del comando PING. Esto se puede observar en las Figuras 10 y 11:

```
[root@servidor1 ~]# ping 172.16.0.6
PING 172.16.0.6 (172.16.0.6) 56(84) bytes of data:
64 bytes from 172.16.0.6: icmp_seq=1 ttl=64 time=0.612 ms
64 bytes from 172.16.0.6: icmp_seq=2 ttl=64 time=0.588 ms
64 bytes from 172.16.0.6: icmp_seq=3 ttl=64 time=0.585 ms
64 bytes from 172.16.0.6: icmp_seq=4 ttl=64 time=0.860 ms
64 bytes from 172.16.0.6: icmp_seq=5 ttl=64 time=0.584 ms
64 bytes from 172.16.0.6: icmp_seq=6 ttl=64 time=0.668 ms
64 bytes from 172.16.0.6: icmp_seq=7 ttl=64 time=0.591 ms
64 bytes from 172.16.0.6: icmp_seq=8 ttl=64 time=0.591 ms
64 bytes from 172.16.0.6: icmp_seq=9 ttl=64 time=0.587 ms
64 bytes from 172.16.0.6: icmp_seq=10 ttl=64 time=0.594 ms
64 bytes from 172.16.0.6: icmp_seq=11 ttl=64 time=0.595 ms
64 bytes from 172.16.0.6: icmp_seq=12 ttl=64 time=0.600 ms
64 bytes from 172.16.0.6: icmp_seq=13 ttl=64 time=0.596 ms
64 bytes from 172.16.0.6: icmp_seq=14 ttl=64 time=0.596 ms
64 bytes from 172.16.0.6: icmp_seq=15 ttl=64 time=0.644 ms
64 bytes from 172.16.0.6: icmp_seq=16 ttl=64 time=0.581 ms

--- 172.16.0.6 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15007ms
rtt min/avg/max/mdev = 0.581/0.617/0.860/0.066 ms
[root@servidor1 ~]#
```

Figura 10. Envío de PING desde el Servidor hacia el cliente.

Fuente: Elaboración propia.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

```
[root@servidor2 ~]# ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=0.575 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=64 time=0.562 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=64 time=1.94 ms

--- 172.16.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 0.562/1.027/1.944/0.648 ms
```

Figura 11. Envío de PING desde el Cliente hacia el Servidor.

Fuente: Elaboración propia.

VI.5 Establecimiento de la Conexión

La conexión entre los servidores en la UCV y la UCAB a través de la red privada virtual se puede comprobar por medio de la aparición del túnel VPN en la siguiente imagen:

```
root@telem1-tesis:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:02:b3:ef:0b:44
          inet addr:200.2.15.200  Bcast:200.2.15.255  Mask:255.255.255.0
          inet6 addr: fe80::202:b3ff:feef:b44/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:161476089  errors:0  dropped:0  overruns:0  frame:0
          TX packets:4115084  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:100
          RX bytes:4177362528 (4.1 GB)  TX bytes:2159335684 (2.1 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:88428  errors:0  dropped:0  overruns:0  frame:0
          TX packets:88428  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:9616934 (9.6 MB)  TX bytes:9616934 (9.6 MB)

tun0     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.3.10  P-t-P:192.168.3.9  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0  errors:0  dropped:0  overruns:0  frame:0
          TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Figura 12. Túnel VPN de conexión UCV - UCAB.

Fuente: Elaboración propia.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Luego de verificar el establecimiento del túnel entre el servidor y el cliente, se comprobó la correcta conectividad entre los miembros de la red VPN a través del comando PING. Esto se puede observar en la siguiente figura:

```
root@teleml-tesis:~# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=64 time=38.2 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=64 time=15.9 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=64 time=15.2 ms
64 bytes from 192.168.3.1: icmp_seq=4 ttl=64 time=13.9 ms
64 bytes from 192.168.3.1: icmp_seq=5 ttl=64 time=24.2 ms
64 bytes from 192.168.3.1: icmp_seq=6 ttl=64 time=13.1 ms
64 bytes from 192.168.3.1: icmp_seq=7 ttl=64 time=33.5 ms
64 bytes from 192.168.3.1: icmp_seq=8 ttl=64 time=23.5 ms
64 bytes from 192.168.3.1: icmp_seq=9 ttl=64 time=5.16 ms
64 bytes from 192.168.3.1: icmp_seq=10 ttl=64 time=36.5 ms
64 bytes from 192.168.3.1: icmp_seq=11 ttl=64 time=23.8 ms
64 bytes from 192.168.3.1: icmp_seq=12 ttl=64 time=37.4 ms
64 bytes from 192.168.3.1: icmp_seq=13 ttl=64 time=8.51 ms
64 bytes from 192.168.3.1: icmp_seq=14 ttl=64 time=19.8 ms
64 bytes from 192.168.3.1: icmp_seq=15 ttl=64 time=25.6 ms
64 bytes from 192.168.3.1: icmp_seq=16 ttl=64 time=19.8 ms
64 bytes from 192.168.3.1: icmp_seq=17 ttl=64 time=19.1 ms
^C
--- 192.168.3.1 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16024ms
rtt min/avg/max/mdev = 5.164/21.984/38.258/9.640 ms
root@teleml-tesis:~# ping 192.168.2.4
PING 192.168.2.4 (192.168.2.4) 56(84) bytes of data.
64 bytes from 192.168.2.4: icmp_seq=1 ttl=63 time=11.8 ms
64 bytes from 192.168.2.4: icmp_seq=2 ttl=63 time=6.54 ms
64 bytes from 192.168.2.4: icmp_seq=3 ttl=63 time=8.26 ms
64 bytes from 192.168.2.4: icmp_seq=4 ttl=63 time=8.97 ms
64 bytes from 192.168.2.4: icmp_seq=5 ttl=63 time=23.6 ms
64 bytes from 192.168.2.4: icmp_seq=6 ttl=63 time=20.3 ms
64 bytes from 192.168.2.4: icmp_seq=7 ttl=63 time=28.2 ms
64 bytes from 192.168.2.4: icmp_seq=8 ttl=63 time=21.6 ms
64 bytes from 192.168.2.4: icmp_seq=9 ttl=63 time=38.3 ms
64 bytes from 192.168.2.4: icmp_seq=10 ttl=63 time=26.8 ms
^C
--- 192.168.2.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 6.541/19.475/38.307/9.851 ms
root@teleml-tesis:~#
```

Figura 13. Envío de PING entre los servidores conectados por VPN.

Fuente: Elaboración propia.

VI.6 Sincronización de los servidores

Una vez realizadas las configuraciones necesarias para llevar a cabo la conexión y sincronización de ambos servidores, se realizaron las pruebas pertinentes, logrando verificar el correcto funcionamiento tanto de la conexión VPN como del establecimiento del servidor de respaldo.

DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA (UCV) Y TELEMEDICINA (UCAB)

En la siguiente imagen se puede observar que la sincronización de ambos servidores se realizó de forma exitosa, ya que al colocar el comando especificado en la parte de desarrollo, se actualizaron los archivos correspondientes a la base de datos contenidos en el servidor principal (consulta, especialistas, pacientes y seguridad). Permitiendo obtener en el servidor de la UCAB un respaldo de toda la información de los pacientes en caso de que el servidor de la UCV presente alguna falla.

```
root@teleml-tesis:/var/lib/mysql/db_tesis20136# rsync -vuArtlpoge 'ssh -p 22' root@192.168.2.4:/var/lib/mysql/bdtesis/ /var/lib/mysql/db_tesis20136/
receiving incremental file list
/
consulta.MYD
consulta.MYI
consulta.frm
db.opt
especialistas.MYD
especialistas.MYI
especialistas.frm
lock -> /run/lock
pacientes.MYD
pacientes.MYI
pacientes.frm
run -> /run
seguridad.MYD
seguridad.MYI
seguridad.frm
backups/
backups/apt.extended_states.0
backups/apt.extended_states.1.gz
backups/apt.extended_states.2.gz
backups/apt.extended_states.3.gz
backups/apt.extended_states.4.gz
backups/dpkg.status.0
```

Figura 14. Sincronización de la base de datos hacia el servidor de respaldo.

Fuente: Elaboración propia.

Luego, para verificar que efectivamente los archivos de la base de datos se sincronizaron correctamente en la carpeta MySQL del servidor de la UCAB, se procedió a hacer lo siguiente:

- Para ir al directorio del servidor de la UCAB en el que se guardaron los archivos de la base de datos, se utilizó el comando:

```
#cd /var/lib/mysql/db_tesis20136
```

- Posteriormente, para observar todos los archivos que se encuentran en ese directorio, se utilizó el comando:

```
#ls
```

Esto se puede observar en la Figura 15:

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

```
root@telem1-tesis:~# cd /var/lib/mysql/db_tesis20136
root@telem1-tesis:/var/lib/mysql/db_tesis20136# ls
backups      consulta.MYD  db.opt       especialistas.MYI  local  mail      pacientes.MYD  seguridad.frm  spool
cache        consulta.MYI  especialistas.frm  games            lock  opt       pacientes.MYI  seguridad.MYD  tmp
consulta.frm  crash        especialistas.MYD  lib              log   pacientes.frm  run           seguridad.MYI
root@telem1-tesis:/var/lib/mysql/db_tesis20136#
```

Figura 15. Base de datos alojada en el servidor de respaldo (UCAB).

Fuente: Elaboración propia.

VI.7 Resultado del Desarrollo de la Aplicación

Luego de comprobar que la conexión entre el cliente y el servidor fuese exitosa, y después de haber creado completamente la base de datos, se realizó la página web mediante el software de Dreamweaver.

Para poder ejecutar las pruebas de funcionamiento, se trasladó al servidor principal (UCV) la carpeta que contenía todos los archivos correspondientes a la aplicación.

A continuación se muestra en forma detallada el resultado final de la aplicación.

Para poder acceder a la página principal de la página web, se debe colocar la siguiente dirección:

<https://fis-lab.ciens.ucv.ve>

Una vez hecho esto, se mostrará la Página principal, en donde se presentará al usuario una ventana solicitando la introducción de un usuario y contraseña. Si no se introducen los datos correctamente, no se tendrá acceso a la aplicación. Dicha información será otorgada por los administradores de la aplicación en cada una de las casas de estudio. (Ver Figura 16)

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**



Figura 16. Ingreso a la Página web.

Fuente: Elaboración propia.

Una vez logrado el acceso a la aplicación, se mostrará la siguiente página:

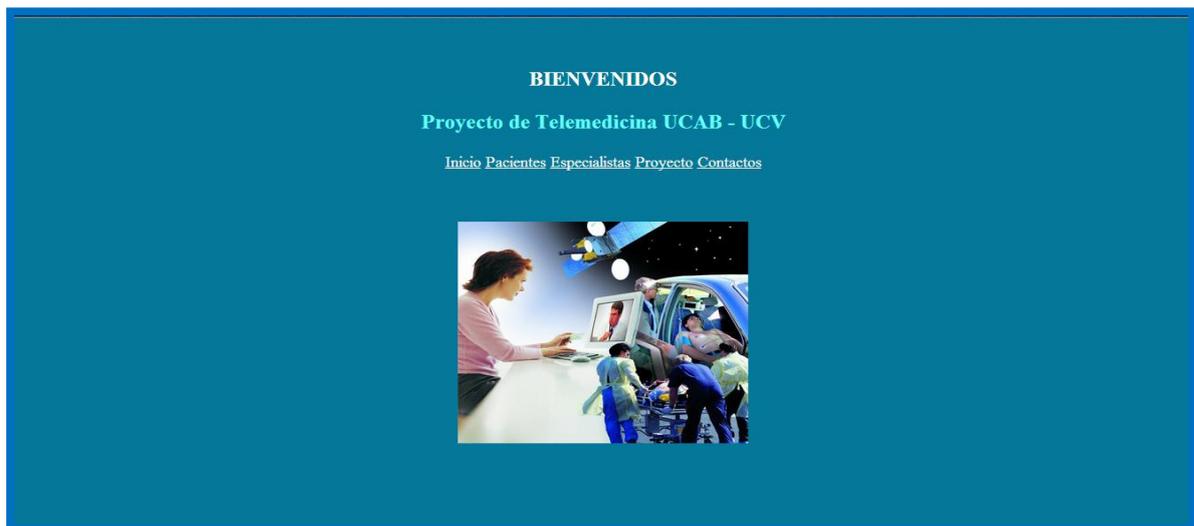


Figura 17. Página de Inicio.

Fuente: Elaboración propia.

Para que el usuario pueda tener acceso a la información contenida en la página web debe registrarse previamente.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Justo arriba de la imagen que se observa en la página de inicio, se pueden ver cinco vínculos, mediante los cuales el usuario puede acceder a las distintas partes de la aplicación dependiendo de lo que desee hacer: Inicio, Pacientes, Especialistas, Proyecto y Contactos.

- **Inicio**
Conduce al usuario a la página de inicio.
- **Pacientes.** En caso de que el usuario sea paciente debe elegir esta opción, y a continuación le saldrá una pantalla, en la cual tendrá tres opciones:

Opción 1: Acceso. Si el paciente ya posee una cuenta podrá acceder con su nombre de usuario y su contraseña.

Si el usuario coloca sus datos de forma correcta, le aparecerá una pantalla en la que debe llenar una serie de preguntas que quedarán registradas en la base de datos, de manera que esta información luego pueda ser vista por especialistas a fin de que puedan realizar un diagnóstico preliminar a distancia de la salud del paciente.

Cabe destacar que en esa sección, el paciente debe indicar los valores de tres parámetros fisiológicos (temperatura de piel, frecuencia cardíaca, frecuencia respiratoria) que puede medir directamente de manera sencilla por sí mismo mediante el dispositivo BioHarness BioModule y transcribirlos manualmente o bien puede hacer uso de un dispositivo portátil que los adquiera y los transmita por alguna vía.

Opción 2: Registro de usuarios. En este caso, los pacientes que no posean una cuenta podrán hacerlo registrando sus datos en la aplicación web.

Una vez que el paciente llene todos los campos requeridos para registrarse, se mostrará una pantalla que indique que se ha registrado exitosamente. Además, en dicha página tendrá la opción de Iniciar sesión, en donde ahora sí podrá acceder colocando el nombre de usuario y la clave que indicó al momento de registrarse.

Opción 3: ¿Olvidó su contraseña?. Si el usuario ya se registró pero no recuerda su clave, deberá seleccionar esta opción.

A continuación, se le pedirá el correo electrónico al usuario para poder enviarle por esa vía su nombre de usuario y su contraseña.

- **Especialistas.** En caso de que el usuario sea especialista debe elegir esta opción, y a continuación le saldrá una pantalla, en la cual tendrá tres opciones:

Opción 1: Acceso. Si el especialista ya posee una cuenta podrá acceder con su nombre de usuario y su contraseña.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Si el especialista coloca sus datos de forma correcta, le aparecerá una pantalla en la que se muestra toda la información de cada uno de los pacientes que se encuentran registrados en la base de datos. De esta manera el especialista podrá realizar un diagnóstico preliminar de la salud de alguno de los pacientes y contactarlo a través del correo electrónico del mismo.

Opción 2: Registro de usuarios. En este caso, los especialistas que no posean una cuenta podrán hacerlo registrando sus datos en la aplicación web.

Una vez que el especialista llene todos los campos requeridos para registrarse, se mostrará una pantalla que indique que se ha registrado exitosamente. Además, en dicha página tendrá la opción de Iniciar sesión, en donde ahora si podrá acceder colocando el nombre de usuario y la clave que indicó al momento de registrarse.

Opción 3: ¿Olvidó su contraseña?. Si el usuario ya se registró pero no recuerda su clave, deberá seleccionar esta opción.

A continuación, se le pedirá el correo electrónico al usuario para poder enviarle por esa vía su nombre de usuario y su contraseña.

- **Proyecto.** Contiene una breve explicación acerca del objetivo general del proyecto.
- **Contactos.** Muestra información correspondiente a quienes diseñaron la aplicación y una dirección de correo electrónico como medio de contacto en caso de dudas, sugerencias o fallas.

Haciendo referencia a los resultados obtenidos al realizar las pruebas de funcionamiento de la aplicación, se tomaron en consideración una serie de parámetros claves para garantizar el correcto funcionamiento, tales como la vinculación entre la base de datos y la aplicación, las restricciones en el acceso de usuarios, inicio y cierre de sesión, ofreciendo en todo momento la confidencialidad de la información procesada.

VII. Conclusiones

Mediante la elaboración del presente Trabajo Especial de Grado, se logró llevar a cabo el diseño de una red privada virtual que permitiera la conexión y sincronización de los servidores para aplicaciones en Telesalud ubicados con los Grupos de Física Médica (UCV) y Telemedicina (UCAB). También, se logró desarrollar una aplicación web con el fin de que los pacientes puedan obtener un diagnóstico preliminar oportuno y objetivo de una forma segura, sencilla, confiable y eficaz, sin necesidad de trasladarse a un centro clínico.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

De esta manera, se pudo brindar una solución en el caso de los pacientes que se encuentran ubicados en zonas alejadas de los centros urbanos y con dificultades de acceso a centros hospitalarios y la atención médica adecuada.

Es importante mencionar que el desarrollo de este proyecto permitió adquirir conocimientos más extensos en el área de la telemedicina, logrando experimentar la importancia y necesidad que ésta tiene en el mundo actual. Así como también, en otros temas, tales como: creación de páginas web, bases de datos, entre otros aspectos de gran interés.

Cabe destacar que el proyecto se desarrolló en equipos que poseen información confidencial y el tipo de información enviada a través de la red también lo es, por lo tanto la protección de la seguridad y confiabilidad de los datos fueron los puntos más importantes a tomar en cuenta tanto en el diseño de la red como en la aplicación.

Por último, se puede decir que las redes VPN son una alternativa altamente confiable para el intercambio de información confidencial entre dos o más usuarios, ya que envía la información cifrada a través de un túnel por lo que la información que viaja a través del mismo lo hará de una manera más segura y confiable.

VIII. Recomendaciones

- Se recomienda tomar en cuenta el estado y la disponibilidad de los equipos a utilizar, considerando aspectos como: sistema operativo, capacidad de almacenamiento, procesamiento, etc., antes de realizar el diseño de la red privada virtual. De esta manera, se facilitará luego el desarrollo de la misma.
 - Solicitar con tiempo los permisos necesarios para poder acceder a los servidores o equipos a utilizar, por ello se sugiere comunicarse constantemente con los distintos departamentos que controlan dichos equipos.
 - Es importante que sólo personal autorizado pueda acceder a la aplicación para poder manejar la confidencialidad de los datos. En este caso, sólo personal de la UCAB y de la UCV.
 - Para evitar sobrecargas del servidor, se recomienda hacer la sincronización en horas de poco tráfico y simular localmente la funcionalidad de cada comando antes de ejecutarlos directamente en los servidores.
 - Se recomienda tener un mantenimiento constante del servidor donde se aloja la base de datos y mantener un respaldo actualizado para evitar posibles fallas del sistema y pérdidas significativas de información.
-

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

- Por último, se sugiere evaluar diferentes alternativas u opciones antes de seleccionar una tecnología o protocolo, para de esta forma seleccionar luego la opción que mejor se ajuste a las necesidades del proyecto.

IX. Bibliografía

Benítez, F. y Méndez, A. (2010). *Estudio e implementación, en una red de hospitales, de servicios de intercambio de imágenes médicas, usando FTP y el modelo cliente-servidor*. Trabajo Especial de Grado, Universidad Católica Andrés Bello.

Gutiérrez, Paulo (2012). Computación y electrónica. Consultado el día 16 de Agosto de 2013 de la World Wide Web: http://www.ehowenespanol.com/codigo-html-sitio-web-como_161728/

Herrera, W. (2011). *Qué es el protocolo HTTPS, cómo funciona y para qué sirve?*. Consultado el día 30/03/2013 de la World Wide Web: <http://www.webadictos.com.mx/2011/04/13/que-es-el-protocolo-https-y-comofunciona/>

Lamana, Ángel. (2012). *Transferencia segura de datos SFTP*. Consultado el día 07 de Junio de 2013 de la World Wide Web: <http://www.hardwareyredes.es/2012/transferencia-segura-de-datos-sftp/>

López, José (2004). *Protocolo SSH*. Recuperado el 10 de Abril de 2013, de: http://sopa.dis.ulpgc.es/ii-aso/portal_aso/lelinux/seguridad/ssh/ssh.pdf

Rodríguez, Yorleny. (03 de Julio de 2012). *VPN - Red privada virtual*. Recuperado el día 16 de Mayo de 2013, de: <http://vpnyorle.blogspot.com/>

Sánchez, Carlos. (2011). *Telesalud*. Recuperado el día 20 de Septiembre de 2013, de: <http://www.slideshare.net/bsuve/telesalud-6451538>

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Sierra, Manuel (2012). *¿Qué es un servidor y cuáles son los principales tipos de servidores?*. Consultado el día 05 de Diciembre de 2012 de la World Wide Web: http://www.aprenderaprogramar.com/index.php?option=com_attachments&task=download&id=487

Torres, Ariel. (2013). *Cursos telecomunicaciones*. Consultado el día 24 de Agosto de 2013 de la World Wide Web:

<http://www.alegsa.com.ar/Dic/sincronizar%20archivos.php>

Universidad Pública de Navarra. (s.f.). *TCP: Características Establecimiento y finalización de conexiones*. Consultado el día 10 de Diciembre de 2012 de la World Wide Web: https://www.tlm.unavarra.es/~daniel/docencia/ro_is/ro_is06_07/slides/11-TCP.pdf

Universidad Tecnológica Nacional. (s.f.). *Redes de Información*. Consultado el día 10 de Diciembre de 2012 de la World Wide Web: http://www.profesores.frc.utn.edu.ar/sistemas/ingsanchez/Redes/Archivos/Protocolo_UDP.pdf

Valade, J. (2008). *PHP y MySQL Para Dummies*, 2a Edición.

Ximenez, P. (s.f.). *Protocolo SSL (Secure Socket Layer)*. Consultado el día 20 de Febrero de 2013 de la World Wide Web: <http://www.pedroximenez.com/ssl.htm>

Zephyr Technology Corporation. (2010). *Manual BioHarness BioModule*.

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

APÉNDICES

APÉNDICE A

Tabla de comandos empleados en CENTOS

**DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)**

Comandos empleados en CENTOS

<code>#su - root</code>	Entrar en el Shell del root.
<code>#man 'comando_a_consultar'</code>	Permite ver el manual de cada comando.
<code>#man man</code>	Permite ver todo el manual.
<code>#mount</code>	Permite visualizar si hay unidad de DVD montada.
<code>#mount /dev/sr0 /mnt</code>	Montar un CD en el directorio /mnt.
<code>#unmount /mnt</code>	Desmontar el CD ubicado en el directorio.
<code>#cd /mnt</code>	Entrar en el CD que se encuentre montado.
<code>#ls</code>	Permite ver todos los archivos del directorio en donde se encuentre.
<code>#mkdir 'nombre_del_directorio'</code>	Crear un directorio.
<code>#pwd</code>	Mostrar el directorio actual.
<code>#nmap localhost</code>	Observar si los puertos se encuentran activos.
<code>#tail -f /var/log/messages</code>	Mostrar los últimos errores de línea.
<code>#kill num_proceso</code>	Terminar el servicio especificado.
<code>#/etc/init.d/'servicio' start</code>	Iniciar el servicio.
<code>#find / -name 'archivo_a_buscar'</code>	Buscar un archivo.
<code>#chmod 777</code>	Activar lectura, escritura y compresión para el propietario, grupo y otros.
<code>#/etc/init.d/network restart</code>	Reiniciar el servicio de red.
<code>#tar cvfz 'archivo'</code>	Comprimir un archivo.
<code>#rm -rf *</code>	Borrar todos los archivos dentro del directorio.
<code>#cat nombre_archivo</code>	Observar el script desde la línea de comandos.
<code>#scp archivo_a_transferir ip_vpn_destino:/root/</code>	Transferir un archivo a través de la VPN.

Tabla 5. Tabla de Comandos empleados en CENTOS.

Fuente: Elaboración propia.

APÉNDICE B

Esquema de la Página Web

DISEÑO DE UNA VPN PARA LA CONEXIÓN Y SINCRONIZACIÓN ENTRE LOS SERVIDORES
PARA APLICACIONES EN TELESALUD UBICADOS EN LOS GRUPOS DE FÍSICA MÉDICA
(UCV) Y TELEMEDICINA (UCAB)

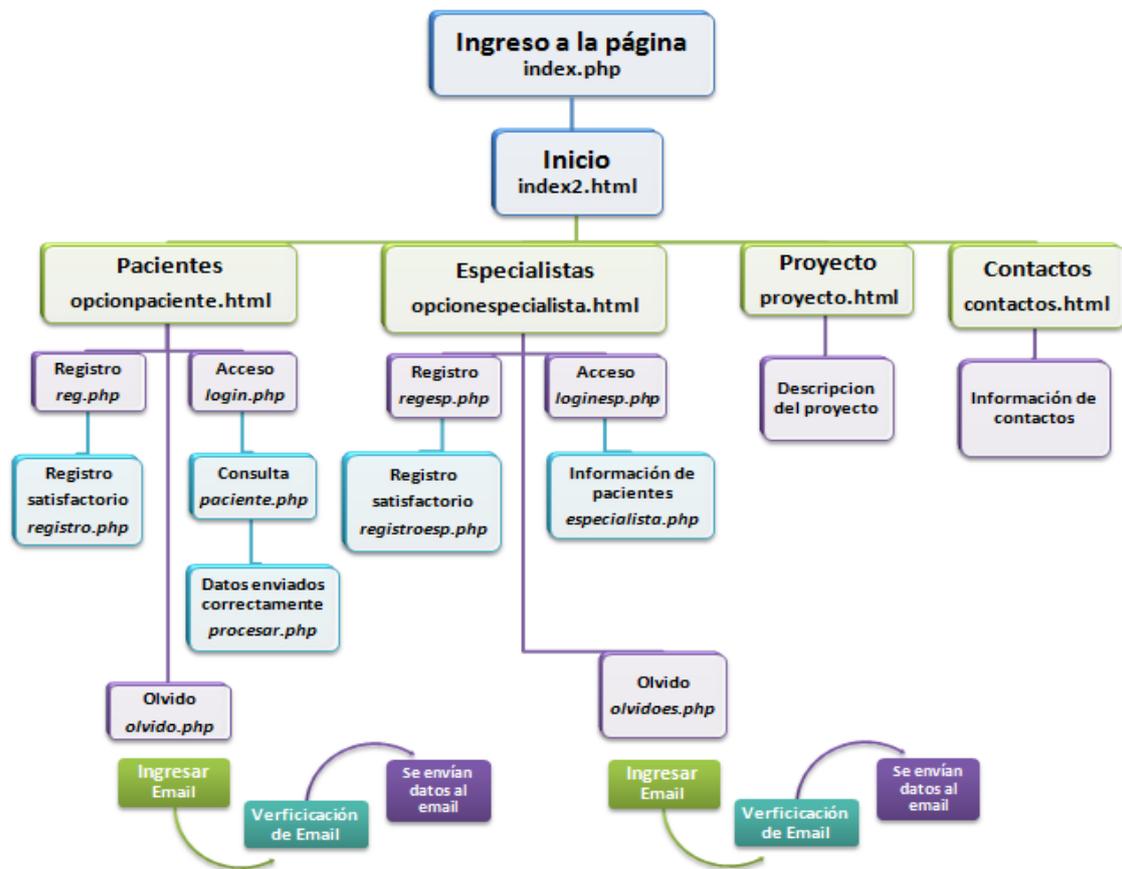


Figura 18. Esquema de la Página Web.

Fuente: Elaboración propia.
