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)

TRABAJO ESPECIAL DE GRADO

Presentado ante la:

UNIVERSIDAD CATÓLICA ANDRÉS BELLO.

Como parte de los requisitos para optar por el título de:

INGENIERO EN TELECOMUNICACIONES.

REALIZADO POR: María G. Camacho R.
Mirelly S. Carrillo C.

TUTOR: Iván Escalona.

FECHA: Octubre de 2013.

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)

TRABAJO ESPECIAL DE GRADO

Presentado ante la:

UNIVERSIDAD CATÓLICA ANDRÉS BELLO.

Como parte de los requisitos para optar por el título de:

INGENIERO EN TELECOMUNICACIONES.

REALIZADO POR: María G. Camacho R.
Mirelly S. Carrillo C.

TUTOR: Iván Escalona.

FECHA: Octubre de 2013.

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)

Este Jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: _____

JURADO EXAMINADOR

Firma:	Firma:	Firma:
Nombre: _____	Nombre: _____	Nombre: _____

REALIZADO POR: María G. Camacho R.
Mirelly S. Carrillo C.

TUTOR: Iván Escalona.

FECHA: Octubre de 2013.

Dedicatoria

A mis padres y a mi hermana por estar siempre a mi lado y apoyarme en cada momento. Los amo.

María G. Camacho R.

A mis padres, por creer en mí y apoyarme en cada momento.
A mi abuela y mis tíos, por brindarme su apoyo incondicional.
Gracias por estar a mi lado.

Mirelly S. Carrillo C.

Agradecimientos

A nuestros padres y familiares por acompañarnos en todo momento y por apoyarnos en cada una de nuestras metas.

A nuestro tutor Iván Escalona y al Profesor Germán Tovar, quienes nos brindaron todo su apoyo, su dedicación y sus conocimientos en el desarrollo de este proyecto.

A Christian Carro, por toda la ayuda y el apoyo que nos brindó durante la elaboración del presente trabajo.

A todos nuestros amigos, quienes nos acompañaron en todo momento a lo largo de nuestra carrera universitaria, y con los cuales esperamos seguir contando el resto de nuestras vidas.

Muchas gracias a todos, sin ustedes nada de esto habría sido posible.

María G. Camacho R.

Mirelly S. Carrillo C.

Resumen

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

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.

Índice General

Índice de Figuras

Índice de Tablas

Introducción

Hoy en día la telemedicina ha tomado fuerte presencia dentro del mundo de las telecomunicaciones, aprovechándola para brindar asistencia remota de personal médico especializado sin importar la zona geográfica en la que se encuentre, pudiendo intercambiar datos médicos entre distintos centros de salud.

Las telecomunicaciones, las tecnologías multimedia y el acceso a Internet son de alguna forma, imprescindibles en el sector médico, ya que la telemedicina actúa como integrador de diferentes tecnologías y sobre todo para mejorar la calidad del sistema asistencial médico. Aplicaciones asíncronas, como el uso del correo electrónico para la transferencia de imágenes o consultas de los pacientes vía web, o síncronas, como el uso de videoconferencias para realizar consultas o examinar pacientes en tiempo real son las más utilizadas en distintos centros médicos a nivel mundial.

El hecho de contar con una aplicación que integre los grupos de Física Médica de la Facultad de Ciencias de la UCV y Telemedicina de la UCAB, es lo que se viene desarrollando, de manera que estos grupos puedan interactuar de forma remota mediante una página web que procese la información. La meta de este proyecto consiste en poder contar con atención médica especializada para realizar diagnósticos y estudios de pacientes a distancia, así como también tener un respaldo de toda la información que se maneja entre dichos grupos, dado que la información que se encuentra almacenada podría correr cualquier riesgo informático, como fallas mecánicas del disco duro, virus u otros riesgos, por lo que de alguna manera el servicio que se presta fallaría, inhabilitando la conexión. Surge entonces la idea de resguardar la información contenida en el servidor principal (UCV) en un servidor de respaldo (UCAB). Con todo esto se asegura el correcto funcionamiento y disponibilidad de la conexión entre ambos centros.

La telemedicina en el presente no debe entenderse sencillamente como una tecnología, sino como un nuevo sistema organizativo de la profesión médica, brindando ayuda tanto a médicos y personal auxiliar como a pacientes, ahorrando tiempo y dinero.

El contenido del presente proyecto se presentará en seis capítulos, organizados de la siguiente manera:

- Capítulo I: se describe el planteamiento del problema, los objetivos, alcances y limitaciones del proyecto y la justificación que le da origen.

- Capítulo II: se presentan las bases teóricas que fundamentan todo el desarrollo del trabajo, brindando una base firme de los conocimientos necesarios a saber.

- Capítulo III: se presentan la metodología y procedimientos utilizados para poder llevar a cabo el presente proyecto.

- Capítulo IV: contempla el desarrollo de los pasos y actividades detalladas, describiendo la manera de lograr concretar el proyecto.

- Capítulo V: se presentan los resultados obtenidos en el desarrollo de la aplicación, describiendo cada uno con su respectiva interpretación.

- Capítulo VI: se describen las conclusiones y recomendaciones tomando en cuenta los resultados obtenidos.

Capítulo I
Planteamiento del Problema

En este capítulo se plantea el problema que da origen al proyecto en general. Así como también, se establecen los objetivos, se justifica el proyecto y la importancia en el área de las telecomunicaciones, y finalmente se definen los alcances y limitaciones que delimitan de forma clara y precisa hasta dónde se va a desarrollar el proyecto.

I.1 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, así como llevar a cabo el intercambio de información entre distintos centros de salud e investigación científica.

Se puede decir que la telemedicina es un recurso tecnológico que posibilita la optimización de los servicios de atención en salud, ahorrando tiempo y dinero al ofrecer la facilidad de contar con la atención de especialistas médicos a distancia.

Sin embargo, la tecnología no está exenta de fallas o errores, ya que los archivos contenidos en servidores utilizados para aplicaciones de telemedicina pueden borrarse por distintos motivos, como por ejemplo: virus, fallas mecánicas del disco duro, ataques malintencionados, fallas en el hardware, o incluso por accidentes (robos, incendios, inundaciones). En la mayoría de los casos, ante estos eventos, la información una vez perdida es muy difícil y hasta imposible de

recuperar, a menos que se haya hecho un respaldo de la misma. Un archivo perdido puede representar el trabajo de varios días o meses, que en un segundo pueden quedar totalmente eliminados e imposibles de recuperar.

Es por esto que, 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 o personal especializado, 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), específicamente de la Escuela de Física de la Facultad de Ciencias, y el Grupo de Telemedicina de la Universidad Católica Andrés Bello (UCAB), específicamente de la Escuela de Ingeniería en Telecomunicaciones de la Facultad de Ingeniería, con el fin de que puedan intercambiar información, para que pueda ser estudiada y evaluada por personal especializado. Por simplicidad en el desarrollo ambos grupos serán referidos solamente con la respectiva universidad de adscripción.

I.2 Objetivos

I.2.1 Objetivo 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 de la Universidad Central de Venezuela (UCV) y el Grupo de Telemedicina de la Universidad Católica Andrés Bello (UCAB).

I.2.2 Objetivos 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 correspondientes a los centros de investigación: Grupo de Física Médica de la Universidad Central de Venezuela (UCV) y Grupo de Telemedicina de la Universidad Católica Andrés Bello (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.

I.3 Alcances y limitaciones

I.3.1 Alcances

Este Trabajo Especial de Grado incluye la elaboración del diseño e implementación de 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 de la Universidad Central de Venezuela (UCV) y el Grupo de Telemedicina de la Universidad Católica Andrés Bello (UCAB). Así como también, la elaboración de una página web que le permita a los especialistas de dichos centros, la posibilidad de realizar diagnósticos a distancia a partir de la información que quede registrada en la aplicación por parte de los pacientes.

I.3.2 Limitaciones

- El establecimiento de los servidores se realizará únicamente en la Universidad Católica Andrés Bello y en la Universidad Central de Venezuela.
- Todas las herramientas y software utilizados, serán destinados a su uso en LINUX.
- Se requiere contar con los permisos correspondientes por parte de las correspondientes Direcciones de Tecnologías de Información de la UCAB y de la UCV para la construcción de la red VPN.

I.4 Justificación

La realización de una interconexión entre la UCAB (Universidad Católica Andrés Bello) y la UCV (Universidad Central de Venezuela) surge con la necesidad de los grupos de Física Médica de la UCV y Telemedicina de la UCAB, de realizar un intercambio de información entre ambos, con el propósito de que los profesionales vinculados, puedan aportar su opinión en los casos correspondientes.

La elaboración del presente proyecto se plantea 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, sencilla, 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 los distintos centros de salud e investigación científica o personal especializado.

Capítulo II
Marco Referencial

Luego de tener una visión general de lo que es el planteamiento del problema y tomando en cuenta los objetivos propuestos, se deben reflejar las bases teóricas para la realización del proyecto de grado.

En primer lugar se hace referencia a los proyectos que constituyen sus antecedentes, precedido de una serie de conceptos que definen el contenido teórico que abarca el trabajo.

Como se puede apreciar en la Figura 1, las bases teóricas que le dan apoyo se dividen en varias ramas, partiendo desde los aspectos generales de la telemedicina, tratando definiciones aún más específicas de términos utilizados en el desarrollo práctico del proyecto, como son ciertos parámetros fisiólogicos (temperatura, frecuencia cardíaca, frecuencia respiratoria), así como lo referente a redes privadas virtuales y a las herramientas disponibles para desarrollar una aplicación con el propósito de lograr llevar a cabo el intercambio de información entre los pacientes y especialistas de ambos centros de salud, tales como MySQL para el lenguaje y la gestión de las bases de datos utilizadas, y PHP para la vinculación de la aplicación con la base de datos.

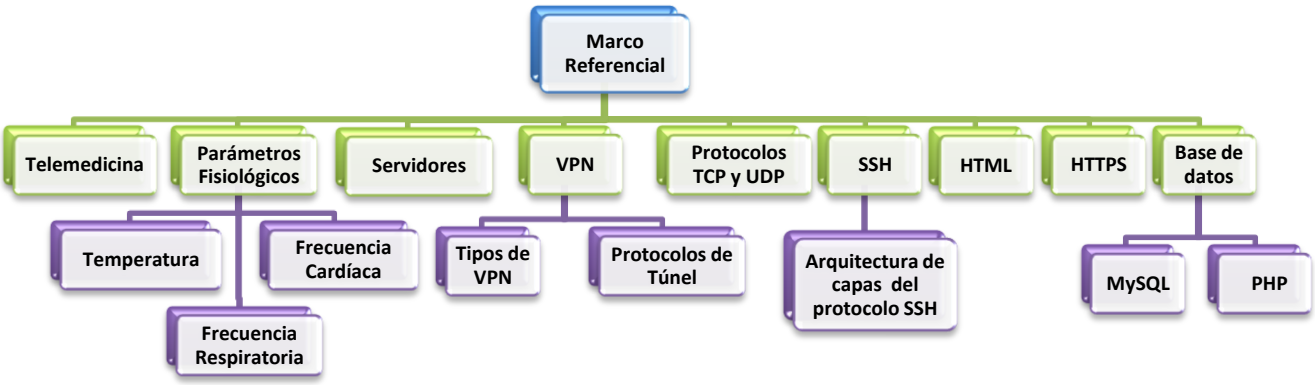

Figura 1. Estructura general del Marco Referencial.

Fuente: Elaboración propia.

II.1 Antecedentes

Desde hace aproximadamente ocho (8) años, se han ido desarrollando un conjunto de trabajos especiales de grado en el área de telemedicina en la Universidad Católica Andrés Bello. Para la realización del presente trabajo especial de grado, se tomaron en cuenta dos trabajos en específico.

El primero de ellos es el de Christian Carro y Yeberlin De Lira (2012), titulado "Diseño de una red privada de teleradiología para el intercambio de imágenes DICOM entre UCV-Física Médica y UCAB Telemedicina.", presentado para optar al título de Ingeniería de Telecomunicaciones en la UCAB, cuyos objetivos principales fueron diseñar una VPN entre los servidores de la UCV y de la UCAB, realizar envío de imágenes en formato DICOM y desarrollar una aplicación que facilite el manejo de datos.

El segundo trabajo a tomar en cuenta fue realizado por Vanessa Quintana (2013), presentado para optar al título de Ingeniería de Telecomunicaciones en la UCAB, titulado "Desarrollo de una aplicación móvil para transmisión y recepción

de parámetros fisiológicos básicos detectados con un módulo portátil", cuyo objetivo principal fue desarrollar una aplicación móvil que permitiera la visualización gráfica de los valores recibidos por el teléfono móvil y la tableta.

Los resultados obtenidos en ambos proyectos, garantizan de alguna manera la ejecución del presente trabajo especial de grado, tomando como base los hallazgos logrados en estos.

II.2 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).

La primera vez que se utilizó la idea de transferir información a larga distancia con fines médicos, ocurrió poco después de inventado el teléfono por Alexander Graham Bell, en la cual el médico fue consultado respecto a tratamientos e indicaciones por pacientes ubicados en zonas alejadas. En la literatura se describe que en 1950, en la Universidad de Pennsylvania, se utilizó el teléfono para transmitir imágenes de radiografías. En 1959, en la Universidad de Nebraska, se unen dos equipos de televisión bidireccional, con otras salas, transmitiendo imágenes y sonido que fueron posteriormente utilizados en terapias de grupo. Adicionalmente, a principios de los años 60 se dio el comienzo de la transmisión radial desde barcos que se encontraban lejos de puerto, y que necesitaban informes médicos de radiografías y electrocardiogramas. En 1967, la Universidad de Miami y el Hospital Jackson Memorial, se transformaron en los pioneros en la transmisión de electrocardiogramas desde unidades móviles de los

bomberos que acuden al rescate de pacientes con sintomatología de origen cardíaco. Ya en 1968, en el Hospital de Massachusetts se transmitieron los primeros sonidos de un estetoscopio, una imagen de microscopio y un electrocardiograma.

II.2.1 Telemedicina en el mundo

Se han desarrollado proyectos en muchos países que han conseguido una gran aceptación en la medicina y en la población que utilizan estos servicios. La ATA (*American Telemedicine Association*), es una de las promotoras de telemedicina en diferentes partes del mundo, en especial en EE. UU., donde promueve el acceso a la atención medica para los pacientes a través de las tecnologías de información y comunicaciones.

Otra de las instituciones es el EHAS (Enlace Hispano Americano de Salud), el cual es una institución sin fines de lucro, que actúa con el propósito de promover el uso apropiado de las nuevas Tecnologías de la Información y la Comunicación (TIC) para mejorar los procesos de salud, especialmente en las zonas rurales. (Díaz y Mazzochi, 2009).

II.2.2 Telemedicina en Venezuela

Una de las primeras organizaciones venezolanas sin fines de lucro en considerar e implementar la telemedicina fue la Fundación Maniapure, la cual en el año 2000 instituyó un ambulatorio rural llamado La Milagrosa, el cual brinda apoyo a la región ubicada en el estado Bolívar, ofreciendo servicio médico integral a través de la telemedicina, así como servicios de laboratorio, odontología y nutrición, además de educación y desarrollo comunitario, lo cual representa hoy en día una importante mejora en la calidad del servicio de salud ofrecido a los habitantes de la zona, donde anteriormente el acceso de los médicos era

prácticamente imposible.

Otras iniciativas importantes desarrolladas en Venezuela se encuentran a cargo de varias universidades desplegadas en todo el territorio venezolano como la Universidad de Carabobo (UC), la Universidad Centrooccidental Lisandro Alvarado (UCLA), la Universidad Simón Bolívar (USB), la Universidad Central de Venezuela (UCV) y la Universidad Católica Andrés Bello (UCAB). Un claro ejemplo es el "Proyecto SOS Telemedicina para Venezuela" desarrollado en la UCV. (Díaz y Mazzochi, 2009).

La medicina a distancia puede clasificarse, en tres grupos básicos:

- Aprendizaje: utilización de tecnologías como el Internet para la enseñanza (*e-learning*), teleconferencias, clases con presencia virtual, entre otros; orientados a la formación de profesionales en medicina y educación en salud al público en general.

- Diagnóstico: este campo de la telemedicina incluye la interconsulta con otros especialistas, envío de electrocardiogramas, imágenes tomográficas, etc.

- Tratamiento: se incluye desde terapias psicológicas hasta el manejo remoto de piezas robóticas, por especialistas calificados, para la realización de intervenciones quirúrgicas.

II.2.3 Sistemas para Telemedicina

Dadas las exigencias de la gran variedad de aplicaciones médicas en telemedicina, adquiere mayor importancia el manejo adecuado de la información del paciente, que pueda brindar una interfaz integrada que mantenga bajo un solo

ambiente la interconsulta y el conjunto de señales e imágenes que describen la enfermedad. Entre los requerimientos de un sistema de telemedicina se encuentran los siguientes:

- Un sistema de Video-Conferencias sobre el cual se establecen las relaciones médico-médico, médico-especialista, médico-especialista-paciente.

- Comunicación de imágenes estáticas y dinámicas de baja resolución en tiempo real, como en el caso de las imágenes ecográficas, otoscópicas y oftalmoscópicas.

- Comunicación de imágenes estáticas o dinámicas de alta definición en tiempo diferido. Este es el caso de la Teleradiología y la Tele-patología.

- Video clip: imágenes dinámicas de alta o baja definición, y operación compartida origen destino.

- Comunicación de señales básicas como estetoscopia (sonido cardíaco y pulmonar).

- Manejo de historias clínicas y bases de datos.

- Comunicación de señales específicas como ECG (electrocardiograma), EEG (electroencefalografía) y Vectocardiogramas.

II.2.4 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)

II.3 Parámetros Fisiológicos

Para poder trabajar, entender y realizar una aplicación que muestre correctamente los parámetros fisiológicos de un paciente se debe primero conocer de forma clara el comportamiento de los valores temperatura, frecuencia cardíaca y frecuencia respiratoria, para luego compararlos con los valores normales.

II.3.1 Temperatura

La temperatura es una magnitud física que expresa el nivel de calor que ostenta un cuerpo determinado, un objeto, un ambiente, entre otros, en tanto, la misma se encuentra estrechamente vinculada a las nociones de frío (menor temperatura) y de calor (mayor temperatura).

La temperatura de un individuo puede variar dependiendo de muchos factores como el sexo de la persona, momento del día, actividad que está realizando en ese momento, la alimentación e ingesta de líquidos (Vorvick, 2011). La medición de la temperatura puede realizarse en distintas zonas del cuerpo, como las axilas, el recto y la boca, entre otros. Dependiendo de la zona en que se tome el valor puede tener una variación entre ± 0,3 º C.

Según la Asociación Médica Americana, los valores promedios de temperatura de una persona normal oscilan entre 36,5º C - 37,2º C (grados Celsius) ó 97,8º F - 99º F (grados Fahrenheit): cualquier valor que sobrepase el valor del límite superior se puede considerar fiebre. (Vorvick, 2011)

II.3.2 Frecuencia Cardíaca

La frecuencia cardíaca, también conocida como pulso cardíaco, es el número de veces que se contrae el corazón en un tiempo determinado y se mide en latidos por minuto o contracciones por minuto. Los valores de frecuencias pueden variar de forma significativa, dependiendo de las demandas que hace el cuerpo humano. Una persona que está durmiendo tendrá la frecuencia cardíaca mucho más baja que una que está realizando ejercicio (Nordqvist, 2011).

Los factores que pueden afectar la frecuencia cardíaca son la temperatura del aire, la posición del cuerpo, el tamaño corporal, peso, y medicación que use la persona. Los rangos de valores adecuados o no adecuados para cada sexo y edad se muestran en la Tabla 1 que se muestra a continuación:

HOMBRES	Mala	Normal	Buena	Muy Buena
20-29	86 o más	70-84	62-68	60 o menos
30-39	86 o más	72-84	64-70	62 o menos
40-49	90 o más	74-88	66-72	64 o menos
50-59	90 o más	74-88	68-74	66 o menos
60 o más	94 o más	76-90	70-76	68 o menos

MUJERES	Mala	Normal	Buena	Muy Buena
20-29	96 o más	78-94	72-76	70 o menos
30-39	98 o más	80-96	72-78	70 o menos
40-49	100 o más	80-98	74-78	72 o menos
50-59	104 o más	84-102	76-82	74 o menos
60 o más	108 o más	88-106	78-88	78 o menos

Tabla 1. Valores Promedio de frecuencia cardíaca.

Fuente: Hernández (s.f.)

II.3.3 Frecuencia respiratoria

La frecuencia respiratoria es el número de veces que una persona respira por minuto. Se suele medir cuando la persona está en reposo, y consiste simplemente en contar el número de respiraciones durante un minuto contando las veces que se eleva su pecho. La frecuencia respiratoria es un signo vital que puede variar con la edad, el sexo, la tolerancia al ejercicio y la condición médica del individuo. La frecuencia respiratoria normal de un adulto que esté en reposo oscila entre 12 y 18 respiraciones por minuto (Dugdale, 2011).

II.3.4 Hipertensión

La hipertensión arterial es el aumento de la presión arterial de forma crónica. Es una enfermedad que no da síntomas durante mucho tiempo y, si no se trata, puede desencadenar complicaciones severas como un infarto de miocardio, una hemorragia o trombosis cerebral, lo que se puede evitar si se controla adecuadamente. Las primeras consecuencias de la hipertensión las sufren las arterias, que se endurecen a medida que soportan la presión arterial alta de forma continua, se hacen más gruesas y puede verse dificultado al paso de sangre a su través. Esto se conoce con el nombre de arteriosclerosis.

La tensión arterial tiene dos componentes:

- La tensión sistólica es el número más alto. Representa la tensión que genera el corazón cuando bombea la sangre al resto del cuerpo.
- La tensión diastólica es el número más bajo. Se refiere a la presión en los vasos sanguíneos entre los latidos del corazón. (Dugdale, 2011)

II.4 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)

La recepción de los datos obtenidos por el sensor puede realizarse mediante un radio o telefonía móvil (Bluetooth) para luego ser enviados a las personas interesadas en tomar decisiones críticas, que serán basadas en la fisiología del individuo. El Bluetooth utilizado para esta tecnología transmite en una frecuencia aproximada de 2,4 GHz y el receptor debe encontrarse posicionado en un rango de 10 mts del equipo que recibirá la señal. (Zephyr Technology Corporation, 2010)

En la Figura 2 se puede observar una imagen del dispositivo BioHarness. Del lado izquierdo se observa el dispositivo principal que contiene todos los sensores encargados de recoger toda la información del paciente. Este maneja valores de tiempo, frecuencia cardíaca, frecuencia respiratoria, posición, temperatura y aceleración del individuo.

Figura 2. Dispositivo BioHarness BioModule.

Fuente: Elaboración propia.

II.5 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.

Los clientes pueden ser personas, o también pueden ser otros dispositivos como ordenadores, móviles, impresoras, etc.

Por lo tanto básicamente tendremos el siguiente esquema general, en el denominado esquema "cliente-servidor" que es uno de los más usados ya que en él se basa gran parte de Internet.

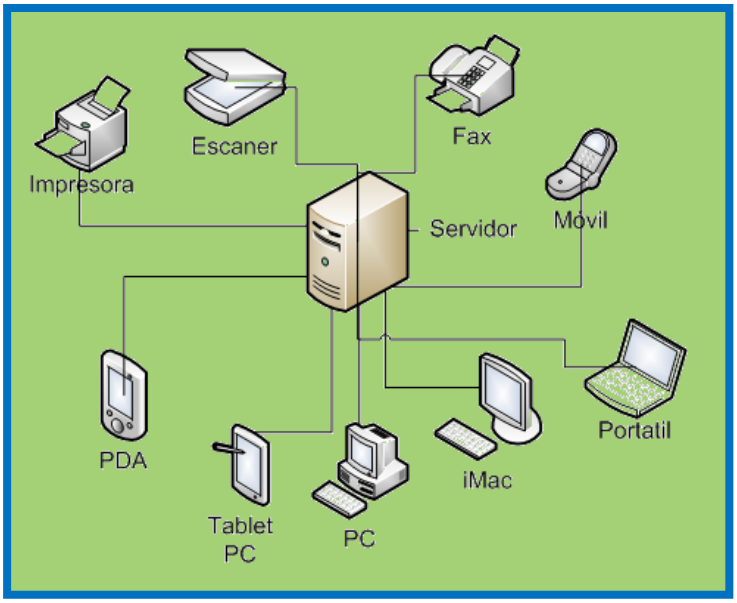

Figura 3. Esquema "Cliente-Servidor".

Fuente: Sierra, Manuel (2012).

Como se puede observar en la Figura 3, se tiene una máquina servidora que se comunica con variados clientes, todos demandando algún tipo de información. Esta información puede ser desde archivos de texto, video, audio, imágenes, emails, aplicaciones, programas, consultas a base de datos, etc.

Por regla general, las máquinas servidoras suelen ser algo más potentes que un ordenador normal. Sobre todo suelen tener más capacidad tanto de almacenamiento de información como de memoria principal, ya que tienen que dar servicio a muchos clientes. Pero como todo, también depende de las necesidades, ya que se puede tener un servidor de menores prestaciones si se va a tener pocos clientes conectados, o si los servicios que se quieran en el servidor no

requieren una gran capacidad servidora. A modo de ejemplo, se podría hacer funcionar un ordenador en la casa como si fuera un servidor, aunque esto no es lo más habitual. Por general, los servidores suelen estar situados en centros de datos de empresas (edificios con grandes salas dedicadas a alojar a los servidores).

II.5.1 Tipos de servidores

Entre los principales tipos de servidores se pueden encontrar:

- Servidor de Correo: es el servidor que almacena, envía, recibe y realiza todas las operaciones relacionadas con el e-mail de sus clientes.

- Servidor Proxy: es el servidor que actúa de intermediario de forma que el servidor que recibe una petición no conoce quién es el cliente que verdaderamente está detrás de esa petición.

- Servidor Web: almacena principalmente documentos de Lenguaje de Marcas de Hipertexto o comúnmente conocido por sus siglas en inglés HTML (HyperText Markup Language), los cuales se presentan a modo de archivos con un formato especial para la visualización de páginas web en los navegadores de los clientes, imágenes, videos, texto, presentaciones, y en general todo tipo de información. Además se encarga de enviar estas informaciones a los clientes.

- Servidor de Base de Datos: da servicios de almacenamiento y gestión de bases de datos a sus clientes. Una base de datos es un sistema que permite almacenar grandes cantidades de información. Por ejemplo, todos los datos de los clientes de un banco y sus movimientos en las cuentas.

- Servidores Clúster: son servidores especializados en el almacenamiento de la información teniendo grandes capacidades de almacenamiento y

permitiendo evitar la pérdida de la información por problemas en otros servidores.

- Servidores de imágenes: recientemente también se han popularizado servidores especializados en imágenes, permitiendo alojar gran cantidad de imágenes sin consumir recursos del servidor web en almacenamiento o para almacenar fotografías personales, profesionales, etc.

- Servidor de archivos: almacena varios tipos de archivo y los distribuye a otros clientes en la red.

- Servidor de telefonía: realiza funciones relacionadas con la telefonía, como la de contestador automático, sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o Internet.

- Servidor de fax: almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax. (Sierra, 2012)

II.5.2 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.

La sincronización permite mantener la misma versión de los archivos en múltiples ubicaciones, generalmente directorios en una computadora, en dispositivos de almacenamiento extraíble, e incluso entre una computadora y un dispositivo móvil.

Este proceso puede hacerse manualmente o automáticamente utilizando alguna herramienta de software, lo que permite más confiabilidad.

La sincronización puede ser en una o dos direcciones. En la sincronización unidireccional, los archivos son copiados sólo desde una ubicación fuente hacia una o más ubicaciones de destino, pero ningún archivo es copiado en el sentido inverso. Por lo tanto las modificaciones hechas en el destino no afectan a la fuente.

En la sincronización bidireccional, los archivos se copian en ambas direcciones, por lo que los archivos se mantienen sincronizados en ambas ubicaciones. Cada vez que agrega, cambia o elimina un archivo en cualquier ubicación, ese mismo cambio también se realiza en la otra ubicación de sincronización. (Torres, 2013)

II.6 VPN *(Virtual private network)*

Las redes de área local (LAN) son las redes internas de las organizaciones, es decir, las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante un equipo de interconexión. Muchas veces, las empresas necesitan comunicarse por Internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente.

Sin embargo, los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no está definida por anticipado, lo que significa que los datos deben atravesar una infraestructura de red pública que pertenece a distintas entidades. Por esta razón, es posible que a lo largo de la línea, un usuario entrometido tenga acceso a la información transmitida. Por lo tanto, la información confidencial de una organización o empresa no debe ser enviada bajo tales condiciones.

Una buena solución para esta situación consiste en utilizar Internet como medio de transmisión con un protocolo de túnel, a través del cual los datos se encapsulan antes de ser enviados de manera cifrada. El término red privada virtual (abreviado VPN) se utiliza para hacer referencia a la red creada artificialmente de esta forma. 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.

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.

La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que cifra y descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario. (Rodríguez, 2012)

II.6.1 Protocolos de túnel

Los principales protocolos de túnel son:

- **Protocolo PPTP (Protocolo de túnel punto a punto):** consiste en crear tramas con el protocolo PPP (Punto a Punto) y encapsularlas mediante un datagrama de IP. Por lo tanto, con este tipo de conexión, los equipos remotos en dos redes de área local se conectan con una conexión de igual a igual (con un sistema de autenticación/cifrado) y el paquete se envía dentro de un datagrama de IP. De esta manera, los datos de la red de área local (así como las direcciones de los equipos que se encuentran en el encabezado del mensaje) se encapsulan dentro de un mensaje PPP, que a su vez está encapsulado dentro de un mensaje IP.

- **Protocolo L2TP:** es un estándar creado por la IETF (Internet Engineering Task Force) que combina las mejores características de dos protocolos: L2F (Cisco's Layer 2 Forwarding) y el protocolo PPTP, permitiéndoles a los usuarios conectarse a su intranet o extranet corporativa a través de cualquier medio que soporte datagramas point to point como IP, Frame Relay, X25 o ATM (Modo de Transferencia Asíncrona). El túnel L2TP (Layer 2 Tunneling Protocol) se crea encapsulando una trama L2TP en un paquete UDP (User Datagram Protocol) el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Esto no sólo reduce el costo asociado al overhead de los métodos de acceso remoto tradicionales, sino que mejora la flexibilidad y escalabilidad.

- **Protocolo IPSEC (*Internet Protocol security*):** es un protocolo definido por el IETF que se usa para transferir datos de manera segura en la capa de red. En realidad es un protocolo que mejora la seguridad del protocolo IP para garantizar la privacidad, integridad y autenticación de los datos enviados. Está basado en tres módulos:

- ✓ Encabezado de autenticación IP (AH, Authentication Header), que incluye integridad, autenticación y protección contra ataques de REPLAY a los paquetes.

- ✓ Carga útil de seguridad encapsulada (ESP, Encapsulating Security Payload), que define el cifrado del paquete. ESP brinda privacidad, integridad, autenticación y protección contra ataques de REPLAY.

- ✓ Asociación de seguridad (SA) que define configuraciones de seguridad e intercambio de clave. Las SA incluyen toda la información acerca de cómo procesar paquetes IP (los protocolos AH y/o ESP, el modo de transporte o túnel, los algoritmos de seguridad utilizados por los protocolos, las claves utilizadas, etc.). El intercambio clave se realiza manualmente o con el protocolo de intercambio IKE (en la mayoría de los casos), lo que permite que ambas partes se escuchen entre sí.

- **Protocolo OpenVPN:** es un protocolo que permite establecer redes privadas virtuales de forma segura, encriptada, fácil, rápida y con múltiples características para usos diversos en implementación de redes virtuales corporativas basadas en el protocolo SSL (Secure Socket Layer) también conocido como Capa de conexión segura.

  OpenVPN ofrece conectividad punto a punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas IEEE 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. (León, 2012)

Actualmente existen muchas arquitecturas para la implementación de una VPN. Dentro de las más importantes se encuentran:

- **VPN basada en Firewall:** es probablemente la forma más común de implementar VPN hoy en día. Esta arquitectura consta básicamente de un Firewall, el cual posee la facultad de establecer túneles VPN. Este equipo se

encuentra ubicado entre la red privada de una empresa y la red pública.

- **VPN basada en caja negra:** en este tipo de arquitectura, la VPN se establece gracias a un equipo (caja negra), el cual es básicamente es un dispositivo equipado con software de encriptación para crear un túnel VPN.
- **VPN basada en router:** las VPN basadas en router son posibles para una organización que tienen una gran inversión en router y un equipo de administración experimentado con ellos. Hay dos tipos de VPN basadas en router. Una es donde el software es agregado al router para permitir que el proceso de encriptación ocurra. Un segundo método es donde una tarjeta externa (posiblemente de otro fabricante) es insertada dentro del mismo chasis del router. Este segundo método es diseñado para dejarle el overhead asociado con el proceso de encriptación a la tarjeta y no a la Unidad Central de Procesamiento ó CPU (Central Processing Unit) del router.
- **VPN basada en software:** una VPN basada en software es básicamente un software que implementa tunneling o encriptación hacia otro host. Esto es usualmente usado en clientes y servidores. Por ejemplo, en una VPN PPTP el software ejecutándose en el cliente se conecta al software ejecutándose en el servidor y establece una sesión VPN. Cuando se elige una solución de este tipo se necesita tener un buen proceso de administración de llaves y posiblemente una autoridad certificadora. Con los otros tipos de VPN las únicas llaves que son necesarias son desde VPN hasta VPN. Esto significa que el tráfico en la red interna esta desencriptado, así que solamente se necesitan llaves para los dispositivos VPN. Pero en el caso de cliente/servidor cada estación debe tener su propio par de llaves públicas/privadas. (Sánchez, 2013)

II.6.2 Tipos de VPN

- **VPN de acceso remoto:** es el tipo de VPN más comercial ya que le facilita tanto al cliente como al proveedor de servicio tener acceso a la red una vez sea autenticada la identidad del mismo desde cualquier zona geográfica siempre y cuando haya servicio de Internet. Esta tecnología ha impulsado el cambio de *Dial-up* a la implementación de las VPN en forma más eficaz y segura. (Ver Figura 4)

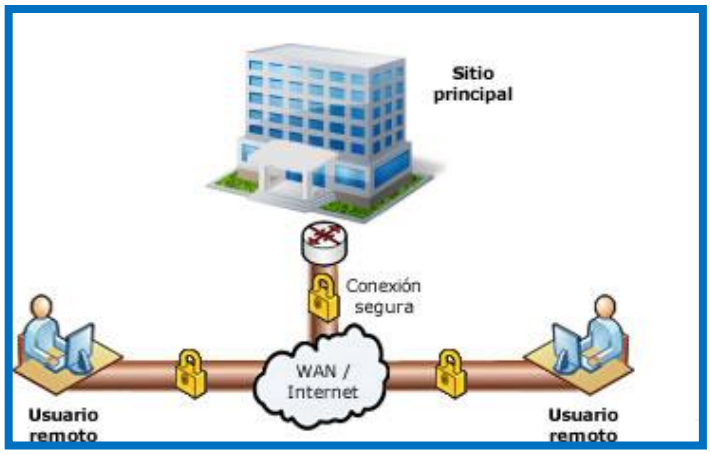

Figura 4. VPN con acceso remoto.

Fuente: Net Humans. (s.f.).

- **VPN punto a punto:** está compuesto por un servidor VPN fijo con conexión a Internet permanente, el cual crea un túnel con el fin de establecer conexión con distintos servidores que deseen intercambiar información con el mismo a través del Internet. Generalmente es utilizado en las grandes empresas con sucursales en distintas ciudades y/o países alejados del servidor VPN. Ahorra los costos de conexión y facilita la comunicación entre las sucursales, es por ello que ha sido tan implementado por las grandes empresas a nivel mundial. Comúnmente ha sido utilizado con Internet de Banda Ancha. (Ver Figura 5)

Figura 5. VPN punto a punto.

Fuente: Carro, C. y De Lira, Y. (2012).

- **VPN Interna:** su aplicación se deriva de la VPN con acceso remoto, sin embargo en este caso no se utiliza Internet para establecer conexión con el servidor, se conecta a través de una red LAN (Local Area Network) lo cual permite tener más control sobre la información que se encuentre en el servidor, separando tanto partes de la red como servicios. Generalmente este tipo de VPN no es muy utilizado, sin embargo al contar con la ventaja de ofrecer un servicio que garantiza mayor seguridad es implementado en casos especiales como es el caso de los bancos, departamento de finanzas, recursos humanos, entre otros. (Ver Figura 6)

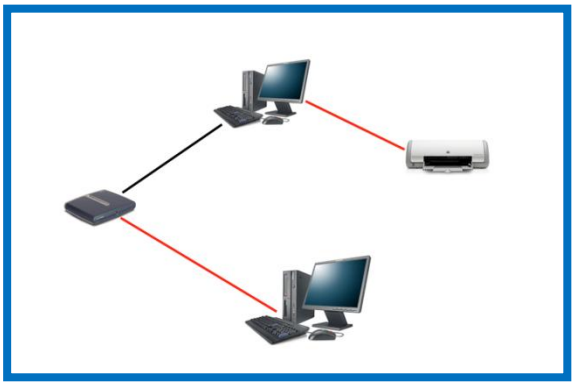

Figura 6. VPN interna.

Fuente: Carro, C. y De Lira, Y. (2012).

II.6.3 Tipos de Conexión VPN

- **Conexiones *Client-to-Site*:** permite establecer conexión entre el cliente y el servidor de forma segura a los recursos del mismo a un costo bastante bajo, dándole la oportunidad a los usuarios de tener acceso remoto a los servidores sin importar la ubicación del mismo, lo cual resulta sumamente importante para aquellos que no poseen una ubicación fija. (Ver Figura 7)

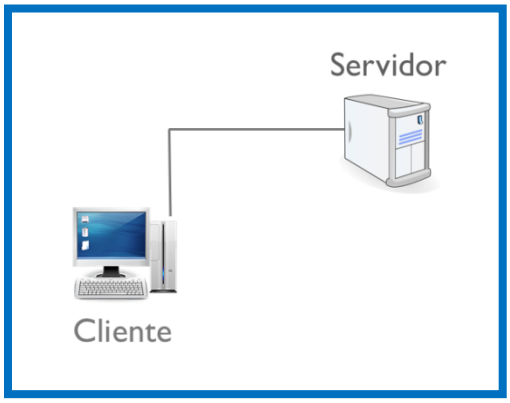

Figura 7. Conexión Client-to-Site.
Fuente: Carro, C. y De Lira, Y. (2012).

- **Conexiones *Site-to-Site*:** Representa la forma más común de establecer una conexión remota segura entre dos ubicaciones geográficamente separadas. Es el tipo de conexión más utilizado por las empresas. Su propósito es establecer conexión entre dos servidores independientemente de la ubicación geográfica de cada uno, ofreciendo las mismas ventajas de una conexión física. (Alejandro, 2010) (Ver Figura 8)

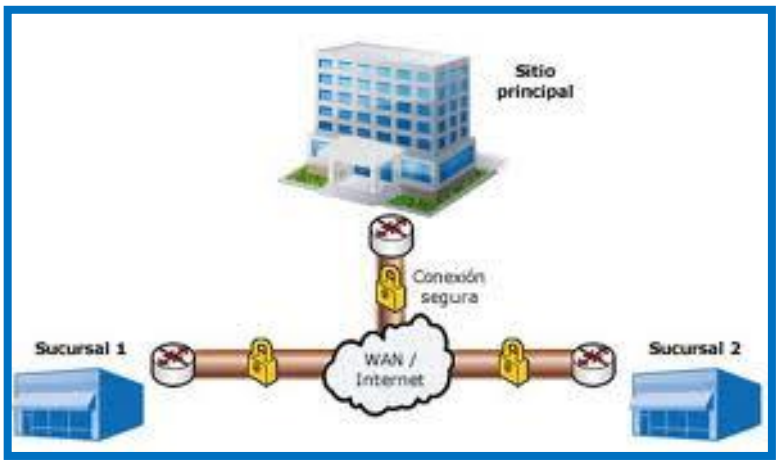

Figura 8. Conexión *Site to Site.*

Fuente: Net Humans. (s.f.).

II.6.4 Ventajas y desventajas de una VPN

Según Fernández (2008) las ventajas y desventajas de una VPN son:

Ventajas:

- Ahorro: permite realizar la conexión de distintas redes independientemente de la distancia que las separe a través de Internet.
- Transparencia: el proceso de conexión es transparente para el usuario.
- Seguridad: garantiza la funcionalidad de varios servicios.
- Movilidad: la conexión entre usuarios móviles y fijos es segura y estable.
- Simplicidad: facilita la conexión de servidores y aplicaciones entre distintos dominios.

Desventajas:

- Fiabilidad: Internet no es del todo fiable, lo que provoca que la conexión tampoco lo sea al ésta depender de dicho servicio.

- Confianza entre las redes: los componentes de la VPN son afectados por inconvenientes causados en la subred donde esté la VPN.

- Interoperabilidad: algunas soluciones para ser aplicadas en la VPN son incompatibles con otras ya implementadas.

Las VPN manejan algoritmos de encriptación, lo cual permite encapsular los datos en un paquete seguro. La encriptación es tan importante como la autenticación, ya que protege los datos transportados a través de la red en los dos extremos de la conexión. Entre los tipos de encriptación se encuentran: la encriptación de clave secreta o privada, y la encriptación de clave pública.

Por otro lado, en la encriptación de clave pública se utilizan dos claves, una pública y una secreta. La primera se envía a los participantes. Cuando se encripta, se utiliza la clave privada propia del usuario y la clave pública del otro participante de la conversación. Al recibir esta información, ésta se desencripta usando su propia clave privada y la pública del generador de la información. La gran desventaja de esta encriptación es que resulta ser más lenta que la clave secreta.

II.7 Protocolos TCP (*Transmition Control Protocol*) y UDP (*User Datagram Protocol*)

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.)

Servicios que ofrece:

- Transferencia de archivos FTP (File Transfer Protocol).
- Acceso remoto.
- Sistemas de archivo en red.
- Servidores de nombres y de terminales.
- Comunicación fiable.
- Reconocimiento positivo con retransmisores.
- Revisa el contenido tanto del encabezado como del cuerpo del segmento para verificar si ha sido o no alterado al ser enviado.
- Detecta y ordena el mensaje en caso de ser necesario.
- Reenvía el mensaje si no recibe confirmación.

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.)

Es simple y sencillo. Cuenta con un encabezado pequeño y no ofrece control de congestión.

Servicios que ofrece:

- Flujos multimedia.
- DNS (Domain Name Server).

Comparación entre TCP y UDP

A continuación se presenta una tabla comparativa entre los protocolos de transporte, pudiendo observar sus principales características:

TCP	UDP
Orientado a la conexión	No orientado a la conexión
Fiable	Poco fiable
Utilizado en servicios Telnet, FTP y SSH	Utilizado en servicios DNS y de streaming
Conexión Full Duplex	Conexión Half Duplex
Recupera y reenvía los paquetes perdidos	No recupera y tampoco reenvía los paquetes perdidos

Tabla 2. Diferencias entre TCP y UDP.

Fuente: Elaboración propia.

II.8 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.

Características:

- Protege de ataques.
- Todas las conexiones son encriptadas.
- La versión OpenSSH utilizada en LINUX no tiene ningún costo.
- Presta servicios a través del puerto 22 en TCP.

II.8.1 Arquitectura de capas del protocolo SSH

- Capa de transporte: maneja el intercambio inicial de las claves y autentificación del servidor. Establece los métodos de cifrado, compresión y verificación de la integridad. Organiza el re-intercambio de claves después de una hora de conexión.

- Capa de autenticación: el proceso de autentificación es dirigido por el cliente. Proporciona un conjunto de métodos de autentificación.

- Capa de conexión: define el concepto de canal, peticiones de canal y peticiones globales para el uso de los servicios que proporciona. Los canales transfieren datos en ambas direcciones.

II.9 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. Por lo tanto, la seguridad no la provee directamente el protocolo SFTP, sino SSH o el protocolo que sea utilizado en su caso para este cometido.

Con SFTP, los datos transferidos entre el cliente y el servidor están cifrados, lo que evita que usuarios no autorizados tengan acceso a ellos. (Lamana, 2012)

II.10 HTML (*HyperText 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)

II.11 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)

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.

Características de SSL

- Confidencialidad: el mensaje es enviado y recibido en forma segura.
- Integridad: no se pierden paquetes al enviar la información.

- Autenticación: las empresas que hagan uso de este protocolo, deben estar autorizadas para ello, a través de la obtención de un Certificado Digital emitido por la empresa de nombre Autoridad Certificadora. (Ximenez, s.f.)

II.12 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.

El objetivo de la creación de una base de datos es resolver las necesidades de información de una comunidad o sociedad.

II.12.1 MySQL

Es un sistema administrativo relacional de bases de datos (RDBMS por sus siglas en inglés Relational Database Management System). 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.

MySQL es un servidor multi-usuarios muy rápido y robusto de ejecución de instrucciones en paralelo, es decir, que múltiples usuarios distribuidos a lo largo de una red local o Internet podrán ejecutar distintas tareas sobre las bases de datos localizadas en un mismo servidor.

Utiliza el lenguaje SQL (Structured Query Language) que es el estándar de

consulta a bases de datos a nivel mundial.

MySQL ha estado disponible desde 1996, pero su desarrollo data desde 1979 y ha ganado en tres años consecutivos el premio Linux Journal Reader's Choice Award. Actualmente disponible en código abierto.

Ventajas de MySQL:

- Implementación multihilo.
- Ofrece soporte para gran cantidad de datos para las columnas.
- API's en gran cantidad de lenguajes (C, C++, Java, PHP).
- Portabilidad entre sistemas.
- Como máximo soporta 32 índices por tabla.
- Buen nivel de seguridad de datos.
- Fácil instalación y configuración.
- No tiene ningún costo siempre y cuando no se utilice para desarrollar un software a comercializar.
- Ofrece soporte técnico.
- Es bastante rápido en comparación con otros SABD. (Valade, 2008)

II.12.2 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.

Ventajas de PHP:

- Es rápido, basado en código HTML.
- No tiene costo.

- Fácil de usar.
- Funciona en muchos sistemas operativos.
- Ofrece soporte técnico.
- Es seguro, el usuario no tiene acceso al código PHP.
- Está diseñado para interactuar con bases de datos. (Valade, 2008)

Capítulo III
Metodología

En esta sección se presentan cada una de las etapas que permitirán el desarrollo exitoso del presente Trabajo Especial de Grado.

III.1 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.

III.2 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 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.

III.3 Fase 3: Diseño e implementación de una red privada virtual que permita establecer la conexión y sincronización entre los servidores de los centros de investigación en Telesalud: Grupo de Física Médica de la Universidad Central de

Venezuela (UCV) y Grupo de Telemedicina de la Universidad Católica Andrés Bello (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.

III.4 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.

III.5 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.

III.6 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.

Capítulo IV
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.

IV.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.

La configuración de los servidores se basó en el sistema operativo LINUX, con versión CENTOS para la UCV y UBUNTU para la UCAB. La configuración de los servidores se realizó de manera satisfactoria, debido a que LINUX trabaja con software de licencia libre, lo cual resultó fructífero.

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

En este espacio se muestra el proceso mediante el cual se establece la conexión de los servidores a través de una VPN, mostrando la relevancia de las fases mencionadas anteriormente.

IV.2.1 Diseño

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.

IV.2.2 Simulación de la conexión cliente-servidor

Para la simulación de 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. La simulación se hizo en dos equipos con sistema operativo LINUX con versión CENTOS, de manera que se pudiera establecer la conexión correctamente, garantizando el establecimiento seguro de la red. Una vez hechas las pruebas se procedió a establecer quién sería el servidor principal y el cliente dentro de los grupos de la UCAB y la UCV.

IV.2.2.1 Configuración del Servidor VPN

En la configuración del servidor se instalaron todos los paquetes necesarios para su óptimo funcionamiento, ajustando parámetros precisos, para un correcto desempeño de la red privada virtual.

A continuación se presentan los comandos empleados para la configuración del servidor:

- Instalación de los paquetes OpenVPN y OpenSSL para la configuración de la red privada virtual:

#yum install openvpn

#yum install openssl

- Directorio en el cual se configuran todos los archivos necesarios para establecer la conexión VPN, se debe cambiar del directorio actual al directorio */etc/openvpn/*

#cd /etc/opemvpn/

- Se configura el archivo */etc/openvpn/vars*, de manera que se puedan cargar las variables en el momento en que se registre el cliente.

#vi /etc/openvpn/vars

- Se ejecuta el archivo */etc/openvpn/vars*, a fin de que cargue las variables de entorno configurado anteriormente.

#source /etc/openvpn/./vars

- Se ejecuta el siguiente archivo a fin de limpiar cualquier firma digital que accidentalmente estuviera presente.

#sh /usr/share/easy-rsa/clean-all

- Se crea la entidad emisora de certificados.

#sh /usr/share/openvpn/easy-rsa/2.0/build-ca

- Se crea la llave Diffie Hellman de 2048 bits.

#sh /usr/share/openvpn/easy-rsa/2.0/build-dh

- Se genera la firma digital en el servidor:

#sh /usr/share/openvpn/easy-rsa/2.0/build-key-server server

- Se crea el certificado para el cliente:

#sh /usr/share/openvpn/easy-rsa/2.0/build-key ucabserver

- Se crea un archivo en el fichero */etc/openvpn/'nombre del fichero en el cual se guardará la configuración*', el cual certificará la conexión a establecer:

#vi /etc/openvpn/server.conf

Dentro de este archivo se configura el servidor. La Figura 9 refleja la configuración de la máquina servidor, indicando los puertos a utilizar, la ubicación de los certificados y llaves del servidor, la dirección de red a emplear para la VPN, entre otros.

Figura 9. Configuración del servidor VPN.

Fuente: Elaboración propia.

- Se transfieren las llaves y certificados creados, al cliente por una vía segura.

IV.2.2.2 Configuración del Cliente VPN

La configuración del cliente es un poco más sencilla en comparación con la configuración del servidor, igualmente se descargaron e instalaron todos los paquetes necesarios para permitir el correcto funcionamiento de la red privada virtual. Al tener la configuración establecida, se inicia la conexión del servidor y posteriormente en el cliente, de manera que la VPN se encuentre activa, y genere la creación de un túnel entre ambos equipos, mediante el cual se encuentran conectados de forma privada y segura. La forma de garantizar un buen desempeño en la red es haciendo un PING a la dirección IP asignada por el túnel VPN a la máquina cliente y viceversa, comprobando el correcto establecimiento de la conexión privada.

Los comandos utilizados para la configuración del cliente se describen a continuación:

- Instalación de los paquetes OpenVPN y OpenSSL para la configuración de la red privada virtual:

#yum install openvpn
#yum install openssl

- Configuración del archivo *client.conf* dentro del directorio */etc/openvpn/*, colocando la información necesaria, como los puertos requeridos y los certificados específicos del servidor.

En la Figura 10 puede observarse el archivo de configuración del cliente (en esta prueba denominado *client.conf*), indicando los puertos a utilizar, la ubicación de los certificados y llaves del cliente (se deben especificar la carpeta donde están alojados), entre otros.

Figura 10. Configuración del cliente VPN.

Fuente: Elaboración propia.

- Se procede a establecer la conexión de red privada virtual, el servidor debe iniciar el servicio, y posteriormente procede a hacerlo el cliente, con esto se logra crear el túnel VPN. Para conseguir esto se debe ejecutar el siguiente comando:

 # openvpn --config /etc/openvpn/server.conf

IV.3 Implementación de la conexión

Luego de realizada la simulación de la conexión VPN, se procedió a realizar la conexión entre el servidor de la UCV y el servidor de la UCAB. La UCAB y la UCV por motivos de seguridad han condicionado ciertas libertades, es por esto que los administradores de las redes respectivas en ambas casas de estudio proporcionaron la instalación del sistema operativo, VPN, activación de los puertos requeridos, entre otras configuraciones necesarias para lograr establecer la conexión de red.

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

A continuación se presentan los comandos utilizados para acceder de forma remota a los servidores:

- Acceder de forma remota a un equipo:

#ssh nombre_de_usuario@ip_destino

- Transferir archivos al equipo destino:

 # scp archivo_a_transferirnombre_de_usuario@ip_destino:/dir_destino/

IV.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 11 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.

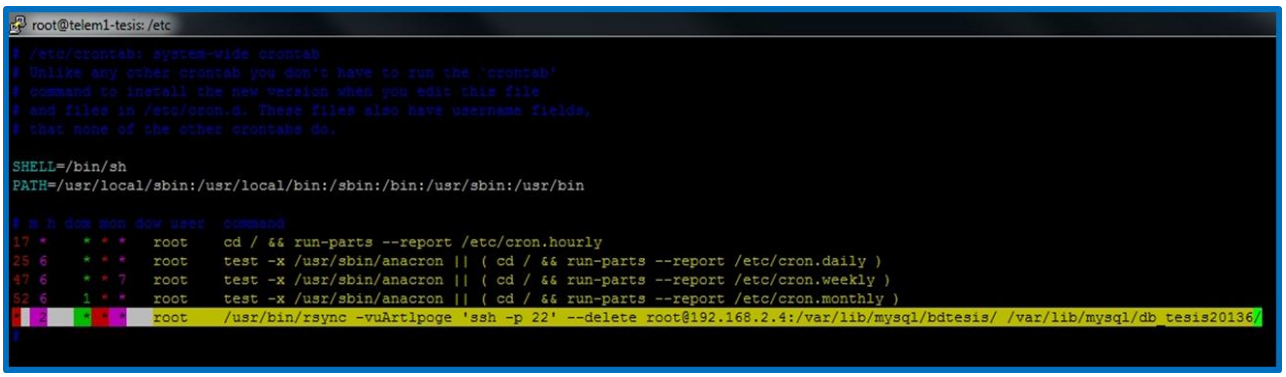

Figura 11. Configuración de la hora de sincronización.

Fuente: Elaboración propia.

IV.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. Para esto se diseñó la estructura de la base de datos que se muestra a continuación:

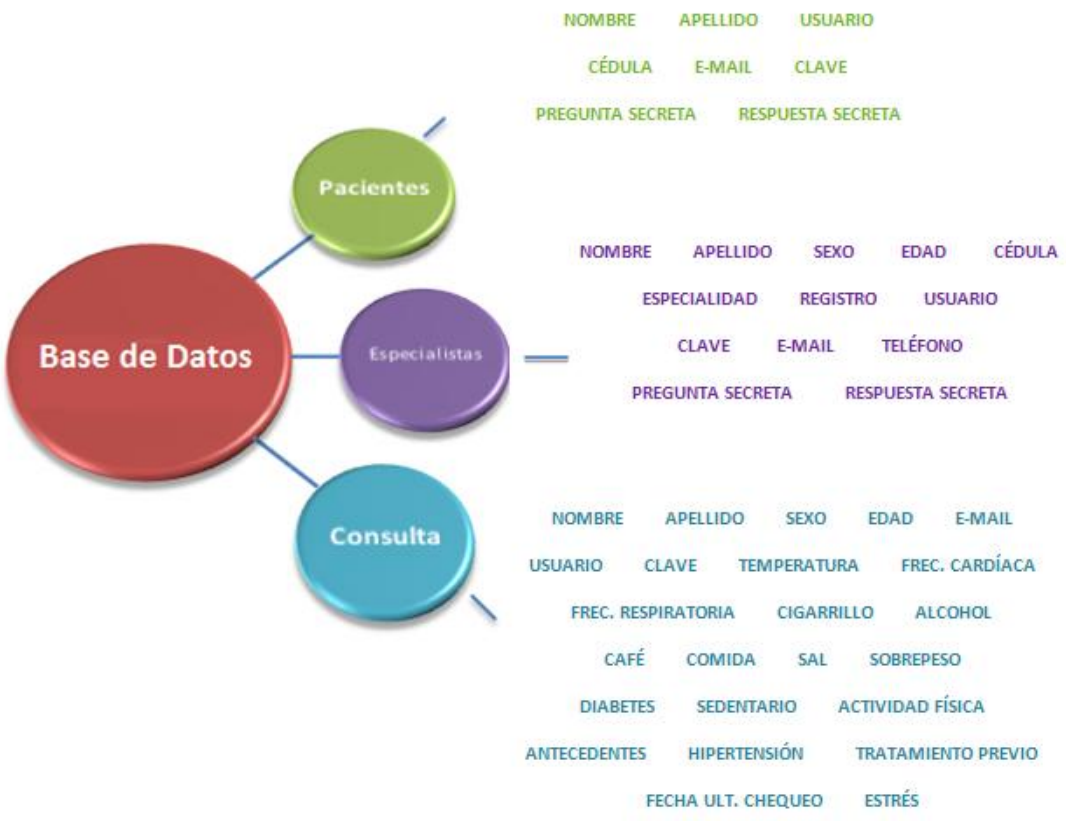

Figura 12. Diagrama de la base de datos.

Fuente: Elaboración propia.

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. A continuación, se muestra en detalle cada procedimiento:

- Se muestra la plataforma *PhpMyAdmin*, con base de datos MySQL, en la cual se debe ingresar usuario y contraseña, debido a que cualquier persona que tenga acceso a esta información, fácilmente puede dañar o formatear el sistema. A continuación se muestra la ventana de inicio de sesión:

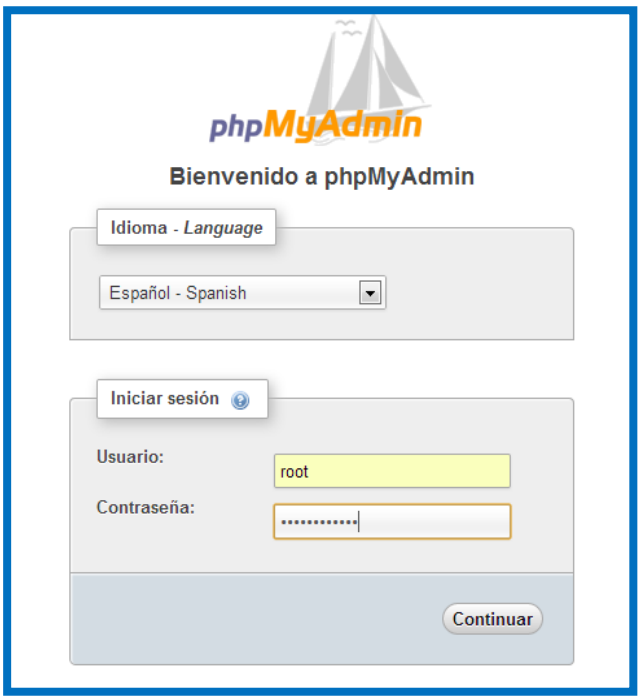

Figura 13. Inicio de sesión en PhpMyAdmin.

Fuente: Elaboración propia.

- Se crea una base de datos:

Figura 14. Creación de base de datos en MySQL.

Fuente: Elaboración propia.

- Se crea una tabla en la base de datos:

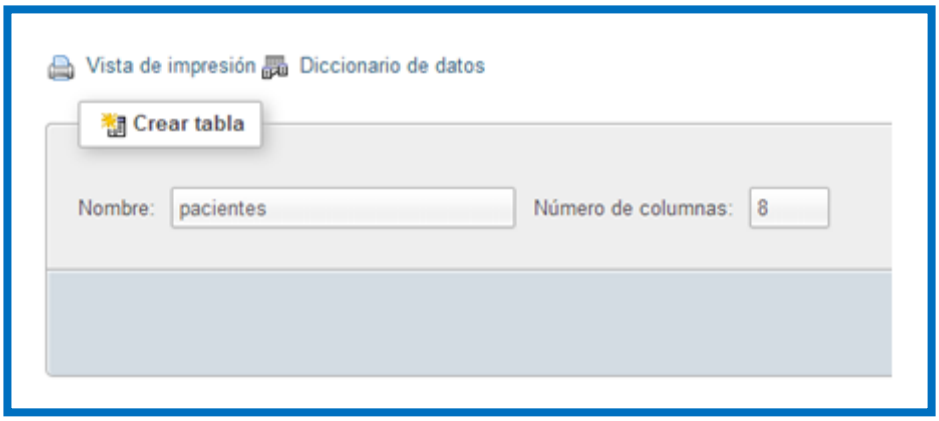

Figura 15. Creación de tablas dentro de la base de datos en MySQL.

Fuente: Elaboración propia.

- Se insertan datos en la tabla creada anteriormente:

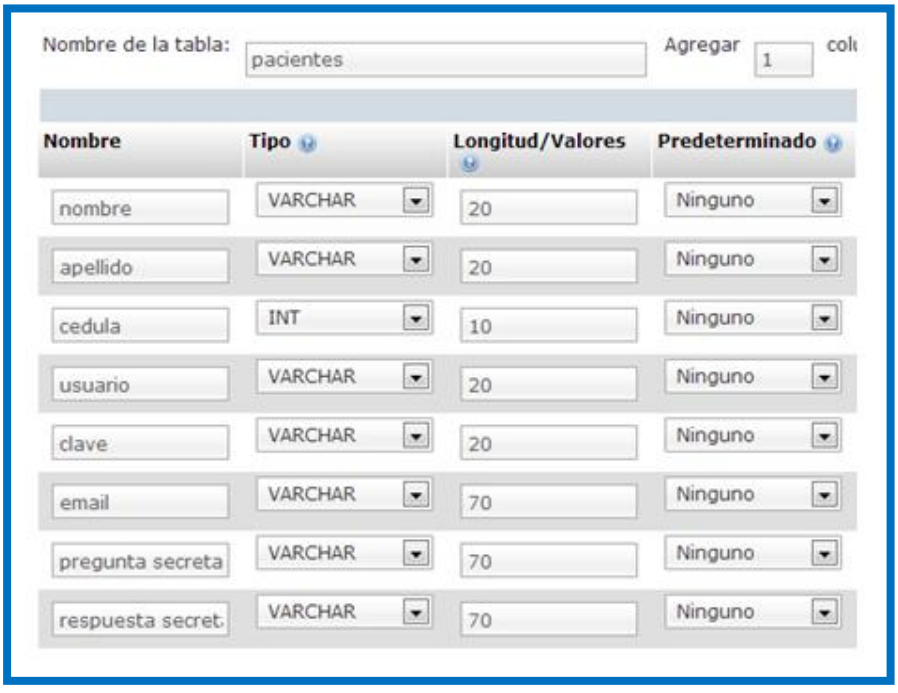

Figura 16. Inserción de datos en la tabla de la base de datos en MySQL.

Fuente: Elaboración propia.

- Se observan las bases de datos existentes:

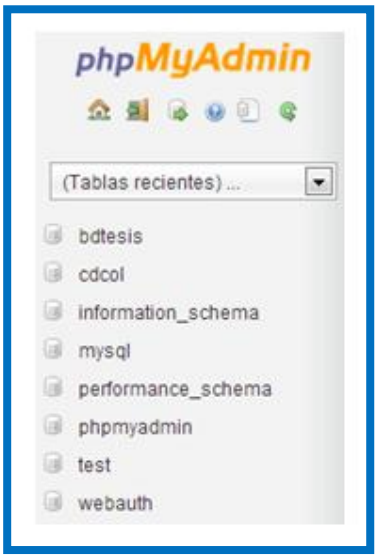

Figura 17. Presentación de las bases de datos existentes.

Fuente: Elaboración propia.

- Se observan las tablas contenidas en la base de datos:

Figura 18. Presentación de las tablas contenidas en la base de datos.

Fuente: Elaboración propia.

- Se observa la información contenida en las tablas de la base de datos en MySQL. A continuación, se da como ejemplo una de las tablas creadas en la base de datos.

Figura 19. Presentación de la información contenida en la tabla “pacientes” de la base de datos.

Fuente: Elaboración propia.

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 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.

En el Apéndice A, se muestra la manera en la cual está conformado el sitio Web que representa la aplicación del proyecto. En primer lugar, se encuentra el archivo index.html, el cual corresponde a la página de inicio, y se encuentra vinculado directamente con los archivos *opcionpaciente.html*, *opcionespecialista.html, proyecto.html* y *contactos.html,* los cuales corresponden a la sección de pacientes, sección de especialistas, descripción del proyecto y contactos respectivamente.

El usuario puede registrarse o ingresar, bien sea paciente o especialista. En caso de que el usuario olvide su contraseña, el sistema le pedirá que ingrese el correo electrónico con el cual se registró, si el correo es correcto se le enviarán los datos de inicio de sesión al correo suministrado. Esta opción de olvido de contraseña se encuentra vinculada en las opciones: *opcionpaciente.html* y *opcionespecialista.html.*

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.

Capítulo V
Resultados

Una vez hecho el desarrollo del trabajo de grado se proceden a mostrar los resultados obtenidos.

V.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 (máx.)
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 3. Características del dispositivo Nro. 1.

Fuente: Elaboración propia.

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 4. 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 5. Características del dispositivo Nro. 3.

Fuente: Elaboración propia.

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 6. 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 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.

V.2 Acceso a los servidores

Para poder acceder al servidor de la UCAB se utilizaron dos programas: VPN Client y Filezilla. En la Figura 20 se puede observar la interfaz del software de VPN Client al correr el programa, antes de aplicar alguna configuración.

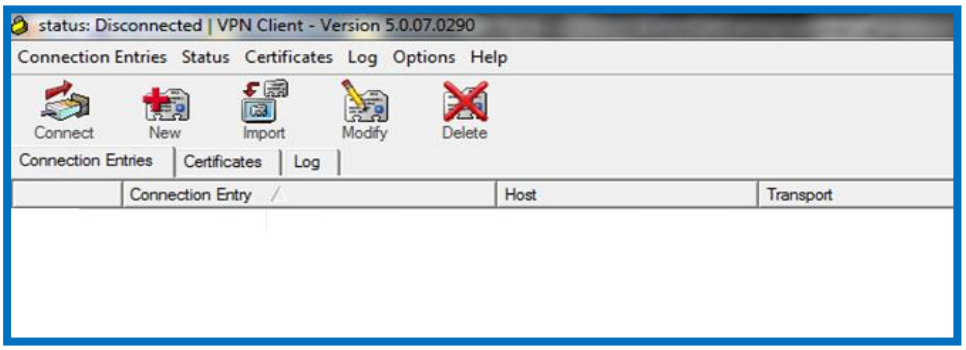

Figura 20. Interfaz de VPN Client.

Fuente: Elaboración propia.

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. La configuración se puede observar en la Figura 21:

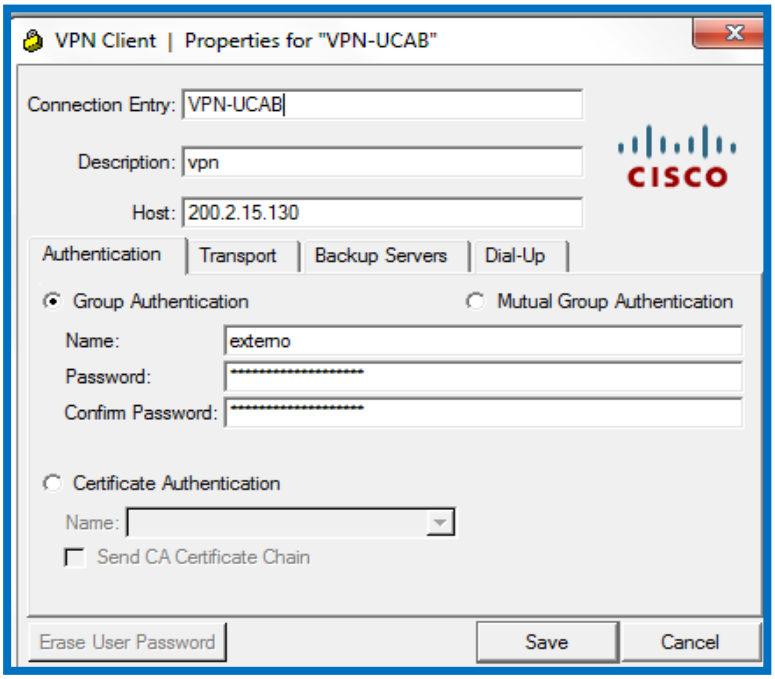

Figura 21. Configuración del VPN Client.

Fuente: Elaboración propia.

Una vez configurado el punto externo que da acceso para la red interna de la UCAB se procedió a la conexión, para la cual se debe acceder con un usuario específico, en nuestro caso “tesis20136”, con la clave correspondiente.

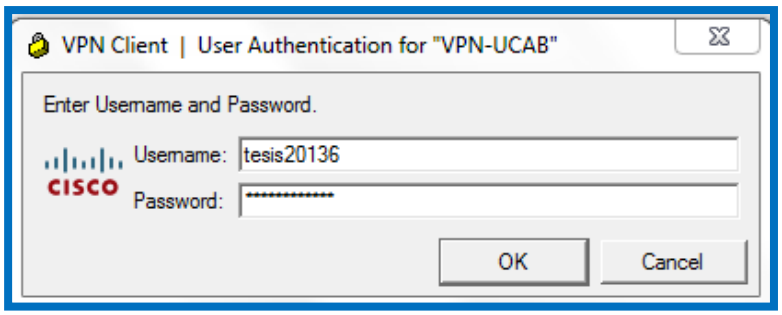

Figura 22. Ventana de configuración de usuario interno.

Fuente: Elaboración propia.

Y finalmente se muestra un mensaje de que la conexión se realizó de manera exitosa.

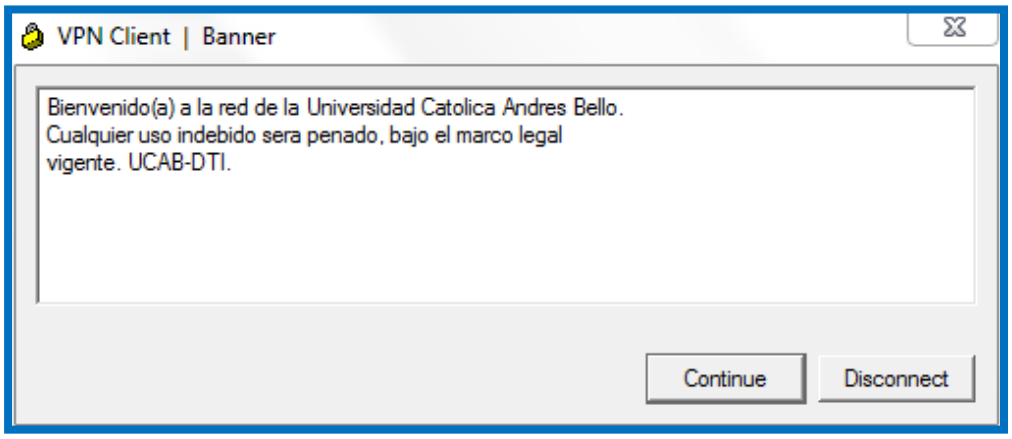

Figura 23. Mensaje de bienvenida al conectar con el servidor remoto.

Fuente: Elaboración propia.

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 24:

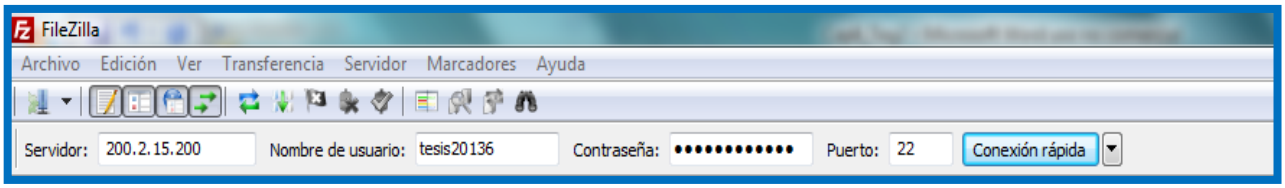

Figura 24. Ventana de conexión al servidor UCAB.

Fuente: Elaboración propia.

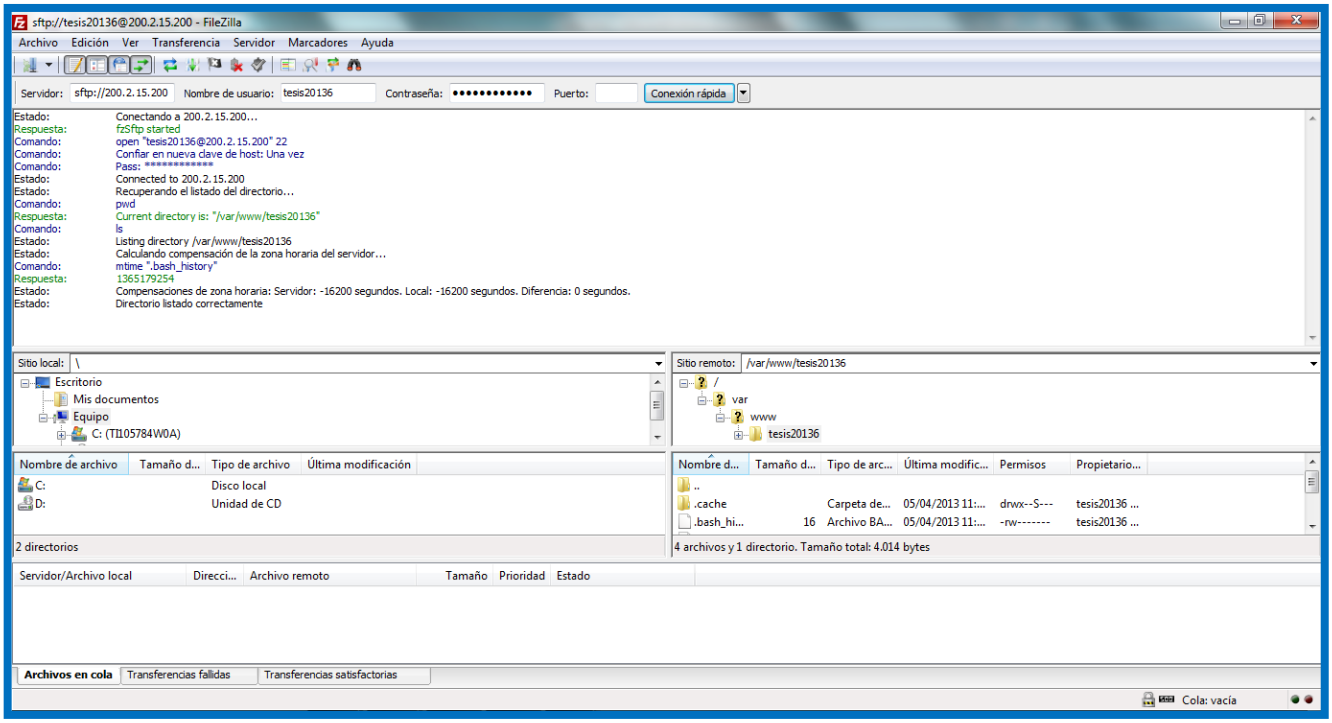

Figura 25. Ventana de conexión Filezilla (UCAB).

Fuente: Elaboración propia.

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.

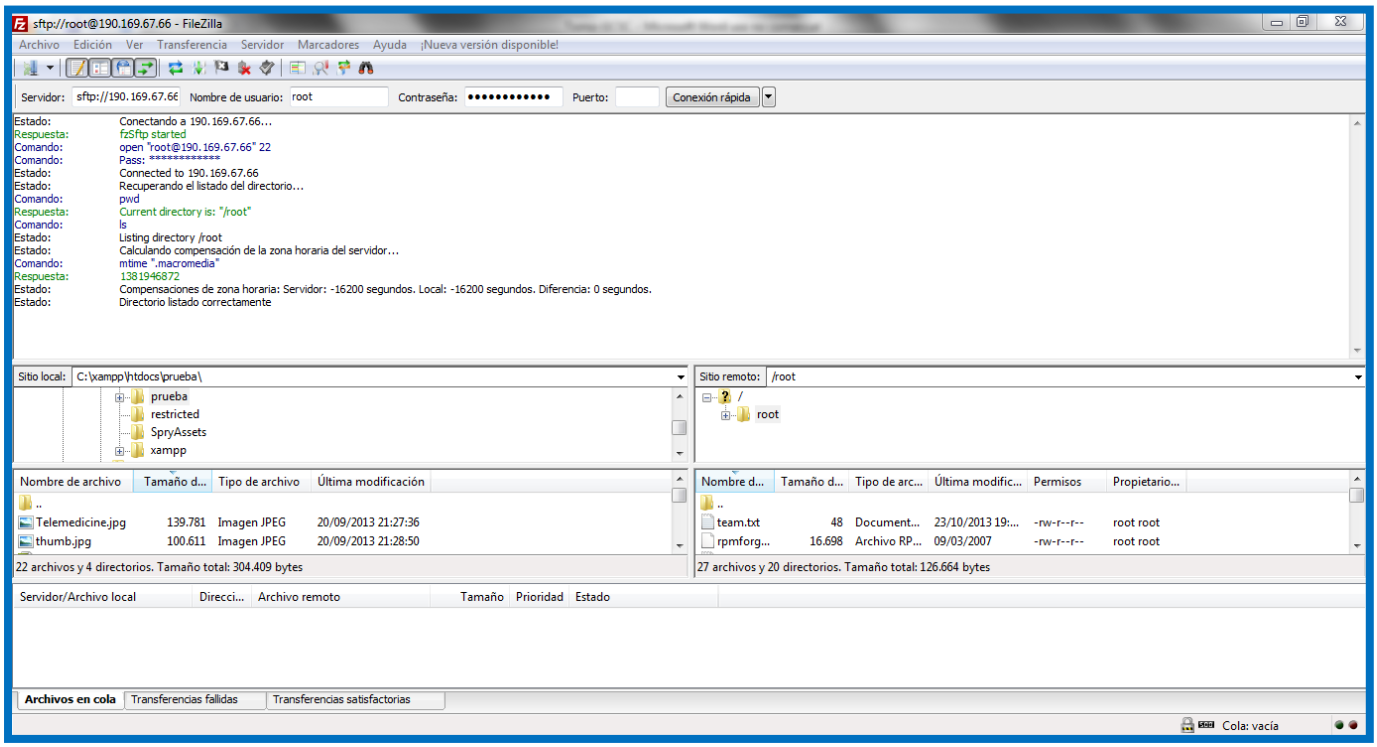

Figura 26. Ventana de conexión Filezilla (UCV).

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.

V.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 27). 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.

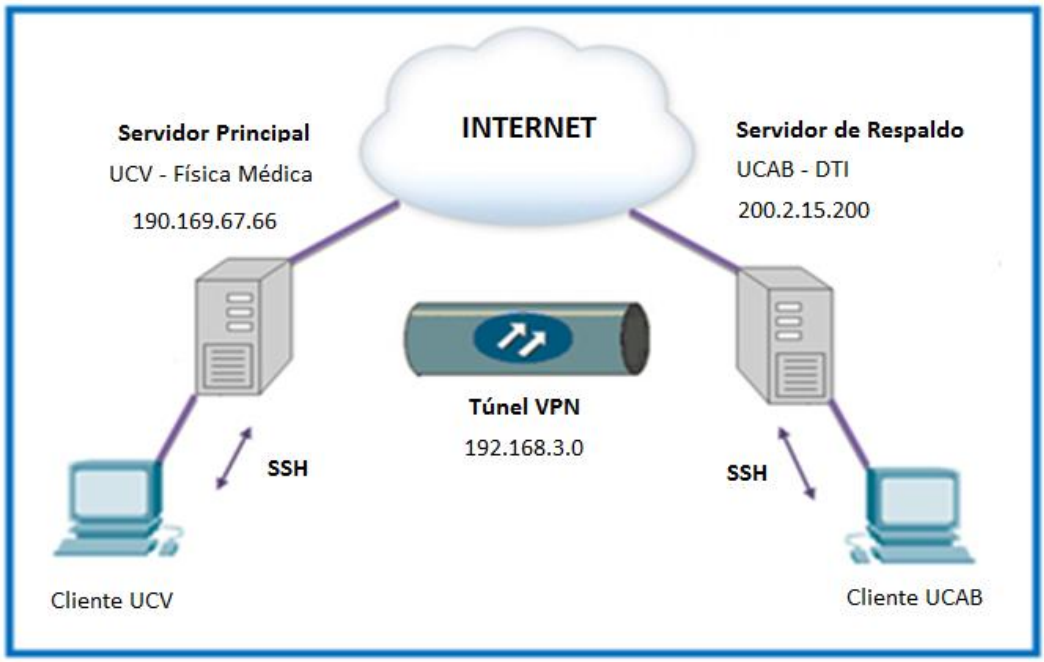

Figura 27. Diseño de la red.

Fuente: Elaboración propia.

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

V.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 28 y 29 que aparecen a continuación:

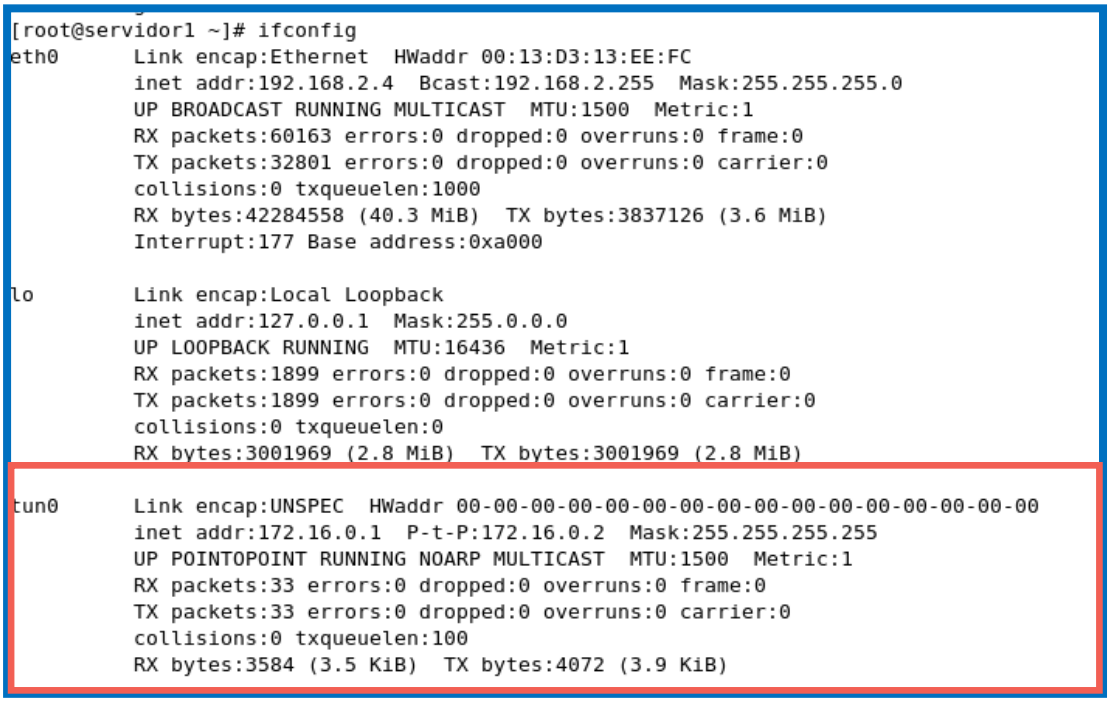

Figura 28. Establecimiento del túnel desde el servidor VPN.

Fuente: Elaboración propia.

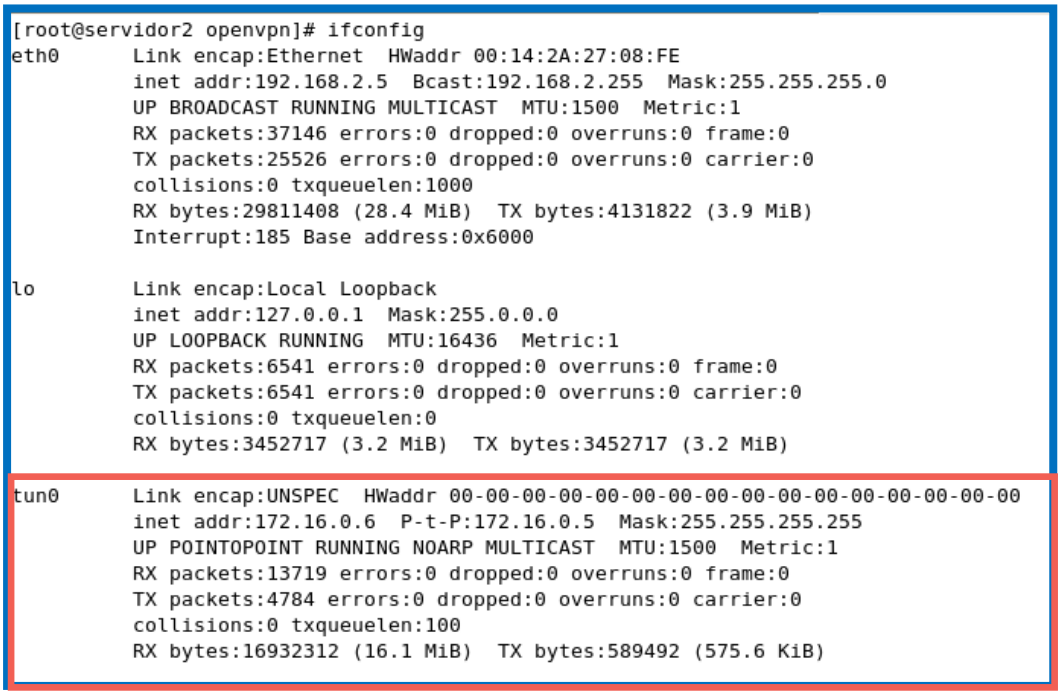

Figura 29. Establecimiento del túnel desde el cliente VPN.

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 30 y 31:

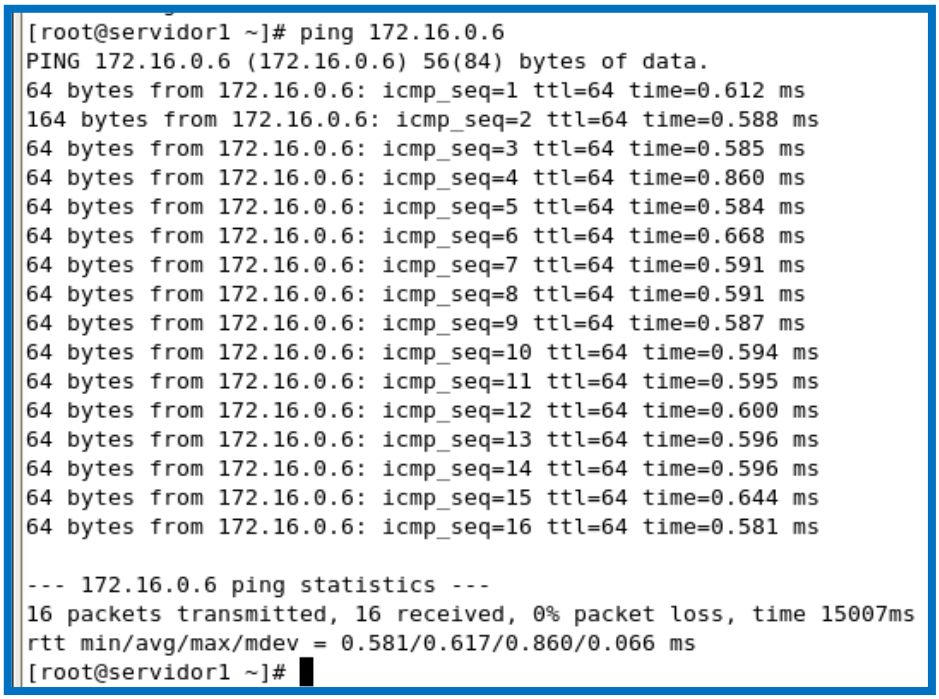

Figura 30. Envío de PING desde el Servidor hacia el cliente.

Fuente: Elaboración propia.

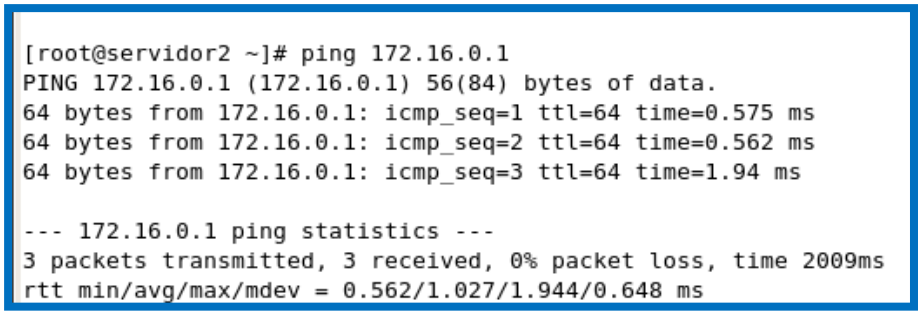

Figura 31. Envío de PING desde el Cliente hacia el Servidor.

Fuente: Elaboración propia.

V.5 Establecimiento de la Conexión

La conexión entre los servidores de 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:

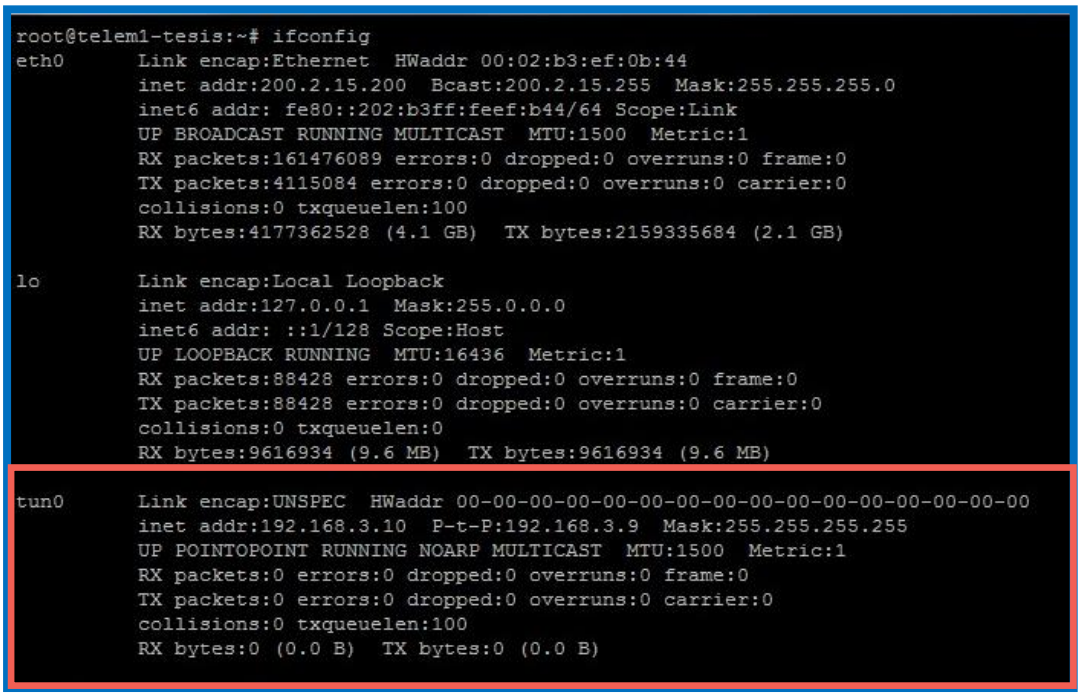

Figura 32. Túnel VPN de conexión UCV - UCAB.

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 la Figura 33:

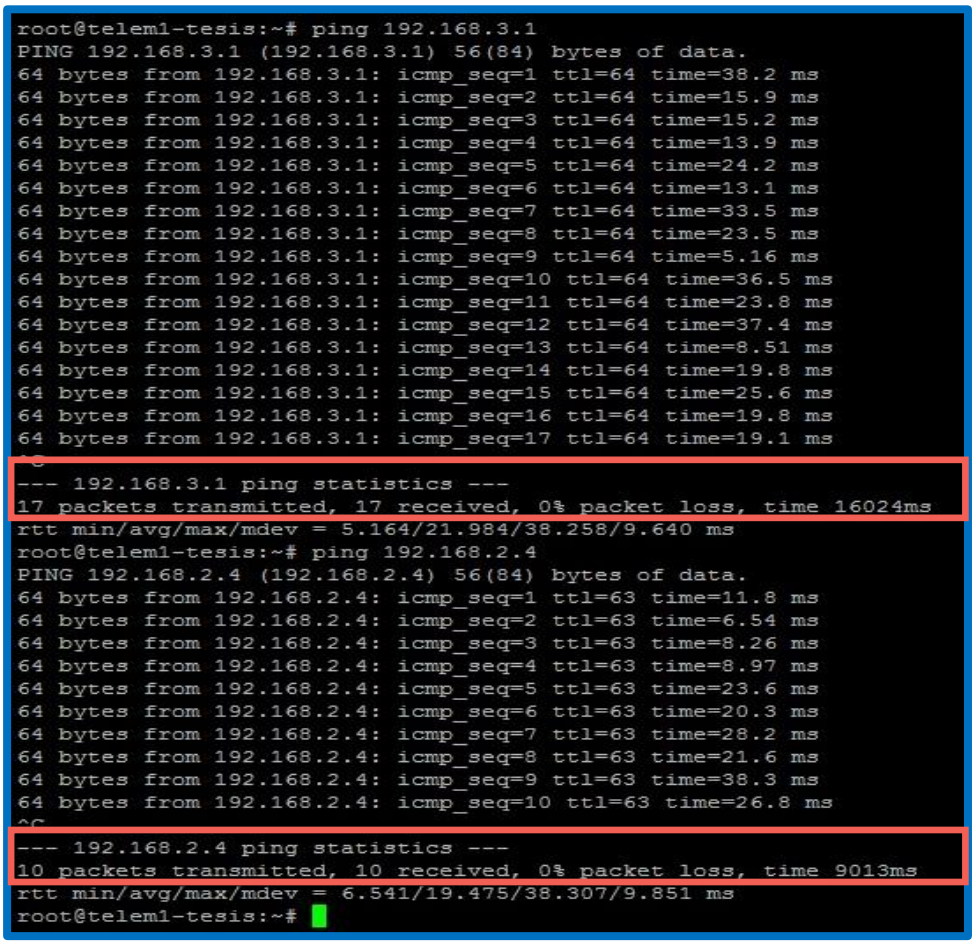

Figura 33. Envío de PING entre los servidores conectados por VPN.

Fuente: Elaboración propia.

V.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.

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.

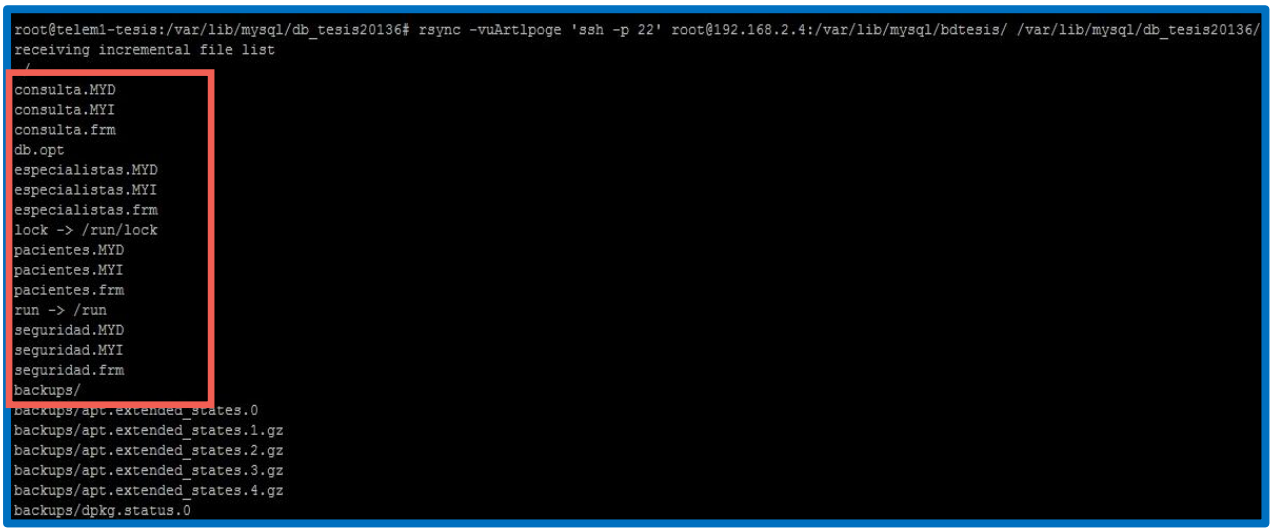

Figura 34. Sincronización de la base de datos hacia el servidor de respaldo.

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 35:

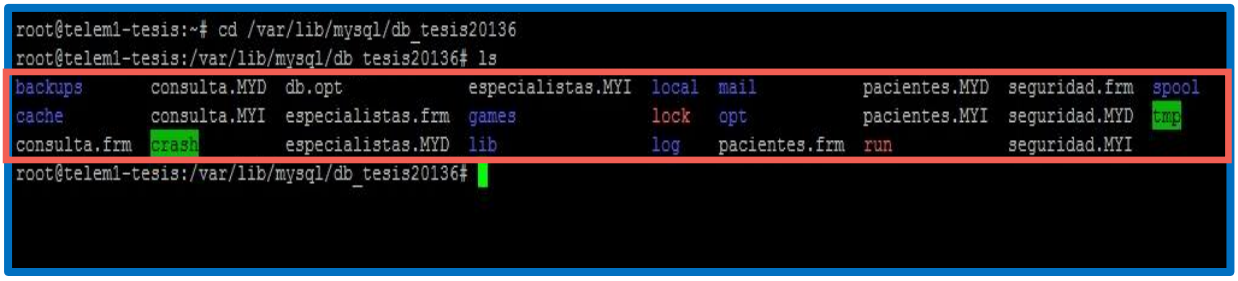

Figura 35. Base de datos alojada en el servidor de respaldo (UCAB).

Fuente: Elaboración propia.

V.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 36)

Figura 36. Ingreso a la Página web.

Fuente: Elaboración propia.

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

Figura 37. Página de Inicio.

Fuente: Elaboración propia.

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

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 aparecerá la pantalla que se muestra en la Figura 38, la cual tendrá tres opciones:

Figura 38. Opciones en el caso de que el usuario sea paciente.

Fuente: Elaboración propia.

Opción 1. Acceso: si el paciente ya posee una cuenta podrá acceder con su nombre de usuario y su contraseña. La página de acceso se puede apreciar en la Figura 39:

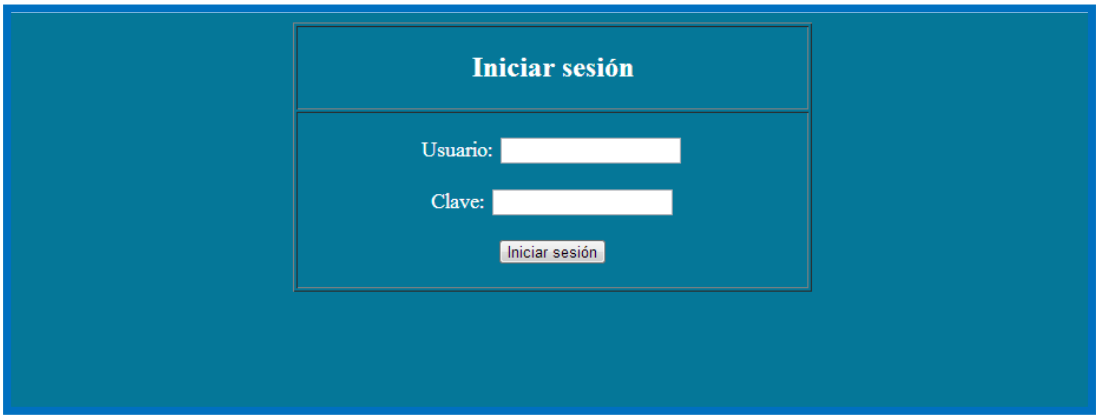

Figura 39. Página de acceso.

Fuente: Elaboración propia.

Si el usuario coloca sus datos de forma correcta, le aparecerá la imagen que se puede observar en las Figuras 40, 41 y 42, donde 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.

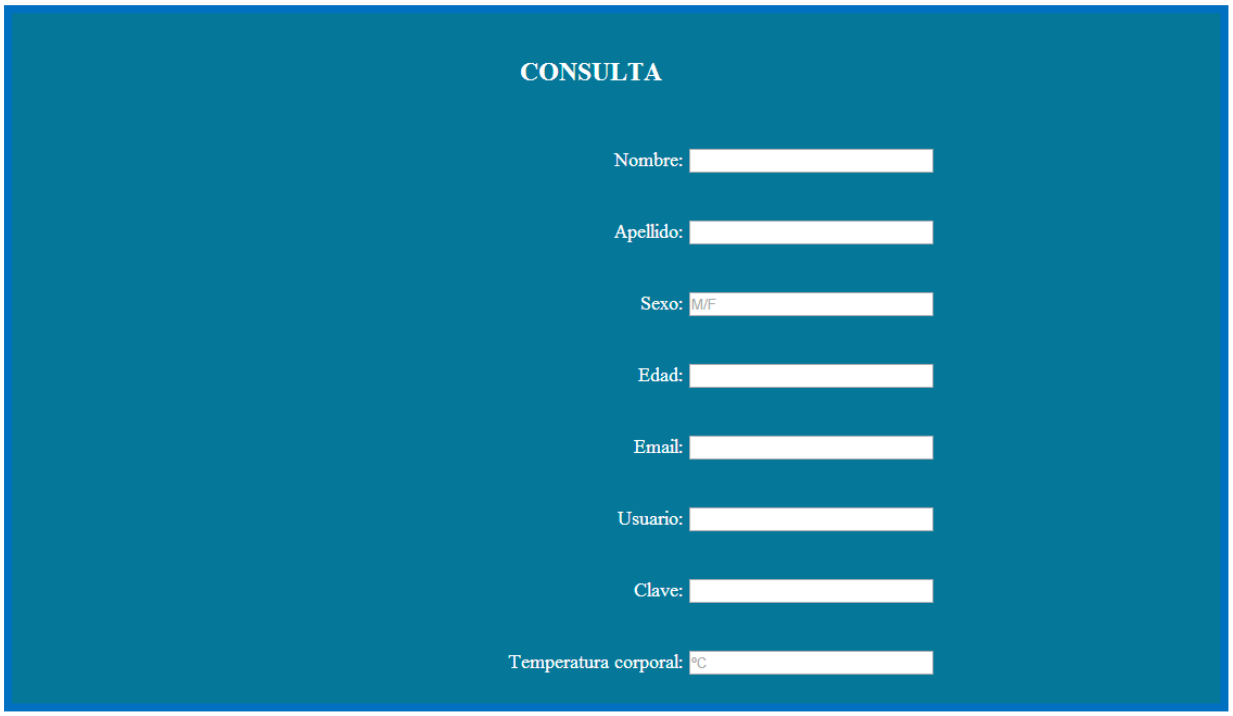

Figura 40. Consulta parte 1.

Fuente: Elaboración propia.

Figura 41. Consulta parte 2.

Fuente: Elaboración propia.

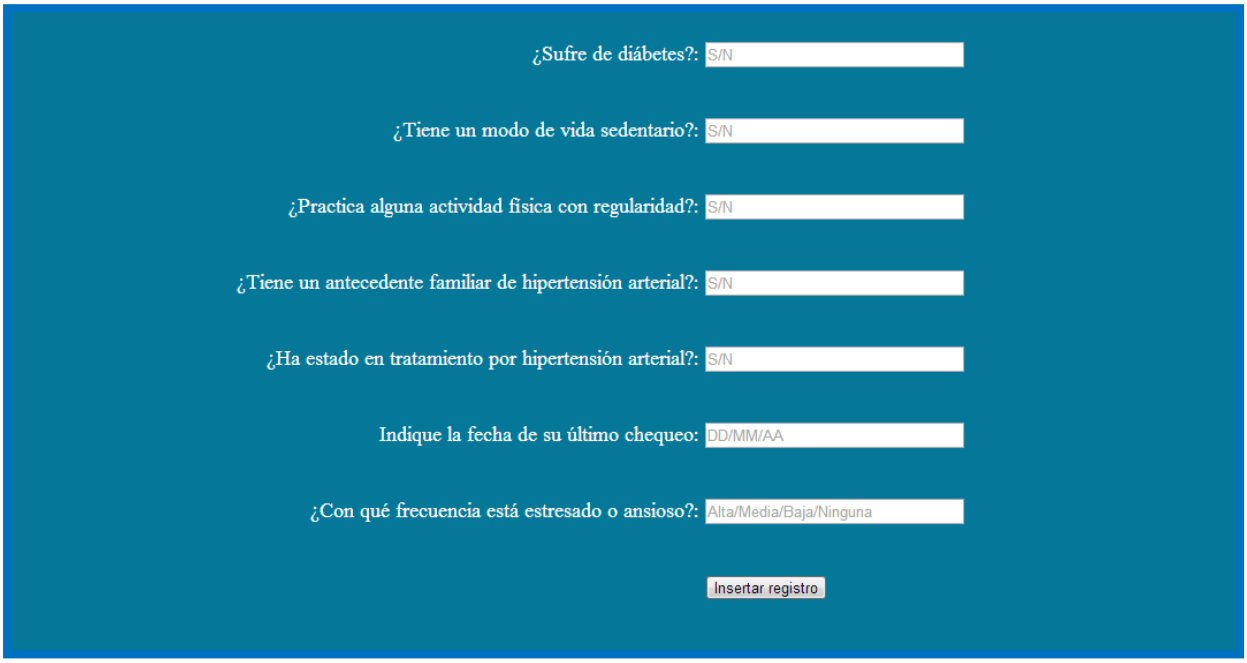

Figura 42. Consulta parte 3.

Fuente: Elaboración propia.

Nótese que el usuario 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.

Una vez que el paciente responda cada una de las preguntas, aparecerá la imagen de la Figura 43, indicándole al usuario que sus datos se han enviado correctamente. En la parte izquierda aparecerá un vínculo que dice: “Desconectar” por si el usuario desea cerrar sesión. En caso de que el usuario cierre sesión, le aparecerá nuevamente la página principal.

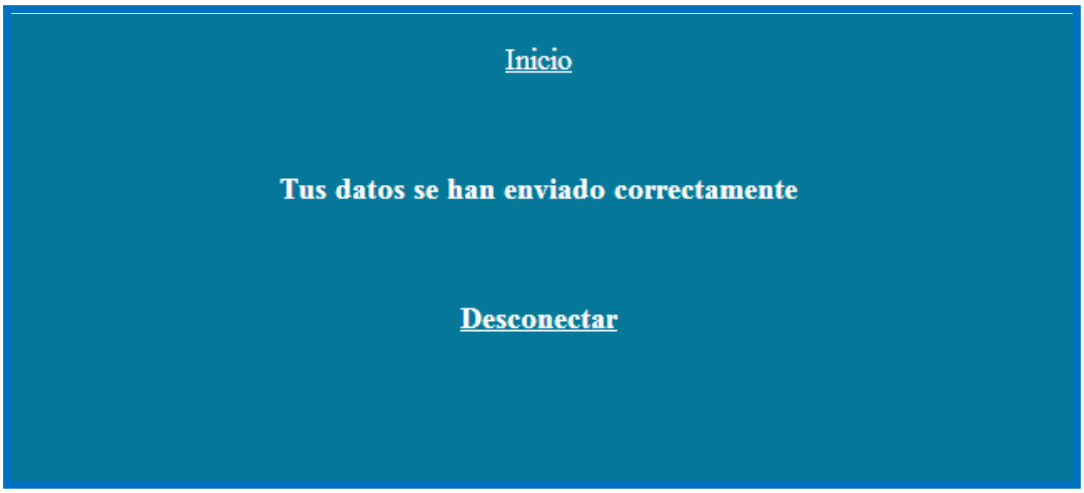

Figura 43. Datos enviados correctamente.

Fuente: Elaboración propia.

***Opción 2. Registro de usuarios*:** en este caso, los pacientes que no posean una cuenta podrán hacerlo registrando sus datos en la aplicación web. Al darle clic en esta opción aparecerá la imagen de la Figura 44.

Figura 44. Registro de pacientes.

Fuente: Elaboración propia.

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 si podrá acceder colocando el nombre de usuario y la clave que indicó al momento de registrarse. (Ver Figura 45)

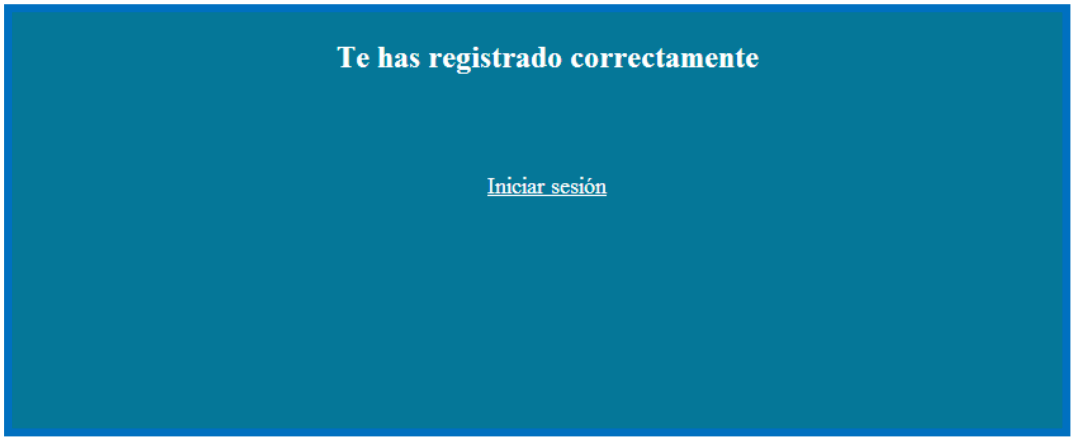

Figura 45. Pantalla que indica que se ha registrado correctamente.
Fuente: Elaboración propia.

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

Aparecerá la imagen de la Figura 46, en la que se le solicita su correo electrónico para enviarle por esa vía su nombre de usuario y su contraseña.

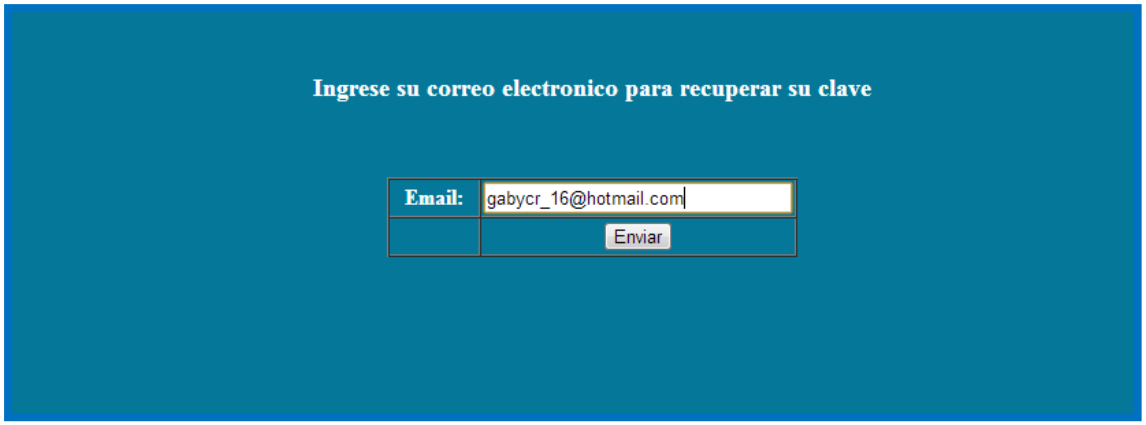

Figura 46. Recuperación de clave.

Fuente: Elaboración propia.

Luego de ingresado el correo electrónico, se verifica el envío correcto del email con los datos solicitados, el cual se muestra en la Figura 47.

Figura 47. Verificación de correo electrónico.

Fuente: Elaboración propia.

- **Especialistas**

En caso de que el usuario sea especialista debe elegir esta opción, y le aparecerá la pantalla de la Figura 48, en la cual tendrá tres opciones.

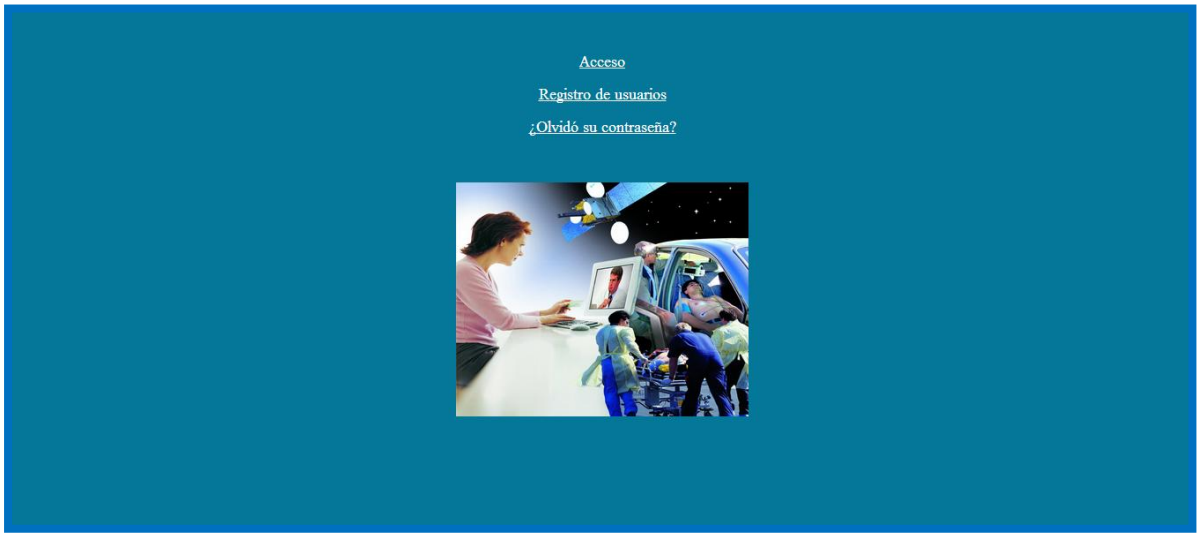

Figura 48. Opciones en el caso de que el usuario sea un especialista.

Fuente: Elaboración propia.

Opción 1. Acceso: si el especialista ya posee una cuenta podrá acceder con su nombre de usuario y su contraseña. La página de acceso se puede apreciar en la imagen que aparece en la Figura 49:

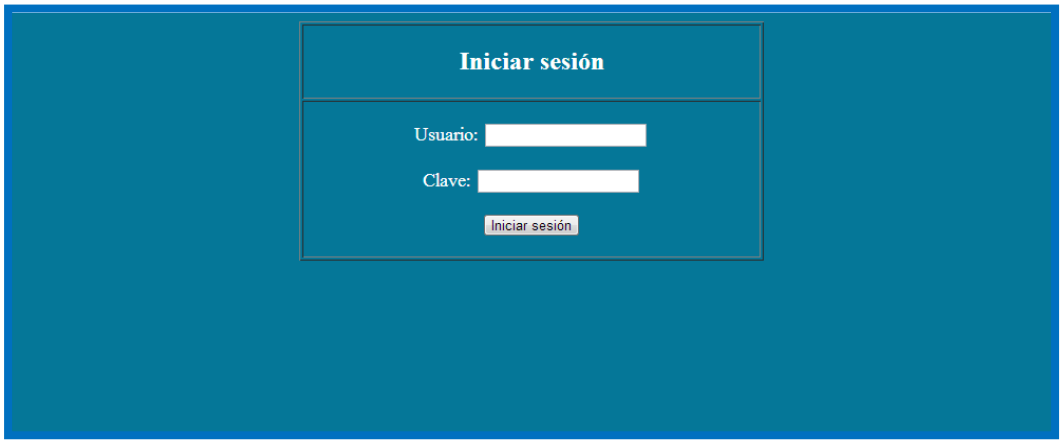

Figura 49. Página de acceso.

Fuente: Elaboración propia.

Si el especialista coloca sus datos de forma correcta, le aparecerá la imagen que se puede observar en la Figura 50, en donde 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. Además, al final de la página, en la parte central, hay un vínculo que dice: "Desconectar", en cual el especialista deberá dar clic si desea cerrar su sesión. En caso de que el usuario cierre sesión, le aparecerá nuevamente la página principal.

Figura 50. Información de pacientes.

Fuente: Elaboración propia.

Opción 2. Registro de usuarios: en este caso, los especialistas que no posean una cuenta podrán hacerlo registrando sus datos en la aplicación web. Al darle clic en esta opción aparecerá la imagen de la Figura 51:

Figura 51. Registro de especialistas.

Fuente: Elaboración propia.

Una vez que el especialista llene todos los campos requeridos para registrarse, se mostrará una pantalla que indica 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. (Ver Figura 52)

Figura 52. Pantalla que indica que se ha registrado correctamente.

Fuente: Elaboración propia.

Opción 3. ¿Olvidó su contraseña?: si el usuario ya se registró pero no recuerda su clave, deberá seleccionar esta opción. A continuación aparecerá la imagen de la Figura 53, en la que se le solicita su correo electrónico para enviarle por esa vía su nombre de usuario y su contraseña:

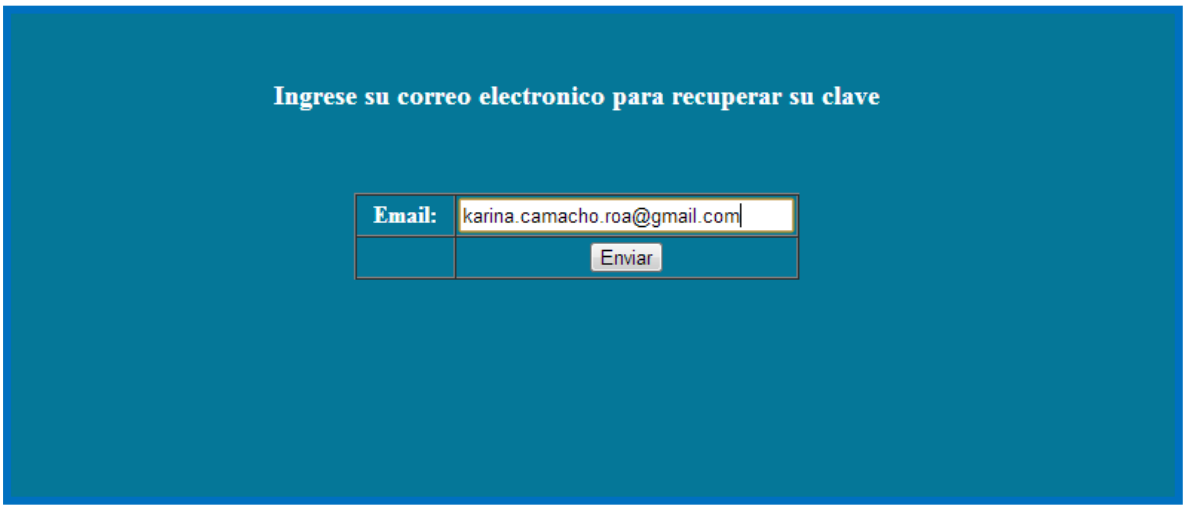

Figura 53. Recuperación de clave.

Fuente: Elaboración propia.

Luego de ingresado el correo electrónico, se verifica el envío correcto del email con los datos solicitados, el cual se muestra en la Figura 54:

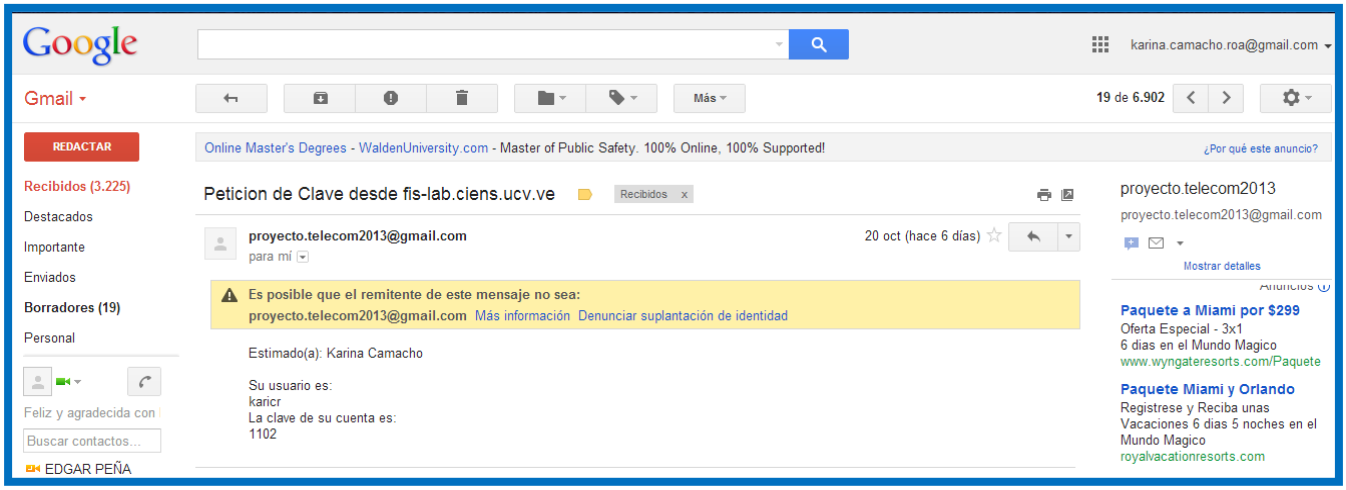

Figura 54. Verificación de correo electrónico.

Fuente: Elaboración propia.

- **Proyecto**

Contiene una breve explicación acerca del objetivo general del proyecto.

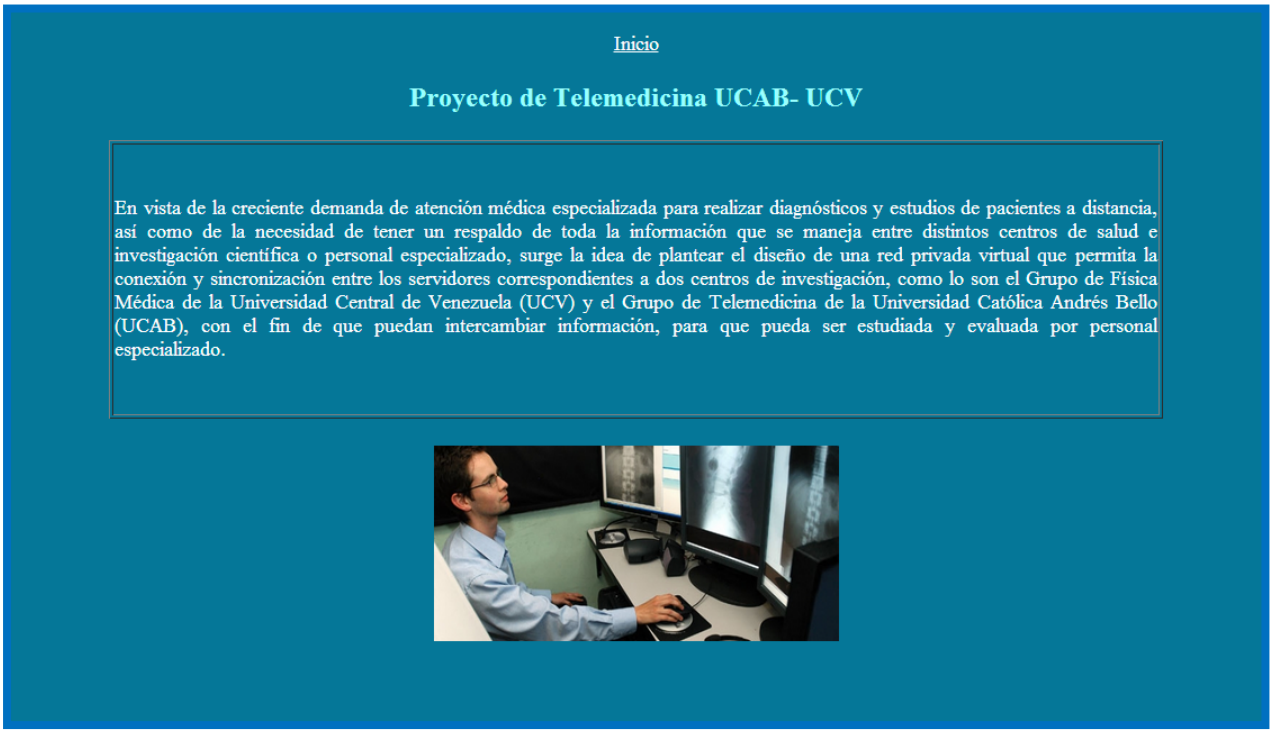

Figura 55. Objetivo del proyecto.
Fuente: Elaboración propia.

- **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.

Figura 56. Página de contactos.

Fuente: Elaboración propia.

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.

Capítulo VI
Conclusiones y Recomendaciones

Una vez realizadas las pruebas y simulaciones correspondientes, se procede a mostrar las conclusiones y recomendaciones pertinentes.

VI.1 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 en 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.

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.

VI.2 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.

- 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.

Bibliografía

Alejandro. (2010). *Qué es una VPN y Tipos de VPN*. Consultado el día 16 de Octubre de 2012 de la World Wide Web: http://enredajo.blogspot.com/2009/03/que-es-una-vpn-y-tiposde-vpn.html.

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.

Carro, C. y De Lira, Y. (2012). *Diseño de una red privada de Teleradiología para el intercambio de imágenes Dicom entre UCV- Física médica y UCAB Telemedicina.* Trabajo Especial de Grado, Universidad Católica Andrés Bello.

Díaz, K. y Mazzochi, S. (2009). *Diseño de una Red para las Unidades de Radioterapia Oncológica del Grupo GURVE.* Trabajo especial de grado, Universidad Católica Andrés Bello.

Dugdale, D. C. (20 de Febrero de 2011). *University of Maryland Medical Center.* Recuperado el 15 de Julio de 2012, de: http://www.umm.edu/ency/article/002341.htm

Fernández, T. (2008). *Ventajas de una VPN*. Consultado el día 28 de Septiembre de 2012 de la World Wide Web: http://www.ac.usc.es/docencia/ASRII/Tema_4html/node19.html

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/

Hernández, J. A. (s.f.). *Mundo Atletismo.* Recuperado el 10 de Abril de 2012, de http://www.mundoatletismo.com/Site/atletismopopular/01d67c944b0dec402.html

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/

León, Rommel. (2012). *Openvpn como solución de Redes privadas virtuales.* Consultado el día 20 de Julio de 2013 de la World Wide Web: http://www.slideshare.net/phylevn/openvpn-como-solucin-de-redes-privadas-virtuales-corporativas

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

Net Humans. (s.f.). *Redes privadas virtuales.* Consultado el día 10 de Mayo de 2013 de la World Wide Web: http://www.nethumans.com/solutions/itSecurity/VPN.aspx

Nordqvist, C. (08 de Octubre de 2011). *Medical News Today.* Recuperado el 16 de Agosto de 2013, de: http://www.medicalnewstoday.com/articles/235710.php

Quintana, Vanessa. (2013). *Desarrollo de una aplicación móvil para transmisión y recepción de parámetros fisiológicos básicos detectados con un módulo portátil.* Trabajo Especial de Grado, Universidad Católica Andrés Bello.

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

Sánchez, Luis. (2013). *Redes privadas virtuales.* Recuperado el día 17 de Agosto de 2013, de: http://luisalfonsosad.files.wordpress.com/2013/03/redes-privadas-virtuales-vpn.pdf

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.

Vorvick, L. (17 de Febrero de 2011). *University of Maryland Medical Center*. Recuperado el 08 de Agosto de 2013, de:
http://www.umm.edu/esp_ency/article/001982.htm

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.*

ANEXOS

ANEXO A

Tabla de Comandos utilizados en CENTOS

Comandos empleados en CENTOS

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

Tabla 7. Tabla de Comandos empleados en CENTOS.

Fuente: Elaboración propia.

APÉNDICES

APÉNDICE A

Esquema de la Página Web

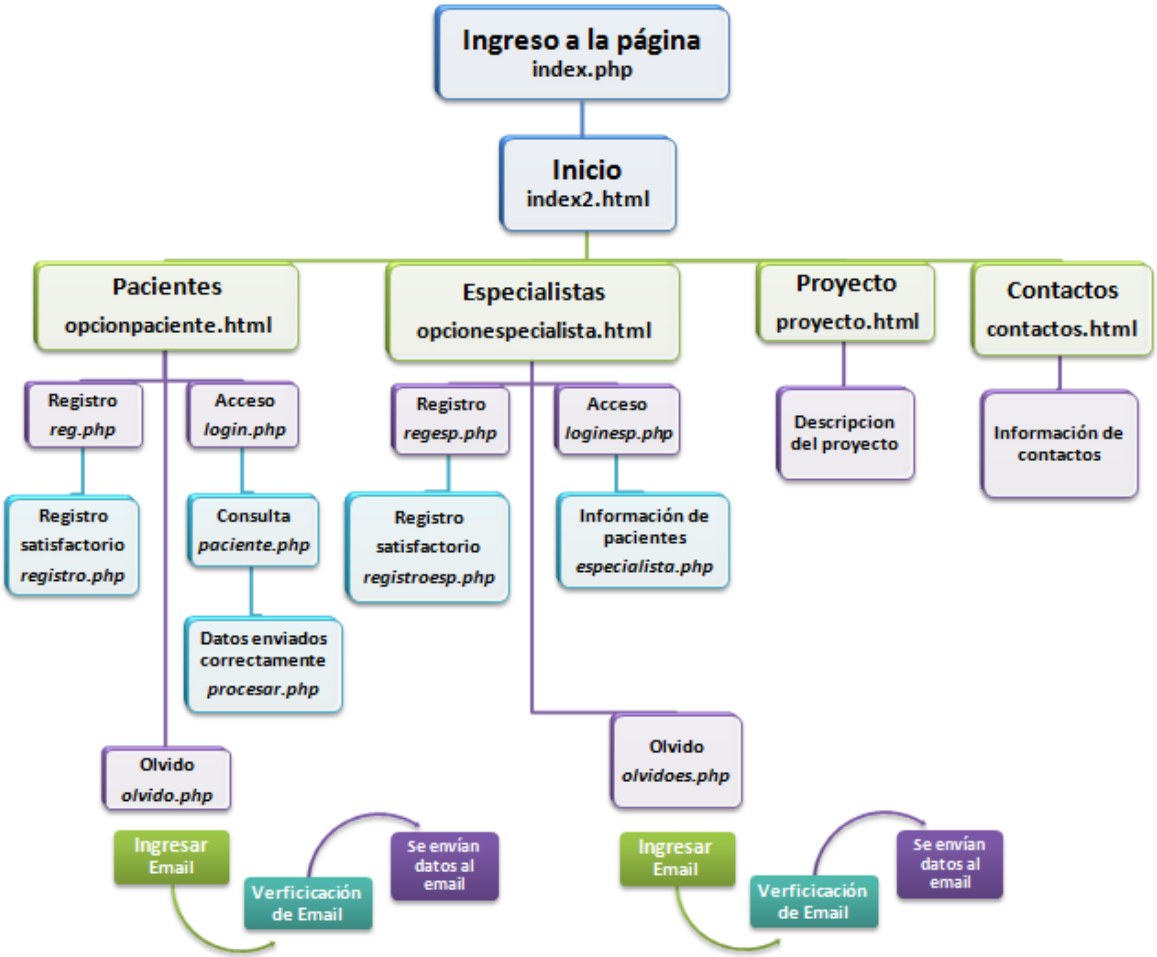

Figura 57. Esquema de la Página Web.

Fuente: Elaboración propia.

APÉNDICE B

Código fuente de la página que muestra información acerca de los pacientes existentes en la base de datos

```
<?php
//initialize the session
if (!isset($_SESSION)) {
  session_start();
}

// ** Logout the current user. **
$logoutAction = $_SERVER['PHP_SELF']."?doLogout=true";
if ((isset($_SERVER['QUERY_STRING'])) && ($_SERVER['QUERY_STRING']
!= "")){
  $logoutAction .="&". htmlentities($_SERVER['QUERY_STRING']);
}

if ((isset($_GET['doLogout'])) &&($_GET['doLogout']=="true")){
  //to fully log out a visitor we need to clear the session varialbles
  $_SESSION['MM_Username'] = NULL;
  $_SESSION['MM_UserGroup'] = NULL;
  $_SESSION['PrevUrl'] = NULL;
  unset($_SESSION['MM_Username']);
  unset($_SESSION['MM_UserGroup']);
  unset($_SESSION['PrevUrl']);

  $logoutGoTo = "index.php";
  if ($logoutGoTo) {
    header("Location: $logoutGoTo");
    exit;
  }
}
```

```
?>
<?php require_once('conex.php'); ?>
<?php
if (!function_exists("GetSQLValueString")) {
function GetSQLValueString($theValue, $theType, $theDefinedValue = "",
$theNotDefinedValue = "")
{
  $theValue = get_magic_quotes_gpc() ? stripslashes($theValue) : $theValue;

  $theValue = function_exists("mysql_real_escape_string") ?
mysql_real_escape_string($theValue) : mysql_escape_string($theValue);

  switch ($theType) {
    case "text":
      $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
      break;
    case "long":
    case "int":
      $theValue = ($theValue != "") ? intval($theValue) : "NULL";
      break;
    case "double":
      $theValue = ($theValue != "") ? "'" . doubleval($theValue) . "'" : "NULL";
      break;
    case "date":
      $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
      break;
    case "defined":
      $theValue = ($theValue != "") ? $theDefinedValue : $theNotDefinedValue;
      break;
  }
  return $theValue;
```

```
}
}

$currentPage = $_SERVER["PHP_SELF"];

$maxRows_cons = 10;
$pageNum_cons = 0;
if (isset($_GET['pageNum_cons'])) {
  $pageNum_cons = $_GET['pageNum_cons'];
}
$startRow_cons = $pageNum_cons * $maxRows_cons;

mysql_select_db($database_conexion, $conexion);
$query_cons = "SELECT * FROM consulta";
$query_limit_cons = sprintf("%s LIMIT %d, %d", $query_cons, $startRow_cons,
$maxRows_cons);
$cons = mysql_query($query_limit_cons, $conexion) or die(mysql_error());
$row_cons = mysql_fetch_assoc($cons);

if (isset($_GET['totalRows_cons'])) {
  $totalRows_cons = $_GET['totalRows_cons'];
} else {
  $all_cons = mysql_query($query_cons);
  $totalRows_cons = mysql_num_rows($all_cons);
}
$totalPages_cons = ceil($totalRows_cons/$maxRows_cons)-1;

$queryString_cons = "";
if (!empty($_SERVER['QUERY_STRING'])) {
  $params = explode("&", $_SERVER['QUERY_STRING']);
  $newParams = array();
```

```
 foreach ($params as $param) {
  if (stristr($param, "pageNum_cons") == false &&
      stristr($param, "totalRows_cons") == false) {
    array_push($newParams, $param);
  }
 }

if (count($newParams) != 0) {
  $queryString_cons = "&" . htmlentities(implode("&", $newParams));
 }
}
$queryString_cons = sprintf("&totalRows_cons=%d%s", $totalRows_cons,
$queryString_cons);

?><style type="text/css">
<!--
a:link {
        color: #FFFFFF;
}
a:visited {
        color: #FFFFFF;
}
body {
        background-color: #057798;
}
.Estilo5 {color: #FFFFFF}
.Estilo6 {color: #99FFFF}
.Estilo8 {font-size: 18px}
-->
</style>
<p align="center"><a href="index2.html">Inicio</a></p>
```

```
<p> </p>
<p> 

<table border="1" align="center">
  <tr>
    <td><div align="center" class="Estilo6">Nombre</div></td>
    <td><div align="center" class="Estilo6">Apellido</div></td>
    <td><div align="center" class="Estilo6">Sexo</div></td>
    <td><div align="center" class="Estilo6">Edad</div></td>
    <td><div align="center" class="Estilo6">Email</div></td>
    <td><div align="center" class="Estilo6">Usuario</div></td>
    <td><div align="center" class="Estilo6">Clave</div></td>
    <td><div align="center" class="Estilo6">Temperatura</div></td>
    <td><div align="center" class="Estilo6">Frecuencia cardiaca</div></td>
    <td><div align="center" class="Estilo6">Frecuencia
respiratoria</div></td>
    <td><div align="center" class="Estilo6">Fuma</div></td>
    <td><div align="center" class="Estilo6">Frecuencia de consumo de
alcohol</div></td>
    <td><div align="center" class="Estilo6">Frecuencia de consumo de
cafe</div></td>
    <td><div align="center" class="Estilo6">Come de forma
saludable</div></td>
    <td><div align="center" class="Estilo6">Nivel de sal en sus
comidas</div></td>
    <td><div align="center" class="Estilo6">Tiene sobrepeso</div></td>
    <td><div align="center" class="Estilo6">Sufre de diabetes</div></td>
    <td><div align="center" class="Estilo6">Modo de vida
sedentario</div></td>
    <td><div align="center" class="Estilo6">Practica alguna actividad fisica
con regularidad</div></td>
```

```
  <td><div align="center" class="Estilo6">Antecedente familiar con
hipertension arterial</div></td>
  <td><div align="center" class="Estilo6">Ha estado en tratamiento por
hipertension</div></td>
  <td><div align="center" class="Estilo6">Fecha de su ultimo
chequeo</div></td>
  <td><div align="center" class="Estilo6">Con frecuencia esta estresado o
ansioso</div></td>
 </tr>

 <?php do { ?>
  <tr>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['nombre']; ?>  </span></div></td>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['apellido']; ?>  </span></div></td>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['sexo']; ?></span>  </div></td>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['edad']; ?></span>  </div></td>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['email']; ?></span>  </div></td>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['usuario']; ?></span>  </div></td>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['clave']; ?></span>  </div></td>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['temperatura']; ?></span>  </div></td>
   <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['frec cardiaca']; ?>  </span></div></td>
```

```
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['frec respiratoria']; ?> </span> </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['cigarrillo']; ?></span>  </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['alcohol']; ?></span>  </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['cafe']; ?></span>  </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['comida']; ?></span>  </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['sal']; ?></span>  </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['sobrepeso']; ?></span>  </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['diabetes']; ?></span>  </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['sedentario']; ?></span>  </div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['actividad fisica']; ?>  </span></div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['antecedente hipertension']; ?>  </span></div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['tratamiento previo']; ?>  </span></div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['fecha ult chequeo']; ?>  </span></div></td>
    <td><div align="center"><span class="Estilo5"><?php echo
$row_cons['estres']; ?></span>  </div></td>
  </tr>
  <?php } while ($row_cons = mysql_fetch_assoc($cons)); ?>
</table>
```

```
<br />
<table border="0">
  <tr>
    <td><?php if ($pageNum_cons > 0) { // Show if not first page ?>
        <a href="<?php printf("%s?pageNum_cons=%d%s", $currentPage, 0, $queryString_cons); ?>">Primero</a>
        <?php } // Show if not first page ?>    </td>
    <td><?php if ($pageNum_cons > 0) { // Show if not first page ?>
        <a href="<?php printf("%s?pageNum_cons=%d%s", $currentPage, max(0, $pageNum_cons - 1), $queryString_cons); ?>">Anterior</a>
        <?php } // Show if not first page ?>    </td>
    <td><?php if ($pageNum_cons < $totalPages_cons) { // Show if not last page ?>
        <a href="<?php printf("%s?pageNum_cons=%d%s", $currentPage, min($totalPages_cons, $pageNum_cons + 1), $queryString_cons); ?>">Siguiente</a>
        <?php } // Show if not last page ?>    </td>
    <td><?php if ($pageNum_cons < $totalPages_cons) { // Show if not last page ?>
        <a href="<?php printf("%s?pageNum_cons=%d%s", $currentPage, $totalPages_cons, $queryString_cons); ?>">Último</a>
        <?php } // Show if not last page ?>    </td>
  </tr>

</table>
<p><span class="Estilo6">Registros <?php echo ($startRow_cons + 1) ?> a
<?php echo min($startRow_cons + $maxRows_cons, $totalRows_cons) ?> de
<?php echo $totalRows_cons ?>
  </p>
```

```
<?php
mysql_free_result($cons);
?>
</span></p>
<p align="center"><a href="<?php echo $logoutAction ?>"
class="Estilo8">Desconectar</a></p>
```

APÉNDICE C

Código fuente de la página de consulta a los pacientes

```
<?php require('conex.php'); ?>
<?php
if (!function_exists("GetSQLValueString")) {
function GetSQLValueString($theValue, $theType, $theDefinedValue = "",
$theNotDefinedValue = "")
{
  $theValue = get_magic_quotes_gpc() ? stripslashes($theValue) : $theValue;

  $theValue = function_exists("mysql_real_escape_string") ?
mysql_real_escape_string($theValue) : mysql_escape_string($theValue);

  switch ($theType) {
    case "text":
      $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
      break;
    case "long":
    case "int":
      $theValue = ($theValue != "") ? intval($theValue) : "NULL";
      break;
    case "double":
      $theValue = ($theValue != "") ? "'" . doubleval($theValue) . "'" : "NULL";
      break;
    case "date":
      $theValue = ($theValue != "") ? "'" . $theValue . "'" : "NULL";
      break;
    case "defined":
      $theValue = ($theValue != "") ? $theDefinedValue : $theNotDefinedValue;
      break;
  }
  return $theValue;
```

```
}
}

$editFormAction = $_SERVER['PHP_SELF'];
if (isset($_SERVER['QUERY_STRING'])) {
  $editFormAction .= "?" . htmlentities($_SERVER['QUERY_STRING']);
}

if ((isset($_POST["MM_insert"])) && ($_POST["MM_insert"] == "form1")) {
  $insertSQL = sprintf("INSERT INTO consulta (nombre, apellido, sexo, edad,
email, usuario, clave, temperatura, `frec cardiaca`, `frec respiratoria`, cigarrillo,
alcohol, cafe, comida, sal, sobrepeso, diabetes, sedentario, `actividad fisica`,
`antecedente hipertension`, `tratamiento previo`, `fecha ult chequeo`, estres)
VALUES (%s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s,
%s, %s, %s, %s, %s, %s, %s)",
                       GetSQLValueString($_POST['nombre'], "text"),
                       GetSQLValueString($_POST['apellido'], "text"),
                       GetSQLValueString($_POST['sexo'], "text"),
                       GetSQLValueString($_POST['edad'], "int"),
                       GetSQLValueString($_POST['email'], "text"),
                       GetSQLValueString($_POST['usuario'], "text"),
                       GetSQLValueString($_POST['clave'], "text"),
                       GetSQLValueString($_POST['temperatura'], "int"),
                       GetSQLValueString($_POST['frec_cardiaca'], "int"),
                       GetSQLValueString($_POST['frec_respiratoria'], "int"),
                       GetSQLValueString($_POST['cigarrillo'], "text"),
                       GetSQLValueString($_POST['alcohol'], "text"),
                       GetSQLValueString($_POST['cafe'], "text"),
                       GetSQLValueString($_POST['comida'], "text"),
                       GetSQLValueString($_POST['sal'], "text"),
                       GetSQLValueString($_POST['sobrepeso'], "text"),
```

```
                GetSQLValueString($_POST['diabetes'], "text"),
                GetSQLValueString($_POST['sedentario'], "text"),
                GetSQLValueString($_POST['actividad_fisica'], "text"),
                GetSQLValueString($_POST['antecedente_hipertension'], "text"),
                GetSQLValueString($_POST['tratamiento_previo'], "text"),
                GetSQLValueString($_POST['fecha_ult_chequeo'], "date"),
                GetSQLValueString($_POST['estres'], "text"));

  mysql_select_db($database_conexion, $conexion);
  $Result1 = mysql_query($insertSQL, $conexion) or die(mysql_error());

  $insertGoTo = "procesar.php";
  if (isset($_SERVER['QUERY_STRING'])) {
    $insertGoTo .= (strpos($insertGoTo, '?')) ? "&" : "?";
    $insertGoTo .= $_SERVER['QUERY_STRING'];
  }
  header(sprintf("Location: %s", $insertGoTo));
}

?><style type="text/css">
<!--
body {
        background-color: #057798;
}
.Estilo1 {
        font-size: 24px;
        color: #FFFFFF;
}
.Estilo4 {color: #FFFFFF; font-size: 18px; }
-->
</style>
```

```
<script src="SpryAssets/SpryValidationTextField.js"
type="text/javascript"></script>
<link href="SpryAssets/SpryValidationTextField.css" rel="stylesheet"
type="text/css" />

<div align="center">
  <p> </p>
  <p><strong><span class="Estilo1">CONSULTA</span></strong></p>
  <p> </p>
</div>

<form action="<?php echo $editFormAction; ?>" method="post"
name="form1" id="form1">
  <table align="center">
    <tr valign="baseline">
      <td nowrap="nowrap" align="right"><p class="Estilo4">Nombre:</p>
      <p class="Estilo4"> </p></td>
      <td><span id="sprytextfield1">
        <input type="text" name="nombre" value="" size="32" />
      <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

 </tr>
    <tr valign="baseline">
      <td nowrap="nowrap" align="right"><p class="Estilo4">Apellido:</p>
      <p class="Estilo4"> </p></td>
      <td><span id="sprytextfield2">
        <input type="text" name="apellido" value="" size="32" />
      <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>
```

```
    </tr>
    <tr valign="baseline">
      <td nowrap="nowrap" align="right"><p class="Estilo4">Sexo:</p>
      <p class="Estilo4"> </p></td>
      <td><span id="sprytextfield3">
        <input name="sexo" type="text" placeholder="M/F" value="" size="32" />
      <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

    </tr>
    <tr valign="baseline">
      <td nowrap="nowrap" align="right"><p class="Estilo4">Edad:</p>
      <p class="Estilo4"> </p></td>
      <td><span id="sprytextfield4">
        <input type="text" name="edad" value="" size="32" />
      <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

    </tr>
    <tr valign="baseline">
      <td nowrap="nowrap" align="right"><p class="Estilo4">Email:</p>
      <p class="Estilo4"> </p></td>
      <td><span id="sprytextfield5">
        <input type="text" name="email" value="" size="32" />
      <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

    </tr>
    <tr valign="baseline">
      <td nowrap="nowrap" align="right"><p class="Estilo4">Usuario:</p>
      <p class="Estilo4"> </p></td>
```

```
    <td><span id="sprytextfield6">
      <input type="text" name="usuario" value="" size="32" />
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
  <tr valign="baseline">
    <td nowrap="nowrap" align="right"><p class="Estilo4">Clave:</p>
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield7">
      <input type="text" name="clave" value="" size="32" />
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
  <tr valign="baseline">
    <td nowrap="nowrap" align="right"><p class="Estilo4">Temperatura
corporal:</p>
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield8">
      <input name="temperatura" type="text" placeholder="ºC" value=""
size="32" />
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

 </tr>
  <tr valign="baseline">
    <td nowrap="nowrap" align="right"><p class="Estilo4">Frecuencia
card&iacute;aca:</p>
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield9">
```

```
<input name="frec_cardiaca" type="text" placeholder="Latidos/minuto"
value="" size="32" />
<span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

</tr>
<tr valign="baseline">
<td nowrap="nowrap" align="right"><p class="Estilo4">Frecuencia
respiratoria:</p>
<p class="Estilo4"> </p></td>
<td><span id="sprytextfield10">
<input name="frec_respiratoria" type="text"
placeholder="Respiraciones/minuto" value="" size="32" />
<span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

</tr>
<tr valign="baseline">
<td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Con qué
frecuencia fuma diariamente?:</p>
<p class="Estilo4"> </p></td>
<td><span id="sprytextfield11">
<input name="cigarrillo" type="text"
placeholder="Alta/Media/Baja/Ninguna" value="" size="32" />
<span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

</tr>
<tr valign="baseline">
<td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Con
qu&eacute; frecuencia hace consumo de alcohol?:</p>
```

```
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield12">
      <input name="alcohol" type="text"
placeholder="Alta/Media/Baja/Ninguna" value="" size="32" />
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
  <tr valign="baseline">
    <td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Con
qu&eacute; frecuencia consume caf&eacute; diariamente?:</p>
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield13">
      <input name="cafe" type="text" placeholder="Alta/Media/Baja/Ninguna"
value="" size="32" />
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
  <tr valign="baseline">
    <td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Come de
forma saludable?:</p>
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield14">
      <input name="comida" type="text" placeholder="S/N" value="" size="32"
/>
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
  <tr valign="baseline">
```

```
<td nowrap="nowrap" align="right"><p class="Estilo4">Indique el nivel de sal en sus comidas:</p>
<p class="Estilo4"> </p></td>
<td><span id="sprytextfield15">
 <input name="sal" type="text" placeholder="Alta/Media/Baja/Ninguna" value="" size="32" />
<span class="textfieldRequiredMsg">Se necesita un valor.</span></span></td>

</tr>
<tr valign="baseline">
<td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Tiene sobrepeso?:</p>
<p class="Estilo4"> </p></td>
<td><span id="sprytextfield16">
 <input name="sobrepeso" type="text" placeholder="S/N" value="" size="32" />
<span class="textfieldRequiredMsg">Se necesita un valor.</span></span></td>

</tr>
<tr valign="baseline">
<td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Sufre de di&aacute;betes?:</p>
<p class="Estilo4"> </p></td>
<td><span id="sprytextfield17">
 <input name="diabetes" type="text" placeholder="S/N" value="" size="32" />
<span class="textfieldRequiredMsg">Se necesita un valor.</span></span></td>
```

```
  </tr>
    <tr valign="baseline">
     <td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Tiene un
modo de vida sedentario?:</p>
     <p class="Estilo4"> </p></td>
     <td><span id="sprytextfield18">
      <input name="sedentario" type="text" placeholder="S/N" value=""
size="32" />
     <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

    </tr>
    <tr valign="baseline">
     <td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Practica
alguna actividad f&iacute;sica con regularidad?:</p>
     <p class="Estilo4"> </p></td>
     <td><span id="sprytextfield19">
      <input name="actividad_fisica" type="text" placeholder="S/N" value=""
size="32" />
     <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
    <tr valign="baseline">
     <td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Tiene un
antecedente familiar de hipertensi&oacute;n arterial?:</p>
     <p class="Estilo4"> </p></td>
     <td><span id="sprytextfield20">
      <input name="antecedente_hipertension" type="text" placeholder="S/N"
value="" size="32" />
```

```
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
  <tr valign="baseline">
    <td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Ha
estado en tratamiento por hipertensi&oacute;n arterial?:</p>
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield21">
      <input name="tratamiento_previo" type="text" placeholder="S/N"
value="" size="32" />
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
  <tr valign="baseline">
    <td nowrap="nowrap" align="right"><p class="Estilo4">Indique la fecha
de su &uacute;ltimo chequeo:</p>
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield22">
      <input name="fecha_ult_chequeo" type="text" placeholder="DD/MM/AA"
value="" size="32" />
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

  </tr>
  <tr valign="baseline">
    <td nowrap="nowrap" align="right"><p class="Estilo4">&iquest;Con qué
frecuencia est&aacute; estresado o ansioso?:</p>
    <p class="Estilo4"> </p></td>
    <td><span id="sprytextfield23">
```

```
      <input name="estres" type="text" placeholder="Alta/Media/Baja/Ninguna"
value="" size="32" />
    <span class="textfieldRequiredMsg">Se necesita un
valor.</span></span></td>

   </tr>
   <tr valign="baseline">
    <td nowrap="nowrap" align="right"> </td>
    <td><input type="submit" value="Insertar registro" /></td>
   </tr>
  </table>
  <input type="hidden" name="MM_insert" value="form1" />

</form>
<p> </p>
<script type="text/javascript">
<!--
var sprytextfield1 = new Spry.Widget.ValidationTextField("sprytextfield1");
var sprytextfield2 = new Spry.Widget.ValidationTextField("sprytextfield2");
var sprytextfield3 = new Spry.Widget.ValidationTextField("sprytextfield3");
var sprytextfield4 = new Spry.Widget.ValidationTextField("sprytextfield4");
var sprytextfield5 = new Spry.Widget.ValidationTextField("sprytextfield5");
var sprytextfield6 = new Spry.Widget.ValidationTextField("sprytextfield6");
var sprytextfield7 = new Spry.Widget.ValidationTextField("sprytextfield7");
var sprytextfield8 = new Spry.Widget.ValidationTextField("sprytextfield8");
var sprytextfield9 = new Spry.Widget.ValidationTextField("sprytextfield9");
var sprytextfield10 = new Spry.Widget.ValidationTextField("sprytextfield10");
var sprytextfield11 = new Spry.Widget.ValidationTextField("sprytextfield11");
var sprytextfield12 = new Spry.Widget.ValidationTextField("sprytextfield12");
var sprytextfield13 = new Spry.Widget.ValidationTextField("sprytextfield13");
var sprytextfield14 = new Spry.Widget.ValidationTextField("sprytextfield14");
```

```
var sprytextfield15 = new Spry.Widget.ValidationTextField("sprytextfield15");
var sprytextfield16 = new Spry.Widget.ValidationTextField("sprytextfield16");
var sprytextfield17 = new Spry.Widget.ValidationTextField("sprytextfield17");
var sprytextfield18 = new Spry.Widget.ValidationTextField("sprytextfield18");
var sprytextfield19 = new Spry.Widget.ValidationTextField("sprytextfield19");
var sprytextfield20 = new Spry.Widget.ValidationTextField("sprytextfield20");
var sprytextfield21 = new Spry.Widget.ValidationTextField("sprytextfield21");
var sprytextfield22 = new Spry.Widget.ValidationTextField("sprytextfield22");
var sprytextfield23 = new Spry.Widget.ValidationTextField("sprytextfield23");
//-->
</script>
```