ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE LOS NIVELES DE SERVICIO ACORDADOS POR LOS PROVEEDORES DE SERVICIO DE INTERNET PARA LA SUPERINTENDENCIA DE TELECOMUNICACIONES

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

ANDRES CAMILO TOBAR GAMBA
EMAIL: andresflcl@gmail.com

DIRECTOR: ING. XAVIER CALDERÓN HINOJOSA, MSc.
EMAIL: xavier.calderon@epn.edu.ec

Quito, febrero 2015

DECLARACIÓN

Yo, Andrés Camilo Tobar Gamba, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se incluyen en el presente documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a éste trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

Andrés Camilo Tobar Gamba

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el señor Andrés Camilo Tobar Gamba bajo mi supervisión.

_____

ING. XAVIER CALDERÓN HINOJOSA, MSc.

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Agradezco a mis padres Jorge y Leticia por su apoyo inconmensurable e irrestricto a lo largo de mi vida que me han permitido llegar a culminar una etapa más de mi vida, proveyendo lo que estaba a su alcance sin ninguna dilación.

A mis hermanos Carolina y Franco, por la constante motivación que han sabido transmitirme para no claudicar nunca y por todos esos pequeños detalles que supieron colaborarme en algún momento de mi vida.

A mi amigos Mercedes Dávalos y Pierre del Rosario que en algún momento de mi vida tuvieron la gentileza de colaborarme con alguna necesidad personal o tecnológica para poder culminar mis estudios universitarios.

A mi director de tesis, el ingeniero Xavier Calderón por el apoyo y conocimientos brindados para que éste proyecto llegue a un feliz término.

A todos y cada uno de mis profesores, que han contribuido en el desarrollo profesional y personal a lo largo de mi vida como estudiante de la para mi muy querida Escuela Politécnica Nacional del Ecuador.

Andrés Camilo Tobar Gamba

DEDICATORIA

Dedico éste trabajo a mis padres Jorge y Leticia ya que sin ellos éste no hubiera sido posible. A mis hermanos Carolina y Franco por estar siempre ahí cuando necesitaba su ayuda. A mis amigos Mercedes Dávalos y Pierre del Rosario por la ayuda prestada a lo largo del tiempo que nos conocemos.

Andrés Camilo Tobar Gamba

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el presente proyecto, se describe el análisis, diseño e implementación de una aplicación computacional para la Superintendencia de Telecomunicaciones, que permite la medición, almacenamiento y consulta, tanto de la información de ancho de banda de bajada y subida, como el índice de disponibilidad al que tienen acceso los usuarios residenciales del servicio de Internet, con el propósito de establecer un marco técnico que permita en un futuro normar y controlar el ancho de banda ofrecido por los Proveedores de Servicio de Internet.

El primer capítulo corresponde a fundamentos teóricos donde se define el problema a resolver, además de la descripción de cada una de las herramientas tecnológicas en las cuales se basa el presente proyecto, con especial énfasis en la descripción del funcionamiento del protocolo SNMP y de los Servicios Web corporativos de Java Enterprise Edition.

El segundo capítulo se centra en el análisis necesario para el desarrollo del proyecto, iniciando con un análisis de la situación actual de la Superintendencia de Telecomunicaciones, para luego centrarse en el análisis de los requerimientos de funcionamiento y seguridad con los que deberá contar la nueva aplicación.

En el tercer capítulo se detallan el diseño y la implementación de la nueva aplicación mediante la descripción de cada uno de los módulos con las que cuenta ésta.

Para el cuarto capítulo, se realizan las respectivas pruebas de funcionamiento de la nueva aplicación, además del análisis de los resultados obtenidos y la comparación de éstos con los obtenidos por otras aplicaciones semejantes.

Finalmente, el quinto capítulo comprende las conclusiones y recomendaciones referentes a cada uno de las etapas realizadas a lo largo de la presente tesis.

PRESENTACIÓN

El Internet en la actualidad es sin lugar a dudas, uno de los servicios más importantes y necesarios del ser humano, para comunicarse de manera rápida y sin restricciones, por lo que su uso es casi masivo alrededor del mundo. El Ecuador no se ha visto ajeno a ésta realidad y es así que la presencia del Internet es cada vez mayor en los hogares ecuatorianos, con índices de penetración creciendo de manera exponencial año a año, ésto debido en gran parte al continuo decremento de los costos que los usuarios de éste servicio tienen que desembolsar para su uso, haciéndose tan accesible e importante que en la actualidad es considerado como un servicio fundamental comparable con otros servicios básicos tradicionales.

Por ésta razón, la Superintendencia de Telecomunicaciones en función de cumplir con su labor de proteger y cuidar los derechos y obligaciones de los usuarios de Servicios de Telecomunicaciones en el Ecuador, se ve en la necesidad de implementar un sistema que permita el control y monitoreo del Servicio de Internet entregado por los Proveedores de Servicio de Internet a sus usuarios, y a partir de ésta base técnica, poder establecer una normativa de operación para éste tipo de servicio, ya que en la actualidad no se encuentra tipificado en ningún reglamento ecuatoriano los términos técnicos mininos para la prestación del servicio de Internet.

Mediante la solución computacional presentada en el presente documento, se propone el control y monitorización de los niveles de calidad del Servicio de Internet por medio de la medición de ancho de banda de bajada y subida, y el índice de disponibilidad del servicio de Internet al que tienen acceso los usuarios finales de éste servicio con la ayuda del protocolo de gestión de redes de datos SNMP y los servicios web corporativos de Java Enterprise Edition.

CAPÍTULO I: MARCO TEÓRICO

Para una comprensión correcta del presente proyecto, es necesario tener claro la definición y manera en que funcionan los diferentes elementos, protocolos y tecnologías involucradas en la creación de la herramienta computacional que permitirá el control y monitoreo de los niveles de servicio de internet en los usuarios. De ésta manera, se hará un breve repaso de que es Ancho de banda, cómo funcionan los medidores de Ancho de Banda disponibles, que son los sistemas de monitorización y gestión, que es y cómo funciona SNMP, la forma en que funcionan las aplicaciones distribuidas por medio de servicios web Java Enterprise Edition.

1.1 DEFINICIÓN DEL PROBLEMA

La Superintendencia de Telecomunicaciones (SUPERTEL), en la necesidad de controlar y reglamentar la calidad del Servicio de Internet prestado por los respectivos proveedores de dicho servicio, requiere de un software computacional que permita la medición y captura del ancho de banda de acceso al Internet para su posterior consulta y análisis y así determinar si los Proveedores del Servicio de Internet cumplen con los términos de servicio acordado con sus clientes. La idea es crear el ambiente técnico necesario para que el Servicio de Internet o de Valor Agregado sea normado y reglamentado ya que en la actualidad éste tipo de servicios no lo están.

En la actualidad, la SUPERTEL no cuenta con ningún sistema o arquitectura computacional que le permita capturar y almacenar el ancho de banda disponibles para los usuarios del servicio de Internet; por ésta razón, la solución computacional presentada en éste documento parte de cero, y es desarrollada en base al análisis de requerimientos y al análisis de los recursos de hardware y software disponibles en la SUPERTEL.

1.2 ANCHO DE BANDA Y VELOCIDAD DE TRANSMISIÓN

Los términos ancho de banda (bandwidth en inglés) y velocidad de transmisión (transmission rate o bit rate en inglés) describen aspectos técnicos en las telecomunicaciones muy diferentes, pero han terminado definiendo al mismo fenómeno dentro de las comunicaciones de redes de datos, ya que según la ley de Shannon-Hartley la velocidad o capacidad máxima de transmisión de un canal de transmisión es proporcional al ancho de banda, pero no la misma.

Técnicamente, el término ancho de banda representa el espectro o banda de frecuencia resultante de la diferencia entre la frecuencia más alta y la frecuencia más baja utilizado en una transmisión de datos por un canal de transmisión, el mismo que está medido en Hertzios (Hz).[1] A su vez, el término Velocidad de Transmisión describe la velocidad máxima a la que se puede transmitir datos a través de un medio de transmisión y su unidad es bits por segundo (bps).[2]

Los proveedores del servicio de Internet han optado por utilizar el término ancho de banda para definir la velocidad máxima de transmisión a la que pueden transmitir paquetes de datos sus usuarios dentro de Internet a pesar de que por definición sea incorrecto, tal cual se ha señalado. Con el fin de mantener concordancia con ésta terminología, en el presente proyecto se utilizará el término ancho de banda en lugar del término velocidad de transmisión.

Por lo tanto, en el presente documento el término ancho de banda se refiere a la velocidad de transmisión máxima o cantidad de bits máximos transmitidos por segundo dentro de una red datos, que puede ser el Internet, y su unidad será bits por segundo (bps), pudiendo también ser bytes por segundo (Bps) ya que de bits a bytes solo existe un factor de conversión de 8 unidades (1 byte = 8 bits).

---

[1] Spectra and Bandwidth of Emissions, Recomendacion ITU-R SM.328-10, 1999.

[2] W. Stallings,“Digital Data Communications Techniques” en *Data and Computer Communications*, 8va Edición, Upper Saddler River: Pearson Prentice Hall, 2007, página 91.

1.2.1 ANCHO DE BANDA DE BAJADA Y ANCHO DE BANDA DE SUBIDA

Existen dos tipos de ancho de banda, el primero es el llamado ancho de banda de bajada y el segundo el denominado ancho de banda de subida.

Suponiendo el caso de tener dos computadores A y B, que intercambian paquetes de datos entre sí a través de una red de comunicación como el Internet, como se muestra en la Figura 1.1. Los paquetes de datos no son más que bits de información transmitidos por el medio de transmisión.

El ancho de banda de bajada para el computador A es la velocidad máxima con la que descarga o recibe los paquetes de datos provenientes del computador B. De igual manera, para el computador B su ancho de banda de bajada es la velocidad máxima con que recibe paquetes de datos desde el computador A.

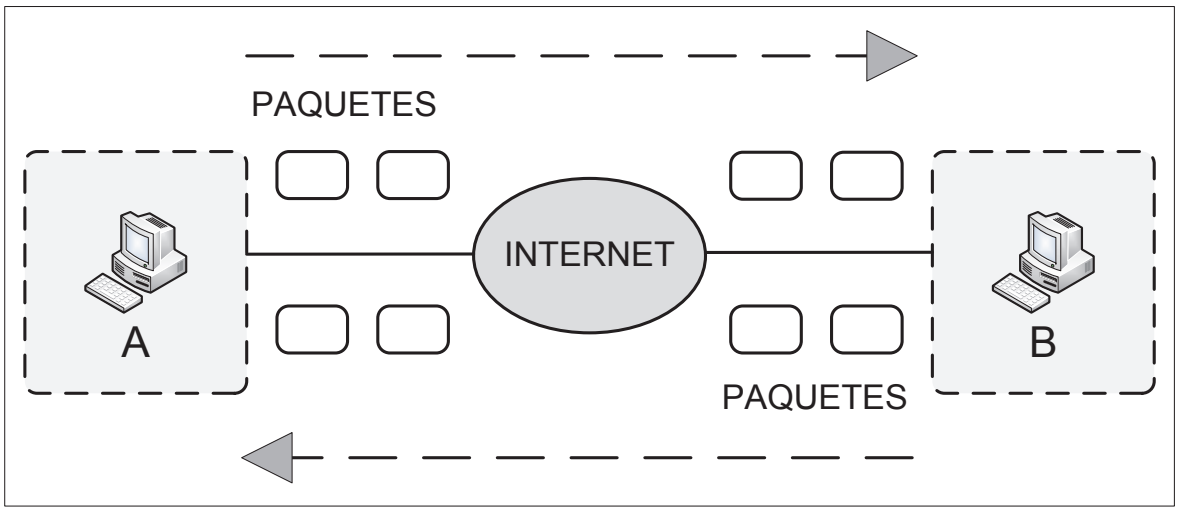


Figura 1.1. Ejemplo Intercambio de paquetes entre 2 computadores.

Por el contrario el ancho de banda de subida para el computador A y B, corresponde a la velocidad máxima con que envían o “suben” paquetes de datos hacia el computador B y A respectivamente.

1.2.2 EL ANCHO DE BANDA DENTRO DEL SERVICIO DE INTERNET

El servicio de Internet proveído por los Proveedores de Servicio de Internet (ISP) conlleva un ancho de banda específico y limitado, el mismo que es estipulado en el contrato de renta del servicio de Internet entre el ISP y el usuario final. Por lo tanto el ancho de banda disponible para los clientes es controlado por los ISP pudiendo éste modificarlo o restringirlo de acuerdo a su capacidad de operación y provisión.

El ancho de banda para el servicio de Internet, hace una clara diferenciación entre ancho de banda de bajada y ancho de banda de subida haciendo que el ancho de banda de bajada sea mayor que el ancho de banda de subida con el fin de maximizar los recursos propios del ISP, ya que de manera general los usuarios del servicio de Internet descargan o bajan mayor cantidad de datos desde el Internet de lo que suben o envían hacia éste. Por tal razón, los ISP proveen un canal asimétrico de transmisión entre el usuario y el Internet.

1.3 MEDIDORES DE ANCHO DE BANDA

Los medidores de ancho de banda son programas computacionales que permiten la verificación o consulta del ancho de banda al cual tienen acceso a Internet los usuarios de éste servicio a través de una prueba que consiste en el envío de paquetes de datos entre un computador a otro a través del Internet durante un tiempo determinado y mediante un simple cálculo matemático se obtienen valores de ancho de banda medidos en bits por segundo o bps. De manera general, éstas aplicaciones son de tipo Web, es decir que se encuentran disponibles en el Internet sin requerir algún tipo de instalación en el computador donde se realizan las pruebas y únicamente usan los navegadores web como interfaces entre el programa y el usuario.

El objetivo de estos medidores es el de presentar a los usuarios del servicio de Internet el ancho de banda real con el que disponen en sus conexiones a Internet

para que luego lo comparen con el ancho de banda contratado con sus respectivos ISP.

Para la obtención de resultados de ancho de banda más cercanos a la realidad, los medidores de ancho de banda requieren que el usuario asegure que ninguna otra aplicación o usuario de su red de datos esté haciendo uso de Internet durante el proceso de medición.

1.3.1 FUNCIONAMIENTO DE LOS MEDIDORES DE ANCHO DE BANDA

Los medidores de ancho de banda constan fundamentalmente de dos elementos, un computador que funciona como servidor y otro que hace de cliente, Figura 1.4. El medidor de ancho de banda más utilizado es la aplicación encontrada en el sitio web http://www.speedtest.net, el mismo que funciona de la siguiente manera:

1. El servidor se mantiene indefinidamente a la espera de solicitudes al servicio de medición de ancho de banda por parte de los clientes.
2. El cliente a través de un navegador web solicita el servicio a través de una página web.
3. El servidor recibe la solicitud e inicia el proceso de medición.
4. Desde el servidor se envía paquetes de datos; una tras de otro, hacia el cliente durante un tiempo determinado, que para la aplicación de medición de ancho de banda encontrada en el sitio web http://speedtest.net, es de 10 segundos.
5. El cliente recibe los paquetes de datos enviados desde el servidor.
6. El servidor determina el número de paquetes de datos que fueron enviados durante ese tiempo.
7. Ya que el servidor conoce el tamaño de cada uno de los paquetes de datos en bits o Bytes, mediante la división del número de éstos sobre el tiempo determinado se obtiene el valor correspondiente a ancho de banda de bajada.

$$ABbajada[bps] = \frac{\#\ PaquetesEnviados * TamañoPaqueteDatos[Bytes] * 8}{TiempoEnvio[segundos]}$$

Figura 1.2. Fórmula para el cálculo de ancho de banda de bajada para el medidor speedtest.net.

8. Seguidamente, el servidor inicia el proceso para la medición del ancho de banda de subida ordenando al cliente que envíe paquetes de datos al servidor mediante el uso de la operación HTTP Post durante 10 segundos.
9. El servidor recibe los paquetes enviados desde el cliente.
10. El servidor procede a realizar el cálculo de ancho de banda de subida conociendo el número de paquetes de datos recibidos, el tamaño de éstos y el tiempo que tomó en recibir los paquetes de datos.

$$ABsubida[bps] = \frac{\#\ PaquetesRecibidos * TamañoPaqueteDatos[Bytes] * 8}{TiempoRecibo[segundos]}$$

Figura 1.3 Formula para el cálculo ancho de banda de subida para el medidor speedtest.net.

11. El servidor envía los resultados de la medición tanto de ancho de banda de bajada como de subida al cliente.
12. El cliente presenta los resultados al usuario por medio del navegador web desde donde se accedió inicialmente a la aplicación de medición.

1.4 SISTEMAS DE MONITORIZACIÓN Y GESTIÓN DE REDES

En toda empresa u organización comercial y de servicios es cada vez más evidente el crecimiento continuo hacia redes computacionales cada vez más grandes, con mayor número de usuarios y aplicaciones, haciéndolas a su vez más difíciles de administrar y monitorear. Ésto ha obligado a la creación de sistemas, normativas y protocolos de gestión que faciliten el control, mantenimiento, análisis, detección de fallas y mejoramiento de los diferentes parámetros de la red, permitiendo que ésta

funcione adecuadamente, reduciendo la intervención humana paulatinamente. A éste conjunto de sistemas, normativas y protocolos de monitorización y gestión se le denomina sistema de monitorización y gestión de redes.

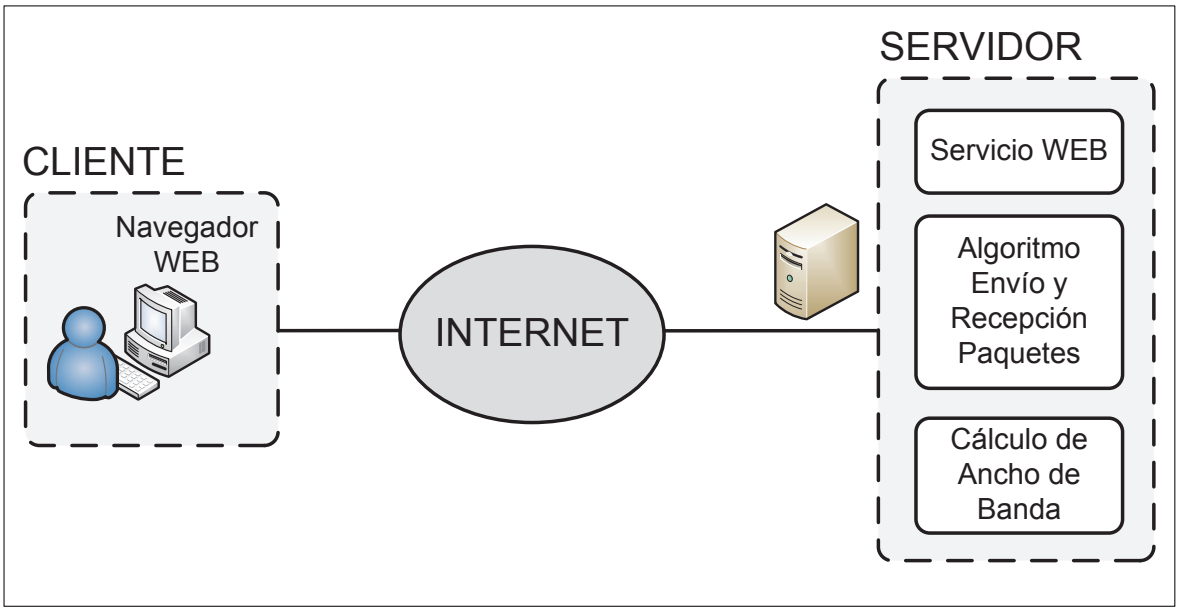


Figura 1.4. Componentes de los Medidores de Ancho de Banda.

De manera más formal, se puede definir a la gestión de redes como el conjunto de recursos humanos y computacionales; tanto hardware como software, destinados a la monitorización, realización de pruebas, mantenimiento, ubicación de fallas y mejoramiento de los diferentes elementos de la red disponibles para la utilización y aprovechamiento eficiente de todos los recursos utilizados por la red de forma centralizada.

1.4.1 FUNCIONES DE LOS SISTEMAS DE MONITORIZACIÓN Y GESTIÓN DEREDES

Las funciones fundamentales de los sistemas de gestión y monitorización, están en estrecha relación con salvaguardar y proteger cada uno de los factores que determinan el funcionamiento eficiente y sin fallos de una red. Es así, que los

sistemas de monitorización y gestión están encargados de cumplir las siguientes funciones primordialmente:

- Detección de fallos.
- Configuración de dispositivos.
- Control de cuentas de usuario.
- Determinación de la funcionalidad de la red.
- Seguridad de la red.

Cada uno de las funciones antes indicadas, pueden determinar también, en qué grado o que tan bien el sistema de monitorización y gestión está siendo utilizado en la red, además de cómo éste puede ser mejorado o ampliado.

1.4.1.1 Detección de fallos

Ésta función permite detectar, separar y almacenar la información de fallos y errores ocurridos dentro de la red de manera rápida y oportuna para luego repararlos de manera automática y eficaz sin comprometer la disponibilidad de los servicios provistos a los usuarios.

1.4.1.2 Configuración de dispositivos

La función de configuración de dispositivos se encuentra relacionado con la tarea de verificar y detectar cambios de configuración de los dispositivos que forman parte de la red; así como también, la recopilación de información referente a cambios de versiones, actualizaciones, expansiones y adiciones tanto de hardware, como de software, que permitan la posterior adecuación de la red a los mencionados cambios.

1.4.1.3 Contabilidad de Recursos de Red

Por medio de ésta función, es posible obtener información referente al grado de utilización de todos los recursos de red disponibles por los usuarios, departamentos o unidades de trabajo con el fin de repartir éstos recursos de manera eficiente,

priorizando las áreas más críticas e importantes dentro de la organización que hace uso de la red.

1.4.1.4 Determinación de la Funcionalidad de la Red

El objetivo de ésta función, es determinar si la red funciona de manera eficiente a través de la captura de información que permita comparar el nivel de utilización de la red actual con la máxima capacidad permitida por ésta con el propósito de prever futuros cambios o mejoras manteniendo los niveles funcionales y de disponibilidad a pesar de que la red crezca en cuanto a número de usuarios, número de aplicaciones, número de enlaces, etc.

1.4.1.5 Seguridad de la Red

La función de seguridad de la red tiene que ver con el hecho de garantizar que la red funcione de manera confiable y segura, a través de la implementación de sistemas y servicios de autenticación de usuarios, privacidad de datos, integridad de la información y auditoría. Ésta función también está relacionada con la configuración de los distintos dispositivos y elementos encargados de la seguridad de la red como cortafuegos, antivirus, listas de acceso, detectores de intrusos, etc.

1.4.2 CLASIFICACIÓN DE LOS SISTEMAS DE MONITORIZACIÓN Y GESTIÓN DE RED

Existen diferentes tipos de redes en la actualidad, diferenciándose principalmente dos grandes grupos, las redes de computadoras y las redes de telecomunicaciones, lo que ha obligado a la creación de sistemas de monitoreo y gestión que se adapten a éstas y a sus requerimientos. Es así, que los sistemas de monitorización y gestión se dividen en Sistema de Gestión de Redes de Computadoras y el Sistema de Gestión de Redes de Telecomunicaciones, los mismos que a su vez se subdividen de acuerdo al punto de vista de diferentes entidades de estandarización internacionales, tal como se indica en la Figura 1.5.

1.4.2.1 Modelo de Gestión OSI

Éste modelo de monitorización y gestión fue creado por la Organización Internacional de Estándares (OSI), con el fin de ser integrado a los diferentes dispositivos basados en el modelo referencial OSI y lograr la gestión de sistemas de interconexión abierta por medio del uso del protocolo CMIP que son las siglas para Protocolo de Información y Administración Común.

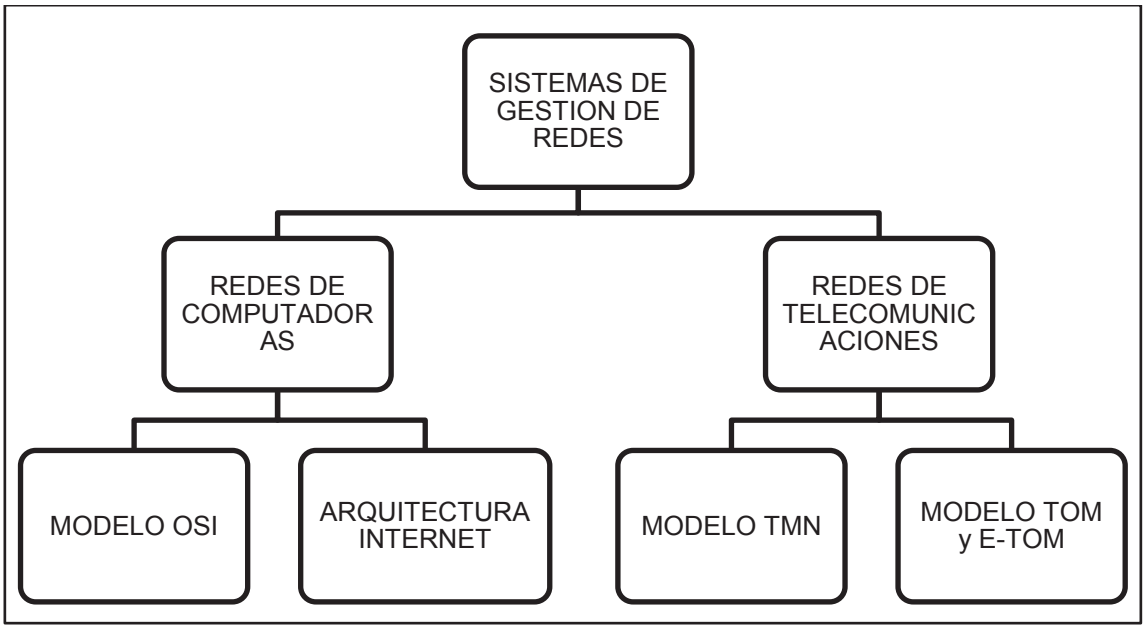


Figura 1.5. Clasificación de los modelos de los Sistemas de Gestión de Redes.

1.4.2.2 Arquitectura Internet

Es el modelo más extendido en la actualidad en cuanto a redes de computadoras se refiere. Creado por la Fuerza Especial sobre Ingeniería de Internet, IETF sus siglas en inglés, para ser utilizado por los sistemas basados en el sistema de referencia TCP/IP en base al protocolo SNMP, el mismo que será descrito a detalle más adelante.

1.4.2.3 Modelo TMN (Red de Gestión para las Telecomunicaciones)

Impulsado por la Unión Internacional de Telecomunicaciones UIT – T sección Telecomunicaciones para la monitorización y gestión de redes de

telecomunicaciones basado en los modelos para monitorización y gestión de redes de computadoras. El modelo se define como una red separada de la red de telecomunicaciones, conectada a ésta en varios puntos específicos con el fin de monitorearla y gestionarla sin interferir su correcto funcionamiento.

1.4.2.4 Modelo TOM (Mapa de Operaciones para TELECOM) y E-TOM (TOM-Mejorado)

Desarrollado por Telemanagement Forum, que forma parte de la UIT y busca el mejoramiento de la gestión de redes de telecomunicaciones empresariales, dividiendo los procesos operacionales y empresariales del usuario de los del proveedor de servicios de telecomunicaciones.

1.4.3 ELEMENTOS Y FUNCIONAMIENTO DE LOS SISTEMAS DE MONITORIZACIÓN Y GESTIÓN DE RED

Los sistemas de monitorización y gestión de redes deben contar con una serie de elementos que permitan su trabajo de manera correcta sin interferir con el adecuado funcionamiento de la red, cumpliendo con la premisa fundamental de hacerlo de manera centralizada, automatizada e integrada.

Tal como se expuso anteriormente, principalmente existen dos tipos de redes, redes de datos y redes de telecomunicaciones; teniendo ésto en cuenta, los elementos de los sistemas de monitorización y gestión deben acoplarse e integrarse a la red sin importar de que tipo sea ésta. Es por ésto que se ha convenido que todos los tipos de redes cuenten de manera general con los elementos descritos a continuación:

- NMS o Gestor.
- NME o Agente.
- MIB o Base de datos de información de monitorización y gestión.
- Protocolo de monitorización y gestión de red.

1.4.3.1 NMS (Sistema de Gestión de Red)

El sistema de gestión de red; también conocido como Gestor, es el componente que se encarga de consultar, obtener y recibir información referente al comportamiento de la red por medio de los llamados polls y traps, consultas o alarmas respectivamente, como se describe en la Figura 1.6. En base a ésta información es posible realizar las funciones que todo sistema de monitorización y gestión de redes debe cumplir, para luego tomar las decisiones correspondientes y necesarias por parte del personal encargado de la administración de la red.

El gestor es también considerado como la interfaz entre el sistema de monitorización y el recurso humano a cargo de controlar y monitorear la red, pudiéndose encontrar en el mercado un gran número de programas computacionales tanto de licencia libre como pagos que se encargan de realizar las tareas básicas de los NMSs diferenciándose entre sí principalmente por la manera en que muestran la información de monitorización al usuario. Por lo general está localizado en un computador centralizado que hace las veces de cliente del servicio de monitorización y gestión.

1.4.3.2 NME (Entidad de Gestión de Red)

La entidad de gestión de red se encuentra en todos aquellos dispositivos que forman parte de una red; llámense éstos computadores, conmutadores, encaminadores o ruteadores, puertas de acceso, puentes, módems, etc., ya sea integrados como servicios en sus respectivos sistemas operativos o como programas instalados y escritos en algún lenguaje de programación compatible.

El NME es también conocida como Agente y tiene como funciones, capturar y almacenar continuamente información de administración de red del dispositivo, para luego enviarlos al NMS; ya sea como una Notificación(trap), o en respuesta a una Solicitud (poll) enviado por el NMS, tal cual se explica en la Figura 1.6. La información de administración puede contener datos relacionados por ejemplo, a que interfaces de red se encuentran activas y cuáles no, la cantidad de octetos saliendo y

entrando por cada interfaz, descripción del equipo a nivel de hardware y software, tipo de protocolos utilizados, etc.

De manera general, a los dispositivos monitoreados y gestionados se les conoce como agentes, por lo que dentro de una red pueden existir cientos de agentes, dependiendo del número y tipo de dispositivos que se desee monitorear y gestionar a través del NMS.

1.4.3.3 MIB (Base de Datos de Información de Monitorización y Gestión)

La base de datos de información referente a la monitorización y gestión de redes, es como su nombre lo indica, un repositorio o base de datos de un conjunto de aspectos, características u objetos propios del dispositivo de red a monitorear, como por ejemplo, información de las interfaces, hardware, protocolos disponibles, etc., La información guardada en éstas bases de datos es capturada almacenada y utilizada por el NME según ésta le sea requerida por el NMS.

De manera general, las MIBs funcionan de manera volátil; es decir, que cuando el equipo es apagado la información almacenada en éstas bases de datos se pierde y solo es obtenida y almacenada nuevamente cuando el dispositivo sea iniciado. De igual manera, existen ciertas MIBs que pueden ser cambiadas a discreción del usuario o del personal de administración de la red; pero en su gran mayoría, las MIBs son solo modificables por el NME presente en el dispositivo de acuerdo al comportamiento y funcionamiento de los aspectos y objetos del dispositivo dentro de la red.

1.4.3.4 Protocolo de Gestión de Red

El protocolo de gestión de red es la forma o reglas en las que el gestor y el agente establecen la comunicación, encapsulan en una PDU la información, intercambian paquetes de datos y terminan la comunicación; entre otras cosas, con el propósito de llevar a cabo la monitorización y gestión de redes.

Dependiendo del modelo de monitorización y gestión de red utilizado, varía el protocolo de gestión necesario, siendo SNMP el protocolo de monitorización y gestión de red más utilizado ya que el modelo de monitorización y gestión de Internet se basa en el modelo referencial TCP/IP, que en la actualidad es el más extendido en lo referente a redes de computadoras, y en base al cual se han creado otros protocolos de gestión de red, tanto para redes de computadoras como para redes de telecomunicaciones.

Dentro de la arquitectura de monitorización y control de redes, el protocolo de gestión de red debe cumplir con ciertas tareas fundamentales sobre cada uno de los objetos gestionados o simplemente MIBs presentes en los agentes, como son:

- Obtener *(Get).*
- Establecer *(Set).*
- Notificar *(Trap).*

1.4.3.4.1 Obtener (get)

La función de obtener permite que el gestor adquiera la información necesaria de las MIBs de cada uno de los agentes monitoreados, siendo posible acceder a todas las MIBs disponibles en los agentes si se tienen los permisos necesarios. El gestor es el único capaz de llevar a cabo ésta función sobre los agentes.

1.4.3.4.2 Establecer (set)

El establecer está relacionado con la función de asignar, establecer o cambiar las distintas MIBs en todos los agentes desde el gestor, ya sea de manera automática o por el personal responsable de la administración de la red. Es necesario recordar, que ciertas MIBs permiten ser manipuladas de ésta forma ya que en su gran mayoría no lo son. De igual manera el gestor es el único que puede realizar la función de establecer sobre los agentes.

1.4.3.4.3 Notificar (trap)

La notificación es la función encargada de enviar alarmas o notificaciones de los sucesos ocurridos en las MIBs de los agentes hacia el gestor con el propósito de que éste último se entere y actué frente a los fallos detectados en los agentes que generaron dichas alarmas. El agente es el único capaz de generar y enviar notificaciones al gestor.

1.4.3.5 Comunicación entre el NMS y el NME

El gestor y el agente deben basarse en las reglas definidas por el protocolo de gestión de red para la comunicación correcta e inequívoca entre ellos, por lo que dependiendo del tipo de red gestionado; y por ende el tipo de protocolo de gestión de red, será la forma en la cual éstos dos elementos tengan contacto. De manera general, en los sistemas de monitorización y gestión, el gestor y el agente establecen una comunicación de la manera representada en la Figura 1.6, basados principalmente en el sistema de monitorización y gestión de redes de computadoras de Internet.

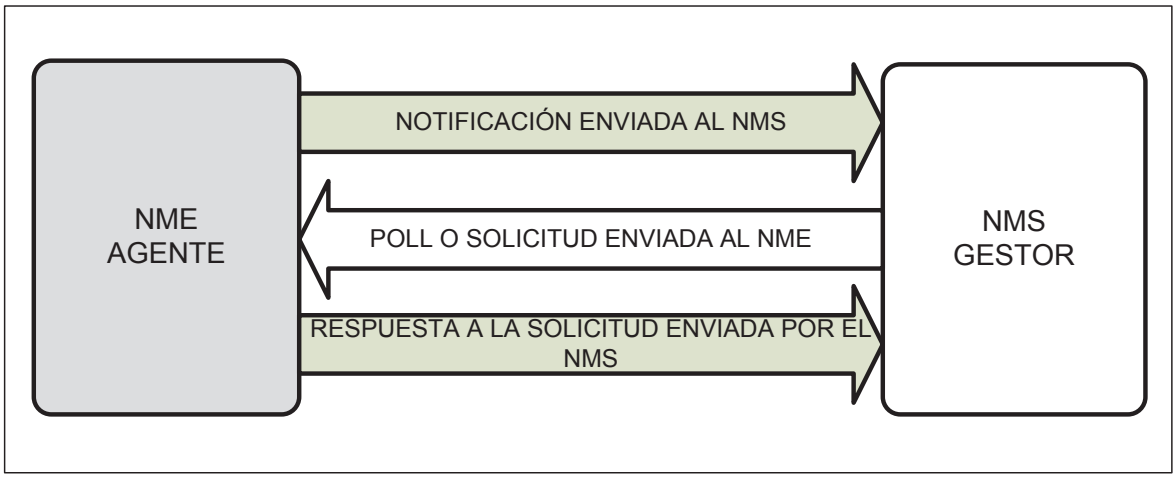


Figura 1.6. Manera como se comunica el NMS con la NME.

El gestor continuamente envía solicitudes al agente, con el fin de establecer el estado de las MIBs de éste último y poder determinar la manera que los dispositivos que contienen los agentes están funcionando dentro de la red, éstas solicitudes son

de tipo *obtener*. El gestor en respuesta a éstas solicitudes, se encarga de analizar e identificar que MIBs son requeridas para luego enviar las respectivas respuestas hacia el gestor. Por ejemplo, imaginar que se necesite conocer el tiempo que lleva activo o encendido el dispositivo donde se encuentra el agente. Para ésto desde el gestor se envía una solicitud a la MIB respectiva del agente, éste consultara su base de datos de gestión en busaca de tal MIB, para luego enviar la respuesta al gestor informando desde cuando el dispositivo gestionado se encuentra activo.

A su vez, las solicitudes de tipo *establecer* hechas del gestor al agente solo buscan cambiar la información contenida en las MIBs, por lo tanto, no existe una respuesta del agente al gestor para ésta solicitud. El agente al recibir éstas solicitudes se encarga de buscar la MIB requerida y cambiar la información contenida en ésta por la nueva especificada dentro de la solicitud

El agente por su parte, puede ser capaz de enviar información al gestor únicamente cuando existe una novedad o emergencia detectada en el agente y que requiera la urgente intervención del gestor. La información enviada de ésta forma, es conocida como *notificación* y son programadas para activarse en situaciones graves que comprometan el funcionamiento del dispositivo donde se encuentra el agente, y su operación dentro de la red. Ejemplos de ésto son, el apagado no programado del dispositivo, la caída de una interfaz de red en el dispositivo, la detección de un intruso, etc. El gestor recibirá dicha alarma y dependiendo de la gravedad del suceso, tomara los correctivos necesarios, ya sea de manera automática o informando al personal humano cuando el problema esté fuera del alcance del sistema de monitorización y gestión.

1.5 MODELO DE MONITORIZACIÓN Y GESTIÓN DE REDES DE COMPUTADORAS DE INTERNET

El modelo de monitorización y gestión de redes de computadoras de internet; o llamado simplemente Modelo de Gestión de Internet, se creó para brindar la

capacidad de monitorizar y administrar todos los elementos y dispositivos de las redes de computadoras que basan su funcionamiento en el modelo referencial TCP/IP, cuyo conjunto de protocolos son utilizados en la gran mayoría de redes de computadoras, siendo tal su alcance, que el internet trabaja en base a éste modelo de referencia.

A medida que las redes de computadoras han ido creciendo en número de dispositivos, número de aplicaciones, número de usuarios, etc.; y con la popularidad en aumento que ha tenido el Internet, han obligado a la IETF a crear un protocolo capaz de facilitar el monitoreo y gestión de éste tipo de redes que cada vez se vuelven más complejas y difíciles de administrar. Para cubrir con ésta necesidad fue creado SNMP, que son las siglas en inglés de Protocolo Simple de Gestión de Red y en base al cual el modelo de monitorización y gestión de redes de computadoras de Internet está definido.

De igual manera, el modelo de gestión de Internet cuenta en su arquitectura con su respectivo gestor, agentes, y MIBs, además del ya menciona protocolo de gestión SNMP, por lo que la forma en que éste modelo funciona es básicamente la misma a la descrita para los modelos de monitorización y gestión en general en los puntos previos.

Tradicionalmente, la arquitectura del modelo de gestión de Internet describe un esquema centralizado; es decir, que se cuenta con un solo gestor encargado de monitorear a todos los agentes presentes dentro de la red, Figura 1.7. Si bien éste tipo de esquema funciona adecuadamente en redes de computadoras pequeñas, no lo es tanto cuando se habla de redes de computadoras de gran tamaño, en donde es más apropiado utilizar sistemas distribuidos donde se dispone de más de un gestor a cargo de la gestión de una gran cantidad de agentes dentro de la red, Figura 1.8.

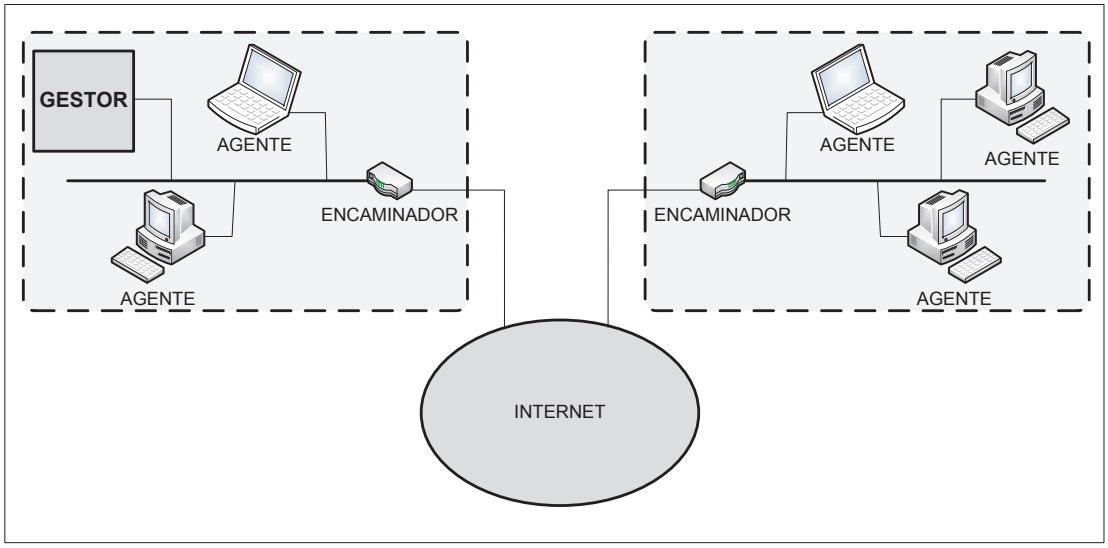


Figura 1.7. Esquema con NMS centralizado.

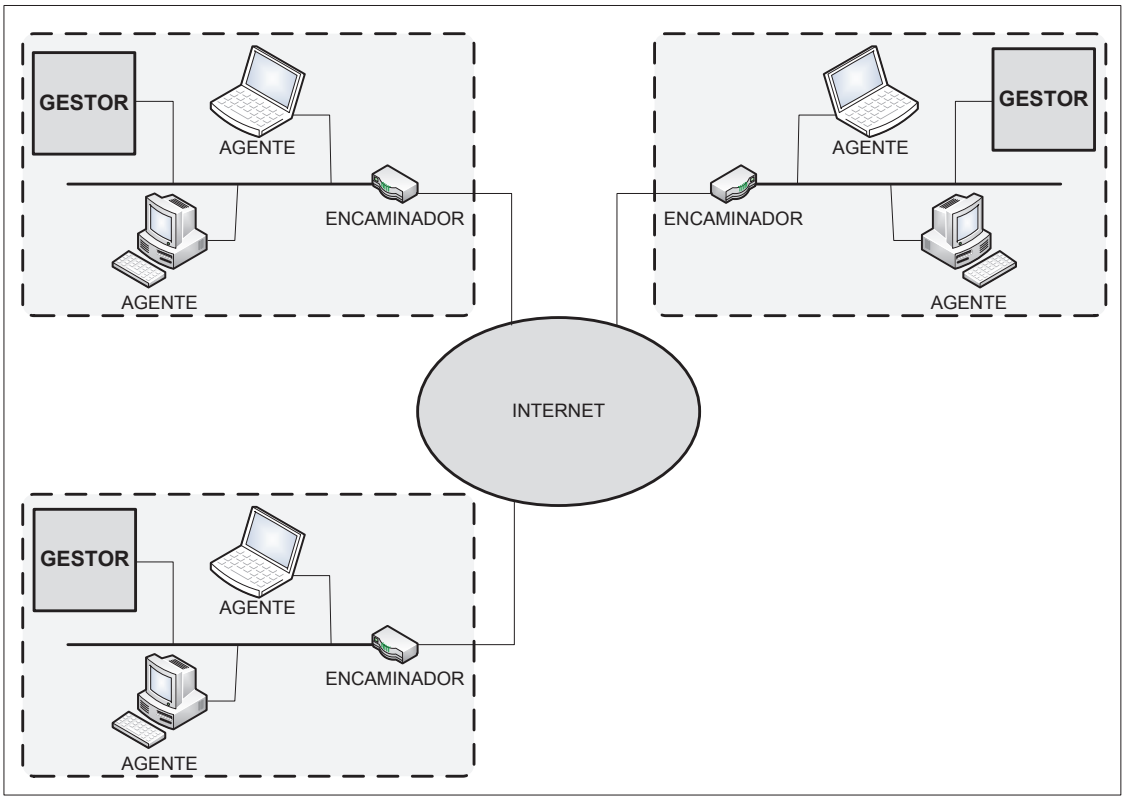


Figura 1.8. Esquema con Gestor distribuido.

1.5.1 NMS Y EL MODELO DE GESTIÓN DE INTERNET

En el modelo de gestión de Internet, el NMS o gestores el dispositivo o dispositivos encargados de realizar la tarea de monitorización y gestión de los agentes gestionados presentes en una red de computadoras en base a SNMP, éste dispositivo por lo general es un computador o estación de trabajo con capacidad de interactuar con el componente humano encargado de la gestión de la red.

La comunicación entre el gestor y el agente en el modelo de gestión de Internet es la misma que la descrita para cualquier tipo de NMS y NME, pero bajo lo dispuesto por SNMP, de ésta forma, el gestor puede realizar solicitudes al agente y recibir de éste la respuesta a dichas solicitudes, además de las llamadas notificaciones producto de eventos extraordinarios sucedidos en el agente.

El gestor se lo puede encontrar como una herramienta computacional escrita en algún lenguaje de programación o como parte de un servicio de gestión propio del sistema operativo del gestor, capaz de comunicarse con sus agentes en base a SNMP, la elección de éste tipo de programas dependerá del tipo de licencia; pudiendo ser de distribución libre o paga, capaces de funcionar en distintos ambientes operativos; principalmente Windows y Unix (incluidas todas sus distribuciones), siendo éste último en donde se ha logrado un desarrollo mayor y extenso de SNMP como tal. Algunas de las aplicaciones más conocidas son Zabbix, Open View, NetView, Open NMS, MRTG-PRTG, Nagios, etc.

De igual forma, es posible la creación de soluciones computacionales que cumplan la labor del gestor pero adecuado a las necesidades específicas de la red de computadoras a monitorizar; es así que lenguajes de programación como C++ y Java cuentan con librerías y conjuntos de instrucciones que permiten el desarrollo de éste tipo de aplicaciones sin que el programador tenga que preocuparse más que en elegir y adecuar el tipo de información de gestión que necesite y la manera en que ésta es visualizada.

El concepto de gestor también tiene que ver con el hardware presente en el dispositivo o dispositivos que van a ser utilizados para llevar a cabo ésta función de gestión; es así, que la elección y dimensionamiento de las características y recursos con que deberán contar éste tipo de dispositivos puede llegar a ser crítica.

Fundamentalmente, el tamaño de la red, el número y tipo de agentes a monitorear y gestionar, determinaran las capacidades en cuanto a procesamiento, memoria física, almacenamiento, interfaz de red, etc., con que los gestores deberán contar para realizar la monitorización y gestión de forma adecuada, teniendo siempre en cuenta un margen de contingencia en relación del inevitable crecimiento que tendrá la red de computadoras.

Los dispositivos en donde funcionan los gestores, también disponen de un agente, el mismo que les permite capturar y almacenar información de los objetos gestionados de éstos dispositivos brindándoles también la capacidad de ser monitoreados y gestionados por el gestor en ellos mismos o por el gestor en otro dispositivo; en otras palabras, el gestor y el agente pueden coexistir en el mismo dispositivo; tal como se indica en la Figura 1.9, lo que a su vez permite que múltiples tipos de gestores (pertenecientes a diferentes empresas desarrolladoras)trabajen simultáneamente sin interferirse entre sí en la labor de gestionar la red, con el propósito de obtener diferentes beneficios en cuanto a la manera en que se visualizan los datos más no en la forma en que funciona el modelo de gestión de Internet basado en SNMP.

El dispositivo donde se halla el gestor funciona lógicamente tal cual se observa en la Figura 1.9, colocándose éste en la parte superior, sobre el agente y las demás aplicaciones del sistema, éstas a su vez por encima de los programas que permiten la comunicación entre éste y otros dispositivos, por debajo de todo se halla el sistema operativo, el mismo que principalmente controlara el uso del hardware por parte de los niveles lógicos superiores y el modo en que éstos niveles se comunican.

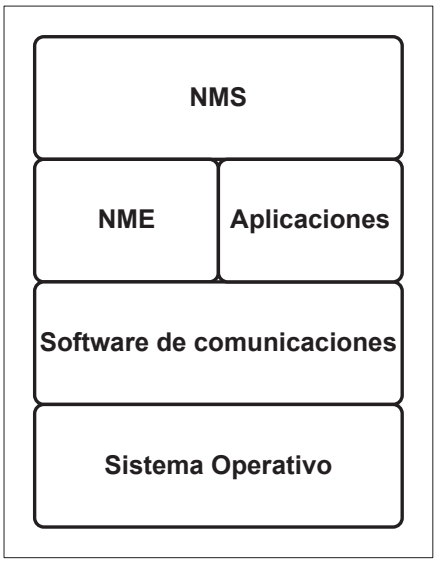


Figura 1.9. Funcionamiento lógico del dispositivo Gestor.

De acuerdo al modelo de gestión de Internet, el gestor utiliza el puerto número 163 UDP de la capa transporte del modelo referencial TCP/IP, para la recepción de notificaciones provenientes desde el agente y cualquier puerto entre 49.152 y 65.535 para él envió de solicitudes a los agentes, que corresponden a puertos no definidos. Para el caso de las solicitudes hacia el agente, el gestor específico en el destino es el puerto 162 UDP.

1.5.2 NME Y EL MODELO DE GESTIÓN DE INTERNET

El NME o agente dentro del modelo de gestión de Internet, es considerado todo dispositivo propio de una red de computadoras; llámese éste, computador personal, estación de trabajo, servidor, conmutador, enrutador, punto de acceso, puente, puerta de acceso, etc., que pueda ser gestionado por el gestor o gestores de acuerdo a lo dispuesto por SNMP.

Principalmente, el agente se encarga de responder las solicitudes realizadas por el gestor y a enviar notificaciones en base a hechos urgentes acontecidos en el agente, tal cual se explicó en la comunicación entre el NMS y el NME, pero siguiendo los parámetros estipulados por SNMP.

El agente puede estar instalado y activado por defecto en los dispositivos gestionados, sin embargo en ciertas ocasiones éste puede ser instalado o activado de forma manual, siendo ese el caso de los computadores o estaciones de trabajo con el sistema operativo Windows, en donde es necesario instalar y activar el servicio de gestión de Windows con el propósito de tener funcionando un agente de gestión; cosa que es muy diferente en los dispositivos con sistema operativo UNIX (y todos sus derivados), donde el agente viene instalado y activado por defecto. En los equipos de conectividad propios de las redes de computadoras; como conmutadores, enrutadores, puntos de acceso, puentes, etc., se suele contar con el agente instalado y funcionando de fábrica dependiendo de la marca fabricante.

El funcionamiento normal del agente en los dispositivos gestionados no exige la contemplación de alguna capacidad o recurso de hardware adicional al inicial, ya que el agente solo se encarga de generar notificaciones y almacenar información en las MIBs que luego será usada para responder a las solicitudes del gestor de manera regular, lo que conlleva requerir pequeñas cantidades de recursos de procesador, memoria física, almacenamiento, etc., lo que es distinto en el gestor que maneja diferente información de gestión proveniente de múltiples agentes de forma continua, requiriendo gran capacidad de recursos de hardware.

Los dispositivos de una red de computadoras dentro del modelo de gestión de Internet que realizan la labor de agentes, funcionan lógicamente de acuerdo a lo indicado en la Figura 1.10, sin importar del tipo de dispositivo que hace de agente; es decir, que tanto en el enrutador como en el servidor y el computador cuentan con los mismos niveles lógicos; inclusive, llegan a tener casi todos los niveles del dispositivo gestor exceptuando obviamente el nivel NMS.

Por lo general, en los dispositivos gestionados se dispone de un solo agente, pero es posible tener varios agentes funcionando de manera simultánea en el mismo dispositivo, logrando extender de ésta manera las MIBs que pueden ser utilizadas y que van más allá de las establecidas por el modelo de gestión de Internet. Para

lograr que dos o más agentes trabajen adecuadamente en un solo dispositivo gestionado, uno de los agentes debe convertirse en el agente principal y los demás deberán estar subordinados a éste agente que de alguna manera se le puede llamar agente primario y los demás agentes secundarios.

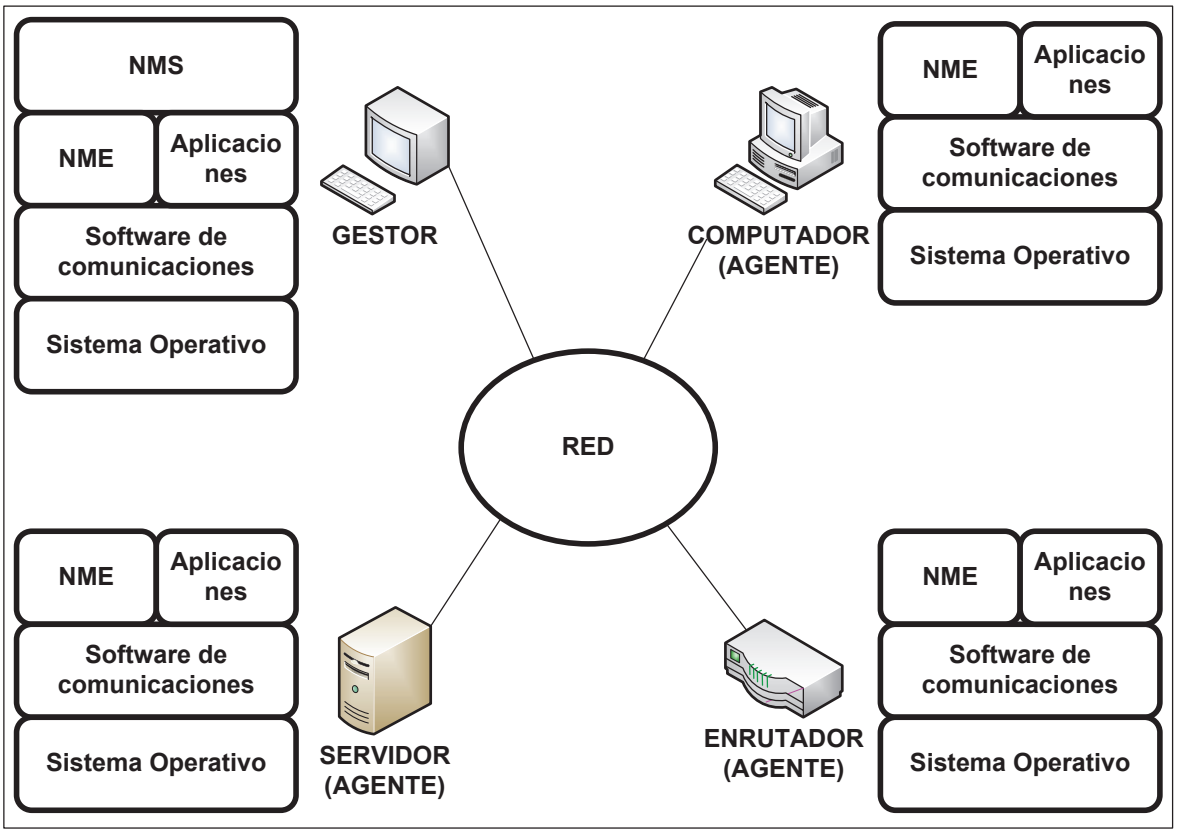


Figura 1.10. Funcionamiento Lógico del dispositivo Agente y Gestor en la red de datos.

El agente hace uso del puerto 162 UDP de la capa transporte del modelo referencial TCP/IP para recibir las solicitudes provenientes desde el gestor, para luego enviar las respuestas a través de cualquier puerto entre 49.152 y 65.535 hacia el gestor. Al enviar las notificaciones al gestor, el agente específica el puerto 163 UDP como destino.

1.5.3 MIB DENTRO DEL MODELO DE GESTIÓN DE INTERNET

En el modelo de gestión de Internet, las MIBs son las bases de datos donde se almacenan la información referente a cada uno de las características y objetos gestionados de los dispositivos monitoreados en donde residen los agentes, los mismos que hacen uso de éstas MIBs para realizar la labor de monitoreo y gestión a través del protocolo SNMP, que es controlado desde el gestor.

La estructura y forma que tienen las MIBs, se encuentra especificada de acuerdo a lo estipulado por la Estructura de Información de Gestión o SMI (Structure Management Information), la misma que ha organizado a las MIBs de acuerdo a una estructura jerárquica semejante a un árbol, Figura 1.11, ubicándolas específicamente en lo que podría considerarse las hojas o terminales del mismo. A ésta estructura tipo árbol se la conoce como árbol de objetos SMI, y permite al Agente disponer de un medio de localización ordenada y univoca de las MIBs por medio de las OID (Object Identifier) o Identificador de Objeto propio de cada objeto dentro del árbol.

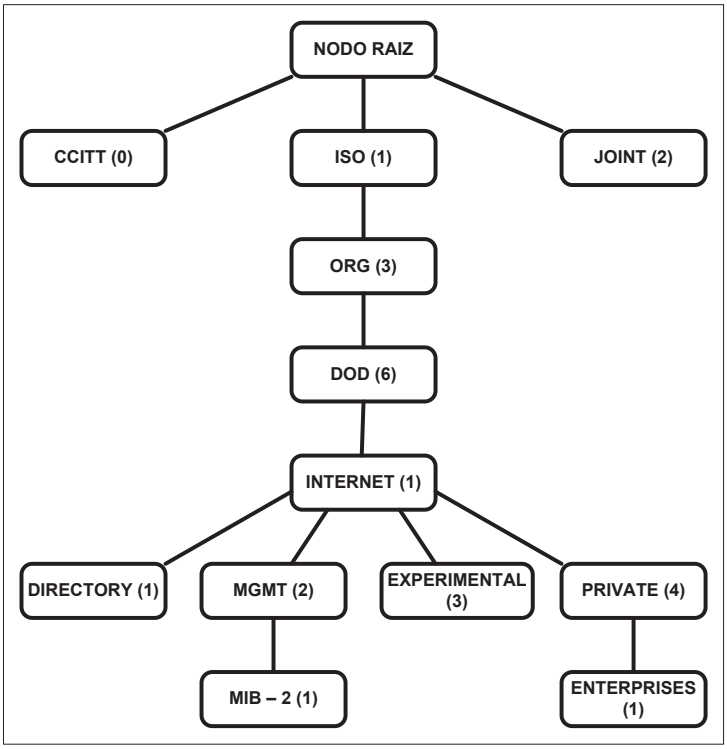


Figura 1.11. Árbol de Objetos SMI.

En la Figura 1.12, se muestra en detalle el contenido del nodo llamado Internet, donde están especificados la gran parte de los elementos funcionales del modelo referencial TCP/IP que requieren ser monitoreados y gestionados por medio del protocolo SNMP, asegurando de ésta forma el correcto funcionamiento de éste tipo de redes.

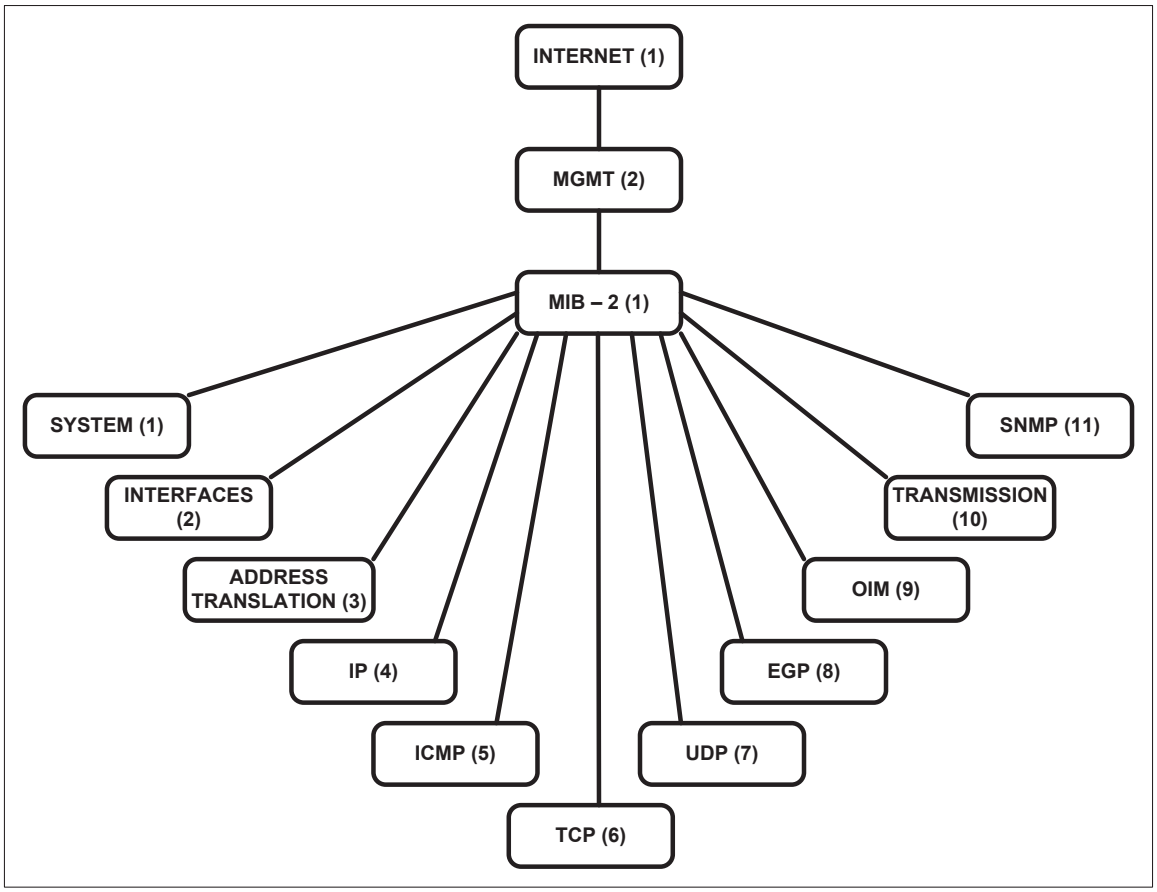


Figura 1.12. Detalle del nodo Internet dentro del Árbol de Objetos SMI.

Dentro del árbol de objetos SMI, los nodos pueden ser divididos de dos maneras; como grupo MIB u objeto MIB, siendo los primeros, nodos que contienen varias MIBs que pueden estar a su vez dentro de otros nodos. Por el contrario, los objetos MIB solo contienen información referente a solo una característica u objeto gestionado del dispositivo donde está el agente. Por ejemplo, en la Figura 1.13, se detalla el contenido del nodo System, en donde cada uno de los nodos dentro de éste,

SysDescription, SysName, SysLocation, etc., son de tipo objeto MIB, ya que contienen información específica del dispositivo como: descripción de hardware y software, nombre, localización, etc., de éste dispositivo. A su vez, los nodos MIB-2 y System como tal son de tipo grupo MIB por el hecho de contener otros nodos o MIBs.

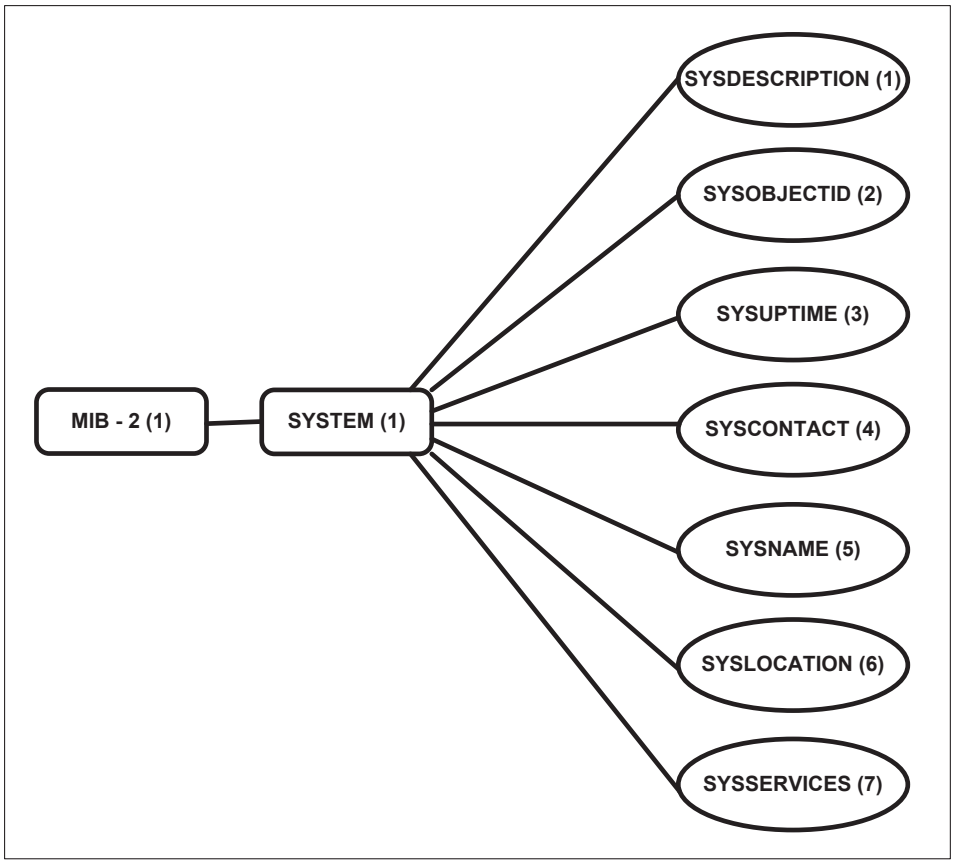


Figura 1.13. Objetos MIB del Grupo MIB System.

La información almacenada dentro de cada MIB puede ser representada de dos formas, como información única del dispositivo a la cual se accede directamente al consultar la MIB o como información contenida en una tabla y que permite la consulta de dos o más elementos afines del dispositivo compartiendo la misma MIB o característica. Es así, que las MIB dentro del nodo System (sysDescription, sysName, sysLocation, etc.) contienen información de un solo aspecto del sistema (descripción, nombre, ubicación, etc.); por el contrario, las MIB contenidas en el nodo Interfaces (ifType, ifSpeed, ifPhysAddress, etc.); Figura 1.14 y 1.15, almacenan

información representada en tablas, donde todas las interfaces de red del dispositivo presentan su respectiva información (tipo, velocidad nominal, dirección física, etc.) que es accedida a través de la misma MIB.

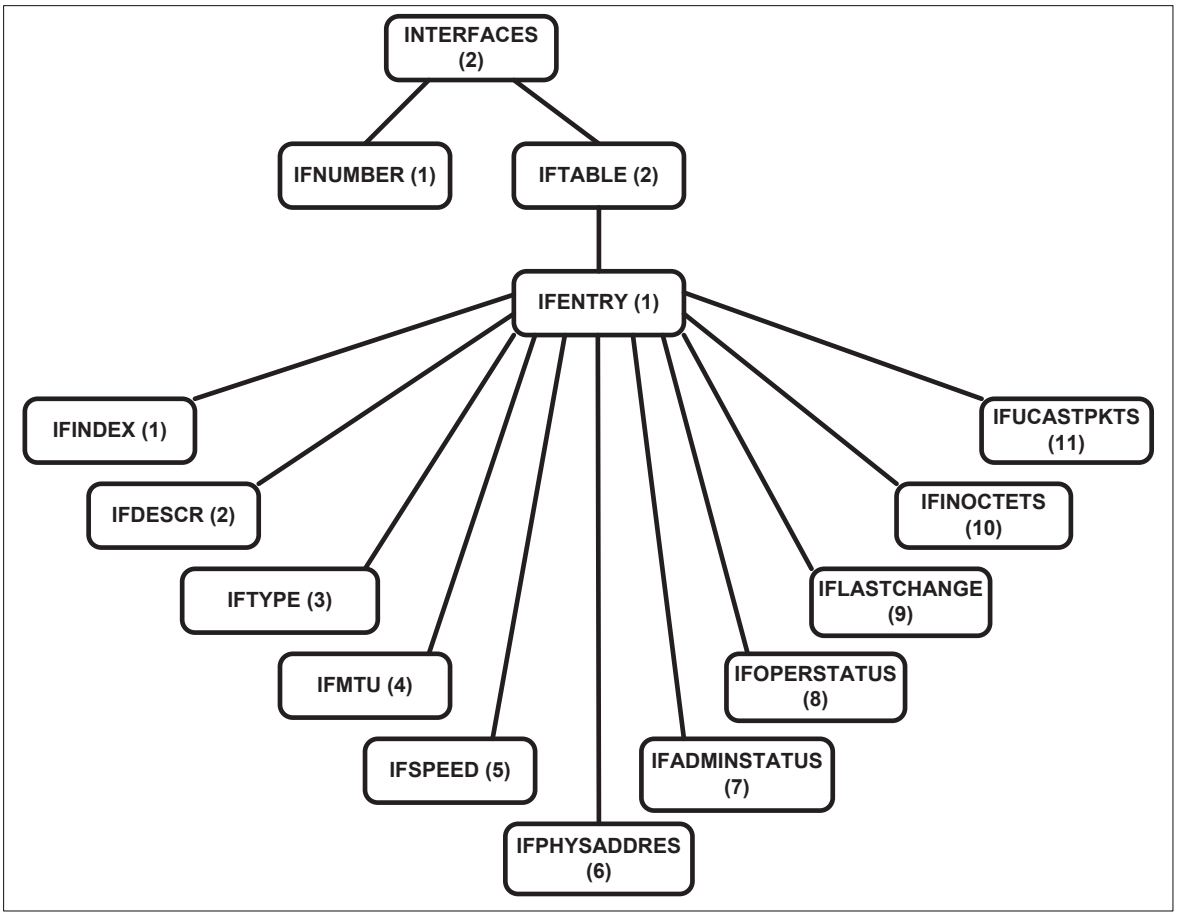


Figura 1.14. Objetos MIB dentro del Grupo MIB Interfaces.

1.5.3.1 OID (Identificador de Objeto)

El identificador de objeto, no es más que la identificación numérica que cada uno de los objetos dentro del árbol de objetos SMI; sean éstos grupos MIB, objetos MIB o elementos de tablas MIB, tienen con el fin de ser localizados de manera sencilla y rápida por los dispositivos involucrados en el modelo de gestión de Internet.

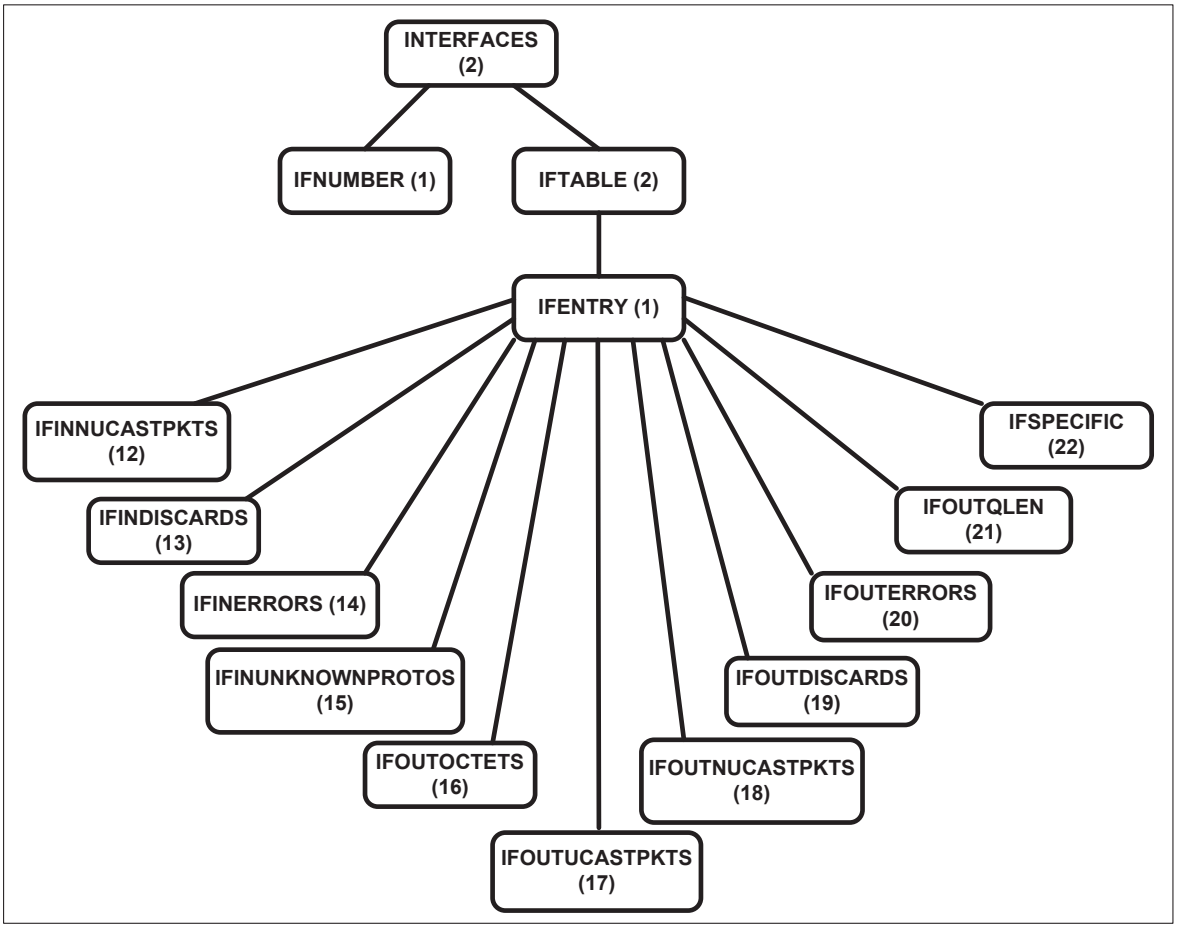


Figura 1.15. Objetos MIB dentro del Grupo MIB Interfaces (continuación).

El formato de las OID está compuesto por números separados por puntos, donde los números representan la ubicación de los objetos en el mismo nivel y los puntos dividen cada uno de los niveles del árbol de objetos SMI. De ésta manera, la OID inicia a la izquierda con el número del objeto más cercano al nodo raíz (CCITT, ISO o JOINT), seguido por un punto para señalar el cambio de nivel para a continuación colocar el número del siguiente objeto perteneciente al segundo nivel y así sucesivamente hasta llegar al objeto requerido.

Por ejemplo, se desea conocer la información almacenada en el objeto del árbol de objetos SMI que representa que representa el nombre del dispositivo (MIB

sysName), el gestor deberá especificar la siguiente OID en la solicitud de gestión hacia el agente:

1.3.6.1.2.1.1.5

Correspondientes a los siguientes objetos dentro del árbol de objetos SMI:

Iso.org.dod.internet.mgmt.mib-2.system.sysName

En el caso de consultas a MIBs representadas como tablas (cualquier MIB dentro del nodo Interfaces) se debe especificar además del número de la MIB, el número asignado por el sistema para la interfaz requerida y que es el mismo en todas las MIB de Interfaces (ifMTU, ifOperStatus, ifInErrors. etc).

Suponiendo que a la interfaz inalámbrica del dispositivo se le ha asignado como la interfaz número 3 por el sistema y que se requiere conocer el estado administrativo del mismo, el gestor deberá hacer uso de la siguiente OID en su solicitud:

1.3.6.1.2.1.2.2.1.7.3

Que equivale a lo siguiente:

Iso.org.dod.internet.mgmt.mib-
2.interfaces.ifTable.ifEntry.ifAdminStatus.numero_Interfaz

1.5.3.2 SMI (Estructura de Información de Gestión)

La Estructura de Información de Gestión (SMI), es la encargada de especificar la forma en que los objetos gestionados o MIBs son nombrados y los tipos de datos asociados a éstos. De igual forma, ha establecido la forma en que las MIBs están ordenadas dentro del árbol SMI.

En la actualidad existen dos versiones de SMI, SMIv1 y SMIv2, cuya gran diferencia radica en la versión de SNMP con la que trabajan, siendo SMIv2 creada para satisfacer las demandas de SNMPv2 ya en la definición de cada MIB incluye nuevas características necesarias para el funcionamiento de la versión 2 de SNMP.

SMI estipula que tres aspectos deben ser considerados para la definición de MIBs:

- Nombre.
- Tipo y Sintaxis.
- Codificación.

1.5.3.2.1 Nombre

Tal como indica, es el nombre que la MIB tiene, pudiendo ser de manera numérica o alfabética (entendible al ser humano), ésta última representación puede conllevar inconvenientes en su implementación al poder llegar a ser de gran tamaño y complejidad, por lo que la representación numérica por medio de OIDs resulta ser más eficiente.

1.5.3.2.2 Tipo y Sintaxis

Tienen que ver con la manera en que los datos de la MIB son representados y transmitidos entre el gestor y el agente, siendo la norma ASN.1[3] la elegida por el modelo de gestión de Internet para la representación de los datos para que ésta sea independiente de la máquina y la arquitectura del sistema computacional.

De acuerdo a ASN.1 las MIBs deben contar con los siguientes campos dentro de su sintaxis para poder ser incorporadas dentro del modelo de gestión de Internet:

- Syntax
- Access
- Status
- Description
- UnitsParts
- Max-Access
- Augments

[3] ASN.1 – Siglas en inglés de Notación Sintáctica Abstracta, que permite representar de datos sin importar el tipo de máquina o ambiente operativo. Fuente: OSI Networking and system aspects – Abstract Syntax Notation 1, ITU-T X.690, 2002.

La Tabla 1.1 detalla el contenido de cada uno de éstos campos.

Tabla 1.1. Elementos del contenido de una MIB según ASN.1.

SYNTAX	Ésta propiedad establece el tipo de dato que la MIB puede manejar, los diferentes tipos de datos que una MIB es capaz de almacenar se encuentran especificados en la Tabla 1.2.
ACCESS	Establece la forma en la que puede ser accedida la MIB, pudiendo ser de solo lectura (read-only), lectura y escritura (read-write), o no acceso (not-accessible).
STATUS	Sugiere la utilización o no utilización de la MIB basado en las normativas del Modelo de Gestión de Internet presente y en sus futuras actualizaciones, de ésta forma el uso de la MIB puede ser mandatorio (Current), opcional (Optional), obsoleta (Obsolete), y no recomendado (Deprecated).
DESCRIPTION	Ofrece una descripción textual del propósito y trabajo de la MIB.
UNITSPARTS	Indica la descripción textual de las unidades utilizadas para la representación de la MIB.

MAX-ACCESS	Campo presente en la especificación de las MIBs que usan SNMPv2 y que brindan más niveles de acceso a éstas a las establecidas por el campo ACCESS, lectura y creación (read-create) y accesible para notificar (accessible-for-notify).
AUGMENTS	Permite la extensión de la tabla de una MIB por medio de la adición de una o más columnas de otro objeto.

1.5.3.2.3 Codificación

Es la forma en que se codifica y decodifica el contenido de la MIB para ser transmitida entre el agente y el gestor con el fin de facilitar el transporte y agilitar el des empaquetamiento de los paquetes que en éste caso serán de gestión de redes TCP/IP. El modelo de gestión de Internet, utiliza para éste efecto las reglas BER (Basic Encoding Rules), la misma que utiliza el método TLV (Codificación Type-Length-Value) para la codificación y decodificación de cadena de octetos presentes en el intercambio de información referente a las MIBs entre el gestor y sus agentes.

Tabla 1.2. Tipos de datos usadas por las MIBs.

INTEGER	Número de 32 bits usado comúnmente para enumerar varios tipos de elementos dentro de un solo objeto gestionado.
OCTET STRING	Cadena de ceros o más octetos útiles para la representación de direcciones físicas.

Counter	Número de 32 bits que tiende a crecer y que es utilizado principalmente en las interfaces para representar el número de octetos recibidos o paquetes perdidos en una interface de red desde el arranque del dispositivo. El valor de tipo Counter es reiniciado cada vez que reinicia el dispositivo.
OBJECT IDENTIFIER	Cadena de números decimales separados por puntos que representan un objeto gestionado.
NULL	Ya no es utilizado por el SNMP.
SEQUENCE	Listas que contienen ceros u otros tipos de datos ASN.1
SEQUENCE OF	Objeto gestionado que es construido en base al tipo de dato SEQUENCE.
IpAddress	Direcciones IPv4 de 32 bits.
NetworkAddress	Igual al anterior pero puede representar diferentes tipos de direcciones de red.
Gauge	Número de 32 bits que puede crecer como decrecer sin superar su máximo. Utilizado para medir la velocidad nominal de una interfaz de red.
TimeTicks	Número de 32 bits capaz de almacenar el tiempo hasta en centésimas de segundo y que es usado para determinar el tiempo de actividad del dispositivo.
Opaque	Permite cualquier otracodificaciónASN.1 ser adaptada dentro de un tipo de dato OCTET STRING.

1.5.4 PROTOCOLO SIMPLE DE GESTIÓN DE RED (SNMP)

SNMP es básicamente un protocolo de capa aplicación dentro del modelo de referencia TCP/IP, el mismo que se encuentra definido en el RFC 1157. Éste protocolo es manejado por todos los dispositivos de red de datos que basan su funcionamiento en la pila de protocolos TCP/IP, es decir todos los dispositivos de red de datos que trabajan en Internet con el fin de que éstos sean monitoreados o gestionados.

Éste protocolo funciona en los puertos UDP 161 y 162, siendo el primer puerto el utilizado por los agentes de la red gestionada para recibir solicitudes de consulta o monitoreo, específicamente, consultas a las MIBs de los agentes. Para el caso del puerto UDP 162, es utilizado en el lado del gestor para recibir las llamadas traps o alarmas notificando que han ocurrido sucesos urgentes en los agentes.

La función principal de SNMP es la encapsulación de datos de control en PDUs con el propósito de definir la manera en que los agentes y el gestor establecen la comunicación, intercambian información y finalizan la comunicación; todo ésto, según sea el requerimiento de gestión.

En la actualidad, el protocolo SNMP dispone de 3 versiones, que son:

- SNMP Versión 1
- SNMP Versión 2c
- SNMP Versión 3

Cada una de éstas versiones fue introducida con el fin de mejorar características y funcionamiento de las versiones anteriores.

1.5.4.1 SNMP Versión 1

La versión inicial con la cual se introdujo el modelo de gestión de Internet para el monitoreo y gestión de redes de datos TCP/IP. Incluye seguridad muy básica a

través de un nombre de comunidad que es una cadena de caracteres en texto claro que hace de contraseña entre el gestor y los agentes.

1.5.4.1.1 PDUs de SNMP Versión 1

SNMP maneja básicamente 5 tipos de PDU, los mismos que se menciona a continuación:

- GetRequest
- GetNextRequest
- GetResponse
- SetRequest
- Trap Versión 1

1.5.4.2 SNMP Versión 2C

SNMP versión 2c es la versión revisada de de SNMP versión 1 incorporando mejoras en de desempeño, comunicación entre gestores y nuevas PDU. SNMP versión 2c es una versión de facto ya que los fabricantes de equipos de conectividad la utilizaron en lugar de la versión 2 al considerar que ésta última tenía un sistema de seguridad demasiado complejo, decidiendo entonces reutilizar el sistema de seguridad de la versión 1, el cual adolecía de graves falencias.

El funcionamiento de ésta versión de SNMP está detallada desde RFC 1901 al RFC 1908.

1.5.4.2.1 PDUs de SNMP Versión 2C

SNMP Versión 2c además de incorporar las PDU de la versión 1 añade 3 nuevas PDU, las mismas que se detallan a continuación.

- GetBulkRequest
- InformRequest
- Trap Version 2

1.5.4.3 SNMP Versión 3

Ésta nueva versión del protocolo SNMP está basada en la versión anterior a éste, con la gran diferencia que incorpora mejoras en cuanto a seguridad se refiere, añadiendo sistemas criptográficos para la protección, tanto de las entidades SNMP (agentes y gestores), como de los paquetes SNMP intercambiados entre éstos. El protocolo SNMP versión 3 es capaz de cubrir los siguientes aspectos de seguridad:

- **Integridad de mensajes**: Se asegura que el contenido de los mensajes SNMP no sea alterado.
- **Enmascaramiento:** Previene que entidades no autorizadas asuman la identidad de entidades si autorizadas, para la realización de operaciones de administración no designadas a ésta.
- **Integridad de flujo de mensajes:** Se asegura que el flujo y orden de los mensajes SNMP sea el correcto y no sea modificado por entidades no autorizadas.
- **Divulgación:** Se protegen los mensajes SNMP contra entidades Sniffer o analizadores de paquetes maliciosos.

El modelo de seguridad usado por SNMP versión 3es el modelo USM (User-Based Security Model), el mismo que define el nivel de seguridad implementado por las entidades durante el proceso de administración SNMP, y que sigue el esquema indicado en la tabla 1.3.

El protocolo SNMP Versión 3 modifica el formato de los mensajes SNMP 2c, con el propósito de dar soporte a las nuevas características de seguridad, Figura 1.16.

El funcionamiento detallado de SNMP Versión 3 se encuentra definido en el RFC 3408 – RFC 3411.

Tabla 1.3. Niveles de seguridad USM de SNMP versión 3.

Nivel	Autenticación	Encriptación
noAuthNoPriv	Nombre de usuario	No
authNoPriv	MD5 o SHA	No
authPriv	MD5 o SHA	AES o DES

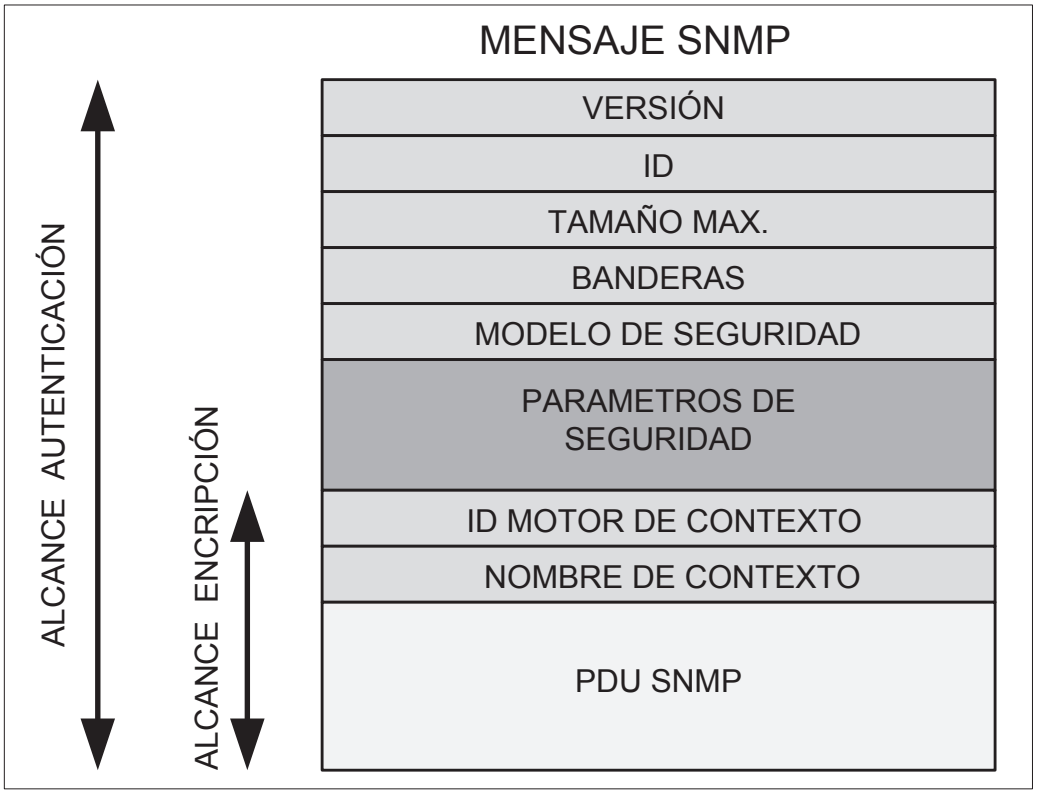


Figura 1.16. Formato del mensaje SNMP Versión 3.

1.5.5 ESTRUCTURA DE LAS ENTIDADES SNMP

Las entidades SNMP, tanto los NME como los NMS SNMP tienen una estructura común, la misma que se encuentra ilustrada en la Figura 1.17. Las entidades SNMP se encuentran constituidas principalmente por un Motor (Engine en inglés) el cual es identificado por un ID llamado SNMPEngineID y por medio del cual las entidades

SNMP conocen que otras entidades pueden realizar operaciones de gestión SNMP sobre ellas.

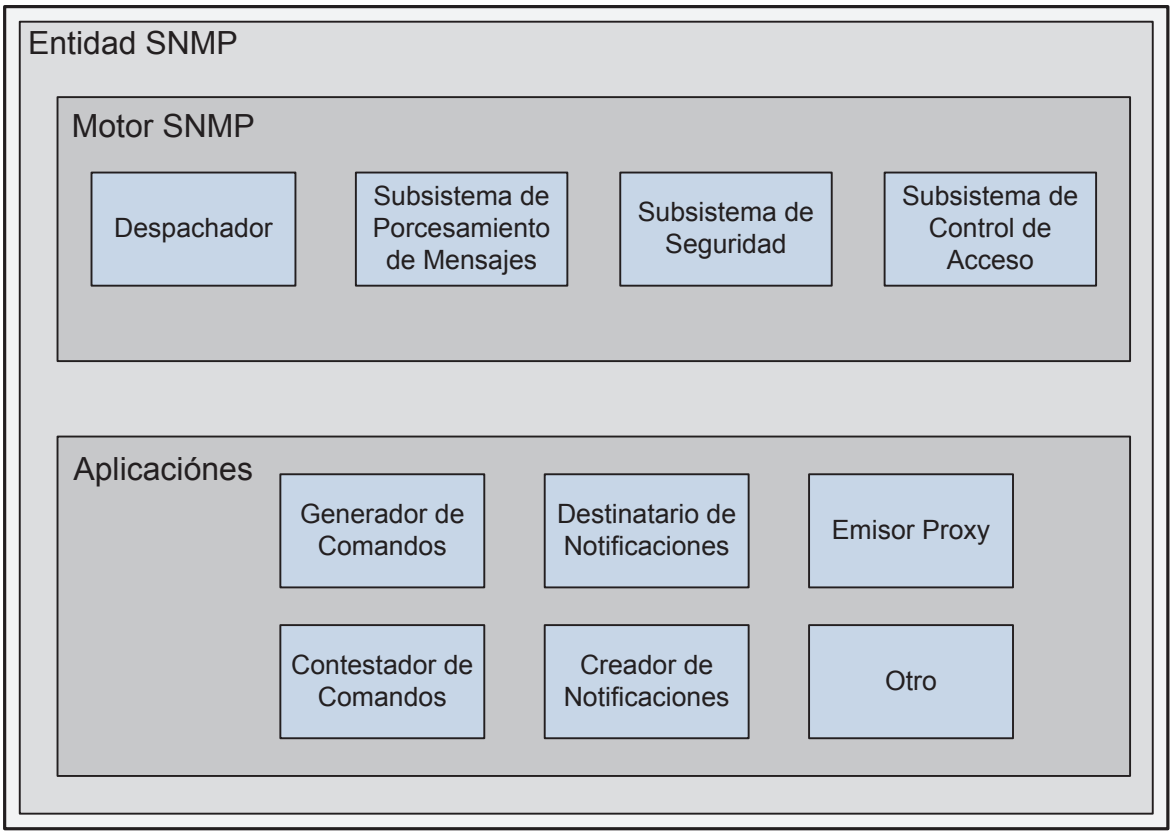


Figura 1.17. Estructura de las entidades SNMP.

- **Despachador.**

El despachador está encargado de coordinar la comunicación entre los diferentes subsistemas de la entidad SNMP y determina a que aplicación una PDU entrante debe ser redirigida.

- **Subsistema de Procesamiento de Mensajes.**

El subsistema de procesamiento de mensajes se encarga de encapsular y desencapsular los mensajes SNMP de las PDUs recibidas, además de que dispondrá de varios sub-módulos de procesamiento de mensajes con el fin de poder a tender a las diferentes versiones de mensajes SNMP (versión 1, 2c y 3).

- **Subsistema de seguridad.**

El subsistema de seguridad está encargado de proveer los mecanismos de autenticación y encriptación de mensajes SNMP.

- **Subsistema de Control de Acceso.**

El subsistema de control de acceso se encarga de autorizar o no el acceso a las MIBs y qué tipo de operaciones SNMP se puede realizar sobre éstas.

- **Generador de Comandos.**

El generador comandos se encarga de generar los diferentes tipos de PDUs SNMP, como por ejemplo *getRequest*, *getNextRequest, setRequest,* etc.

- **Contestador de Comandos.**

El contestador de comandos tiene como función la de recibir, procesar y contestar a las solicitudes hechas por los PDUs enviados por el generador de comandos de otra entidad SNMP.

- **Creador de notificaciones.**

El creador de notificaciones se encarga de generar las llamadas *Traps* o mensajes *InformRequest*.

- **Destinatario de Notificaciones.**

El destinatario de notificaciones tiene la labor de recibir las notificaciones generadas por el creador de notificaciones.

- **Emisor Proxy.**

El emisor proxy es el intermediario del intercambio de mensajes entre entidades SNMP.

1.6 JAVA ENTERPRISE EDITION

Java Enterprise Edition o JEE por sus siglas en inglés, es una plataforma propia del lenguaje de programación Java, desarrollada sobre la plataforma Standar Edition de Java y que tiene como objetivo la creación y ejecución de aplicaciones distribuidas de gran escala, las mismas que tienen la característica de ser escalables, confiables, seguras y multi-nivel.

Ésta plataforma consiste en una Máquina Virtual y una Interface de Desarrollo conocida generalmente como API que provee las ventajas del lenguaje de programación Java, como son: independencia de plataforma, estabilidad, facilidad de desarrollo y seguridad.

La API utilizada por JEE permite a los desarrolladores de programas, crear aplicaciones de manera sencilla, preocupándose únicamente en la funcionalidad de los mismos ya que la API se encargará de todo lo demás aspectos necesarios en el desarrollo de aplicaciones.

1.6.1 APLICACIONES CORPORATIVAS

Las aplicaciones corporativas son llamadas de ésta manera debido a que generalmente son utilizadas por grandes compañías o empresas, caracterizadas por tener gran cantidad de usuarios y recursos, por lo que sus aplicaciones deben ser de gran escala, multi-nivel, escalables, confiables y seguras, lo que las hace muy complejas a la hora de desarrollar, pero gracias a JEE éste trabajo se hace más sencillo.

1.6.1.1 Aplicaciones Multi-nivel

En las aplicaciones multi-nivel se divide la funcionalidad de éstas en varias capas o niveles para que trabajen de manera aislada la una de la otra con el objetivo de mejorar la eficiencia de las mismas. Para JEE existen 4 tipos de niveles, Figura 1.18:

- Nivel de Cliente

- Nivel Web
- Nivel de Negocio
- Nivel del Sistema de Información.

1.6.1.1.1 Nivel de Cliente

El nivel de cliente consiste en aplicaciones de cliente que acceden a servicios ofrecidos en un servidor JEE ubicado en una estación distinta. Una aplicación de cliente puede ser un navegador web, una aplicación de escritorio u otro servidor JEE, desarrollado con Java u otro lenguaje de programación. De manera general, la aplicación cliente realiza solicitudes al servidor JEE, éste procesa las solicitudes para luego responder a la aplicación cliente con la información solicitada.

1.6.1.1.2 Nivel Web

El nivel web está encargado de manejar la interacción entre el nivel de cliente y el nivel de negocio a través de varios componentes o tecnologías como por ejemplo: Servlets, Java Server Pages (JSP), tecnología JavaServer Faces, etc. Principalmente, éste nivel cumple con las siguientes funciones:

- Generar dinámicamente contenido en varios formatos para el cliente.
- Recoger información ingresada por el cliente y devolver resultados apropiados desde los componentes del Nivel de Negocio.
- Controlar el flujo de páginas y pantallas en el cliente.
- Mantener el estado de la información para la sesión de usuarios.
- Mantener información temporal en componentes JavaBean.

1.6.1.1.3 Nivel de Negocio

En éste nivel, se encuentra la lógica de negocio de una aplicación; o dicho de otra manera, es el código de programación que provee funcionalidad a un dominio de negocio en particular. Para una aplicación corporativa apropiadamente diseñada, el núcleo de su funcionalidad reside en éste nivel.

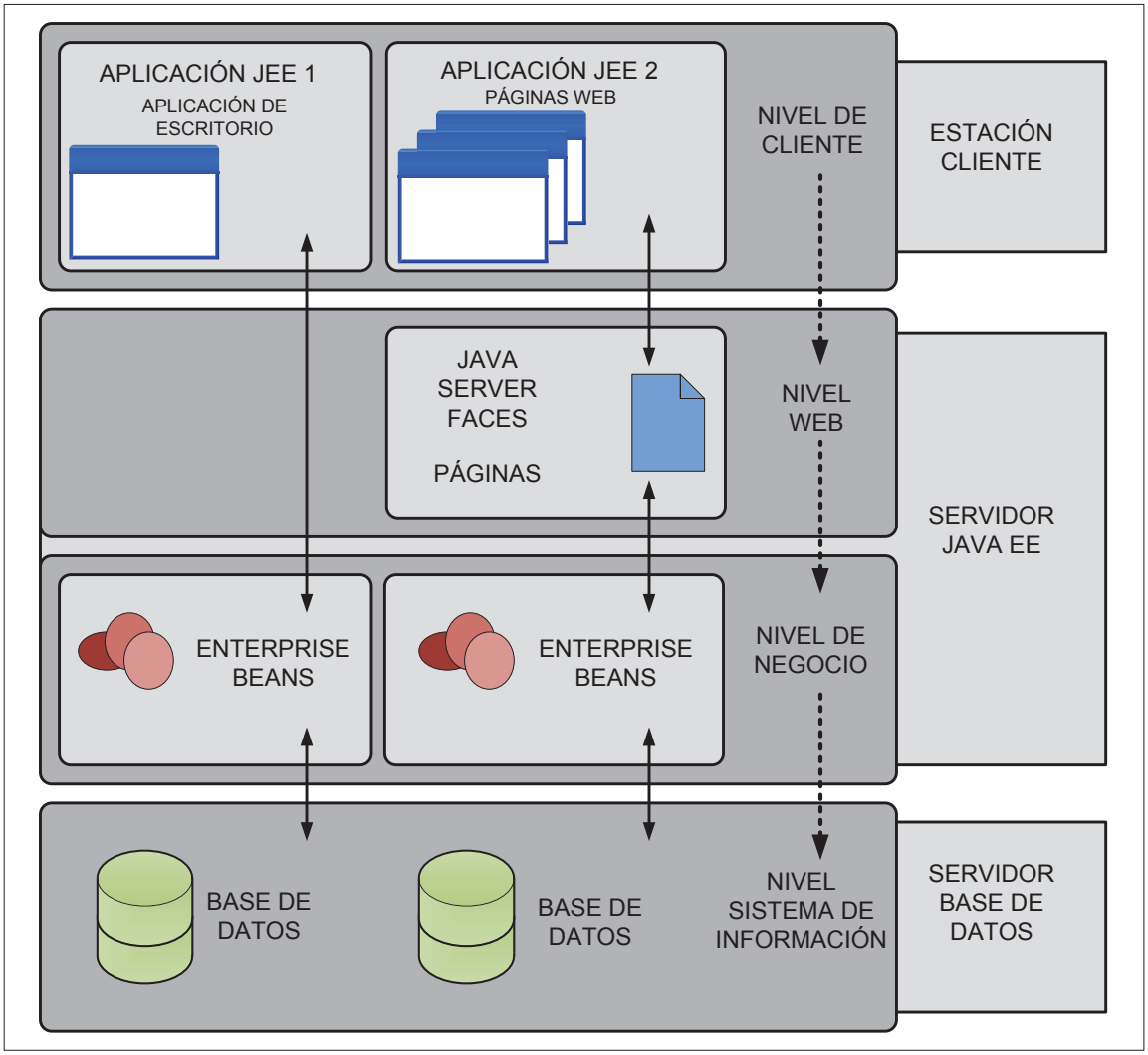


Figura 1.18. Estructura de Aplicaciones Multi-nivel.

Éste nivel cuenta con varias tecnologías en base a los cuales basa su funcionamiento:

- Enterprise JavaBeans (EJB) y Spring.
- Servicio Web JAX-RS.
- Servicio Web JAX-W.
- Entidades del API de Persistencia de Java (JPA).

- **Enterprise JavaBeans y Spring**

Las Enterprise JavaBeans son porciones de código de programación que contienen atributos y métodos para la implementación de módulos del nivel de negocio. Pueden funcionar solos o en conjunto con otros EJB dentro del servidor EE.

Por su parte, Spring constituyen una alternativa a EJB ya que es un framework que integra en código de programación, varias funcionalidades del nivel de negocio de las aplicaciones Java EE, como la persistencia[4] y la integridad transaccional[5] del manejo de objetos relacionales de una base de datos.

- **Servicio Web JAX-RS**

Los servicios web JAX-RS o servicios web RESTful con JAX (Java API paraXML), son aplicaciones web creadas para brindar servicios sobre Internet usando la tecnología REST (Representational State Transfer), la misma que describe el estilo de la arquitectura de las aplicaciones cliente-servidor. El estilo de la arquitectura junto con la información y la funcionalidad, son considerados recursos de la aplicación, los mismos que son intercambiados entre el cliente y el servidor por medio de solicitudes y respuestas, y accedidos por los llamados links web URI (Uniform Resource Identifier).Los recursos de aplicación son representados por archivos o documentos, como por ejemplo documentos XML, páginas HTML, archivo de imágenes, etc.

[4] La persistencia en Java EE consiste en el mapeo entre objetos Java y objetos relacionales de una base de datos. Fuente: https://docs.oracle.com/javaee/7/tutorial/doc/persistence-intro.htm

[5] La integridad transaccional en Java EE permite guardar la integridad de los objetos relacionales de una base de datos por medio del uso de transacciones (una serie de pasos que realizan una tarea) para que su información sea exacta.
Fuente: https://docs.oracle.com/javaee/7/tutorial/doc/transactions.htm

La tecnología REST fue diseñada para utilizar protocolos de comunicación stateless[6], típicamente HTTP por lo que el manejo de los recursos de aplicación se lo hace por medio de las operaciones HTTP: POST, GET, PUT y DELETE.

- **Servicio Web JAX-WS**

El servicio web JAX-WS es una tecnología utilizada para el desarrollo de servicios web y clientes que se comunican a través de protocolo basados en XML, como lo es SOAP (Simple Object Access Protocol), que define la estructura del mensaje, reglas de codificación y convenciones para representar las solicitudes y respuestas del servicio web sobre HTTP.

Los mensajes SOAP están caracterizados por ser muy complejos, pero el API JAX-WS lo simplifica haciendo que el programador solo se preocupe de diseñar las operaciones del servicio web por medio de métodos definidos en una interface Java escrita en el lenguaje de programación Java, para luego crear uno o varios métodos que implementen dichas interfaces Java. Los clientes de servicio web, son igual de fácil de desarrollar ya que la traducción de lenguaje de programación Java a lenguaje SOAP de las solicitudes y respuestas lo realiza por sí solo el API JAX-WS.

Una de las ventajas de los servicios web JAX-WS, es que el servidor o cliente, no es restrictivo con el hecho de que uno de éstos se ejecute en una plataforma distinta a Java. Ésta flexibilidad es posible ya que el API JAX-WS utiliza una tecnología definida por W3C: HTTP, SOAP y WSDL (Web Service Description Language). Lo que hace WSDL es especificar un formato XML para describir un servicio como un conjunto de interfaces operando dentro de sus mensajes.

---

[6]En las comunicaciones stateless, cada solicitud de servicio puede ser entendida independientemente sin necesidad de llevar un seguimiento de ellas. Fuente: Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing RFC 7230, Junio 2014.

- **Entidades del API de Persistencia de Java**

Las entidades como tal, típicamente representan tablas de una base de datos relacional, y cada instancia de la entidad, corresponde a una fila dentro de la tabla. Las entidades están definidas en la plataforma Java a través de clases Java en las cuales se específica mediante anotaciones el mapeo o traducción de las entidades y sus relaciones con otras entidades, a datos que se almacenan en un nivel inferior dentro de los sistemas de almacenamiento como lo son las bases de datos. Dentro de JEE, éste servicio de mapeo se denomina API de persistencia de Java (JPA).

1.6.1.1.4 Nivel del Sistema de Información

El nivel del sistema de información o EIS por sus siglas en inglés, consiste en los servidores de base de datos o cualquier otra fuente de almacenamiento y consulta de datos. Por lo general, éstos recursos se localizan en una estación distinta al servidor Java EE y son accedidos por medio de componentes del nivel de negocio.

Las tecnologías con las que cuenta éste nivel son las siguientes:

- API de Conectividad Java a Base de Datos (JDBC).
- API de Persistencia Java.
- Arquitectura de Conector Java EE.
- API de Transacción Java (JTA).

1.6.2 SERVIDORES JAVA EE

El servidor Java EE es una aplicación que implementa las API de la plataforma Java EE, además de proveer los servicios estándar Java EE. Se puede nombrar algunos ejemplos de servidores Java EE como Glassfish, Oracle Weblogic o JBoss, entre los más comunes.

Los servidores Java EE contienen varios tipos de componentes de aplicación que corresponden a uno o varios niveles dentro de una aplicación multi-nivel. Éstos componentes son presentados en forma de contenedores.

1.6.2.1 Contenedores Java EE

Los contenedores en los servidores Java EE son la interface entre los componentes y la funcionalidad de bajo nivel desplegada por la plataforma para dar soporte a éstos componentes. La funcionalidad de los contenedores está definida por la plataforma y es diferente para cada tipo de componente los mismos que pueden trabajar en conjunto para proveer funcionalidad a una aplicación corporativa.

Existen los siguientes tipos de contenedores dentro de un Servidor Java EE:

- **Contenedor WEB**: Básicamente, éste contenedor sirve como interface entre los componentes web y el servidor web.
- **Contenedor de Aplicación de Cliente**: El contenedor de aplicación de cliente es la interface entre la aplicación de cliente Java EE y el servidor Java EE, además de que se ejecuta únicamente en la estación del cliente.
- **Contenedor EJB (Enterprise Java Bean)**: Éste contenedor funciona como interface entre los Enterprise Beans y el servidor Java EE. El contenedor EJB se ejecuta dentro del servidor Java EE y administra la ejecución de los Enterprise Beans de una aplicación.

1.6.3 SEGURIDAD EN JAVA EE

La seguridad en Java EE es provista por los contenedores, los mismos que proveen dos tipos diferentes de seguridad: declarativa y programática.

1.6.3.1 Seguridad Declarativa

La seguridad declarativa establece los requerimientos de seguridad para los componentes de una aplicación por medio del uso de descriptores de despliegue o anotaciones.

Los descriptores de despliegue son archivos XML externos a la aplicación como tal, que contienen la estructura de seguridad para la aplicación incluyendo: roles, control de acceso y requerimientos de autenticación.

Las anotaciones o también llamadas metadatos, especifican la información de seguridad dentro del código de las clases Java de la aplicación.

1.6.3.2 Seguridad Programativa

Éste tipo de seguridad se encuentra anidada dentro de la aplicación con el propósito de tomar decisiones de seguridad y es útil cuando la seguridad declarativa por sí sola no es suficiente para establecer el modelo de seguridad para una aplicación.

1.6.3.3 Mecanismos de Seguridad de Java EE

El servicio de seguridad de Java EE proporciona mecanismos de seguridad robustos y de fácil configuración para la autenticación y control de acceso de usuarios a las funciones de aplicación e información asociada de acuerdo a varios niveles o capas.

- Seguridad a nivel de capa Aplicación.
- Seguridad a nivel de capa Transporte.
- Seguridad en base a Mensajes.

Java EE al estar desarrollado sobre la plataforma Java SE, incluye también todos los mecanismos de seguridad manejados por ésta última, entre los que destacan:

- **Java Authenticaction and Autorization Service (JASS):** Conjunto de APIs para proveer servicios con control de acceso y autenticación.
- **Java Generic Security Services (Java GSS-API):** Es un API basado en tokens para el intercambio seguro de mensajes entre aplicaciones.
- **Java Cryptography Extension (JCE):** Proporciona la plataforma para el uso de algoritmos de encriptación y generación de llaves.
- **Java Secure Sockets Extension (JSSE):** Provee la plataforma para la implementación de SSL y TLS.
- **Simple Authentication and Security LAYER (SASL):** Es un estándar de Internet que específica un protocolo para la autenticación y establecimiento óptimo de una capa segura entre aplicaciones servidor y cliente.

1.6.3.3.1 Seguridad a Nivel de Capa Aplicación

Los contenedores de componentes de Java EE son los responsables de ofrecer seguridad en ésta capa, acomodando perfectamente el tipo de seguridad a las necesidades de la aplicación. De igual manera, permiten la configuración e implementación de controles de acceso a usuarios de las funciones e información de las aplicaciones de una manera parcial (fine-grained access control).

1.6.3.3.2 Seguridad a Nivel de Capa Transporte

La seguridad a nivel de capa transporte es confiada en las manos de SSL, que es usado para proveer a las comunicaciones extremo – extremo entre el servidor y el cliente, de autenticación, integridad y confidencialidad de mensajes. Ésta seguridad está únicamente presente desde que el mensaje sale del cliente hasta que arriba al servidor, y viceversa.

De manera general, el cliente y el servidor utilizan como mecanismos de seguridad la encriptación a través de llave pública y de autenticación basada en certificados digitales.

1.6.3.3.3 Seguridad en Base a Mensajes

En la seguridad en base a mensajes, la información de seguridad está almacenada dentro los mensajes SOAP y/o sus adjuntos, permitiendo que la información de seguridad viaje en conjunto con el mensaje lo que permite que diferentes porciones del mensaje utilicen diferentes tipos de encriptación o autenticación. A través de la seguridad de capa mensaje se puede tener intermediarios entre el remitente y el destinatario. Es completamente independiente del protocolo de capa transporte.

1.7 EL MODELO REFERENCIAL SAFE

El modelo referencial SAFE fue creado por el fabricante de dispositivos de conectividad de red CISCO, con el fin de establecer una guía para el diseño, implementación y administración de redes de datos seguras. La seguridad es el

aspecto más importante para el modelo SAFE por el hecho de ser el punto más crítico al determinar si una red de datos funciona adecuadamente o no.

SAFE se encarga primordialmente de determinar las vulnerabilidades de una red de datos frente a ataques que conlleven que la misma funcione erráticamente o simplemente deje de funcionar. De igual manera, se ha encargado de agrupar todos los recursos de red de una empresa o corporación, en una serie de módulos que según su importancia, determinen los mecanismos para prevenir, monitorear y responder ante la presencia de ataques que interfieran con el funcionamiento normal de la red.

El modelo de referencia SAFE, permitirá en el análisis de los recursos de hardware y software disponibles en la SUPERTEL para el desarrollo de la solución computacional presentada en el presente proyecto, el mismo que se describe en el capítulo 2 correspondiente al análisis del proyecto.

CAPÍTULO II: ANÁLISIS

En éste capítulo, se realiza un análisis de la situación actual de los recursos de hardware y software de red con que dispone la Superintendencia de Telecomunicaciones, el análisis legal del servicio de Internet, diseño de el cuestionario para la consulta de los requerimientos de la nueva aplicación a los usuarios finales de ésta, análisis del resultado del cuestionario de requerimientos y los casos de uso que tendrá la nueva aplicación.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

Los recursos de hardware y software de red con que dispone la Superintendencia de Telecomunicaciones serán analizados en base al modelo referencial de redes de 7 capas OSI. Con el fin de simplificar éste análisis se han sintetizado las 7 capas en 3 grandes capas: capa de red física (capa física y enlace), capa de red lógica (capas red y transporte) y capa aplicación (capas sesión, presentación y aplicación). Para la capa de red física se realiza además, un análisis de a través del modelo referencial SAFE con el fin de conocer que buenas prácticas de seguridad son utilizadas en éste nivel.

2.1.1 ANÁLISIS DE LA CAPA DE RED FÍSICA

La capa de red física de datos de la Superintendencia de Telecomunicaciones tiene una topología tipo estrella, donde los dispositivos de red se encuentran distribuidos de una forma similar a los módulos del modelo SAFE, Figura 2.1. Los equipos de conectividad están divididos en dos niveles; core y acceso, sin contar con el nivel de distribución, lo cual limita a ésta red en términos de escalabilidad y rendimiento.

El modo de acceso al medio de las estaciones de trabajo y equipos de conectividad está descrito por el estándar IEEE 802.3ab o conocido también como Ethernet 1000 Base-T, proveyendo a la red de datos, escalabilidad y velocidad de transmisión de hasta 1 Gbps.

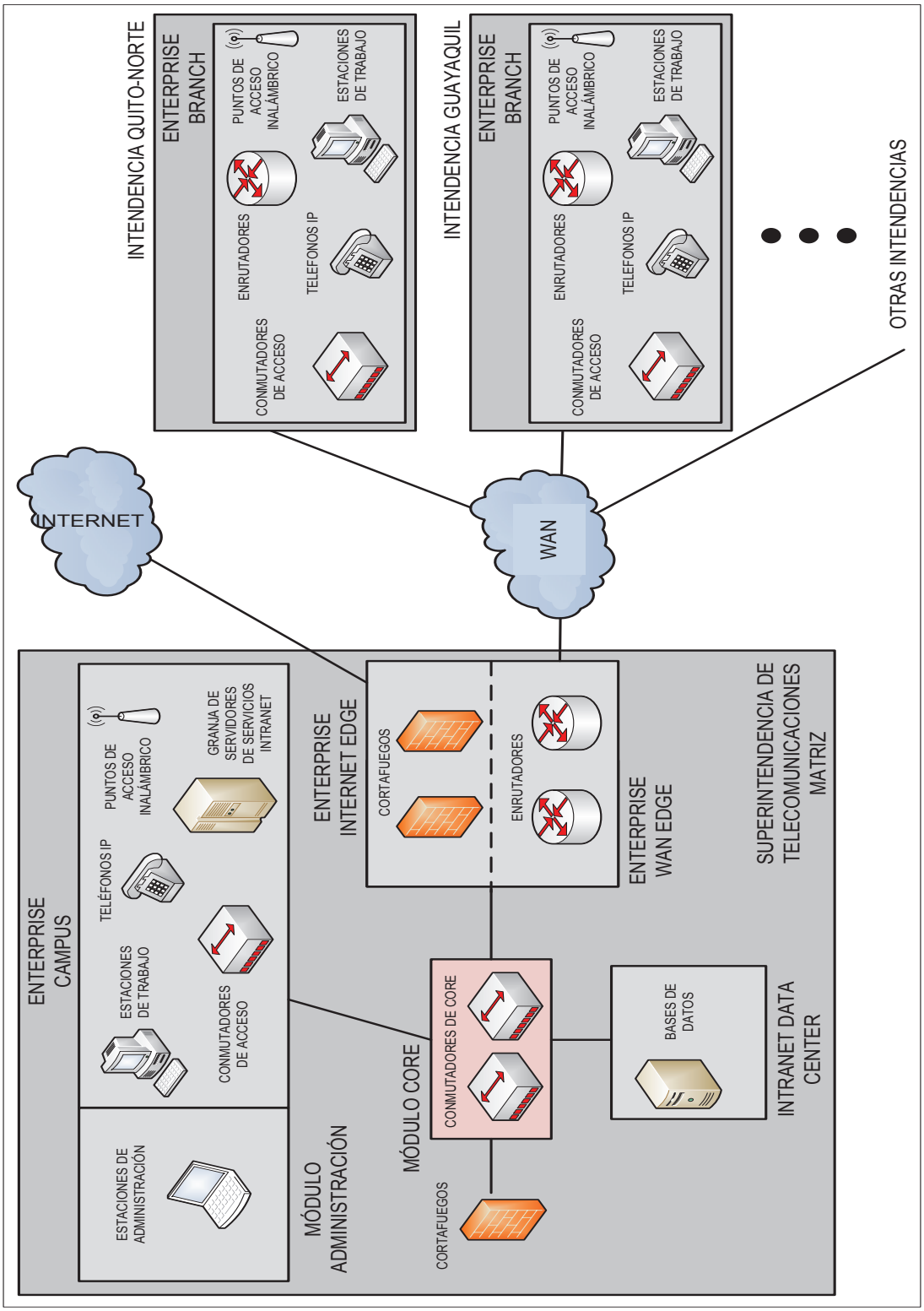


Figura 2.1. Topología de la red física de la Superintendencia de Telecomunicaciones distribuida por módulos del modelo referencial SAFE.

En la tabla 2.1 se resumen los recursos de hardware con los que cuenta la SUPERTEL de acuerdo al modelo referencial SAFE y que se encuentran disponibles para ser utilizados por la solución computacional descrita en éste documento.

Tabla 2.1. Recursos de Hardware de la SUPERTEL.

Módulo SAFE	Equipos	Cantidad	Estándares y Protocolos
Enterprise Core	Conmutadores Cisco 4500	3	IEEE 802.3ab, IEEE 802.3i, IEEE 802.3u, HSRP, EAP, RADIUS, TACACS+, STP, etc.
	Cortafuegos Cisco ASA 5520	2	
	Servidor ACS (Access Control System)	1	
	Controlador WLC (Wireless LAN Controller)	1	
	Controlador NAC (Network Admission Control)	1	
	Cisco Prime	1	
Intranet Data Center	Servidores IBM Power 750	1	IEEE 802.3ab, IEEE 802.3i, IEEE 802.3u, etc.

Módulo SAFE	Equipos	Cantidad	Estándares y Protocolos
Enterprise Campus	Conmutadores de acceso Cisco 3560	varios	IEEE 802.3ab, IEEE 802.3i, IEEE 802.3u, IEEE 802.3q, IEEE 802.11g/n STP, ARP, ACL, etc.
	Estaciones de trabajo	varias	
	Puntos de acceso inalámbrico	varios	
	Teléfonos IP	varios	
	Impresoras	varias	
Enterprise Internet Edge	Cortafuegos Cisco ASA 5520	2	IEEE 802.3ab, IEEE 802.3i, IEEE 802.3u, IEEE 802.3q, STP, ARP, ACL, IPSec, TLS, etc.
	Enrutadores Cisco 3845	2	
	Conmutador de acceso Cisco 3560	1	
Enterprise WAN Edge	Enrutadores Cisco 3845	2	MPLS (RFC-3031), VPN, TLS, etc.

Módulo SAFE	Equipos	Cantidad	Estándares y Protocolos
Enterprise Branch	Enrutadores Cisco 3845	1	IEEE 802.3ab, IEEE 802.3i, IEEE 802.3u, IEEE 802.3q, IEEE 802.11g/n STP, ARP, ACL, MPLS (RFC-3031), IPSec, TLS, etc.
	Conmutadores de acceso Cisco 3560	varios	
	Estaciones de trabajo	varias	
	Puntos de acceso inalámbrico	varios	
	Teléfonos IP	varios	
	Impresoras	varias	
Administración	Conmutador de acceso Cisco 3560	1	IEEE 802.3ab, IEEE 802.3i, IEEE 802.3u, IEEE 802.3q, STP, ARP, ACL, SSH, etc.
	Estaciones de trabajo	varias	

Fuente: Basado de: Ing. Carlos Garzón Alvarado, Departamento de Tecnologías de Información, Superintendencia de Telecomunicaciones, julio 2013.

2.1.2 ANÁLISIS DE LA CAPA DE RED LÓGICA

En la Superintendencia de Telecomunicaciones la topología de la red lógica es de tipo estrella y su funcionamiento lógico se basa en los siguientes aspectos:

- Direccionamiento.
- Enrutamiento.
- Forwarding (Re-envío).

2.1.2.1 Direccionamiento

La red de datos de la SUPERTEL utiliza para la asignación de direcciones IP el protocolo IP versión 4 mediante la técnica de mascara de sub red de longitud variable (VLSM), para optimizar el uso de direcciones IP, y segmentar los dominios de difusión en varias subredes, proveyendo mayor eficiencia y seguridad a la red.

Las subredes se encuentran divididas en base a la dirección IP privada sin clase 172.20.1.0, y básicamente son las siguientes:

- Interfaces WAN en enrutadores.
- Servidores.
- Impresoras.
- Telefonía IP.
- Datos (subdivididas de acuerdo al departamento).

Es importante mencionar, que los servidores manejan una única subred para todos los servicios, lo que puede resultar en un problema de seguridad, ya que si un servicio es interrumpido, también lo serán los demás servicios.

La asignación de dirección IP a los usuarios finales se lo realiza por medio del protocolo DHCP de forma estática, permitiendo el acceso lógico a la red únicamente a los dispositivos registrados.

2.1.2.2 Enrutamiento

El enrutamiento entre subredes remotas, se realiza por medio de rutas estáticas establecidas en los enrutadores ubicados en el módulo Enterprise WAN Edge y modulo Enterprise Branch. Se utiliza enrutamiento estático ya que existe una única ruta (enlaces WAN) entre las diferentes subredes remotas, lo que no justifica el uso de protocolos de enrutamiento IGP como RIP o EIGRP.

Para el caso del enrutamiento entre subredes locales, los conmutadores de core de capa 3 se encargan de conectar diferentes subredes. Ya que las subredes se encuentran directamente conectadas al conmutador, éste conoce los caminos necesarios para llegar a cada una de éstas por lo que no requiere de protocolos de enrutamiento. A pesar de que éste sistema de enrutamiento local es aceptable, sería mucho más eficiente si se utilizan para ésta función, enrutadores independientes en lugar de conmutadores de core de capa 3.

2.1.2.3 Forwarding

El forwarding está relacionado con los protocolos utilizados para el transporte de la información entre los nodos o usuarios finales dentro de la red de datos. Para éste caso, la red de datos de la Superintendencia de Telecomunicaciones hace uso de los protocolos: IP, TCP, UDP, ARP e ICMP, los mismos que ofrecen los siguientes servicios:

- Empaquetamiento y desempaquetamiento de datos.
- Direccionamiento lógico de paquetes.
- Multiplexación de datos.
- Segmentación de datos.
- Establecimiento de comunicaciones confiables y no confiables.
- Clasificación de servicio (CoS).
- Direccionamiento por aplicaciones.

2.1.3 ANÁLISIS DE LA CAPA APLICACIÓN

En ésta capa se encuentran las aplicaciones y servicios de la Intranet de la Superintendencia de Telecomunicaciones, entre las que destacan las siguientes:

- Servicio DHCP.
- Servicio DNS.
- Servicio HTTP.
- Servicio NTP.
- Servicio FTPS.

- Servicio Active Directory.
- Servicio de correo electrónico (SMTP y POP3).
- VMWare.
- Servicio corporativo Java EE (Weblogic 12c).

Para el presente proyecto son de interés únicamente los servicios HTTP, correo electrónico y el servicio corporativo Java EE (Servicios Web), al ser las aplicaciones que más recursos de hardware y de red consumen y que pueden incidir en el desarrollo de la nueva aplicación.

2.1.3.1 Análisis de Flujo de Datos de la Capa Aplicación

El flujo de datos a través de la red para la aplicación HTTP se encuentra ilustrada en la Figura 2.2, donde los datos de solicitud del servicio primeramente cruzan por los conmutadores de acceso, ascendiendo luego a los conmutadores de core donde posteriormente son enviados al cortafuegos para luego volver a los conmutadores de core y finalmente enrutados al servidor HTTP que se encuentra directamente conectado a éstos. Los datos de respuesta del servicio HTTP siguen la misma ruta física de las solicitudes pero en sentido contrario.

Para el caso de la aplicación de correo electrónico, la ruta física que los datos de la aplicación utilizan a lo largo de la red entre los clientes y el servidor, es la misma a la descrita para el servicio HTTP, tal como se muestra en la Figura 2.3, con la diferencia de que en un sentido es el envió de correo electrónico con el protocolo SMTP, y en el otro sentido es la recuperación de correo electrónico con el protocolo POP3.

Para los casos de las Figuras 2.2 y 2.3, se observa que la información atraviesa los conmutadores de core dos veces antes de llegar a sus destino, ya que los cortafuegos se ubican detrás de los conmutadores de core, lo que sin dudas merma el rendimiento y seguridad de la red para atender a éstos servicios.

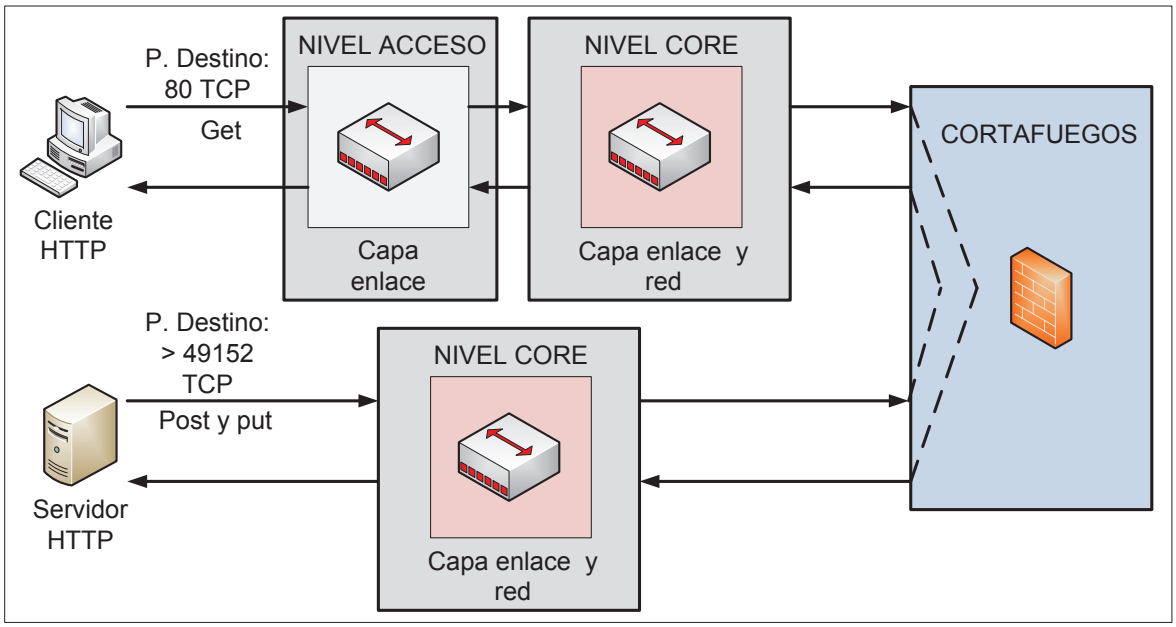


Figura 2.2. Flujo de datos para el servicio HTTP.

Fuente: Ing. Carlos Garzón Alvarado, Departamento de Tecnologías de Información, Superintendencia de Telecomunicaciones, julio 2013.

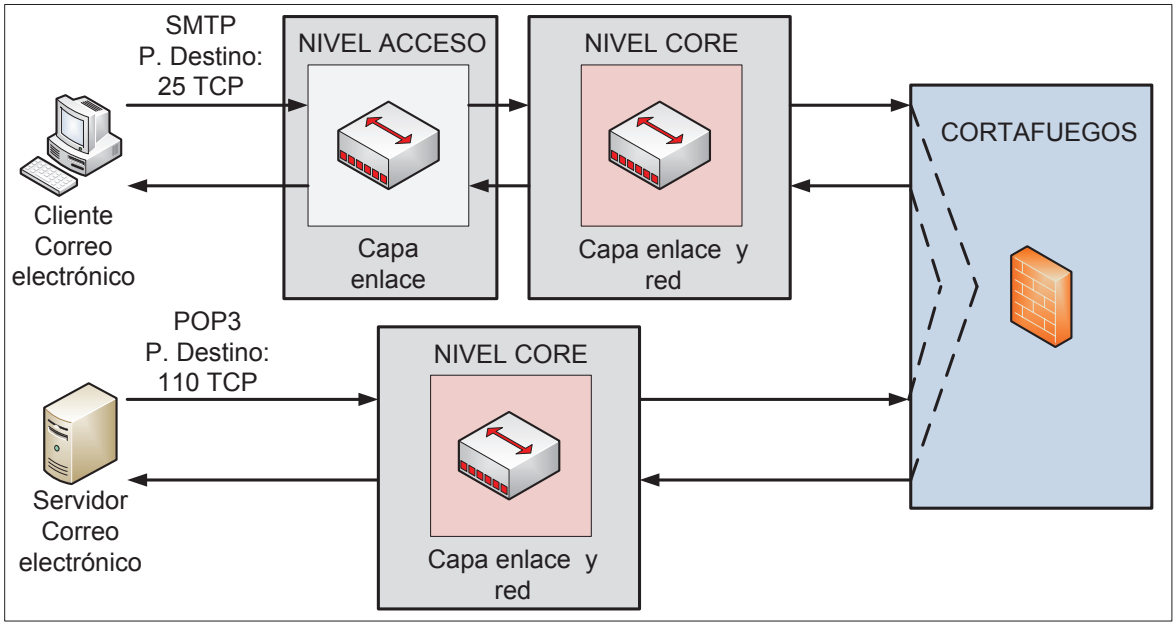


Figura 2.3. Flujo de datos para el servicio de correo electrónico.

Fuente: Ing. Carlos Garzón Alvarado, Departamento de Tecnologías de Información, Superintendencia de Telecomunicaciones, julio 2013.

El flujo de datos para el servicio Java EE se detalla en la Figura 2.4, donde los clientes acceden a la red a través de Internet; y una vez dentro de ésta, la información de solicitudes al servicio cruzan por los cortafuegos y enrutadores ubicados en la frontera con Internet, para luego dirigirse a los conmutadores de core donde serán enrutados al servidor Java EE directamente conectado al conmutador de core. Por su parte, las respuestas enviadas desde el servidor a los clientes utilizan la misma ruta pero en sentido inverso.

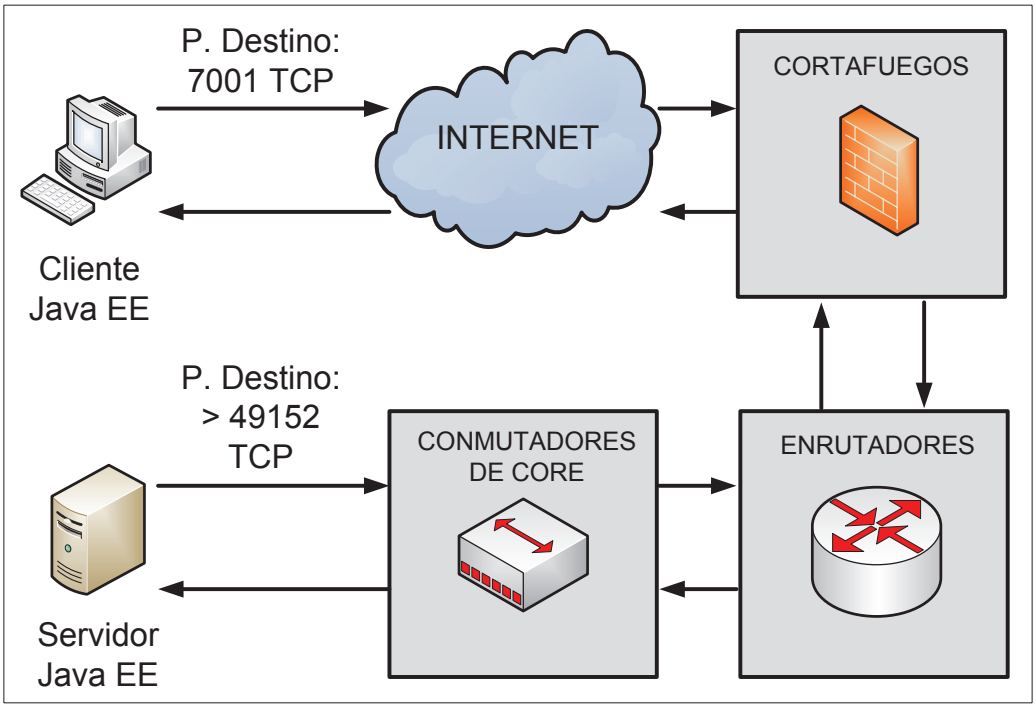


Figura 2.4. Flujo de datos para el servicio Java EE.

Fuente: Ing. Carlos Garzón Alvarado, Departamento de Tecnologías de Información, Superintendencia de Telecomunicaciones, julio 2013.

2.1.3.2 Análisis de Capacidades de la Capa Aplicación

Los servicios de correo electrónico, HTTP y Java EE se encuentran funcionando dentro del mismo terminal, un servidor IBM Power750 sobre una plataforma AIX y RISC, cuyas capacidades computacionales y de almacenamiento se encuentran descritas en la tabla 2.2.

Tabla 2.2. Características técnicas de los servidores para aplicaciones y servicios.

Aspecto Técnico	Total	Utilización aproximada (Hora pico)	Disponibilidad aproximada (Hora pico)
Procesamiento	8 x 3.5 GHz	50 %	50 %
Memoria RAM	35 GBytes	50 %	50 %
Almacenamiento	100 TBytes	88 TBytes	12 TBytes

Fuente: Ing. Carlos Garzón Alvarado, Departamento de Tecnologías de Información, Superintendencia de Telecomunicaciones, julio 2013.

2.1.3.3 Análisis de Seguridad de la Capa Aplicación

Las aplicaciones de correo electrónico y HTTP hacen uso de los plugings Ironport Email y Ironport Web como métodos de seguridad. Para el caso del servicio corporativo Java EE, ésta está en capacidad de implementar sistemas de autenticación, integridad y privacidad, se define a nivel de capa aplicación, bien sea dentro del código de aplicación a través de la implementación del protocolos de seguridad como TLS u otro; o definida a través del servidor Java EE Weblogic 12c y sus APIs de seguridad.

Todas las aplicaciones de la Superintendencia de Telecomunicaciones están restringidas en su uso por medio de autenticación de usuarios usando el protocolo LDAP sobre servidores CAS Jasig.

2.1.4 ANÁLISIS DE LA SITUACIÓN LEGAL DEL SERVICIO DE INTERNET

El servicio de Internet en el Ecuador, se encuentra normado en el Reglamento para los abonados de los servicios de telecomunicaciones y de valor agregado, donde se definen los aspectos cualitativos a los cuales los usuarios del servicio de Internet

tienen derecho a disponer por parte de sus respectivos proveedores[7], más no los aspectos técnicos cuantitativos de operación y calidad de servicio que deben ser provistos por éstos.

De forma general, los términos cuantitativos de operación y niveles de calidad del servicio de Internet se definen entre el proveedor y el usuario a través de un contrato o Acuerdo de Nivel de Servicio (SLA). En nuestro país, para usuarios residenciales éstos contratos únicamente consideran como parámetro técnico cuantitativo de calidad de servicio, el ancho de banda y el factor de compartición. Para el caso de Internet dedicado, los proveedores de servicio de Internet (ISP) acuerdan con sus usuarios a través de SLAs porcentajes de disponibilidad y latencia mínima, además del ancho de banda y factor de compartición.

Comparando nuestra realidad con otros países considerados de primer mundo, los parámetros técnicos cuantitativos de los SLA para usuarios residenciales del servicio de Internet residencial son los mismos, pero para el caso de Internet dedicado, se aseguran adicionalmente a los mencionados anteriormente, el porcentaje máximo de paquetes perdidos y en ciertos casos incluso niveles de Jitter máximo. En la tabla 2.3, se detallan los valores de aspectos técnicos que establecen los niveles de calidad para el servicio de Internet dedicado del ISP americano Verizon.

Tabla 2.3. SLA para el servicio de Internet dedicado de la empresa Verizon.

Disponibilidad Mínima	100 %
Latencia Máxima	45 mseg.
Paquetes perdidos Máximo	0.5 %
Jitter Máximo	1 mseg.

[7] Sección III, Artículos 13-25 del Reglamento para los Abonados de los Servicios de Telecomunicaciones y de Valor Agregado. Fuente: http://www.supertel.gob.ec/pdf/reglamento_abonados_clientes_usuarios.pdf

La Superintendencia de Telecomunicaciones, en la obligación de controlar la calidad del servicio de Internet y al no contar con una herramienta computacional que le permita llevar a cabo ésta labor, se ve en la necesidad de desarrollar una aplicación que le permita controlar y monitorizar cuantitativamente los niveles de calidad del servicio de Internet provisto por los ISP a sus usuarios, y hacer que los contratos de prestación del servicio suscritos se cumplan. En un inicio, ésta aplicación deberá encargarse de la medición de ancho de banda a nivel residencial únicamente, por lo que el alcance del presente proyecto constituirá en la medición del ancho de banda de bajada y subida del servicio de Internet a nivel residencial.

2.2 ANÁLISIS DE REQUERIMIENTOS

En éste apartado, se realiza el análisis de los requerimientos con los que deberá contar la nueva aplicación, en base a un cuestionario realizado a los técnicos de la Superintendencia de Telecomunicaciones encargados de controlar el servicio de Internet. Las respuestas obtenidas del cuestionario serán después presentadas y analizadas.

2.2.1 ELABORACIÓN DEL CUESTIONARIO DE REQUERIMIENTOS

El objetivo del cuestionario de requerimientos, es facilitar la determinación de los requerimientos funcionales, de rendimiento y seguridad con los que deberá contar la nueva aplicación.

El cuestionario va dirigido al director de la Unidad de Control de la Prestación de Servicios de la Superintendencia de Telecomunicaciones (UCPS), el mismo que representa a todos los técnicos que utilizaran la nueva aplicación. Por el hecho de que para los técnicos es transparente lo que sucede en las capas red y lógica, el cuestionario se concentra únicamente en los requerimientos funcionales, de rendimiento y seguridad a nivel de capa aplicación.

El cuestionario es de autoría propia, elaborado en base al estándar IEEE STD 830-1998[8], tomando en cuenta las características del problema que la nueva aplicación pretende resolver, los recursos de hardware y software disponibles en la SUPERTEL, y de las tecnologías afines disponibles que puedan dar solución a dicho problema.

2.2.1.1 Requerimientos Funcionales

En la siguiente tabla se especifican las preguntas del cuestionario determinadas para los requerimientos funcionales de la nueva aplicación:

Tabla 2.4. Cuestionario para los requerimientos funcionales.

Número	*Pregunta*
1	¿Conoce usted si existen en la actualidad sistemas de monitoreo para el control de ancho de banda? ¿Es ésta una opción factible para el presente proyecto?
2	¿Dónde se ubicará el sistema de monitoreo?
3	¿A quién se pretende monitorear?
4	¿Qué nivel de intervención de los usuarios monitoreados es requerida?
5	¿Cuál será el flujo de datos de los resultados obtenidos, desde su captura hasta su visualización?
6	¿Qué tipo de usuarios harán uso de la nueva aplicación? (Por ejemplo: administrativo. ejecutivo, operativo, etc.)
7	¿Qué tipo de información se pretende capturar en los usuarios monitoreados? (Por ejemplo: fecha, dirección IP, ancho de banda de subida, etc.)

[8] Estándar que define las buenas prácticas para la creación de documentos donde se detallan los requerimientos necesarios para el desarrollo de software. Fuente: http://www.math.uaa.alaska.edu/~afkjm/cs401/IEEE830.pdf

Número	*Pregunta*
8	¿Qué operaciones se llevarán a cabo por la nueva aplicación? (Por ejemplo: visualización de resultados, configuración de usuarios, etc.)
9	¿Qué tipo de información es necesaria ingresar para los usuarios monitoreados?
10	¿Qué frecuencia de obtención de resultados seria la óptima para sus necesidades? (Por ejemplo: cada 10 minutos, cada hora, etc.)
11	¿Qué tipo de reportes son necesarios? (Por ejemplo: datos de usuarios, mediciones por usuario, mediciones por fecha, etc.)
12	De las opciones de monitoreo descritas a continuación, ¿Cuál cree usted que encajaría con sus necesidades? a. Aplicación de escritorio. b. Aplicación Web. c. Cliente-servidor. d. SNMP. e. RMON. f. Otra (especificar).
13	Para el envío de resultados de monitorización, ¿Cuál de éstas opciones podría utilizarse? a. Aplicación distribuida de escritorio. b. Aplicación web. c. Cliente-servidor. d. SNMP. e. RMON. f. Servicios Web. g. Otra (especificar).

Número	*Pregunta*
14	Para la visualización de resultados capturados, ¿Qué tipo de sistema sería más conveniente? a. Aplicación de escritorio. b. Web. c. Cliente-servidor. d. Java EE (JSF, JSP, applets, etc.). e. Otra (especificar).
15	Para el almacenamiento de datos ¿Cuál de las siguientes opciones sería conveniente? a. Base de datos local. b. Discos duros internos o externos. c. La nube. d. Otra (especificar).

2.2.1.2 Requerimientos de Rendimiento

Los requerimientos de rendimiento fueron determinados en base al siguiente cuestionario:

Tabla 2.5. Cuestionario para los requerimientos de rendimiento.

Número	*Pregunta*
1	¿Cuál es el número estimado de usuarios monitoreados para la nueva aplicación?
2	¿Cuál es el número estimado de usuarios operativos que podrían utilizar la aplicación simultáneamente?

Número	*Pregunta*
3	¿Cuál deberá ser la velocidad de respuesta de la aplicación para los usuarios monitoreados?
4	¿Cuál deberá ser la velocidad de respuesta de la aplicación para los usuarios técnicos de la SUPERTEL?

2.2.1.3 Requerimientos de Seguridad

A continuación se encuentra la tabla con el contenido del cuestionario para el apartado de requerimientos de seguridad de la nueva aplicación:

Tabla 2.6. Cuestionario para los requerimientos de seguridad.

Número	*Pregunta*
1	¿Qué nivel de disponibilidad es requerida por la nueva aplicación?
2	De los siguientes aspectos de seguridad, ¿Cuáles son necesarios a ser implementados por la nueva aplicación? a. Autenticación. b. Privacidad. c. Integridad.

2.2.2 RESULTADO DEL CUESTIONARIO DE REQUERIMIENTOS

Debido a que el cuestionario fue dirigido a una sola persona, el índice de error del resultado del cuestionario es del 0%, asegurando que los requerimientos de la aplicación son indudables y están claramente identificados.

2.2.2.1 Requerimientos Funcionales

Los resultados del cuestionario de requerimientos funcionales se detallan en la tabla a continuación:

Tabla 2.7. Resultado del cuestionario para los requerimientos funcionales.

Número	*Respuesta*
1	El personal técnico si conoce de sistemas de monitoreo de ancho de banda, como la aplicación ubicada en el sitio web “speedtest.net”, pero requieren de un sistema independiente que podría funcionar como éste.
2	El sistema de monitoreo se debe ubicar en la matriz de la Superintendencia de Telecomunicaciones ya que aquí es donde se implementan todos los sistemas de control de ésta entidad.
3	Los usuarios monitoreados serán los usuarios finales residenciales del servicio de Internet.
4	El nivel de intervención de los usuarios monitoreados debe ser el mínimo, asegurando que la monitorización sea imperceptible para éstos.
5	Los resultados capturados en los usuarios monitoreados deben ser trasmitidos por Internet hasta una base de datos ubicada en la matriz de la Superintendencia de Telecomunicaciones, para luego ser accedidos por el personal técnico de la Superintendencia de Telecomunicaciones para su análisis.
6	Harán uso de la aplicación únicamente personal técnico de la Superintendencia de Telecomunicaciones.

Número	*Respuesta*
7	En los usuarios monitoreados se deben capturar la siguiente información: • Ancho de banda de subida. • Ancho de banda de bajada. • Fecha de captura. • Dirección MAC. • Dirección IP. Las dos últimas con el propósito de identificar el origen de las mediciones.
8	Las operaciones de la aplicación necesarias para la aplicación son, gestión de usuarios monitoreados y visualización de resultados de monitorización.
9	Los usuarios monitoreados deben contar con la siguiente información: • Cédula de identidad. • Nombre. • Dirección. • Sector. • Ciudad. • Provincia. • ISP.
10	La frecuencia de captura de datos de monitorización debe ser la mínima posible, asegurando que no se vean afectadas o saturadas otro tipo de aplicaciones de la Superintendencia de Telecomunicaciones.

Número	*Respuesta*
11	En un inicio, son requeridos los siguientes tipos de reportes: • Todas las mediciones de ancho de banda registradas. • Mediciones de ancho de banda por usuario. • Mediciones de ancho de banda por usuario y fecha de captura. • Índice de disponibilidad del servicio de Internet por hora de fecha de captura, para el seguimiento de cortes de servicio programados por el ISP y controles de servicio programados por la UCPS.
12	La opción de monitoreo más adecuada sería la que mayor beneficio provee al menor costo de recursos de hardware, software y de red posible. La opción de SNMP puede ser una opción, al ser éste un sistema ampliamente implementado.
13	Para el envío de resultados de monitorización a través de Internet se debe usar el sistema utilizado en la actualidad por las aplicaciones distribuidas de la Superintendencia de Telecomunicaciones que es Servicios Web JEE.
14	Los resultados capturados deben ser visualizados; ya sea por medio de JSP, o JSF, ya que éste es el método de visualización de resultados utilizado por las aplicaciones de la Superintendencia de Telecomunicaciones.
15	Debido a que la Superintendencia de Telecomunicaciones maneja una base de datos local Oracle, ésta debe ser la utilizada para el almacenamiento de los resultados capturados por la aplicación.

2.2.2.2 Requerimientos de Rendimiento

La siguiente tabla muestra los resultados del cuestionario para el apartado de requerimientos de rendimiento:

Tabla 2.8. Resultado del cuestionario para los requerimientos de rendimiento.

Número	*Respuesta*
1	Cumpliendo con el alcance del presente proyecto, el número de usuarios monitoreados será de máximo 2.
2	El número de usuarios operativos que podría usar la aplicación simultáneamente no sobrepasa de 5, ya que es el número máximo de técnicos encargados del control de los servicios de valor agregado.
3	La velocidad de respuesta de la nueva aplicación para los usuarios monitoreados es indiferente, pero siempre tratando que la aplicación responda cuando le sea posible.
4	La velocidad de respuesta de la aplicación para los usuarios técnicos de la SUPERTEL puede ser desde casi inmediata hasta un par de segundos, tratando siempre que la aplicación tenga tiempos de respuesta aceptables.

2.2.2.3 Requerimientos De Seguridad

Los resultados del cuestionario para los requerimientos de seguridad se muestran en la siguiente tabla:

Tabla 2.9. Resultado del cuestionario para los requerimientos de seguridad.

Número	*Respuesta*
1	El nivel de disponibilidad de la aplicación debe ser 24/7 los 365 días del año, siempre y cuando no existan factores externos a la aplicación que lo impidan.
2	Por la naturaleza de los datos, el único método de seguridad necesario será la autenticación sin encriptación de usuarios monitoreados.

2.3 CASOS DE USO DE LA APLICACIÓN

La utilización de la aplicación descrita en éste documento, será principalmente realizada por los técnicos de la Unidad de Control de la Prestación de Servicios (UCPS) de la SUPERTEL, y en base al análisis de requerimientos, se han identificado los siguientes casos de uso:

- Gestión de usuarios.
    - Ingreso de nuevo usuario.
    - Búsqueda de usuario.
    - Modificación de usuario existente.
    - Eliminación de usuario existente.
    - Consulta de los usuarios registrados.

- Consulta de resultados.
    - Consulta de todas las mediciones obtenidas.
    - Consulta de mediciones por usuario
    - Consulta de mediciones por usuario y fecha de captura.
    - Consulta del índice de disponibilidad del servicio de Internet.

2.3.1 GESTIÓN DE USUARIOS MONITOREADOS

El proceso de gestión de usuarios, es aquel que permite a los técnicos de la UCPS, el ingreso, eliminación, modificación, visualización y búsqueda de los usuarios monitoreados y de su información.

2.3.1.1 Ingreso de Nuevo Usuario

Éste proceso permite a los técnicos de la UCPS ingresar nuevos usuarios monitoreados y su información al sistema, Figura 2.6.

Tabla 2.10. Caso de uso para el ingreso de nuevos usuarios monitoreados.

Caso de Uso	Ingreso de nuevos usuarios monitoreados
Versión	1.0 (16/10/2012)
Autor	Andrés Tobar
Descripción	Proceso por medio del cual el personal técnico de la UCPS ingresa nuevos usuarios monitoreados en la base de datos del sistema de monitorización.
Actores	Personal Técnico de la UCPS.
Pre-condición	Ninguna.
Secuencia	
1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web. 2) El personal técnico elije la opción de “Nuevo Usuario” en la sección Gestión de Usuarios dentro de la aplicación. 3) El sistema muestra un formulario donde se debe ingresar toda la información referente al nuevo usuario monitoreado.	

4) El personal técnico acepta el ingreso del nuevo usuario presionando el botón “Ingresar”. 5) El sistema accede a la base de datos a través de un sistema de persistencia para efectuar el ingreso del nuevo usuario dentro de la misma. 6) El sistema devuelve un mensaje a través de la aplicación de que el proceso de ingreso de nuevo usuario se ha realizado con éxito. 7) El personal técnico de la UCPS puede ingresar otros usuarios siguiendo el proceso nuevamente desde el paso 2.	
Post-condición	Visualización de todos los usuarios registrados.

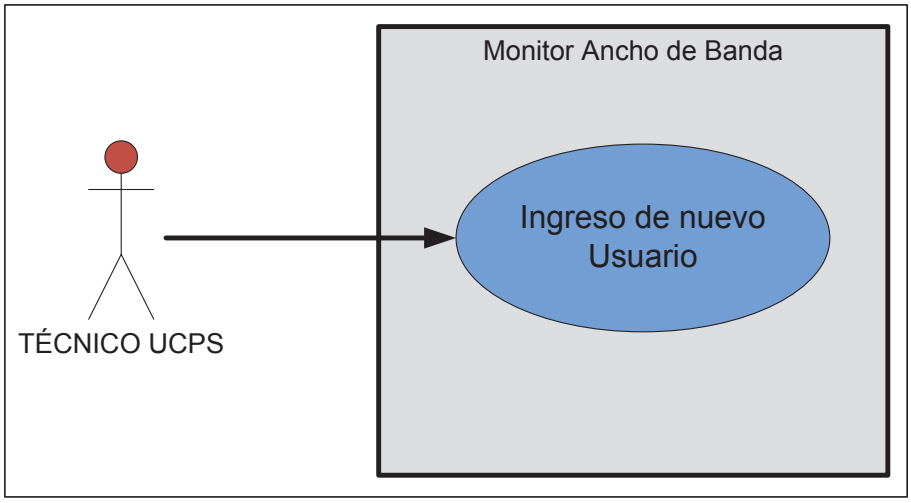


Figura 2.5. Caso de uso para el ingreso de nuevos usuarios.

2.3.1.2 Búsqueda de Usuario

A través de éste proceso, los técnicos de la UCPS serán capaces de buscar un usuario determinados dentro de la base de datos de la aplicación, Figura 2.7.

Tabla 2.11. Caso de uso para la búsqueda de usuario monitoreado.

Caso de Uso	Búsqueda de usuario monitoreado
Versión	1.0 (16/10/2012)
Autor	Andrés Tobar
Descripción	Proceso por medio del cual el personal técnico de la UCPS realiza la búsqueda de un usuario monitoreado en la base de datos del sistema de monitorización.
Actores	Personal Técnico de la UCPS.
Pre-condición	Conocer la dirección MAC del usuario.
Secuencia	
1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web. 2) El personal técnico elije la opción de “Buscar Usuario” en la sección Gestión de Usuarios dentro de la aplicación. 3) Dentro de ésta opción se ingresa la dirección MAC con la cual se encuentra registrado el usuario a modificar su información. 4) El personal técnico acepta la consulta presionando el botón “Buscar”. 5) El sistema accede a la base de datos a través de un sistema de persistencia para efectuar la búsqueda del usuario dentro de la misma. 6) Si el usuario se encuentra registrado, el sistema devuelve toda la información referente al usuario, de lo contrario devuelve un mensaje de error.	

7) El personal técnico de la UCPS puede realizar la búsqueda de otros usuarios siguiendo el proceso nuevamente desde el paso 2.	
Post-condición	Ninguna.

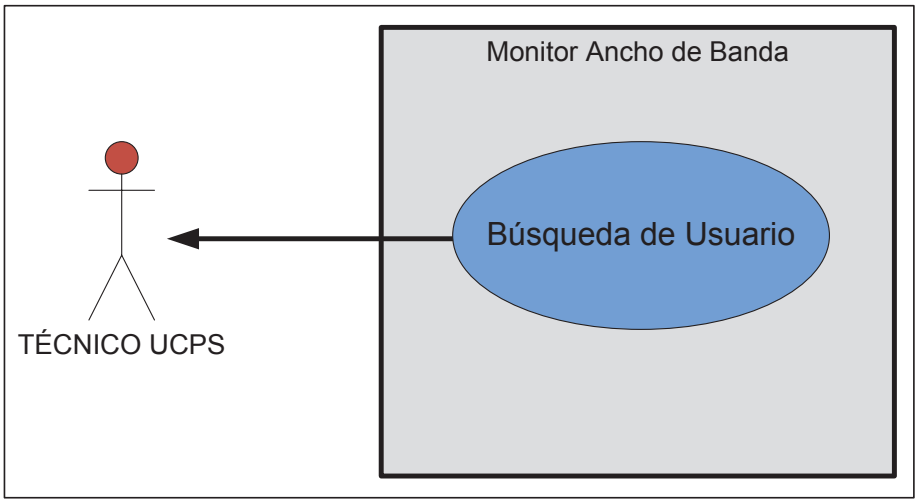


Figura 2.6. Caso de uso para la búsqueda de usuario.

2.3.1.3 Modificación de Usuario Existente

Éste proceso servirá para la modificación de la información perteneciente a los usuarios existentes en la base de datos del sistema de monitorización, Figura 2.8.

Tabla 2.12. Caso de uso para la modificación de usuario monitoreado.

Caso de Uso	Modificación de usuarios monitoreados
Versión	1.0 (16/10/2012)
Autor	Andrés Tobar

Descripción	Proceso por medio del cual el personal técnico de la UCPS modifica la información de los usuarios monitoreados en la base de datos del sistema de monitorización.
Actores	Personal Técnico de la UCPS.
Pre-condición	Conocer la dirección MAC del usuario.
Secuencia	

1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web.
2) El personal técnico elije la opción de “Buscar Usuario” en la sección Gestión de Usuarios dentro de la aplicación.
3) Dentro de ésta opción se ingresa la dirección MAC con la cual se encuentra registrado el usuario a modificar su información.
4) El sistema accede a la base de datos a través de un sistema de persistencia para efectuar la búsqueda del usuario dentro de la misma.
5) Si el usuario se encuentra registrado, el sistema devuelve toda la información referente al usuario, de lo contrario devuelve un mensaje de error.
6) En ésta instancia, el personal técnico elije la opción “Modificar Usuario”.
7) El sistema devuelve un formulario para el ingreso de la nueva información perteneciente al usuario a modificar.
8) El personal técnico acepta la modificación de la información del usuario presionando el botón “Modificar”.

9) La aplicación accede a la base de datos por medio de un sistema de persistencia para la actualización de los nuevos datos de usuario. Si el proceso no se puede completar se devuelve un mensaje de error. 10) El personal técnico de la UCPS puede modificar otros usuarios siguiendo el proceso nuevamente desde el paso 2.	
Post-condición	Visualización de todos los usuarios registrados.

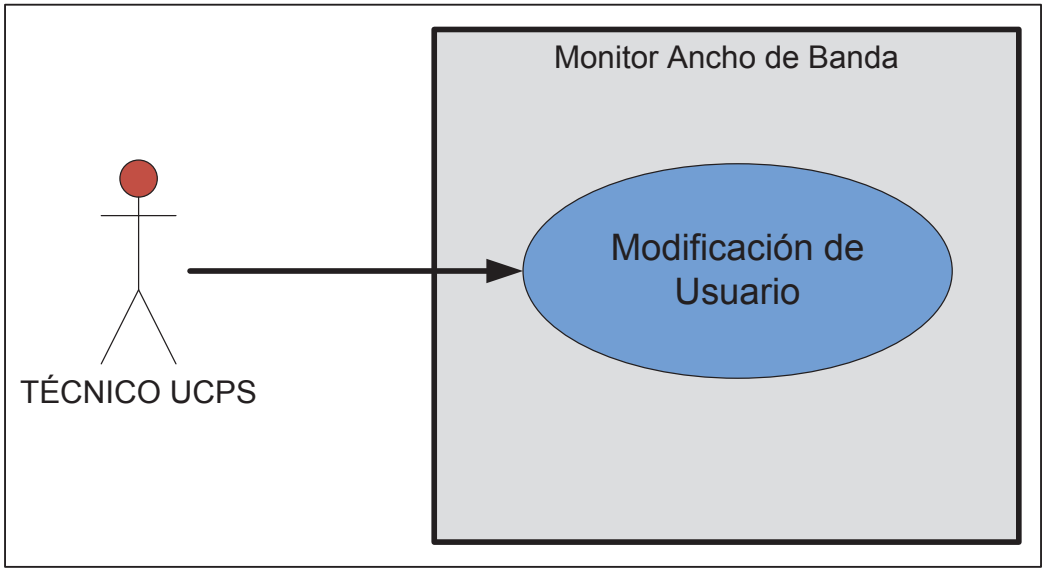


Figura 2.7. Caso de uso para la modificación de usuario.

2.3.1.4 Eliminación de Usuario Existente

Para la eliminación de un usuario existente en la base de datos de la aplicación, se realiza el siguiente procedimiento, Figura 2.9.

Tabla 2.13. Caso de uso para la eliminación de usuario monitoreado.

Caso de Uso	Eliminación de usuarios monitoreados
Versión	1.0 (16/10/2012)

Autor	Andrés Tobar
Descripción	Proceso por medio del cual el personal técnico de la UCPS elimina usuarios monitoreados y toda su información contenida en la base de datos del sistema de monitorización.
Actores	Personal Técnico de la UCPS.
Pre-condición	Conocer la dirección MAC del usuario.
Secuencia	

1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web.
2) El personal técnico elije la opción de “Buscar Usuario” en la sección Gestión de Usuarios dentro de la aplicación.
3) Dentro de ésta opción se ingresa la dirección MAC con la cual se encuentra registrado el usuario a modificar su información.
4) El sistema accede a la base de datos a través de un sistema de persistencia para efectuar la búsqueda del usuario dentro de la misma.
5) Si el usuario se encuentra registrado, el sistema devuelve toda la información referente al usuario, de lo contrario devuelve un mensaje de error.
6) En ésta instancia, el personal técnico elije la opción “Eliminar Usuario”.
7) El personal técnico confirma la eliminación del usuario presionando el botón “Eliminar”.
8) La aplicación accede a la base de datos por medio de un sistema de persistencia para la eliminación del usuario.

9) El personal técnico de la UCPS puede eliminar otros usuarios siguiendo el proceso nuevamente desde el paso 2.	
Post-condición	Visualización de todos los usuarios registrados.

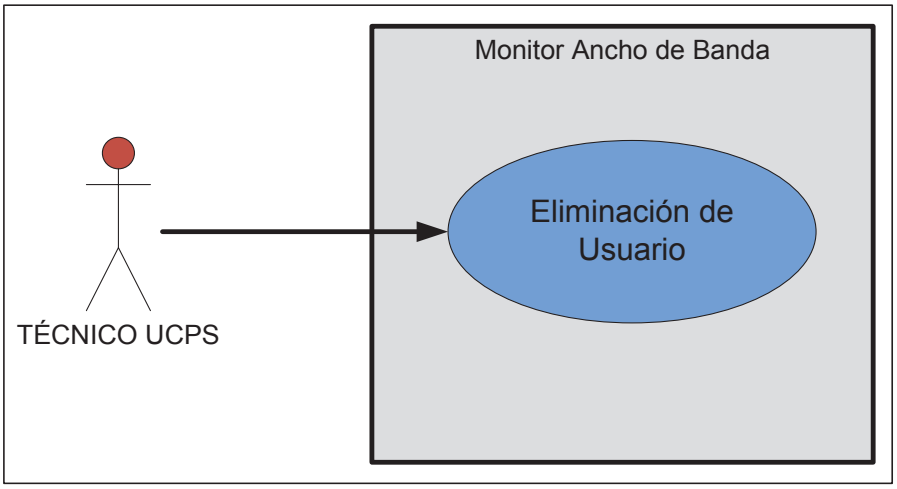


Figura 2.8. Caso de uso para la eliminación de usuario.

2.3.1.5 Consulta de Usuarios Registrados

Éste proceso permite la consulta de todos los usuarios monitoreados existentes en la base de datos del sistema, Figura 2.10.

Tabla 2.14. Caso de uso para la consulta de usuarios monitoreados registrados.

Caso de Uso	Búsqueda de usuario monitoreado
Versión	1.0 (16/10/2012)
Autor	Andrés Tobar

Descripción	Proceso por medio del cual el personal técnico de la UCPS realiza la consulta de todos los usuarios monitoreados existentes en la base de datos del sistema de monitorización.
Actores	Personal Técnico de la UCPS.
Pre-condición	Ninguna.
Secuencia	
1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web. 2) El personal técnico elije la opción de “Usuarios Registrados” en la sección Gestión de Usuarios dentro de la aplicación. 3) El sistema accede a la base de datos a través de un sistema de persistencia para efectuar la consulta de los usuarios almacenados dentro de la misma. 4) El sistema devuelve todos los registros existentes en la base de datos referentes a los usuarios monitoreados. 5) El personal técnico de la UCPS puede realizar una nueva consulta de los usuarios registrados siguiendo el proceso nuevamente desde el paso 2.	
Post-condición	Ninguna.

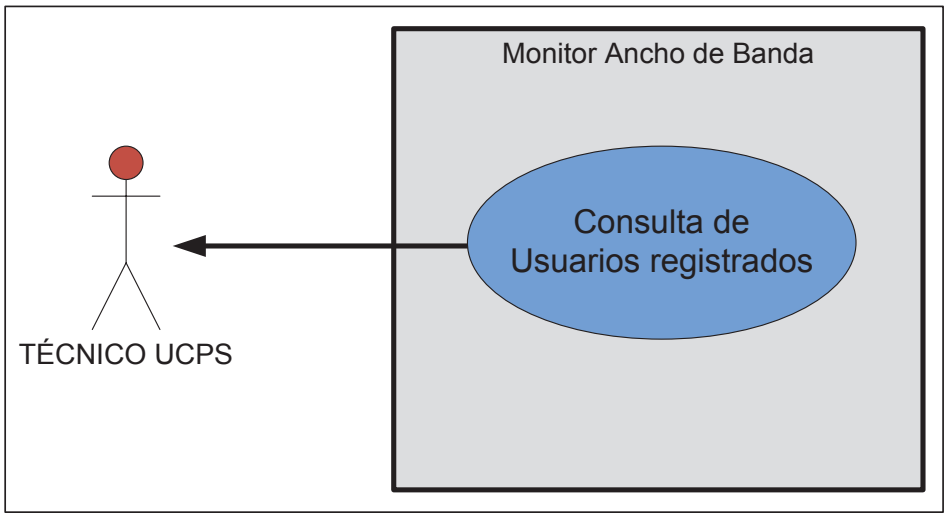


Figura 2.9. Caso de uso para la consulta de usuarios registrados.

2.3.2 CONSULTA DE RESULTADOS

En éste apartado se llevan a cabo las diferentes consultas referentes a las mediciones obtenidas desde los usuarios monitoreados, éstas consultas filtrarán las mediciones por usuarios y por fecha de captura de la medición, de igual manera se podrá visualizar todas las mediciones registradas en la base de datos.

2.3.2.1 Consulta de Todas las Mediciones

Éste proceso permite la visualización de todos los registros almacenados en la base de datos referentes a las mediciones capturadas desde los usuarios monitoreados, Figura 2.11.

Tabla 2.15. Caso de uso para consulta de todas las mediciones.

Caso de Uso	Consulta todas las Mediciones
Versión	1.0 (16/10/2012)
Autor	Andrés Tobar

Descripción	Proceso que permite la consulta de las mediciones realizadas por los todos los usuarios almacenadas en base de datos de la aplicación.
Actores	Personal Técnico de la UCPS.
Pre-condición	Ninguna.
Secuencia	
1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web. 2) El personal técnico elije la opción de “Mediciones Registradas” dentro de la sección de Mediciones. 3) El sistema devuelve todas las mediciones registradas hasta ese momento en la base de datos a través del sistema de persistencia. 4) El personal técnico de la UCPS puede realizar una nueva consulta de todas las mediciones registradas siguiendo el proceso nuevamente desde el paso 2.	
Post-condición	Ninguna.

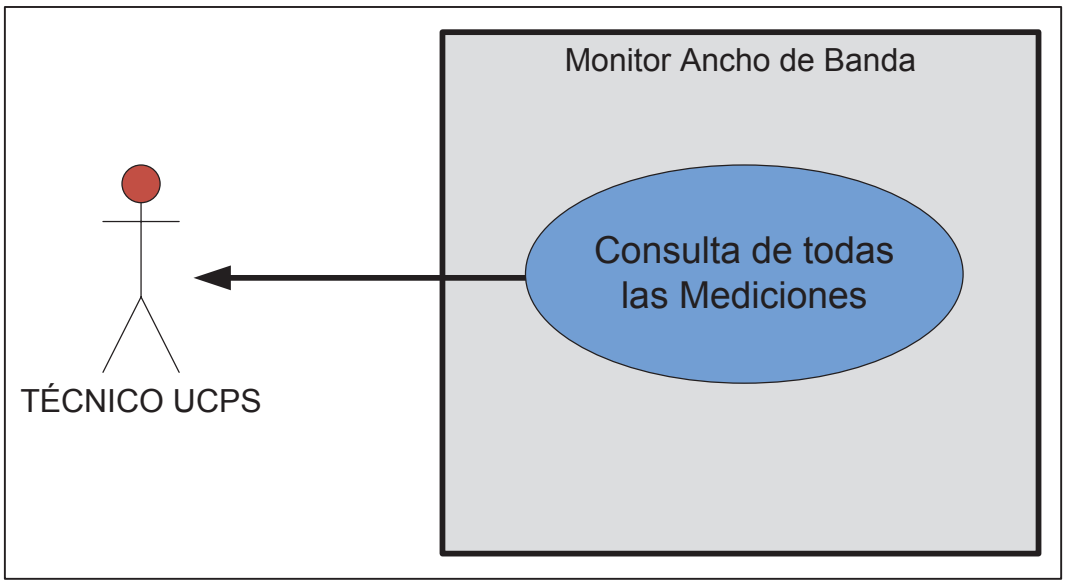


Figura 2.10. Caso de uso para la consulta de todas las mediciones.

2.3.2.2 Consulta de Mediciones por Usuario

Por medio de éste proceso, es posible la consulta de mediciones capturadas para un usuario monitoreado específico, las mismas que se encuentran almacenadas en la base de datos, Figura 2.12.

Tabla 2.16. Caso de uso para consulta de mediciones por usuario.

Caso de Uso	Consulta de Mediciones por Usuario
Versión	1.0 (16/10/2012)
Autor	Andrés Tobar
Descripción	Proceso que permite la consulta de mediciones realizadas por un usuario específico, y que se encuentran almacenadas en base de datos de la aplicación.
Actores	Personal Técnico de la UCPS.

Pre-condición	Conocer la dirección MAC del usuario.
Secuencia	
1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web. 2) El personal técnico elije la opción de “Buscar por Usuario” dentro de la sección de Mediciones. 3) Dentro de ésta opción se debe ingresar la dirección MAC del usuario monitoreado del cual se requiere consultar sus mediciones. 4) El personal técnico acepta la consulta presionando en el botón “Buscar”. 5) Si el usuario se encuentra registrado, el sistema accede a la base de datos por medio del sistema de persistencia y devuelve todas las mediciones registradas hasta ese momento para el usuario especificado, de lo contrario se devuelve un mensaje de error. 6) El personal técnico de la UCPS puede realizar una nueva consulta de las mediciones pertenecientes a un usuario específico siguiendo el proceso nuevamente desde el paso 2.	
Post-condición	Ninguna.

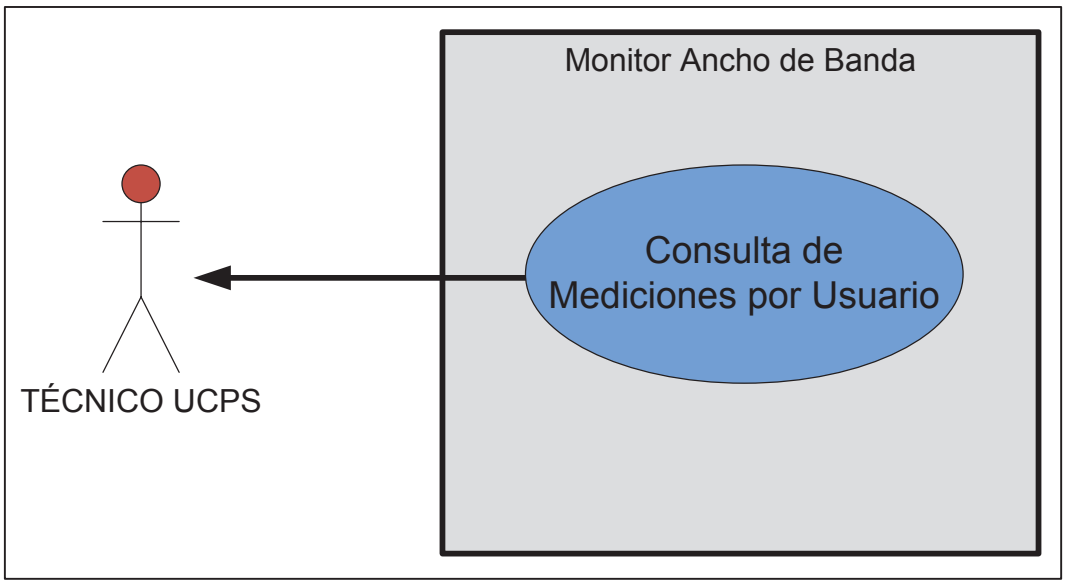


Figura 2.11. Caso de uso para la consulta de mediciones por usuario.

2.3.2.3 Consulta de Mediciones por Usuario y Fecha

La consulta de las mediciones obtenidas para un usuario monitoreado específico en una fecha determinada, se realiza por medio de éste procedimiento, Figura 2.13.

Tabla 2.17. Caso de uso para consulta de mediciones por usuario y fecha.

Caso de Uso	Consulta de Mediciones por Usuario
Versión	1.0 (16/10/2012)
Autor	Andrés Tobar
Descripción	Proceso que permite la consulta de mediciones realizadas por un usuario específico en una fecha determinada, y que se encuentran almacenadas en base de datos de la aplicación.
Actores	Personal Técnico de la UCPS.

Pre-condición	Conocer la dirección MAC del usuario.
Secuencia	
1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web. 2) El personal técnico elije la opción de “Buscar por Usuario” dentro de la sección de Mediciones. 3) Dentro de ésta opción se debe ingresar la dirección MAC del usuario monitoreado del cual se requiere consultar sus mediciones. 4) El personal técnico acepta la consulta presionando en el botón “Buscar”. 5) Si el usuario se encuentra registrado, el sistema accede a la base de datos por medio del sistema de persistencia y devuelve todas las mediciones registradas hasta ese momento para el usuario especificado, de lo contrario se devuelve un mensaje de error. 6) Aquí, el personal técnico ingresa una fecha determinada para filtrar los resultados de acuerdo a ésta. 7) El personal técnico acepta la consulta por fecha presionando el botón “Buscar”. 8) La aplicación devuelve todas las mediciones registradas en la fecha especificada para ese usuario. 9) El personal técnico de la UCPS puede realizar una nueva consulta por fecha eligiendo la opción “Regresar” y siguiendo el proceso desde el paso 6.	
Post-condición	Ninguna.

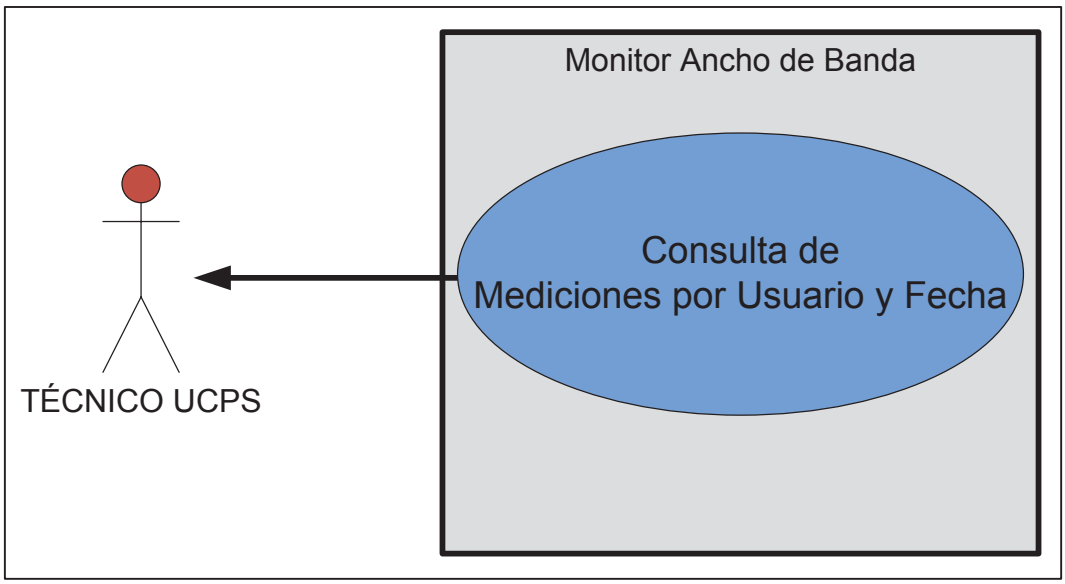


Figura 2.12. Caso de uso para la consulta de mediciones por usuario y fecha.

2.3.2.4 Consulta del Índice de Disponibilidad del Servicio de Internet

Mediante éste proceso es posible la consulta del índice de disponibilidad del servicio de Internet para un usuario especificado, Figura 2.14.

Tabla 2.18. Caso de uso para consulta del índice de disponibilidad del servicio de Internet.

Caso de Uso	Consulta del Índice de disponibilidad del servicio de Internet
Versión	1.0 (16/10/2012)
Autor	Andrés Tobar
Descripción	Proceso que permite la consulta del índice de disponibilidad del servicio de Internet para un usuario monitoreado especificado.
Actores	Personal Técnico de la UCPS.

Pre-condición	Conocer la dirección MAC del usuario.
Secuencia	

1) El personal técnico de la UCPS ingresa a la aplicación de monitoreo de Medición de Ancho de Banda localizada en el servidor HTTP de la Intranet por medio de un navegador web.
2) El personal técnico elije la opción de “Buscar por Usuario” dentro de la sección de Mediciones.
3) Dentro de ésta opción se debe ingresar la dirección MAC del usuario monitoreado del cual se requiere consultar sus mediciones.
4) El personal técnico acepta la consulta presionando en el botón “Buscar”.
5) Si el usuario se encuentra registrado, el sistema accede a la base de datos por medio del sistema de persistencia y devuelve todas las mediciones registradas hasta ese momento para el usuario especificado, de lo contrario se devuelve un mensaje de error.
6) Aquí, el personal técnico ingresa una hora y fecha determinada para filtrar los resultados de acuerdo a ésta.
7) El personal técnico acepta la consulta por hora y fecha presionando el botón “Buscar”.
8) La aplicación devuelve todas las mediciones registradas en la hora y fecha especificada, junto con el índice de disponibilidad del servicio de Internet para esa hora y fecha.
9) El personal técnico de la UCPS puede realizar una nueva consulta del índice de disponibilidad del servicio de Internet para otra hora y fecha del usuario eligiendo la opción “Regresar” y siguiendo el proceso desde el paso 6.

Post-condición	Ninguna.

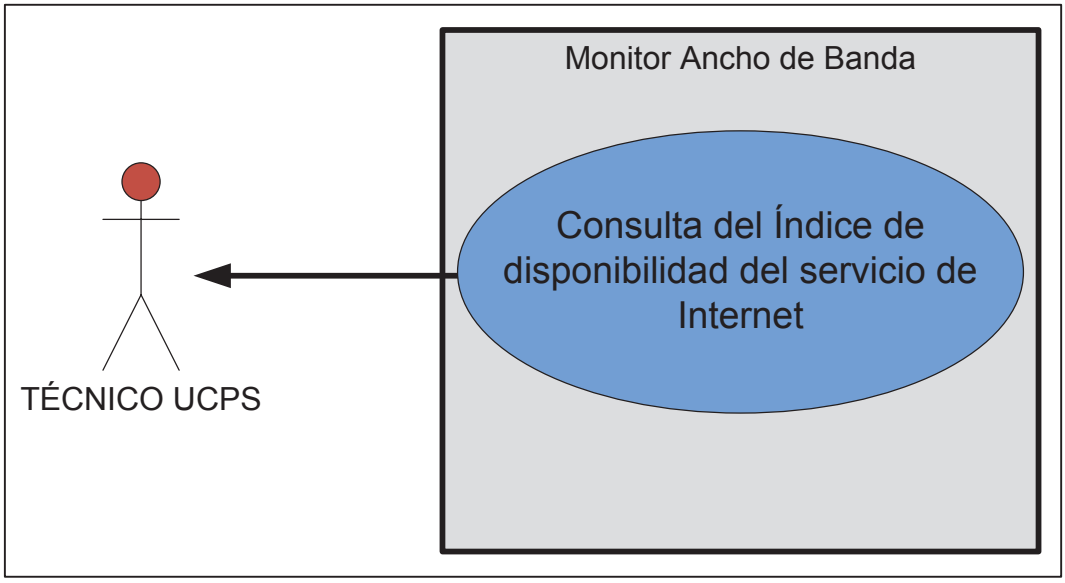


Figura 2.13. Caso de uso para la consulta del índice de disponibilidad del servicio de Internet.

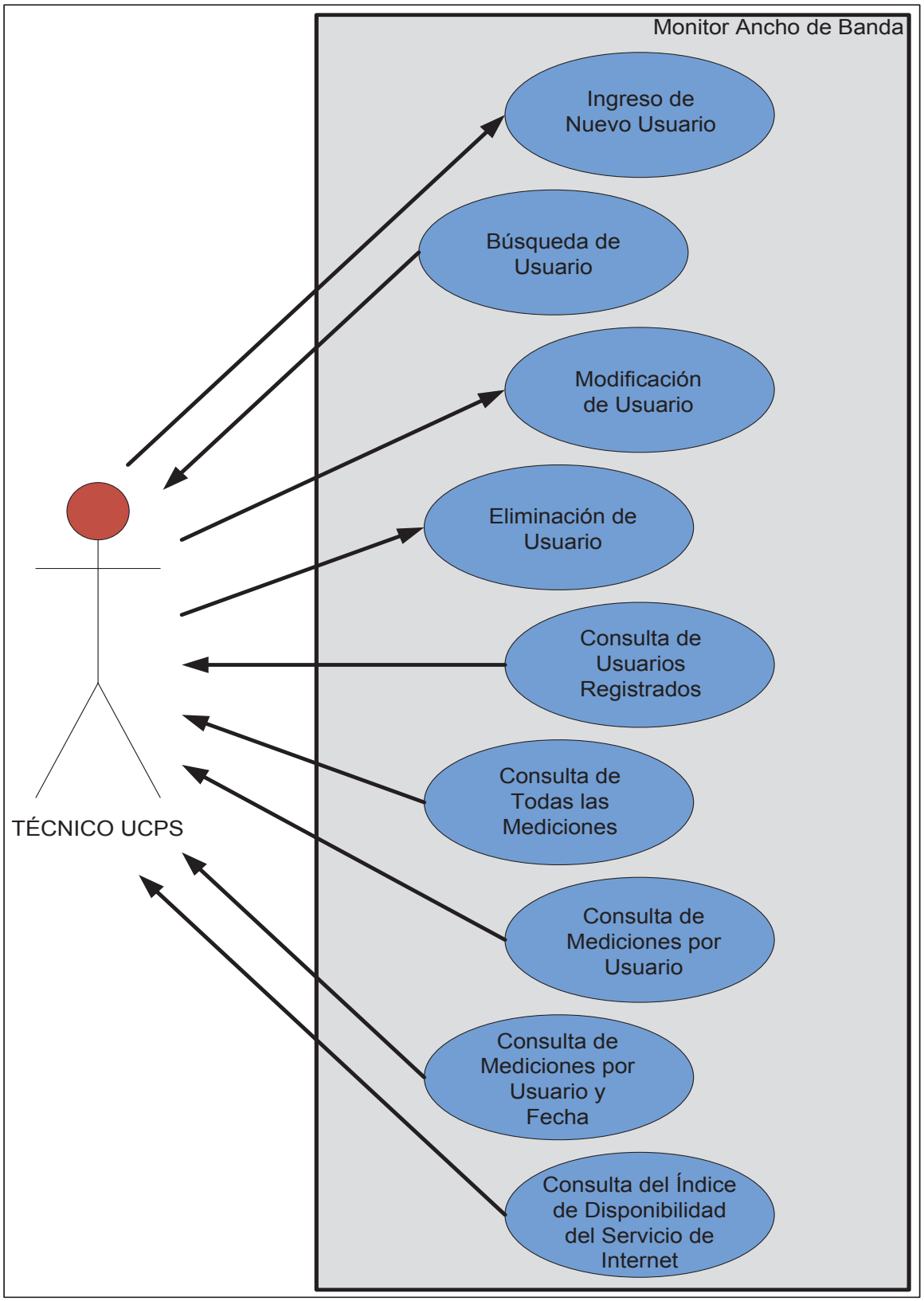


Figura 2.14. Diagrama de todos los casos de uso de la aplicación.

CAPÍTULO III: DISEÑO E IMPLEMENTACIÓN

A lo largo de éste capítulo se describe el diseño e implementación del prototipo de la aplicación de monitoreo de ancho de banda y cálculo del índice disponibilidad del servicio de Internet. Primeramente, se determinan las herramientas y el modelo de desarrollo, para luego establecer los módulos con que contara la nueva aplicación, los mismos que serán detallados en su diseño e implementación en base al modelo de desarrollo seleccionado.

3.1 HERRAMIENTAS DE DESARROLLO

La herramienta de programación seleccionada para el desarrollo de la nueva aplicación, será el lenguaje de programación orientada a objetos Java, ésto con el propósito principal de cumplir con la iniciativa de todas las entidades públicas del Ecuador en desarrollar software con lenguajes de programación de libre distribución y código abierto, además que el lenguaje de programación Java provee los siguientes beneficios: independencia de plataforma, alto rendimiento, seguridad, portabilidad, y disponibilidad de un gran número de librerías o APIs. El IDE de desarrollo Java seleccionado es Eclipse por integrar en una sola plataforma todas las herramientas y tecnologías utilizadas por la nueva aplicación.

La nueva aplicación usará a UML como sistema de modelado de sus clases Java, y utilizara como recursos de soporte a los APIs Adventnet y Sigar.

- **API Advennet**

El API Advetnet es un conjunto de librerías que simplifican el desarrollo de entidades SNMP, ya que ésta se encarga de implementar componentes que permiten tanto la utilización de MIBs, como el uso de las PDUs SNMP más comunes. El API brinda la capacidad de desarrollar e implementar aplicaciones SNMPv1, SNMPv2c y SNMPv3.

- **API SIgar**

El API Sigar es una librería encargada de analizar y monitorear los recursos de hardware presentes en un dispositivo computacional.

3.2 SELECCIÓN DE LA ARQUITECTURA

La medición del ancho de banda en los clientes del servicio de Internet se puede realizar de varias formas, pero se ha elegido al modelo de gestión de redes de Internet SNMP como método para la obtención de ancho de banda de bajada y subida en éstos, ya que el modelo SNMP ofrece grandes beneficios al proveer una arquitectura ya establecida, segura y eficiente.

Los datos de monitorización capturados en los clientes del servicio de Internet serán enviados a la SUPERTEL a través del Internet utilizando la arquitectura de Servicios Web. La SUPERTEL utiliza Servicios Web para la gran mayoría de sus aplicaciones distribuidas, logrando que ésta se encuentre bien establecida y funcional, sumando ésto a las ventajas que ofrece la arquitectura de Servicios Web sobre otras arquitecturas, la convierte en la opción más viable sobre la cual deberá funcionar la nueva aplicación.

Una de las grandes ventajas que conlleva la utilización de éstas arquitecturas para la captura y monitorización del ancho de banda, es que no se satura el enlace de comunicación entre los usuarios monitoreados y la SUPERTEL, ya que los mensajes utilizados por SNMP están en el orden de las centenas de bytes. Por el contrario, el método tradicional de cálculo de ancho de banda requiere saturar el canal de transmisión enviando mensajes en el orden de los Mega Bytes; incluso a las decenas de Mega Bytes, provocando que el canal de comunicación sea inutilizable para otras aplicaciones con mayor prioridad.

Para el almacenamiento de los datos de monitorización obtenidos por la aplicación, se ha optado por utilizar la base de datos relacional utilizada en la actualidad por la

SUPERTEL. De igual manera, se ha elegido la arquitectura de Servicios Web, para la consulta de datos de monitorización de la nueva aplicación por parte de los técnicos de la SUPERTEL, por los beneficios antes mencionados.

3.2.1 REQUERIMIENTOS MÍNIMOS DE LA APLICACIÓN

En base al análisis de requerimientos y a la arquitectura seleccionada, se han identificado los requerimientos mínimos con los que debe cumplir la aplicación presentada en el presente proyecto, Tabla 3.1, a partir de los cuales se realizara el desarrollo e implementación de la nueva aplicación.

Tabla 3.1. Resumen de requerimientos mínimos de la aplicación.

Número	*Requerimiento*
1	Los usuarios residenciales del servicio de Internet deben contar con una aplicación de escritorio para la captura de datos de monitorización.
2	La SUPERTEL dispondrá de una aplicación JEE para la recepción y almacenamiento de datos de monitorización provenientes desde los usuarios del servicio de Internet monitoreados.
3	La comunicación de la aplicación de escritorio y la aplicación JEE se debe realizar a través de Servicios Web de Java usando como medio de transporte a Internet
4	Los datos de monitorización obtenidos en la aplicación de escritorio serán capturados por medio de SNMP.
5	Los datos de monitorización de la aplicación serán almacenados en una base de datos relacional Oracle
6	Los técnicos de la SUPERTEL acceden a los resultados de monitorización almacenados en la base de datos por medio de Servicios Web de Java

Número	*Requerimiento*
7	El transporte de los datos de monitorización debe ser protegida con un sistema de autenticación.

3.3 METODOLOGÍA DE DISEÑO

Como metodología para el diseño de la nueva aplicación se hará uso del framework SCRUM, el mismo que permite organizar los componentes de una aplicación de acuerdo a su importancia; así como también, designar cierto periodo de tiempo para el desarrollo de uno o varios componentes (Sprints).

La Tabla 3.2, corresponde a la lista de sprints en donde se detallan todos los componentes de la nueva aplicación que fueron identificadas tanto en el análisis de requerimientos, como en la selección de la arquitectura, y que deben ser desarrolladas durante el tiempo que se lleve a cabo el proyecto. A cada componente de la aplicación se le asigna un nivel de prioridad con el propósito de diferenciar las características que requirieren ser desarrolladas con más urgencia. En la lista de sprints la prioridad con valor 1 es la prioridad más alta.

Tabla 3.2. Lista de Sprints de la aplicación.

N°	Sprint	Prioridad	Duración (días)
1	Agente SNMP v3	1	30
2	Gestor SNMP v3	1	30
3	MIBs	2	3
4	Capturador de datos de monitorización	3	15
5	Calculador de ancho de banda	3	15
6	Cliente del servicio web	4	30
7	Servidor del servicio web	4	30
8	Sistema de persistencia	5	15
9	Base de datos	5	15
10	Cliente del servicio web para consultas	6	30

N°	Sprint	Prioridad	Duración (días)
11	Interfaz gráfica del cliente del servicio web de consultas	7	15
12	Sistema de seguridad del servicio web	8	3

3.4 MÓDULOS DE LA APLICACIÓN

Para el diseño de la nueva aplicación se parte primordialmente del análisis de la situación actual de la Superintendencia de Telecomunicaciones y del análisis de requerimientos del programa, expuesto en el capítulo 2, y en base a los cuales se ha subdividido a éste en dos grandes módulos, Figura 3.1, que son:

- Módulo aplicación de cliente monitoreado.
- Módulo aplicación de servidor de monitoreo.

3.4.1 MÓDULO APLICACIÓN DE CLIENTE MONITOREADO

Éste módulo es un aplicación de escritorio escrita en lenguaje de programación Java, la cual está ubicada en el cliente que recibe el servicio de Internet. Básicamente se encarga de capturar, calcular y enviar información de monitorización en base a la arquitectura SNMP y Servicios Web. Consta de los siguientes sub-módulos, Figura 3.2:

- Módulo de captura y cálculo de datos de monitorización.
- Módulo Agente SNMP versión 3.
- Módulo Gestor SNMP versión 3.
- Módulo Cliente del Servicio Web para el Envío de Mediciones.

El conjunto de módulos que conforman la Aplicación de Cliente Monitoreado, únicamente funcionarán en computadores de escritorio y portátiles (laptops) con sistema operativo compatible con Java 1.6 o mayor y que sean soportados por el API Sigar, que son la gran mayoría de los existentes en el mercado; ya que ese ha sido el alcance considerado por éste proyecto.

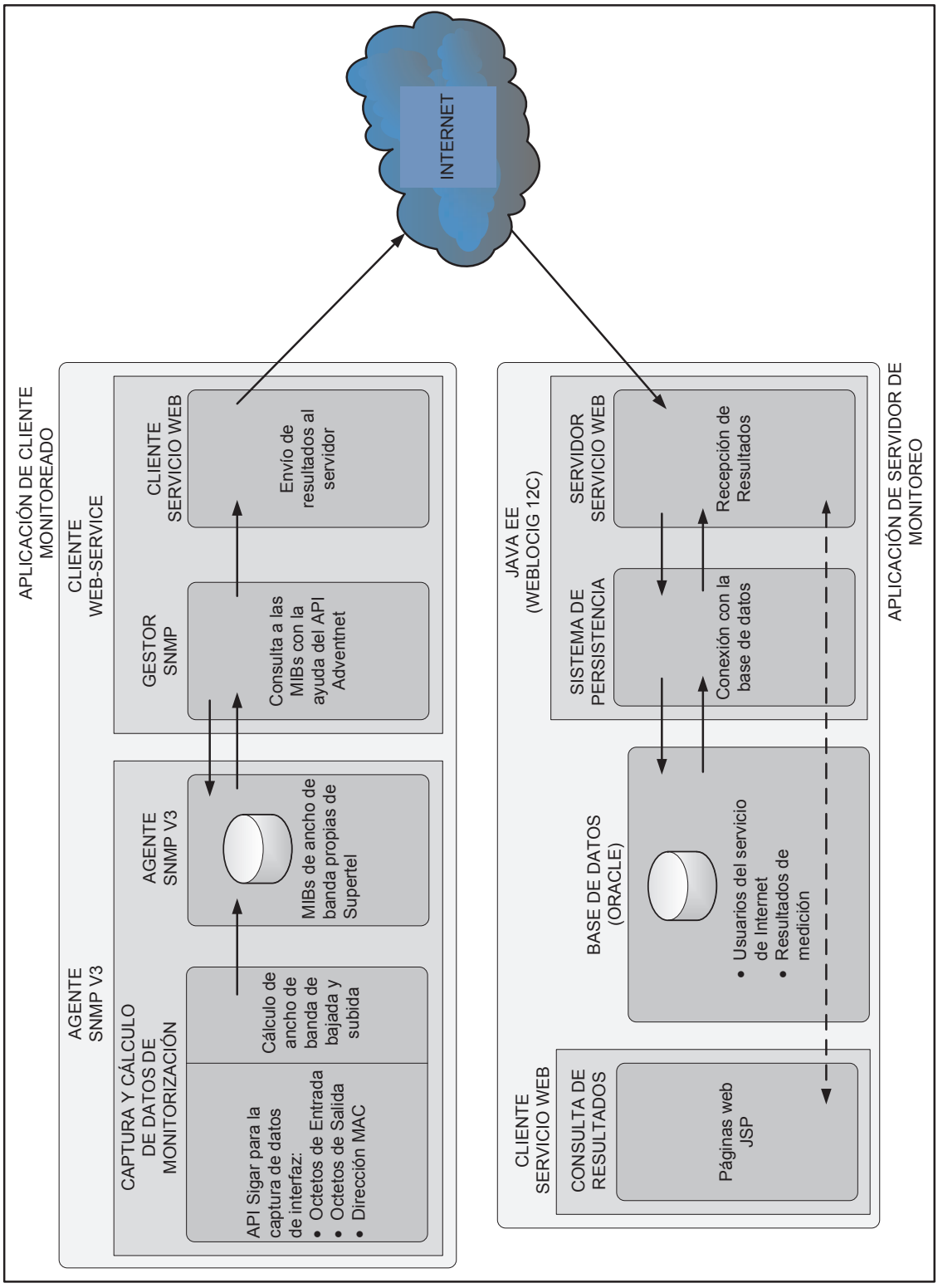


Figura 3.1. Esquema y módulos de la nueva aplicación para el monitoreo de ancho de banda

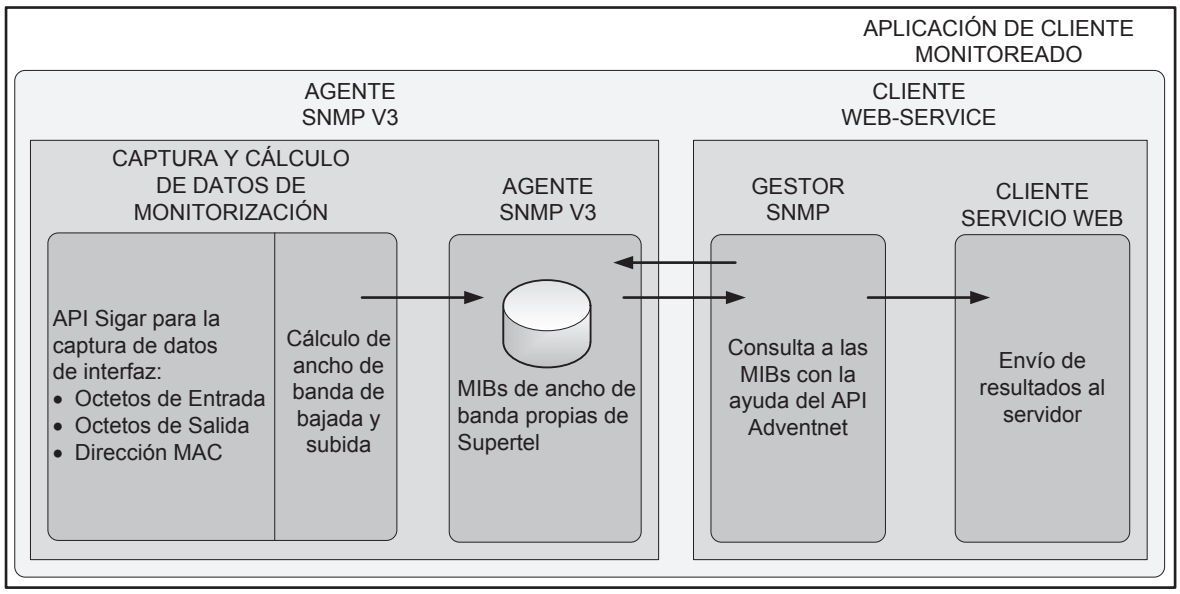


Figura 3.2. Módulo Aplicación de Cliente Monitoreado.

El presente módulo no contará con ninguna interfaz gráfica de usuario, ya que su función es únicamente enviar datos de monitorización al Módulo Aplicación de Servidor de Monitoreo. La aplicación prototipo presentada en el presente proyecto, diseñará e implementará éste módulo por medio del IDE Eclipse, razón por la cual no habrá ningún archivo de distribución de la aplicación.

3.4.1.1 Módulo de Captura y Cálculo de Datos de Monitorización

Éste módulo se encuentra compuesto por la clase *MonitorABImplementacionSigar* y la librería externa Sigar, Figura 3.3, la misma que se encarga primordialmente de realizar 2 labores:

- Determinación de la interfaz de red conectada a Internet.
- Captura de datos de interfaz de red.
- Cálculo de ancho de banda de interfaz de red.

3.4.1.1.1 Determinación de La Interfaz de Red Conectada a Internet

Antes de proceder a la captura de datos de monitorización, se debe determinar la interfaz de red conectada al Internet; pudiendo ser ésta de tipo IEEE 802.3, IEEE

802.11, etc., de entre todas las que pueden estar presentes dentro del dispositivo monitoreado. Para realizar ésta tarea se analiza la cantidad de octetos recibidos en cada una de éstas con la ayuda del método *determinacionInterface* de la clase *MonitorABImplementacionSigar*, y se selecciona a aquella interfaz de red con el mayor número de octetos de entrada.

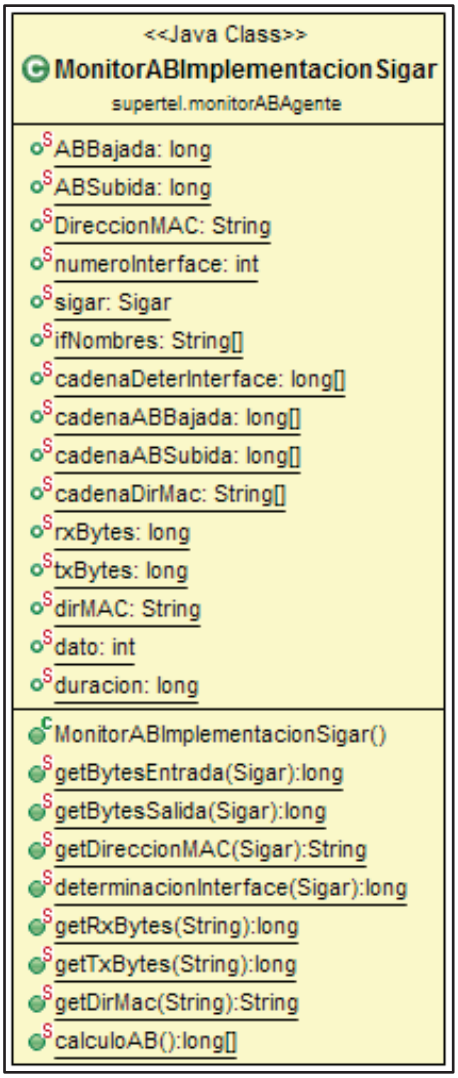


Figura 3.3. Diagrama de clases del módulo de captura y cálculo de datos de monitorización.

De manera general, los usuarios residenciales del servicio de Internet a lo máximo contarán en sus dispositivos monitoreados con 2 interfaces de red para acceder al

Internet, una de tipo IEEE 802.3 y otra de tipo IEEE 802.11., teniendo la aplicación de monitorización del presente proyecto la capacidad de soportar a cualquiera de éstas o de otro tipo, siempre y cuando se encuentren registradas correctamente en el sistema operativo.

Una limitante que podría tener éste método de determinación de la interfaz de red conectada a Internet, es si el usuario del dispositivo monitoreado forma parte de una red LAN donde se comparte gran cantidad de información multimedia a través de una de sus interfaces de red, y a su vez en otra de sus interfaces de red se accede a Internet, lo que podría provocar la determinación errónea de la interfaz de red monitoreada, cosa que es bastante difícil ya que por lo general éste tipo de usuarios del servicio de Internet habitan dentro de una única LAN a través de la cual acceden a Internet. De todos modos se debe asegurar que para la utilización de ésta aplicación de monitorización el usuario se comprometa a utilizar la misma interfaz de red para conectarse a la LAN y a Internet.

3.4.1.1.2 Captura de Datos de Interfaz de Red

Con el propósito de monitorización, todos los sistemas operativos se encargan de capturar y almacenar información de hardware durante el periodo de tiempo que éstos se encuentren activos, ésto incluye a las interfaces de red, de las cuales se captura y almacena gran cantidad de información, pero para la presente aplicación son de interés los siguientes datos de monitorización:

- Octetos de entrada o recibidos.
- Octetos de salida o enviados.
- Dirección MAC.

El sistema operativo almacena los octetos de entrada y octetos de salida de las interfaces de red de forma acumulativa creciente durante el tiempo que se encuentre éste activo, sin importar que las interfaces de red se encuentren o no transfiriendo datos, por lo que la desconexión de los enlaces conectados a éstas interfaces de red

no reiniciará el valor acumulado de éstos, más si lo hará la desactivación por software de éstas interfaces de red desde el sistema operativo.

Una vez determinada la interfaz de red conectada a internet, se obtiene de ésta los datos referentes a octetos de entrada, octetos de salida y dirección MAC, valores ya capturados y almacenados por el sistema operativo, los mismos que serán obtenidos por la aplicación con la ayuda del API Sigar, Figura 3.4, junto con los métodos *getBytesEntrada, getBytesSalida* y *getDireccionMac* de la clase *MonitorABImplementacionSigar*, Figura 3.3, en intervalos de tiempo determinados en el punto a continuación referente al cálculo de ancho de banda de interfaz de red.

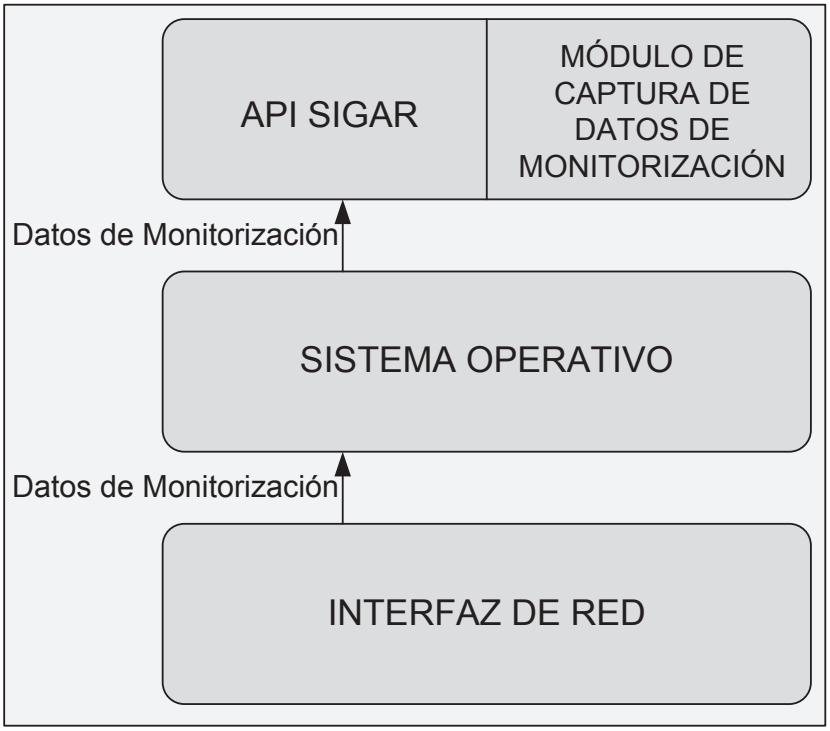


Figura 3.4. Forma de captura de los datos de monitorización por el módulo de captura y cálculo de datos de monitorización.

Los valores de octetos de entrada y de octetos de salida serán posteriormente utilizados para el cálculo de ancho de banda de bajada y de subida, tal como se presenta en el siguiente punto. La dirección MAC de la interfaz de red conectada al

Internet es capturada con el propósito de identificar el origen de los datos de monitorización obtenidos de entre todos los que podrá recibir el presente sistema de monitorización.

3.4.1.1.3 Cálculo de Ancho de Banda de Interfaz de Red

Con los valores obtenidos en la sección anterior correspondientes a octetos de entrada y octetos de salida de la interfaz conectada a Internet, se procede al cálculo del ancho de banda de bajada y al ancho de banda de subida, a través del uso de la fórmula de cálculo de velocidad de transferencia de datos de una interfaz de red a nivel de capa física del modelo OSI, también llamado Bit Rate, Figura 3.5.

$$ABbajada[bps] = \frac{\#bits\ de\ Entrada\ Final - \#bits\ de\ Entrada\ Inicial}{\Delta Tiempo[segundos]}$$

, y

$$ABsubida[bps] = \frac{\#bits\ de\ Salida\ Final - \ \#bits\ de\ Salida\ Inicial}{\Delta Tiempo[segundos]}$$

Figura 3.5. Formulas base para el cálculo de Bit Rate de una interfaz.

En la presente aplicación de monitorización se toman como base éstas formulas para el cálculo de ancho de banda de subida y bajada, usándose en definitiva las formulas indicadas en la Figura 3.6, las mismas que serán implementadas en el método *calculoAB* de la clase *MonitorABImplementacionSigar,* Figura 3.3.

Debido a que los SLAs acordados entre los usuarios residenciales del servicio de Internet y sus proveedores contemplan un ancho de banda máximo medido en bits/segundo (bps), es conveniente calcular el ancho de banda en éstas unidades. Por ésta razón es que la diferencia entre los octetos o Bytes final e inicial, ya sean octetos de entrada o salida, se multiplica por 8, Figura 3.6.

$$ABbajada[bps] = \frac{(OctetosEntradaFinal - OctetosEntradaInicial)[bytes] * 8}{2\ [segundos]}$$

, y

$$ABsubida[bps] = \frac{(OctetosSalidaFinal - OctetosSalidaInicial)[bytes] * 8}{2\ [segundos]}$$

Figura 3.6. Formulas para el cálculo de ancho de banda, utilizadas por la aplicación.

Para la utilización de éstas formulas de cálculo de ancho de banda, es necesario tener 2 mediciones distintas tomadas en distintos instantes de tiempo. El periodo de tiempo elegido para la captura de datos de monitorización y para el posterior cálculo de ancho de banda, es el de 2 segundos. Éste periodo de tiempo ha sido determinado después de varias pruebas y tras el análisis de utilización promedio del servicio de Internet, Tabla 3.3, demostrando ser el menor periodo de tiempo posible para el cual se obtienen resultados de ancho de banda confiables.

Tabla 3.3. Análisis de utilización promedio del servicio de Internet en Ecuador.

Peso página web promedio	Velocidad de acceso residencial fijo a Internet promedio en Ecuador	Tiempo de carga de página web
1.5 MBytes[9]	438 KBps (3.5Kbps)[10]	3.42 segundos

El ancho de banda calculado por éste módulo, a través de la fórmula de la Figura 3.6, puede ser únicamente cero u otro valor positivo mayor a cero. El ancho de banda obtenido es cero en el caso de que no exista actividad de consumo de Internet en el usuario monitoreado. La aplicación de monitorización del presente proyecto almacenará el ancho de banda igual a cero con el propósito de tener constancia de la disponibilidad del servicio de Internet por parte del usuario en el instante que se ha

[9] Fuente: http://www.websiteoptimization.com/speed/tweak/average-web-page/
[10] Fuente: http://www.cepal.org/publicaciones/xml/9/48449/estadobandaanchaenamlc.pdf

tomado la medición, y para el posterior cálculo del índice de disponibilidad del servicio, el mismo que se realiza en el módulo Servicio Web de Intranet en el lado del servidor de la aplicación.

El método expuesto en éste punto para el cálculo del ancho de banda de bajada y subida, puede permitir o no el cálculo del ancho de banda máximo disponible por el canal de acceso a Internet, ésto depende del nivel de utilización que le da el usuario monitoreado a su conexión de Internet. Ésto quiere decir que se obtendrán valores de ancho de banda más cercanos a la capacidad máxima disponible cuando los usuarios utilicen aplicaciones que saturen su canal de acceso a Internet.

De igual forma si los usuarios utilizan mínimamente la capacidad de su conexión a Internet, el cálculo de ancho de banda de bajada y subida será extremadamente sensible al periodo de tiempo en el que se tomen las muestras, por lo que es recomendable hacerlo en el menor tiempo posible para obtener resultados más cercanos posibles a la realidad.

La incapacidad de la aplicación de capturar en todo momento el ancho de banda máximo disponible por el canal no es crítico ya que los proveedores de Internet están únicamente comprometidos con sus clientes a través de sus SLAs, a proveer un ancho de banda máximo, y si el cliente percibe que su capacidad de acceso a internet no es la acordada será porque precisamente hará uso de aplicaciones que saturan su conexión, instancia en la cual la aplicación brinda resultados más precisos.

En el caso de que sea posible la medición del ancho de banda máximo al que tiene acceso el dispositivo del usuario del servicio de Internet monitoreado, la precisión de ésta se verá condicionada si en la LAN del usuario existen otros dispositivos que simultáneamente acceden a la misma conexión de Internet. Por éste motivo, el usuario monitoreado debe asegurar que su dispositivo sea el único accediendo a la conexión a Internet durante el tiempo que se realicen las pruebas de monitorización.

El método de cálculo de ancho de banda utilizado en éste módulo, es independiente del tipo de aplicaciones que hagan uso del servicio de Internet ya que éste se obtiene en base a los octetos de entrada y salida a nivel de capa física en donde no se hace ninguna distinción por tipo de aplicación, por lo tanto, la presente aplicación no afectará en el cálculo de ancho de banda.

Los valores de monitorización, ancho debanda de bajada, ancho de banda de subida y dirección MAC, obtenidos hasta aquí, son representados por las variables *ABBajada*, *ABSubida* y *DireccionMAC*, respectivamente. Éstas variables tienen las características detalladas en la tabla 3.4, las mismas que serán replicadas por los subsiguientes módulos de la Aplicación de Monitorización.

Tabla 3.4. Características de las variables de la aplicación de monitorización.

Variable	Tipo	Tamaño en Memoria [Bytes]
ABBajada	Long	8
ABSubida	Long	8
DireccionMAC	String	17

3.4.1.2 Módulo Agente SNMP Versión 3

Para el desarrollo del Agente SNMP versión 3, se utilizó la librería adventnet, en conjunto con las clases *MonitorABAgenteSNMPv3, MonitorABRequestHandler* y *MonitorABInstrument.* Figura 3.7.

La clase *MonitorABAgenteSNMPv3* es la encargada de ejecutar el agente SNMP versión 3 como tal, a través de la herencia de varios métodos de la clase *SnmpAgent* del API Adventnet, y mediante la aplicación de métodos de la clase *MonitorABRequestHandler.* Además, La clase *MonitorABAgenteSNMPv3* realiza la

función de recibir y responder a las solicitudes SNMP provenientes desde el Módulo Gestor SNMP versión 3.

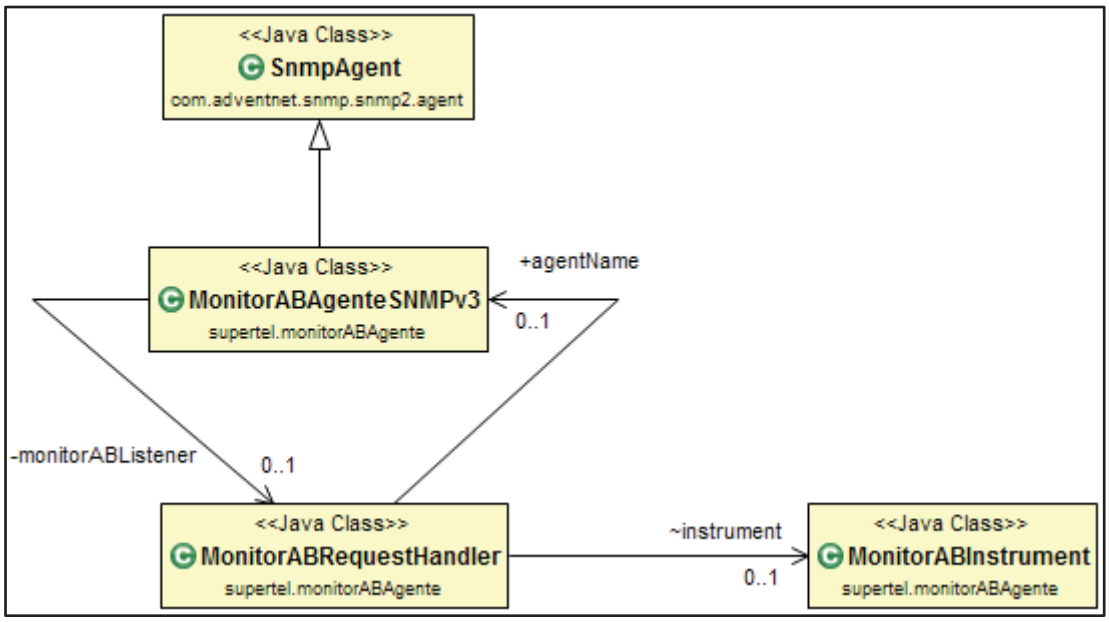


Figura 3.7. Diagrama de clases del módulo agente SNMP versión 3.

Por su parte, la clase *MonitorABRequestHandler* se encarga de procesar las solicitudes de tipo *GetRequest* que arriban al agente SNMP versión 3 y de dar respuesta a éstas a través de la instanciación de la clase *MonitorABInstrument*. La clase *MonitorABRequestHandler,* también implementa las OIDs requeridas y las asocia con los objetos gestionados implementados en la clase *MonitorABInstrument*, Figura 3.8.

La clase *MonitorABInstrument* tiene la función de implementar efectivamente los datos que deben ser devueltos por el Módulo Agente SNMP versión 3, Figura 3.8, a través de sus métodos *getAbBajada, getAbSubida* y *getDireccionMAC*, los mismos que implementan los métodos *calculoAB* y *getDireccionMac* presentes en la clase *MonitorABImplementacionSigar* del módulo de captura y cálculo de datos de monitorización descrito en el punto 3.4.1.1.

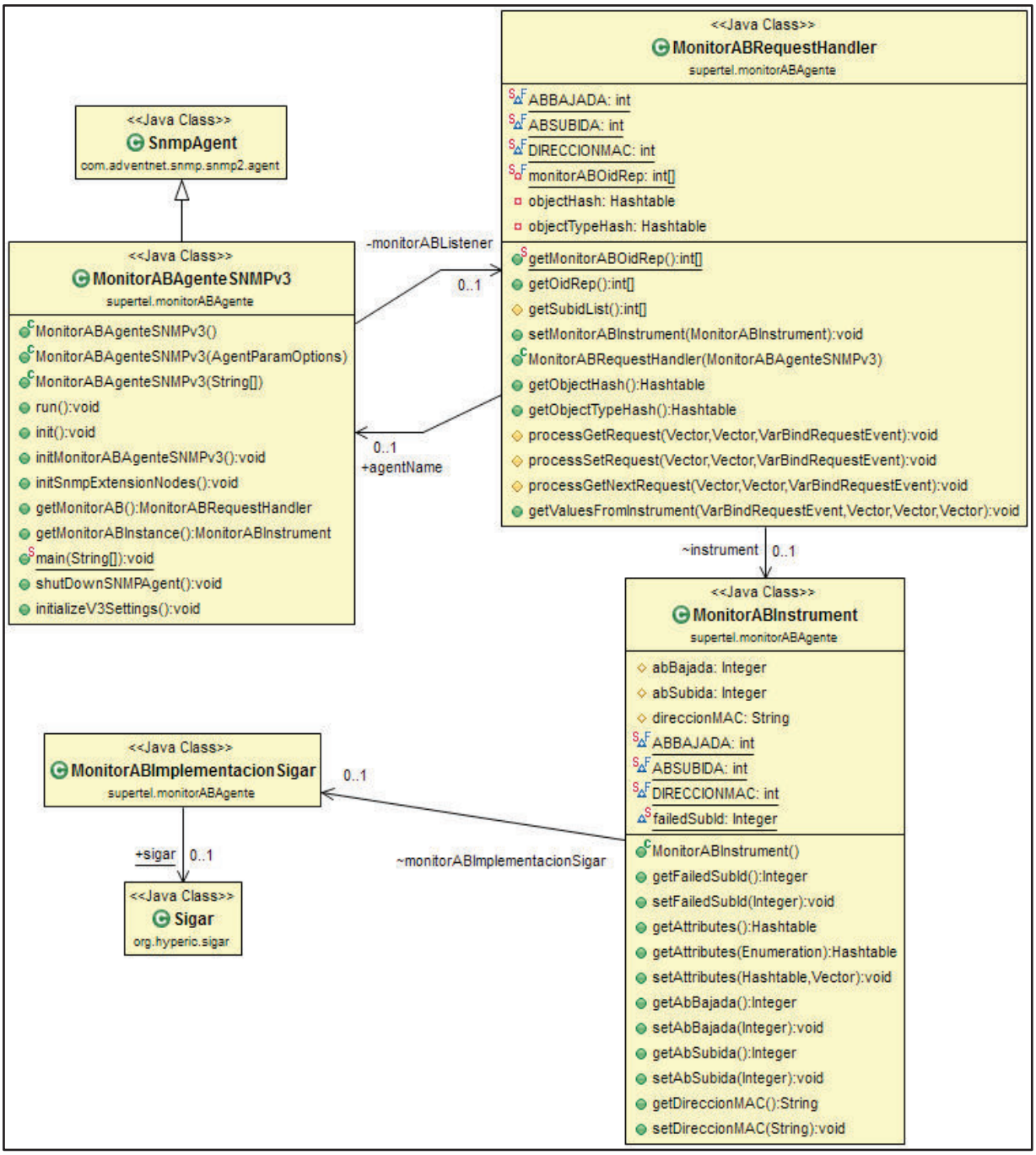


Figura 3.8. Diagrama de clases del módulo agente SNMP versión 3 y su interacción con el módulo de captura y cálculo de datos de monitorización.

El Agente SNMP versión 3 una vez iniciado, atenderá a las consultas SNMP provenientes de gestores SNMP versión 3 a través del puerto UDP 161. Además, el

Agente SNMP versión 3, no implementará notificaciones (traps), ya que no han sido consideradas dentro del funcionamiento de la presente aplicación de monitorización.

3.4.1.2.1 MIBs de la Aplicación de Monitorización

Con el propósito de realizar el monitoreo del ancho de banda presente en los usuarios del servicio de Internet mediante el uso de SNMP versión 3, se han creado algunas MIBs siguiendo las reglas SMI versión 2 y la notación ASN.1. Éstas MIBs se encuentran dentro del nodo del árbol SMI llamado *monitorAB* del nodo *Supertel*, los mismos que se encuentran dentro del nodo *Enterprises*, Figura 3.9. Tanto las MIBs como los nodos fueron creados con la ayuda de la aplicación MIB Editor de WebNMS.

Como se puede observar en la Figura 3.9, se ha asignado el OID número 1 al nodo *Supertel* dentro del nodo *Enterprises*, a pesar de que éste número de OID ya ha sido reservado para otra entidad dentro del registro oficial que lleva IANA, pero al tratarse la presente aplicación de un prototipo no hay ningún inconveniente de manejarlo de ésta forma, además de que éste número de OID puede ser cambiado al que sea asignado por la IANA el momento en que la SUPERTEL aplique para registro del mismo. Por lo tanto todas las MIBS dentro del nodo *Supertel* serán accedidas a través del siguiente OID:

.1.3.6.1.4.1.1

Por lo que el OID para el nodo *monitorAB* de la aplicación será:

.1.3.6.1.4.1.1.1

Las MIBs creadas dentro del nodo *monitorAB,* indicadas en la Figura 3.9, se describe en la tabla 3.5, y su completa definición en notación ASN.1 se encuentra en el archivo llamado *MonitorABModulo* en los anexos de éste documento.

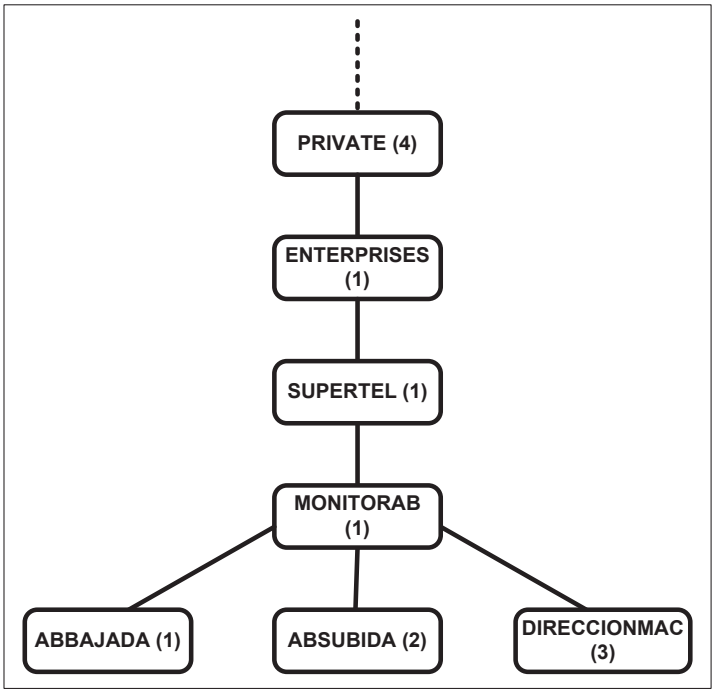


Figura 3.9. Parte del árbol SMI donde se ilustra el nodo Supertel.

Tabla 3.5. Características de las MIBs del nodo MonitorAB.

Nombre	Syntax	Max-Access	Status	OID
abBajada	Integer32	Read-only	current	.1.3.6.1.4.1.1.1.1
abSubida	Integer32	Read-only	current	.1.3.6.1.4.1.1.1.2
direccionMAC	DisplayString	Read-only	current	.1.3.6.1.4.1.1.1.3

La MIB *abBajada* se encarga de almacenar la información del objeto gestionado ancho de banda de bajada, por su parte la MIB *abSubida* almacena información del objeto gestionado ancho de banda subida, y la MIB *direccionMAC* guarda la información del objeto gestionado dirección MAC de la interfaz de red conectada a Internet del dispositivo monitoreado.

Las consultas SNMP que se realizan simultáneamente a las MIBs *abBajada* y *abSubida*, tardan 4 segundos en retornar respuesta, debido a que la clase

*MonitorABRequestHandler*del Agente SNMP, atiende a todas las solicitudes SNMP *GetRequest* de forma secuencial, lo que ocasiona que el ancho de banda de bajada y el ancho de banda de subida no sean calculados de forma simultánea, y tengan una diferencia de tiempo de captura de 2 segundos.

3.4.1.2.2 Seguridad del Agente SNMP

Al ser el agente SNMP de versión 3 el implementado en la presente aplicación, se garantiza: la autenticación segura de los Gestores SNMP autorizados a realizar consultas a éste agente SNMP, y la encriptación de la información SNMP compartida entre éstos.

De los protocolos de seguridad disponibles por SNMP y el API Adventnet, en base al cual se desarrolla la presente aplicación de monitorización, se ha elegido como nivel de seguridad USM a *authPriv* mediante el uso del protocolo de autenticación SHA sobre MD5, por su mayor robustez frente a ataques de resistencia de colisión[11], y del protocolo de encriptación AES sobre DES por ser un protocolo más seguro frente ataques diferenciales, de interpolación, etc.[12].

En la práctica será difícil que la nueva aplicación; especialmente en éste módulo, se enfrente a ataques de éste tipo, por lo que la utilización de éstos protocolos no es crítica pero de todos modos se han añadido en éste módulo con el fin de disponer de la mayor seguridad posible a éste nivel.

3.4.1.3 Módulo Gestor SNMP Versión 3

El Gestor SNMP versión 3, contenido en la clase *MonitorABGestorSNMPv3,* se encuentra implementado en base a la clase *SnmpTarget* de la librería Adventnet. La clase *MonitorABGestorSNMPv3* utiliza el método *consultaSNMP* para realizar las

[11] Fuente: http://security.stackexchange.com/questions/19705/is-sha1-better-than-md5-only-because-it-generates-a-hash-of-160-bits
[12] Fuente: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_4-2/goodbye_des.html

consultas SNMP versión 3 al Agente SNMP versión 3 ubicado en el módulo Agente SNMP versión 3. Figura 3.10.

Las variables en donde se almacena la información enviada desde el Agente SNMP, en respuesta a las consultas realizadas por el Gestor SNMP, son *ABBajada*, *ABSubida* y *DireccionMac* de la clase *MonitorABGestorSNMPv3,* Figura 3.10.

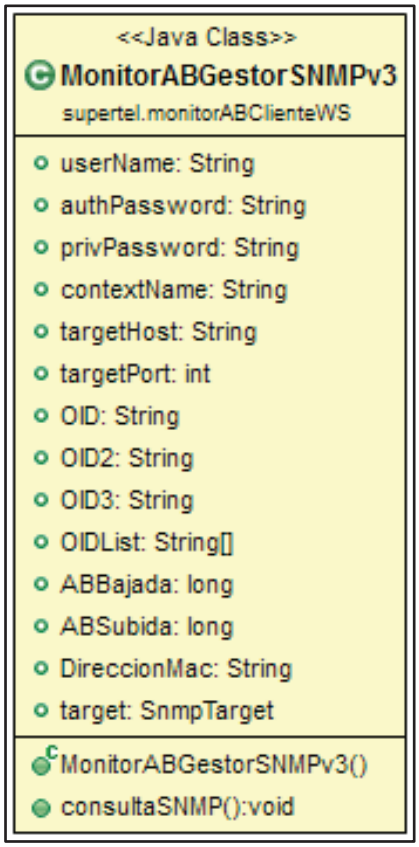


Figura 3.10. Diagrama de Clases del módulo Gestor SNMP versión 3.

Éste módulo realiza la consulta de los datos de monitorización relacionados con los objetos gestionados de ancho de banda de bajada, ancho de banda de subida y dirección MAC almacenados en las MIBs *abBajada*, *abSubida* y *direccionMAC* respectivamente, a través de solicitudes de tipo *GetRequest* encapsuladas dentro del método *snmpGetList,* propio de la clase *SnmpTarget* del API Adenvetnet. La respuesta por parte del Agente SNMP será un arreglo o array con tres datos,

correspondientes a la información almacenada en ese momento en las MIBs *abBajada*, *abSubida* y *direccionMAC.*Figura 3.11.

Después de haber recibido respuesta desde el Agente SNMP, inmediatamente se efectúa una nueva consulta, sin pausa una tras otra, durante el tiempo en el cual el dispositivo monitoreado se encuentre activo. El único periodo de espera que tiene el Gestor SNMP para hacer consultas, es durante el tiempo que toma el módulo de captura y cálculo de datos de monitorización en calcular el ancho de banda de bajada y ancho de banda de subida, es decir 4 segundos ya que 2 segundos requiere para el cálculo de ancho de banda de bajada y 2 segundos para el cálculo de ancho de banda de subida.

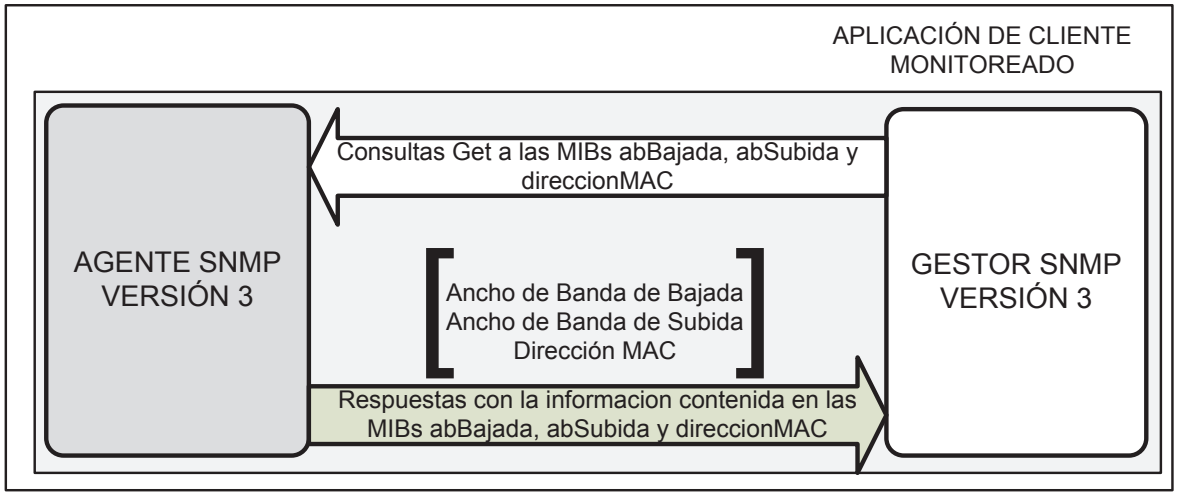


Figura 3.11. Comunicación entre el Gestor SNMP versión 3 y el Agente SNMP versión 3.

3.4.1.3.1 Localización del Gestor SNMP Versión 3

El Gestor SNMP versión 3, se encuentra ubicado en el mismo dispositivo donde se realiza la captura de datos de monitorización del servicio de Internet, funcionando junto al Agente SNMP versión 3. Figura 3.1, ésto debido principalmente a la limitante que tiene la arquitectura ADSL utilizada por el proveedor de Internet CNT, para

proveer direcciones IP públicas de manera gratuita en conjunto con la prestación del servicio de Internet.

Éste factor indudablemente desanimaría la utilización de ésta aplicación de monitoreo debido al gasto económico adicional que conllevaría a los clientes de éste proveedor o a la misma SUPERTEL si pretende distribuirlo masivamente. Por lo pronto, el alcance de éste proyecto contempla un par de usuarios de prueba pertenecientes al ISP CNT.

Otra razón de peso que obligó a ubicar al Gestor SNMP en el lado del cliente del servicio de Internet, fue la necesidad de incorporar la aplicación presentada en éste documento, a la arquitectura actual usada por la SUPERTEL para la implementación de sus aplicaciones distribuidas, Servicios Web de JEE (Java Enterprise Edition), tal como se comentó en el punto de selección de la arquitectura.

Si fuese necesario y si la arquitectura utilizada por el proveedor de Internet donde funciona el dispositivo monitoreado lo permite, el Agente SNMP versión 3 puede ser consultado por otro Gestor SNMP versión 3 diferente al implementado en el módulo Gestor SNMP versión 3, siempre y cuando éste esté autorizado y cuente con las credenciales necesarias, pero por el momento ésto se encuentra fuera del alcance del presente proyecto.

3.4.1.4 Módulo Cliente del Servicio Web para el envío de mediciones

El Módulo Cliente del Servicio Web para el Envío de Mediciones es un cliente JAX-WS, de la aplicación corporativa JEE para la monitorización de clientes residenciales del servicio de Internet. En éste módulo se realizan de manera general las siguientes funciones:

- Implementación y conexión del Servicio Web.
- Conversión de objetos Java a contenido XML.

Éste módulo se encarga de tomar los valores de monitorización capturados por el Módulo Gestor SNMP version3; Figura 3.12, y junto con la fecha de la medición, Tabla 3.6, que es capturada por la clase *MonitorABClienteWSAplicacion* del presente módulo, los envía al Servidor del Servicio Web, Figura 3.13.

De éste modo la siguiente información de la interfaz de red conectada a Internet del dispositivo monitoreado es enviada desde el Cliente del Servicio Web al Servidor del Servicio Web cada 4 segundos:

- El ancho de banda de bajada en ese instante.
- El ancho de banda de subida en ese instante.
- La dirección MAC.
- La fecha de captura de los datos de monitorización.

La fecha de captura de medición, tiene el siguiente formato:

yyyy/MM/dd_HH:mm:ss

Tabla 3.6. Características de la variable fecha.

Variable	Tipo	Tamaño en Memoria [Bytes]
Fecha	String	19

Los datos de monitorización obtenidos por éste módulo son enviados uno tras otro sin pausa al servidor de servicios web, durante el tiempo en el cual el dispositivo monitoreado se encuentre activo. En el caso de que el servidor de servicios web no sea accesible por cualquier causa, el cliente del servicio web reintentará el envío de datos de monitorización durante el tiempo en el que se encuentre activo, desechándose todas aquellas mediciones capturadas en el periodo de tiempo en el cual no existió conexión para el consumo del servicio web.

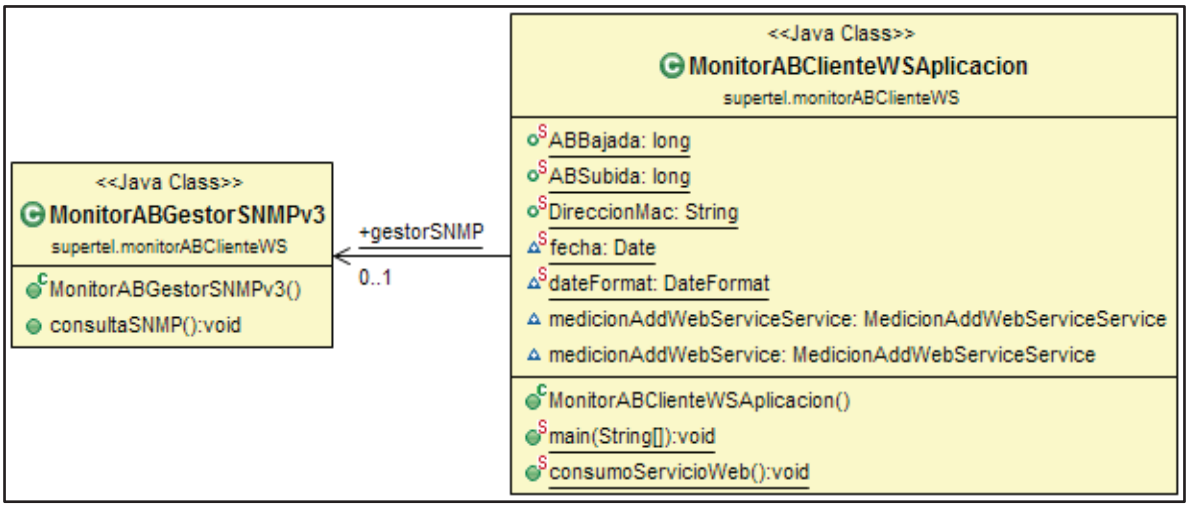


Figura 3.12. Diagrama de Clases para la interacción entre el módulo Gestor SNMP y el módulo Cliente del Servicio Web para el envío de Mediciones.

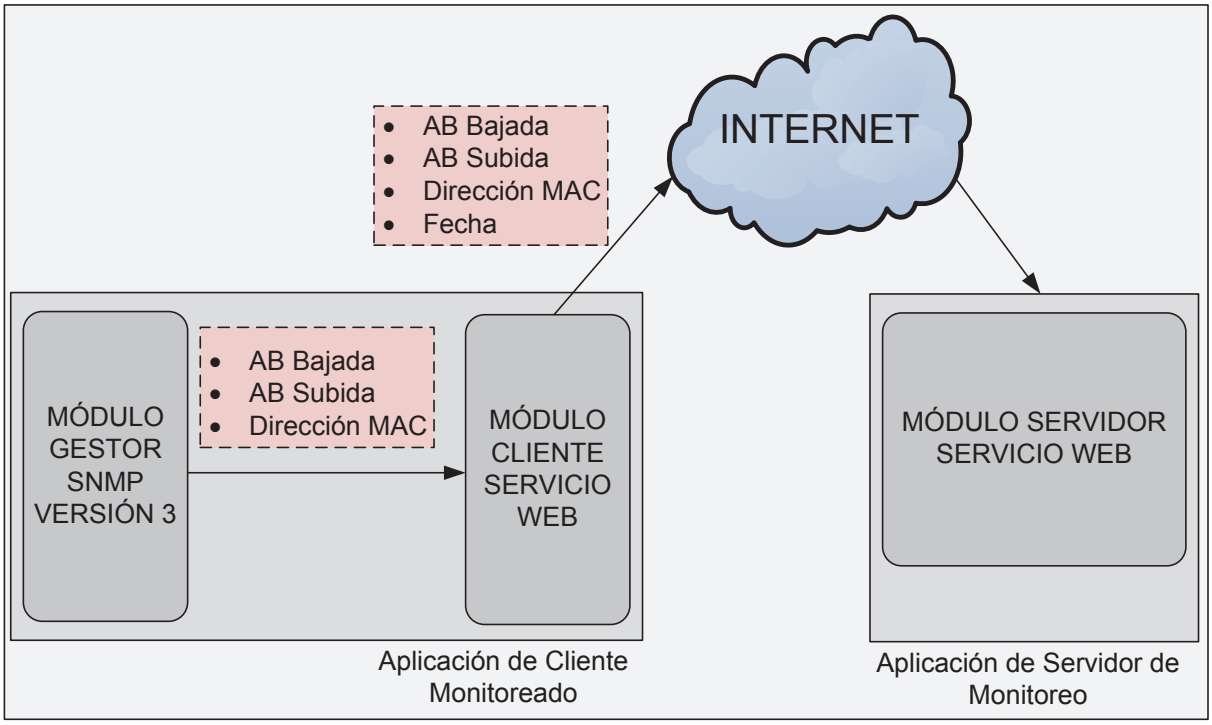


Figura 3.13. Datos de de monitorización enviados entre los módulos que participan en el consumo del Servicio Web.

3.4.1.4.1 Implementación y Conexión del Servicio Web

En éste módulo se implementa el Cliente del Servicio Web que consumirá el Servicio Web dedicado al monitoreo de ancho de banda, el mismo que se encuentra publicado en el Internet por el Servidor del Servicio Web ubicado en la Superintendencia de Telecomunicaciones. La clase encargada de realizar ésta labor será la clase *MonitorABClienteWSAplicacion*, Figura 3.14.

La clase *MedicionAddWebServiceService* es la encargada de establecer la conexión HTTP a nivel de capa Aplicación, estableciéndose en ésta, la URL donde funciona el Servidor del Servicio Web, al que deben ser enviados los datos de monitorización. Por lo tanto, la aplicación de monitorización utiliza al protocolo HTTP para el transporte de información y establecimiento de la conexión a nivel de capa Aplicación, entre el Cliente y el Servidor del Servicio Web.

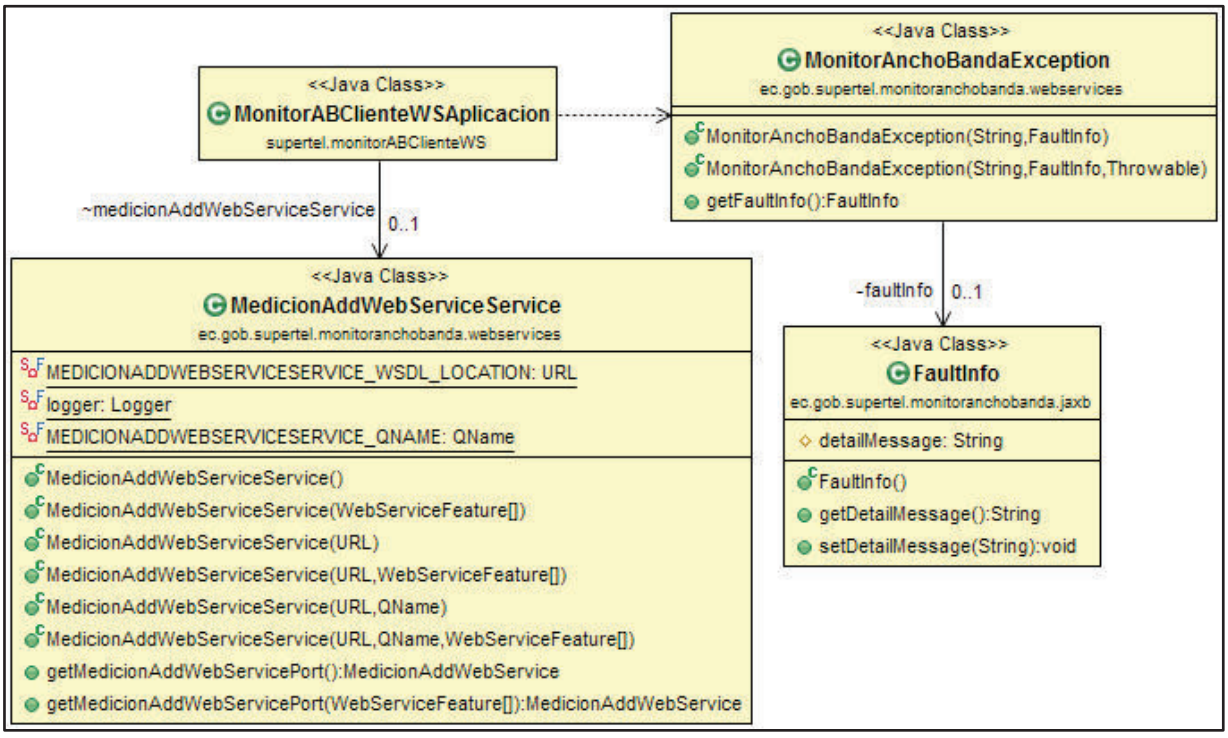


Figura 3.14. Diagrama de clases para la implementación y Conexión del Servicio Web dentro del módulo Cliente del Servicio Web para el envío de Mediciones.

La clases *MonitorAnchoBandaException* y *FaulInfo* son las encargas de determinar los posibles fallos que puedan ocurrir en el establecimiento de la conexión con el Servidor del Servicio Web, para que puedan ser expuestos por la clase ejecutable *MonitorABClienteWSAplicacion*.

3.4.1.4.2 Conversión de Objetos Java a Contenido XML

Los datos de monitorización obtenidos hasta éste punto, se encuentran definidos mediante Objetos Java, y para que éstos puedan consumir el Servicio Web publicado en el Servidor del Servicio Web, es necesario que sean convertidos a lenguaje XML y encapsulados en mensajes SOAP. Al proceso de conversión de objetos Java a XML se le denomina Binding de datos, y se lo realiza con la ayuda del API JAXB[13].

Cabe mencionar aquí, que en el lado del Servidor del Servicio Web se crearon las clases Bean JPA (o entidades Bean JPA) *Medición* y *Usuario*, las mismas que serán explicadas en detalle en éste documento en puntos posteriores. Por el momento es necesario saber que la clase *Medición* es la que contendrá la información obtenida de la monitorización en el lado del Servidor de la Aplicación de Monitorización (en la SUPERTEL), y que ésta forma parte de la clase *Usuario* también localizada en éste servidor.

Para que el Cliente del Servicio Web pueda consumir el Servicio Web, es necesario especificar aquí a las clases *Medición* y *Usuario*, las mismas que deberán contener la información de monitorización hasta éste momento capturada. Éstas clases se encuentran especificadas en el Cliente del Servicio Web a través de las clases *MedicionType* y *UsuarioType,* Figura 3.15, las mismas que definen su esquema de conversión a XML.

El Servicio Web publicado en el Servidor del Servicio Web contiene una clase llamada *AddMedicion* (posteriormente definido en éste documento) que básicamente

[13] Fuente: http://docs.oracle.com/cd/E13222_01/wls/docs103/webserv/data_types.html

se encarga de añadir nuevas mediciones en la base de datos de la aplicación. Con el propósito de poder consumir éste Servicio Web, las clases *AddMedicion* y *AddMedicionResponse,* Figura 3.15, contienen el esquema de conversión a XML para poder acceder a la clase *AddMedicion*, desde el Cliente del Servicio Web.

La clase *MedicionAddWebService*, Figura 3.15 se encarga de realizar la conversión o Marshalling[14] de los datos de monitorización capturados, en base a los esquemas de conversión definidos por las clases *MedicionType, UsuarioType, AddMedicion* y *AddMedicionResponse*. Por su parte, la clase *ObjectFactory* contiene métodos para la creación de otros objetos *MedicionType* y *UsuarioType.*

La forma en que se realiza el Marshalling de objetos Java a contenido XML de los datos de monitorización, y la posterior encapsulación del contenido XML dentro de mensajes SOAP, se detalla en la Figura 3.16.

Todos los mensajes SOAP con información de monitorización generados por la presente aplicación, serán transmitidos en una sola dirección, siempre desde los Clientes hacia el Servidor del Servicio Web. Figura 3.17.

Hasta éste punto llega el diseño e implementación del módulo Aplicación Cliente Monitoreado ubicado en el usuario del servicio de Internet monitoreado. En la Figura 3.18, se detalla el diagrama de secuencia para éste módulo.

[14] Termino computacional en inglés utilizado para la denominación del proceso de conversión de un objeto a un formato de representación diferente. Fuente: https://docs.oracle.com/javase/tutorial/jaxb/intro/arch.html

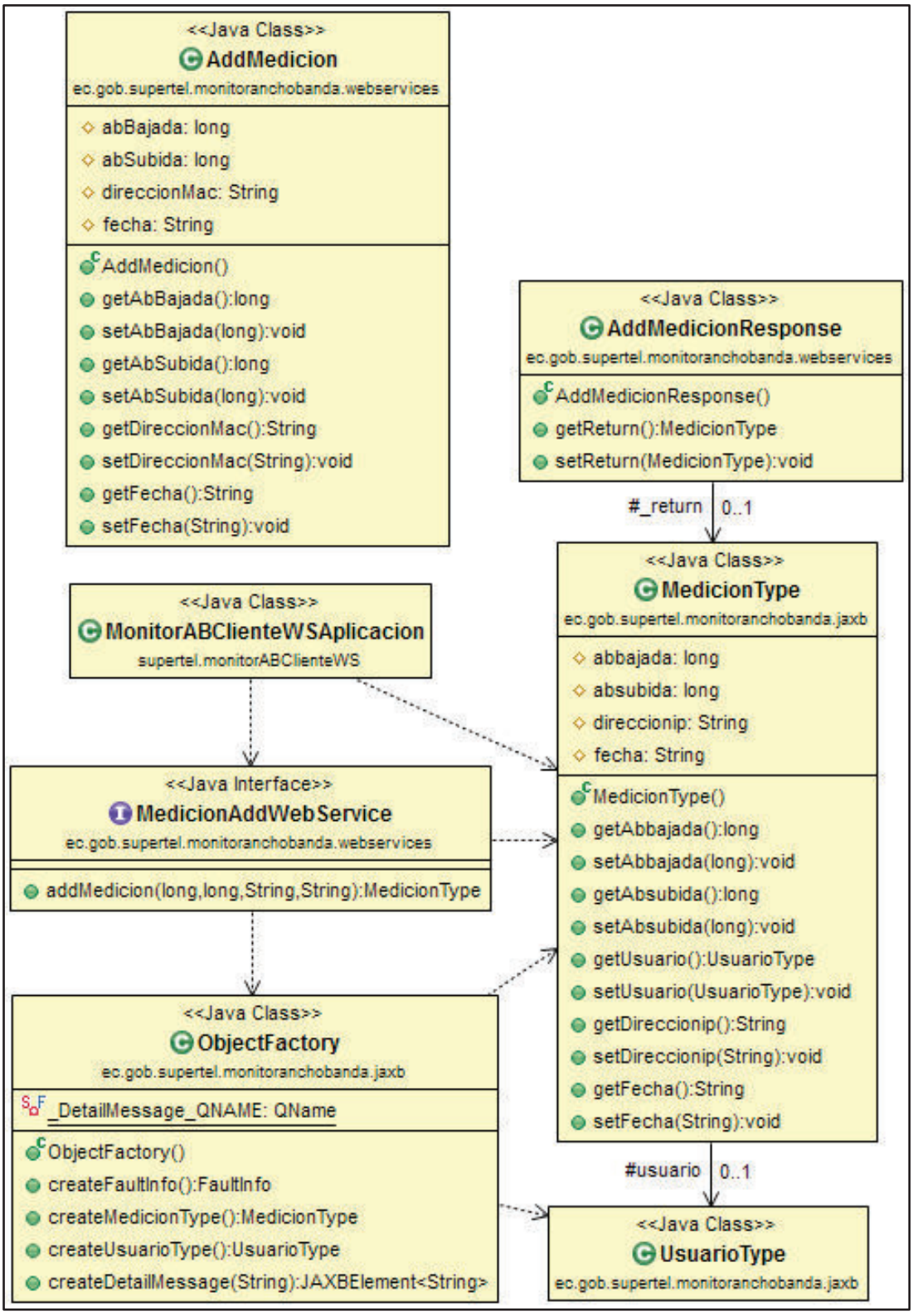


Figura 3.15. Diagrama de clases para la conversión de objetos Java en contenido XML.

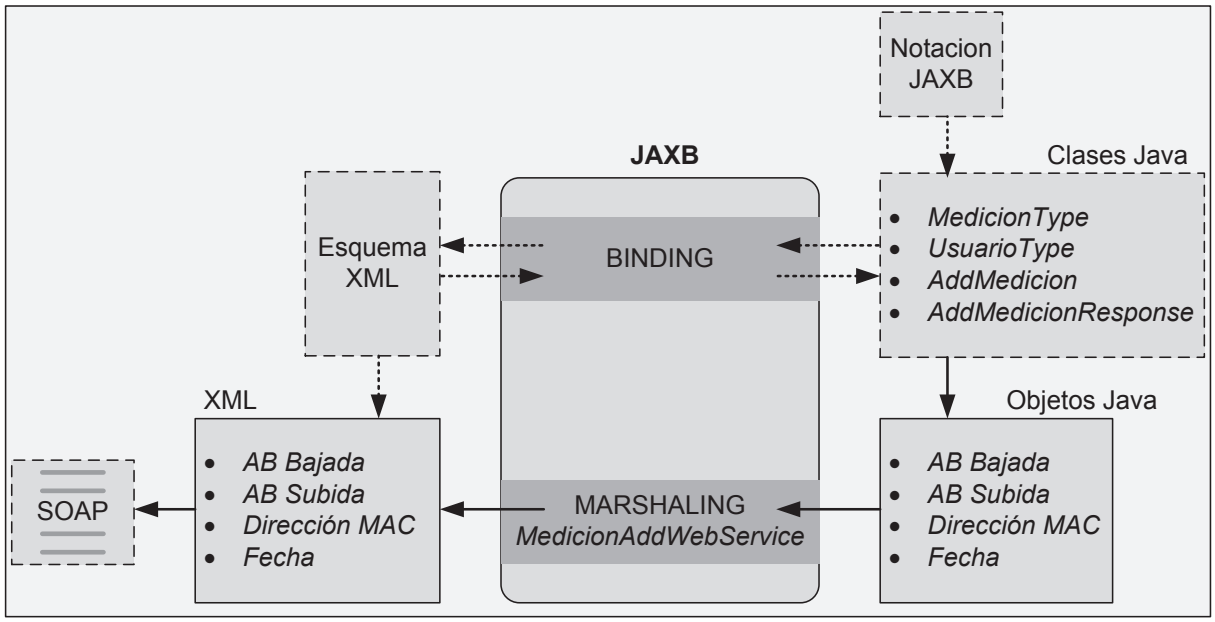


Figura 3.16. Conversión de Objetos Java a contenido XML en el Cliente del servicio web para el envío de Mediciones.

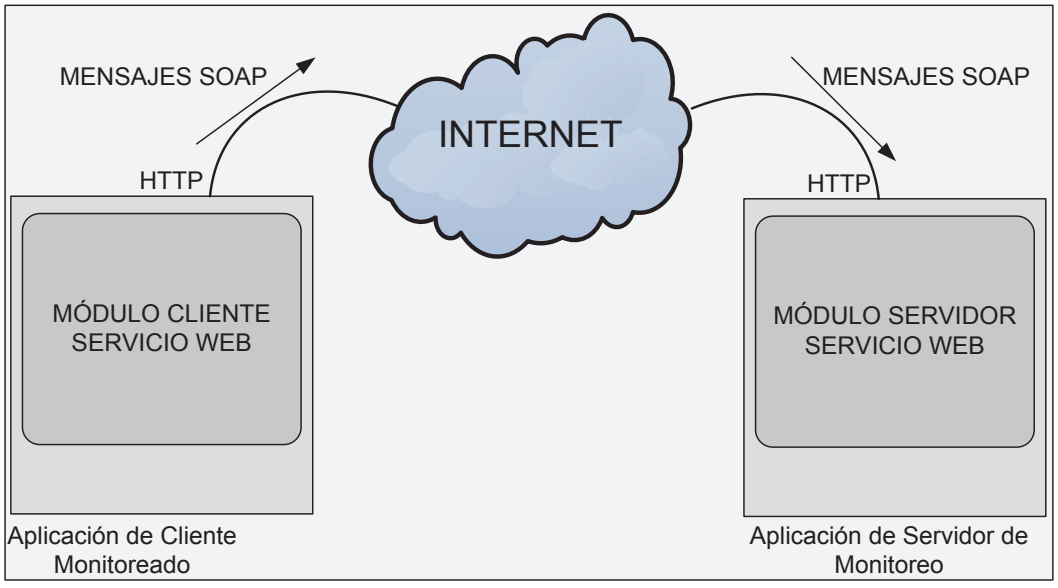


Figura 3.17. Mensajes SOAP entre el Cliente y el Servidor del Servicio Web.

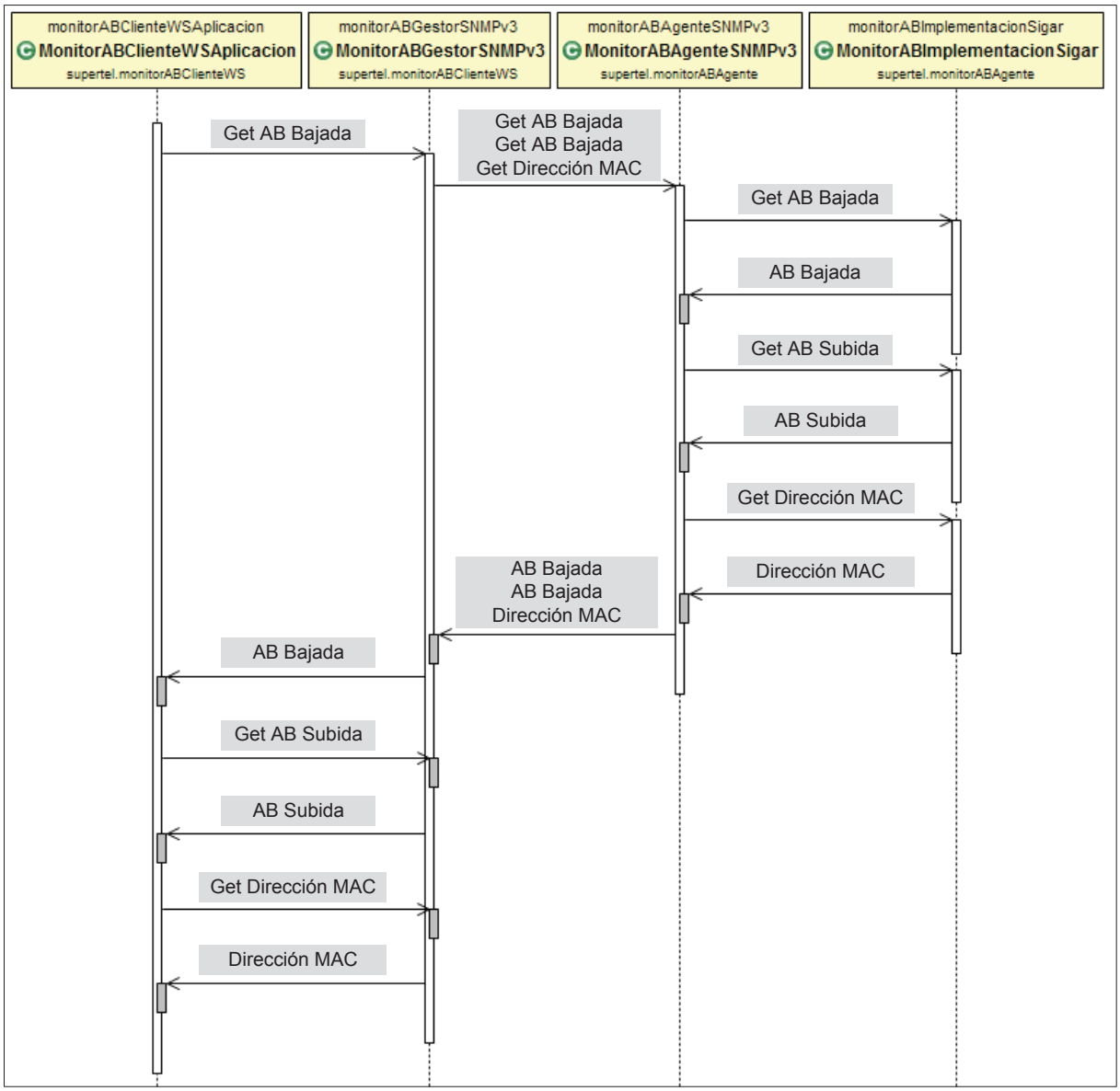


Figura 3.18. Diagrama de Secuencia del Módulo Aplicación de Cliente Monitoreado.

3.4.2 MÓDULO APLICACIÓN DE SERVIDOR DE MONITOREO

Éste módulo consiste en una aplicación corporativa JEE, localizada en la SUPERTEL, y que se encuentra conformada por los siguientes sub-módulos, Figura 3.19:

- Módulo Base de Datos.

- Módulo Sistema de persistencia.
- Módulo Servidor Servicio Web.
- Módulo Cliente del Servicio Web de Consultas.

Básicamente, éstos sub-módulos se encargan de la recepción, almacenamiento y consulta de los datos de monitorización enviados desde los clientes monitorizados.

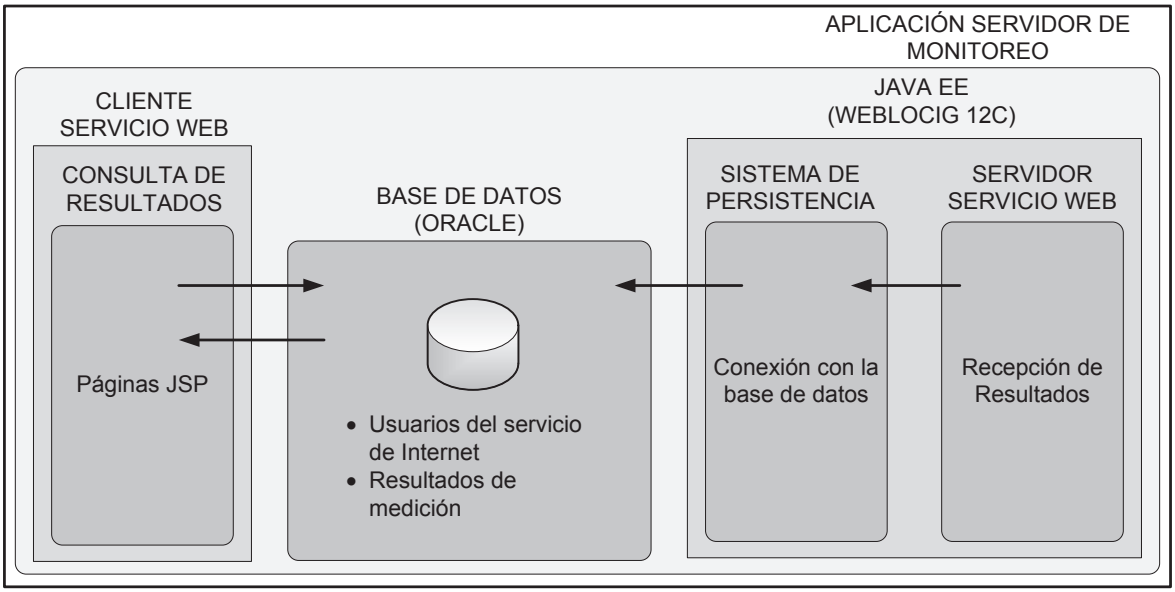


Figura 3.19. Módulo Aplicación Servidor de Monitoreo.

3.4.2.1 Módulo Base de Datos

Éste módulo constituye el nivel de Sistema de Información de la aplicación corporativa JEE para la monitorización, siendo éste el encargado de almacenar los datos de monitorización capturados, en una base de datos relacional en la que se ha creado el esquema o usuario llamado MonitorABUsuario, Figura 3.20.

La base de datos utilizada y presentada aquí a manera de prototipo, es Oracle Database XE 11.2, ya que como se determinó en el análisis de la situación actual, la SUPERTEL maneja una base de datos Oracle 10g, por lo que, la presente aplicación de monitoreo será completamente compatible con los recursos de hardware y software de la SUPERTEL relacionados con el almacenamiento de datos.

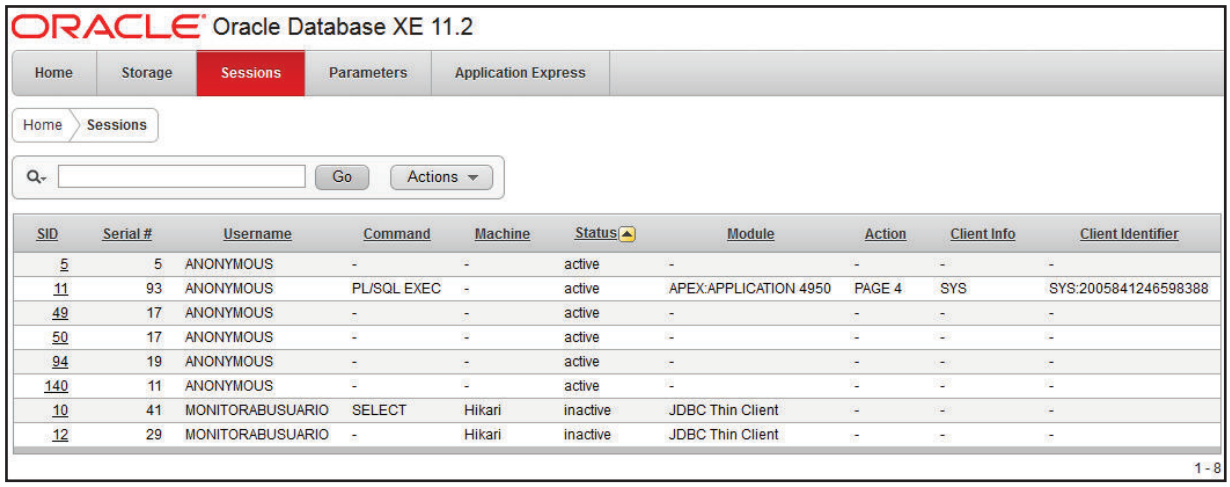


Figura 3.20. Usuario MonitorABUsuario de la base de datos Oracle XE 11.2.

En base a los análisis de los requerimientos funcionales de la nueva aplicación de monitorización de éste proyecto, se ha determinado que el dominio de datos MonitorABUsuario debe contar con 2 tablas:

- Usuario.
- Medición.

Éstas tablas se encuentran relacionadas entre sí de acuerdo al modelo relacional presentado en la Figura 3.21, en la cual se puede observar que un usuario tiene ninguna o muchas mediciones.

La tabla Usuario será la encargada de almacenar toda la información referente a los usuarios monitorizados, tabla 3.7, y la tabla Medición almacenará la información de las mediciones recibidas desde la Aplicación de Cliente Monitoreado, tabla 3.8.

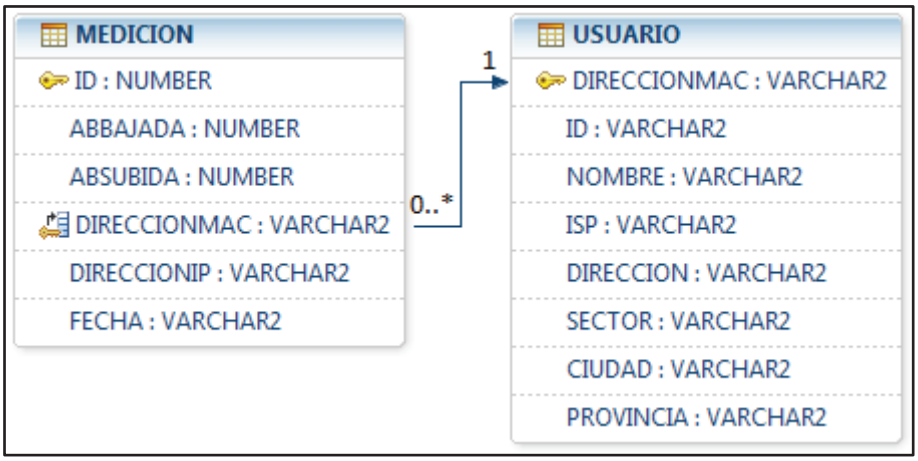


Figura 3.21. Modelo relacional del dominio de datos MonitorABUsuario.

Tabla 3.7. Información contenida en la tabla Usuario.

Campo	Descripción	Tipo	Tamaño [Bytes]	Requerido
DIRECCIONMAC	Dirección MAC del dispositivo monitoreado.	VARCHAR2	17	Sí
ID	Identificación del usuario del dispositivo.	VARCHAR2	10	Sí
NOMBRE	Nombre del usuario del dispositivo.	VARCHAR2	50	Sí
ISP	Nombre del ISP del usuario.	VARCHAR2	30	Sí
DIRECCION	Dirección de la residencia del usuario.	VARCHAR2	50	No
SECTOR	Barrio o sector de residencia del usuario.	VARCHAR2	30	No

Campo	Descripción	Tipo	Tamaño [Bytes]	Requerido
CIUDAD	Ciudad de residencia del usuario.	VARCHAR2	30	No
PROVINCIA	Provincia de residencia del usuario	VARCHAR2	20	No
Tamaño total por registro [Bytes]			237	

Tabla 3.8. Información contenida en la tabla Medición.

Campo	Descripción	Tipo	Tamaño [Bytes]	Requerido
ID	Identificación de la medición.	NUMBER	22	Sí
ABBAJADA	Ancho de banda de bajada de la medición.	NUMBER	22	Sí
ABSUBIDA	Ancho de banda de subida de la medición.	NUMBER	22	Sí
DIRECCIONMAC	Dirección MAC de la medición.	VARCHAR2	17	Sí
DIRECCIONIP	Dirección IP v4 de la medición.	VARCHAR2	15	Sí
FECHA	Fecha de la medición.	VARCHAR2	19	Sí
Tamaño total por registro [Bytes]			117	

El tamaño de los campos indicados en las tablas 3.6 y 3.7, para los registros de tipo VARCHAR2, representa el tamaño máximo en bytes de almacenamiento, y se asigna de acuerdo al número de caracteres máximo que debe tener cada registro que será almacenado en éstos campos. Se indica ésto, para no generar confusión con el tamaño en bytes de transmisión que puedan tener la dirección MAC y dirección IP, que es diferente a su tamaño en bytes de almacenamiento.

El campo DIRECCIONMAC es la llave primaria de la tabla Usuario, usada en la tabla Medición como llave foránea, para la asociación de los registros de la Tabla Medición con los registros de la tabla Usuario.

3.4.2.1.1 Estimación de utilización de la base de datos

En el análisis de la situación actual de los recursos de hardware y software de la SUPERTEL, se determinó la disponibilidad del espacio de almacenamiento con el que cuenta la base de datos de ésta entidad. Con el propósito de que la nueva aplicación pueda ser implementada usando la base de datos actual de la SUPERTEL, es necesario calcular el espacio de utilización que requerirá la nueva aplicación en base al tamaño en disco que puedan tener los registros de las tablas Usuario y Medición, Tabla 3.9.

Tabla 3.9. Estimación de utilización de la base de datos para un usuario

Número de Mediciones / Periodo de tiempo	Tamaño de la tabla Usuario [Bytes]	Tamaño de la tabla Medición [Bytes]	Tamaño total ocupado en la Base de Datos [Bytes]
900 / 1 hora	237	105,300	105,537
21,600 / 1 día	237	2,527,200	2,527,437
648,000 / 30 días	237	75,816,000	75,816,237

La estimación de utilización de la base de datos por parte de la aplicación, se calculó para un usuario monitorizado que envía una medición cada 4 segundos.

La capacidad de almacenamiento utilizada por la aplicación para un usuario y sus mediciones en un mes, es de aproximadamente 76 MBytes. Éste espacio de almacenamiento es considerable, pero representa el 0.0008 % de la capacidad total disponible en la base de datos; que como se vío en el capítulo de análisis, es de 12 TBytes.

3.4.2.1.2 Conexión de la Aplicación con la base de datos

Para que la aplicación de monitorización pueda acceder a la base de datos, requiere establecer una conexión con ésta, por medio de la definición de la siguiente información, tabla 3.10:

- Localización de la base de datos.
- Nombre de usuario o esquema.
- Contraseña del usuario.
- API JDBC apropiado para la base de datos Oracle.

Tabla 3.10. Información para la conexión con la base de datos.

Localización	jdbc:oracle:thin:@localhost:1521:xe
Nombre de Usuario	MonitorABUsuario
Contraseña de Usuario	supertel123
API JDBC	oracle.jdbc.OracleDriver

Debido a que en el dispositivo donde funciona el Servidor del Servicio Web prototipo, funciona también la base de datos, la información de la localización para la conexión contiene la dirección IP local (localhost), como se ve en la tabla 3.8.

3.4.2.2 Módulo Sistema de Persistencia

Éste módulo representa una parte del nivel de Negocio JEE de la aplicación corporativa de monitorización, en la cual se realiza la función de mapear los datos relacionales de la base de datos en objetos Java y de garantizar integridad transaccional, a través del framework Spring y del API JPA. Los objetos Java obtenidos permitirán a la aplicación manipular y consultar la información contenida en la base de datos. La configuración del framework Spring se encuentra definida en el archivo XML *applicationContext.xml*, incluida junto con éste documento en la sección de anexos.

Las clases *Usuario* y *Medicion*, Figura 3.22, serán las entidades Bean JPA, Figura 3.23, a través de las cuales se hará el mapeo a objetos Java, de los datos relacionales de las tablas Usuario y Medición de la base de datos. Éstas clases contienen en su código notación JPA, por medio de la cual son capaces de realizar el mapeo.

El API JPA usa como contexto de mapeo entre datos relacionales y objetos Java, al archivo *persistence.xml* (adjunto en los anexos del presente documento) escrito en lenguaje XML, en el que se definen, el nombre de la unidad de persistencia, el nombre y ubicación de las clases Java relacionadas con las tablas de la base de datos, y la información de la conexión, necesaria para la comunicación entre la aplicación con la base de datos, indicada ya en la tabla 3.8.

Una vez definidas las entidades Bean JPA *Usuario* y *Medicion*, se procede a la implementación (manipulación y consulta) de la información contenida en las tablas Medición y Usuario de la base de datos, a través de la instanciación de éstas entidades Bean JPA dentro de clases Java DAO (Data Access Object), Figura 3.24.

Básicamente, se crean 3 tipos de implementaciones DAO:

- Usuario DAO.

- Medición DAO.
- Añadir Medición DAO.

Las mismas que se definen en el archivo *applicationContext.xml*, para la configuración del framework Spring.

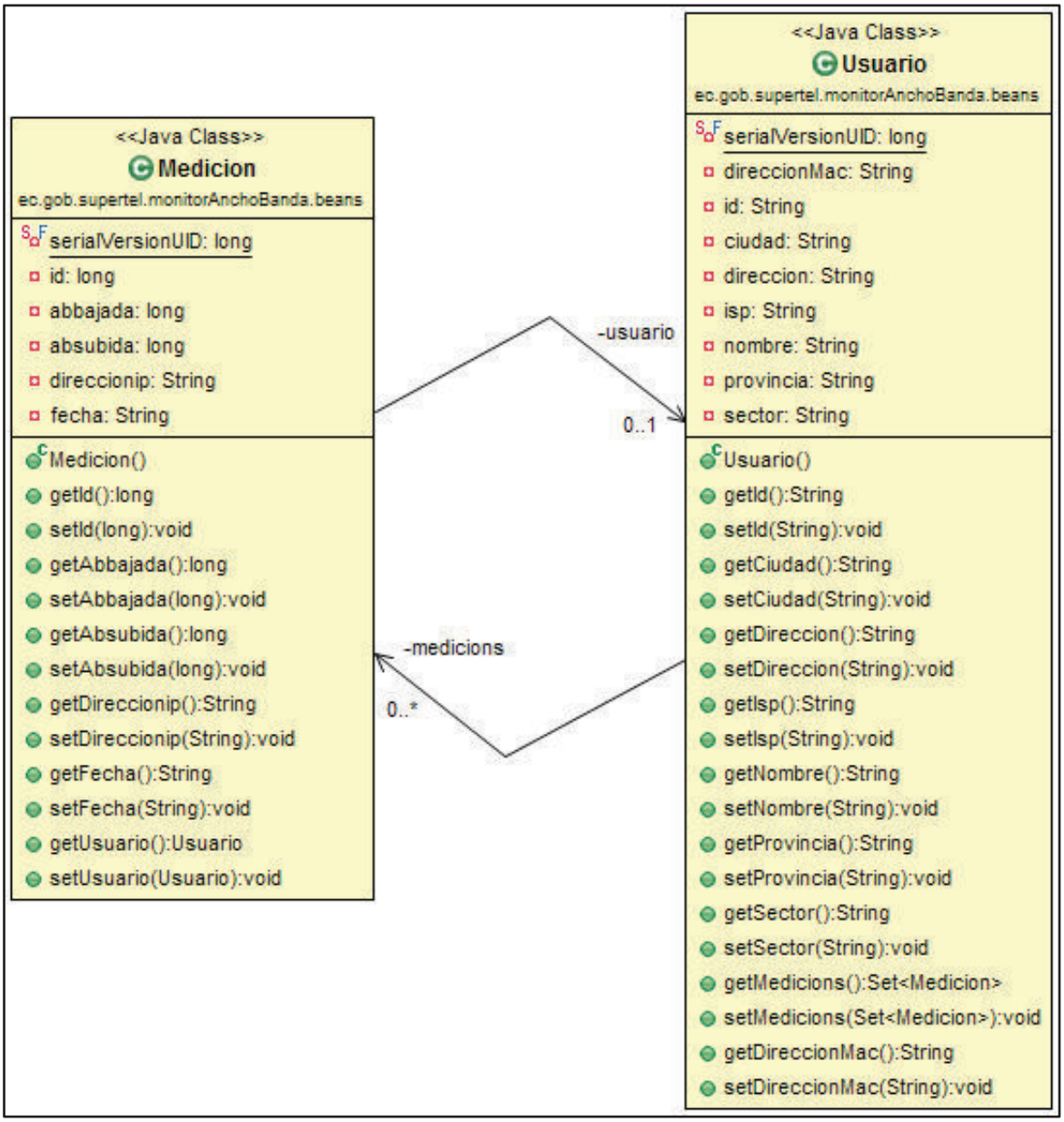


Figura 3.22. Diagrama de clases de las entidades Bean JPA de la aplicación.

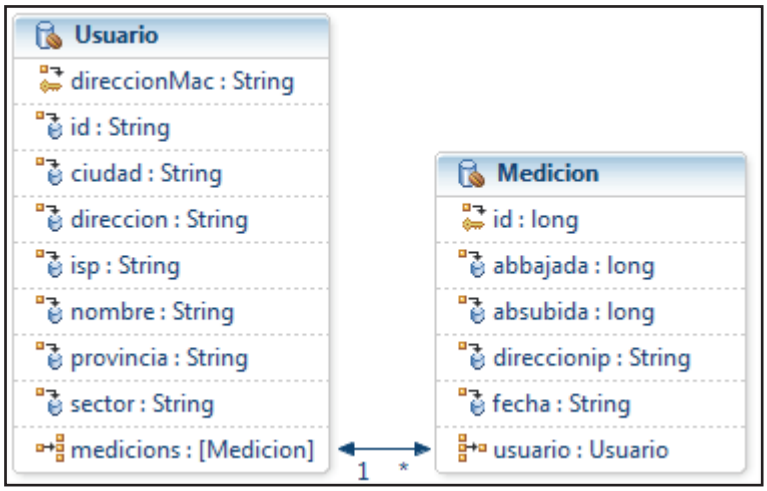


Figura 3.23. Entidades Bean JPA del módulo Sistema de Persistencia.

Las implementaciones Usuario DAO y Medición DAO serán utilizadas por el personal técnico de control de la SUPERTEL a través del nivel Web JEE asignado a éstos. Por el contrario, la implementación Añadir Medición DAO será utilizada únicamente por el servicio web asignado a la recepción de los datos de monitorización enviados desde los usuarios monitoreados. El propósito de segmentar el tipo de manipulación (creación, modificación, eliminación y consulta de registros) que se le da a la tabla Medición, es con el propósito de independizar los roles de utilización de ésta tabla, de acuerdo al tipo de usuario de la aplicación.

3.4.2.2.1 Implementación Usuario DAO

La implementación Usuario DAO comprende las clases java encargadas de la creación, modificación, eliminación y consulta de los registros almacenados en la tabla Usuario, a través de la entidad Bean JPA *Usuario,* Figura 3.25. Específicamente, la implementación se realiza a través de las clases *IUsuarioDao* y *UsuarioJPADao,* siendo la primera la interfaz Java que define los métodos para la implementación, y la segunda, la encargada de implementar efectivamente los métodos definidos en ésta interfaz Java.

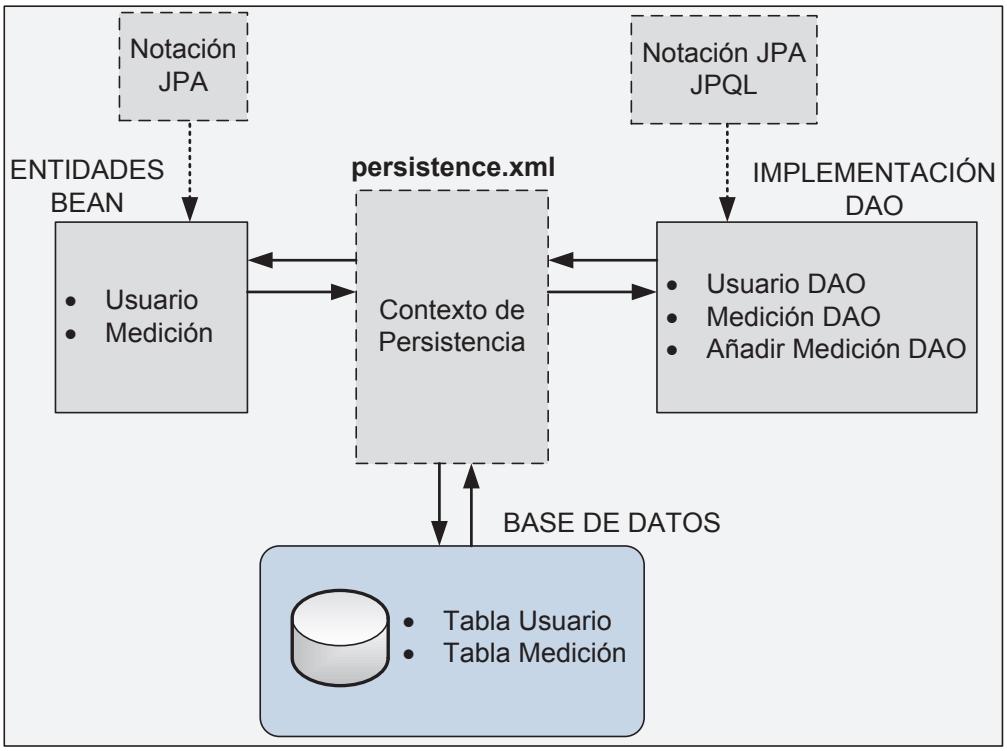


Figura 3.24. Sistema de persistencia de la aplicación de monitorización.

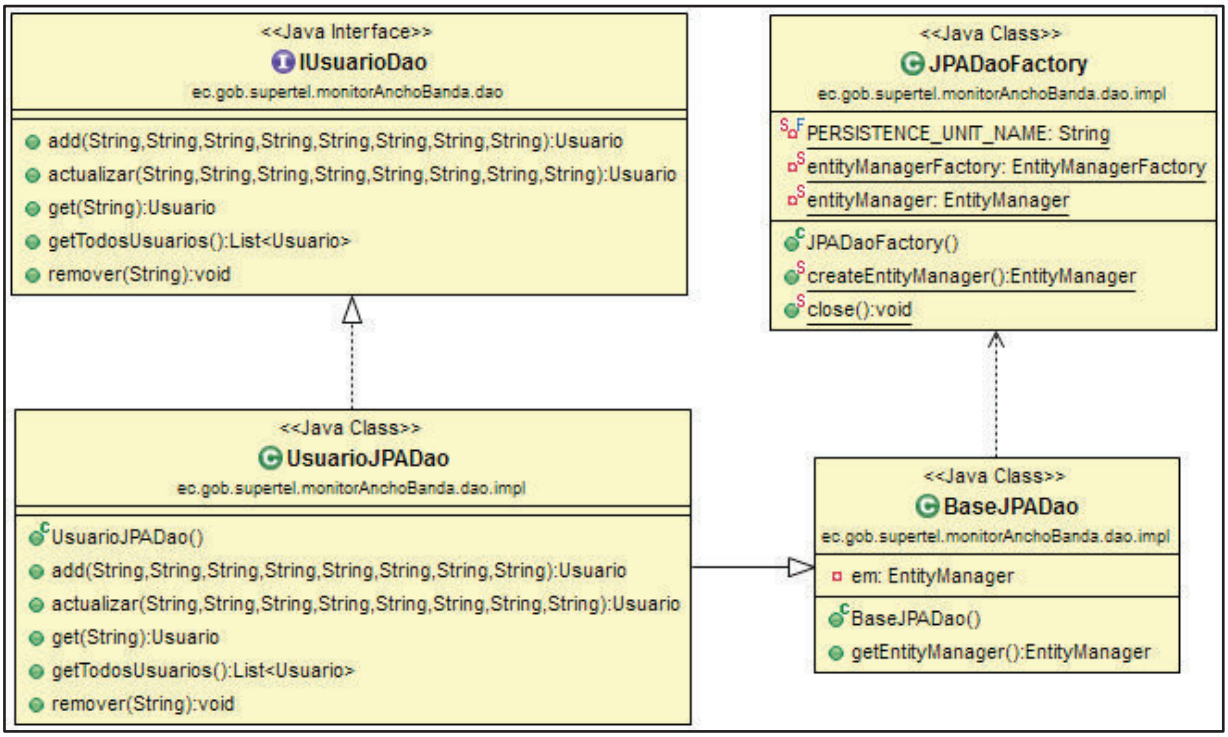


Figura 3.25. Diagrama de clases de la Implementación Usuario DAO.

La clase *JPADaoFactory* es la encargada de utilizar las instancias de entidades persistentes definidas en el contexto de persistencia *persistence.xml,* para la creación, modificación, eliminación y consulta de la entidad Bean JPA asociada con los registros de la tabla Usuario. La clase *BaseJPADao* es utilizada como "accesor[15]" o medio de acceso a los atributos privados de la clase *JPADaoFactory.*

3.4.2.2.2 Implementación Medición DAO

La implementación Medición DAO se realiza con la ayuda de los métodos de las clases *IMedicionDao* y *MedidionJPADao,* Figura 3.26,las mismas que permiten únicamente, consultas de la información almacenada en la tabla Medición, por medio de la entidad Bean JPA *Medicion* y el lenguaje de consultas JPQL.

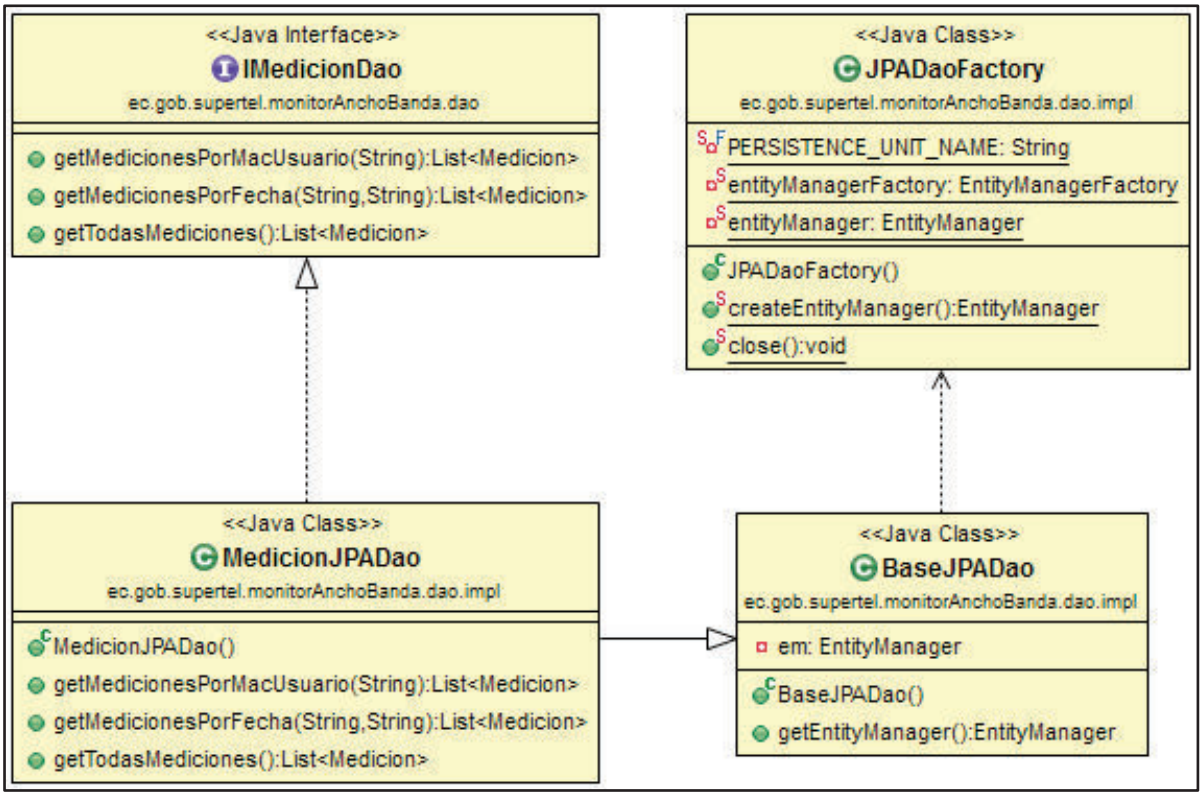


Figura 3.26. Diagrama de clases de la Implementación Medición DAO.

[15] Fuente: http://java.about.com/od/workingwithobjects/a/accessormutator.htm

De igual forma, las clases *JPADaoFactory* y *BaseJPADao* permiten el nexo entre la entidad Bean JPA asociada a la información contenida en la tabla Medición, con su implementación DAO definida en las clases *IMedicionDao* y *MedidionJPADao.* Para ésto, utiliza el contexto de persistencia establecido en el archivo *persistence.xml.*

3.4.2.2.3 Implementación Añadir Medición DAO

Ésta implementación DAO es introducida en la aplicación, con el único fin de atender a las solicitudes provenientes desde la Aplicación Cliente Monitoreado en el lado del usuario monitoreado, para el ingreso de nuevos registros a la tabla Medición, por medio de las clases *IMedicionAddDao* y *MedicionAddDao.*

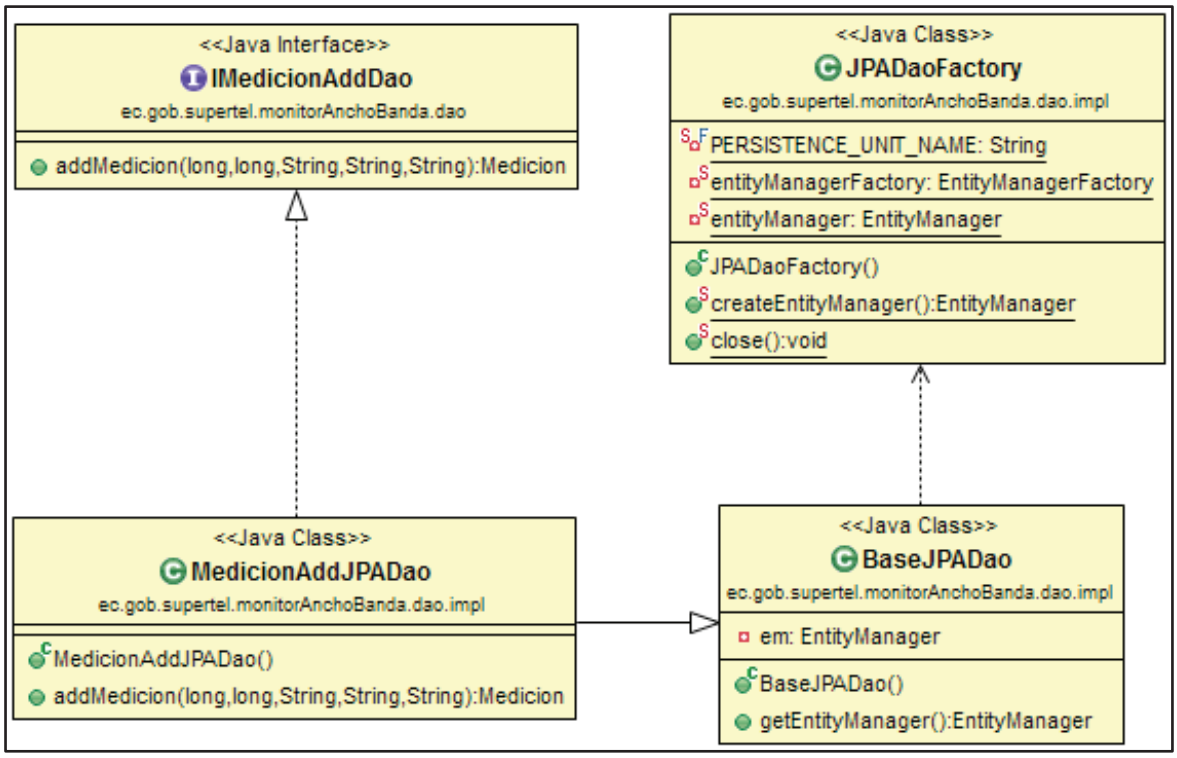


Figura 3.27. Diagrama de clases de la Implementación Añadir Medición DAO.

La función de las clases *JPADaoFactory* y *BaseJPADao,* es la misma que se encuentra definida en las implementaciones DAO anteriores.

3.4.2.3 Módulo Servidor de Servicios Web

El módulo Servidor de Servicios Web consiste en un servidor JAX-WS desplegado en un servidor JEE Weblogic 12c, el mismo que está encargado de publicar los servicios web necesarios para la recepción de datos provenientes de los clientes monitoreados, y para la utilización del Módulo Cliente del Servicio Web de Consultas de los resultados almacenados en la base de datos.

De ésta manera, el Módulo Servidor Servicio Web publicará los siguientes tipos de servicios web:

- Servicio Web para la recepción de mediciones.
- Servicio Web para la consulta de mediciones.
- Servicio Web para la consulta y gestión de usuarios.

Donde el primer servicio web es consumido únicamente por los clientes del servicio web que envían datos de monitorización, y los 2 siguientes, completamente consumidos por el personal técnico de control.

De forma general, éste módulo se encarga de realizar las siguientes funciones:

- Conversión entre contenido XML y objetos Java.
- Implementación de servicios web JAX-WS.

El Módulo Servidor Servicio Web en conjunto con el Módulo Sistema de Persistencia, conforman el nivel de negocio de la aplicación corporativa JEE para la monitorización del presente proyecto.

3.4.2.3.1 Conversión entre Contenido XML y objetos Java

La conversión entre contenido XML y objetos Java consiste en mapear, tanto la información de monitorización contenida en los mensajes SOAP recibidos desde el cliente JAX-WS de la aplicación, como las consultas a la base de datos realizadas por parte del personal técnico. Los objetos Java obtenidos puedan ser almacenados

en la base de datos por medio del Módulo Sistema de Persistencia antes explicado, o a su vez consultados por el Módulo Cliente del Servicio Web de Consultas. El proceso de conversión es el mismo ya sea que se lo haga desde contenido XML a objetos Java, o desde objetos Java a contenido XML, todo depende del servicio web que se consuma.

La conversión entre contenido XML y objetos Java se realiza con la ayuda del API JAXB, y del esquema XSD definido en el archivo *MonitorAnchoBanda.xsd*, Figura 3.28. Éste esquema define en lenguaje XML, la forma en que deben ser creadas las clases JAXB asociadas con las entidades Bean JPA *Usuario* y *Medicion*. Las clases JAXB se encuentran definidas en el esquema XSD por medio de los Tipos XSD (XSD types) *UsuarioType, UsuarioResultType, MedicionType* y *MedicionResultType*, Figura 3.29 y 3.30. El contenido del archivo *MonitorAnchoBanda.xsd* puede ser consultado en los anexos del presente documento.

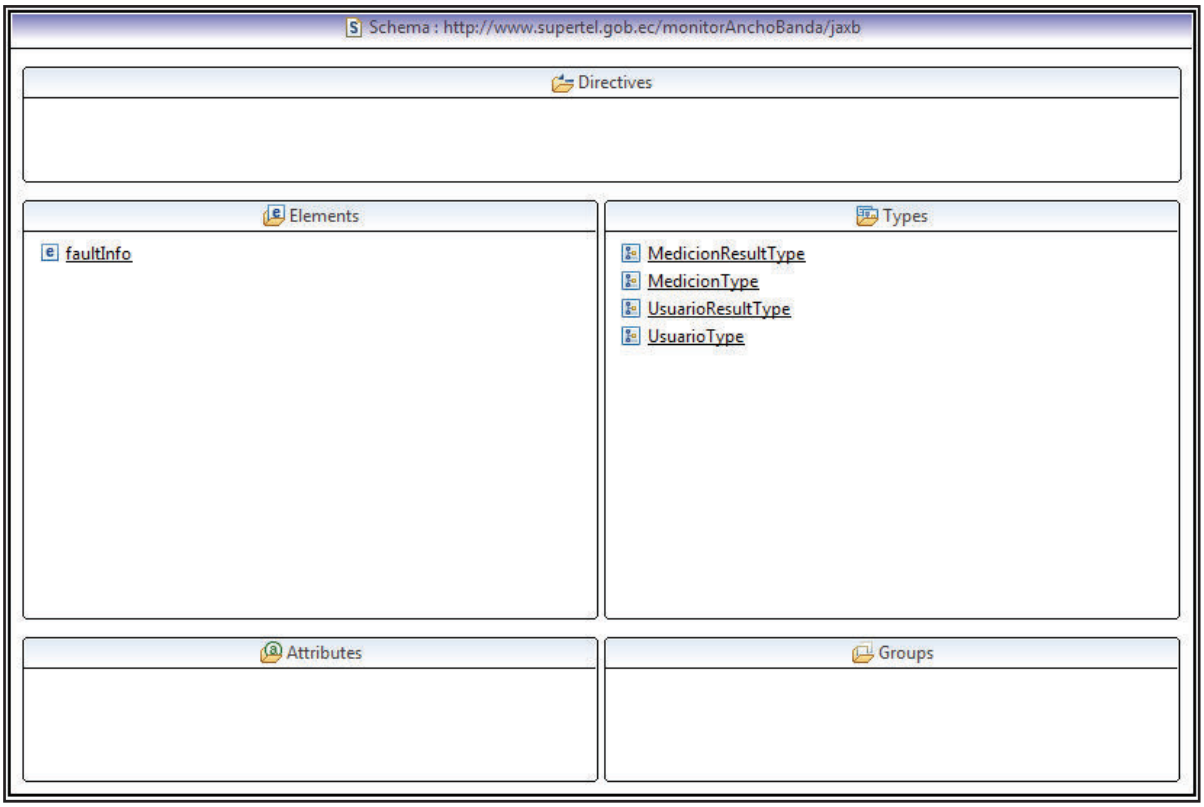


Figura 3.28. Esquema XSD MonitorAnchoBanda.xsd.

Los tipos XSD *UsuarioResultType* y *MedicionResultType*, constituyen una lista de tipos XSD *UsuarioType* y *MedicionType*, respectivamente.

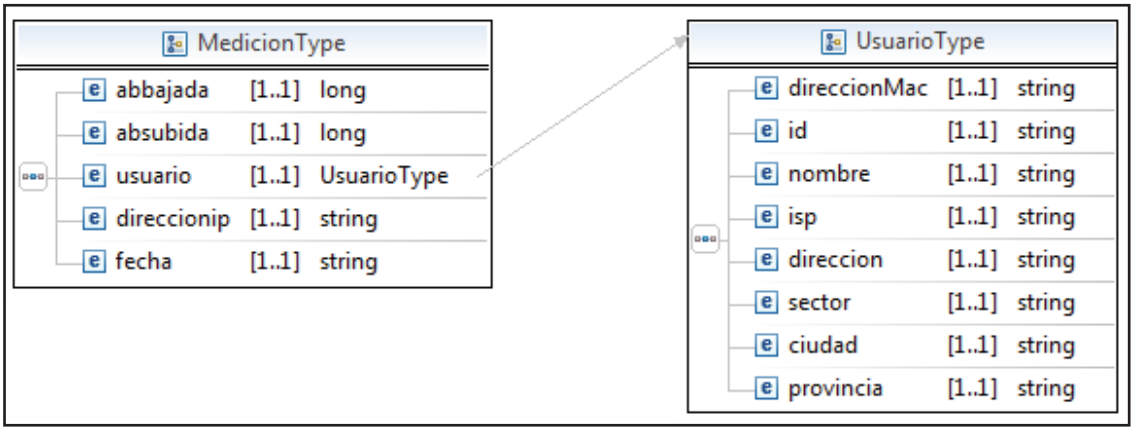


Figura 3.29. Tipos XSD UsuarioType y MedicionType.

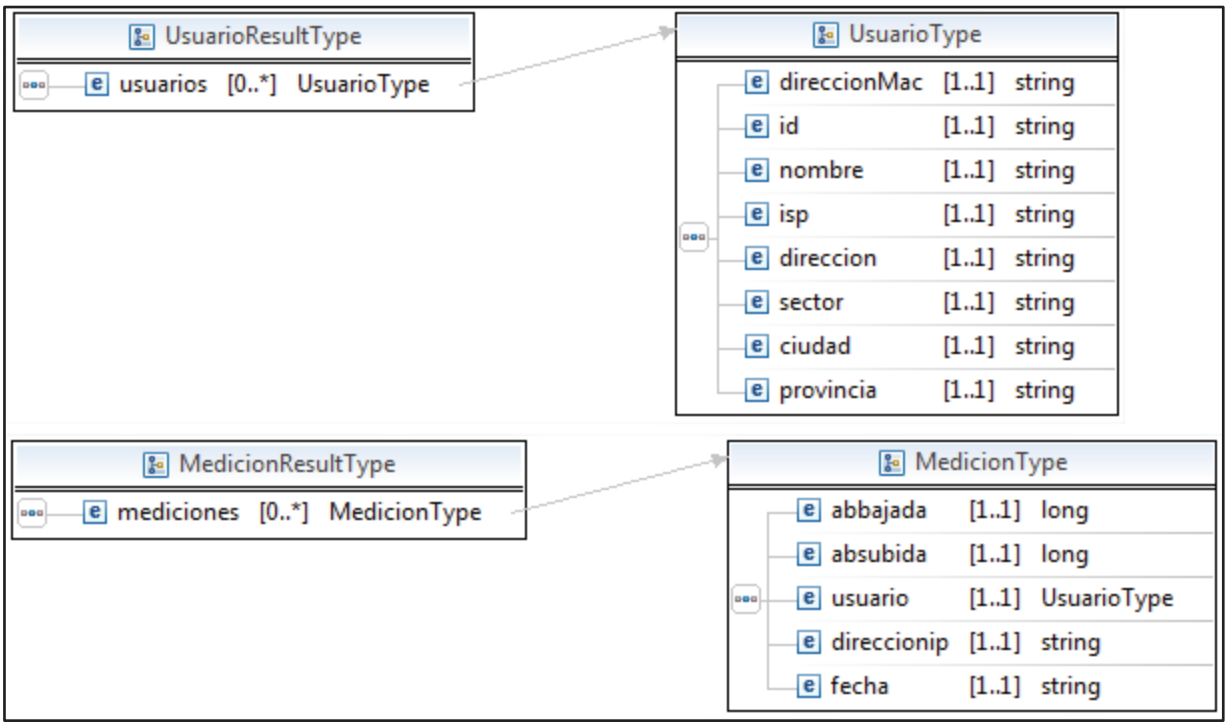


Figura 3.30. Tipos XSD UsuarioResultType y MedicionResultType.

- **Conversión de contenido XML a objetos Java para el servicio web relacionado con la recepción de mediciones.**

La conversión de contenido XML encapsulados en mensajes SOAP enviados desde los Clientes Web monitoreados, a objetos Java para su posterior almacenamiento en la base de datos, se lo realiza por medio de las clases JAXB *MedicionType* y *MedicionResultType*, Figura 3.31, las mismas que fueron creadas por el esquema XSD.

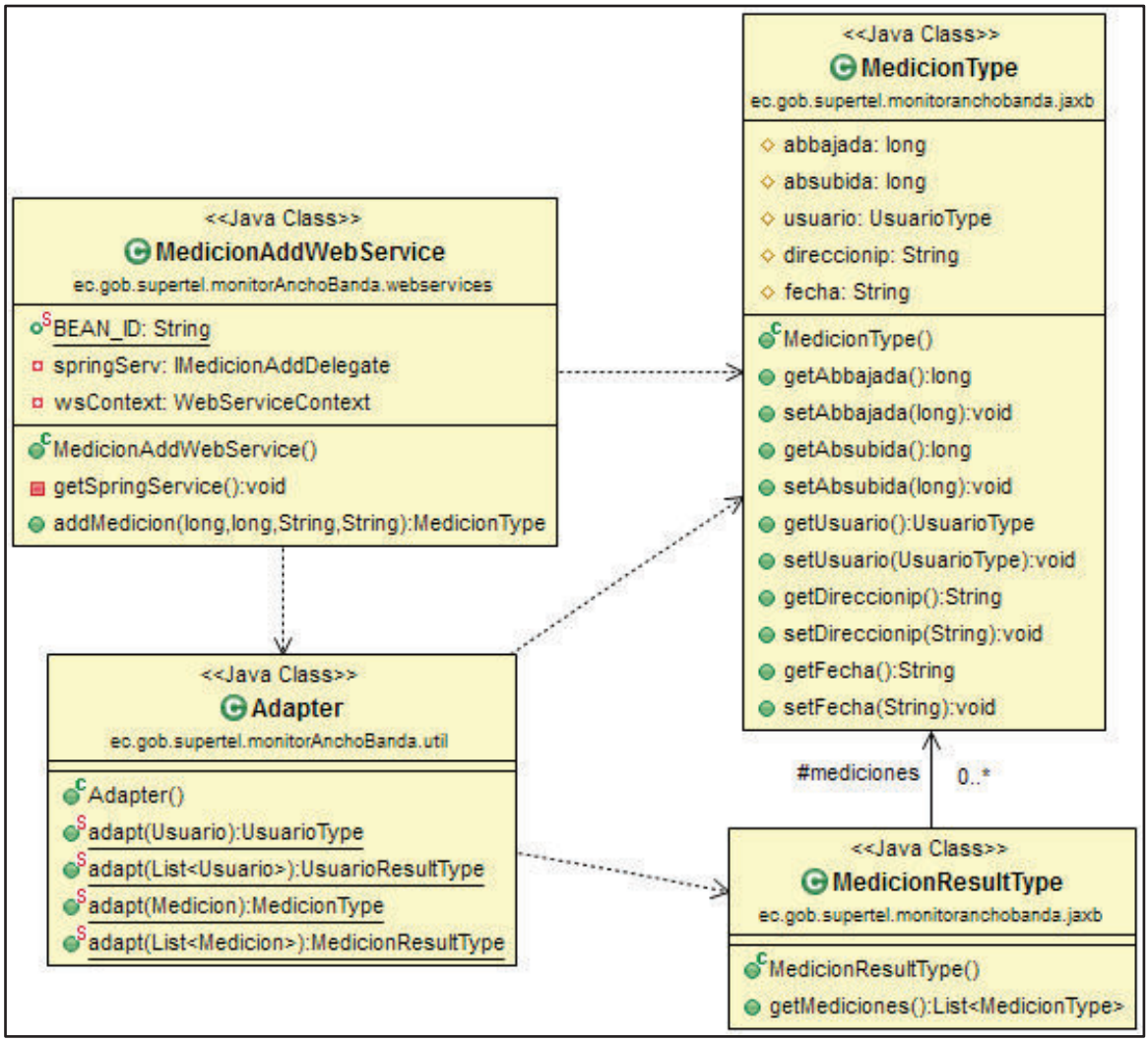


Figura 3.31. Diagrama de clases para la conversión de contenido XML a objetos Java del servicio web asociado a la recepción de mediciones.

La clase *Adapter* es la encargada de convertir la clase JAXB *MedicionType* en la clase Bean JPA *Medicion*. La clase *MedicionAddWebService* es la encargada de implementar la conversión de contenido XML a objetos Java de las mediciones de monitorización recibidas por el Servicio Web relacionado.

La conversión para éste tipo de servicio web es una dirección, es decir, de contenido XML a objetos Java.

- **Conversión entre contenido XML y objetos Java para el servicio web relacionado con la consulta de mediciones.**

El servicio web relacionado con la consulta de mediciones requiere de la conversión de contenido XML a objetos Java y la conversión en sentido contrario, ya que las consultas que se realizan a la base de datos desde el Módulo Cliente del Servicio Web de Consultas, requieren de parámetros de búsqueda que deben ser especificados para retornar resultados acordes a éstos. Para éste servicio web se utilizan igualmente las clases JAXB *MedicionType* y *MedicionResultType*, Figura 3.32.

Al igual que la conversión del servicio web anterior, la clase *Adapter* convierte la entidad JAXB *MedicionType* en la entidad Bean JPA *Medicion*, y viceversa. Por su parte, la clase *MedicionAddWebService* realiza la implementación de la conversión necesaria para la realización de consultas de la tabla Medición de la base de datos.

- **Conversión entre contenido XML y objetos Java para el servicio web relacionado con la consulta y gestión de usuarios.**

La conversión entre contenido XML y objetos Java para éste servicio web se lo realiza por medio de las clases JAXB *UsuarioType* y *UsuarioResultType*, Figura 3.33. La conversión se realiza tanto desde contenido XML a objetos Java, como desde objetos Java a contenido XML, ya que para la consulta y manipulación de registros de la tabla Usuario de la base de datos, existe flujo de datos bidireccional, desde y hacia la aplicación.

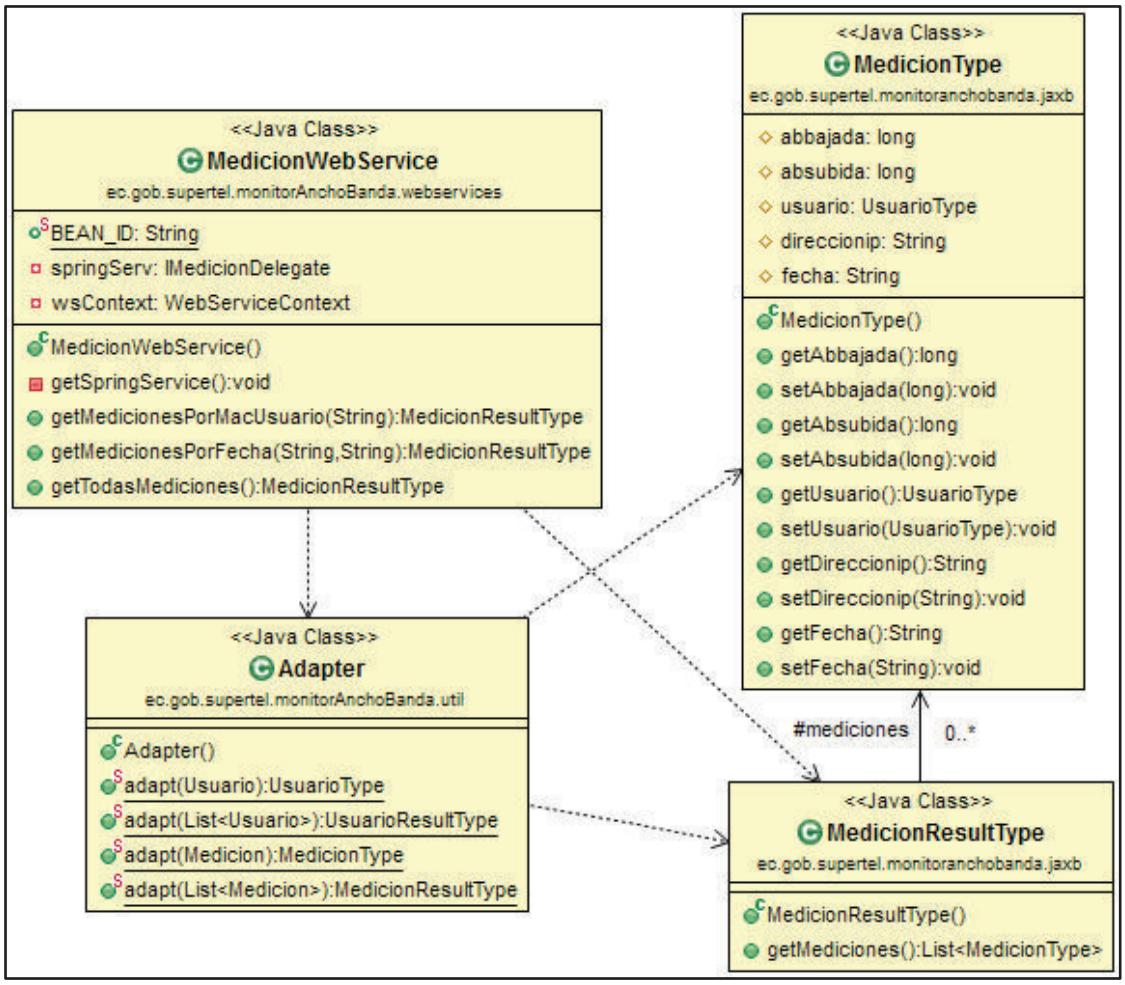


Figura 3.32. Diagrama de clases para la conversión entre contenido XML y objetos Java del servicio web asociado a la consulta de mediciones.

La clase *Adapter* contiene métodos para la conversión entre la clase JAXB *UsuarioType* y la clase Bean JPA *Usuario.* La conversión es implementada por medio de la clase *UsuarioWebService*.

3.4.2.3.2 Implementación de Servicios Web

La implementación de los servicios web está relacionada con la manera en la que los servicios web creados para la aplicación, son ejecutados y publicados en el servidor JEE Weblogic 12c. En la Figura 3.35 se observa a los servicios de la aplicación de monitorización publicados por el servidor JEE Weblogic 12c.

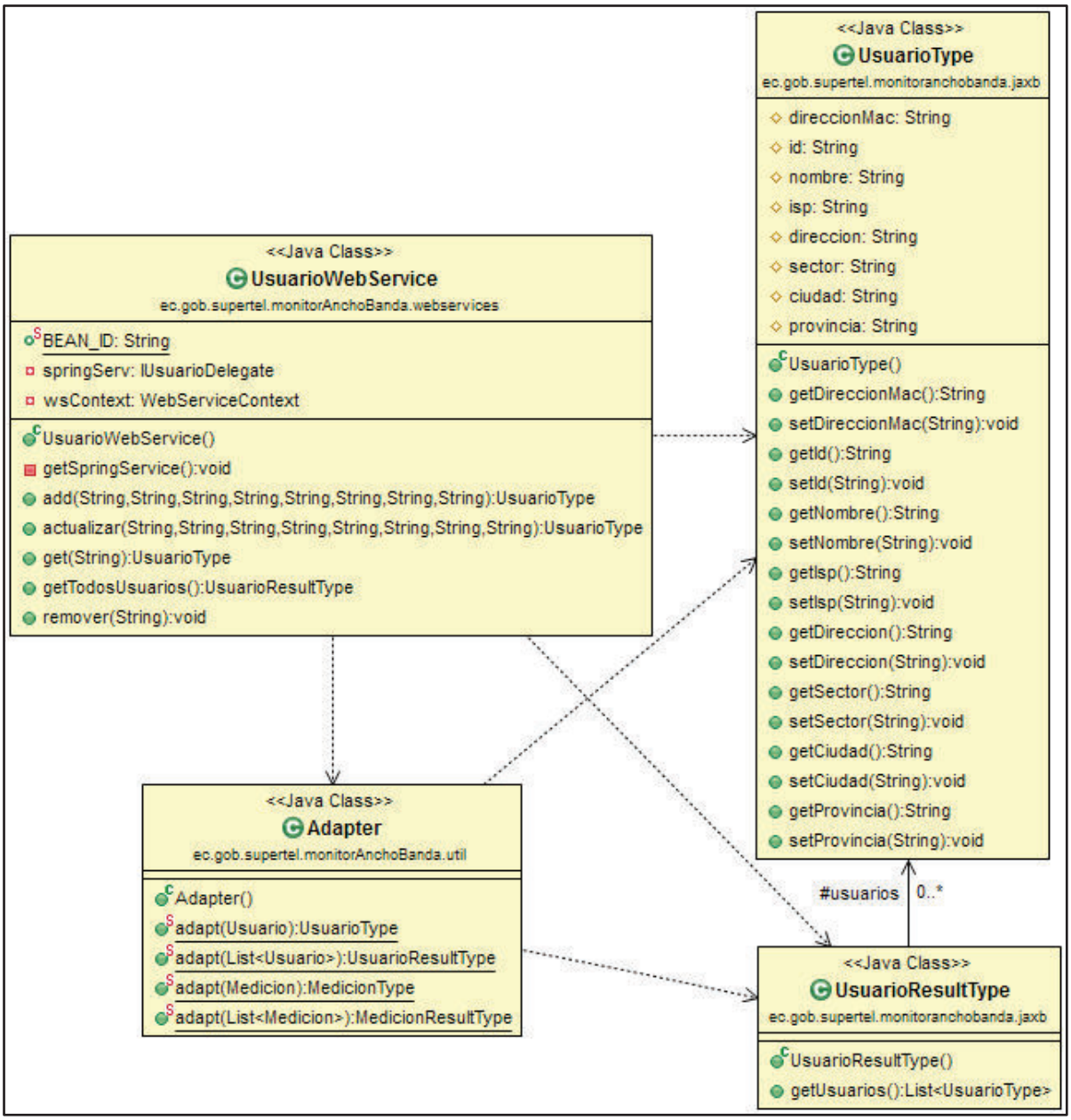


Figura 3.33. Diagrama de clases para la conversión entre contenido XML y objetos Java del servicio web asociado a la consulta y gestión de usuarios.

El servidor JEE Weblogic 12c publica los servicios web sobre Internet o sobre la intranet de la SUPERTEL, por medio de archivos WSDL escritos con código XML. Los archivos WSDL definen la funcionalidad del servicio web y la lógica necesaria para su consumo; además son accedidos por los clientes web mediante un URL especificado dentro del servidor JEE.

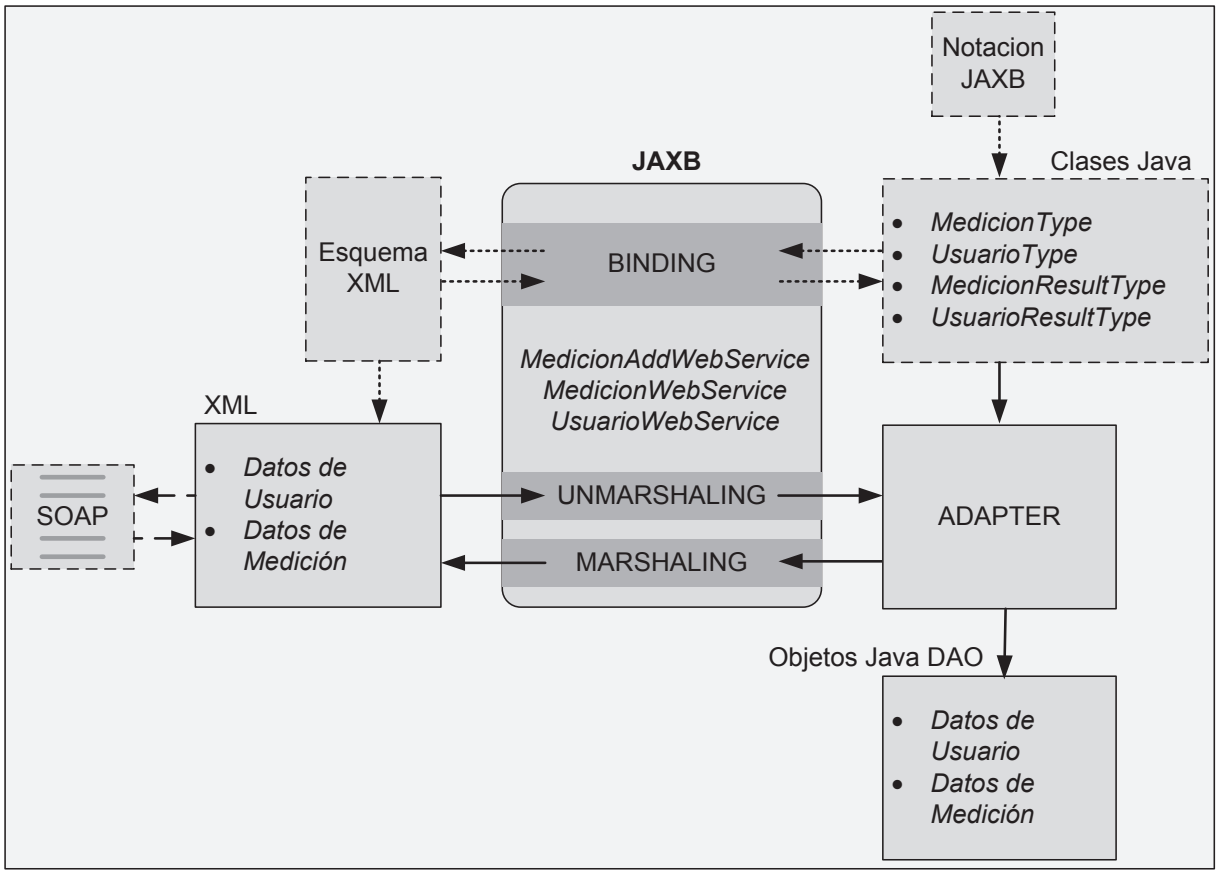


Figura 3.34. Conversión entre objetos Java y contenido XML en el Servidor de servicios web.

El servidor JEE Weblogic 12c es el mismo usado tanto por el servidor JEE del prototipo como por el servidor JEE en producción usado por la SUPERTEL, garantizándose la compatibilidad de los servicios web desarrollados en la aplicación prototipo que serán distribuidos luego al servidor en producción a través de un archivo de unidad de despliegue EAR o WAR.

- **Implementación del servicio web para la recepción de mediciones.**

El servicio web para la recepción de resultados de monitorización se implementa por medio de la clase *MedicionAddWebService*, Figura 3.36. La clase *MonitorAnchoBandaException* se encarga de mapear los posibles errores a nivel de contenido XML, a errores a nivel de objetos Java.

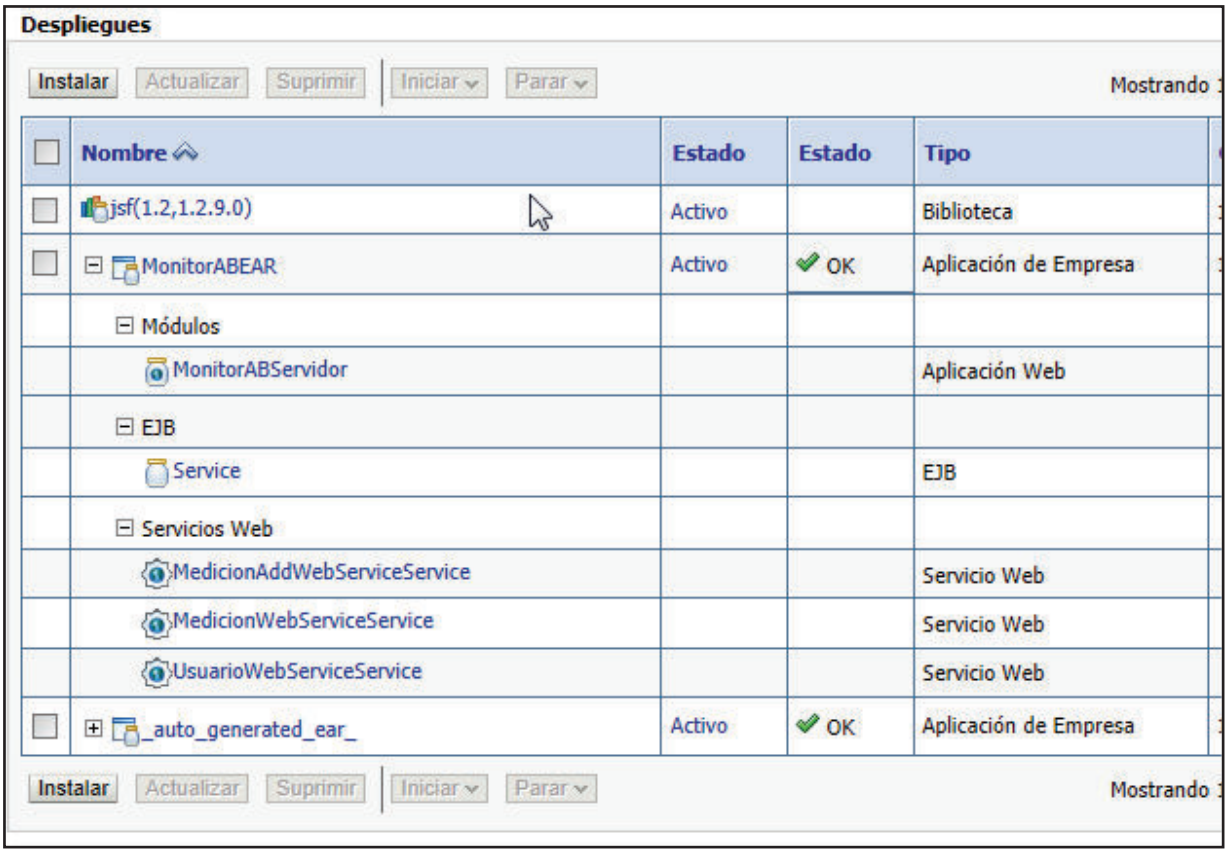


Figura 3.35. Despliegue de los servicios web de la aplicación de monitorización dentro del servidor JEE Weblogic 12c.

Las clases *IMediacionAddDelegate* y *MedicionAddSpringDelegate*, son clases delegadas[16] del framework Spring, para establecer la integridad transaccional del servicio web de recepción de mediciones. La clase *MedicionAddSpringDelegate*instancia a la implementación DAO *MedicionAddDao* por medio de la interfaz Java *IMedicionAddDao* (explicadas anteriormente), para proveer de integridad transaccional al ingreso de nuevos registros en la tabla Medición. La clase delegado *MedicionAddSpringDelegate* se encuentra definida en el archivo de configuración del framework Spring, *applicationContext.xml*.

[16] La delegación es la labor de encargar la ejecución de una tarea a otra clase o entidad Java. Fuente: http://docs.oracle.com/cd/E19879-01/820-4336/gfqpi/index.html

Las mediciones recibidas por éste servicio web, desde los clientes monitoreados, contiene la información referente a ancho de banda de bajada, ancho de banda de subida, dirección MAC y fecha de captura. Para cumplir con los requerimientos funcionales de la aplicación, es necesario determinar la dirección IP de donde provienen las mediciones, la misma que es obtenida por medio de la clase *MedicionAddWebService*, Figura 3.37.

La dirección IP capturada de la medición, será almacenada dentro de la variable *direccionIP*, para su posterior uso dentro de la aplicación. La Tabla 3.11 describe las características de ésta variable.

El servicio web para la recepción de resultados de monitorización se encuentra publicado en el servidor JEE a través del archivo WSDL incluido en la siguiente URL:

http://www.supertel.gob.ec:7001/MonitorABServidor/MAWSS?WSDL

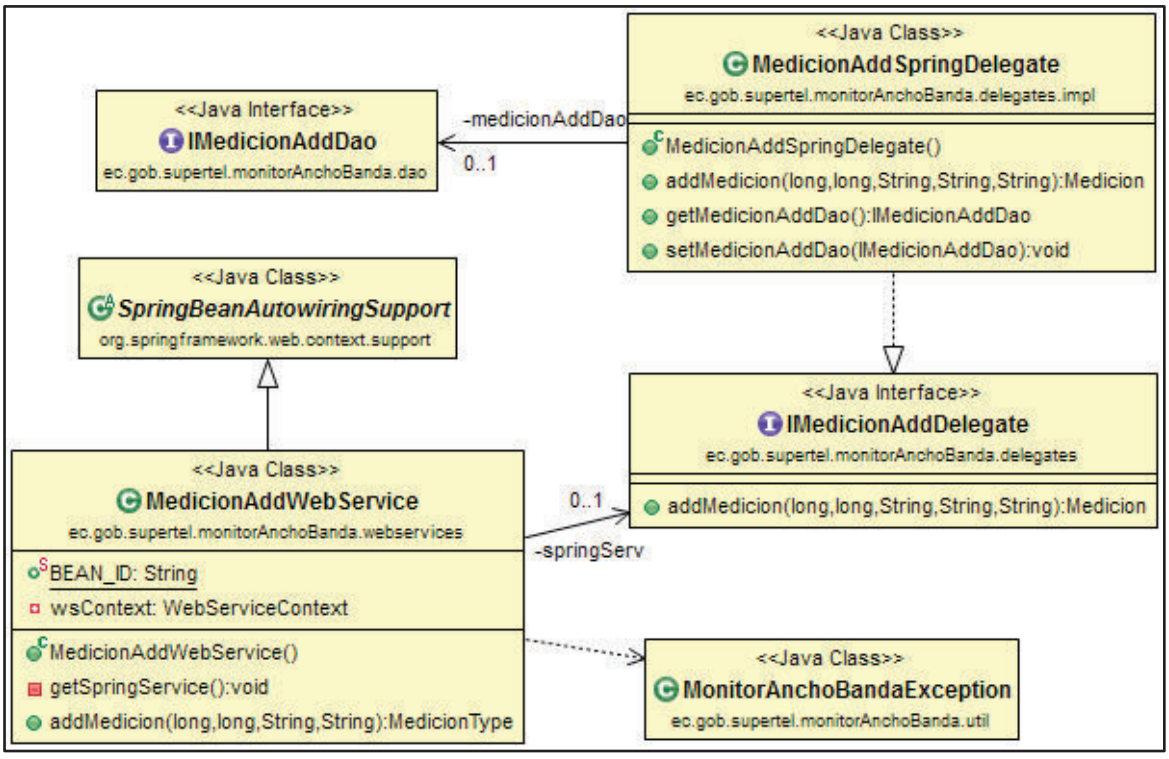


Figura 3.36. Diagrama de clases de la implementación del servicio web relacionado con la recepción de mediciones.

```
// Conseguir direccion IP del cliente
            MessageContext mc = wsContext.getMessageContext();
            HttpServletRequest req = (HttpServletRequest)mc.get(MessageContext.SERVLET_REQUEST);
            String direccionIp = req.getRemoteAddr();
// ----------------------------------------
```

Figura 3.37. Código para la determinación de la dirección IP del cliente del servicio web para el envío de mediciones.

Tabla 3.11. Características de la variable direccionIP.

Variable	Tipo	Tamaño en Memoria [Bytes]
direccionIP	String	15

- **Implementación del servicio web para la consulta de mediciones.**

La clase *MedicionWebService*, Figura 3.38, es la encargada de implementar el servicio web relacionado con la consulta de los registros almacenados en la tabla Medición.

Las clases *IMedicionDelegate y MedicionSpringDelegate*, son clases delegadas del framework Spring para el manejo de la integridad transaccional de la consulta de los registros de la tabla Medición. Éste servicio web utiliza a la clase DAO *MedicionDao*, llamándola a través de su interfaz Java *IMedicionDao*, para la implementación de las consultas de las mediciones capturadas por la aplicación. La clase *MedicionSpringDelegate* se encuentra definida en el archivo *applicationContext.xml*, usado por el framework Spring para su configuración.

Dentro del servidor JEE Weblogic 12c, el servicio web de consulta de mediciones se encuentra publicado a través del archivo WSDL incluido en la siguiente URL:

http://www.supertel.gob.ec:7001/MonitorABServidor/MWSS?WSDL

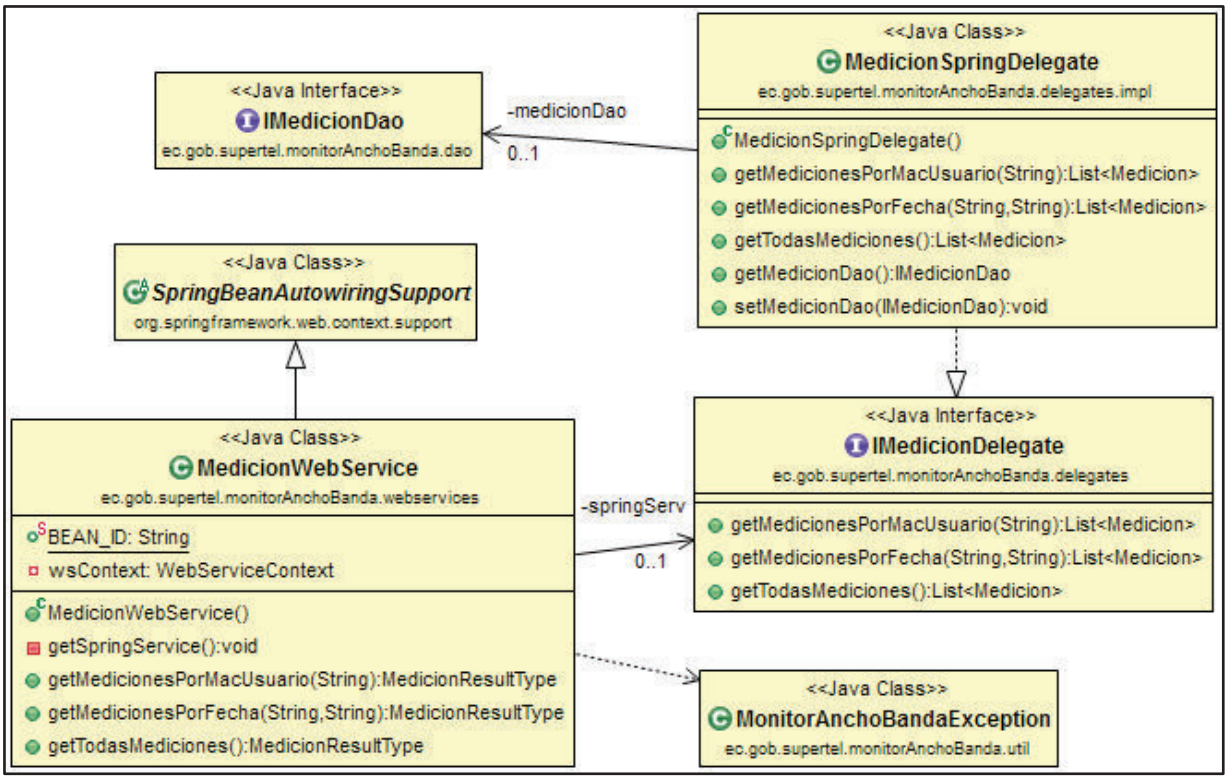


Figura 3.38. Diagrama de clases de la implementación del servicio web relacionado con la recepción de mediciones.

- **Implementación del servicio web para la consulta y gestión de usuarios.**

La implementación del servicio web para la consulta y manipulación de los registros almacenados en la tabla Usuario se lo hace por medio de la clase *UsuarioWebService*, Figura 3.39, la misma que usa la clase *MonitorAnchoBandaExcepcion* para conversión de errores capturados a nivel de contenido XML, a errores a nivel de objetos Java.

La integridad transaccional de la consulta, creación, actualización y eliminación de los registros almacenados en la tabla Usuario, se lo realiza con la ayuda del Framework Spring y de las clases delegadas *IUsuarioDelegate* y *UsuarioSpringDelegate*.

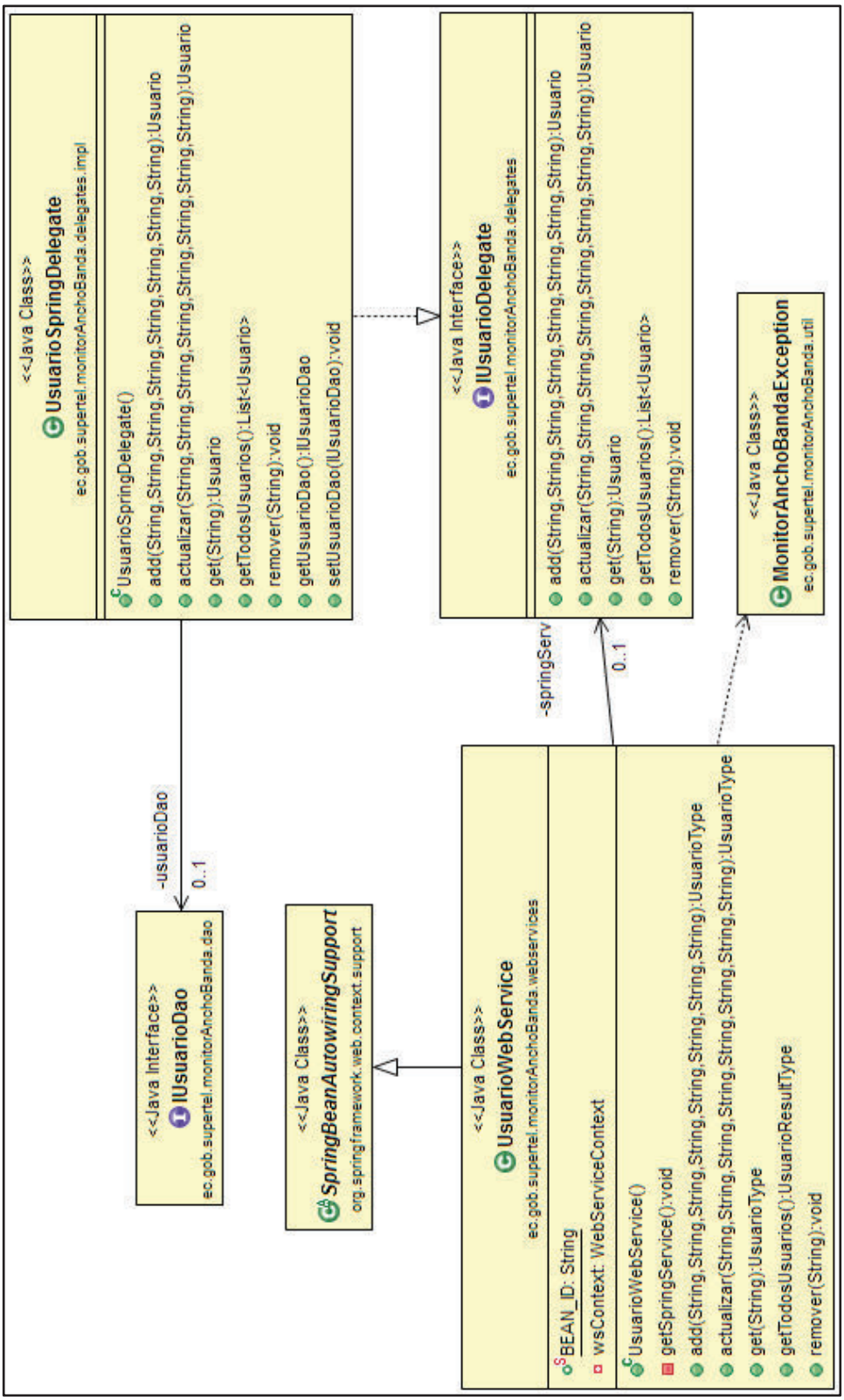


Figura 3.39. Diagrama de clases de la implementación del servicio web relacionado con la consulta y gestión de usuarios.

La clase *UsuarioSpringDelegate* realiza la integridad transaccional para la consulta y gestión de usuarios mediante el llamado de la clase *UsuarioDao* a través de la interface Java *IUsuarioDao*. La clase *UsuarioSpringDelegate* también se encuentra definida en el archivo *applicationContext.xml*.

La implementación de éste servicio a nivel de servidor JEE, se lo realiza publicando en el servidor Weblogic, el archivo WSDL indicado en la siguiente URL:

http://www.supertel.gob.ec:7001/MonitorABServidor/UWSS?WSDL

3.4.2.3.3 Seguridad de los Servicios Web de la Aplicación

La publicación de servicios web sobre Internet, involucra el riesgo de que éstos sean utilizados indebidamente o sean usados como vía de ataque a los recursos de hardware y software de la SUPERTEL. Debido a que la presente aplicación utiliza un servicio web publicado en Internet, es necesario establecer para el mismo un sistema de seguridad capaz de disminuir las amenazas que puedan afectar el correcto funcionamiento de éste.

Por la naturaleza de los datos utilizados por el servicio web expuesto en Internet para la recepción de datos de monitorización, se ha determinado que la aplicación de monitorización únicamente utilizara como método de seguridad, la autenticación de usuarios monitoreados a nivel de mensajes sin encriptación.

De ésta manera, en el servidor JEE Weblogic se ha creado un grupo de usuarios específico para autenticar a los usuarios monitoreados que requieran acceder al servicio web de recepción de mediciones, Figura 3.40. La autenticación de éstos usuarios será a través del nombre del grupo de usuarios monitorizados y de una contraseña, Tabla 3.12.

Debido a que la autenticación de los usuarios monitoreados se realiza a nivel de mensajes, es necesario que el Módulo Aplicación de Cliente Monitoreado conozca los datos de autenticación, indicándolos en la clase *MonitorABClienteWSAplicacion*,

Figura 3.41. De ésta forma los datos de autenticación requeridos son incluidos dentro de los mensajes SOAP que portan datos de monitorización de los clientes.

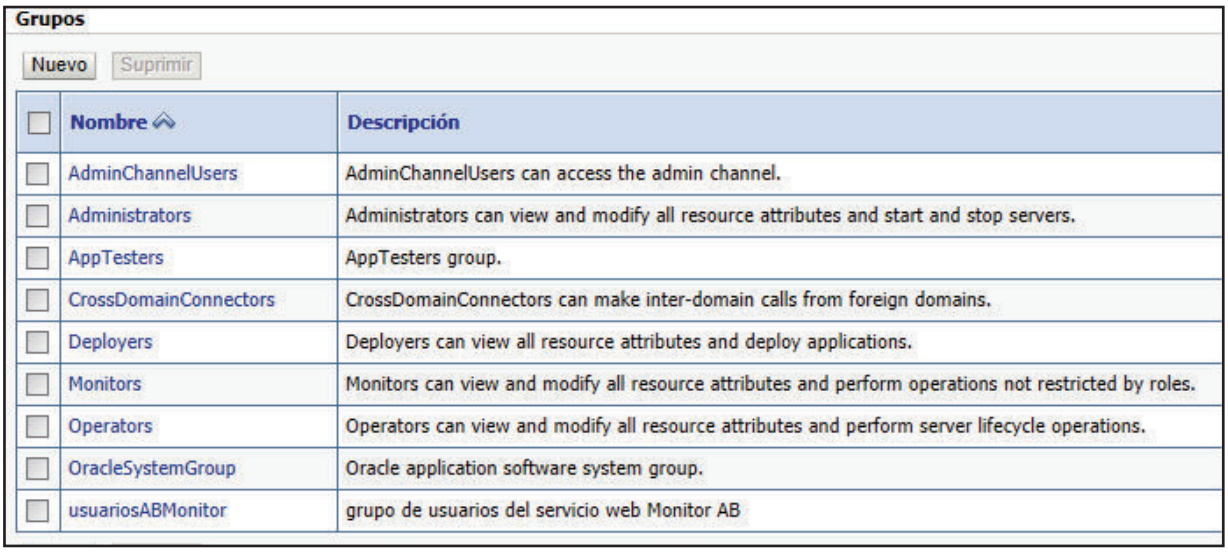


Figura 3.40. Grupo de Usuarios monitoreados creado en Weblogic 12c.

Tabla 3.12. Datos de autenticación para el grupo de usuarios monitoreados.

Nombre del grupo de usuarios	usuarioABMonitor
Contraseña	Supertel123

Fuente: Autoría propia.

De igual manera los archivos *web.xml* y *weblogic.xml* (adjuntos a éste documento en la sección anexos) del nivel de capa de negocio de la aplicación corporativa para el monitoreo de usuarios del servicio de Internet, deben ser modificados para dar soporte a la autenticación de usuarios a nivel de mensajes.

Hasta éste punto se encuentra diseñada e implementada la aplicación que recibe y almacena las mediciones pertenecientes a los usuarios monitorizados a través de servicios web, y cuyo diagrama de secuencia se encuentra detallado en la Figura 3.42.

```
// Autenticacion
BindingProvider bp = (BindingProvider) soap;
Map<String, Object> context = bp.getRequestContext();
context.put("javax.xml.ws.security.auth.username", "usuarioABMonitor");
context.put("javax.xml.ws.security.auth.password", "supertel123");
// ---------------------------------------------------------------------
```

Figura 3.41. Código especificado en la clase *MonitorABClienteWSAplicacion* necesario para la autenticación.

En el siguiente punto se tratan el diseño e implementación de los servicios web restantes.

3.4.2.4 Módulo Cliente del Servicio Web de Consultas

El módulo Cliente del Servicio Web de Consultas representa el nivel web de la aplicación corporativa JEE designado para ser utilizado únicamente por el personal técnico de la Unidad de Control de la Prestación de Servicios de la Superintendencia de Telecomunicaciones (UCPS), a través de un cliente de servicios web JAX-WS.

Los servicios web consumidos por éste módulo, son publicados por el servidor de servicios web Weblogic 12c sobre la Intranet de la SUPERTEL. El personal de la UCPS accede a éste servicio por medio de cualquier tipo de navegador web.

El módulo Cliente del Servicio Web de Consultas basa su funcionamiento en el uso de páginas web JSP, las mismas que proveen la interfaz gráfica y la lógica de programación Java para el acceso a los registros almacenados en las tablas Usuario y Medición de la base de datos relacional de la aplicación.

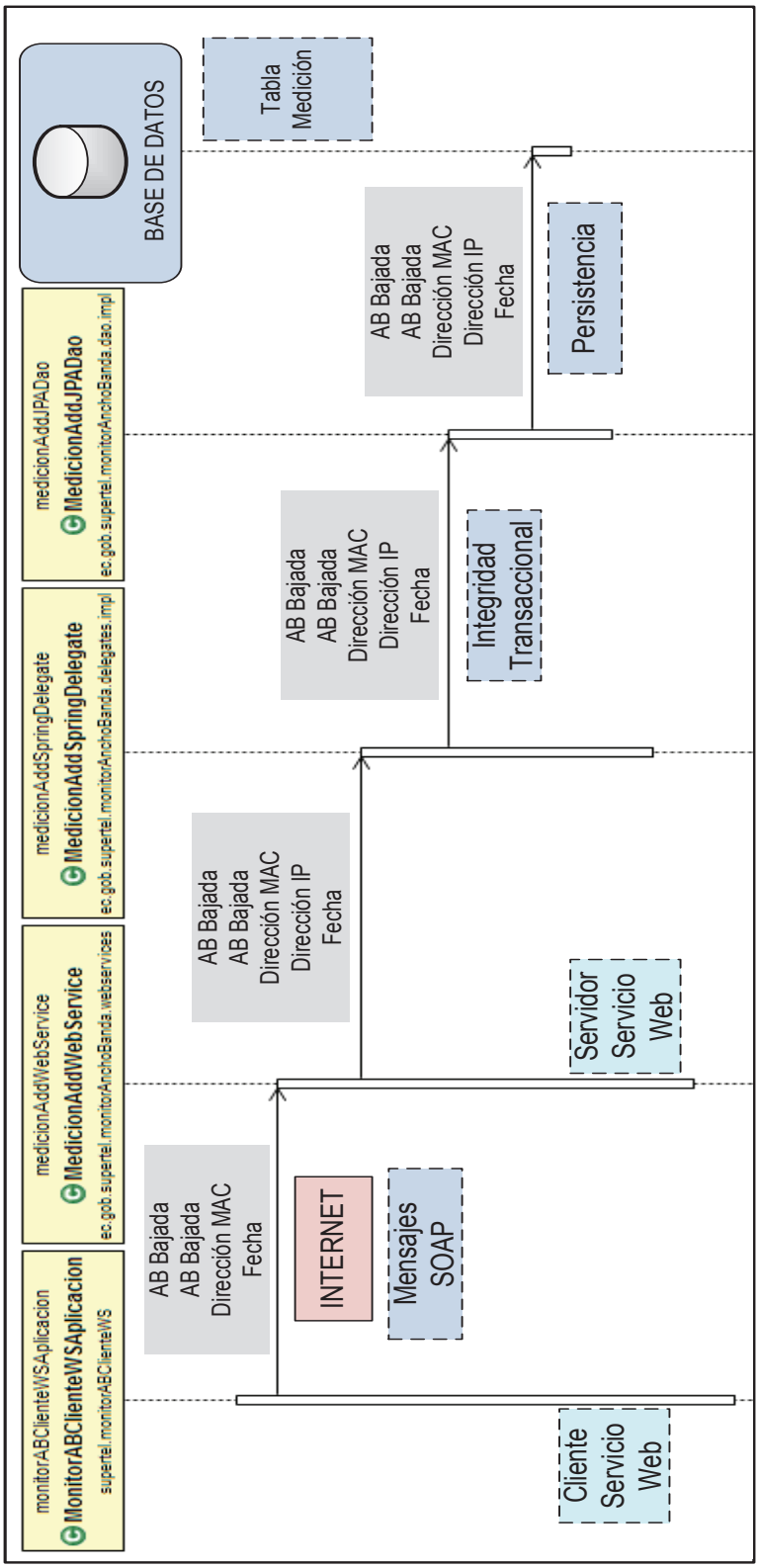


Figura 3.42. Diagrama de secuencia del servicio web para la recepción de mediciones.

La lógica de programación dentro de las páginas web JSP, se encuentra indicada por medio de scriptlets[17], los mismos que se encargan del consumo de los servicios web asignados al cliente del servicio web de consultas.

Para que las páginas web JSP puedan consumir los servicios web publicados en el servidor JEE, es necesario realizar primeramente una conversión entre contenido XML y objetos Java, labor que es realizada por medio de JAXB, Figura 3.43.

El cliente del servicio web de consultas se encargará de consumir los siguientes servicios web:

- Servicio Web para la consulta de mediciones.
- Servicio Web para la consulta y gestión de usuarios.

Por medio de los siguientes clientes del servicio web:

- Cliente del Servicio Web para la consulta de mediciones.
- Cliente del Servicio Web para la consulta y gestión de usuarios.

Éste módulo contará con una página web JSP de inicio a través de la cual es posible acceder a las demás páginas web JSP encargadas de labores de consulta y gestión específicas. La página de inicio se la ha denominado como *bienvenida.jsp*, Figura 3.44.

3.4.2.4.1 Cliente del Servicio Web para la consulta de mediciones

Éste cliente del servicio web tiene como único propósito, realizar la consulta de los resultados de monitorización almacenados en la tabla Medición de la base de datos relacional. Para lograr ésto, el cliente del servicio web recurre a los esquemas de conversión definidos por las clases JAXB *MedicionType* y *MedicionResultType*, Figura 3.45, las mismas que en conjunto con las páginas web JSP respectivas, permiten la conversión entre contenido XML y objetos Java.

[17] Los scriptlets son código Java embebido dentro de código HTML de las páginas web JSP. Fuente: https://docs.oracle.com/javaee/5/tutorial/doc/bnaou.html

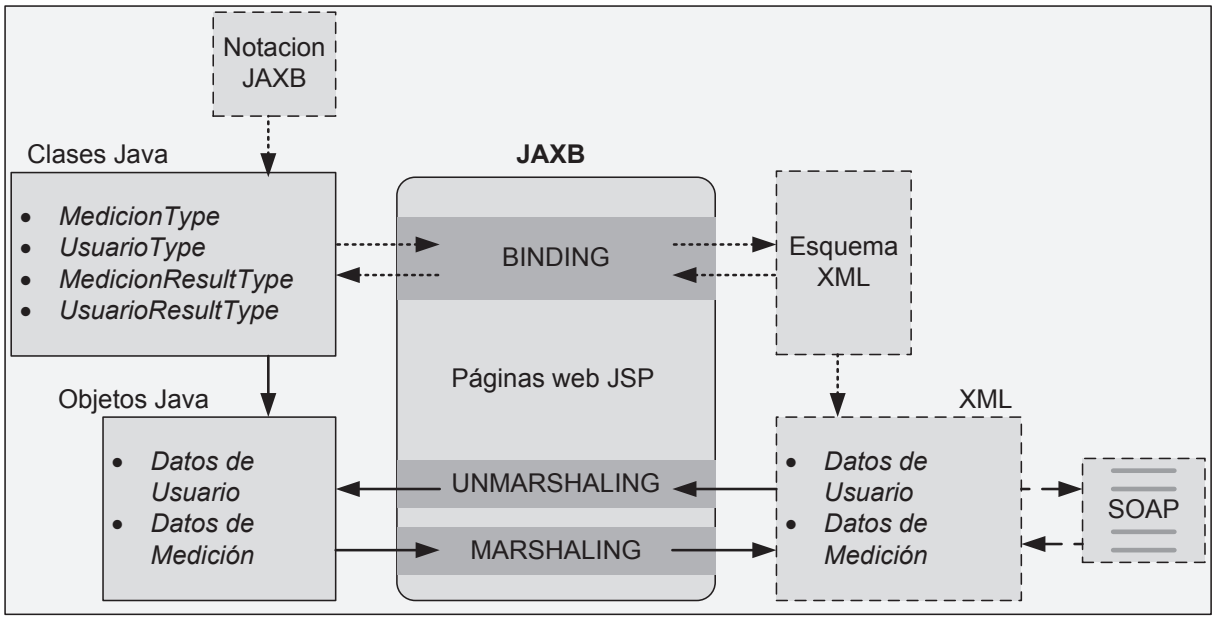


Figura 3.43. Conversión entre contenido XML y objetos Java en el cliente del servicio web de consultas.

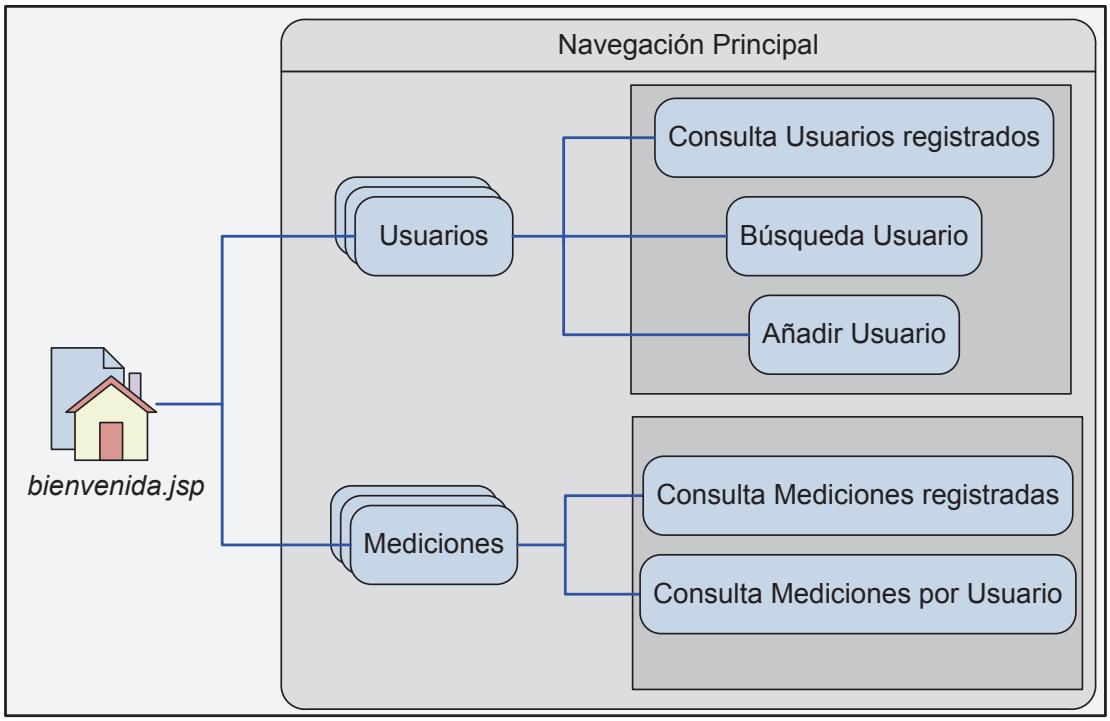


Figura 3.44. Diagrama de navegación web para el cliente del servicio web de consultas.

Éste cliente del servicio web no es capaz de ingresar, modificar o eliminar los registros localizados en la tabla Medición, únicamente puede consultarlos.

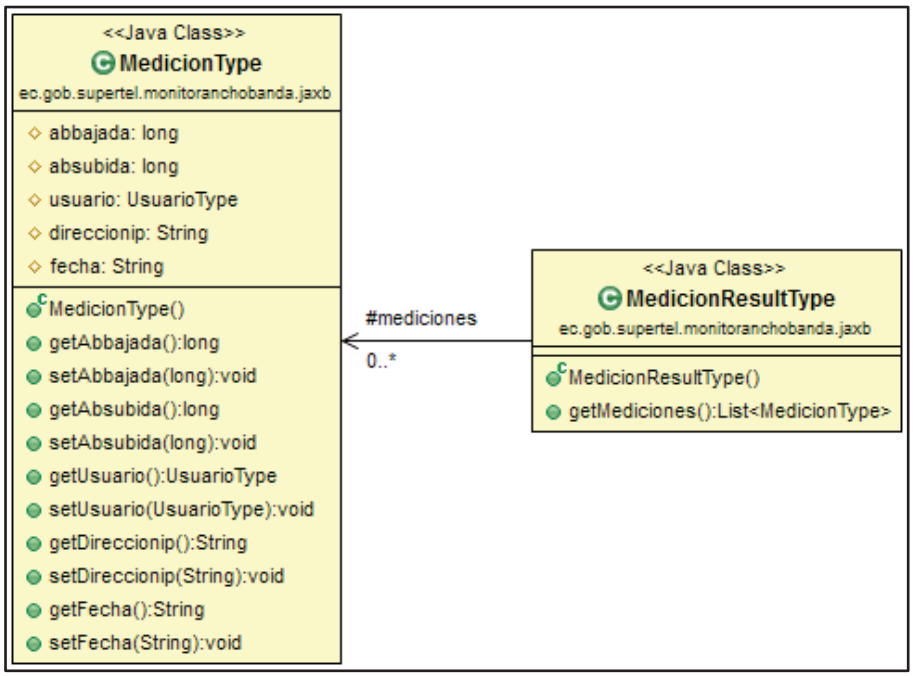


Figura 3.45. Diagrama de clases de las clases JAXB del cliente del servicio web para la consulta de mediciones.

De acuerdo a los requerimientos funcionales de la aplicación, y en base a los casos de uso, determinados en el capítulo de análisis, se ha establecido que el cliente del servicio web para la consulta de mediciones debe realizar las siguientes consultas:

- Consulta de mediciones registradas.
- Consulta de mediciones por usuario.
- Consulta de mediciones por usuario y fecha de medición.
- Consulta del índice de disponibilidad del servicio de Internet de usuario.

➢ **Consulta de mediciones registradas.**

La consulta de todas las mediciones registradas por la aplicación, se realiza a través de la opción "*Registradas"* dentro de la página web JSP de inicio. Al seleccionar ésta opción se accederá a la página web JSP *resultadoTodasMediciones.jsp*, la misma

que desplegará una lista de todas las mediciones registradas por la aplicación hasta ese momento, Figura 3.46 y 3.47.

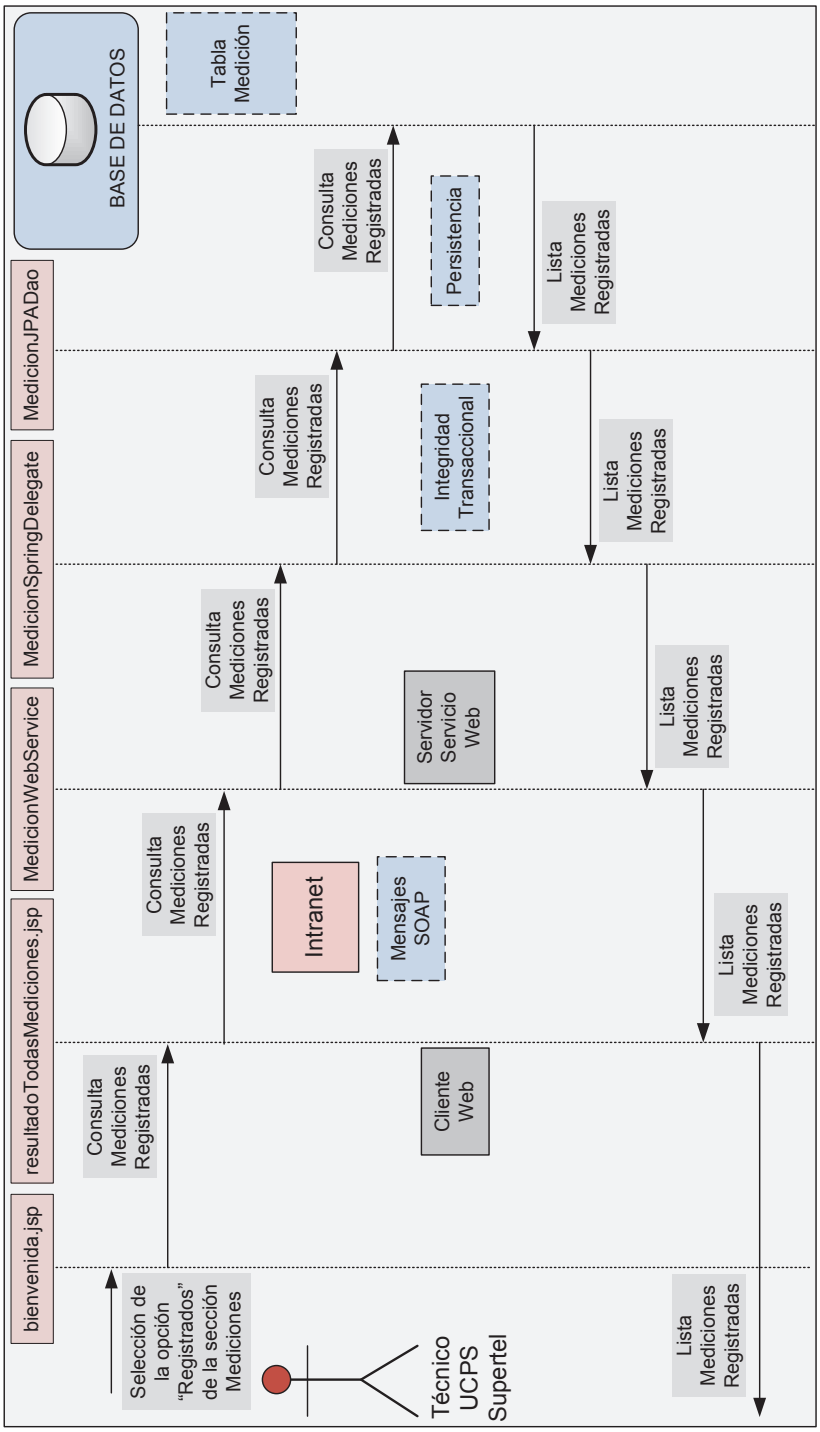


Figura 3.46. Diagrama de secuencia para la consulta de mediciones registradas.

La página web JSP *resultadoTodasMediciones.jsp* es también la encargada de realizar el consumo del servicio web, y la conversión entre objetos java y contenido XML con la ayuda de las clases JAXB *MedicionType* y *MedicionResultType*.

- **Consulta de mediciones por usuario.**

La consulta de mediciones pertenecientes a un usuario monitoreado, se realiza por medio de ésta consulta, y en la cual es requerido ingresar como parámetro de consulta la dirección MAC con la que fue registrado el usuario. Por ésta razón, el personal técnico de la UCPS debe conocer de antemano la dirección MAC del usuario monitoreado del cual se requiere consultar sus mediciones.

Desde la página web JSP de inicio, en el apartado de Mediciones, se selecciona la opción *"Buscar por Usuario"*, la misma que direccionará a la página web JSP *buscarMedicionXMac.jsp*. En la página *buscarMedicionXMac.jsp* se presenta un formulario para el ingreso de la dirección MAC del usuario, y un botón de aceptación de búsqueda. Al aceptar la búsqueda, la solicitud será direccionada a la página *handlerBuscarMedicionXMac.jsp*, la misma que se encargará de consumir el servicio web, y de realizar la conversión de objetos java a contenido XML de la dirección MAC indicada.

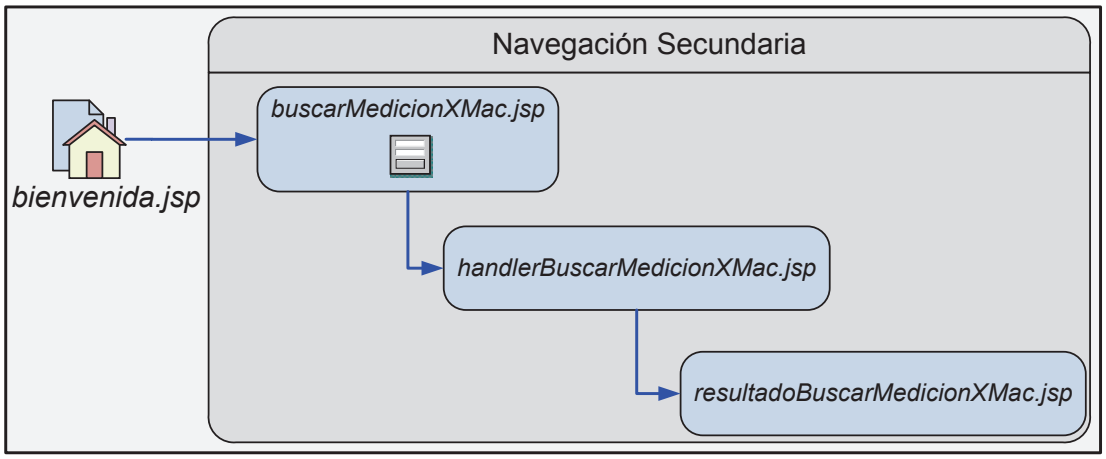


Figura 3.47. Diagrama de navegación web para la consulta de mediciones por usuario.

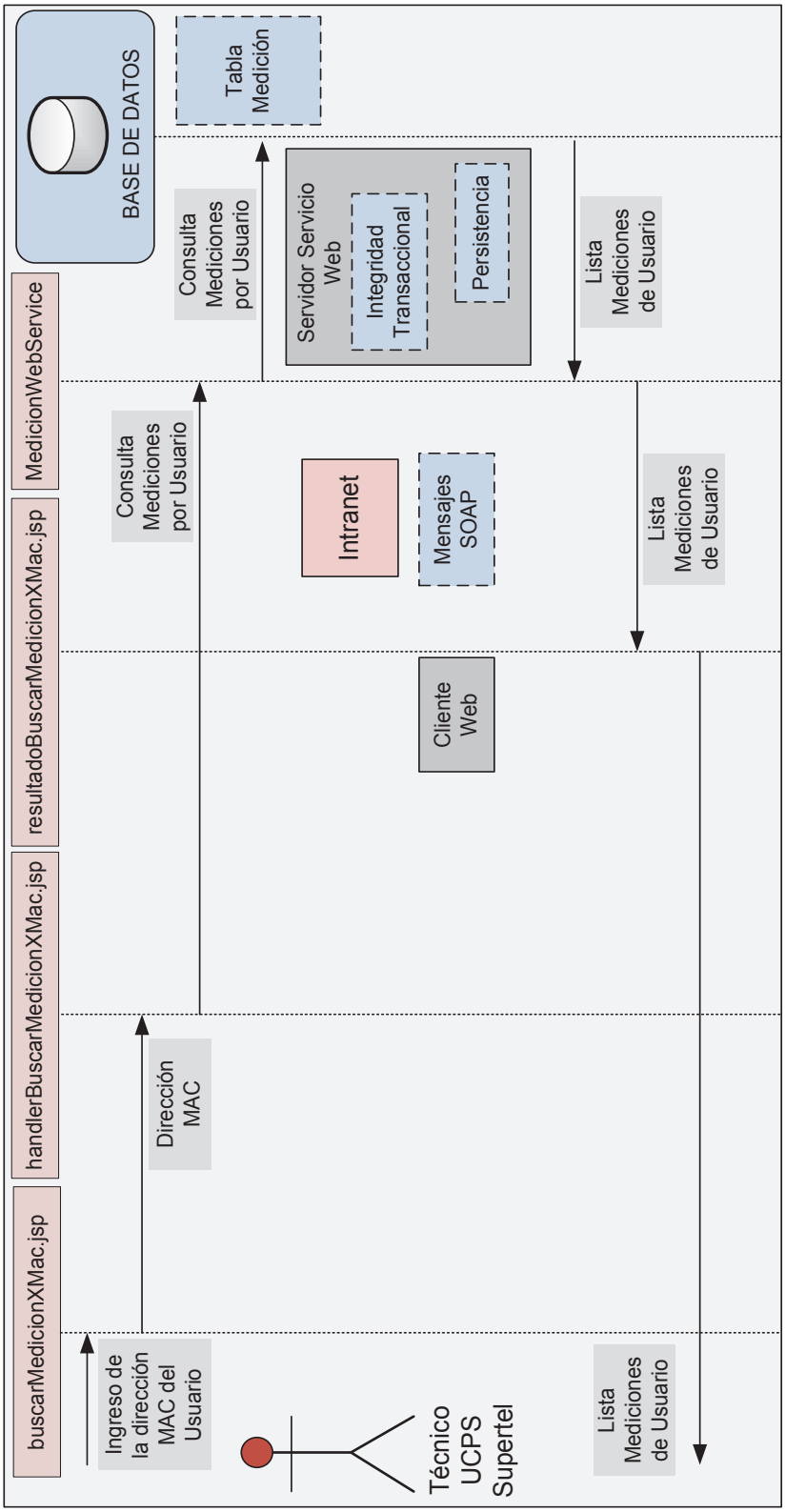


Figura 3.48. Diagrama de secuencia para la consulta de mediciones por usuario

Una vez que la página *handlerBuscarMedicionXMac.jsp* envía la solicitud de consulta al servicio web, delega a la página *resultadoBuscarMedicionXMac.jsp* la conversión de contenido XML a objetos Java para la presentación de los resultados obtenidos de la consulta. Figura 3.47 y Figura 3.48. La página *resultadoBuscarMedicionXMac.jsp* dispondrá de un espacio de ingreso de texto que será usado por el tipo de consulta a continuación.

- **Consulta de mediciones por usuario y fecha de medición.**

El proceso para la consulta de mediciones por usuario y fecha de medición es semejante a la expuesta para la búsqueda de mediciones por usuario, pero se extiende un poco más allá, ya que en la página web JSP *resultadoBuscarMedicionXMac.jsp* se dispone de un cuadro de texto para el ingreso de la fecha para la cual se requiere la nueva consulta de las mediciones pertenecientes al usuario ya especificado. La consulta por fecha es aceptada por medio del uso de un botón web.

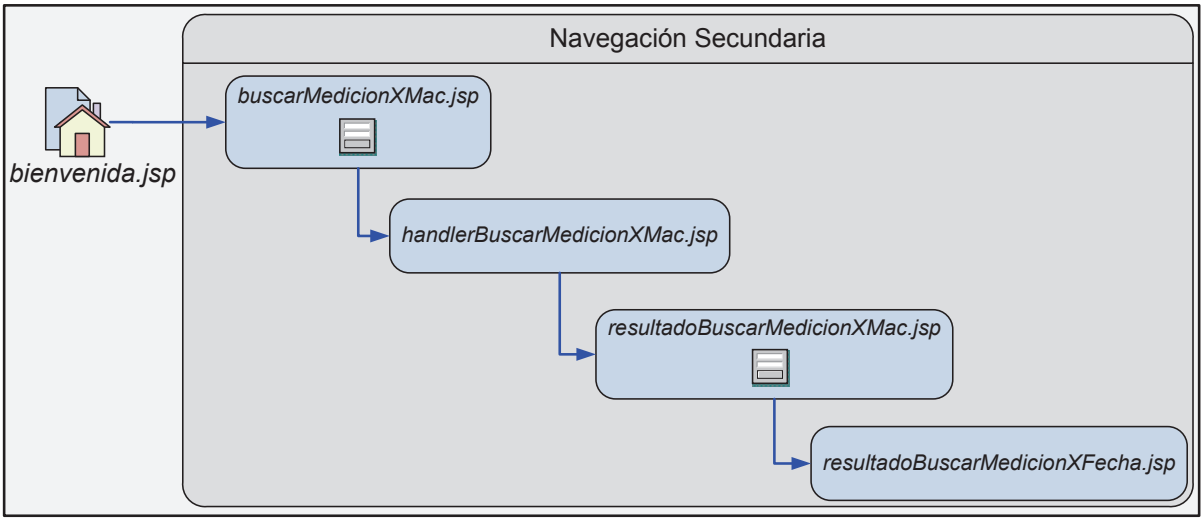


Figura 3.49. Diagrama de navegación web para la consulta de mediciones por usuario y fecha de medición.

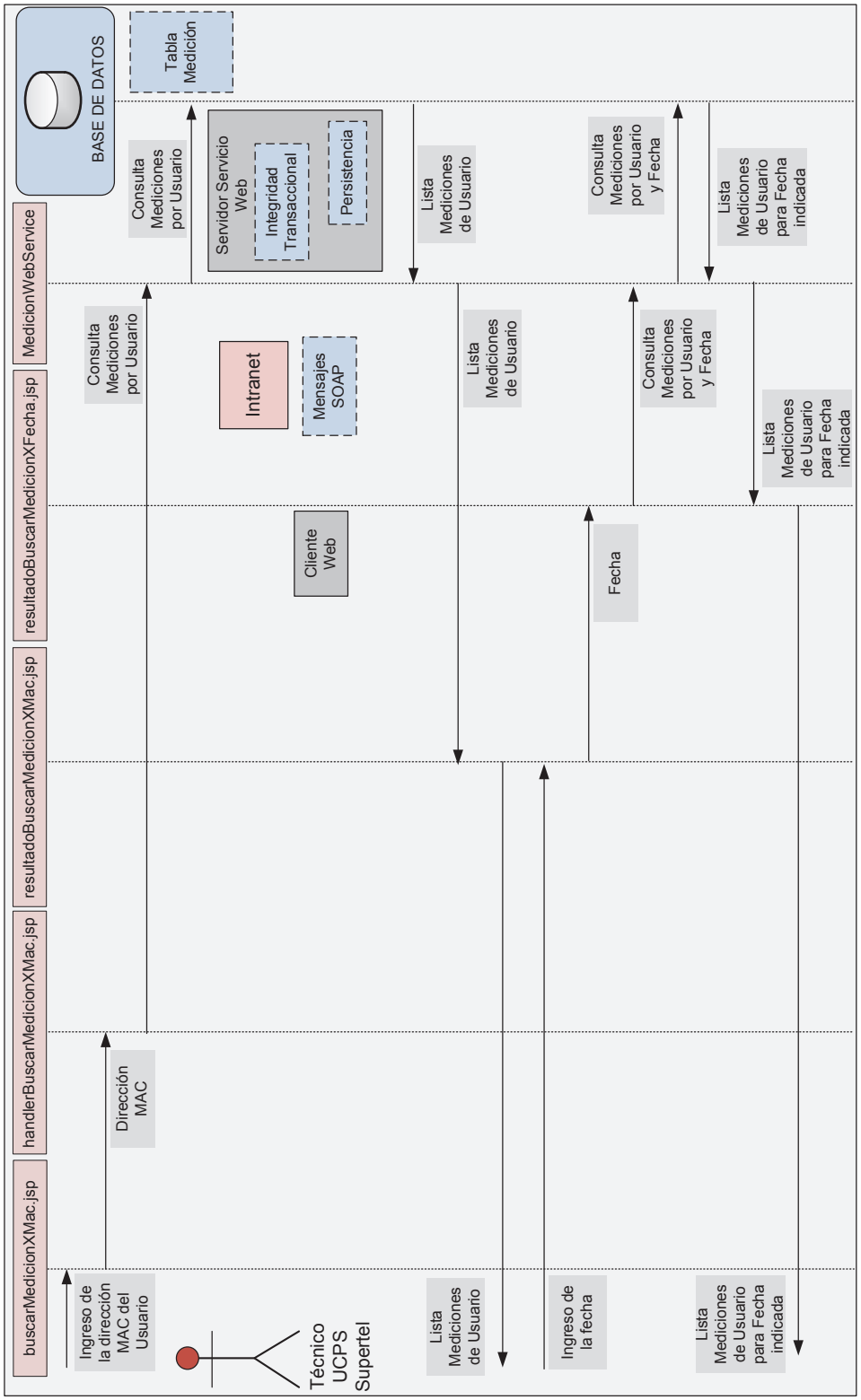


Figura 3.50. Diagrama de secuencia para la consulta de mediciones por usuario y fecha de medición.

La página *resultadoBuscarMedicionXMac.jsp*, toma la fecha indicada por el operario del cliente del servicio web, y la envía a la página *resultadoBuscarMedicionXFecha.jsp*, la misma que se encargará de hacer la consulta al servidor del servicio web respectivo, y de realizar la conversión entre objetos Java y contenido XML. Además, la clase *resultadoBuscarMedicionXMac.jsp*, representa la interfaz gráfica por medio de la cual se presentaran los resultados de la consulta de mediciones por usuario y fecha. Figura 3.49 y Figura 3.50.

Para realizar la búsqueda de mediciones de un usuario en una fecha determinada de captura, es necesario introducir la fecha siguiendo el siguiente formato:

yyyy/MM/dd_HH:mm:ss

Bajo éste formato es posible realizar la consulta de mediciones capturadas por minuto, hora, día, mes e incluso año, todo depende de la porción del formato que sea introducida para la consulta, tabla 3.13.

Tabla 3.13. Formato de fecha para la consulta de mediciones por usuario y fecha.

Porción de formato	Tipo de consulta
yyyy/MM/dd_HH:mm	Por minuto
yyyy/MM/dd_HH	Por hora
yyyy/MM/dd	Por día
dd/MM/	Por mes

- **Consulta del índice de disponibilidad del servicio de Internet del usuario.**

En base al análisis de los requerimientos funcionales de la aplicación de monitorización, definido en el capítulo de análisis, el personal técnico de la UCPS

deberá realizar la consulta del índice de disponibilidad del servicio de Internet con el que cuenta el usuario por hora.

Ésta consulta se realiza partiendo desde la página *resultadoBuscarMedicionXMac.jsp* resultante de la consulta de mediciones por usuario previamente desarrollada. En la página *resultadoBuscarMedicionXMac.jsp* existe una opción llamada *"Calcular el índice de disponibilidad del servicio de Internet"* el mismo que direccionará a la página *calculoDisponibilidad.jsp*.

La página *calculoDisponibilidad.jsp* despliega un formulario para el ingreso de la hora para la cual se desea calcular el índice de disponibilidad del servicio de Internet. Además, existe un botón de aceptación de búsqueda, el mismo que llamará a la página *resultadoDisponibilidad.jsp*, encargada de presentar la lista de mediciones de usuario para la hora indicada, junto con el valor de disponibilidad del servicio de Internet obtenido, Figura 3.52 y Figura 3.53.

El formato de búsqueda requerido para el cálculo del índice de disponibilidad por hora es el siguiente:

yyyy/MM/dd_HH

El cálculo del índice de disponibilidad se efectúa en base al número de mediciones almacenadas en la tabla Medición, ya que las mediciones recibidas por la aplicación son prueba fehaciente de que el usuario monitorizado dispone con el servicio de Internet en el periodo de tiempo en el que fueron registradas.

Para que los resultados del cálculo del índice de disponibilidad sean más cercanos a la realidad, se debe asegurar que el usuario tenga su dispositivo monitoreado activo durante el tiempo considerado para la prueba, teniendo así la certeza de que las mediciones no recibidas corresponden efectivamente a la ausencia del servicio y no otra causa.

Por definición, el índice de disponibilidad del servicio de Internet se calcula en base al tiempo durante el cual el servicio se encuentra disponible, pero es posible determinar un valor bastante aproximado de acuerdo a la siguiente fórmula basada en el número de mediciones capturadas por la aplicación durante una hora:

$$\%Disponibilidad\ por\ hora = \frac{\#\ Mediciones\ en\ una\ hora}{870} * 100$$

Figura 3.51. Fórmula para el cálculo del índice de disponibilidad del servicio de Internet usada por la aplicación.

El valor de 870 mediciones es estimado en base a que entre 14 y 15 mediciones son recibidas por la aplicación por minuto (una medición cada 4 segundos).

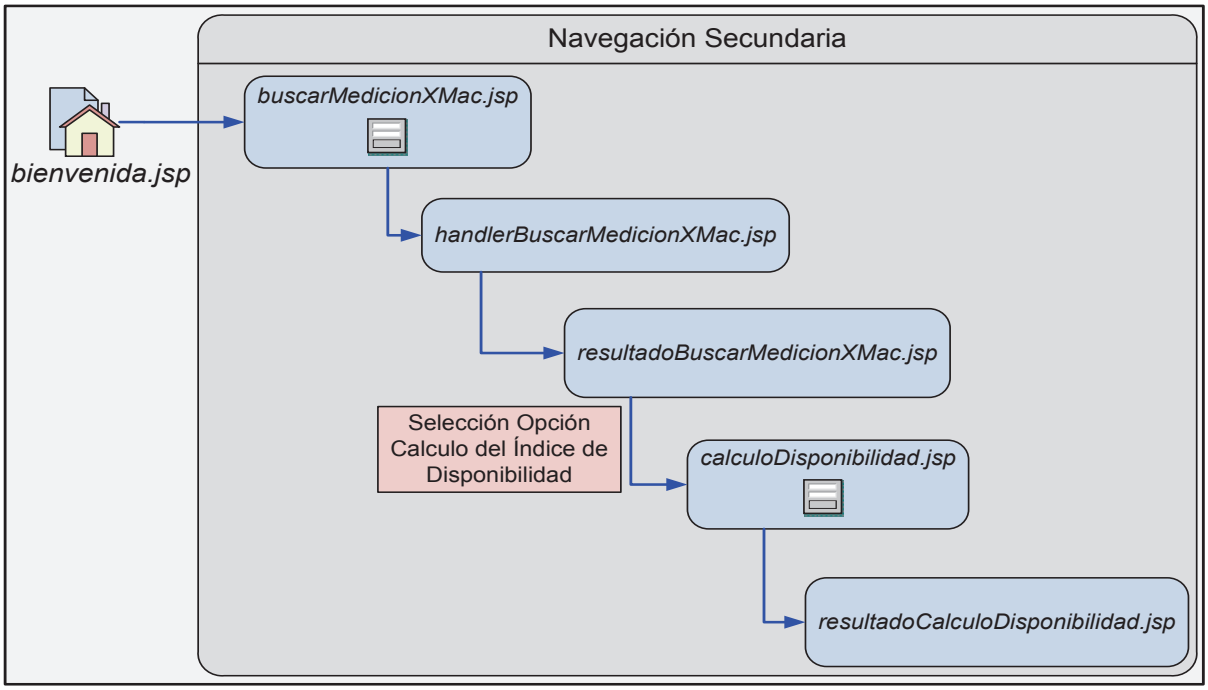


Figura 3.52. Diagrama de navegación web para el cálculo del índice de disponibilidad del servicio de Internet del usuario.

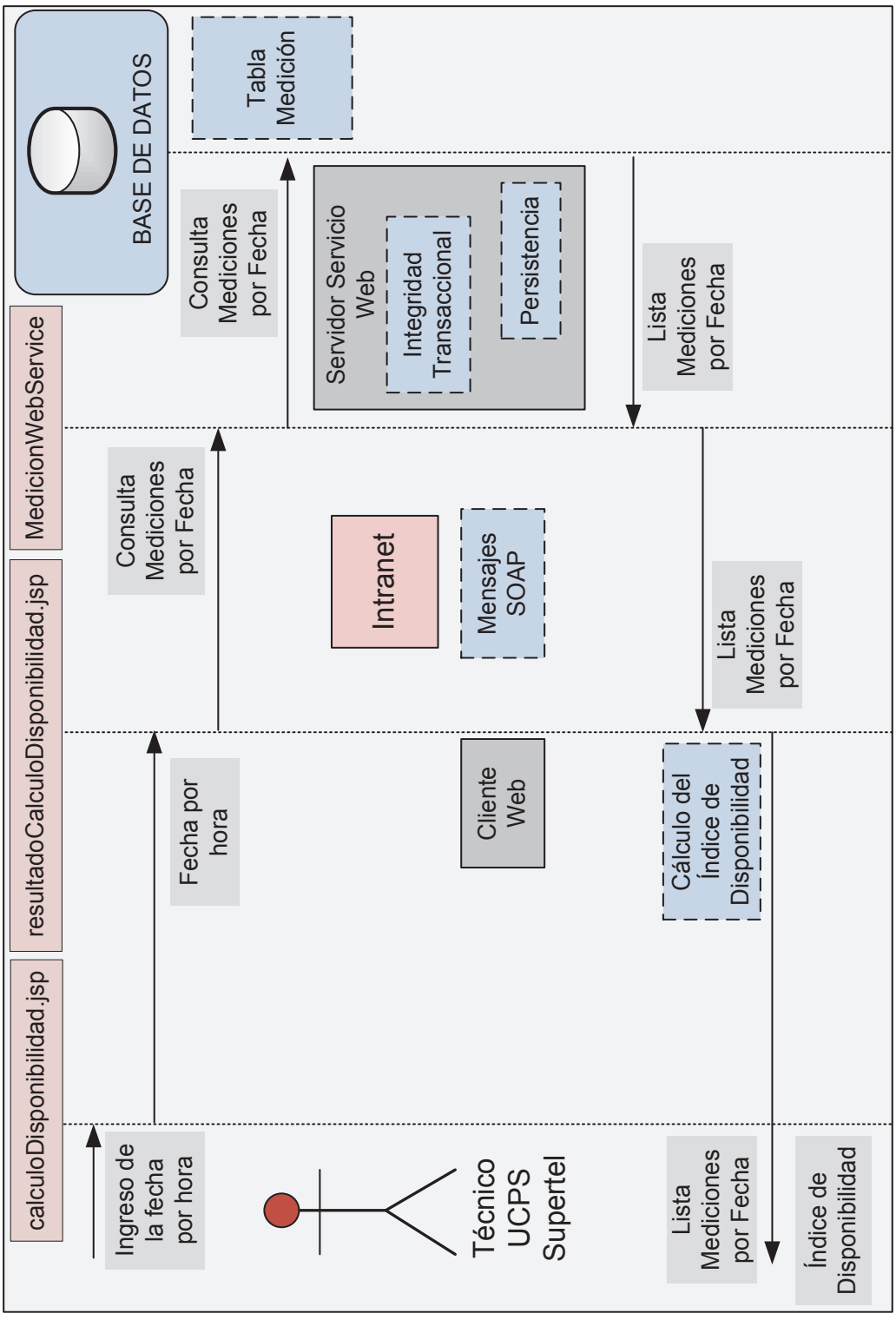


Figura 3.53. Diagrama de secuencia para la consulta del índice de disponibilidad del servicio de Internet del usuario.

3.4.2.4.2 Cliente del Servicio Web para la consulta y gestión de usuarios

El cliente del servicio web para la consulta y gestión de usuarios tiene como propósito, el consumo de los servicios web relacionados con la tabla Usuario de la base de datos relacional de la aplicación.

En base al análisis de requerimientos de la nueva aplicación, y de los casos de uso determinados en el capítulo de análisis, se ha determinado que éste cliente del servicio web realice las siguientes operaciones sobre los registros de la tabla Usuario:

- Consulta de usuarios registrados.
- Ingreso de nuevo usuario.
- Búsqueda de usuario.
- Modificación de usuario.
- Eliminación de usuario.

Todas las operaciones antes mencionadas, son realizadas por éste cliente con la ayuda de páginas web JSP, y de los esquemas JAXB *UsuarioType* y *UsuarioResultType*, Figura 3.54, necesarios para la conversión entre objetos Java y contenido XML relacionados con las operaciones realizadas por éste cliente.

- **Consulta de usuarios registrados**

El personal técnico de la UCPS realiza la consulta de todos los usuarios registrados hasta ese momento, seleccionando dentro la sección de gestión de usuarios, de la página de inicio *bienvenida.jsp* la opción llamada *"Registrados"*, para posteriormente ser direccionados a la página *resultadoTodosUsuarios.jsp.*

La página web *resultadoTodosUsuarios.jsp* está encargada de desplegar en pantalla la lista de usuarios registrados, de consumir el servicio web designado, y de convertir contenido XML a objetos Java con la ayuda de las clases JAXB *UsuarioType* y *UsuarioResultType*, Figura 3.55.

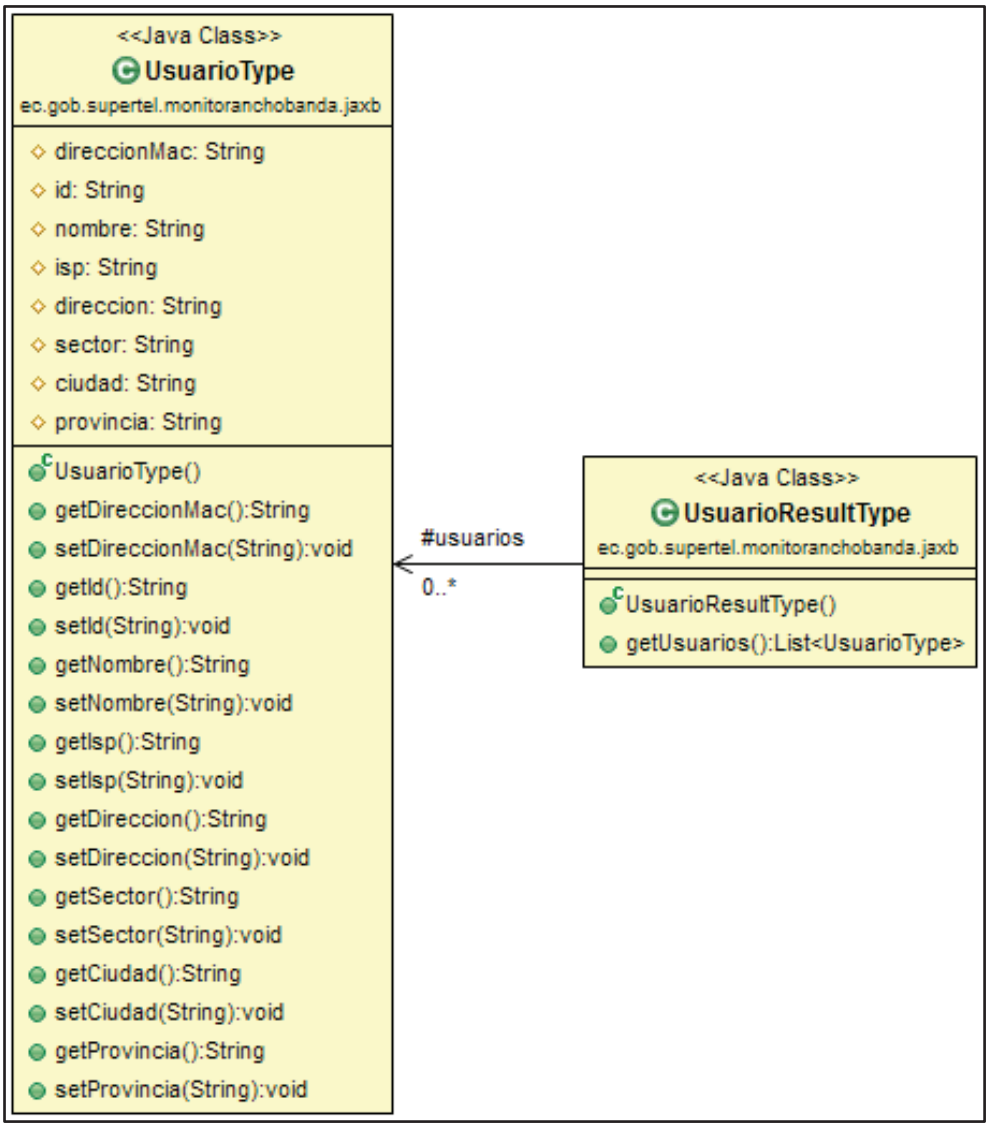


Figura 3.54. Diagrama de clases de las clases JAXB del cliente del servicio web para la consulta de usuarios.

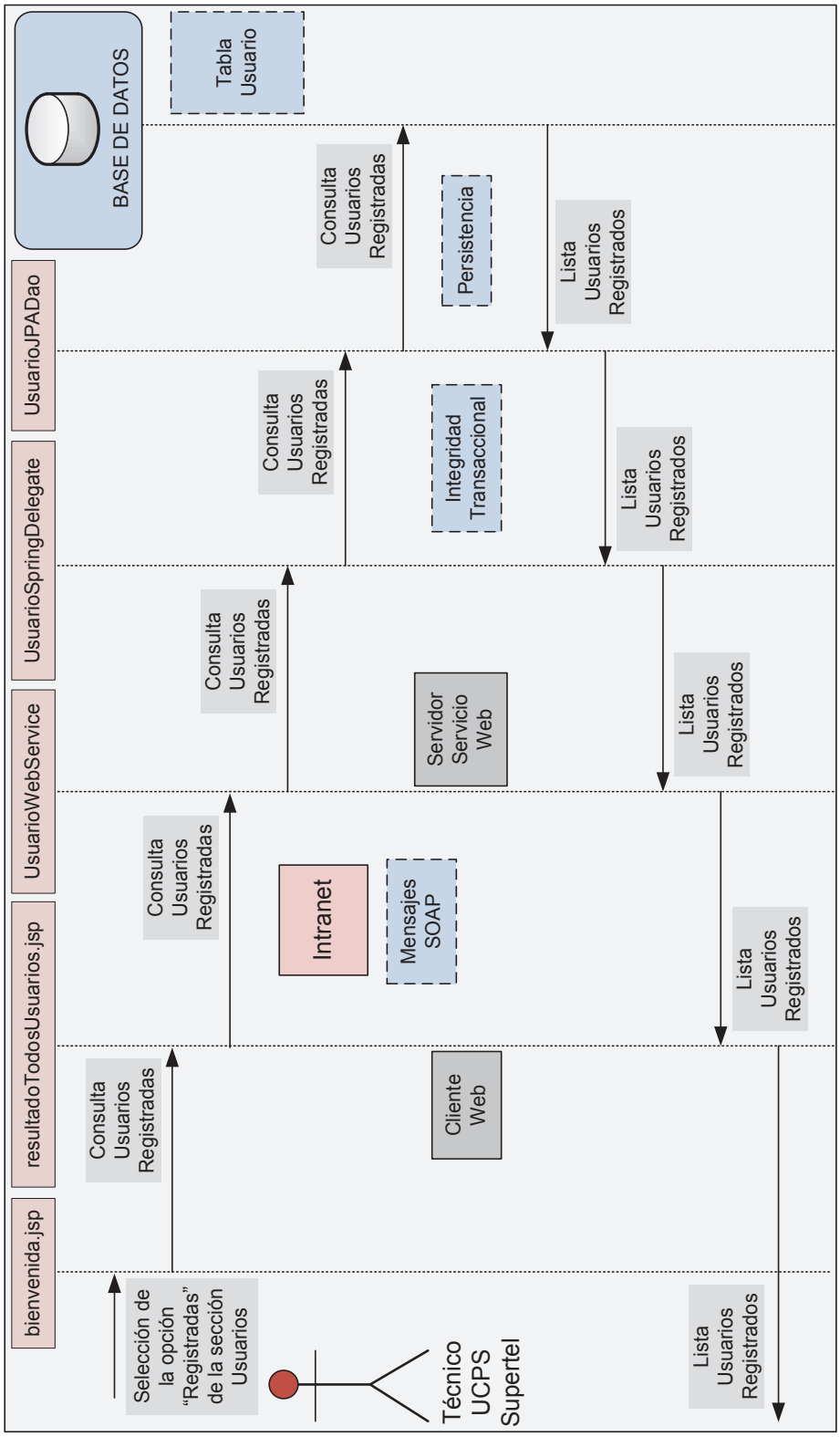


Figura 3.55. Diagrama de secuencia para la consulta de usuarios registrados.

- **Ingreso de nuevo usuario.**

El ingreso de nuevos usuarios se realiza desde la página web JSP de inicio *bienvenida.jsp*, seleccionando en ésta la opción llamada *"Nuevo"* dentro de la sección destinada a la administración de usuarios monitorizados. Al seleccionar ésta opción, la aplicación llamará a la página web *addUsuario.jsp*, la misma que presentará un formulario en la que el personal técnico de la UCPS deberá ingresar los datos pertenecientes al nuevo usuario monitoreado que se desea ingresar al sistema.

Una vez ingresados los datos del nuevo usuario, se acepta el ingreso mediante un botón web, y la información recolectada por la página *addUsuario.jsp* es enviada a la página *handlerAddUsuario.jsp*, la misma que se encarga de la conversión de objetos java a contenido XML, y del consumo del servicio web para el ingreso del nuevo usuario. Si el nuevo usuario es ingresado con éxito, se llama a la página *resultadoTodosUsuarios.jsp*, para que muestre todos los usuarios registrados hasta ese momento, incluyendo el recién añadido, Figura 3.56 y 3.57.

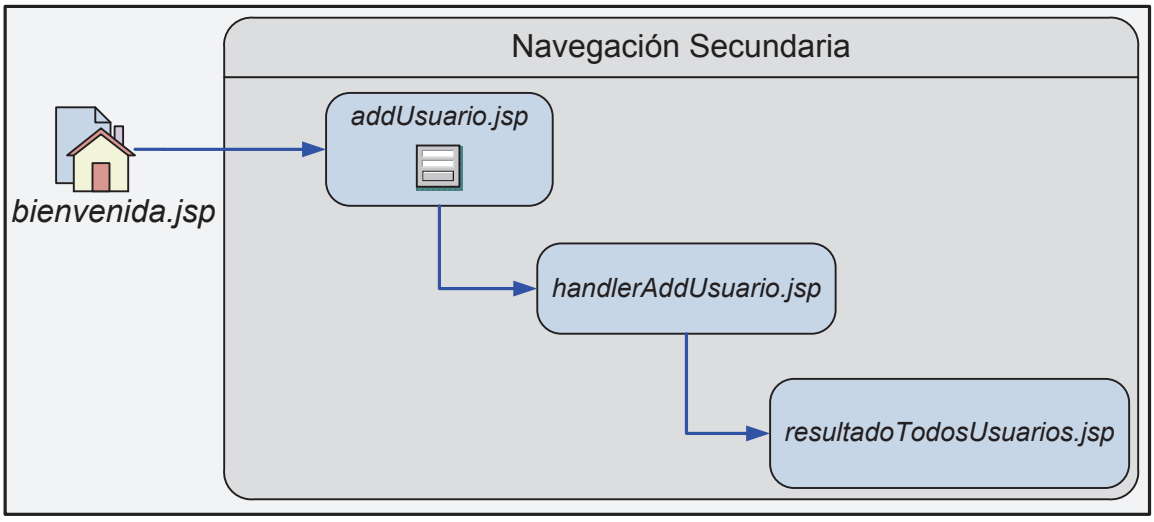


Figura 3.56. Diagrama de navegación web para el ingreso de nuevo usuario.

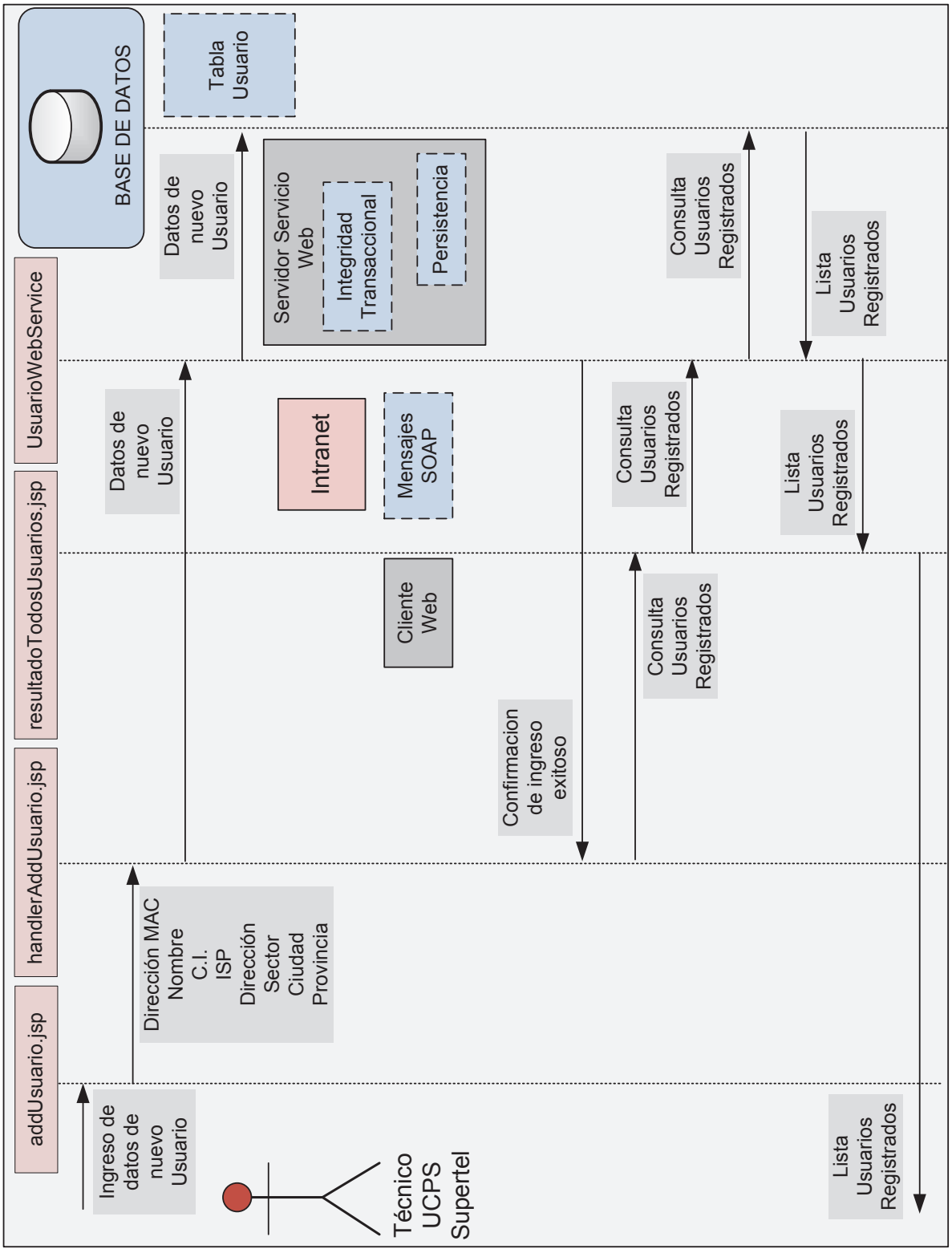


Figura 3.57. Diagrama de secuencia para el ingreso de nuevo usuario.

- **Búsqueda de usuario.**

El proceso de buscar usuarios se inicia mediante la selección de la opción *"Buscar"*, ubicada en la sección de gestión de Usuarios dentro de la página de inicio *bienvenida.jsp*, la misma que llamara a la página *buscarUsuarioXMac.jsp*. La página *buscarUsuarioXMac.jsp* mostrara un formulario para el ingreso de la dirección MAC del usuario al que se desea buscar, y un botón web de aceptación de búsqueda, el que a su vez llamara a la página *handlerBuscarUsuarioXMac.jsp*.

La página *handlerBuscarUsuarioXMac.jsp* es la encargada de realizar la conversión de objetos Java a contenido XML por medio de las clases JAXB *UsuarioType* y *UsuarioResultType*, y del consumo del servicio web designado a la búsqueda de usuarios. Una vez consumido el servicio web de búsqueda, la aplicación llama a la página *resultadoBuscarUsuarioXMac.jsp*, Figura 3.58 y Figura 3.59.

La página *resultadoBuscarUsuarioXMac.jsp* realiza la conversión de contenido XML a objetos java y despliega en pantalla al usuario buscado junto con toda la información de éste.

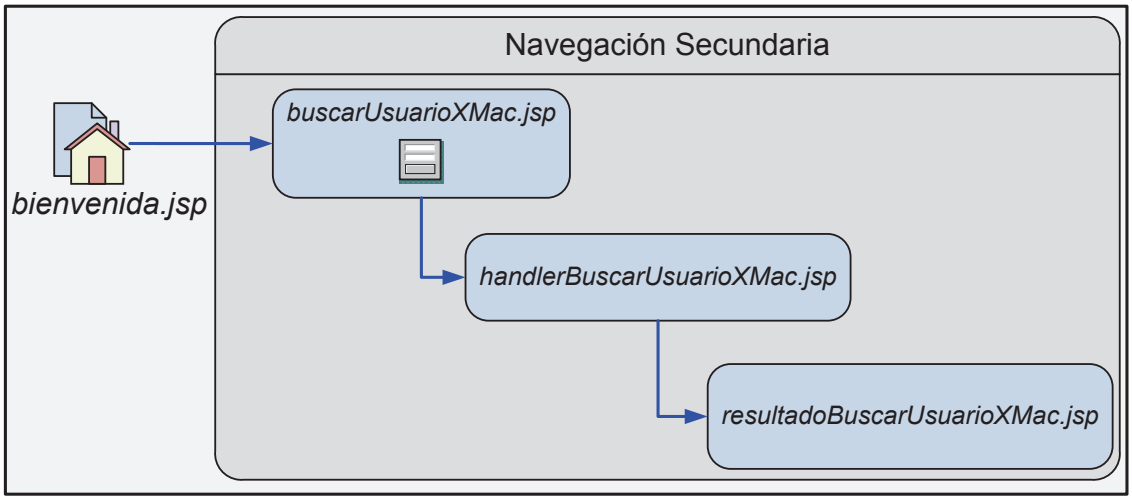


Figura 3.58. Diagrama de navegación web para la búsqueda de usuario.

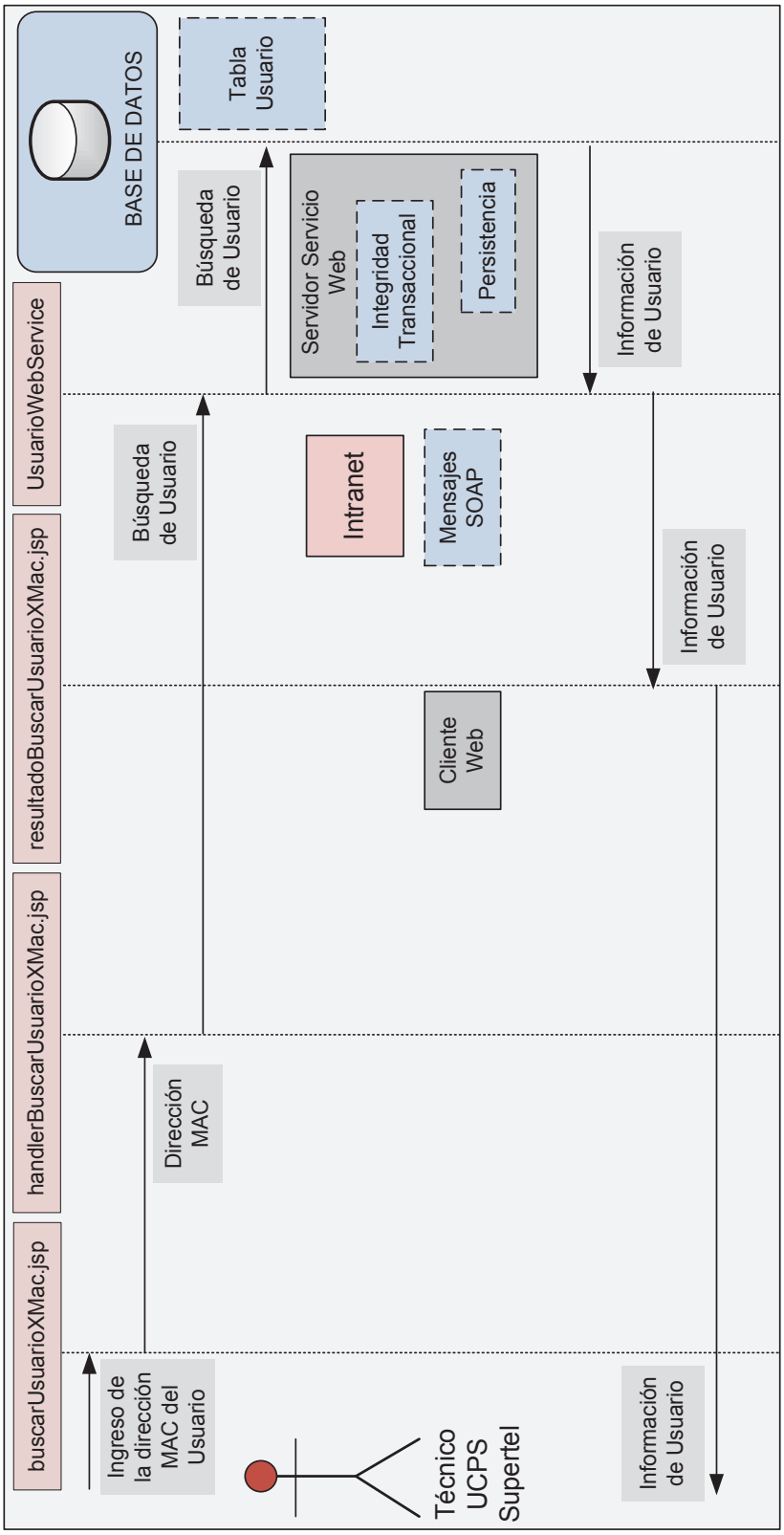


Figura 3.59. Diagrama de secuencia para la búsqueda de usuario.

- **Modificación de usuario.**

La búsqueda de usuarios se realiza a partir del proceso de búsqueda de usuarios explicado en el punto anterior, por lo que se parte de los resultados obtenidos por la página *resultadoBuscarUsuarioXMac.jsp*. Ésta página web presenta la opción llamada *"Modificar"*, a través del cual se acede a la página *modificarUsuario.jsp*.

La página *modificarUsuario.jsp* despliega en pantalla un formulario para el ingreso de los nuevos datos del usuario que se desea modificar, y se encarga de pasar los datos de actualización a la página *handlerModificarUsuario.jsp*, la que a su vez realiza las tareas de consumo del servicio web para la modificación de usuario, y la conversión de objetos Java a contenido XML.

Después de que la modificación de usuario se haya realizado correctamente, la página *resultadoTodosUsuarios.jsp* es llamada para desplegar todos los usuarios registrados, entre los que se encuentra el usuario modificado junto con sus datos actualizados, Figura 3.60 y Figura 3.61.

Es posible modificar todos los valores del registro usuario excepto la dirección MAC, ya que ésta es la llave primaria de los registros almacenados en la tabla Usuario, y por integridad de la base de datos la aplicación no permite modificar éste campo.

- **Eliminación de Usuario.**

La eliminación de usuario parte de la página *resultadoBuscarUsuarioXMac.jsp* obtenida tras el proceso de búsqueda de un usuario a través de su dirección MAC. En la página *resultadoBuscarUsuarioXMac.jsp* se presenta una opción llamada *"Eliminar"*, la misma que al ser seleccionada, direccionará la aplicación a la página *eliminarUsuario.jsp*, la que básicamente pide la confirmación de eliminación del usuario y llama a la página *handlerEliminarUsuario.jsp*.

La página *handlerEliminarUsuario.jsp* es la encargada de consumir el servicio web para la eliminación de los registros de la tabla Usuario, y de realizar la conversión de objetos Java a contenido XML.

Al realizarse la eliminación de usuario correctamente, la página *resultadoTodosUsuarios.jsp* es llamada para mostrar el contenido actualizado de la tabla Usuario, Figura 3.62 y 3.63.

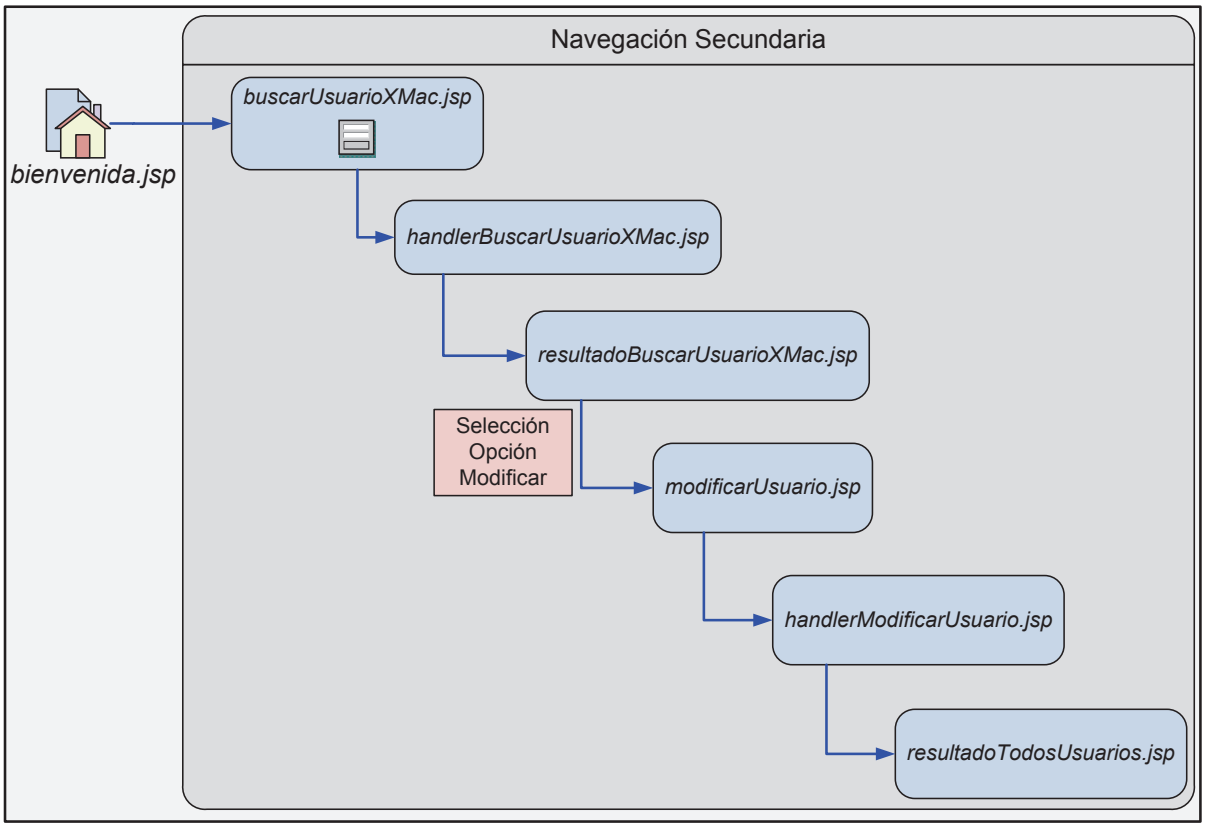


Figura 3.60. Diagrama de navegación web para la modificación de usuario.

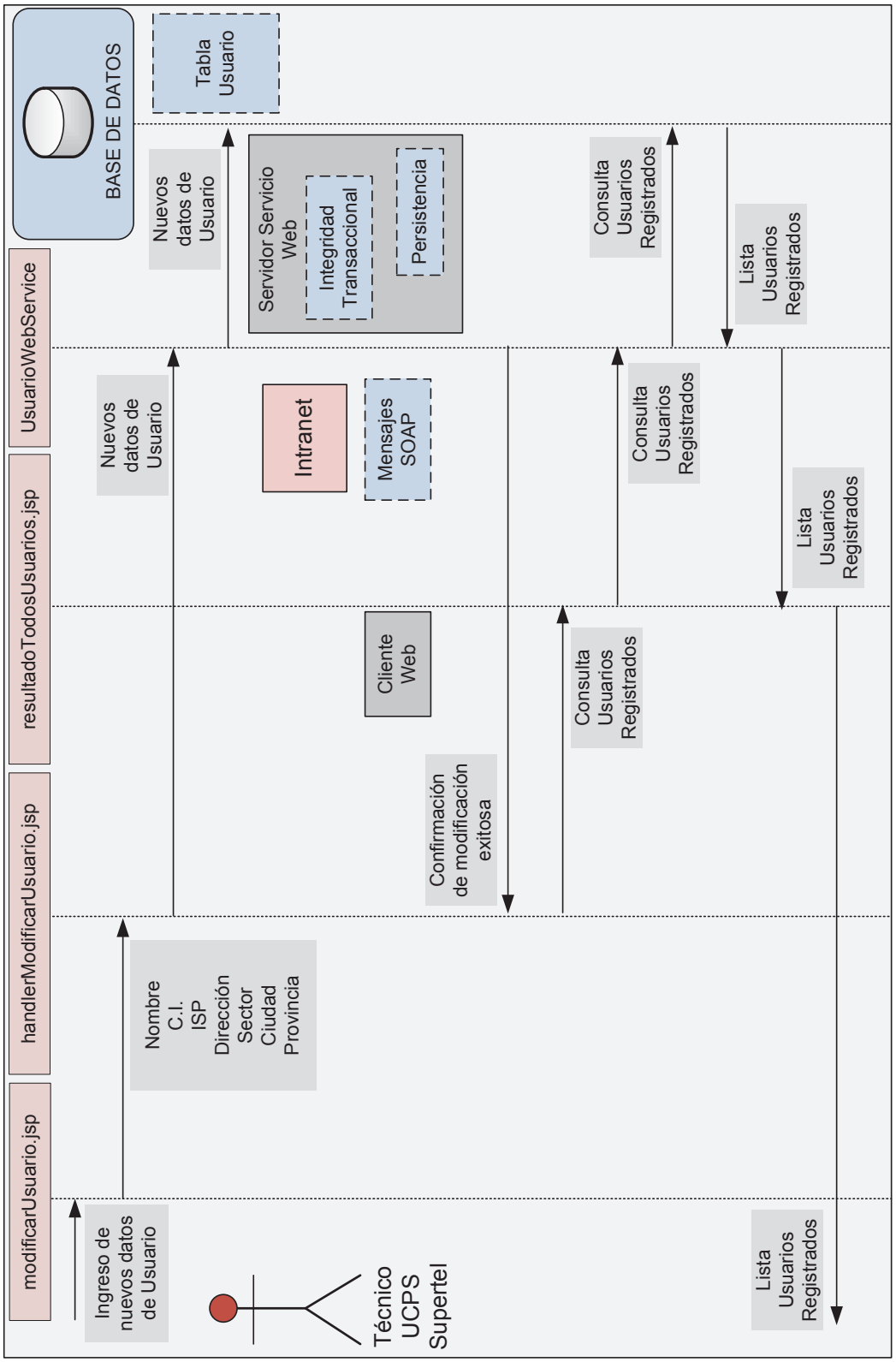


Figura 3.61. Diagrama de secuencia para la modificación de usuario.

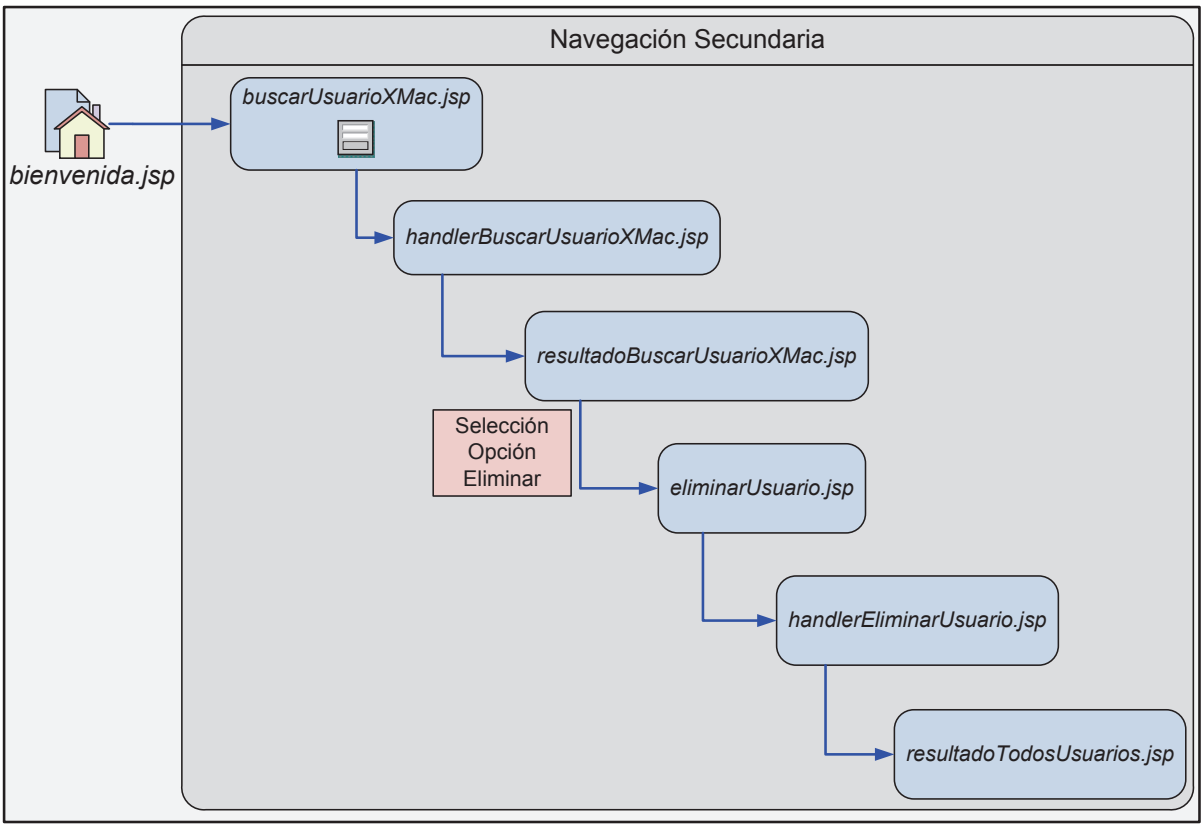


Figura 3.62. Diagrama de navegación web para la eliminación de usuario.

3.4.2.4.3 Acceso y seguridad del Cliente del Servicio Web de Consultas

El sistema de acceso al Cliente del Servicio Web de Consultas de la aplicación, es la autenticación de usuarios mediante el uso del servidor CAS Jasig, ya en funcionamiento en la SUPERTEL. El servidor CAS basa su funcionamiento principalmente en el protocolo LDAP, para determinar los recursos de capa aplicación a los que tiene acceso cada usuario o técnico de la SUPERTEL.

De éste modo, el personal técnico de la UCPS accederá al cliente del servicio web de la presente aplicación presentando sus credenciales a través de la página web institucional de la Intranet, la misma que direccionará al usuario a las página web JSP de inicio del Cliente del servicio Web de Consultas de la aplicación de monitoreo para el control los usuarios del servicio de Internet.

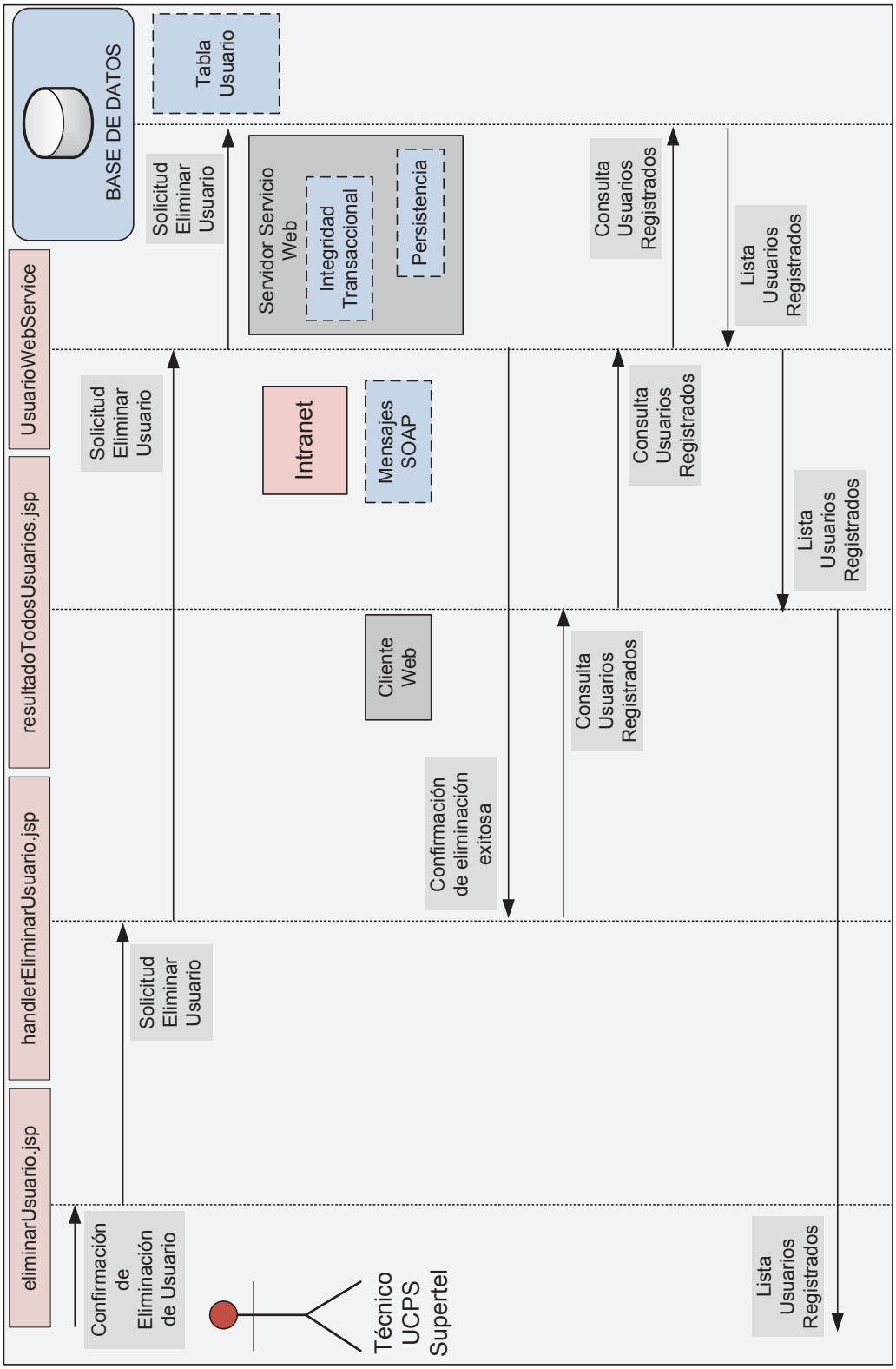


Figura 3.63. Diagrama de secuencia para la eliminación de usuario.

CAPÍTULO IV: PRUEBAS Y ANÁLISIS DE RESULTADOS

En éste capítulo se presentan las pruebas de funcionamiento de todos los módulos que conforman la nueva aplicación de monitoreo, para luego realizar el análisis de resultados obtenidos por la aplicación y determinar si cumplen o no con los requerimientos establecidos en el capítulo de análisis del presente documento. De igual manera, se realizará la comparación de los resultados finales de la aplicación con los resultados obtenidos por otras aplicaciones que realicen la misma función.

4.1 HERRAMIENTAS DE PRUEBA Y ANÁLISIS DE RESULTADOS

La aplicación del presente proyecto realizará las respectivas pruebas y análisis de resultados con la ayuda de las aplicaciones Wireshark 1.12.0, RawCap, y del IDE de desarrollo Java Eclipse 3.8.0, para la visualización de los resultados módulo por módulo. De ésta forma no solo serán probados y analizados los módulos que presenten información a los usuarios, sino que también son considerados todos los módulos que no presenten una interfaz gráfica de usuario.

4.2 PRUEBA DE FUNCIONAMIENTO DEL MÓDULO DE CAPTURA Y CÁLCULO DE DATOS DE MONITORIZACIÓN

Éste módulo será probado y sus resultados analizados por medio del IDE Eclipse, el mismo que permitirá la presentación de los datos obtenidos por éste módulo a través de la pantalla de consola. Para llevar a cabo la prueba, se ha añadido una sección *main* (código ejecutable) a la clase *MonitorABImplementacionSigar* perteneciente a éste módulo, para que despliegue en pantalla la información que ésta debe obtener para ser utilizada por la aplicación de monitorización.

Los datos involucrados en éste módulo son los siguientes:

- Lista de Interfaces de red.
- Número de la interfaz de red conectada a Internet.
- Octetos de Entrada de la interfaz de red.

- Octetos de Salida de la interfaz de red.
- Ancho de banda de bajada de la interfaz de red.
- Ancho de banda de subida de la interfaz de red.
- Dirección MAC de la interfaz de red.

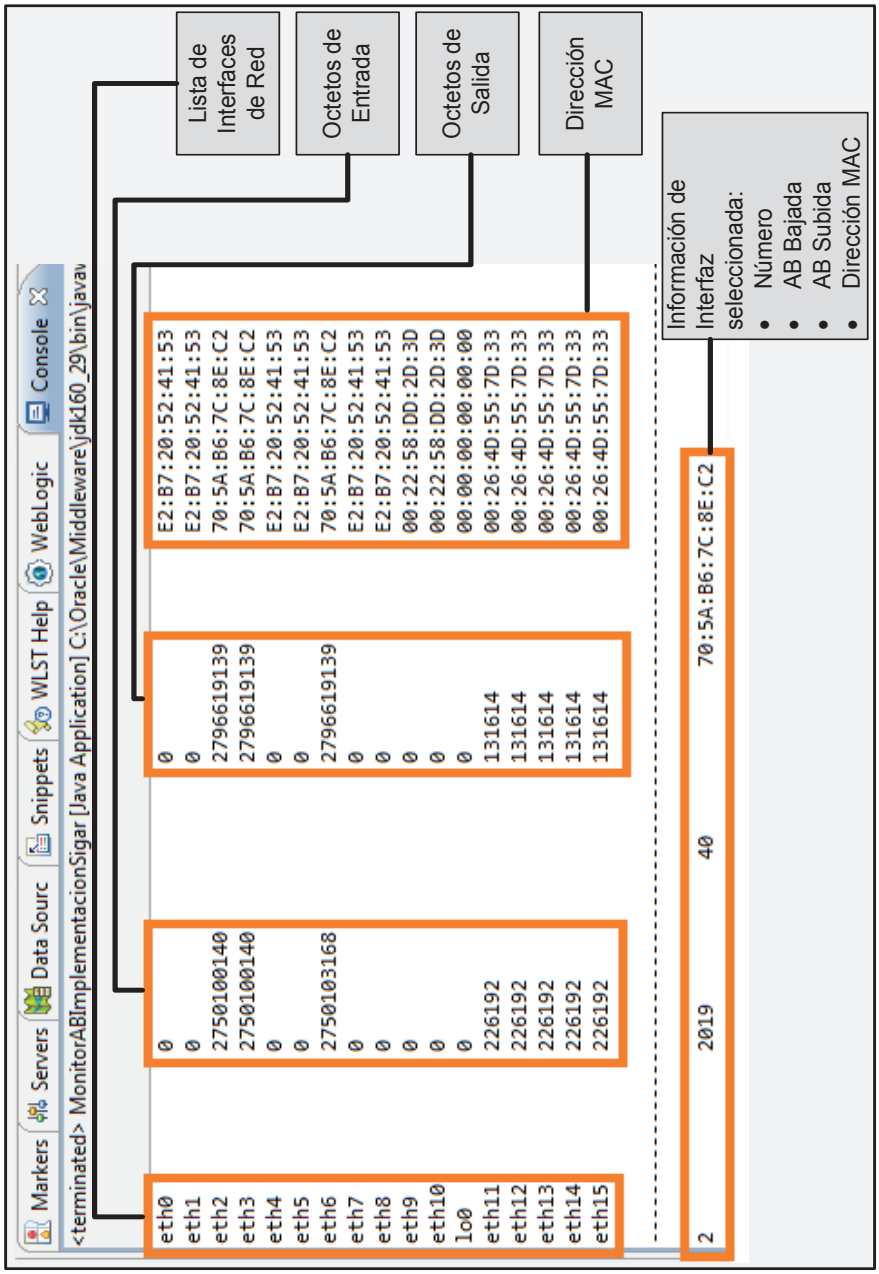


Figura 4.1. Prueba de funcionamiento del Módulo de Captura y Cálculo de datos de Monitorización.

Como se ve en la Figura 4.1, éste módulo efectivamente selecciona la interfaz de red conectada al Internet, ya que es la que más octetos de entrada acumula. Una vez conocida la interfaz de red requerida, el módulo captura la dirección MAC, y calcula el ancho de banda de bajada y de subida para ésta interfaz de red de forma correcta.

Se puede asegurar entonces, que éste módulo cumple con los requerimientos necesarios de la aplicación para la captura de datos de monitorización relacionados con el ancho de banda y dirección MAC del usuario del servicio de Internet.

4.3 PRUEBA DE FUNCIONAMIENTO DEL MÓDULO AGENTE SNMP VERSIÓN 3 Y MÓDULO AGENTE SNMP VERSION 3

La forma adecuada de probar el correcto funcionamiento de éstos módulos, es haciéndolos funcionar de manera conjunta, ya que el propósito del uno depende del propósito del otro.

Éstos módulos son probados mediante la herramienta computacional Wireshark, y el IDE Eclipse, donde éste último permitirá la exposición de los resultados arrojados por el funcionamiento en conjunto de éstos módulos. Por lo tanto a la clase *MonitorABGestorSNMPV3* del módulo Gestor SNMP versión 3 se le ha añadido una sección de código *main* para la impresión en pantalla de consola de los datos consultados por los módulos a prueba.

Los módulos en cuestión se encargan de manejar la información relacionada con las consultas SNMP de los datos de monitorización indicadas a continuación:

- OID MIB para el ancho de banda de bajada.
- OID MIB para el ancho de banda de subida.
- Ancho de banda de bajada.
- Ancho de banda de subida.
- Dirección MAC.

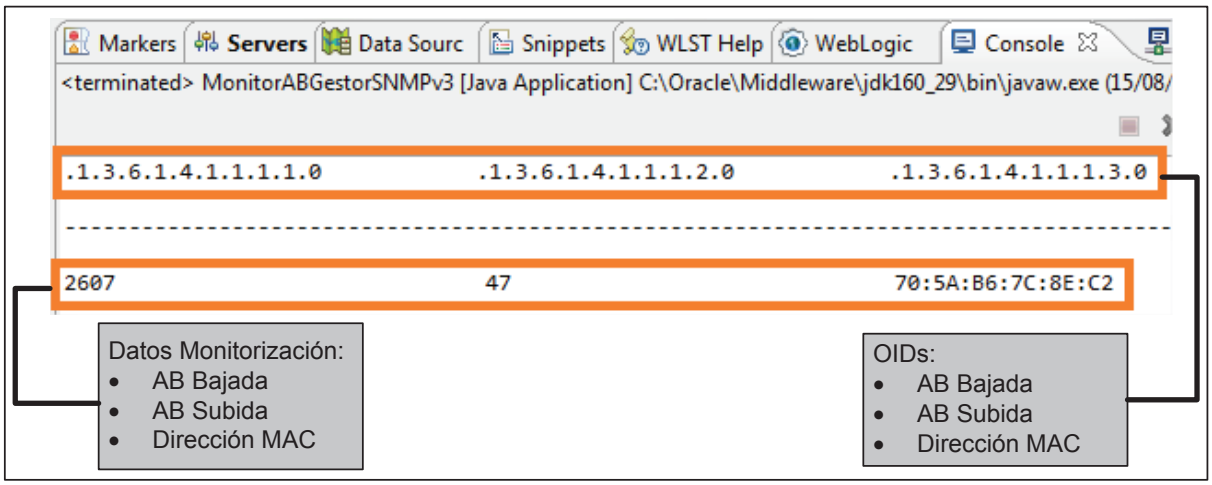


Figura 4.2. Prueba de funcionamiento de los módulos Agente y Gestor SNMP versión 3.

La Figura 4.2 muestra que efectivamente las consultas SNMP realizadas a las MiBs del nodo MIB *monitorAB* retornan los datos de monitorización deseados por la aplicación.

Con el propósito de analizar los resultados de las consultas SNMP versión 3, se recurre al uso de la herramienta computacional RawCap, la misma que permite la captura de paquetes enviados y recibidos en la máquina local por medio de la interfaz de red loopback. Para la visualización de la captura hecha por el programa RawCap se utiliza la herramienta Wireshark, Figura 4.3.

No.	Time	Source	Destination	Protocol	Length	Info
63	10.431597	127.0.0.1	127.0.0.1	SNMP	92	get-request
64	10.435597	127.0.0.1	127.0.0.1	SNMP	141	report 1.3.6.1.6.3.15.1.1.4.0
65	10.493601	127.0.0.1	127.0.0.1	SNMP	137	get-request
66	10.494601	127.0.0.1	127.0.0.1	SNMP	154	report 1.3.6.1.6.3.15.1.1.2.0
67	10.718613	127.0.0.1	127.0.0.1	SNMP	197	encryptedPDU: privKey Unknown
95	15.064862	127.0.0.1	127.0.0.1	SNMP	216	encryptedPDU: privKey Unknown
1102	59.027377	127.0.0.1	127.0.0.1	SNMP	92	get-request
1103	59.028377	127.0.0.1	127.0.0.1	SNMP	141	report 1.3.6.1.6.3.15.1.1.4.0
1120	59.084380	127.0.0.1	127.0.0.1	SNMP	137	get-request
1121	59.085380	127.0.0.1	127.0.0.1	SNMP	154	report 1.3.6.1.6.3.15.1.1.2.0
1134	59.326394	127.0.0.1	127.0.0.1	SNMP	197	encryptedPDU: privKey Unknown
1184	63.421628	127.0.0.1	127.0.0.1	SNMP	217	encryptedPDU: privKey Unknown

Figura 4.3. Paquetes SNMP versión 3 de la aplicación.

Los paquetes SNMP presentados en la Figura 4.3, corresponden a una consulta SNMP realizada desde el módulo Gestor SNMP al módulo Agente SNMP donde se puede observar que los paquetes SNMP conteniendo datos de monitorización se encuentra encriptados tal como se puede corroborar junto con la Figura 4.4 y Figura 4.5

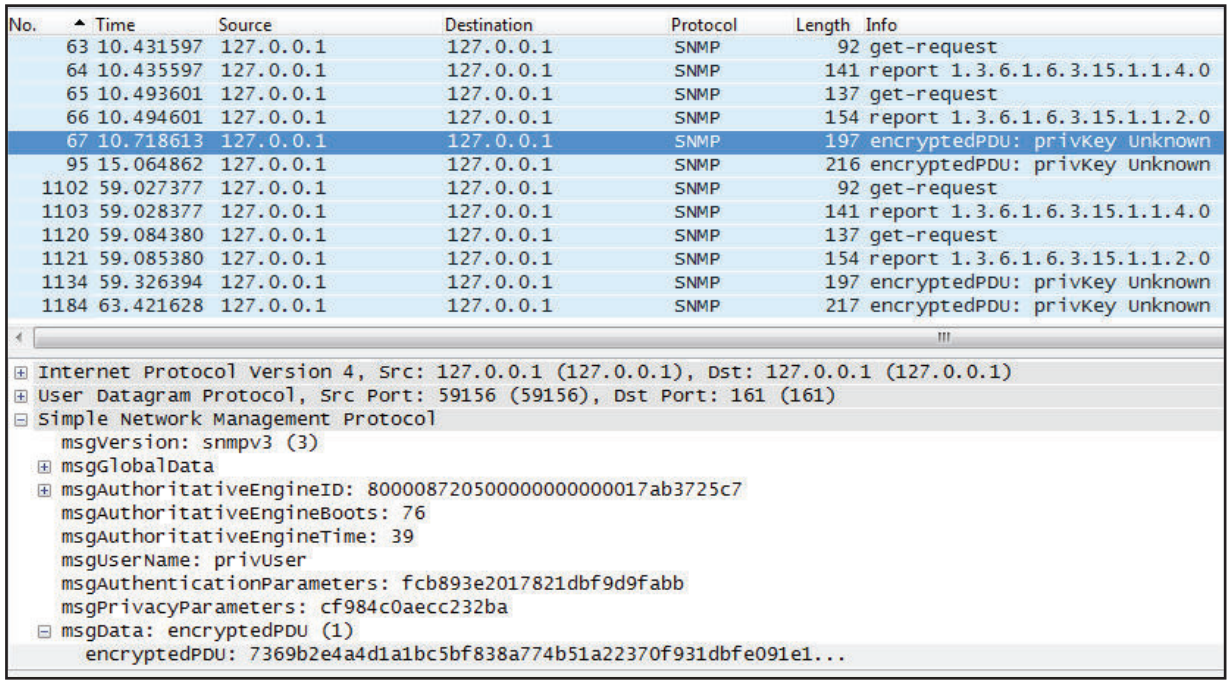


Figura 4.4. Paquete SNMP versión 3 de consulta enviado desde el gestor al agente SNMP.

La Figura 4.4 muestra una consulta SNMP versión 3 realizada por la aplicación, donde es posible observar que efectivamente las consultas son realizadas al puerto UDP 161 del dispositivo local y que éstas contienen información de seguridad para la autenticación segura de usuarios, y encriptación de mensajes SNMP.

La Figura 4.5 a su vez muestra la respuesta de la consulta SNMP realizada por la aplicación y en la que se puede observar que el agente SNMP responde desde el puerto UDP 161 mediante un paquete SNMP protegido con métodos de autenticación y encriptación.

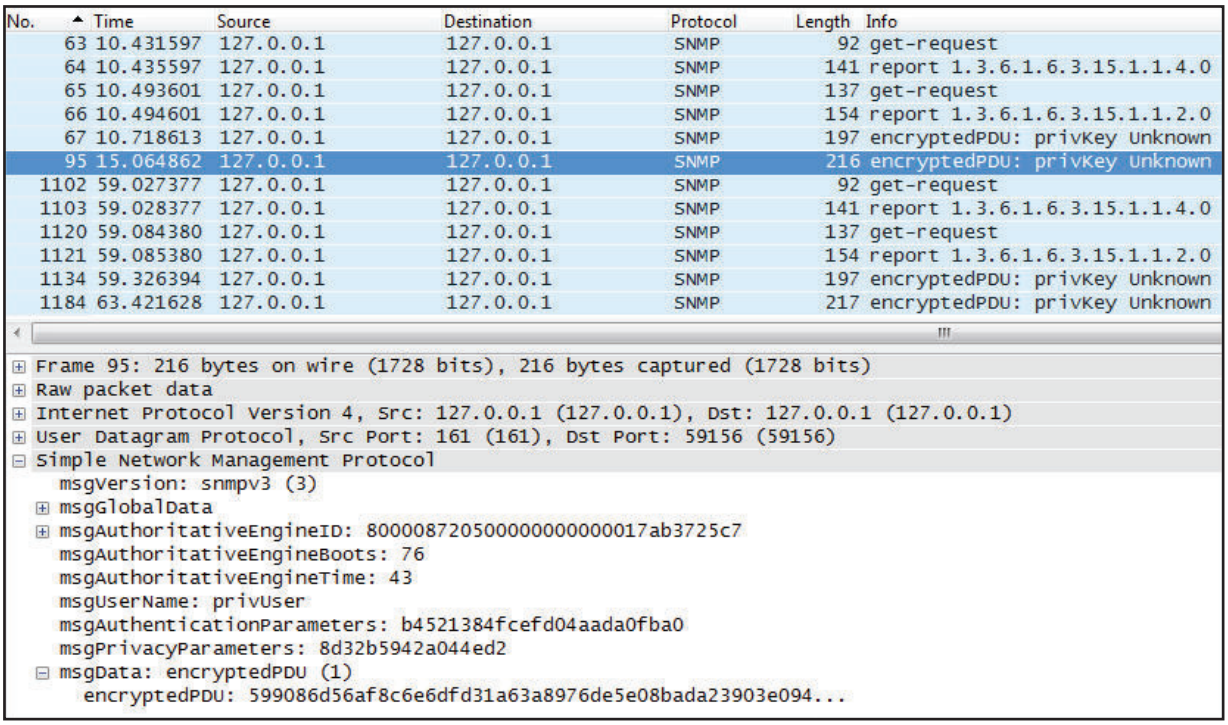


Figura 4.5. Paquete SNMP versión 3 de respuesta enviado desde el agente al gestor SNMP.

Los datos de monitorización obtenidos hasta éste momento a través del uso del protocolo SNMP versión 3, cumplen con los requerimientos funcionales y de seguridad establecidos para la aplicación en el capítulo de análisis.

4.4 PRUEBA DE FUNCIONAMIENTO DEL MÓDULO CLIENTE DEL SERVICIO WEB PARA EL ENVÍO DE MEDICIONES

El módulo Cliente del Servicio Web para el envío de Mediciones será probado y analizado con la ayuda del analizador de protocolos y paquetes Wireshark, y del IDE Eclipse para la visualización de los datos de monitorización obtenidos y enviado por éste módulo de la aplicación.

Debido a que éste módulo no presenta alguna interfaz gráfica de usuario para mostrar la información procesada aquí, se recurre al uso del IDE Eclipse para añadir una sección *main* a la clase *MonitorABClienteWSAplicacion* para que imprima en

pantalla de consola la información que éste módulo envía al Servidor de Servicios Web.

Éste módulo envía el siguiente tipo de información a su contraparte utilizando como medio de transporte el Internet.

- Ancho de banda de bajada.
- Ancho de banda de Subida.
- Dirección MAC.
- Fecha de captura.

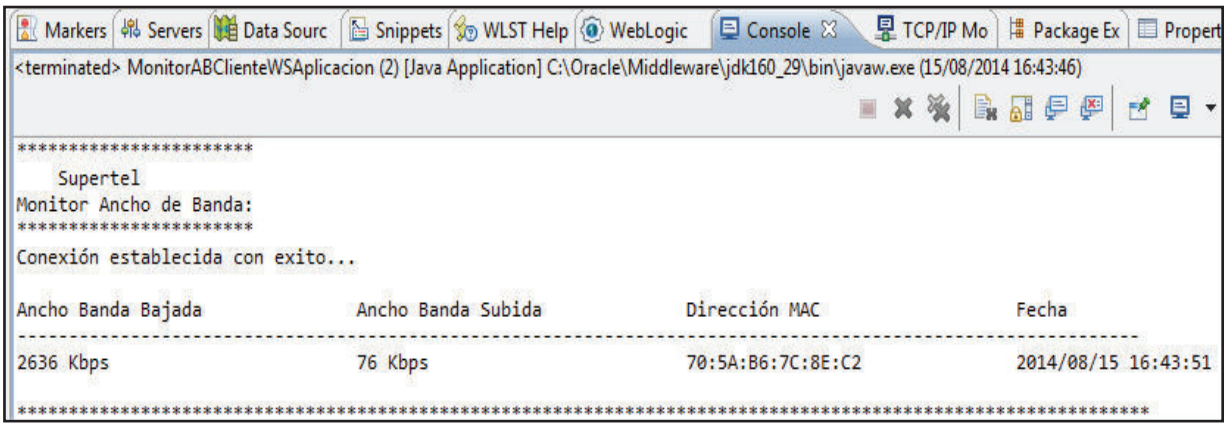
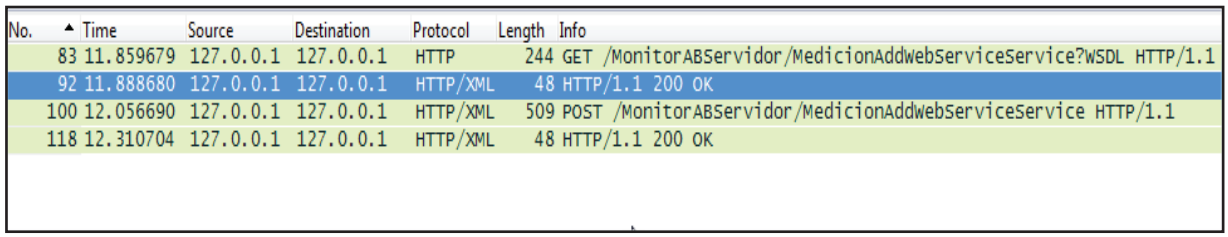


Figura 4.6. Prueba de funcionamiento del módulo Cliente del Servicio Web para el envío de Mediciones.

En la Figura 4.6 se observa que éste módulo efectivamente establece una conexión con el servidor de servicios web para el envío de datos de monitorización, los mismos que corresponden a los requeridos por la aplicación de monitoreo de usuarios del servicio de Internet. Se aprecia también que el formato de la fecha es el requerido por la aplicación.

Para el análisis de resultados del intercambio de mensajes del cliente de servicios web con su servidor, se utiliza nuevamente el programa RawCap para la captura de los mismos. En la Figura 4.7 se puede observar los resultados de la captura, en donde efectivamente se distinguen los paquetes HTTP relacionados con la solicitud

de consumo del servicio web *MedicionAddWebService* por medio del archivo WSDL indicado para éste servicio web.



No.	Time	Source	Destination	Protocol	Length	Info
83	11.859679	127.0.0.1	127.0.0.1	HTTP	244	GET /MonitorABServidor/MedicionAddWebServiceService?WSDL HTTP/1.1
92	11.888680	127.0.0.1	127.0.0.1	HTTP/XML	48	HTTP/1.1 200 OK
100	12.056690	127.0.0.1	127.0.0.1	HTTP/XML	509	POST /MonitorABServidor/MedicionAddWebServiceService HTTP/1.1
118	12.310704	127.0.0.1	127.0.0.1	HTTP/XML	48	HTTP/1.1 200 OK

Figura 4.7. Paquetes HTTP usados por el Cliente del Servicio Web para el envío de Mediciones.

La Figura 4.8 muestra en detalle el contenido del paquete HTTP que envía los datos de monitorización, comprobándose que efectivamente son enviados al servidor de servicios web trabajando en el puerto TCP 7001. De igual manera, se distingue que los paquetes contienen mensajes SOAP en lenguaje XML, en los mismos que se encuentran definidos los valores de monitorización capturados por la aplicación en los usuarios del servicio de Internet.

La seguridad establecida por el servicio web de la aplicación, para la autenticación sin encriptación de los usuarios monitoreados, se puede constatar en la Figura 4.9, en donde además se aprecian las credenciales de autenticación.

Hasta éste punto son cumplidos los requerimientos de la aplicación de escritorio ubicada en los usuarios del servicio de Internet monitoreados, para la captura y envío de información de monitorización necesaria para el control de los proveedores del servicio de Internet.

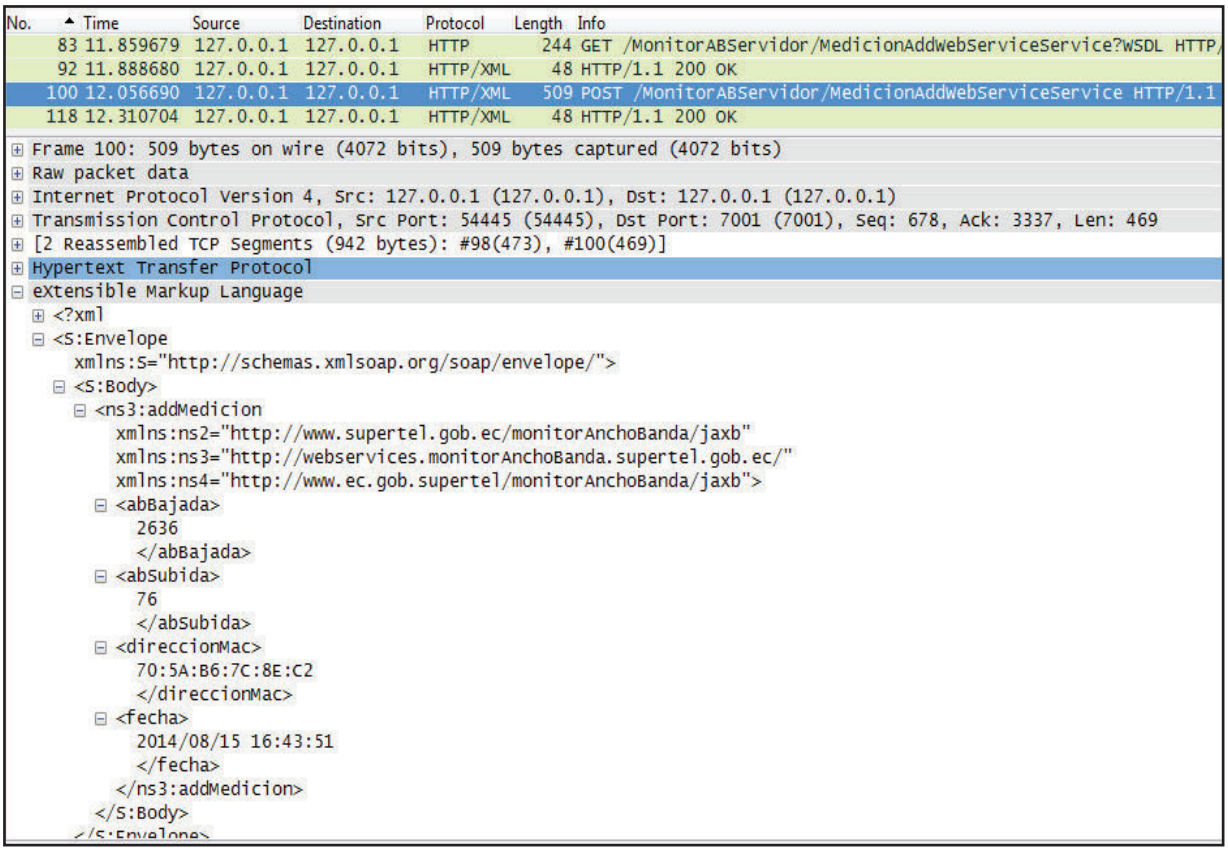


Figura 4.8. Paquete HTTP con datos de monitorización.

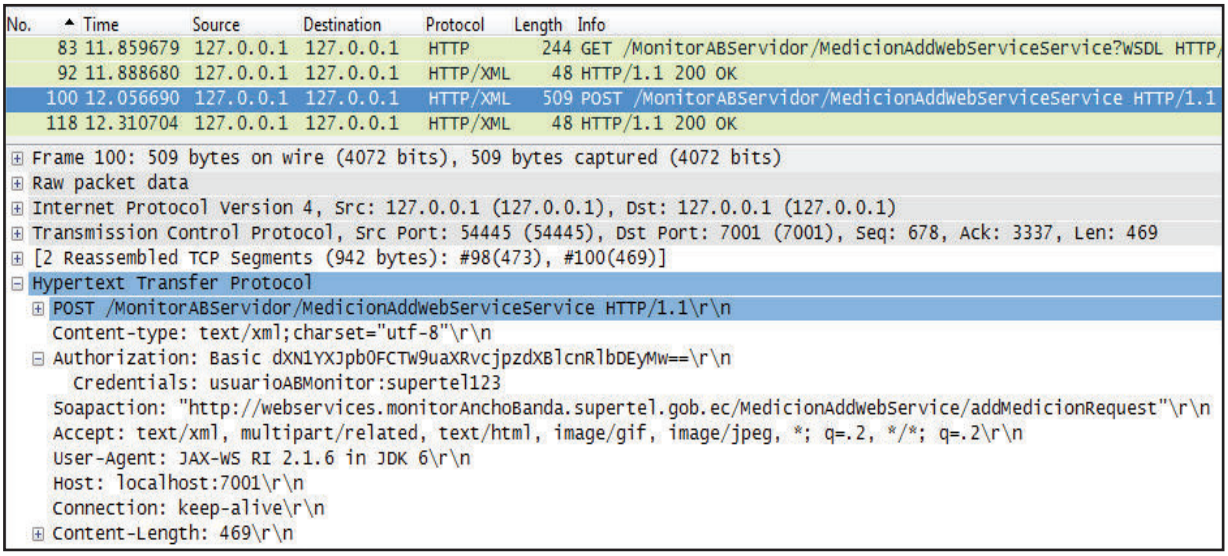


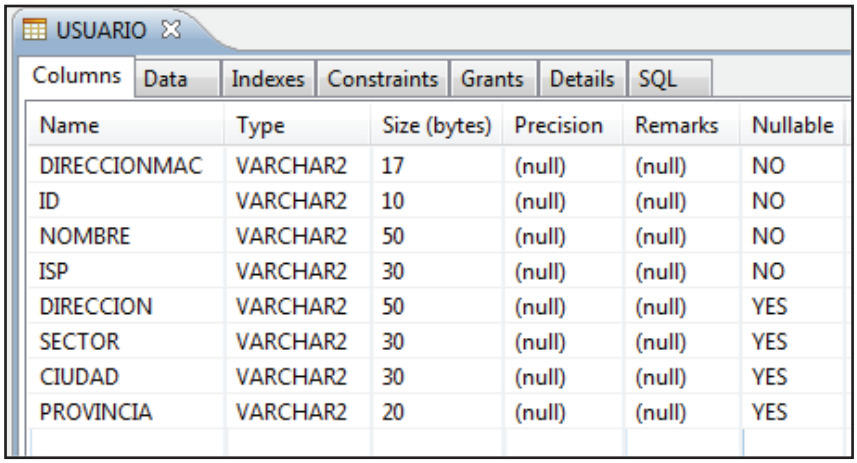
Figura 4.9. Autenticación de Clientes del Servicio Web para el envío de Mediciones.

4.5 PRUEBA DE FUNCIONAMIENTO DEL MÓDULO BASE DE DATOS

La prueba de funcionamiento de la base de datos de la aplicación, se realizará con la ayuda del IDE Eclipse, el mismo que permite visualizar las tablas contenidas en la base de datos y realizar consultas SQL a éstas.

En la Figura 4.10 y Figura 4.11, se observan las características de las tablas Usuario y Medición, constatándose que efectivamente sus campos son los establecidos en el capítulo de diseño e implementación de la presente aplicación.

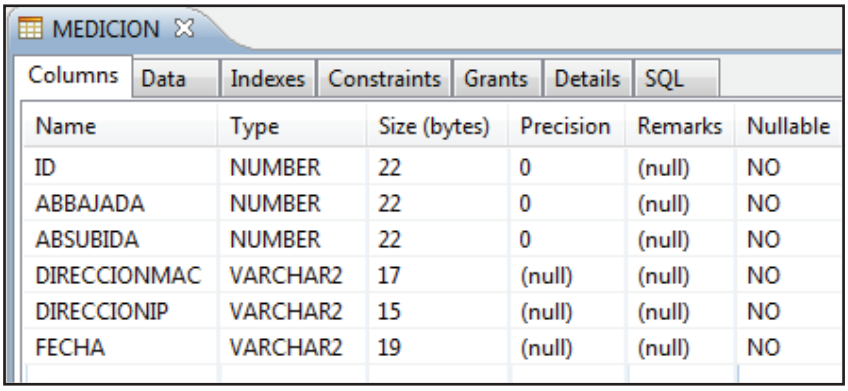
La Figura 4.12 y Figura 4.13 se demuestra el correcto funcionamiento de la base de datos, por medio de consultas SQL desde el IDE Eclipse.


USUARIO

Columns | Data | Indexes | Constraints | Grants | Details | SQL

Name	Type	Size (bytes)	Precision	Remarks	Nullable
DIRECCIONMAC	VARCHAR2	17	(null)	(null)	NO
ID	VARCHAR2	10	(null)	(null)	NO
NOMBRE	VARCHAR2	50	(null)	(null)	NO
ISP	VARCHAR2	30	(null)	(null)	NO
DIRECCION	VARCHAR2	50	(null)	(null)	YES
SECTOR	VARCHAR2	30	(null)	(null)	YES
CIUDAD	VARCHAR2	30	(null)	(null)	YES
PROVINCIA	VARCHAR2	20	(null)	(null)	YES

Figura 4.10. Tabla Usuario de la base de datos de la aplicación.


MEDICION

Columns | Data | Indexes | Constraints | Grants | Details | SQL

Name	Type	Size (bytes)	Precision	Remarks	Nullable
ID	NUMBER	22	0	(null)	NO
ABBAJADA	NUMBER	22	0	(null)	NO
ABSUBIDA	NUMBER	22	0	(null)	NO
DIRECCIONMAC	VARCHAR2	17	(null)	(null)	NO
DIRECCIONIP	VARCHAR2	15	(null)	(null)	NO
FECHA	VARCHAR2	19	(null)	(null)	NO

Figura 4.11. Tabla Medición de la base de datos de la aplicación.

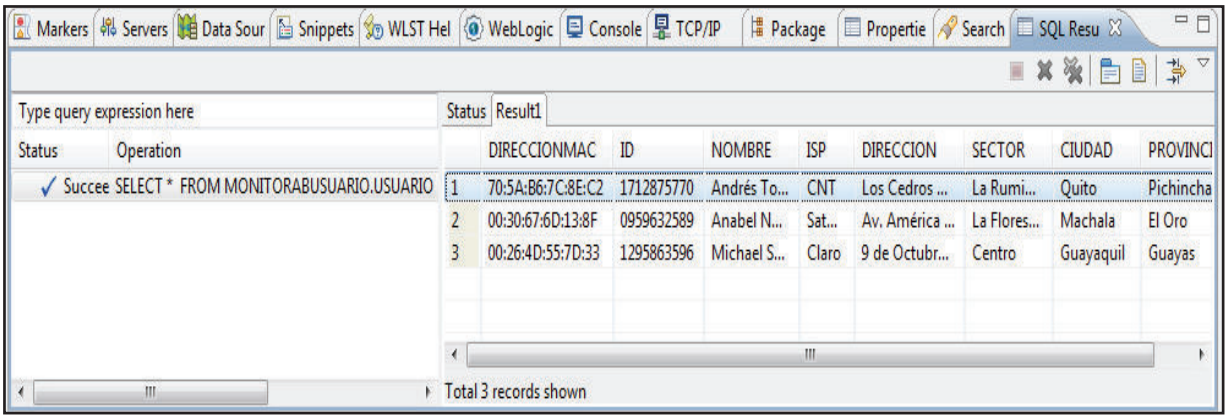


Figura 4.12. Prueba de funcionamiento de la Tabla Usuario de la base de datos de la aplicación.

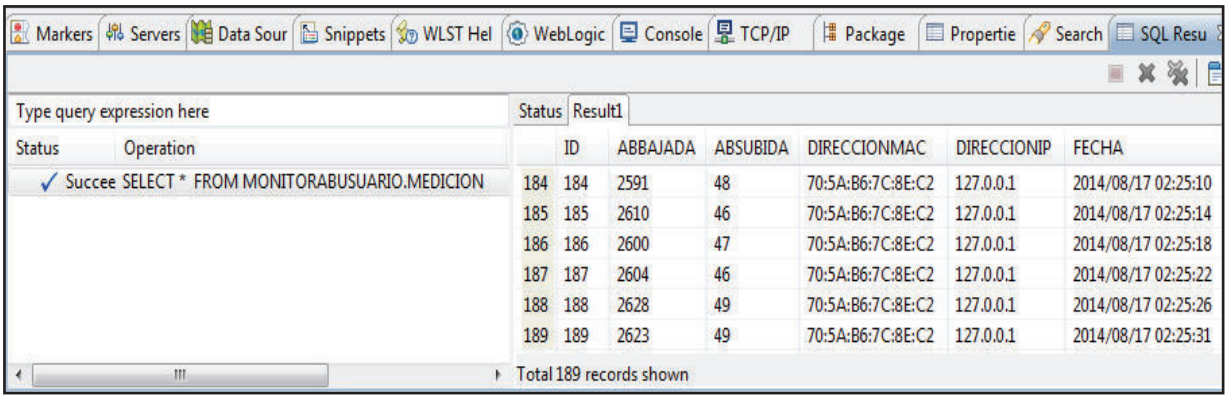


Figura 4.13. Prueba de funcionamiento de la Tabla Medición de la base de datos de la aplicación.

4.6 PRUEBA DE FUNCIONAMIENTO DEL MÓDULO DE PERSISTENCIA Y DEL MÓDULO SERVIDOR DE SERVICIOS WEB

La prueba de funcionamiento de éstos dos módulos se realiza en conjunto, ya que el módulo de persistencia no cuenta con una interfaz gráfica de usuario por medio de la cual se pueda demostrar el proceso de conversión entre objetos Java y objetos relacionales de la base de datos, realizado por éste modulo. De todos modos, el funcionamiento del módulo de persistencia puede ser probado a través de la prueba de funcionamiento del módulo servidor de servicios web, ya que éste último requiere que el sistema de persistencia funcione correctamente para que los objetos

relacionales almacenados en las tablas de la base de datos puedan ser presentados y consumidos a través de los servicios web publicados por la presente aplicación, y en los cuales se manejan primordialmente objetos Java.

Con el propósito de comprobar el funcionamiento de éstos dos módulos, se recurre a la ayuda del servidor corporativo JEE Weblogic 12c, el mismo que dispone de una herramienta para la prueba de funcionamiento de los servicios web desplegados sobre su plataforma.

Los servicios web de la aplicación que son probados y analizados son los siguientes:

- Servicio web para la recepción de mediciones.
- Servicio web para la consulta de mediciones.
- Servicio web para la gestión y consulta de usuarios.

4.6.1 PRUEBA DE FUNCIONAMIENTO DEL SERVICIO WEB PARA LA RECEPCIÓN DE MEDICIONES

El servicio web para la recepción de mediciones tiene la labor de ingresar nuevas mediciones en la tabla Medición de la base de datos, para probar si éste proceso se lleva a cabo correctamente se recurre al probador de servicios web de Weblogic 12c.

En la Figura 4.14 se visualiza como el servicio web es correctamente publicado en el servidor de servicios web, y que los campos de ancho de banda de bajada, ancho de banda de subida, dirección MAC y fecha, con los que debe contar las mediciones recibidas y procesadas por éste servicio web, corresponden a las definidas en el análisis de requerimientos de la nueva aplicación.

El resultado de la recepción e ingreso exitoso de la nueva medición en la base de datos a través del servicio web actual y del sistema de persistencia de la aplicación, es indicado en la Figura 4.15.

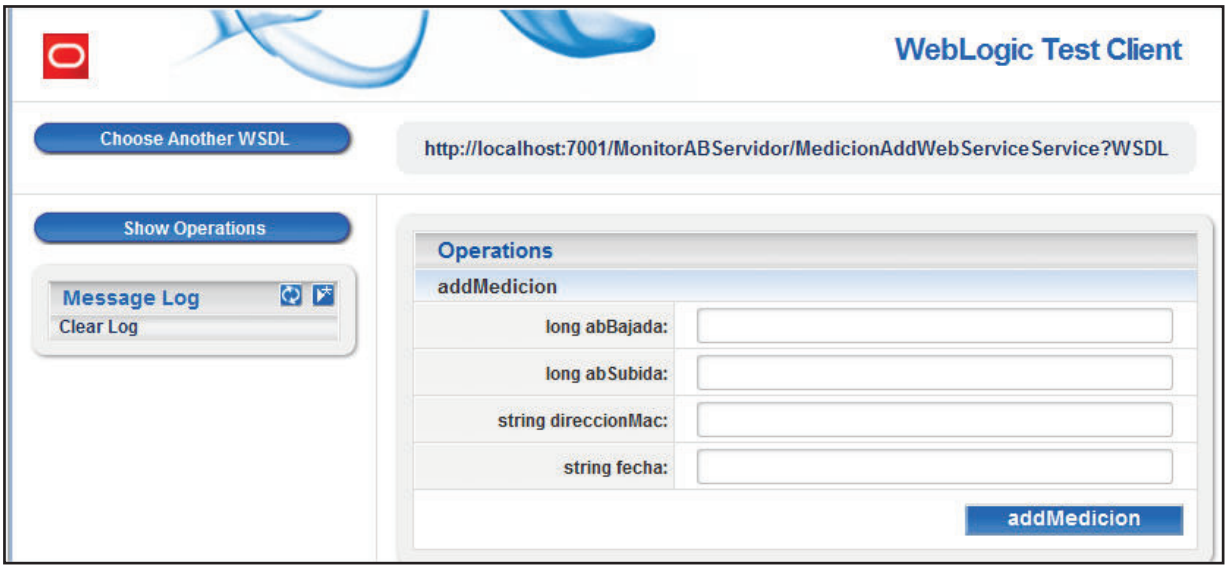


Figura 4.14. Prueba de funcionamiento de la publicación del servicio web para la recepción de mediciones.

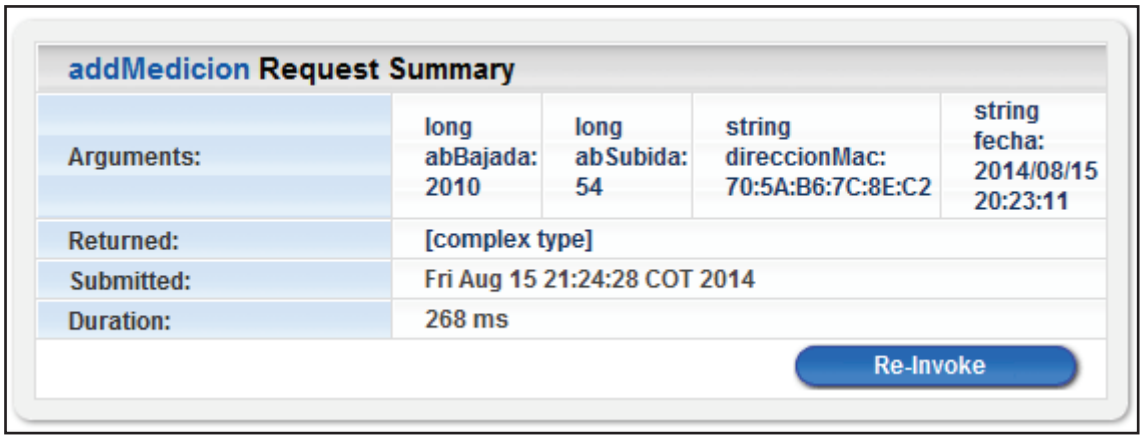


Figura 4.15. Prueba de funcionamiento del consumo del servicio web para la recepción de mediciones.

4.6.2 PRUEBA DE FUNCIONAMIENTO DEL SERVICIO WEB PARA LA CONSULTA DE MEDICIONES

El servicio web para la consulta de mediciones comprende varios tipos de consultas, tal como se diseñaron e implementaron en el capítulo 3, para las cuales se realiza las pruebas de funcionamiento de acuerdo a la siguiente división:

- Prueba de consulta de las mediciones registradas.

- Prueba de consulta de mediciones por usuario.
- Prueba de consulta de mediciones por usuario y fecha.

Cabe mencionar que no se prueba en éste módulo la consulta del índice de disponibilidad del servicio de Internet, ya que ésta es calculada directamente por las páginas web JSP del módulo Cliente Web de Consultas, por lo que su comprobación será efectuada cuando se traten las pruebas referentes a ese módulo.

La publicación del servicio web para la consulta de mediciones sobre el servidor de servicios web, se encuentra ilustrada en la Figura 4.16, donde se puede apreciar que todos los tipos de consultas relacionados con éste servicio web están correctamente definidos y a la espera de ser consumidas.

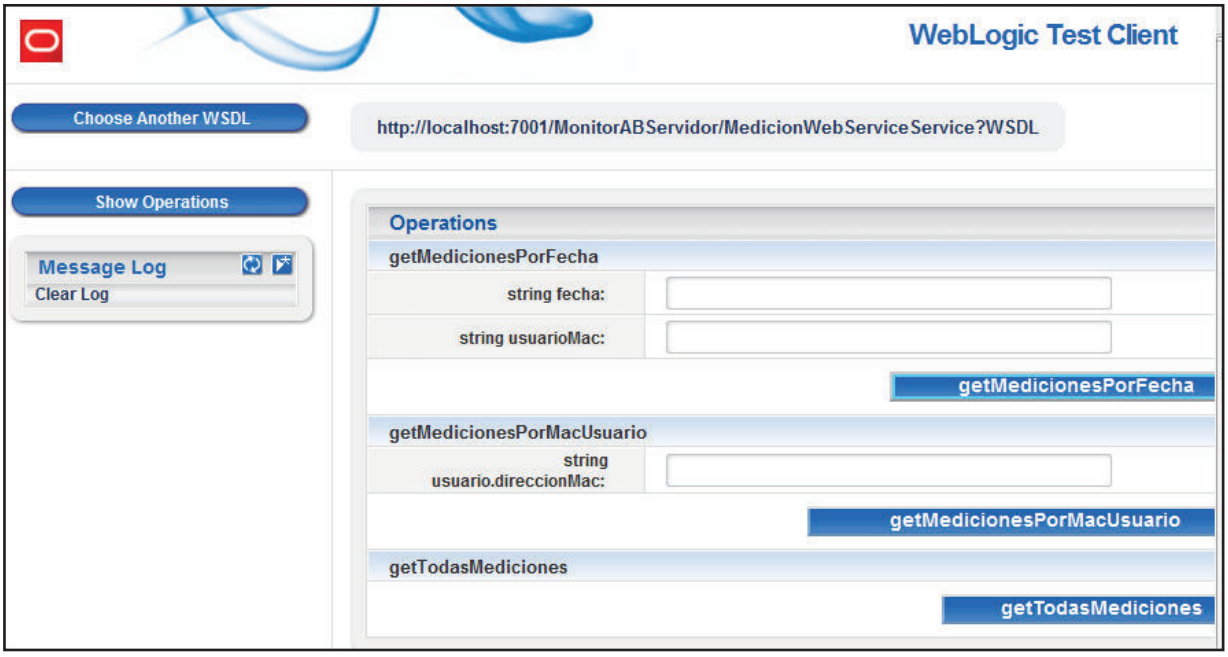


Figura 4.16. Prueba de funcionamiento de la publicación del servicio web para la consulta de mediciones.

4.6.2.1 Prueba de Consulta de Mediciones Registradas

La prueba de funcionamiento de la consulta de todas las mediciones registradas por la aplicación hasta ese momento, se realiza a través del cliente de servicios web de prueba de Weblogic 12c, del cual se aprecia el resultado en la Figura 4.17, y en la cual se comprueba que efectivamente el servicio web es capaz de acceder a los registros de la tabla Medición por medio del sistema de persistencia de la aplicación.

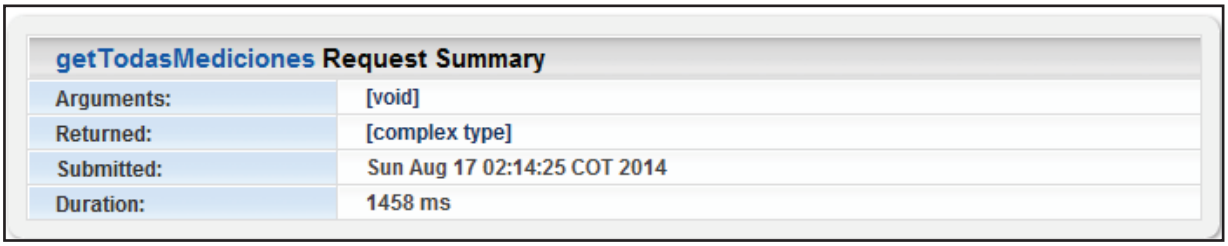


Figura 4.17. Prueba de funcionamiento del consumo del servicio web para la consulta de mediciones registradas.

4.6.2.2 Prueba de Consulta de Mediciones por Usuario

Ésta prueba de funcionamiento se realiza de la misma manera, con la ayuda del cliente de servicios web de prueba, y del cual se obtiene el resultado indicado en la Figura 4.18, y en base al cual, se determina que el servicio web accede de forma correcta a la base de datos para realizar la consulta de mediciones por medio del ingreso de la dirección MAC del usuario.

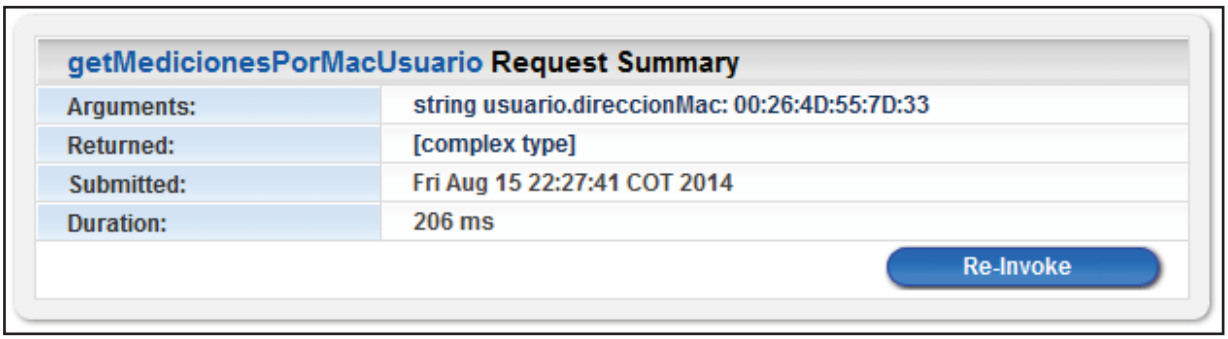


Figura 4.18. Prueba de funcionamiento del consumo del servicio web para la consulta de mediciones por usuario.

4.6.2.3 Prueba de Consulta de Mediciones por Usuario y Fecha

La prueba de la operación correcta de las consultas efectuadas a la tabla Medición de la base de datos en base a la dirección MAC del usuario y la fecha de captura, se realiza con la ayuda del cliente de servicios web de prueba, y cuyo resultado se indica en la Figura 4.19.

El resultado asegura que el servicio web para la consulta de mediciones por usuario y fecha, y el sistema de persistencia, efectivamente procesan la consulta en base a los argumentos de entrada requeridos por la aplicación.

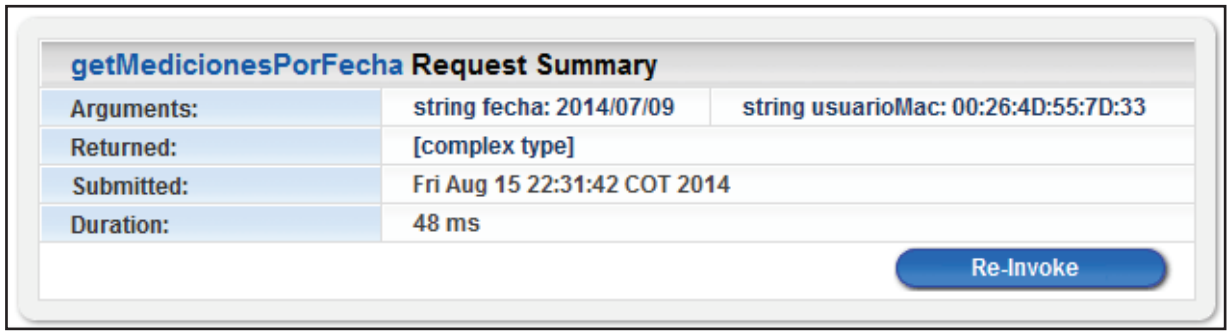


Figura 4.19. Prueba de funcionamiento del consumo del servicio web para la consulta de mediciones por usuario y fecha.

4.6.3 PRUEBA DE FUNCIONAMIENTO DEL SERVICIO WEB PARA LA GESTIÓN Y CONSULTA DE USUARIOS

La prueba de funcionamiento de éste servicio web se realiza en base a los tipos de gestión y consulta hechas a la tabla Usuario de la base de datos, que fueron definidas en el capítulo de diseño e implementación. Por éste motivo, se tendrán los siguientes tipos de pruebas para éste servicio web:

- Prueba de consulta de usuarios registrados.
- Ingreso de nuevo usuario.
- Prueba de búsqueda de usuario.
- Prueba de modificación de usuario.
- Prueba de eliminación de usuario.

El correcto funcionamiento de la publicación del servicio web para la gestión y consulta de usuarios está ilustrado en la Figura 4.20, donde también se puede apreciar, que todos los tipos de consultas y procedimientos establecidos en el diseño e implementación para el manejo de los registros de la tabla Usuario, se encuentran presentes y a la espera de ser solicitados.

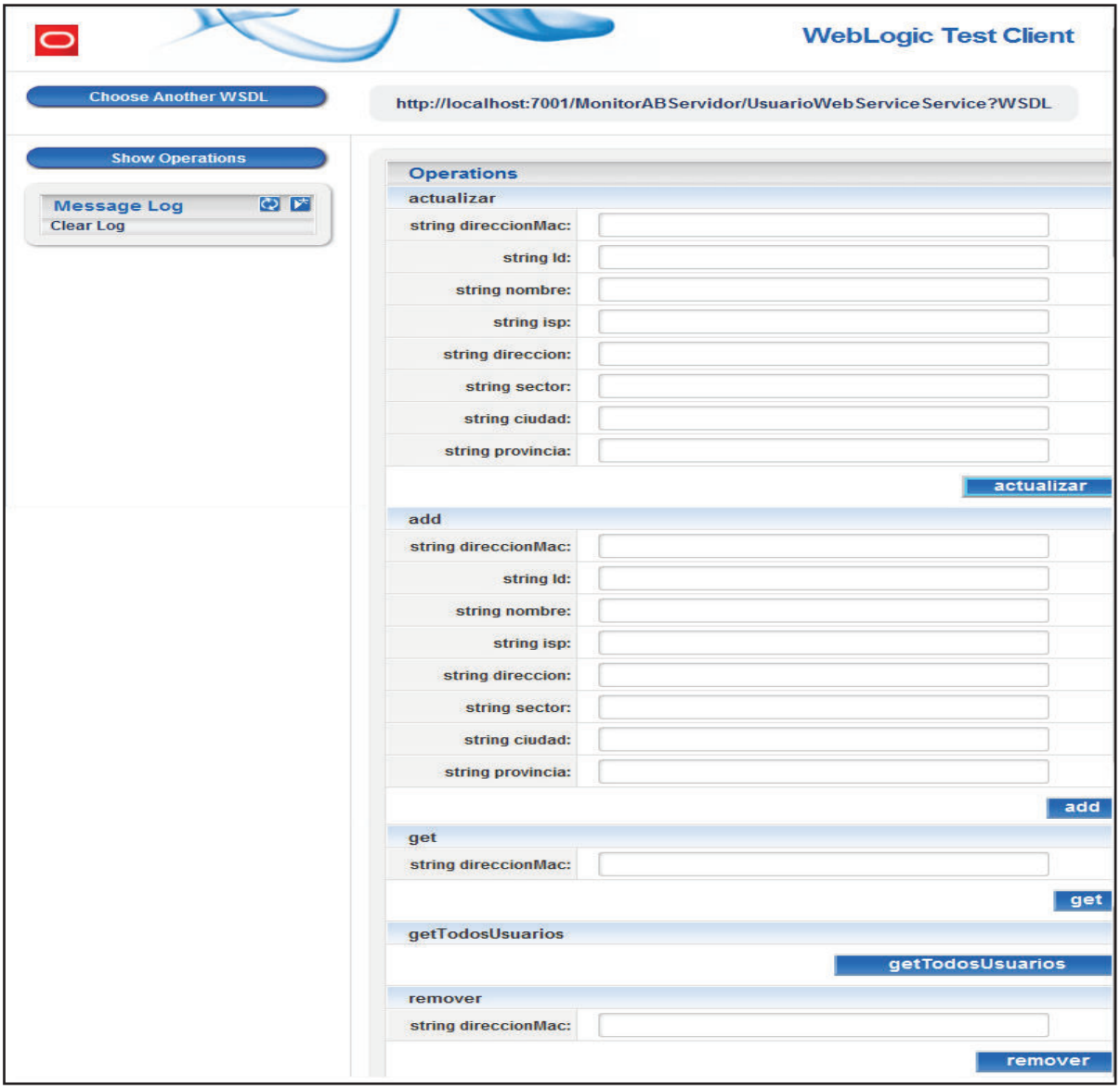


Figura 4.20. Prueba de funcionamiento de la publicación del servicio web para la gestión y consulta de usuarios.

4.6.3.1 Prueba de Consulta de Usuarios Registrados

El resultado de la prueba de la consulta de usuarios registrados se observa en la Figura 4.21, la misma que muestra que la consulta fue efectivamente procesada a través del servicio web para la consulta y gestión de usuarios, y el sistema de persistencia de la aplicación.

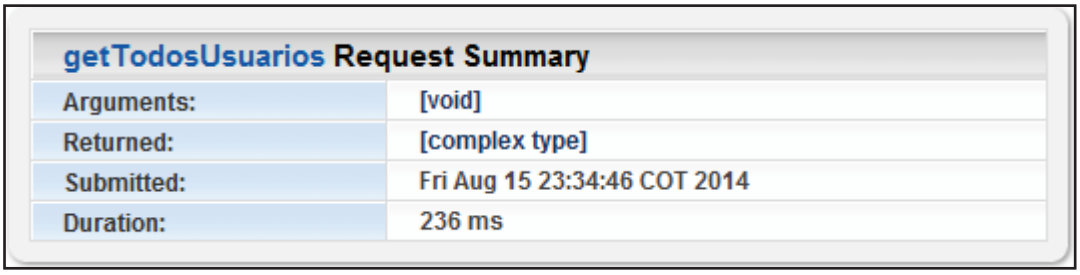


Figura 4.21. Prueba de funcionamiento del consumo del servicio web para la consulta de usuarios registrados.

4.6.3.2 Prueba de Ingreso de Nuevo Usuario

La Figura 4.22 ilustra el resultado de la prueba del ingreso de un nuevo usuario al sistema por medio del servicio web para la gestión y consulta de usuarios, y el sistema de persistencia de la aplicación. Además, se puede observar cómo se realiza el ingreso de un nuevo usuario de forma exitosa por medio de los argumentos de entrada requeridos por la aplicación.

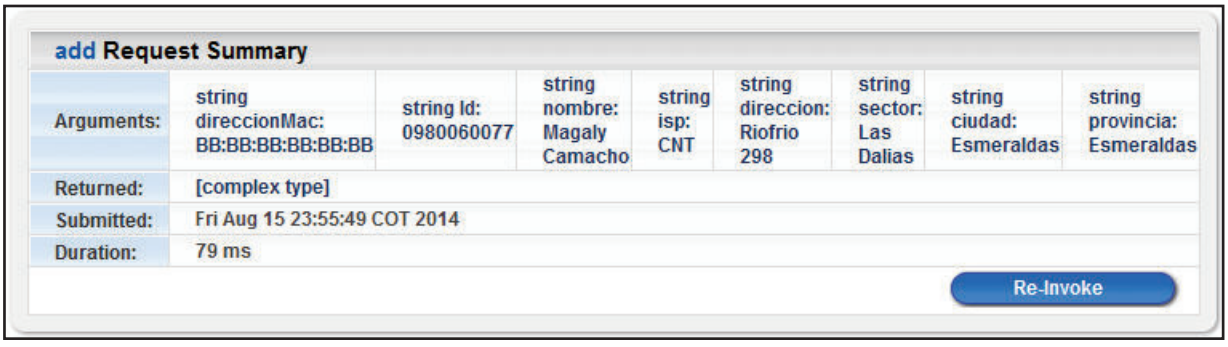


Figura 4.22. Prueba de funcionamiento del consumo del servicio web para el ingreso de nuevo usuario.

4.6.3.3 Prueba de Búsqueda de Usuario

La prueba de búsqueda de usuario se realiza a través del cliente de servicio web de prueba, con la ayuda del cual se obtienen los resultados presentados en la Figura 4.23. Los resultados muestran que la búsqueda de usuario es efectivamente procesada por el servicio web actual y el sistema de persistencia de la aplicación, y los argumentos de búsqueda corresponden a los requeridos y establecidos por el diseño e implementación de la presente aplicación.

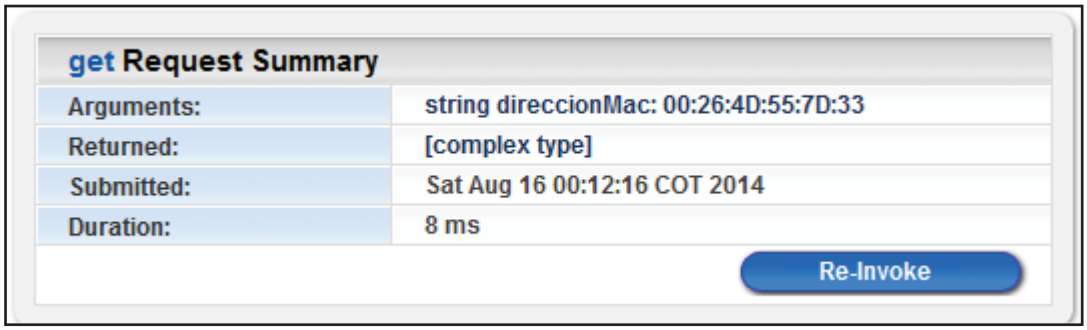


Figura 4.23. Prueba de funcionamiento del consumo del servicio web para la búsqueda de usuario.

4.6.3.4 Prueba de Modificación de Usuario

El resultado de la prueba de modificación de usuario por medio del uso del cliente de servicio web de prueba se encuentra presentado en la Figura 4.24. En éste resultado se observa que por medio del sistema de persistencia, el servicio web para la actualización de los datos de usuario altera correctamente la información contenida en la tabla Usuario de la base de datos de la aplicación.

El resultado demuestra que el único argumento que no es capaz de ser modificado es la dirección MAC del usuario, tal como se estableció con anterioridad en el capítulo de diseño e implementación, ya que por definición los campos correspondientes a la llave primaria de una tabla en la base de datos, no pueden ser modificados para que éste mantenga su integridad.

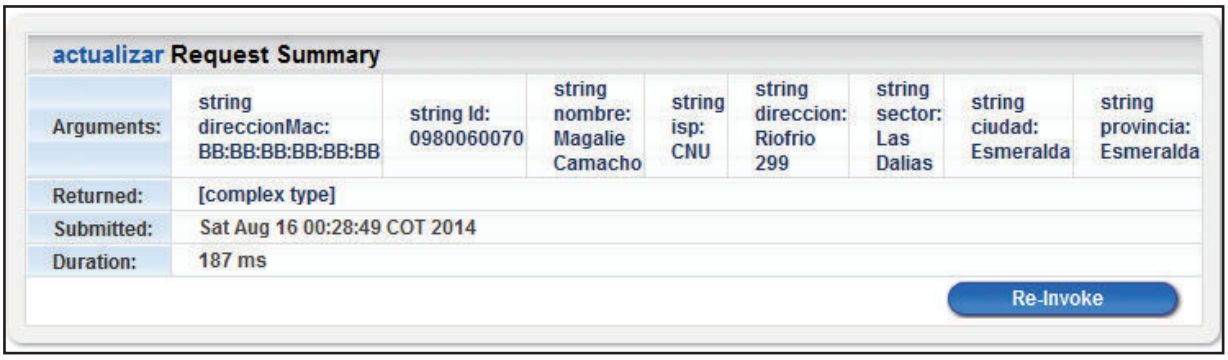


Figura 4.24. Prueba de funcionamiento del consumo del servicio web para la modificación de usuario.

4.6.3.5 Prueba de Eliminación de Usuario

La prueba de funcionamiento del servicio web relacionado con el proceso de eliminación de usuarios de la base de datos de la aplicación a través del sistema de persistencia, se comprueba mediante el uso del cliente de servicio web de prueba de Weblogic 12c, y cuyo resultado es ilustrado en la Figura 4.25. Éste resultado ratifica que los parámetros necesarios para la remoción de un usuario efectivamente corresponden a los definidos en el capítulo de diseño e implementación de la nueva aplicación.

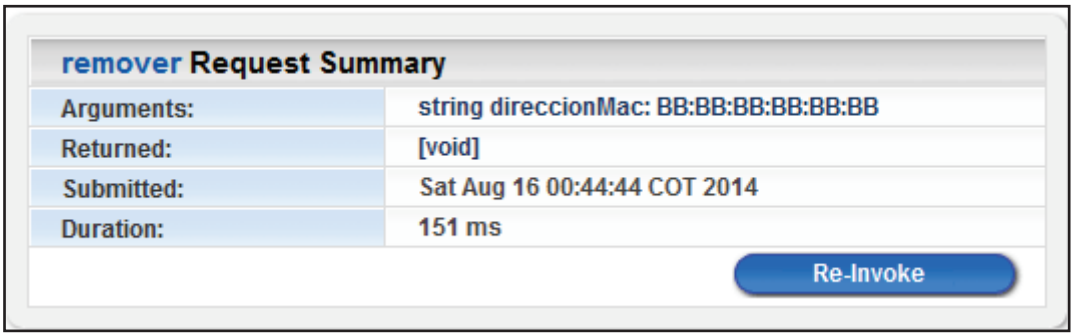


Figura 4.25. Prueba de funcionamiento del consumo del servicio web para la eliminación de usuario.

4.7 PRUEBA DE FUNCIONAMIENTO DEL MÓDULO CLIENTE DEL SERVICIO WEB DE CONSULTAS

Éste módulo es el único de la aplicación que cuenta con una interfaz gráfica de usuario, por medio de la cual serán visualizados los resultados de las pruebas de funcionamiento realizadas a los clientes de servicio web asociados a éste módulo.

Las herramientas utilizadas para la pruebas de funcionamiento de éste módulo serán el navegador web Mozilla Firefox 31.0 y los analizadores de protocolos Wireshark y Rawcap, donde éste último permitirá la captura de paquetes transmitidos por medio de la interfaz de red de loopback.

Las pruebas de funcionamiento realizadas en éste módulo son las siguientes:

- Prueba del cliente del servicio web para la consulta de mediciones.
- Prueba del cliente del servicio web para la gestión y consulta de usuarios.

4.7.1 PRUEBA DE FUNCIONAMIENTO DEL CLIENTE DEL SERVICIO WEB PARA LA CONSULTA DE MEDICIONES

Las pruebas efectuadas al cliente del servicio web para la consulta de mediciones están relacionadas con la visualización de la información contenida en la tabla Medición de la base de datos de la aplicación, para la cual se realizan las siguientes pruebas de consulta:

- Prueba de consulta de mediciones registradas.
- Prueba de consulta de mediciones por usuario.
- Prueba de consulta de mediciones por usuario y fecha.
- Prueba de consulta del índice de disponibilidad del servicio de Internet.

4.7.1.1 Prueba de Consulta de Mediciones Registradas

Ésta prueba arroja como resultado lo mostrado en la Figura 4.26, en donde se puede apreciar que efectivamente la aplicación retorna la lista completa de los registros almacenados en la tabla Medición de la base de datos de la aplicación.

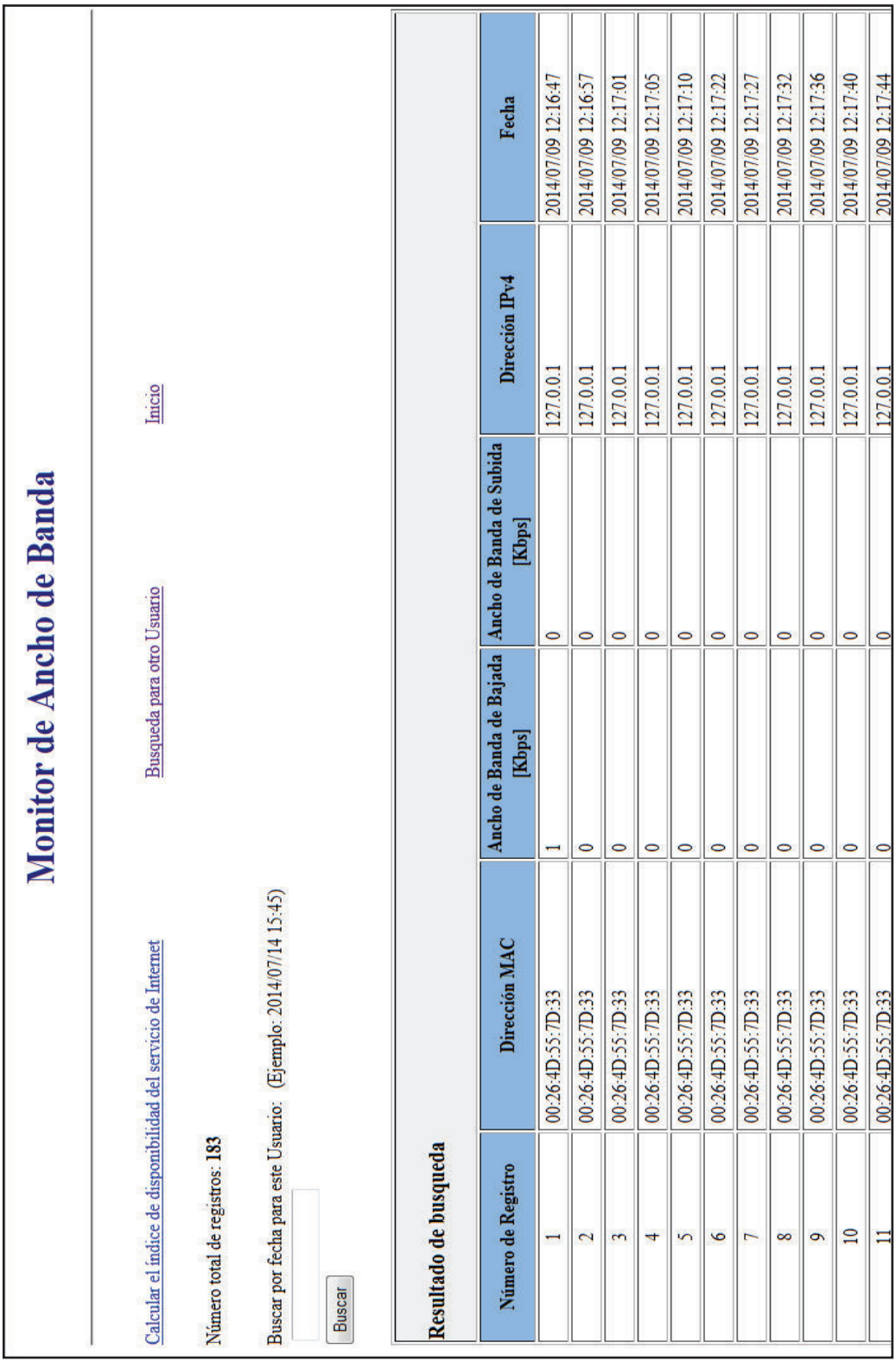
Figura 4.26. Prueba de funcionamiento del cliente del servicio web para la consulta de mediciones registradas.

4.7.1.2 Prueba de Consulta de Mediciones por Usuario

En la prueba de éste tipo de consultas intervienen dos páginas web JSP, para las cuales el ingreso correcto de la dirección MAC de usuario retorna la lista de mediciones perteneciente a éste, Figura 4.27 y Figura 4.28.

Figura 4.27. Formulario de ingreso de la dirección MAC de usuario para la consulta de mediciones por usuario.

Para el caso de que se introduzca como argumento de búsqueda de mediciones por usuario una dirección MAC no válida, la aplicación devolverá un mensaje de error, como se muestra en la Figura 4.29



Monitor de Ancho de Banda

Calcular el índice de disponibilidad del servicio de Internet Busqueda para otro Usuario Inicio

Número total de registros: **183**

Buscar por fecha para este Usuario: (Ejemplo: 2014/07/14 15:45)

Buscar

Resultado de busqueda

Número de Registro	Dirección MAC	Ancho de Banda de Bajada [Kbps]	Ancho de Banda de Subida [Kbps]	Dirección IPv4	Fecha
1	00:26:4D:55:7D:33	1	0	127.0.0.1	2014/07/09 12:16:47
2	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:16:57
3	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:01
4	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:05
5	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:10
6	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:22
7	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:27
8	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:32
9	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:36
10	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:40
11	00:26:4D:55:7D:33	0	0	127.0.0.1	2014/07/09 12:17:44

Figura 4.28. Prueba de funcionamiento del cliente del servicio web para la consulta de mediciones por usuario.

Figura 4.29. Mensaje de error en caso de ingreso de dirección MAC no válida para la búsqueda de mediciones por usuario.

En la Figura 4.28 se observa también que la página que muestra los resultados de búsqueda de mediciones por usuario, brinda la posibilidad de seleccionar las opciones relacionadas tanto, con la búsqueda de mediciones por fecha para ese usuario, como con el cálculo del índice de disponibilidad del servicio por hora para el mismo usuario. Las opciones presentadas en el resultado de ésta consulta serán probadas en los puntos a continuación.

4.7.1.3 Prueba de Consulta de Mediciones por Usuario y Fecha

Para la realización de la prueba de ésta consulta, se parte de la página web JSP de resultados arrojados por la consulta de mediciones por usuario (probada en el punto anterior), tal como se diseñó e implementó en el capítulo correspondiente. En la Figura 4.22 de la consulta anterior, se observa que existe un campo para el ingreso de la fecha que servirá para la consulta en base a ésta. En éste campo se ingresa la fecha de prueba “2014/07/08 02:20”, obteniéndose el resultado ilustrado en la Figura 4.30.

Monitor de Ancho de Banda

Regresar Busqueda para otro Usuario Inicio

Número total de registros: 12

Resultado de busqueda

Número de Registro	Dirección MAC	Ancho de Banda de Bajada [Kbps]	Ancho de Banda de Subida [Kbps]	Dirección IPv4	Fecha
1	00:26:4D:55:7D:33	298	37	127.0.0.1	2014/07/08 02:20:03
2	00:26:4D:55:7D:33	348	31	127.0.0.1	2014/07/08 02:20:07
3	00:26:4D:55:7D:33	327	52	127.0.0.1	2014/07/08 02:20:12
4	00:26:4D:55:7D:33	340	28	127.0.0.1	2014/07/08 02:20:16
5	00:26:4D:55:7D:33	325	41	127.0.0.1	2014/07/08 02:20:20
6	00:26:4D:55:7D:33	326	47	127.0.0.1	2014/07/08 02:20:24
7	00:26:4D:55:7D:33	334	29	127.0.0.1	2014/07/08 02:20:28
8	00:26:4D:55:7D:33	326	13	127.0.0.1	2014/07/08 02:20:33
9	00:26:4D:55:7D:33	326	19	127.0.0.1	2014/07/08 02:20:37
10	00:26:4D:55:7D:33	170	26	127.0.0.1	2014/07/08 02:20:41
11	00:26:4D:55:7D:33	376	11	127.0.0.1	2014/07/08 02:20:45
12	00:26:4D:55:7D:33	230	50	127.0.0.1	2014/07/08 02:20:49

Figura 4.30. Prueba de funcionamiento del cliente del servicio web para la consulta de mediciones por usuario y fecha.

En el caso de que se ingrese como parámetro de búsqueda una fecha de la cual no existan registros, la aplicación retornara una lista de mediciones vacía, Figura 4.31.

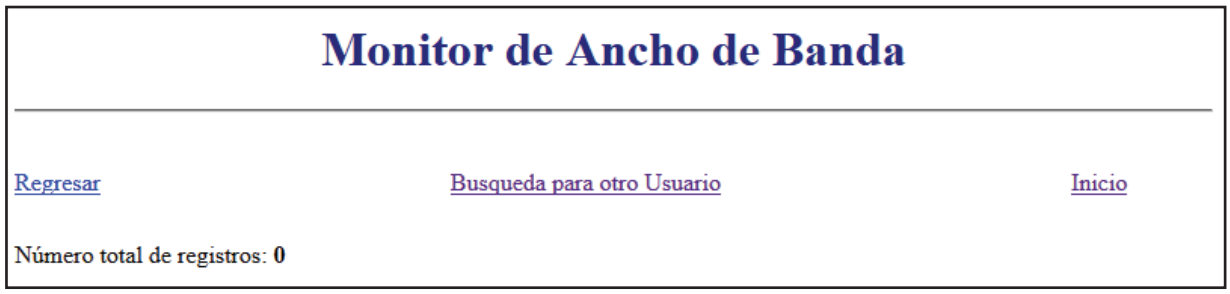
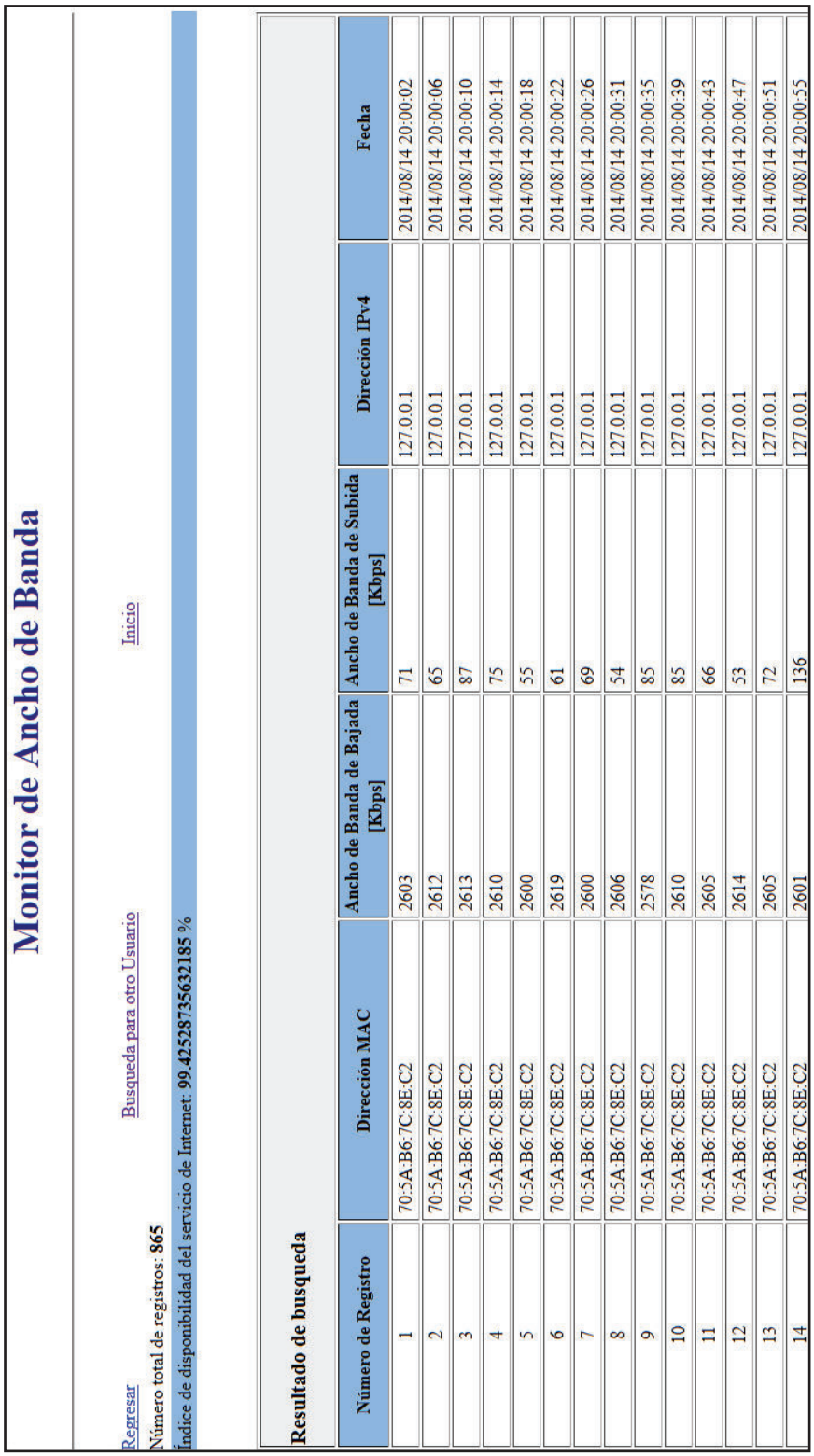


Figura 4.31. Lista de mediciones de usuario en el caso de ingreso de fecha de medición no registrada.

4.7.1.4 Prueba del Cálculo del Índice de Disponibilidad del Servicio de Internet

Al igual que la consulta anterior, ésta consulta parte de la página web JSP de despliegue de resultados de búsqueda de mediciones por usuario, en la cual existe la opción llamada “Calcular el Índice de Disponibilidad del Servicio de Internet”, la misma que al ser seleccionada despliega el formulario mostrado en la Figura 4.32.

Figura 4.32. Formulario para el ingreso de fecha por hora para el cálculo del índice de disponibilidad del servicio de Internet.



Monitor de Ancho de Banda

Regresar Busqueda para otro Usuario Inicio

Número total de registros: **865**

Índice de disponibilidad del servicio de Internet: **99.42528735632185 %**

Resultado de busqueda

Número de Registro	Dirección MAC	Ancho de Banda de Bajada [Kbps]	Ancho de Banda de Subida [Kbps]	Dirección IPv4	Fecha
1	70:5A:B6:7C:8E:C2	2603	71	127.0.0.1	2014/08/14 20:00:02
2	70:5A:B6:7C:8E:C2	2612	65	127.0.0.1	2014/08/14 20:00:06
3	70:5A:B6:7C:8E:C2	2613	87	127.0.0.1	2014/08/14 20:00:10
4	70:5A:B6:7C:8E:C2	2610	75	127.0.0.1	2014/08/14 20:00:14
5	70:5A:B6:7C:8E:C2	2600	55	127.0.0.1	2014/08/14 20:00:18
6	70:5A:B6:7C:8E:C2	2619	61	127.0.0.1	2014/08/14 20:00:22
7	70:5A:B6:7C:8E:C2	2600	69	127.0.0.1	2014/08/14 20:00:26
8	70:5A:B6:7C:8E:C2	2606	54	127.0.0.1	2014/08/14 20:00:31
9	70:5A:B6:7C:8E:C2	2578	85	127.0.0.1	2014/08/14 20:00:35
10	70:5A:B6:7C:8E:C2	2610	85	127.0.0.1	2014/08/14 20:00:39
11	70:5A:B6:7C:8E:C2	2605	66	127.0.0.1	2014/08/14 20:00:43
12	70:5A:B6:7C:8E:C2	2614	53	127.0.0.1	2014/08/14 20:00:47
13	70:5A:B6:7C:8E:C2	2605	72	127.0.0.1	2014/08/14 20:00:51
14	70:5A:B6:7C:8E:C2	2601	136	127.0.0.1	2014/08/14 20:00:55

Figura 4.33. Prueba de funcionamiento del cliente del servicio web para la consulta del índice de disponibilidad del servicio de Internet.

En los capítulos de análisis, diseño e implementación se determinó que el índice de disponibilidad del servicio de Internet será calculado por horas, es decir que en el formulario de la Figura 4.32, es necesario ingresar una dirección en formato de hora, siendo para el caso actual de comprobación la siguiente fecha: “2014/08/14 20”. La Figura 4.33 muestra los resultados de la consulta del índice de disponibilidad junto con una parte de la lista las mediciones consideradas para el cálculo del índice de disponibilidad.

4.7.2 PRUEBA DEL CLIENTE DEL SERVICIO WEB PARA LA GESTIÓN CONSULTA DE USUARIOS

Las pruebas del cliente del servicio web para la gestión y consulta de usuarios, están relacionadas con la demostración de la ejecución correcta de los procedimientos CRUD (Crear, Consultar, Actualizar y Eliminar) sobre los registros de la tabla Usuario de la base de datos de la aplicación, a través del uso del Cliente del Servicio Web de Consultas de la aplicación. Por ésta razón, se efectúan las siguientes pruebas de funcionamiento:

- Prueba de consulta de usuarios registrados.
- Ingreso de nuevo usuario.
- Prueba de búsqueda de usuario.
- Prueba de modificación de usuario.
- Prueba de eliminación de usuario.

4.7.2.1 Prueba de Consulta de Usuarios Registrados

Los resultados de ésta prueba pueden ser consultados en la Figura 4.34, donde se constata que efectivamente el Cliente del Servicio Web para la consulta de Usuarios es capaz de acceder a la lista completa de los usuarios registrados por la aplicación.

Figura 4.34. Prueba de funcionamiento del cliente del servicio web para la consulta de los usuarios registrados.

4.7.2.2 Prueba de Ingreso de Nuevo Usuario

La comprobación del funcionamiento correcto del ingreso de un nuevo usuario monitoreado a la aplicación, se puede consultar en las Figura 4.35 y Figura 4.36, donde además se determina que efectivamente todos los argumentos necesarios para éste procedimiento, son utilizados de forma correcta y en base a lo definido en los capítulos de análisis, diseño e implementación del presente documento.

Figura 4.35. Formulario de ingreso de nuevo usuario a la aplicación.

Monitor de Ancho de Banda

Inicio

Número Total de registros: 5

Usuarios Registrados

Dirección MAC	Identificación	Nombre	Proveedor Internet	Dirección Domicilio	Sector	Ciudad	Provincia
70:5A:B6:7C:8E:C2	1712875779	Andrés Tobar Gamba	CNT	Los Cedros OE3-241 y Pedro Boto	La Rumiñahui	Quito	Pichincha
00:30:67:6D:13:8F	0959632589	Anabel Noboa Bastidas	Satnet	Av. América 368	La Floresta 1	Machala	El Oro
00:C6:10:5F:68:74	1295863596	Michael Suarez Hernandez	Claro	9 de Octubre 580	Centro	Guayaquil	Guayas
00:26:4D:55:7D:33	1955230680	Betty Maldonado	CNT	Toledo 895 y Edmundo Borja	Arenales 2	Tulcan	Carchi
BB:BB:BB:BB:BB:BB	0980060077	Magaly Camacho	CNT	Riofrio 298	Las Dalias	Esmeraldas	Esmeraldas

Figura 4.36. Prueba de funcionamiento del cliente del servicio web para el ingreso de nuevo usuario.

4.7.2.3 Prueba de Búsqueda de Usuario

La prueba de funcionamiento correcto del cliente del servicio web para la búsqueda de un usuario registrado en la base de datos de la aplicación, queda demostrado en la Figura 4.37 y Figura 4.38. La búsqueda se realiza mediante el ingreso de la dirección MAC del usuario tal como se determino en la sección de diseño e implementación del presente proyecto.

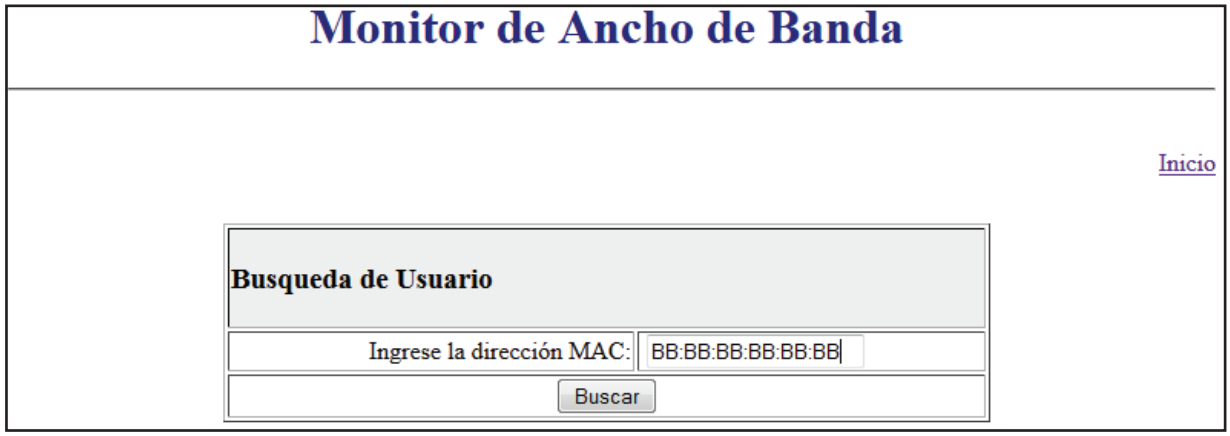


Figura 4.37. Formulario de ingreso de la dirección MAC para la búsqueda de usuario.

En el caso de que la dirección MAC ingresada no pertenezca a algún usuario registrado, la aplicación devolverá un mensaje de error tal como se observa en la Figura 4.39.

En la página web JSP donde se despliegan los resultados de la búsqueda del usuario, se encuentran también las opciones para la gestión de ese usuario, ya sea su modificación o eliminación, Figura 4.38, por lo que ésta página servirá de inicio para la prueba de funcionamiento de los procesos definidos en los puntos a continuación.

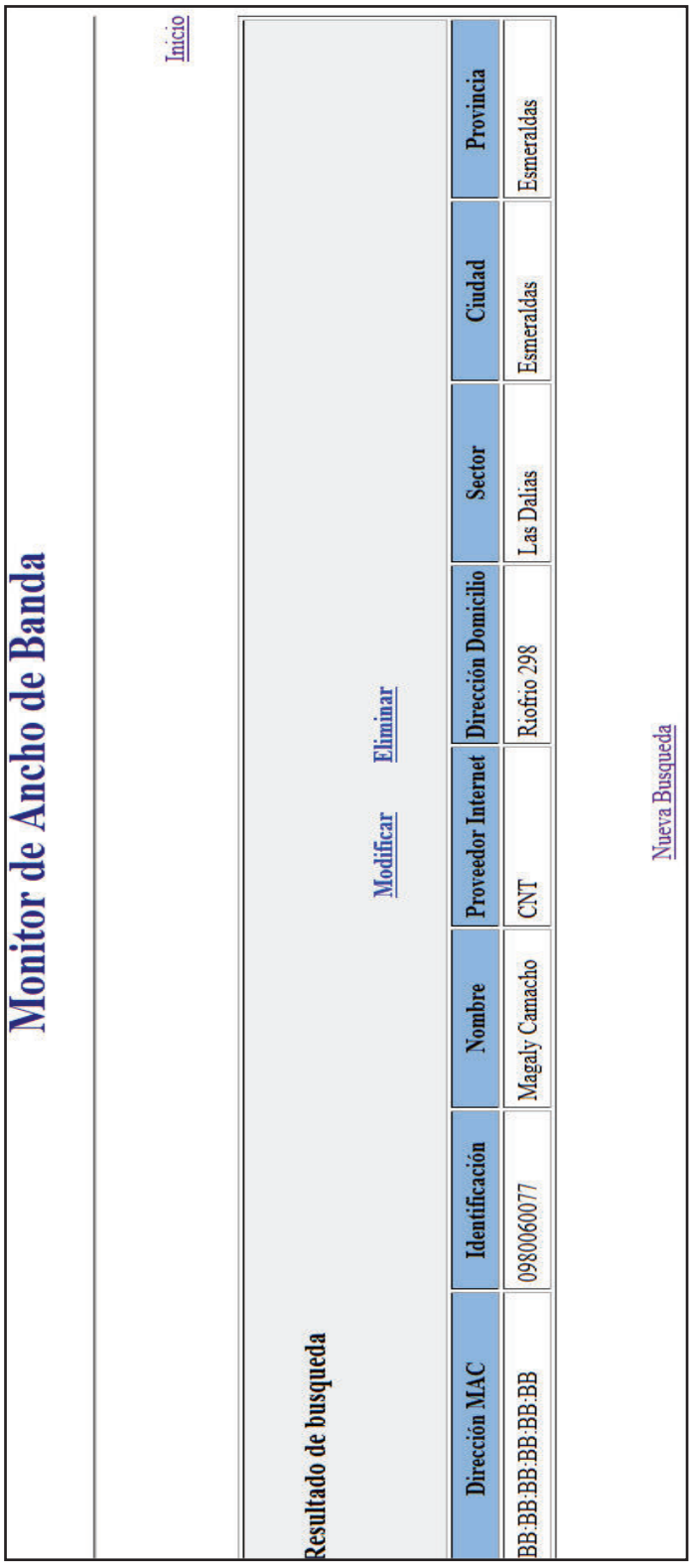


Figura 4.38. Prueba de funcionamiento del cliente del servicio web para la búsqueda de usuario.

Figura 4.39. Mensaje de error en caso de ingreso de dirección MAC no válida para la búsqueda de usuario.

4.7.2.4 Prueba de Modificación de Usuario

La prueba de funcionamiento de éste proceso, se realiza a partir del resultado obtenido por la búsqueda de usuario del punto anterior, y mediante la selección de la opción “Modificar” de ésta, se presenta un formulario en el cual es posible alterar la información del usuario actual, con la excepción de la dirección MAC, tal como se determino en el capítulo de diseño e implementación. Figura 4.40.

Una vez aceptada la modificación se visualiza la lista de todos los usuarios registrados hasta ese momento, en donde aparece el usuario modificado con todos sus datos actualizados, excepto la dirección MAC, Figura 4.41.

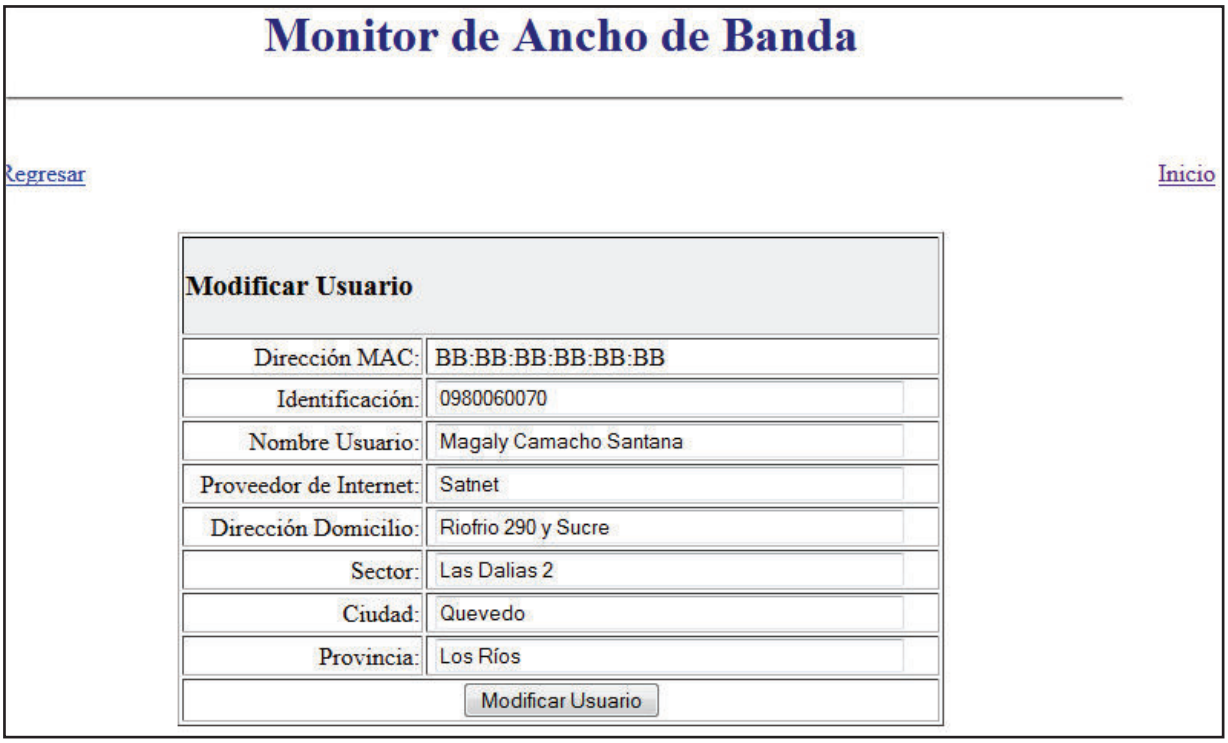


Figura 4.40. Formulario para la modificación de los datos de usuario.

4.7.2.5 Prueba de Eliminación de Usuario

Al igual que la prueba de funcionamiento anterior, ésta prueba parte desde el resultado de búsqueda de usuario, en donde se accede a la opción “Eliminar” para que inmediatamente se presente una página web JSP de confirmación de eliminación de usuario. Figura 4.43.

Si la eliminación de usuarios es aceptada, se presenta a continuación la lista actualizada de todos los usuarios registrados hasta ese momento, en donde se constata que efectivamente el usuario ha sido removido de la base de datos de la aplicación. Figura 4.42.

Monitor de Ancho de Banda

Inicio

Número Total de registros: 5

Usuarios Registrados

Dirección MAC	Identificación	Nombre	Proveedor Internet	Dirección Domicilio	Sector	Ciudad	Provincia
70:5A:B6:7C:8E:C2	1712875779	Andrés Tobar Gamba	CNT	Los Cedros OE3-241 y Pedro Boto	La Rumiñahui	Quito	Pichincha
00:30:67:6D:13:8F	0959632589	Anabel Noboa Bastidas	Satnet	Av. América 368	La Floresta 1	Machala	El Oro
00:C6:10:5F:68:74	1295863596	Michael Suarez Hernandez	Claro	9 de Octubre 580	Centro	Guayaquil	Guayas
00:26:4D:55:7D:33	1955230680	Betty Maldonado	CNT	Toledo 895 y Edmundo Borja	Arenales 2	Tulcan	Carchi
BB:BB:BB:BB:BB:BB	0980060070	Magaly Camacho Santana	Satnet	Riofrio 290 y Sucre	Las Dalias 2	Quevedo	Los Ríos

Figura 4.41. Prueba de funcionamiento del cliente del servicio web para la modificación de usuario.

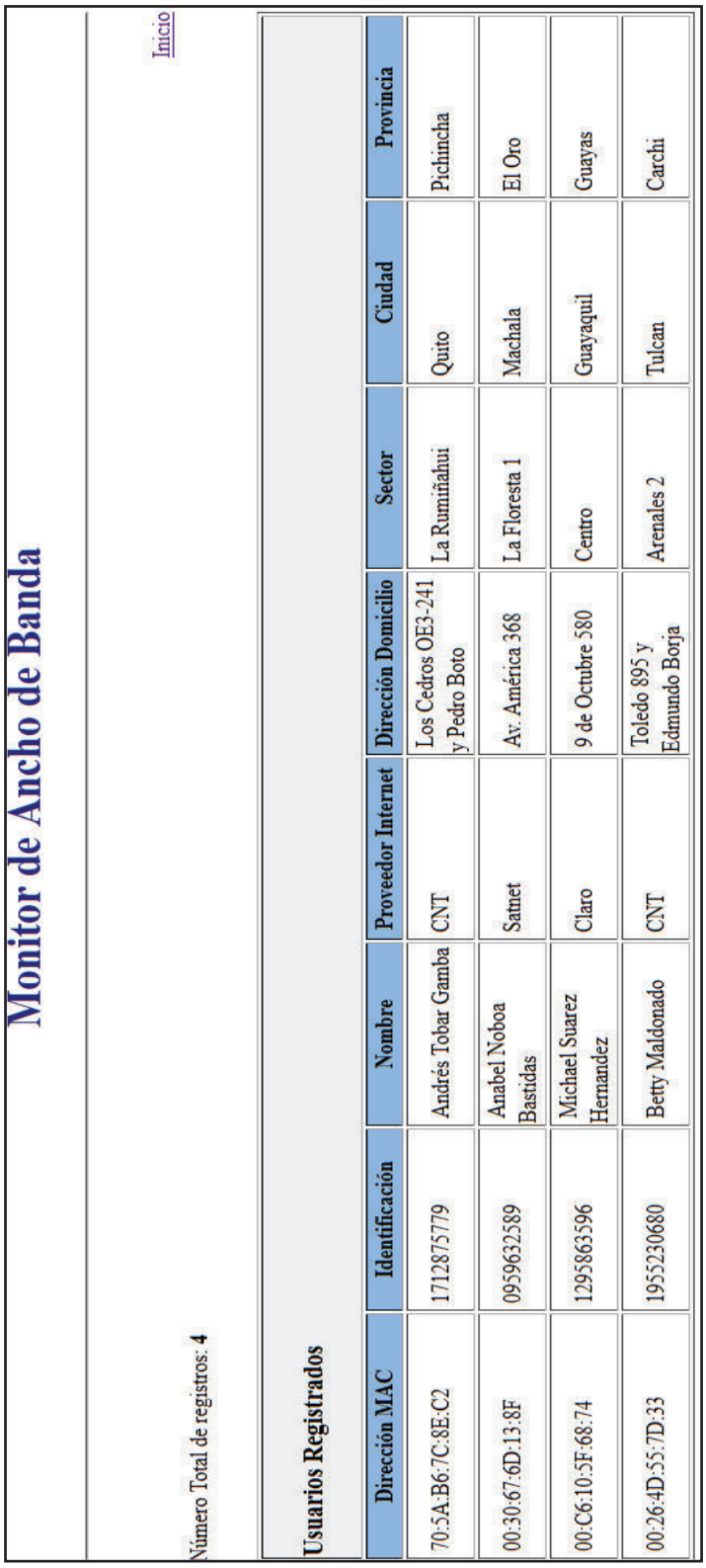


Figura 4.42. Prueba de funcionamiento del cliente del servicio web para la eliminación de usuario.

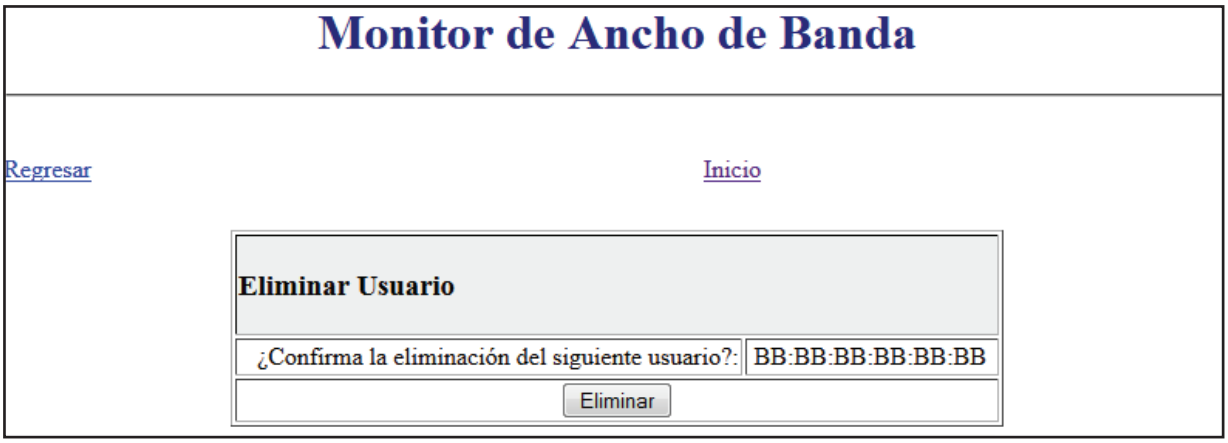


Figura 4.43. Página web JSP para la confirmación de la eliminación de usuario.

4.8 ANÁLISIS DE RESULTADOS DE LA APLICACIÓN

El propósito principal de la aplicación de monitorización del presente proyecto es la de capturar y calcular el ancho de banda de bajada, ancho de banda de subida e índice de disponibilidad del servicio de Internet, por lo que el análisis de los valores relacionados a éstos aspectos técnicos es necesario para determinar si la aplicación cumple con su cometido. De igual manera, los resultados obtenidos serán comparados, con los resultados obtenidos con otras aplicaciones para determinar si los resultados arrojados por la aplicación son confiables.

4.8.1 ANÁLISIS DE RESULTADOS DEL CÁLCULO DEL ÍNDICE DISPONIBILIDAD DEL SERVICIO DE INTERNET DE LA APLICACIÓN

En el mercado no existe una aplicación como tal para el cálculo y medición del nivel de disponibilidad del servicio de Internet, por lo que la única forma de corroborar que el método utilizado por la aplicación para la determinación del índice de disponibilidad es el correcto, se recurre a las definiciones y fórmulas teóricas para la obtención del porcentaje de disponibilidad.

En el capítulo de diseño e implementación se explicó el funcionamiento del método utilizado para el cálculo del índice de disponibilidad, el cual consiste en comparar el

número de mediciones recibidas durante una hora, contra el número de mediciones esperadas para ese periodo de tiempo, tal como se muestra en la Figura 4.44.

$$\%Disponibilidad\ por\ hora = \frac{\#\ Mediciones\ en\ una\ hora}{\#\ Mediciones\ esperadas\ en\ una\ hora} * 100$$

Figura 4.44. Fórmula para el cálculo del índice de disponibilidad del servicio de Internet usada por la aplicación.

Después de varias estimaciones se ha comprobado que el número de mediciones esperadas en una hora para aplicación es de 870 mediciones (entre 15 y 14 mediciones cada minuto), valor con el cual será calculado el índice de disponibilidad del servicio de Internet para una hora de la presenta aplicación.

Por su parte, la definición teórica del índice de disponibilidad de un servicio es la razón entre el tiempo en el cual el servicio está activo y el tiempo total de la prueba, tal como se muestra en la formulad de la Figura 4.45.

$$\%Disponibilidad\ por\ hora = \frac{Tiempo\ del\ servicio\ disponible\ en\ una\ hora}{1\ hora} * 100$$

Figura 4.45. Fórmula teórica para el cálculo del índice de disponibilidad de servicio.

Con el propósito de comparar al método de cálculo del índice de disponibilidad del servicio de Internet utilizado por la aplicación, con el método teórico, se han definido varios escenarios de prueba donde se suponen ciertos periodos de disponibilidad del servicio de internet durante una hora y donde es considerado el número de mediciones reales capturados efectivamente por la aplicación para esos periodos de tiempo dentro de una hora en concreto. Tabla 4.1.

Como se puede observar en la tabla, a medida que aumenta el tiempo de prueba, el índice de disponibilidad obtenida por la aplicación se aleja levemente del índice de

disponibilidad teórico, ésto debido a que el cálculo usado por la aplicación espera que lleguen efectivamente 870 mediciones para arrojar un resultado de índice de disponibilidad igual al 100%, pero factores como la sobrecarga de procesamiento y transmisión en el usuario monitoreado, provocan que cada captura de datos de monitorización tome más tiempo que el previsto, lo que a su vez ocasiona, que un número menor a 870 mediciones llegue al servidor de la aplicación.

Tabla 4.1. Comparativa del método de la aplicación y el método teórico para el cálculo del Índice de disponibilidad del servicio de Internet en una hora.

Tiempo de disponibilidad del servicio [minutos]	Tiempo de ausencia del servicio [minutos]	Número de Mediciones obtenidas por la aplicación	Disponibilidad en base al número de mediciones	Disponibilidad Teórica
0	60	0	0 %	0 %
10	50	145	16,6666 %	16,6666 %
20	40	288	33,1034 %	33,3333 %
30	30	432	49,6541 %	50,0000 %
40	20	577	66,3218 %	66.6666 %
50	10	721	82,8735 %	83,3333 %
60	0	865	99,4252 %	100,0000 %

A ciencia cierta es imposible determinar con certeza el número total de mediciones que son capturadas por la aplicación dentro de un periodo de tiempo determinado, ya que los diferentes módulos de la aplicación funcionando en el usuario monitoreado, en ocasiones sufren pequeñas latencias de procesamiento y transmisión que no

sobrepasan el segundo, pero al irse acumulando ésta latencia de segundo en segundo provoca que menos mediciones sean capturadas.

A pesar de éste inconveniente, el método usado por la aplicación para la obtención del índice de disponibilidad del servicio de Internet obtiene resultados bastante próximos a la realidad con un margen de error de aproximadamente del 0,5748 % en una hora, y que resulta de la diferencia entre el índice de disponibilidad teórico y el índice de disponibilidad en base al número de mediciones, indicadas previamente en la tabla 4.1

4.8.2 ANÁLISIS DE RESULTADOS DEL CÁLCULO DEL ANCHO DE BANDA DE LA APLICACIÓN

El ancho de banda obtenido por la aplicación, es el resultado del uso de las fórmulas indicadas en la Figura 4.46, y en la cual se utilizan los octetos de entrada y de salida presentes en la interfaz de red durante un periodo de tiempo determinado por la frecuencia de captura de los datos de monitorización, que para el caso de la aplicación es de 2 segundos.

$$ABbajada[bps] = \frac{(OctetosEntradaFinal - OctetosEntradaInicial)[bytes] * 8}{2\ [segundos]}$$

, y

$$ABsubida[bps] = \frac{(OctetosSalidaFinal - OctetosSalidaInicial)[bytes] * 8}{2\ [segundos]}$$

Figura 4.46. Fórmulas usadas por la aplicación para el cálculo del ancho de banda.

Los métodos tradicionales de medición de ancho de banda de Internet utilizan, bien sea el método de enviar la mayor cantidad de paquetes en un tiempo determinado, o el método de enviar un número determinado de paquetes para medir el tiempo que demoran éstos en ser transmitidos. Ambos métodos saturan el canal de transmisión en los dos sentidos (desde y hacia el cliente) para determinar tanto el ancho de

banda de bajada como el de subida. Además, ambos métodos utilizan la misma fórmula de cálculo de ancho de banda, presentada en la Figura 4.47.

$$ABbajada[bps] = \frac{\#Paquetes\ HTTP\ recibidos[bytes] * 8}{Tiempo\ de\ prueba}$$

, y

$$ABsubida[bps] = \frac{\#Paquetes\ HTTP\ enviados[bytes] * 8}{Tiempo\ de\ prueba}$$

Figura 4.47. Fórmulas usadas por la aplicación http://www.speedtest.netpara el cálculo del ancho de banda.

Éstos métodos tradicionales tienen el inconveniente de que inutilizan el canal de acceso a Internet para otras aplicaciones, además de que no consideran la sobrecarga de las capas enlace, internet y transporte del modelo TCP/IP, pero entregan resultados muy cercanos al ancho de banda máximo disponible en el canal de transmisión de los usuarios del servicio de Internet. La aplicación más común, que usa éste método para la determinación del ancho de banda es Speedtest.net

Por el contrario el método de cálculo de ancho de banda diseñado e implementado por la presente aplicación basada en SNMP, considera la sobrecarga generadas en las capas TCP/IP, ya que el cálculo se basa en los bits o Bytes que ingresan o salen de la interfaz de red conectada al Internet, además de que la aplicación no satura el canal de acceso a Internet con paquetes de prueba. El único inconveniente que tiene éste método, es que el ancho de banda calculado no siempre es el máximo al que tiene disposición el usuario del servicio, sino que será el ancho de banda de utilización del usuario, por lo que el ancho de banda máximo del canal será obtenido únicamente cuando éste destine su conexión a Internet para el intercambio de información multimedia demandante de gran cantidad de ancho de banda, como puede ser streaming video, consumo de videos en demanda de alta calidad, video-llamada, descarga y compartición P2P de archivos, etc.

Para el análisis de resultados del cálculo de ancho de banda de la presente aplicación, se realiza una prueba de medición del ancho de banda con la aplicación Speedtest, Figura 4.48, simultáneamente con una prueba de medición de ancho de banda a través de la aplicación diseñada e implementada en éste documento, Figura 4.49. Los resultados son presentados en forma resumida en la tabla 4.2 y tabla 4.3.

En la tabla 4.2 y tabla 4.3, se puede apreciar claramente que los resultados de ancho de banda obtenidos por la presenta aplicación, son muy similares a los obtenidos por la aplicación Speedtest.net, con lo que se confirma que los datos capturados y calculados por la aplicación, efectivamente corresponden al ancho de banda máximo disponible en los clientes del servicio de Internet.

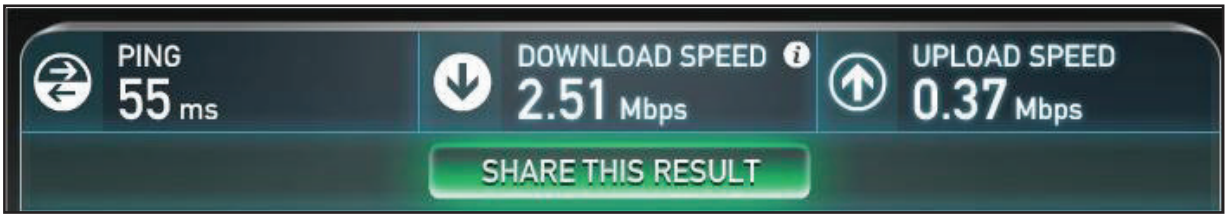


Figura 4.48. Cálculo de ancho de banda por medio de http://www.speedtest.net.

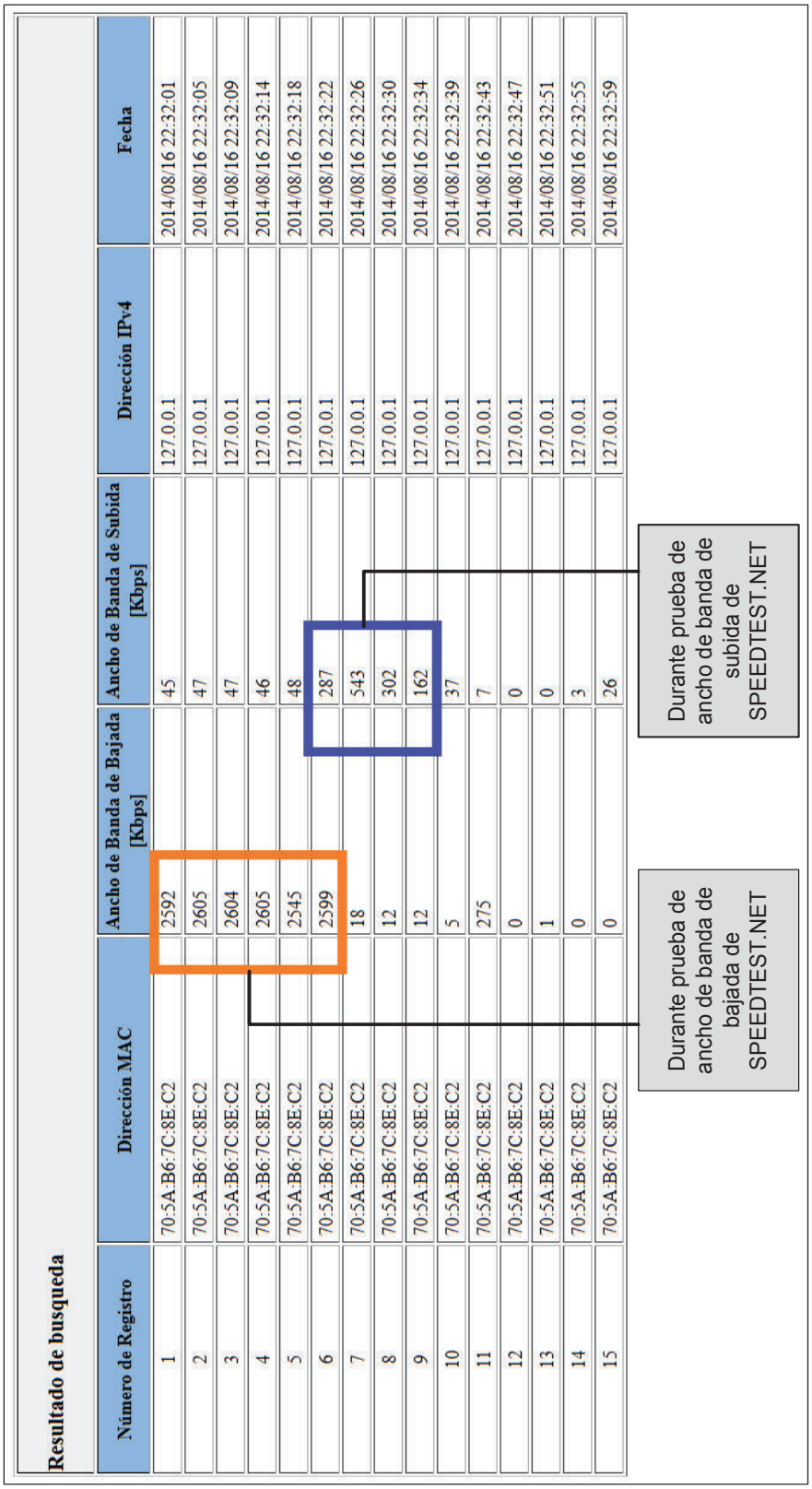


Figura 4.49. Cálculo de ancho de banda por medio de la presente aplicación.

Tabla 4.2. Comparativa de resultados de los métodos de cálculo del ancho de banda de bajada.

Ancho de banda de bajada calculado por la aplicación [Kbps]	Ancho de banda de bajada calculado por Speedtest.net [Kbps]
2592	2510
2605	
2604	
2605	
2545	
2599	
Promedio = 2591,666	

Tabla 4.3. Comparativa de resultados de los métodos de cálculo del ancho de banda de subida.

Ancho de banda de subida calculado por la aplicación [Kbps]	Ancho de banda de subida calculado por Speedtest.net [Kbps]
287	370
543	
302	
162	
Promedio = 323,5	

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

El servicio de Internet en el Ecuador se encuentra especificado en el Reglamento para los Abonados de los Servicios de Telecomunicaciones y de Valor Agregado, el mismo que únicamente norma los aspectos cualitativos del servicio de Internet más no los aspectos cuantitativos técnicos de los niveles mínimos a los que debe tener acceso el abonado de éste servicio, y por el contrario, delega a los proveedores del servicio de Internet la determinación de los términos técnicos mínimos del servicio, los mismos que son acordado entre el abonado y el proveedor mediante contratos o SLAs.

Para abonados residenciales del servicio de Internet el único aspecto técnico que es considerado contractualmente, es el ancho de banda máximo de bajada y de subida, por lo que éstos serán los únicos parámetros técnicos del servicio que puede ser medidos con el fin de controlar y proteger los derechos de los usuarios de éste tipo de servicio. La aplicación diseñada e implementada en éste documento para el control de los niveles del servicio de Internet, provee a la SUPERTEL de una herramienta computacional de control, que además de capturar y medir el ancho de banda de bajada y de subida, es capaz de determinar de forma muy aproximada el índice de disponibilidad al que tienen acceso los usuarios del servicio de Internet.

La implementación de éste tipo de aplicaciones de control permite que las entidades reguladoras de los servicios de telecomunicaciones del Ecuador puedan definir normativas y reglamentos donde se definan parámetros técnicos mínimos a los que deban regirse los proveedores de los servicios de telecomunicaciones y de valor agregado para la prestación de sus servicios, con el propósito de proteger los derechos de los abonados de éstos servicios.

La arquitectura de gestión de redes de computadoras Internet, basado en el protocolo SNMP demuestra ser una tecnología muy versátil con la cual es posible monitorizar y capturar un sin número de elementos y recursos computacionales y de red, que incluso pueden ir más allá de los definidos por el mismo estándar SNMP. La presente aplicación demostró que a pesar que el protocolo SNMP como tal no contempla la medición y monitorización del ancho de banda de bajada y de subida efectivos que son consumidos en una interfaz de red, permite que ésta sea desarrollada e implementada por medio de la creación de MIBs corporativas de propósito específico, aceptadas por el protocolo a través del ingreso de éstas dentro del nodo MIB Enterprises.

Por su parte, las aplicaciones corporativas JEE demostraron ser una arquitectura de aplicaciones distribuidas bastante robusta y segura que permite integrar de forma sencilla todos los componentes de una aplicación corporativa, llámense éstos, base de datos, lógica de las aplicaciones, componentes de usuario, etc. Además, al basar su funcionamiento en la arquitectura Java, se asegura que las aplicaciones distribuidas desarrolladas bajo ésta, hereden todos los beneficios que provee Java, como puede ser independencia de plataforma y portabilidad.

Se comprobó que los servicios web JAX-WS de JEE proveen la capacidad de desarrollar aplicaciones distribuidas que funcionen sobre Internet de forma rápida y eficiente, ya que la información de las aplicaciones basadas en ésta tecnología serán encapsuladas dentro de mensajes SOAP usando como medio de transporte sobre Internet a HTTP, factor que a su vez provoca que ésta información pueda ser consumida por aplicaciones desarrolladas con otro tipo de lenguaje de programación, no solo por aplicaciones Java.

El método de cálculo de ancho de banda propuesto por éste proyecto, demostró obtener resultados bastante aproximados a la realidad, superando incluso a otro tipo de aplicaciones similares, ya que el fuerte de la aplicación descrita en éste documento, es que accede directamente al número de bytes enviados y recibidos por

la interfaz de red conectada al Internet, asegurando que la medición de ancho de banda de bajada y de subida es efectivamente la entregada por el canal de transmisión a través del DCE o modem. Por el contrario, el mayor inconveniente que enfrenta éste método es que no en todo momento se podrá medir el ancho de banda máximo entregado por el proveedor del servicio de Internet al abonado, sino únicamente cuando el usuario sature su conexión mediante el uso de aplicaciones demandantes de gran ancho de banda.

El índice de disponibilidad del servicio de Internet, calculado por la aplicación en base al número de mediciones recibidas por la aplicación desde los usuarios monitoreados, arrojo resultados muy cercanos a la realidad, haciendo que éste método pueda ser una alternativa al método teórico de cálculo del índice de disponibilidad del servicio de Internet, pero todavía es muy temprano afirmar ésto ya que es necesario realizar un número mayor de pruebas para periodos de prueba más extensos.

A pesar que el índice de disponibilidad del servicio de Internet no es considerado dentro del contrato o SLAs entre los proveedores y el abonado residencial del servicio de Internet, la aplicación del presente proyecto implementa la monitorización de éste parámetro con el propósito de disponer de más herramientas de control de la prestación del servicio de Internet, para que en un futuro parámetros de servicio tan fundamentales como éste, sean considerados como parámetros técnicos contractuales que los proveedores del servicio de Internet deban cumplir.

Durante el desarrollo de la nueva aplicación, el componente que genero más inconvenientes para su creación y puesta en funcionamiento, fue sin ligar a dudas el Agente SNMP versión 3, ya que en un inicio se trato de desarrollar éste componente en base al API SNMP4j, el cual cuenta con muy poca documentación, y soporte técnico. Por el contrario el API Adventnet dispone de bastante documentación, y la asistencia técnica siempre está disponible a pesar de no contar con una licencia pagada.

El desarrollo de la aplicación a través del IDE Eclipse resultó de gran ayuda ya que en éste simplifica las labores de creación y prueba de las distintas capas de la estructura multi-nivel de las aplicaciones corporativas JEE, al integrar en la misma plataforma el uso y prueba de la base de datos, uso y prueba del servidor JEE (Weblogic 12c), uso y prueba de JSP a través de un navegador web, y un sin número de otros componentes que si no están disponibles pueden ser descargados por medio del mismo IDE.

De igual manera, el IDE Eclipse ayudó con la creación automática de varios componentes de la aplicación como: entidades JPA en base a tablas relacionales de la base de datos, y clases JAXB y tipos XSD en base al esquema XSD. Lo que sí, el IDE no fue capaz de asistir en la creación de las clases JAXB remotas que se utilizan en el lado del cliente del servicio web, en base al contenido de los archivos WSDL, por lo que para éste caso se recurrió al uso del comando *wsimport*[18] en el procesador de comandos del sistema operativo.

5.2 RECOMENDACIONES

- Por la naturaleza de los datos de monitorización capturados en los usuarios del servicio de Internet, éstos son transportados a través de Internet en texto plano, pero si se desea agregar características de seguridad como privacidad e integridad a ésta información, se recomienda utilizar certificados digitales (protocolo TLS) a nivel del servidor corporativo JEE Weblogic, para lo cual es necesario adquirir un certificado digital a través de una entidad certificadora.
- A pesar de que la aplicación obtiene resultados del índice de disponibilidad del servicio de Internet muy aproximados a la realidad, si se requiere medirlo con mayor precisión, es recomendable implementar el método teórico de cálculo del índice de disponibilidad directamente en los usuario monitoreados; lo que representa un mayor grado de complejidad de diseño e implementación, y no

[18]http://docs.oracle.com/javase/6/docs/technotes/tools/share/wsimport.html

en base a las mediciones recibidas de éstos, como lo hace la presente aplicación.

- En el supuesto caso que la presente aplicación sea utilizada por la SUPERTEL de forma masiva en los usuarios del servicio de Internet, es recomendable que ésta sea distribuida a aquellos usuarios que destinan su conexión de Internet al uso de aplicaciones demandantes de gran ancho de banda, logrando así que los resultados de monitorización de ancho de banda obtenidos desde éstos, sean la mayor parte del tiempo correspondientes al ancho de banda máximo disponible en el canal.
- El tipo de consultas a la base de datos implementadas por la aplicación, fueron creadas en base al análisis de requerimientos consultado al personal técnico de UCPS, que respondía a las necesidades establecidas en su momento para éste, pero es recomendable añadir otro tipo de consultas como puede ser: consulta de mediciones por ISP, consulta de mediciones por sector o nodo del usuario, etc., con el propósito de expandir el control que se puede realizar sobre los proveedores del servicio de Internet, y que la presente aplicación si lo permite.
- Para la creación de componentes SNMP (agentes, gestores y MIBs) de cualquier versión, se recomienda el uso del API Adventnet, debido a que éste cuenta con la documentación y asistencia técnica necesaria provista por la organización WebNMS.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS

- W. Stallings,“Digital Data Communications Techniques” en *Data and Computer Communications*, 8va Edición, Upper Saddler River: Pearson Prentice Hall, 2007, pp. 91-96.

- W. Stallings, *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*, 3ra Edición, Upper Saddler River: Addison-Wesley, 1999.

ESTÁNDARES

- Spectra and Bandwidth of Emissions, Recomendación, ITU-R SM.328-10, 1999. (Ancho de Banda).

- OSI management – Management Communication Service and Protocol,ITU-TX.711, 1997. (CMIP).

- A Simple Network Management Protocol (SNMP), RFC 1157, 1990.

- Introduction to Community-based SNMPv2, RFC 1901, 1996.

- An Arquitechture for Describing Simple Network Management Protocol (SNMP) Managemente Frameworks, RFC 3411, 2002. (SNMPv3).

- OSI Networking and System Aspects – Abstract Syntax Notation 1, ITU-T X.690, 2002.

- Conformance Statements for SMIv2, RFC 2580, 1999.

- Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing RFC 7230, Junio 2014.

- 1000BASE-T Task Force, IEEE 802.3ab, 1999.

- 10BASE-T 10 Mbit/s over twisted pair, IEEE 802.3I, 1990.

- 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s, IEEE 802.3u, 1995.

- Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks, IEEE 802.3q, 2011.

- A TCP/IP Tutorial, RFC 1180, 1991.

- The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, 2008.

- IP Packet Delay Variation Metric for IP Performance Metrics (IPPM), RFC 3393, 2002. (Jitter).

- Rapid Spanning Tree Protocol (RSTP), IEEE 802.1w, 2004.

- Internet Security Glossary, Version 2, RFC 4949, 2007. (ACL).

- Further Higher Data Rate Extension in the 2.4GHz Band, IEEE 802.11g 2003.

- Amendment 5: Enhancements for Higher Throughput, IEEE.802.11n, 2009.

- Security Achitecture for the Internet Protocol, RFC 2401, 1998. (IPSec).

- The Secure Shell (SSH) Transport Layer Protocol, RFC 4253, 2006.
- Network time Protocol Version 4: Protocol and Algorithms Specifications, RFC 5905, 2010.
- Remote Authentication Dial In User Server (RADIUS), RFC 2865, 2000.
- An Access Control Protocol, Sometimes Called TACACS, RFC 1492, 1993.
- Port Based Network Access Control, IEEE 802.1x, 2004.
- Lightweight Directory Access Protocol (LDAP): The Protocol, RFC 4511, 2006.
- IEEE Recommended Practice for Software Requirements Specifications, IEEE STD 830, 1998.
- US Secure Hash Algorithm 1 (SHA1), RFC 3174, 2001.
- The MD5 Message-Digest Algorithm, RFC 1321, 1991.

SITIOS WEB

- Speedtest Support, How does the test itself Work? How the result is calculated? [En línea], Enero 13 de 2012. Disponible en: https://support.speedtest.net/entries/20862782-How-does-the-test-itself-work-How-is-the-result-calculated-
- W3C, Web Services Description Language (WSDL) 2.0 [En línea], 2007. Disponible en: http://www.w3.org/TR/wsdl20-primer

- W3C, Extensible Markup Language (XML) 1.0 (Fifth Edition) [En línea], 2008. Disponible en: http://www.w3.org/TR/2008/REC-xml-20081126

- W3C, Simple Object Access Protocol (SOAP) 1.1 [En línea], 2000. Disponible en: http://www.w3.org/TR/2000/NOTE-SOAP-20000508

- Pivotal Software, Spring Data JPA [En línea], 2014. Disponible en: http://projects.spring.io/spring-data-jpa

- Oracle, Introduction to Contexts and Dependency Injection for the Java EE Platform [En línea], 2013. Disponible en: https://docs.oracle.com/javaee/6/tutorial/doc/giwhb.html

- Cisco Systems, SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) [En línea], 2013. Disponible en: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html

- Oracle, The Java 7 EE Tutorial [En línea], 2014. Disponible en: https://docs.oracle.com/javaee/7/tutorial/doc

- CONATEL, Reglamento para los abonados de los servicios de Telecomunicaciones y de valor agregado [En línea], 2012. Disponible en: http://www.supertel.gob.ec/pdf/reglamento_abonados_clientes_usuarios.pdf

- Cisco Systems, Cisco SAFE Reference Guide [En línea], 2014. Disponible en: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html

- Verizon, Service Level Agreement (SLA) Internet Dedicated Services[En línea], 2014. Disponible en: http://verizonenterprise.com/terms/us/products/internet/sla

- Cisco Systems, Wireless LAN Controller (WLC) FAQ [En línea], 2009. Disponible en: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html

- Cisco Systems, Cisco Network Admission Control (NAC) Solution Data Sheet [En línea], 2014. Disponible en: http://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html

- Cisco Systems, Cisco Secure ACS Overview [En línea], 2006. Disponible en: https://wiki.aarnet.edu.au/download/attachments/32866308/Cisco_ACS_Eduroam.pdf

- Cisco Systems, Cisco Prime for IT and Service Providers [En línea], 2014. Disponible en: http://www.cisco.com/c/en/us/products/cloud-systems-management/prime.html

- Stanford Engineering - Computer Science, RISC Architecture [En línea], 2014. Disponible en: http://cs.stanford.edu/people/eroberts/courses/soco/projects/risc/risccisc

- Microsoft, Active Directory Architecture [En línea], 2014. Disponible en: http://technet.microsoft.com/en-us/library/bb727030.aspx

- Cisco Support Community, Advantages of distribution layer in network [En línea], 2014. Disponible en:

https://supportforums.cisco.com/discussion/10464056/advantages-distribution-layer-network

- Cisco Systems, How Does RADIUS work? [En línea], 2014. Disponible en: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

- Cisco Systems, SSL VPN Security [En línea], 2014. Disponible en: http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html

- Cisco Systems, Hot Standby Router Protocol Features and Functionality [En línea], 2006. Disponible en: http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

- Cisco Systems, Cisco IronPort Email Security Plug-in [En línea], 2006. Disponible en: http://www.cisco.com/c/dam/en/us/td/docs/security/esa/plugin/Cisco_Email_Plug-in_7-1_Admin_Guide.pdf

- M. Adisson, Jasig Introduction, [En línea], 2011. Disponible en: https://wiki.jasig.org/display/CASUM/1.+Introduction

- K. Schwaber y J. Sutherland, La Guía de SCRUM [En línea], 2013. Disponible en: http://www.scrumguides.org/docs/scrumguide/v1/Scrum-Guide-ES.pdf

- W3C, Web Service Architecture [En línea], 2002. Disponible en: http://www.w3.org/TR/2002/WD-ws-arch-20021114

- Hyperic – Spring Source Home, SIGAR – System Information Gatherer and Reporter [En línea], 2010. Disponible en: https://support.hyperic.com/display/SIGAR/Home

- Cisco Systems, Goodbye DES, Welcome AES [En línea], 2001. Disponible en: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_4-2/goodbye_des.html

- CEPAL – Observatorio Regional de Banda Ancha (ORBA), Estado de la Banda Ancha en América Latina y el Caribe (2012) [En línea], 2012. Disponible en: http://www.cepal.org/publicaciones/xml/9/48449/estadobandaanchaenamlc.pdf

- Web Site Optimization, Average Web Page [En línea], 18 Julio de 2014. Disponible en: http://www.websiteoptimization.com/speed/tweak/average-web-page/

- Cisco Support Community, Calculate Bandwidth Using SNMP Index [En línea], 2008. Disponible en: https://supportforums.cisco.com/discussion/10554891/calculate-bandwidth-using-snmp-index

- ZOHO – WebNMS, AdventNet SNMPv3 Index [En línea], 2012. Disponible en: http://www.webnms.com/snmp/help/snmpapi/snmpv3

- Oracle, Using JAXB Data Binding [En línea], 2014. Disponible en: http://docs.oracle.com/cd/E13222_01/wls/docs103/webserv/data_types.html

- D. Bell, UML Basics: The Sequence Diagram [En línea], 16 Febrero de 2004. Disponible en: http://www.ibm.com/developerworks/rational/library/3101.html

- Oracle, A Relational Database Overview [En línea], 2014. Disponible en: https://docs.oracle.com/javase/tutorial/jdbc/overview/database.html

- Oracle, Introduction to Persistence Layer [En línea], 2014. Disponible en: http://docs.oracle.com/cd/E17904_01/web.1111/b32441/persun.htm#JITDG93257

- Oracle, Core J2EE Patterns – Data Access Object [En línea], 2014. Disponible en: http://www.oracle.com/technetwork/java/dataaccessobject-138824.html

- Paul Leahy, Accessors and Mutators [En línea], 2014. Disponible en: http://java.about.com/od/workingwithobjects/a/accessormutator.htm

- Oracle, JPQL Language Reference [En línea], 2011. Disponible en: https://docs.oracle.com/html/E24396_01/ejb3_langref.html

- W3C, XML Schema Definition Language (XSD) 1.1 Part 1: Structures [En línea], 2012. Disponible en: http://www.w3.org/TR/xmlschema11-1/

- Oracle, Delegation [En línea], 2010. Disponible en: http://docs.oracle.com/cd/E19879-01/820-4336/gfqpi/index.html

- Oracle, JavaServer Pages Technology [En línea], 2014. Disponible en: http://www.oracle.com/technetwork/java/faq-137059.html#2

- Oracle, JSP Scriplets [En línea], 2010. Disponible en: https://docs.oracle.com/javaee/5/tutorial/doc/bnaou.html

- Oracle, wsimport – Java API for XML Web Services (JAX-WS) 2.0 [En línea], 2011. Disponible en: http://docs.oracle.com/javase/6/docs/technotes/tools/share/wsimport.html

- Oracle, Methods for CRUD Operations [En línea], 2014. Disponible en: https://docs.oracle.com/cd/E52858_01/books/OnDemJavaDev/OnDemJavaDev_APIRef17.html

PAPERS

- J. Gray y D. Siewiorek, “High Availability Computer Systems”, IEEE Computer Magazine, Volumen 24 – Fascículo 9, IEEE, Septiembre 1991.

TÉSIS

- O. Rosero, D. Proaño y X. Calderón, “Estudio y Desarrollo de una Metodología para la Implementación de un Modelo de Gestión y Administración de Red para la Universidad Técnica Estatal de Quevedo (UTEQ)”, EPN, Quito, Julio 2009.

ANEXOS

Anexo A. Documento de la SUPERTEL de auspicio del proyecto

SUPERINTENDENCIA DE TELECOMUNICACIONES

SUPERTEL

Oficio N° IRN-2013-01555

Quito, 10 de octubre de 2013

Ingeniero
Pablo Hidalgo
COORDINADOR DE LA FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
ESCUELA POLITÉCNICA NACIONAL – E.P.N.
Ladrón de Guevara E11-253
Teléfono: 2507126
Distrito Metropolitano de Quito – Provincia de Pichincha

ASUNTO: APROBACIÓN DE EJECUCIÓN DE TESIS DE GRADO, ESTUDIANTE ANDRÉS CAMILO TOBAR GAMBA.

De mi consideración:

En referencia al oficio IRN-2011-00625 del 13 de septiembre de 2011 relacionado con el Oficio FIEE-CIERI-059-2011 de 5 de septiembre de 2011, enviado por la E.P.N. mediante el cual se solicitó a esta Superintendencia de Telecomunicaciones que prestara las facilidades necesarias para cumplir con el proyecto de titulación "Diseño e implementación de un sistema de control de calidad de los proveedores de servicios de Internet basado en el protocolo SNMP" a ser desarrollado por el señor Andrés Camilo Tobar Gamba; como alcance al oficio mencionado anteriormente y en razón de que la petición ya fue autorizada por este Organismo Técnico de Control, ratificamos nuestro interés y colaboración en el desarrollo del Proyecto.

La coordinación del proyecto estará a cargo de la Unidad de Prestación de Servicios de Telecomunicaciones de esta Intendencia Regional Norte, debiendo el mencionado estudiante acercarse a las instalaciones de esta Unidad Administrativa para revisar las actividades a ejecutar con el fin de desarrollar el proyecto técnico propuesto.

Atentamente,

Ing. Verónica Yerovi Arias
INTENDENTA REGIONAL NORTE

SUPERINTENDENCIA DE TELECOMUNICACIONES SUPERTEL INTENDENCIA REGIONAL QUITO - ECUADOR

Av. Amazonas 40-71 y Gaspar de Villarroel * PBX (593-2) 2 272-180 * info@supertel.gob.ec
Dirección Nacional de Información y Servicio al Ciudadano DIS Quito * Telf.: (02) 2451-340 dis@supertel.gob.ec 1800 567-567
Quito-Ecuador

www.supertel.gob.ec

Anexo B. Archivo MonitorABModulo

```
-- File Name : MonitorABModulo
-- Date      : Tue Aug 05 16:41:50 COT 2014
-- Author    : WebNMS Agent Toolkit Java Edition - MIB Editor 6



MonitorABModulo   DEFINITIONS ::= BEGIN
        IMPORTS
                DisplayString
                        FROM SNMPv2-TC
                DisplayString
                        FROM RFC1213-MIB
                enterprises, MODULE-IDENTITY, OBJECT-TYPE, Integer32
                        FROM SNMPv2-SMI;

        supertel        MODULE-IDENTITY
                LAST-UPDATED    "201407031557Z"
                ORGANIZATION    "Superintendencia de Telecomunicaciones"
                CONTACT-INFO    "info@supertel.gob.ec"
                DESCRIPTION             "Monitor de ancho de banda de la Supertel"
                REVISION            "201407031557Z"
                DESCRIPTION             ""
                ::= { enterprises 1 }

        private         OBJECT IDENTIFIER
                ::= { internet 4 }

        enterprises   OBJECT IDENTIFIER
```

```
        ::= { private 1 }
    monitorAB    OBJECT IDENTIFIER
        ::= { supertel 1 }

    abBajada     OBJECT-TYPE
        SYNTAX              Integer32
        MAX-ACCESS          read-only
        STATUS              current
        DESCRIPTION         "Ancho de banda de bajada"
        ::= { monitorAB 1 }

    abSubida     OBJECT-TYPE
        SYNTAX              Integer32
        MAX-ACCESS          read-only
        STATUS              current
        DESCRIPTION         "Ancho de banda de subida"
        ::= { monitorAB 2 }

    direccionMAC        OBJECT-TYPE
        SYNTAX              DisplayString
        MAX-ACCESS          read-only
        STATUS              current
        DESCRIPTION         "Direccion MAC"
        ::= { monitorAB 3 }

    oid     OBJECT IDENTIFIER
        ::= { enterprises 2 }

END
```

Anexo C. Archivo persistence.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<persistence version="2.0" xmlns="http://java.sun.com/xml/ns/persistence"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/persistence
http://java.sun.com/xml/ns/persistence/persistence_2_0.xsd">
    <persistence-unit name="monitorAnchoBandaServidor" transaction-
type="RESOURCE_LOCAL">
        <provider>org.eclipse.persistence.jpa.PersistenceProvider</provider>
        <class>ec.gob.supertel.monitorAnchoBanda.beans.Medicion</class>
        <class>ec.gob.supertel.monitorAnchoBanda.beans.Usuario</class>
        <properties>
            <property name="eclipselink.target-server" value="WebLogic"/>
            <property name="javax.persistence.jdbc.url"
value="jdbc:oracle:thin:@localhost:1521:xe"/>
            <property name="javax.persistence.jdbc.user"
value="monitorABUsuario"/>
            <property name="javax.persistence.jdbc.password"
value="supertel123"/>
            <property name="javax.persistence.jdbc.driver"
value="oracle.jdbc.OracleDriver"/>
        </properties>
    </persistence-unit>
</persistence>
```

Anexo D. Archivo MonitorAnchoBanda.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"

        targetNamespace="http://www.supertel.gob.ec/monitorAnchoBanda/jaxb"
                xmlns:tns="http://www.supertel.gob.ec/monitorAnchoBanda/jaxb"
elementFormDefault="qualified">

<complexType name="UsuarioType">
        <sequence>
                <element name="direccionMac" type="string" maxOccurs="1"
minOccurs="1"></element>
                <element name="id" type="string" maxOccurs="1"
minOccurs="1"></element>
                <element name="nombre" type="string" maxOccurs="1"
minOccurs="1"></element>
                <element name="isp" type="string" maxOccurs="1"
minOccurs="1"></element>
                <element name="direccion" type="string" maxOccurs="1"
minOccurs="1"></element>
                <element name="sector" type="string" maxOccurs="1"
minOccurs="1"></element>
                <element name="ciudad" type="string" maxOccurs="1"
minOccurs="1"></element>
                <element name="provincia" type="string" maxOccurs="1"
minOccurs="1"></element>
        </sequence>
</complexType>
```

```
<complexType name="MedicionType">
        <sequence>
<!--            <element            name="id"            type="long"            maxOccurs="1"
minOccurs="1"></element> -->
                        <element      name="abbajada"      type="long"      maxOccurs="1"
minOccurs="1"></element>
                <element        name="absubida"        type="long"        maxOccurs="1"
minOccurs="1"></element>
                <element    name="usuario"    type="tns:UsuarioType"    maxOccurs="1"
minOccurs="1"></element>
                        <element    name="direccionip"    type="string"    maxOccurs="1"
minOccurs="1"></element>
                <element        name="fecha"        type="string"        maxOccurs="1"
minOccurs="1"></element>

        </sequence>
</complexType>

<complexType name="UsuarioResultType">
        <sequence>
                <element              name="usuarios"              type="tns:UsuarioType"
maxOccurs="unbounded" minOccurs="0"></element>
        </sequence>
</complexType>

<complexType name="MedicionResultType">
        <sequence>
                <element              name="mediciones"              type="tns:MedicionType"
maxOccurs="unbounded" minOccurs="0"></element>
        </sequence>
</complexType>
```

```
<element name="faultInfo">
        <complexType>
                <sequence>
                        <element name="detailMessage" type="string"></element>
                </sequence>
        </complexType>
</element>

</schema>
```

Anexo E. Archivo applicactionContext.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?><beans
xmlns="http://www.springframework.org/schema/beans"
xmlns:context="http://www.springframework.org/schema/context"
xmlns:tx="http://www.springframework.org/schema/tx"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-2.5.xsd
http://www.springframework.org/schema/tx
http://www.springframework.org/schema/tx/spring-tx-2.5.xsd
http://www.springframework.org/schema/context
http://www.springframework.org/schema/context/spring-context-2.5.xsd">



<!--bean post-processor for JPA annotations-->
<bean
class="org.springframework.orm.jpa.support.PersistenceAnnotationBeanPostProcess
or">
</bean>

<!--Exception translation bean post processor-->
<bean
class="org.springframework.dao.annotation.PersistenceExceptionTranslationPostPro
cessor">
</bean>

<!--Transaction manager for a single JPA EntityManager (alternative to JTA)-->
```

```
<bean class="org.springframework.orm.jpa.LocalEntityManagerFactoryBean"
id="entityManagerFactory">
<property name="persistenceUnitName" value="monitorAnchoBandaServidor"/>
</bean>
<bean class="org.springframework.orm.jpa.JpaTransactionManager"
id="transactionManager">
<property name="entityManagerFactory" ref="entityManagerFactory"/>
</bean>


<!-- enable the configuration of transactional behavior based on annotations -->
<tx:annotation-driven transaction-manager="transactionManager"/>

<bean
class="ec.gob.supertel.monitorAnchoBanda.delegates.impl.UsuarioSpringDelegate"
id="UsuarioDelegateService">
<property name="usuarioDao">
<bean class="ec.gob.supertel.monitorAnchoBanda.dao.impl.UsuarioJPADao"/>
</property>
</bean>

<bean
class="ec.gob.supertel.monitorAnchoBanda.delegates.impl.MedicionAddSpringDeleg
ate" id="MedicionAddDelegateService">
<property name="medicionAddDao">
<bean class="ec.gob.supertel.monitorAnchoBanda.dao.impl.MedicionAddJPADao"/>
</property>
</bean>
```

```
<bean
class="ec.gob.supertel.monitorAnchoBanda.delegates.impl.MedicionSpringDelegate"
id="MedicionDelegateService">
<property name="medicionDao">
<bean class="ec.gob.supertel.monitorAnchoBanda.dao.impl.MedicionJPADao"/>
</property>
</bean>

<context:annotation-config/>
</beans>
```

Anexo F. Archivo web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://java.sun.com/xml/ns/javaee"
xmlns:web="http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd" id="WebApp_ID" version="3.0">
<display-name>MonitorABServidor</display-name>
<welcome-file-list>
<welcome-file>index.html</welcome-file>
<welcome-file>index.htm</welcome-file>
<welcome-file>index.jsp</welcome-file>
<welcome-file>default.html</welcome-file>
<welcome-file>default.htm</welcome-file>
<welcome-file>default.jsp</welcome-file>
</welcome-file-list>
<security-constraint>
<web-resource-collection>
<web-resource-name>webservice</web-resource-name>
<url-pattern>/monitorAnchoBandaServidor/MedicionAddWebService</url-pattern>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>rolUsuarioMonitorAB</role-name>
</auth-constraint>
</security-constraint>
<login-config>
<auth-method>BASIC</auth-method>
<realm-name>default</realm-name>
```

```
</login-config>
<security-role>
<role-name>rolUsuarioMonitorAB</role-name>
</security-role>
<context-param>
<param-name>contextConfigLocation</param-name>
<param-value>/WEB-INF/applicationContext.xml</param-value>
</context-param>
<listener>
<listener-class>org.springframework.web.context.ContextLoaderListener</listener-
class>
</listener>
</web-app>
```

Anexo G. Archivo weblogic.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<wls:weblogic-web-app xmlns:wls="http://xmlns.oracle.com/weblogic/weblogic-web-app" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd
http://xmlns.oracle.com/weblogic/weblogic-web-app
http://xmlns.oracle.com/weblogic/weblogic-web-app/1.4/weblogic-web-app.xsd">

    <wls:weblogic-version>12.1.1</wls:weblogic-version>
    <wls:context-root>MonitorABServidor</wls:context-root>

    <!--Bloqueseguridad -->
    <wls:security-role-assignment>
        <wls:role-name>rolUsuarioMonitorAB</wls:role-name>
        <wls:principal-name>usuariosABMonitor</wls:principal-name>
    </wls:security-role-assignment>
    <!-- Fin debloqueseguridad -->

</wls:weblogic-web-app>
```