SISTEMA DE GESTIÓN DE SERVICIOS PARA EL ICOM CENTREX IP

ORLANDO GUEVARA CORDOBA
OSCAR VIVEROS EGAS

Documento final de trabajo de grado presentado como requisito para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Director
Mag. ANDRÉS LARA SILVA

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telemática
Grupo de Ingeniería Telemática
Popayán
2010

TABLA DE CONTENIDO

FIGURAS

INTRODUCCION

El proyecto iCom Centrex IP, ejecutado por la Universidad del Cauca, brinda una plataforma para telefonía IP, basándose en una arquitectura de servicios convergentes en el marco de las Redes de Nueva Generación (NGN) y soportada con tecnologías abiertas. Este producto, diseñado para operar de forma autónoma e integrado a la infraestructura existente del operador, está compuesto de cuatro servidores que permiten desde el alojamiento de los servicios de comunicaciones de valor agregado (servidor Sailfin) hasta el almacenamiento de la información relacionada con los usuarios y los servicios (servidor Postgres), y todo lo referente al establecimiento y finalización de la comunicación y el consumo de los servicios.

Este trabajo, parte de la necesidad que se tiene del producto final iCom Centrex IP de un sistema responsable de la gestión de sus servicios, y, del estudio de los estándares existentes para la gestión de servicios en el contexto en el que se desenvuelve el centrex, es decir desde las Redes de Nueva Generación y los Servicios IMS (IP Multimedia Subsystem).

La aplicación de gestión debe ser una solución enfocada en tecnologías abiertas que permita realizar la gestión de fallas y seguridad de algunos servicios básicos del total del paquete de servicios. Además, la interacción del usuario con la aplicación de gestión debe ser cómoda y simple, ofreciendo de manera fácil el proceso de operación del sistema. Es necesario dotarla de un diseño flexible, que será determinante para su adaptación con otros productos. Por supuesto, la elección de las tecnologías repercutirá en el coste del desarrollo del sistema, siendo su crecimiento directamente proporcional al número de tecnologías propietarias seleccionadas. Por ello, es natural pensar en su creación mediante tecnologías libres Open Source.

Analizadas las necesidades y requisitos del sistema, es determinante que la aplicación sea capaz de cumplir una serie de objetivos:

Como objetivo general se pretende desarrollar un Sistema de Gestión de servicios con las funciones de fallas y seguridad para el iCom Centrex IP utilizando tecnologías abiertas de gestión.

Se debe definir un mecanismo que permita la gestión de servicios para el iCom Centrex IP y la tecnología de gestión adecuada que permita implementar el sistema de gestión de servicios. También se debe implementar un sistema que permita realizar la gestión de fallas y de seguridad de los servicios de establecimiento de llamada, transferencia de llamada, grabación de llamada, proporcionados por el iCom Centrex IP.

En este documento quedan reflejadas las diferentes etapas para la creación del sistema de gestión de servicios para el iCom Centrex IP desde el principio hasta su fin. El proceso lógico debe pasar por una descripción del sistema en el que estará integrada, un modelado del sistema que deseamos llevar a cabo, el proceso de diseño y las decisiones tomadas en el mismo; el último paso será, por supuesto, la forma de implementar dicho diseño. Deberemos tener en cuenta también, las tecnologías elegidas, y el esfuerzo realizado para su comprensión y utilización.

Así mismo, habrá una reflexión sobre el trabajo realizado, y los posibles cambios que susceptiblemente podrán ser introducidos para su mejora, o bien, para su adaptación con el sistema.

El presente documento está compuesto por cinco capítulos de la siguiente manera:

CAPÍTULO I: Describe las generalidades y fundamentos para el desarrollo de aplicaciones de gestión y estudia los diferentes modelos o arquitecturas de gestión de redes y servicios.

CAPÍTULO II: Define los conceptos de NGN e IMS con el fin de conocer el contexto en el que se desarrolla el sistema iCom Centrex IP, y realiza un estudio de dos de las tecnologías de gestión basada en web más importantes.

CAPÍTULO III: Contiene la elección de la tecnología de gestión a usar, la descripción de la solución planteada, explicando el desarrollo y la implementación del sistema de gestión del iCom Centrex IP.

CAPITULO IV: Describe las pruebas efectuadas sobre el sistema, los resultados obtenidos y los cambios efectuados al mismo.

CAPITULO V: Presenta las conclusiones, recomendaciones y trabajos futuros con relación al desarrollo del proyecto.

1 GENERALIDADES Y FUNDAMENTOS PARA EL DESARROLLO DE APLICACIONES DE GESTIÓN

1.1 GESTIÓN DE REDES Y SERVICIOS

En el campo de las telecomunicaciones, la tendencia más importante está constituida por los sistemas distribuidos y las computadoras, Los recursos informáticos están interconectados mediante medios de transmisión y protocolos de comunicaciones organizados en las conocidas arquitecturas de computadoras y que se pueden denominar sistemas de comunicaciones [1]. Estos sistemas están implementados mediante una infraestructura de equipos de comunicaciones (módems, conmutadores, multiplexores, etc.) y facilidades de transmisión, estos son los que prestan los servicios finales, que los usuarios utilizan en la actividad diaria en las empresas y organizaciones.

El tamaño y la complejidad de las redes han ido creciendo sin cesar debido en gran parte a la aparición de las redes públicas de datos y a la creciente oferta de servicios de comunicaciones de valor agregado.

Actualmente los Sistemas de Comunicaciones prestan servicios a los usuarios utilizando redes Privadas y Redes Públicas. La interconexión entre las mismas proporciona mejores posibilidades en la provisión de servicios pero complica el control de las redes [1].

Una vez se consigue configurar los sistemas de comunicación para la prestación de servicios, surge la necesidad de gestionarlos, es decir, de controlar los recursos que le componen en términos de rendimiento, capacidad, utilización, reconfiguración, diagnósticos, planificación, entre otras.

1.2 CONCEPTOS GENERALES DE GESTION

1.2.1 DEFINICIÓN DE GESTIÓN

En términos generales se puede definir la gestión como una actividad esencial, la cual asegura la coordinación de esfuerzos individuales para el logro de metas grupales. El propósito es establecer un entorno en el cual las personas puedan lograr metas de grupo con la menor cantidad de tiempo, dinero, materiales e insatisfacciones personales [2].

La gestión, como concepto, es muy importante en una gran cantidad de aspectos de la vida personal de cualquier individuo. Gestionar implica el manejo de una serie de recursos. Ejemplos de ámbitos en que la gestión es algo determinante y en los que debemos dedicar cierto tiempo a determinar mecanismos adecuados para llevarla a cabo, son muchos. Desde la forma de administrar un capital económico, hasta la gestión de los recursos humanos de una empresa; otro ejemplo es la gestión de los recursos naturales del planeta, generalmente finitos. La manera de realizar está administración de los recursos, es determinante a la hora de optimizar los beneficios que obtenemos, así como garantizar, en muchos casos, que en un futuro podamos seguir disfrutando de ellos. La

gestión, extrapolando de los ejemplos anteriores, comporta la planificación, la observación de la evolución de los recursos y su mantenimiento para las generaciones futuras.

1.2.2 LA GESTIÓN EN TELECOMUNICACIONES

En este contexto, Gestión son todas las medidas que aseguran la efectiva y eficiente operación de los recursos de un sistema de acuerdo con unas metas corporativas. La gestión es responsable de proveer, asegurar la disponibilidad y el mantenimiento de los servicios y aplicaciones [3].

En el campo tecnológico, y específicamente en el área de las telecomunicaciones, el concepto de gestión se ha podido diferenciar un poco del concepto de administración. Debido a que en el campo de las telecomunicaciones, las aplicaciones generalmente tienen como objetivo asegurar el funcionamiento apropiado de un sistema. Hoy en día con el alcance tecnológico que se tiene, se puede observar que las empresas de telecomunicaciones establece una separación entre el manejo administrativo de la misma y el manejo tecnológico de su infraestructura.

El departamento administrativo se encarga del manejo global de la empresa, es decir, las acciones relacionadas con la asignación de recursos, distribución de la inversión, asuntos de mercado, etc. Por otro lado, la parte tecnológica básicamente se ha orientado a los aspectos relacionados con:

- *Operación:* Garantizar el funcionamiento de los equipos de telecomunicaciones (recursos físicos).

- *Administración:* Verificar el funcionamiento global en términos de las interacciones y las funciones conjuntas de varios equipos de telecomunicaciones.

- *Mantenimiento:* Satisfacer los requerimientos de nivel de funcionamiento de los equipos mediante acciones de prevención y corrección de fallas.

- *Provisión:* Asegurar la oferta y la entrega de servicios de telecomunicaciones basados en la infraestructura de la empresa operadora de telecomunicaciones.

1.2.3 ¿QUÉ ES LA GESTIÓN DE REDES Y SERVICIOS?

La gestión de las redes y los servicios es una parte relevante en el entorno del negocio de las telecomunicaciones, ya que permite verificar que los servicios cumplen con los niveles de calidad establecidos por la compañía, ayuda a controlar los costos asociados a la operación de la red y da soporte al rápido y flexible despliegue de nuevos servicios.

“La gestión de red incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable”. [4]

El objetivo de la gestión de redes y servicios es mantener, el tiempo máximo posible, los sistemas de una organización en un estado óptimo de funcionamiento, minimizando la pérdida que ocasionará si existe una interrupción o un mal funcionamiento del mismo [5]. Además, busca mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos. Asimismo surge la necesidad de hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan acceder a la información que circula en ella; Finalmente hacer uso eficiente de la red y utilizar mejor los recursos, para así, aumentar el rendimiento de la misma.

1.3 ARQUITECTURAS DE GESTION

1.3.1 ARQUIETCTURA DE GESTION OSI

La Gestión de Sistemas OSI se basa en el uso de protocolos del nivel de aplicación para el intercambio de información de gestión según el paradigma Gestor-Agente [1]. La mayoría de herramientas de apoyo de gestión de red se basan en este paradigma, los sistemas de apoyo a la gestión poseen:

- Una interfaz con el operador o el responsable de la red.
- Una serie de componentes hardware y software entre los diferentes componentes de la red.

Las características de estos componentes hardware y software permiten clasificar las partes de un sistema de gestión de red en dos grupos:

- *Gestores:* Son los elementos que interaccionan con los operadores humanos, y desencadenan las acciones pertinentes para llevar a cabo las operaciones solicitadas.

- *Agentes*: Llevan a cabo las operaciones de gestión invocadas por los Gestores de la red.

Los nodos de una red que posean un gestor se denominarán *Nodos Gestores*, mientras que los nodos que tengan un agente se llamarán *Nodos Gestionados*. La base del funcionamiento de los sistemas de apoyo a la gestión reside en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Es lo que se llama *Paradigma Gestor-Agente*.

La arquitectura de gestión OSI se encuentra publicada en el conjunto de recomendaciones del Sector de Normalización de las Telecomunicaciones de la Unión Internacional de las Telecomunicaciones conocidas como Serie X.700 [6]. La arquitectura está compuesta por cuatro modelos, que son [3]:

- Modelo de comunicaciones: Define el acceso a los objetos gestionados y los protocolos de gestión.

- Modelo de información: Describe una base sintáctica y semántica para modelar y describir los recursos.

- Modelo funcional: Organiza la tarea compleja de gestión dentro de unidades gestionables y define las funciones de gestión genéricas.

- Modelo organizacional: Define los roles, modelos de cooperación y dominios de gestión.

1.3.1.1 MODELO DE INFORMACION

El modelo de información proporciona una representación de los recursos gestionados. Para esto, OSI aplica un enfoque totalmente orientado a objetos para construir su (complejo) modelo de información. Este modelo es llamado Structure of Management Information (SMI) [7] [8].

En la figura 1 se muestra el proceso de obtención de la información de gestión del entorno de red.

Figura 1. Proceso de gestión en un entorno de red

El modelo de información de gestión define un objeto gestionable como la interfaz conceptual que han de presentar los dispositivos que ofrecen funciones de gestión. El proceso de supervisión y control de un objeto gestionable se realiza mediante una serie de interacciones.

Estas interacciones son de dos tipos:

- *De operación:* el gestor solicita algún dato al objeto gestionable o desea realizar alguna acción sobre él.

- *De notificación:* cuando el objeto gestionable intenta enviar algún dato al gestor como consecuencia de algún evento ocurrido en el dispositivo.

Un objeto gestionable se caracteriza además por un conjunto de atributos que son las propiedades y/o características del objeto y un comportamiento en respuesta a las operaciones solicitadas.

La comunicación entre el gestor y el objeto gestionable no es directa, se realiza mediante un intermediario: el agente de gestión (esto se corresponde con un modelo centralizado *gestor-agente*).

La función del agente es controlar el flujo de información de gestión entre el gestor y el objeto. Este control lo realiza comprobando una serie de reglas de gestión (por ejemplo que el gestor tenga la capacidad para solicitar una determinada operación), que han de cumplirse para poder realizar la operación. Estas reglas se incluyen en los datos como parte de la solicitud de una operación. El flujo normal de información de gestión y control entre el gestor y el agente se realiza mediante el *Protocolo Común de Información de Gestión* (CMIP, *Common Management Information Protocol*), perteneciente al nivel de aplicación OSI.

Por otra parte, el modelo de información hace uso de los principios de diseño orientado a objetos. Para ello, se requiere adaptar un enfoque que permita estandarizar especificaciones de una manera modular. El enfoque elegido debe proporcionar una fácil capacidad de extensión del protocolo y de los procedimientos. También se debe permitir la reutilización de especificaciones anteriores. Finalmente, hay que tener en cuenta que el ámbito de diseño es aplicado a la especificación de información transmitida en los protocolos de gestión, no a la implantación.

1.3.1.2 MODELO FUNCIONAL

El modelo funcional describe las cinco áreas en las que tradicionalmente se ha dividido la gestión de red:

- Gestión de fallas
- Gestión de configuración
- Gestión de desempeño
- Gestión de contabilidad
- Gestión de seguridad

Mejor conocidas como FCAPS, el cual es un acrónimo de *Fault, Configuration, Accounting, Performance, Security (Falla, Configuración, Contabilidad, Desempeño, Seguridad),* aunque dentro de la arquitectura de administración OSI reciben el nombre de *Systems Management Functional Areas* (SMFAs).

Más adelante se explicaran con mayor detalle cada una de estas áreas funcionales de la gestión OSI.

1.3.1.3 MODELO DE COMUNICACIONES: CMIP

El Protocolo de Información Común de Gestión (CMIP, *Common Management Information Protocol*) ofrece un mecanismo de transporte en la forma de servicio pregunta-respuesta para capas OSI. La especificación del protocolo describe precisamente cómo se ejecutan los servicios CMIS (CMIS, *Common Management Information Services*) individuales [9].

Los Servicios de Información Común de Gestión, son un conjunto de reglas que identifican las funciones de una interfaz OSI entre aplicaciones, utilizado por cada aplicación para intercambiar información y parámetros. CMIS define la estructura de la información que es necesaria para describir el entorno.

Entre las características más importantes del protocolo CMIP se pueden destacar las siguientes:

- CMIS/CMIP requiere de gran cantidad de memoria y capacidad de CPU.
- Se generan largas cabeceras en los mensajes de los protocolos.
- Las especificaciones son difíciles de realizar y tediosas de implementar en aplicaciones.
- La comunicación con los agentes está orientada a conexión.
- La estructura de funcionamiento es distribuida.
- Permite una jerarquía de sistemas de operación.
- El protocolo asegura que los mensajes llegan a su destino.

El hecho de que se trate de una gestión conducida por eventos se traduce en que:

- El agente notifica al gestor de sucesos la información concerniente a los recursos gestionados.
- El agente es responsable de monitorizar los recursos.
- Presenta la ventaja de que existe menor gestión de tráfico.
- Presenta la desventaja de tener agentes más complejos

1.3.1.4 MODELO ORGANIZACIONAL

El modelo organizacional define los actores (elementos que participan en la administración), sus roles y las reglas de cooperación entre ellos. Los modelos de cooperación pueden ser Gestor-Agente o *peer-to-peer*. Pueden definirse dominios para agrupar recursos que serán administrados. En estos dominios se definen políticas (reglas) específicas de administración. Los dominios y las políticas son objetos administrables.

La arquitectura de gestión OSI define dos roles para los sistemas: un rol de gestor (*manager)* y otro de agente (*agent*).

En principio, los sistemas OSI pueden asumir ambos roles, incluso de forma simultánea. La asignación del rol puede cambiar dinámicamente dependiendo de los procesos de comunicación de administración individual. Los MOs (objetos administrables) son considerados activos en el sentido que ellos son autónomos para "activar" notificaciones de eventos asincrónicamente (realmente, es la implementación del MO dentro del agente quien se responsabiliza de generar los reportes de eventos; el recurso en sí mismo puede ser pasivo).

OSI provee un concepto de dominio extensible y flexible, en el cual se diferencia entre *dominio organizacional* y *dominio administrativo*.

Los *dominios organizacionales* son MOs (objetos administrables) agrupados en,

- de acuerdo a la función (por ejemplo, para gestión de seguridad, gestión de desempeño, etc.)
- dentro de un área funcional para facilitar establecer una política común.
- asignación temporal de roles, *gestor y agente*.

Los *dominios administrativos* agrupan los MOs (objetos administrables) que tienen la misma, y única, autoridad administrativa. Estos dominios se utilizan para:

- crear y manipular dominios organizacionales
- controlar el flujo de acciones entre dominios (que pueden llegar a estar traslapados)

1.3.2 AREAS FUNCIONALES DE GESTION

De acuerdo con la clasificación establecida por la Organización Internacional de Estándares **(ISO**, *International Standard Organization***)**, las Áreas Funcionales de la Gestión de Red se engloban en cinco grandes grupos: Gestión de Fallas, Gestión de la Configuración, Gestión del Desempeño, Gestión de la Contabilidad y Gestión de la Seguridad [3] [6].

1.3.2.1 GESTION DE FALLAS

La Gestión de Fallas comprende el conjunto de facilidades que permiten la detección, el aislamiento y la corrección de las operaciones anormales de las redes o sistemas de comunicaciones.

La Gestión de Fallas se encarga de:

- *La supervisión de alarmas*: indicación de fallas, su naturaleza y gravedad.
- *Localización de fallas*: rutinas para la localización.
- *Corrección de Fallas*: emitir reportes de las fallas ocurridas.

Las funciones de la Gestión de Fallas son:

- *Monitorear la red y el estado del sistema:* proceso en el cual siempre se está monitorizando la red para ver que todo este en perfecto orden.

- *Detección e informe de problemas:* este proceso, por medio de dispositivos activos y pasivos, detecta fallos e informa de los mismos a los operadores de red o a los procesos designados al efecto.

- *Determinación de problemas:* se encarga de aislar el problema en un recurso determinado, hardware, software, medio de transporte, o en una causa externa, para así poder identificar al personal específico responsable de su diagnóstico y resolución.

- *Puenteo o recuperación de problemas:* permite minimizar o eliminar el efecto del problema en la red hasta que éste pueda ser resuelto.

- *Diagnóstico y resolución de problemas:* determina la causa precisa del problema y las acciones requeridas para su resolución.

- *Seguimiento y control del problema:* conocido como "*trouble ticketing"*, proporciona los mecanismos necesarios para el seguimiento del problema desde su detección hasta su resolución.

Las siguientes posibilidades técnicas pueden asistir en el análisis de las fallas que se puedan presentar:

- Auto-determinación de componentes del sistema.
- Facilidad de rastreo (es decir, mantener registros del tráfico de mensajes de conmutación o mensajes etiquetados para el propósito de trazabilidad o reportes de compatibilidad especial).

- Tener registro de los errores que se presenten.

- Posibilidades de recuperación para el vaciado de memoria.

- Mensaje "echo" en todos los niveles de protocolo, el cual es útil para hacer comprobaciones sobre el estado de la red.

- Medidas para generar los errores a propósito en ambientes de sistema definidos.

- Posibilidades de Inicio (que también puede ser iniciado y supervisado centralmente) de auto-rutinas de prueba y la transmisión de textos de prueba a determinados puertos (prueba del bucle, prueba remota, problema de archivo) así como conexiones de pruebas tales como paquetes ICMP para ping y análisis del rastreo de la ruta de una de red conexiones.

- Alternativas de configuración para valores de umbral, provocando un reset planeado y un re arranque (dirigido para puertos específicos, grupos de puertos, y componentes).

- Disponibilidad de sistemas de prueba especiales (osciloscopio, reflectómetros de tiempo-dominio, verificar interfaces, analizador de protocolos, monitores de equipo físico para supervisión de línea).

- Apoyo de mecanismos de filtros para mensajes de fallos o alarmas y evento correlacionados para reducir el número de hechos relevantes y de análisis de las causas.

1.3.2.2 GESTIÓN DE CONFIGURACIÓN

El área funcional de la gestión de la configuración incluye al conjunto de facilidades pensadas para monitorizar y controlar la información necesaria para identificar física y lógicamente los recursos de red.

Las funciones de la Gestión de la Configuración son:

- Construcción de la topología de la red de acuerdo con la visión del usuario. Adicionar y dar de baja a dispositivos.

- Establecimiento de los parámetros de funcionamiento, es decir, inicialización y modificación de la configuración de todos los recursos de la red.

- Mantenimiento de un inventario de los dispositivos instalados y de las líneas que los conectan.

- Gestión de la correspondencia entre nombres de dispositivos y sus direcciones de red para que los usuarios manejen los recursos según su visión de la red.
- Gestión racional de los cambios de configuración.

A continuación se presentan otras funciones incluidas en la gestión de configuración:

- Definición de nuevos recursos a gestionar.
- Creación, modificación y eliminación de relaciones entre los recursos.
- Borrado de recursos gestionados.
- Obtención de informes a voluntad de la identidad, condiciones de funcionamiento, etc. de los objetos gestionados.
- Reflejo en tiempo real de los cambios significativos en los modos de operación de los recursos gestionados.

1.3.2.3 GESTIÓN DEL DESEMPEÑO

Es el conjunto de actividades requeridas para que se evalúe continuamente los principales indicadores del rendimiento de operación de la red, para verificar como se mantienen los niveles de calidad del servicio (QoS).

La Gestión del Desempeño consiste en:

- Recolección de información de la utilización actual de la red, dispositivos y enlaces.
- Analizar la información para visualizar la tendencia de utilización.
- Definir límites de utilización de la red.
- Realizar simulaciones para determinar como la red puede alcanzar un máximo rendimiento.

La Gestión del Desempeño se encarga de:

- Monitoreo del desempeño.
- Control de gerencia del desempeño: manipulación de límites y parámetros de medición del tráfico en la red.
- Análisis del desempeño: procesamiento y análisis de datos, y la observación de la calidad del servicio.

Se tienen indicadores de rendimiento como:

- *Disponibilidad*: estado de los dispositivos gestionados.

- *Tiempo de respuesta*: tiempo total, retardos en la red y en los nodos.
- *Exactitud*: calidad del enlace.
- *Grado de utilización*: mediciones dinámicas de la utilización de la red.
- *Demanda*: utilización de recursos de red por parte de dispositivos y/o aplicaciones.
- *Throughput*: mide la relación entre la utilización y la demanda de un recurso de la red.

Estos indicadores sirven para medir el desempeño de la red, se utilizan para saber el estado actual de la red de telecomunicaciones, con el fin de verificar si se está cumpliendo con los estándares de calidad del servicio establecidos.

1.3.2.4 GESTIÓN DE LA CONTABILIDAD

Es el proceso de recopilación, interpretación y reportes del coste e información de carga orientada al uso de los recursos. Proporciona las herramientas necesarias para mantener informados a los usuarios de la red sobre el grado de utilización de los recursos.

La Gestión de la Contabilidad consiste en:

- Obtener información sobre la utilización de los recursos y servicios del sistema.
- Asociar el uso de los recursos con escalas de tarificación, combinando costos.
- Definir una tarifa a los usuarios por el uso del sistema.

La Gestión de la Contabilidad se encarga de:

- *Facturación*: colección de datos, determinación de los valores contables.
- *Tarificación*: determinación de valores de los servicios utilizados.

Las funciones de la Gestión de la Contabilidad son:

- *Identificación de los componentes de costos:* Hardware; software; servicios (voz, datos, vídeo); personal que trabaja en la red; otros (utilidades, mantenimiento, seguros, impuestos, costos de instalaciones, etc.

- *Establecer políticas de recargo a usuarios:* Reflejar una realidad económica, definir el uso de indicadores que serán la base del sistema de recargo, definición clara de las relaciones y reglas.

- *Definición de procedimientos de recargos:* Los procedimientos tienen que ser definidos, desarrollados e implementados con simplicidad, exactitud, responsabilidad, deben poseer estabilidad y ser visibles.

1.3.2.5 GESTIÓN DE LA SEGURIDAD

Es un conjunto de funciones que aseguran la protección de la red y sus componentes en todo aspecto de seguridad. El punto de partida del diseño de la seguridad de un sistema es la identificación de las vulnerabilidades del mismo. Las actuales comunicaciones son vulnerables porque corren el riesgo de ser escuchadas y modificadas de forma impune.

En general una comunicación es vulnerable si existe la posibilidad de que se produzca un efecto desautorizado en la misma.

La *Política de Seguridad* establece en rasgos generales lo que está o no permitido, luego cualquier posibilidad de comportamiento no autorizado en una red es un riesgo para el sistema.

La Gestión de la Seguridad consiste en:

- Identificar información delicada.
- Identificar, proporcionar seguridad y mantener los puntos de acceso.

La Gestión de la Seguridad se encarga de:

- Autentificación: integridad o autenticidad de usuarios.
- Control de accesos: asegurar que los recursos son utilizados por usuarios autorizados.
- Privacidad: secreto o confidencialidad.

Las funciones de la Gestión de la Seguridad son:

- Análisis de riesgos: Incluyen todas las partes relevantes y vulnerables de la red.
- Evaluación de los servicios de seguridad
  - Comprobación de la autenticidad de la información.
  - Control de acceso mediante cuentas de usuario y protección de archivos y directorios.
  - Evitar el acceso no autorizado a datos.
  - Protección del análisis del flujo de tráfico.
  - Protección contra inserción, cambio y duplicación de segmentos de datos.

- Evaluación de las soluciones de gestión de seguridad

  - Encriptación de la información.
  - Utilización de claves para identificación de usuarios.
  - Control de ruteo mediante manejo de ancho de banda dinámico.

1.3.3 ARQUITECTURA DE GESTIÓN TMN

El término Red de Gestión de Telecomunicaciones (TMN, *Telecommunications Management Network*) fue introducido por el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones y está definido en la recomendación M.3010 [10]. Esta recomendación define el concepto de Red de Gestión de Telecomunicaciones (RGT), el alcance que tiene y se describen las arquitecturas funcional y de información, presentando ejemplos de las arquitecturas físicas. Además se expone un modelo de referencia funcional y se identifican conceptos para soportar la arquitectura de TMN. Posteriormente fueron incorporados varios conceptos del modelo OSI al estándar TMN. En concreto, se adoptó el *modelo gestor – agente* del modelo OSI.

TMN sigue el paradigma de la orientación a objetos de la arquitectura OSI y trabajó conjuntamente en el desarrollo del concepto de dominios de gestión. Un aspecto diferenciador de ambos modelos consiste en la introducción, en el modelo TMN, de una red separada de aquella que se gestiona, con el fin de transportar la información de gestión.

La arquitectura TMN presenta las siguientes funciones [11]:

- El intercambio de información entre la red gestionada y la red TMN.
- El intercambio de información entre redes TMN.
- La conversión de formatos de información para un intercambio consistente de información.
- La transferencia de información entre puntos de una TMN.
- El análisis de la información de gestión y la capacidad de actuar en función de ella.
- La manipulación y presentación de la información de gestión en un formato útil para el usuario de la misma.
- El control del acceso a la información de gestión por los usuarios autorizados.

Dentro de la arquitectura RGT general existen tres aspectos básicos de ésta que pueden ser considerados por separado al planificar y diseñar una RGT:

- Arquitectura funcional: describe la distribución de la funcionalidad dentro de la TMN, con el objeto de definir los bloques funcionales a partir de los cuales se construye la TMN.

- Arquitectura física: describe las interfaces y el modo en que los bloques funcionales se implementan en equipos físicos, es decir, que se encarga de definir como se implementan los bloques funcionales mediante equipamiento físico y los puntos de referencia en interfaces

- Modelo de información

El modelo de información TMN utiliza un enfoque orientado a objetos y se basa sobre el modelo de información de la gestión OSI. Según este modelo, la vista de gestión de un objeto gestionado es visible en el límite de un objeto gestionado. En este límite, la vista de gestión se describe en la figura 2.

- Atributos, que son las cualidades o características del objeto.
- Las operaciones, que se realizan sobre el objeto.
- Comportamiento, que se exhibe en respuesta a las operaciones.
- Notificaciones, que se emiten por el objeto.

Figura 2. Objeto gestionado.

Los objetos a ser gestionados en el modelo de información cuentan con *atributos* que expresan las características más importantes. Son caracterizados también por las *operaciones* que representan las acciones que pueden ejecutar, por las *notificaciones* que pueden emitir, el *comportamiento* que indica la forma en que responde el objeto cuando se ejecuta una operación y las condiciones bajo las cuales genera una notificación.

Para que los sistemas de gestión puedan trabajar en conjunto necesitan compartir o entender el medio donde están actuando, es decir tener conocimiento de cuáles son las funciones y objetos gestionados soportados, las capacidades de gestión autorizadas, las capacidades de protocolo soportadas, los ejemplares de objetos gestionados disponibles, y las relaciones de contenencia entre objetos, entre otros, al compendio de estos aspectos se le llama SMK – Conocimiento de Gestión Compartido – Shared Management Knowledge.

1.3.4 SNMP

El organismo encargado de la estandarización de la Gestión en Internet es la Fuerza de Trabajo de Ingeniería del Internet (IETF, *Internet Engineering Task Force*) En 1988, el IAB (*Internet Activities Board*) determinó la estrategia de gestión para TCP/IP (*Transfer Control Protocol/ Internet Protocol*). Esto significó el nacimiento de dos esfuerzos paralelos: la solución a corto plazo, el Protocolo Simple de Gestión de Red (SNMP*, Single Network Management Protocol*) y la solución eventual a largo plazo, el Protocolo de Información Común de Gestión sobre TCP/IP (CMOT, *CMIP Over TCP/IP*). CMOT pretendía implantar los estándares del modelo de gestión OSI en el entorno Internet (TCP/IP).

Utilizando SNMP, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red. SNMP se ha convertido, debido al enorme éxito que ha tenido desde su publicación, en el estándar de la gestión de redes. Prácticamente todo el equipamiento de redes puede ser gestionado vía SNMP.

Este protocolo ha sido definido por la IETF, en [12]. Algunas de las funciones que proporciona SNMP son:

- *Supervisión* del rendimiento de la red y su estado.
- *Control* de los parámetros de operación.
- *Obtención* de informes de fallos.
- *Análisis* de fallos.

Como se puede ver en la figura 3, el protocolo SNMP incorpora varios elementos presentes en otros estándares como el modelo gestor-agente, la existencia de una base de datos de información de gestión (MIB) o el uso de primitivas para manipular dicha información.

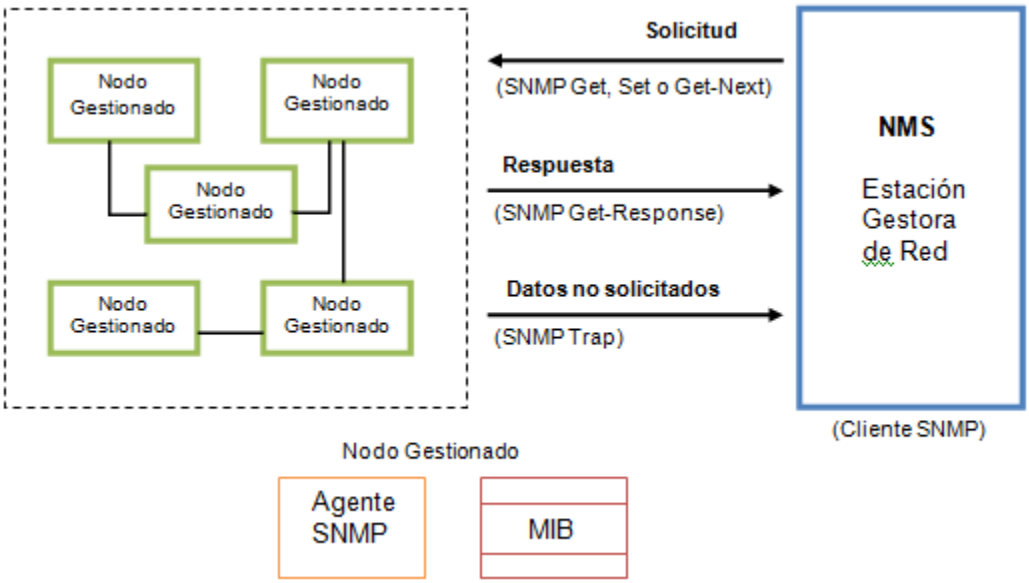

Figura 3. Protocolo SNMP

- *Agente:* equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a las peticiones sobre dichos datos (ver Fig. 4).

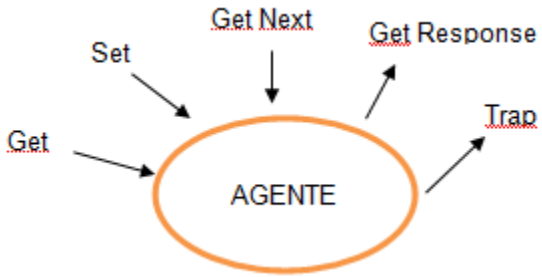

Figura 4. Primitivas SNMP.

- *Gestor:* equipamiento lógico alojado en la estación de gestión de red. Tiene la capacidad de preguntar a los agentes utilizando diferentes comandos SNMP.

- *Base de Información de Gestión (MIB, Management Information Base):* es una base de datos virtual de los objetos gestionables, accesible por un agente, que puede ser manipulada vía SNMP para realizar la gestión de red.

El protocolo SNMP realiza las funciones descritas anteriormente llevando información de gestión entre los gestores y los agentes. El protocolo SNMP es un aspecto dentro de toda la estructura de gestión, compuesta de los siguientes elementos (ver Figuras 3 y 5):

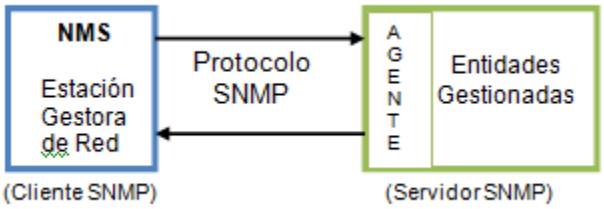

Figura 5. Modelo SNMP.

- Estación de Gestión de Red (NMS, *Network Management Station*): es el elemento central que proporciona al administrador una visión del estado de la red y unas funciones de modificación de este estado (puede ser una estación de trabajo o un ordenador personal).

- Nodos Gestionados (MN, *Managed Nodes*): son elementos como los gateways, routers, etc. Estos nodos residen en el agente gestor que es el encargado de llevar a cabo las funciones requeridas por la estación gestora.

- Protocolo de Gestión de Red (*Protocolo SNMP*): es aquel que define la comunicación entre los nodos gestionados y las estaciones gestoras.

Las limitaciones de SNMP se deben a no haber sido diseñado para realizar funciones de gestión de alto nivel. Sus capacidades lo restringen a la supervisión de redes y a la detección de errores. Como todos los elementos TCP/IP, han sido creados pensando más en su funcionalidad y dejando a un lado la seguridad.

2 GESTIÓN DE SERVICIOS DE NUEVA GENERACION Y TECNOLOGÍAS PARA EL DESARROLLO DE APLICACIONES DE GESTION WEB

El continuo avance tecnológico junto con la creciente demanda de nuevos y mejores servicios en el sector de las telecomunicaciones hace que la evolución de las redes actuales hacia Redes de Nueva Generación – NGN (New Generation Networks) – sea una necesidad imperante. Las NGN constituyen la principal infraestructura para el transporte de la información y para la conectividad de las personas.

Esta evolución implica para los operadores la innovación permanente de su oferta de servicios y redes con el fin de satisfacer las necesidades de la sociedad. La convergencia de servicios, aplicaciones y dispositivos impulsa esta tendencia, para beneficio del cliente, pues obtiene cada vez más y mejores servicios, a un costo competitivo. Las NGN son una realidad que permite avanzar hacia la consecución de estos objetivos. [13]

Paralelo a lo anterior, los nuevos servicios deben ser presentados al usuario final de una forma sencilla para que su uso sea lo más amigable posible y, de la misma forma, se debe garantizar que la información sobre el consumo de dichos servicios pueda ser manipulada por los operadores de tal forma que la gestión de los mismos no represente mayores complicaciones. Así, las aplicaciones de administración y gestión de los servicios de nueva generación asumen un papel de muchísima importancia.

2.1 REDES DE NUEVA GENERACION

Cuando se intenta dar una definición del concepto de NGN, nos encontramos con la singularidad de que no existe una única que sea válida y que abarque todos los escenarios posibles de las Redes de Nueva Generación. Sin embargo, por su validez internacional se considera la definición de la Unión Internacional de Telecomunicaciones (ITU), que sugiere una red basada en la conmutación de paquetes capaz de proporcionar nuevos servicios independiente del tipo de transporte o acceso, para ello utiliza múltiples tecnologías de banda ancha y permiten a los usuarios el acceso sin restricciones a las redes, proveedores de servicios en competencia y servicios a su elección. [14]

La migración hacia las redes NGN se constituye como elemento fundamental para lograr la convergencia de redes y servicios. Esta migración consiste en pasar de las Redes Telefónicas Públicas Conmutadas (PSTN *Public Switched Telephone Network*) basadas en voz a las redes NGN basadas en IP, y le permite a los operadores tener una mayor eficiencia en sus costos, una demanda de consumidores de mayores velocidades de transmisión, diversificar sus fuentes de ingreso, etc.

Entre muchas otras características, estas redes se basan en la conmutación de paquetes, prestan servicios independientes del tipo de transporte, utilizan múltiples tecnologías de banda ancha con calidad de servicio (QoS), soportan movilidad generalizada, etc.

2.1.1 ARQUITECTURA FUNCIONAL DE LAS NGN

Para poder implementar todos los servicios en las redes de nueva generación se requiere que la capacidad de esta red y el despliegue funcional para su aplicación se especifiquen como una arquitectura funcional, la cual debe, entre otras cosas, soportar diferentes tecnologías de acceso, brindar configuración independiente de servicio, adaptarse fácilmente al entorno distribuido y tener como principio básico una seguridad y protección mejoradas.

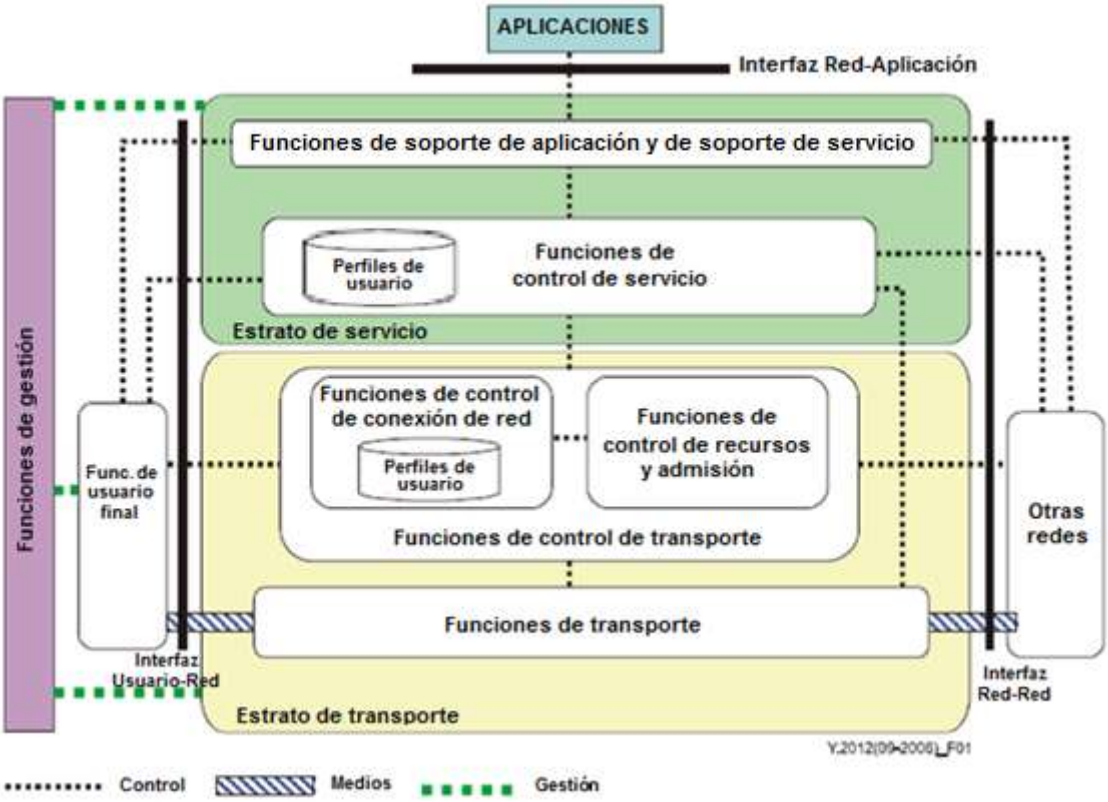

Figura 6. Visión General de la Arquitectura NGN

Conceptualmente, la arquitectura NGN se divide en dos capas. La capa de servicios, que implementa las funciones de servicios de comunicaciones y la capa de transporte para el envío/recepción de paquetes IP de extremo a extremo que garantiza la calidad del servicio (QoS) y la seguridad. Los servicios se proporcionan al usuario final a través de las funciones de soporte de servicio y de soporte de aplicación, además de las funciones de control relacionadas.

Las interfaces Aplicación-Red (*ANI, Application-Network Interface*), Red-Red (*NNI, Network-Network Interface*), y Usuario-Red (*UNI, User-Network Interface*) deben ser vistas como puntos de referencia general NGN, que pueden corresponder con interfaces físicas específicas, dependiendo de las implementaciones físicas del caso. Estas interfaces proporcionan un canal para las interacciones e intercambios entre los elementos NGN y las aplicaciones, redes y usuarios.

2.1.1.1 FUNCIONES DEL ESTRATO DE TRANSPORTE

Las funciones del estrato de transporte incluyen las funciones de transporte y de control de transporte, las cuales proporcionan tanto la conectividad a todos los componentes y funciones que están físicamente separados dentro de las NGN, facilitando así la transferencia de información de medios, de control y de gestión, como el control de recursos y admisión, y el control de la conexión a la red.

Las funciones de control de transporte contienen perfiles de usuario que representan tanto la información de control de conexión de red como la de usuario y se muestran como base de datos funcional. [15]

2.1.1.2 FUNCIONES DEL ESTRATO DE SERVICIO

Las funciones del estrato de servicio incluyen las funciones de control de servicio y las de soporte de aplicación y de servicio. Las primeras proporcionan control de recursos, además del registro, autorización y autenticación en el nivel de servicio. Al igual que en el numeral anterior, las funciones de control de servicio contienen perfiles de usuario que representan tanto la información de usuario como la de control de servicio en una sola función en forma de base de datos funcional.

Las funciones de soporte de aplicación y de soporte de servicio incluyen funciones como las de pasarela, registro, autorización y autenticación en el nivel de aplicación. Estas funciones colaboran con las de control de servicio con el objetivo de prestar los servicios NGN que solicitan los usuarios finales y las aplicaciones. [15]

2.1.1.3 FUNCIONES DEL USUARIO FINAL

A la red de acceso NGN pueden conectarse usuarios finales a través de diversas interfaces o redes, y los equipos de estos usuarios pueden ser tanto móviles como fijos. Se debe tener en cuenta que por usuarios finales o extremos no se entiende aplicaciones que utilizan los servicios NGN.

2.1.1.4 FUNCIONES DE GESTIÓN

La gestión de NGN (*NGN Management - NGNM*) consiste en funciones que gestionan los recursos y los servicios de redes de próxima generación; permite la comunicación entre el plano de gestión y los recursos o servicios de NGN, por una parte, y la comunicación con otros planos de gestión por otra parte, para lo cual se define una arquitectura predeterminada con interfaces normalizadas, que incluye protocolos y mensajes.

Estas funciones dan la posibilidad de realizar dicha gestión con buenos niveles de calidad, fiabilidad y seguridad. Las funciones de gestión son aplicadas en los estratos de servicio y de transporte de las NGN, para cada uno de las cuales se encarga de la gestión de las FCAPS expuestas en el Capítulo I. Se prevé así que la gestión de los dos estratos de la NGN sea similar en lo que respecta al comportamiento de los objetos gestionados, por ejemplo la configuración de los recursos de servicio con respecto a la configuración de los recursos de transporte. [16]

2.1.2 PRINCIPIOS PARA LA GESTIÓN DE NGN

La gestión de NGN plantea un cambio de mentalidad con respecto a la infraestructura ofrecida por el Sistema de Soporte a la Operación (OSS), que se basa en una mezcla de SNMP, CMIP y CORBA y de "islas" de gestión específicas con servicios separados, así como recursos y modelos de información diferentes, a un sistema unificado para gestionar tanto las múltiples redes de acceso como una amplia gama de servicios personalizados. [17]

La colaboración entre distintas organizaciones que tienen experiencia en el campo de la gestión y en la elaboración de especificaciones aplicables a las NGN, posibilitó la creación de una Hoja de Ruta de Gestión para las NGN (*The NGN Management Specification Roadmap*), en el que se define algunas características fundamentales y específicas de la gestión de NGN, como lo son:

- Uso de conceptos y tecnologías de implementación soportadas por las industrias dedicadas a la informática.

- Arquitecturas capaces de soportar gestión distribuida y que sean independientes de la tecnología de comunicaciones que se use.

- Modelos de información interoperables y basados en ambientes multiprotocolo.

La gestión de NGN permite supervisar y controlar los servicios de NGN, así como los recursos de servicios y de transporte, mediante la comunicación de información de gestión a través de interfaces entre recursos de NGN y sistemas de gestión, entre los sistemas de gestión que soportan las NGN, y entre los componentes de NGN y los representantes de proveedores de servicios y operadores de redes

Por otro lado, la NGNM permite el acceso de los usuarios finales a la información de gestión y la presentación de esta información, así como la realización de procesos empresariales iniciados por el usuario final.

De esta forma, los procedimientos de gestión se hacen necesarios para una mayor satisfacción de los clientes y para reducir considerablemente los costos de explotación gracias a la utilización de nuevas tecnologías, nuevos modelos de empresa y nuevos métodos de explotación.

2.1.3 ARQUITECTURA DE GESTION DE NGN

Como se ha podido comprobar anteriormente, en las NGN se da la convergencia de dos mundos, el de las operadoras de telecomunicaciones y el mundo de Internet, lo que complica la gestión de este tipo de redes y hace insuficiente la gestión utilizada en las redes actuales. La gestión de un ambiente de telecomunicaciones NGN se constituye como una aplicación de procesamiento de información, la cual debe interactuar con funciones e información implementada en múltiples entidades proveedoras y consumidoras, por lo que esta gestión debe ser distribuida.

Así, la arquitectura de gestión de NGN se dividirá en cuatro representaciones de arquitecturas diferentes, las cuales constituyen un punto de vista diferente sobre la

gestión y sobre la misma arquitectura final, e incluye también el criterio de seguridad. En la práctica se realiza un proceso iterativo para permitir la evolución necesaria de todos los aspectos de la arquitectura. Estas representaciones se pueden observar en la figura 7. [18]

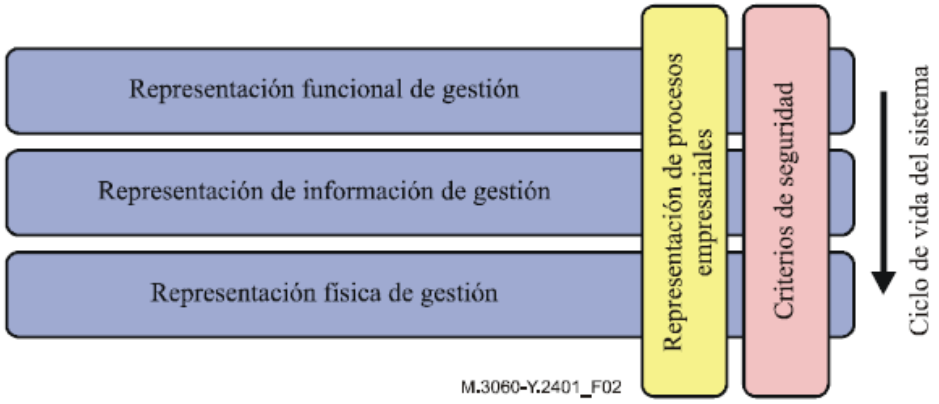

Figura 7. Arquitectura de Gestión de las NGN.

- *Representación de procesos empresariales*: en la arquitectura de NGNM se utiliza el modelo eTOM, que es un marco de referencia para clasificar las actividades empresariales de un prestador de servicios.

- La *representación funcional de gestión* es el componente elemental de un proceso empresarial (o servicio de gestión) desde el punto de vista del usuario del proceso (o del servicio), y se constituye en la base para especificar las funciones que se han de ejecutar en el sistema de gestión.

- La *representación de la información de gestión* establece la información de gestión necesaria en la comunicación entre las entidades de la representación funcional, para poder ejecutar las funciones en el sistema de gestión.

- La *representación física de gestión* describe las distintas formas de ejecutar las funciones de gestión. Se pueden hacer efectivas en varias configuraciones físicas y utilizando varios protocolos de gestión.

- El campo de la seguridad es muy amplio y la finalidad es proteger activos importantes de las empresas contra distintas amenazas.

2.2 SUBSISTEMA IP MULTIMEDIA

IMS (*IP Multimedia Subsystem*) es un sistema estándar que define una arquitectura genérica para ofrecer servicios multimedia sobre la infraestructura IP. El ofrecimiento de estos servicios se posibilita gracias a la flexibilidad del Protocolo de Iniciación de Sesiones (*SIP, Session Initiation Protocol*), que se encarga de la gestión de sesiones multimedia en Internet. SIP aporta las funciones para el registro, establecimiento, modificación y finalización de las sesiones IMS entre diferentes dispositivos. Dado que no todos los

dispositivos pueden soportar los mismos servicios se debe, al momento de establecer las sesiones, negociar las características de dichos servicios, de lo cual se encarga el Protocolo de Descripción de Sesiones (*SDP, Session Description Protocol*). Mediante SDP los extremos de una sesión pueden definir el tipo de sesión a mantener y sus capacidades multimedia. [19]

Esta arquitectura es capaz de soportar múltiples servidores de aplicación, proporcionando así tanto servicios de telefonía tradicional como servicios no telefónicos, tales como mensajería instantánea, streaming de video, mensajería multimedia, etc.

2.2.1 ARQUITECTURA IMS

Desde el punto de vista de la infraestructura, IMS define una clara separación entre las capas de transporte, control y aplicación. IMS adopta el concepto de arquitectura por capas y lo extiende definiendo una arquitectura horizontal en la que los servicios y las capacidades pueden ser reutilizados por múltiples aplicaciones.

Como puede verse en la Figura 8, en la arquitectura de servicios IMS pueden identificarse tres capas: transporte, control y aplicaciones. [20] [21]

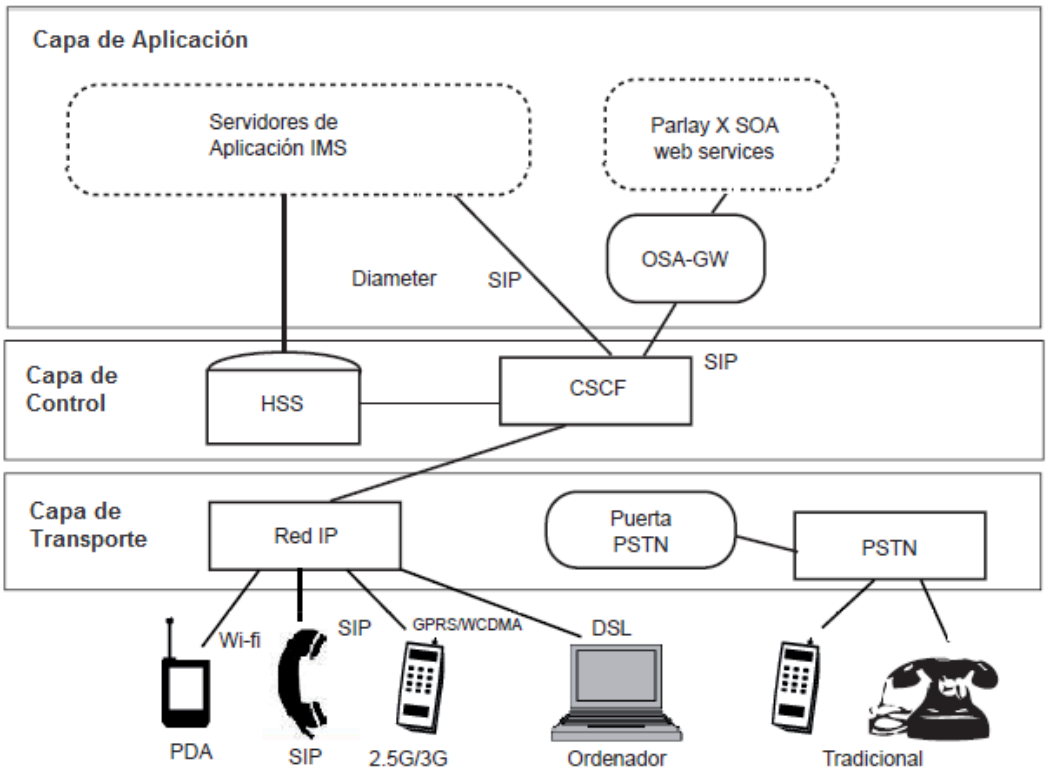

Figura 8. Arquitectura IMS

2.2.1.1 CAPA DE APLICACIÓN

Se compone de servidores o entidades SIP que alojan y ejecutan servicios (*AS Application Servers*) y permite el control de los mismos a través del protocolo SIP. Esta capa provee una infraestructura para la provisión y gestión de servicios, y define interfaces estándar y funcionalidades comunes.

Existen tres tipos de Servidor de Aplicaciones, SIP AS (*SIP Application Server*) que almacena y ejecuta servicios multimedia IP basados en SIP, IM-SSF (*IP Multimedia Servicie Switching Function*) que permite reutilizar servicios que fueron desarrollados para la red GSM, y OSA-SCS (*Open Service Access-Service Capability Server*) que proporciona una interfaz al servidor de aplicaciones del framework de OSA.

2.2.1.2 CAPA DE CONTROL

Consiste de controladores de sesión responsables del enrutamiento de la señalización entre los usuarios y de la invocación de los servicios. Aquí nos encontramos con el núcleo IMS (*IMS Core*), que contiene tanto las bases de datos con toda la información de subscripción del usuario (localización, seguridad, perfil de usuario, etc.) conocidas como HSS (*Home Subscriber* Server), como los CSCF (*Call Session Control Function*) que son servidores SIP que se encargan principalmente de enrutar el tráfico SIP entre las entidades que conforman la arquitectura IMS. Existen tres tipos de CSCF:

- P-CSCF o Proxy-CSCF: es el primer punto de contacto de los usuarios con IMS. Toda la señalización SIP generada por un terminal IMS o destinada a él atraviesa el P-CSCF. Incluye diversas funciones, algunas de ellas relacionadas con la seguridad.

- I-CSCF o Interrogating-CSCF: está situado al borde del dominio administrativo. Si un servidor SIP desea averiguar cuál es el siguiente salto para un determinado mensaje, dicho servidor obtiene la dirección del I-CSCF del dominio de destino, el cual devuelve la información de localización del usuario y encamina las peticiones SIP al destino adecuado.

- S-CSCF o Serving-CSCF: es el nodo central de la señalización SIP. Además de las funcionalidades típicas de un servidor SIP también realiza el registro SIP, es decir que mantiene una relación entre la localización del usuario y su dirección SIP. Las operaciones realizadas por el S-CSCF son controladas por las políticas establecidas en el HSS.

2.2.1.3 CAPA DE TRANSPORTE

Es responsable de la inicialización y terminación de las sesiones SIP y se encarga de la conversión de la voz de un formato analógico a otro digital para formar paquetes IP usando el Protocolo de Tiempo Real (*RTP Real Time Protocol*). En esta capa se ubican las diferentes redes de acceso de diversos operadores de telecomunicaciones. Todas las capacidades de procesamiento se encuentran en esta capa, en especial los dispositivos encargados de la conversión de medios y de la señalización entre redes.

Adicionalmente, la capa de transporte permite a los dispositivos IMS hacer y recibir llamadas hacia o desde una red PSTN u otras redes conmutadas mediante un Gateway PSTN.

2.3 ARQUITECTURAS DE GESTION BASADAS EN WEB

La gestión basada en Web trata de aplicar las características que han permitido a la interfaz Web convertirse en paradigma de interfaz de usuario a herramientas de gestión de red. De esta manera, se presentan diferentes propuestas que permiten visualizar varias opciones para poder realizar dicha gestión a partir del uso de distintas tecnologías.

2.3.1 JMX – EXTENSIONES DE GESTION DE JAVA

Las extensiones de Gestión de Java (JMX *Java Management* eXtensions) no es realmente una arquitectura de gestión, sino de instrumentación de la gestión. De hecho, es un conjunto de librerías Java que posibilitan la construcción de aplicaciones de una manera más sencilla, sin importar el protocolo de intercambio de información. Sin embargo, a partir de este conjunto de bibliotecas se podría diseñar una arquitectura, no sólo de instrumentación, sino de gestión integrada. [22]

La tecnología JMX define una arquitectura, patrones de diseño, Interfaces de Programación de Aplicaciones (API *Application Programming Interface*) y los servicios para el monitoreo y la gestión de redes y aplicaciones basados en el lenguaje de programación Java. Además de dar soporte tanto a algunos protocolos de gestión existentes tales como SNMP y WBEM/CIM., otros, como CMIP, están en proceso de desarrollo; y a otro tipo de tecnologías de comunicación como http, https, rmi y próximamente Web Services. [23]

De esta forma, JMX se integra con soluciones de gestión existentes y tecnologías emergentes. Haciendo que sus Interfaces de Programación de Aplicación (*API*) sean interfaces abiertas que cualquier vendedor de sistemas de gestión puede implementar., y en donde las soluciones planteadas puedan utilizar servicios y protocolos de búsqueda y descubrimiento tales como la tecnología de red Jini y el Protocolo de Localización del Servicio, SLP (Service Location Protocol).

Como se puede ver en la Figura 9. La arquitectura JMX define tres niveles de abajo hacia arriba.

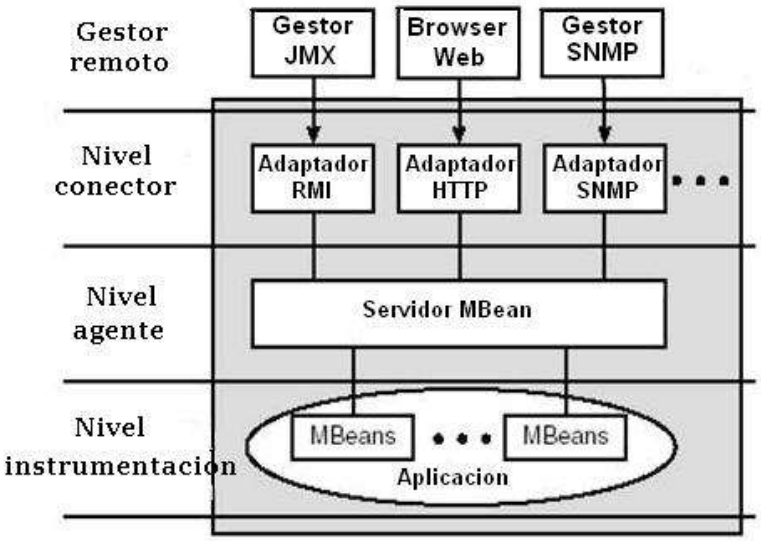

Figura 9. Arquitectura JMX

2.3.1.1 NIVEL DE INSTRUMENTACIÓN

Para gestionar recursos utilizando la tecnología JMX, primero se debe instrumentar los recursos en el lenguaje de programación Java. Esta instrumentación es posible hacer gracias a los componentes de gestión llamados MBeans, los cuales, además de seguir los patrones de diseño y las interfaces definidas en JMX, son desarrollados según las necesidades específicas para cada aplicación.

Un MBean, que no es más que un objeto java gestionado, puede representar un dispositivo, una aplicación o cualquier recurso que necesite ser gestionado, y están diseñados para ser flexibles, simples y fácil de implementar. Estos exponen una interfaz de gestión: un conjunto de atributos leíbles y/o escribibles y un conjunto de operaciones invocables, junto con una auto-descripción. La interfaz de gestión no cambia a través de la vida de una instancia de un MBean. JMX define 5 tipos diferentes de MBeans, que serán utilizados de acuerdo a las necesidades de gestión:

- MBean Estándar: Representa la forma más sencilla de instrumentar un recurso, y realiza una definición estática de la interfaz.

- MBean Dinámico: Implementa una interfaz Java específica y revela sus atributos y operaciones en tiempo de ejecución.

- MBean de Modelo: Dinámico, genérico y configurable. Realiza la instrumentación de recursos en tiempo de ejecución

- MBean Abierto: Realiza el descubrimiento de recursos en ejecución

- MXBean: Referencia solamente tipos de datos predefinido, y son utilizables por cualquier cliente. Tienen una mayor estandarización al acceso.

Para el desarrollo de estos objetos gestionados no se requiere un conocimiento previo acerca del agente JMX con el cual operará. Así, una vez un recurso que ha sido instrumentado por MBeans, puede ser gestionado por un agente JMX.

Dado que en este nivel se hace posible que los recursos sean gestionables, la instrumentación se convierte en el nivel de mayor importancia para los desarrolladores Java. En el nivel de instrumentación se debe entonces definir tanto la estrategia que será usada para realizar la implementación de los recursos de aplicación, como los mismos recursos de aplicación, que pueden ser una conexión, un pool de conexiones, una impresora conectada a una red, etc.

2.3.1.2 NIVEL DE AGENTE

Proporciona una interfaz para el manejo de los componentes del nivel de instrumentación, y provee una especificación para la implementación de agentes de gestión estándar, o agentes JMX, que controlan directamente los recursos y los hacen disponibles para las aplicaciones de gestión remota.

Los agentes JMX consisten de un servidor MBean, que es un objeto Java que actúa como registro para los MBeans, de un conjunto de servicios (temporizador, monitoreo, carga dinámica de MBeans y servicios de relación) para la manipulación de los MBeans, y de al menos un adaptador o conector de comunicaciones para permitir el acceso por una aplicación de gestión. El agente no requiere un conocimiento previo de los recursos que son expuestos o de la aplicación de gestión que usa los MBeans.

Para separar la interacción entre un agente y la instancia del MBean, JMX introduce el concepto de un *nombre de objeto*, el cual permite identificar a un único MBean dentro del Servidor y es usado también para permitir la comunicación entre el agente y el recurso gestionado.

2.3.1.3 NIVEL DE GESTION O ADAPTACIÓN

Para que la instrumentación de JMX sea posible, este nivel permite el acceso a dicha instrumentación a través de protocolos de gestión existentes o protocolos propietarios. Para hacer a un agente JMX accesible, el servidor MBean de la capa de agente, confía en los adaptadores y conectores de protocolo.

Un conector JMX consiste de un cliente y un servidor, que, respectivamente, son responsables de establecer una conexión y escuchar requerimientos de conexión. Los conectores son destinados a cumplir con los objetivos de ocultar los detalles específicos sobre la ubicación de red de los recursos en una aplicación de gestión, y de presentar una visión coherente (a través de una interfaz) de un servidor de MBean que se encuentra en un espacio de proceso diferente que el servidor de MBean locales.

En un adaptador, a diferencia del conector, no tiene un componente cliente. El adaptador se ejecuta del lado del servidor y reenvía el estado del Servidor MBean de forma tal que pueda ser reorganizada por el cliente. Cada adaptador proporciona una vista de los agentes JMX mediante un protocolo específico, es decir, dependiendo el tipo de gestor

que va a acceder a los agentes JMX (gestor SNMP, aplicaciones Java, Web) se tiene un adaptador de protocolo (SNMP, JMX, HTTP).

La API JMX define un protocolo de conexión estándar basado en la Invocación de Métodos Remotos (RMI *Remote Method Invocation*). Este protocolo permite conectar un cliente JMX a un MBean en un servidor de MBeans desde una localidad remota y ejecutar operaciones en el MBean, exactamente como si las operaciones se estuvieran ejecutando localmente.

2.3.2 WBEM – GESTION DE EMPRESA BASADA EN WEB

La Gestión de Empresa Basada en Web (WBEM *Web Based Enterprise Management*) es un estándar del DMTF (*Distributed Management Task* Force) que define un conjunto de tecnologías estándar de gestión e Internet desarrolladas para unificar la gestión de los ambientes computacionales de empresa. WBEM se puede aplicar casi en cualquier área de gestión de redes y ha recibido el respaldo de la mayor parte de la industria computacional. El objetivo de WBEM se resume en proporcionar la habilidad de gestión de todos los sistemas independientemente de la instrumentación. [24]

El DMTF ha desarrollado un conjunto núcleo de estándares que componen a WBEM, el cual incluye un modelo de datos, CIM (*Common Information Model*), que proporciona un formato, un lenguaje y una metodología comunes para colectar y describir datos de gestión; una especificación de codificación, xmlCIM (*eXtensible Markup Language for CIM*), que define los elementos XML que se pueden utilizar para representar clases e instancias CIM; y un mecanismo de transporte, Operaciones CIM sobre HTTP, que define un mapeo de operaciones CIM sobre HTTP que permite a las implementaciones WBEM interoperar de manera abierta y estandarizada.

Como se puede ver en la Figura 10, la arquitectura de WBEM contiene tres componentes principales: CIMOM, los proveedores WBEM y los clientes WBEM.

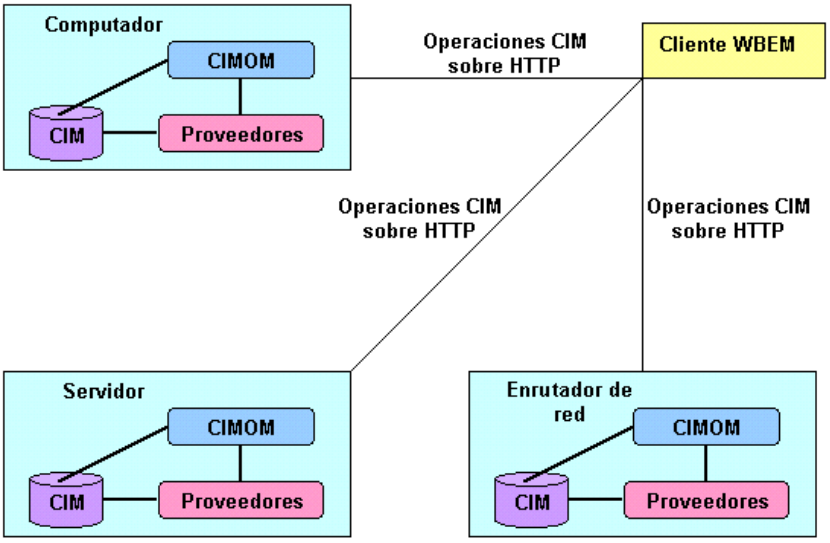

Figura 10. Arquitectura WBEM

2.3.2.1 INFRAESTRUCTURA DE GESTIÓN – CIMOM

CIMOM (*CIM Object Manager*) proporciona a las aplicaciones acceso uniforme a los datos de gestión y un área de almacenamiento central para los datos de gestión (repositorio). Se considera a CIMOM como la parte central de WBEM, y es el responsable de llamar tanto a los proveedores correctos en respuesta a los requerimientos del cliente como a los clientes correctos cuando un evento ocurre.

2.3.2.2 PROVEEDORES WBEM

Puede considerarse a los proveedores WBEM como la interfaz entre los recursos gestionados y el CIMOM. Estos proporcionan al CIMOM los datos del objeto, manejando los requerimientos de las aplicaciones de gestión.

Normalmente los proveedores WBEM se encuentran en el mismo computador en el que está el CIMOM, por lo que no hay una interfaz estándar entre estos dos componentes.

2.3.2.3 CLIENTES WBEM

Puede considerarse a los clientes WBEM como la interfaz entre el gestor y el CIMOM. Lo que garantiza la compatibilidad entre cualquier CIMOM y cualquier cliente WBEM es el uso de las operaciones CIM sobre HTTP.

3 IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN PARA EL SISTEMA ICOM CENTREX IP

3.1 ELECCION DE LA TECNOLOGIA PARA LA GESTIÓN DE LOS SERVICIOS DEL ICOM CENTREX IP

A continuación se presentan algunas consideraciones que se tomarán en cuenta para la definición de la tecnología más apropiada para la gestión de los servicios del sistema iCom Centrex IP:

1. Los servicios del iCom Centrex IP fueron desarrollados principalmente con el lenguaje de programación Java.

2. El sistema iCom Centrex IP fue desarrollado completamente con tecnologías de licencia abierta, por lo que es necesario que el sistema de gestión siga este enfoque.

3. El sistema de gestión desarrollado debe ser independiente del sistema operativo de los equipos donde este alojado.

4. El sistema de gestión debe permitir que la información de gestión esté disponible a cualquier gestor, independiente del equipo, del Browser, de la herramienta de gestión, etc. Teniendo como particularidad las cuestiones de seguridad que serían definidas por las partes.

5. El sistema de gestión debe permitir, a futuro, poder integrar todos los servicios del sistema iCom Centrex IP.

6. El sistema de gestión debe, a futuro, poder brindar todas las áreas funcionales de gestión definidas en las FCAPS.

7. La aplicación de gestión debe ser amigable e intuitiva para el usuario.

8. Ya que la gestión vía Web se ha convertido en un paradigma de interfaz de usuario, la aplicación de gestión deberá poder operar sin contratiempos con protocolos como HTTP, FTP, IGMP, entre otros.

9. El sistema de gestión deberá tener unas características tales que pueda permitirse una fácil y libre distribución del producto final.

Además, para que la tecnología de gestión elegida sea la más apropiada para el desarrollo de este proyecto, se debe tener en cuenta ciertas características de la misma, de las cuales se resaltan:

- El sistema de gestión deberá definir una arquitectura dinámica y escalable, lo que requiere que la tecnología de gestión tenga similares características.

- La tecnología elegida debe permitir que la implementación de las diferentes áreas funcionales de gestión (FCAPS), no represente un cambio significativo en el diseño del sistema actual.

- Se debe garantizar que la aplicación aquí desarrollada pueda interoperar con diferentes aplicaciones de gestión y monitoreo existentes.

- La tecnología debe permitir que la aplicación cliente del sistema de gestión no deba necesariamente estar supeditada al uso y conocimiento de dicha tecnología, sino poder utilizar diferentes estándares de programación.

- Las funciones definidas en la tecnología de gestión no deberán ser las únicas que puedan ser implementadas tanto en el presente desarrollo como en otros futuros, es decir que se debe poder utilizar funcionalidades definidas en diversas tecnologías (no necesariamente de gestión).

- Se deberá poder usar múltiples protocolos no solo en la parte correspondiente a la interfaz web sino en todos los niveles que se definan en el sistema de gestión.

Teniendo en cuenta lo anterior, los documentos de diseño, análisis y arquitectura del iCom Centrex IP, y tomando como referencia también el estudio desarrollado sobre diferentes arquitecturas de gestión, se concluye que JMX es la tecnología que más se ajusta a las necesidades del presente proyecto y representa una herramienta adecuada para el desarrollo de aplicaciones de gestión.

A todo lo anterior se le debe agregar que, una característica importante para la definición de JMX como la tecnología de gestión, es que esta utiliza y extiende el concepto de JavaBeans, concepto con el cual el equipo de desarrollo del presente proyecto ya ha estado familiarizado en el desarrollo de diversas aplicaciones. Esto implica que, además de las facilidades que otorga la tecnología en sí misma, existe la facilidad adicional de haber conocido y utilizado, en desarrollos anteriores, aspectos fundamentales de la misma.

3.2 ESQUEMA GENERAL DEL SISTEMA

El producto iCom Centrex IP es una plataforma para telefonía IP alojada, que opera sobre una infraestructura IMS, soportada completamente con tecnologías abiertas. Un sistema Centrex, ofrece un servicio de comunicaciones dirigido a empresas, alojado en la infraestructura del proveedor, quien es el dueño de la plataforma y la administra. El servicio no está en las instalaciones del suscriptor, y en términos de uso, los recursos de la plataforma son multi-arrendatarios. El proveedor suministra el servicio de mantenimiento, operación diaria, y soporte del software usado por el cliente.

En la figura 11 se presenta el diagrama general del sistema detallando los componentes utilizados para el desarrollo del proyecto.

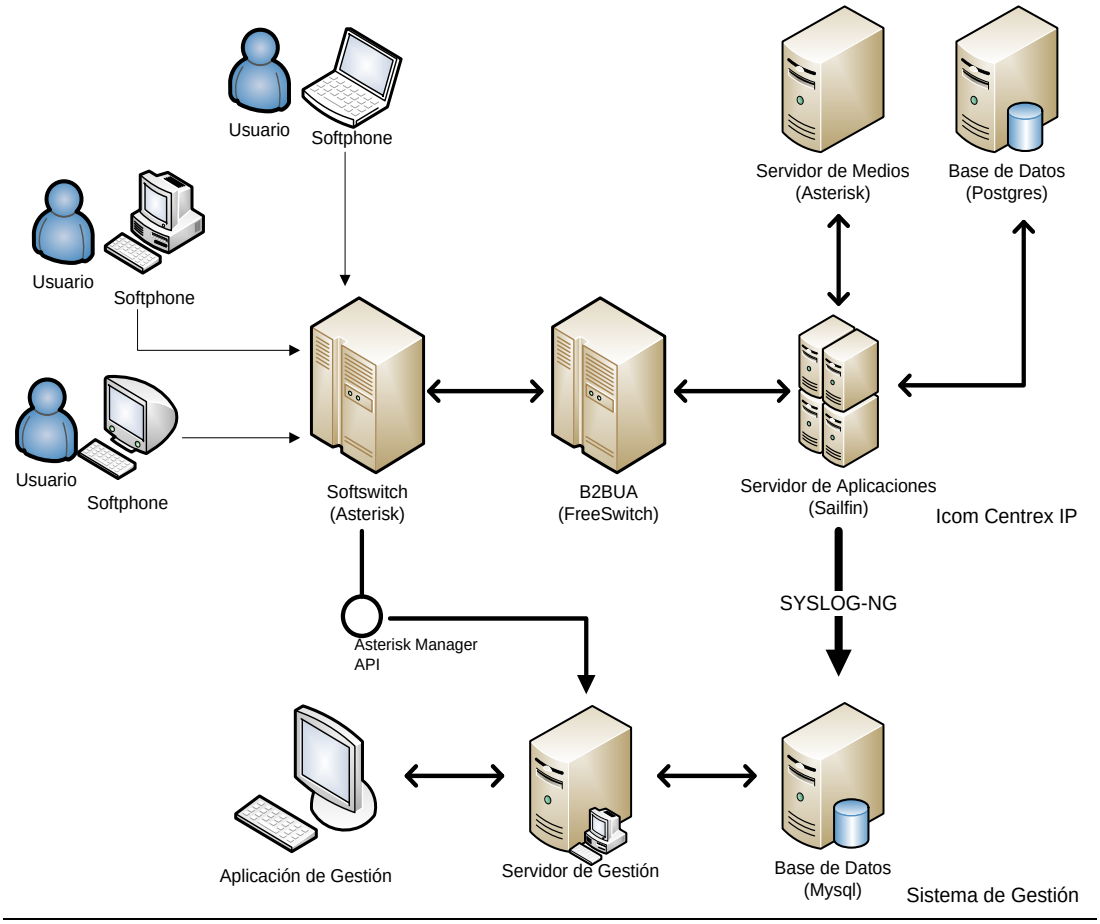

Figura 11. Esquema general del Sistema.

Como se puede observar en la figura 11, el mecanismo que permite la gestión de los servicios del sistema Icom Centrex IP inicia con la recolección de información relevante a la gestión por las interfaces “Asterisk Manager API” y por “Syslog-NG”, la cual es almacenada en el servidor de bases de datos de MySQL para despúes ser procesada y manipulada por el servidor de Gestión. Finalmente, es la Aplicación de Gestión la que permite la visualización de dicha información de una forma sencilla.

3.2.1 SISTEMA ICOM CENTREX IP

Los componentes que conforman el Sistema iCom Centrex IP son:

- **Softphone:** Es un software que hace una simulación de teléfono convencional por computadora. Estos componentes representan los suscriptores que van hacer uso del sistema final.

- **Softswitch:** Es un dispositivo encargado de proporcionar el control de llamada (señalización), procesamiento de llamadas, y otros servicios, en el ambiente de

desarrollo se simulo con un servidor asterisk el cual ofrece las funcionalidades para el registro de suscriptores y la conmutación de las llamadas [25].

- **Back to Back User Agent B2BUA (FreeSwitch):** Es el elemento utilizado para crear una troncal SIP hacia la infraestructura del operador, esta hace las veces de punto de entrada, tanto para la señalización como para el flujo multimedia.

  Entre sus funciones se encuentran la detección de tonos para dar soporte al servicio de transferencia de llamada, realizar la captura de llamada y llevar a cabo la grabación de las llamadas [25].

- **Servidor de Aplicaciones (sailfin)**: Es un elemento acorde a la especificación JavaEE que integra un contenedor de SIP Servlets. Este elemento aloja los servicios de comunicaciones implementados con máquinas de estados.

  Entre los servicios de comunicaciones desplegados en este elemento se encuentran: llamada, desvío de llamada, retorno de llamada, difusión de mensajes y click to dial [25].

- **Servidor de Medios (asterisk):** Es el elemento utilizado para almacenar y reproducir contenido multimedia. Entre sus funciones se encuentra dar soporte a servicios como correo de voz, IVR, ACD y el Fax To email. Para su implantación se utilizó Asterisk 1.4.25.1 [25].

- **Base de Datos (Postgres):** Es el repositorio de la información de configuración de los servicios del CENTREX, las PBX virtuales, grupos y usuarios, también aloja la configuración del servidor de medios Asterisk. Para su implantación se utiliza Postgresql V8.4 [25].

3.2.2 SISTEMA DE GESTIÓN

Los elementos del Sistema de Gestión que hacen parte de la solución son:

- **Syslog-NG:** Syslog permite a los administradores obtener información de registro en sus sistemas de manera uniforme para toda la red. Realizando la tarea de guardar, analizar y procesar los archivos de registro fácilmente, pero lo que la gente espera de los registros del sistema ha cambiado en los últimos años y el servicio Syslog tradicional simplemente no lo puede ofrecer. Syslog-NG (Syslog de próxima generación) [26] cubre esta necesidad.

  La aplicación de syslog-NG soporta UDP y TCP, permite aplicar filtros dependiendo a las necesidades que surjan, clasificar de acuerdo a distintos orígenes y enviar a diferentes destinos los logs que se generen. Partiendo de este concepto, syslog-NG se utiliza para recolectar toda la información que se genera en el iCom Centrex IP, registrada en los logs del servidor de aplicaciones (sailfin), y a su vez se almacena en una base de datos mysql que se crea con el fin de agilizar el manejo de ésta información y poder realizar la gestión de manera más eficaz.

- **Base de Datos (Mysql):** Contiene la información recolectada por syslog-NG y se actualiza en tiempo real a medida de que se genere nueva información en el sistema. En esta base de datos queda almacenado cualquier falla que se presente en el sistema y podrá ser consultada desde la aplicación de gestión en el momento que se desee. Para una mayor agilidad y control de la información para gestión de fallas, en el presente proyecto se definieron tablas complementarias a las elaboradas por syslog-NG.

- **Servidor de Gestión:** Es donde se encuentra toda la lógica para realizar la gestión de los servicios del iCom Centrex IP, de forma permanente está consultando la base de datos (Mysql) en busca de nuevas alertas que se han presentado en el sistema iCom Centrex IP con el fin de brindar una solución rápida y eficaz del problema. Teniendo en cuenta la elección de la tecnología de gestión, el servidor presenta una arquitectura como la definida en JMX. En la figura 14 se puede observar al Servidor constituido por las capas de Agente, Instrumentación y Acceso a datos.

- **Aplicación de Gestión:** Es la interfaz grafica de donde se tiene acceso a todo el sistema de gestión del iCom Centrex IP, brinda estadísticas de las fallas que se han generado a través del tiempo, maneja los perfiles de usuario de acuerdo al nivel de seguridad que se tenga.

  En la figura 12, se puede observar a la Aplicación como la capa del Gestor, la cual utiliza el framwork ZK, que se utiliza para el desarrollo de aplicaciones web, y es realizado completamente en Java de código abierto, permitiendo una completa interfaz de usuario para aplicaciones web con poca programación, y separando casi de forma completa la lógica del negocio de la lógica de la interfaz.

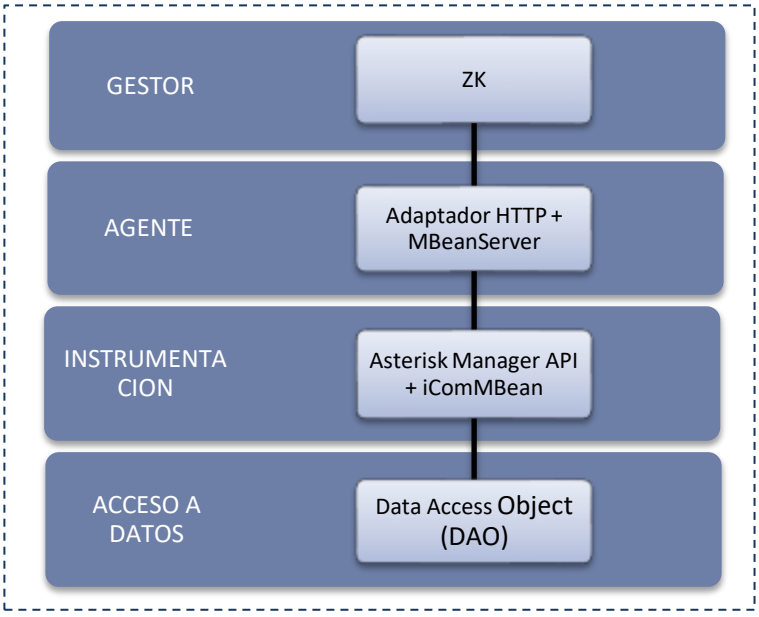

Figura 12. Arquitectura de JMX aplicada al Sistema de Gestión.

3.3 ARQUITECTURA DEL SISTEMA DE GESTIÓN.

En la figura 13 se presentan los modelos de la arquitectura de gestión que se utilizaron para el desarrollo del sistema de gestión.

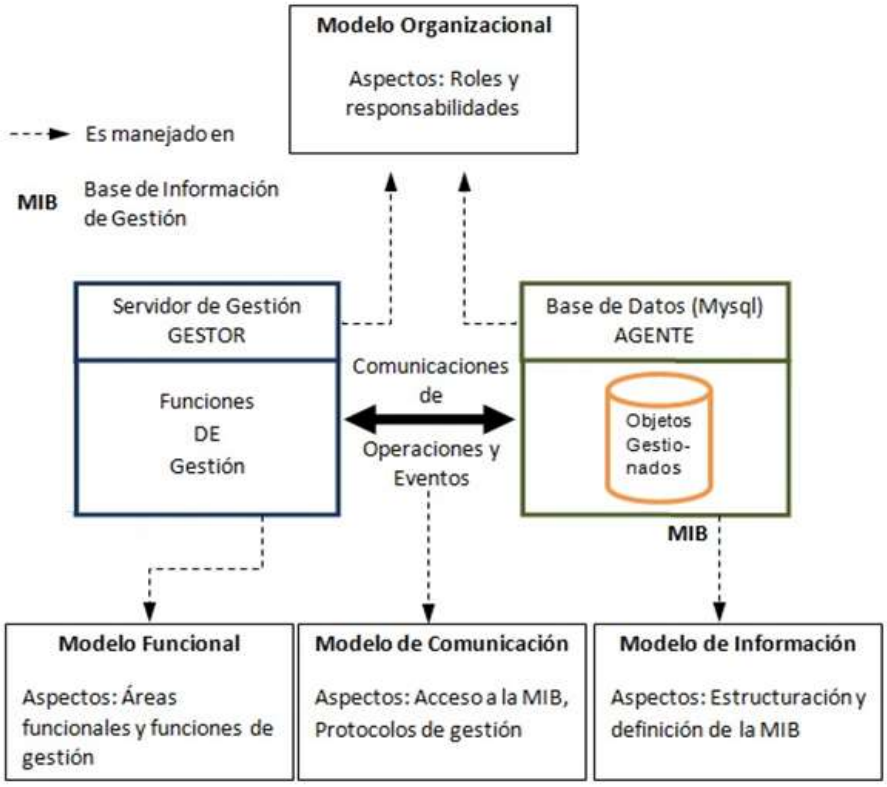

Figura 13. Modelos de Gestión.

En esta gráfica se puede observar a grandes rasgos la definición de un gestor (Servidor de Gestión) y un agente (Base de Datos - MySQL), los cuales contienen las Funciones de Gestión y la Basé de Información de la Gestión respectivamente. Tanto dichas funciones como la MIB, además de la definición y la comunicación de los componentes gestor y agente se controlan y manejan en los modelos que se describen a continuación.

3.3.1 MODELO DE INFORMACIÓN

Recoge todos los datos e información que describen y representan los recursos que deberán gestionarse, monitorizarse o controlarse, aquí se genera la MIB, la cual posteriormente será consultada por las funciones de gestión para poder realizar el análisis de la información almacenada con el fin de dar soporte al sistema de gestión.

La MIB además de contener la información relevante a la gestión obtenida por Syslog-ng, contiene tanto los eventos que son registrados gracias a la interfaz Asterisk Manager API como todos los diagramas que son resultado del diseño del sistema de gestión planteado en el presente proyecto.

La figura 14 describe el contenido de la MIB generada en este modelo.

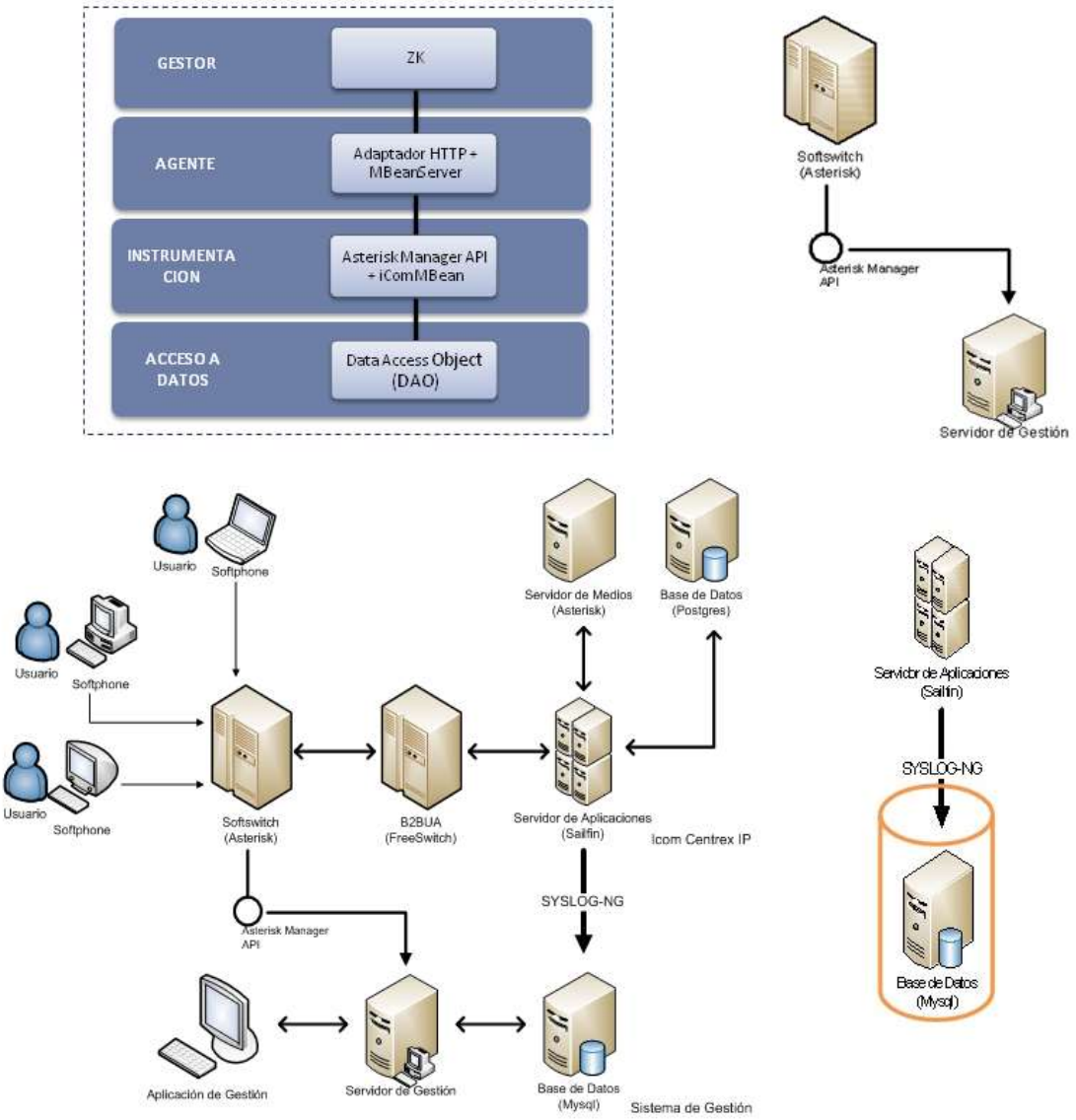

Figura 14. Modelo de Información.

Toda esta información que genera el iCom Centrex IP es posible capturarla gracias al syslog-NG desde el servidor de aplicaciones (Sailfin) y a la Asterisk Manager API desde el servidor softswitch (Asterisk), los cuales permiten clasificarla y filtrarla de acuerdo a las necesidades que se tengan, también cabe resaltar que toda esta información se actualiza en tiempo de ejecución con el fin de que el sistema este el mayor tiempo posible en funcionamiento y no presente falla alguna.

A Continuación se definen algunas de las propiedades de los objetos gestionados:

- **Identificación:** Son los ficheros log que genera el iCom Centrex IP y se logran capturar por medio de syslog-NG.

- **Comportamiento:** Contiene toda la información necesaria para saber cuando ocurre una falla en el sistema, además muestra el origen de la falla, el servicio que la origina y la prioridad que tenga la falla.

- **Actuaciones:** Esta información se almacena en una base de datos con el fin de facilitar su manipulación, para poder así realizar consultas en tiempo de ejecución y responder de manera rápida y sencilla a cualquier inconveniente que se genere.

- **Relaciones:** La base de datos la conforman ocho tablas, de las cuales se usan tres (una generada de forma por Syslog, y dos generadas a partir de la primera). Estas tres tablas se relacionan entre sí con el fin de brindar la información necesaria para poder realizar la gestión de manera eficaz. En el modelo organizacional se ampliará la información sobre estas tres tablas y sus relaciones.

- **Direccionamiento:** Esta información es accedida desde el servidor de gestión atreves de DAO (Data Acces Object), en el modelo de comunicación se ampliara esta información.

El diagrama de clases del sistema, sección 3.3.3 se presenta la forma de acceder a la información de gestión.

3.3.2 MODELO FUNCIONAL

El modelo funcional divide las tareas de gestión en áreas funcionales las cuales en el Capítulo 1 se describieron de forma detallada. Para el sistema de gestión se utilizaron específicamente 2 áreas funcionales: el de fallas y el de seguridad.

3.3.2.1 GESTIÓN DE FALLAS

Tiene como objetivo principal monitorear los servicios y alertar al operador sobre cualquier situación de falla que se presente.

Para poder mantener la red tiene las siguientes subtareas:

- Monitorizar los servicios y la red o estado del sistema, esto lo logra ya que el servidor de gestión siempre está pendiente de si cambia el campo estado de la tabla mensaje (en el modelo organizacional se explica el porqué de este cambio).

- Recibir y procesar alarmas, las alarmas que se generan en el sistema son:

    - Warning
    - Alert
    - Error
    - Emerg

- Diagnosticar las causas de los fallos de acuerdo a la prioridad que estos puedan tener.

- Solucionar los errores que se presenten. El presente proyecto no desarrolla esta parte, dado que no tiene como alcance la función de Configuración y un completo acceso al sistema iCom Centrex IP.

3.3.2.2 GESTIÓN DE SEGURIDAD

El objetivo principal es proteger la red, los servicios y la información que transporta, ante accesos y usos no autorizados. Esto lo logra gracias a que la aplicación tiene una cuenta de administrador con su debida contraseña con el fin de garantizar la información y que solo personas autorizadas puedan tener acceso a la misma, en caso de que una persona no autorizada quiera ingresar a la aplicación tendrá hasta tres intentos para ingresar la contraseña correcta, en caso de que eso no ocurra la aplicación enviara un correo electrónico a la cuenta del administrador indicando que un usuario no autorizado quiere ingresar a la aplicación de gestión. Además de la seguridad inherente a JMX, DAO y la Base de Datos de gestión.

Dentro de las funciones se tienen el análisis de riesgo, el cual, es un proceso que comprende la identificación de activos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo [27].

La evaluación del riesgo incluye las siguientes acciones y actividades, que se pueden determinar mediante el despliegue de estadísticas desde la aplicación de gestión.

- Identificación de los activos
- Valoración de los activos identificados
- Impacto de una pérdida de confidencialidad, integridad y disponibilidad.
- Identificación de las amenazas y vulnerabilidades importantes para los activos identificados.
- Evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Cálculo del riesgo.
- Evaluación de los riesgos frente a una escala de riesgo preestablecido.

Después de efectuar el análisis, el administrador será el encargado de determinar las acciones a tomar respecto a los riesgos residuales que se identificaron. Las acciones pueden ser:

- Controlar el riesgo.- Fortalecer los controles existentes y/o agregar nuevos controles.
- Eliminar el riesgo.- Eliminar el activo relacionado y con ello se elimina el riesgo.
- Compartir el riesgo.- Mediante acuerdos contractuales parte del riesgo se traspasa

a un tercero.

- Aceptar el riesgo.- Se determina que el nivel de exposición es adecuado y por lo tanto se acepta.

Estas acciones serán desarrolladas desde el iCom Centrex IP, y no desde el sistema de Gestión.

3.3.3 MODELO DE COMUNICACIÓN

En este modelo, y como se puede observar en la figura 15, se definen los esquemas para el intercambio de información entre los diferentes componentes del sistema de gestión.

El servidor de gestión obtiene información de dos maneras diferentes, por un lado para poder capturar la información de la base de datos utiliza DAO y por otro lado para obtener la información del Softswitch (Asterisk) utiliza el Asterisk Manager API, a continuación se describen cada uno de estos métodos.

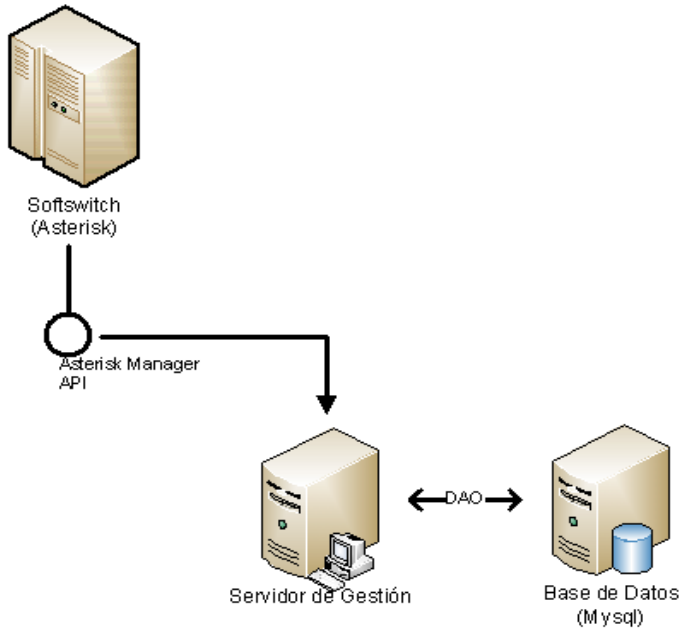

Figura 15. Modelo de Comunicación.

3.3.3.1 DAO (Data Access Object)

Un Data Access Object (DAO, Objeto de Acceso a Datos) es un componente software que suministra una interfaz común entre la aplicación y uno o más dispositivos de almacenamiento de datos, tales como una Base de datos o un archivo [28]. La ventaja de usar objetos de acceso a datos es que cualquier objeto de negocio (aquel que contiene detalles específicos de operación o aplicación) no requiere conocimiento directo del destino final de la información que manipula.

DAO encapsula el acceso a la base de datos. Por lo que cuando la capa de lógica de negocio necesite interactuar con la base de datos, va a hacerlo a través de la API que le ofrece DAO. Generalmente esta API consiste en métodos CRUD (Create, Read, Update y Delete). Entonces por ejemplo cuando la capa de lógica de negocio necesite guardar un dato en la base de datos, va a llamar a un método create(). Lo que haga este método, es problema de DAO y depende de cómo DAO lo implemente, puede que lo implemente de manera que los datos se almacenen en una base de datos relacional como puede que lo implemente de manera que los datos se almacenen en ficheros de texto. Lo importante es que la capa de lógica de negocio no tiene porque saberlo, lo único que sabe es que el método create() va a guardar los datos, así como el método delete() va a eliminarlos, el método update() actualizarlos, etc. Pero no tiene idea de cómo interactúa DAO con la base de datos.

Los DTO (Data Transfer Object) o también denominados VO (Value Object). Son utilizados por DAO para transportar los datos desde la base de datos hacia la capa de lógica de negocio y viceversa.

El uso de DAO permite que a futuro, el desarrollador de gestión pueda implementar las áreas funcionales de gestión no contempladas en este proyecto sin cambios fundamentales en el diseño de lo aquí planteado.

3.3.3.2 ASTERISK MANAGER API

La Manager API es una de las formas para la interacción remota con un servidor Asterisk [29]. Se compone de tres conceptos: acciones, respuestas y eventos. Las acciones pueden ser enviadas a asterisk e instruirle que haga algo en especial. Por ejemplo su aplicación puede enviar una acción a asterisk solicitando que al marcar un número directo este se transfiera a uno de sus teléfonos. En respuesta a una acción, Asterisk envía una respuesta que contiene los resultados de la operación realizada.

Los eventos se envían por Asterisk sin una relación directa con las acciones que su aplicación está enviando. Los eventos informan sobre los cambios pertinentes en el estado de Asterisk. Por ejemplo los eventos se utilizan para informar a su aplicación sobre las llamadas entrantes o usuarios que se registran en el sistema. La conexión con el servidor de Asterisk a través del Manager API se produce a través de TCP/IP por lo general en el puerto por defecto 5038. Para habilitarlo basta con editar el archivo de configuración y reiniciar el servidor asterisk.

A través del uso de esta interfaz, se puede integrar de una forma sencilla las áreas funcionales de gestión no contempladas en este proyecto.

También hace parte de este modelo la manera como se genera la MIB a través del intercambio de información del servidor de aplicaciones y la base de datos por medio de syslog-NG, figura 14, el cual utiliza el protocolo UDP para realizar la captura de forma remota del servidor y establece la conexión por medio del puerto 514 el cual es un puerto por defecto que utiliza sislog-NG para sus conexiones remotas.

Además se debe considerar la forma en que el sistema de gestión presenta el resultado final de una manera grafica y simple utilizando una de las funciones de JMX la cual presenta en su último nivel (gestor), un interpretador HTTP el cual facilita la conexión con

el web browser permitiendo que la aplicación de gestión tenga acceso a través de una interfaz web al sistema de gestión.

3.3.4 MODELO ORGANIZACIONAL

En este modelo se establecen los diferentes roles o funciones dentro del sistema de gestión y su distribución espacial. Básicamente se divide en 2 partes el gestor y el agente, el gestor está conformado por el servidor de gestión y la aplicación cliente, y el agente por la base de datos Mysql.

3.3.4.1 AGENTE DEL SISTEMA DE GESTIÓN

En la figura 16 se muestra la base de datos Mysql que hace parte del agente y las tablas que la conforman.

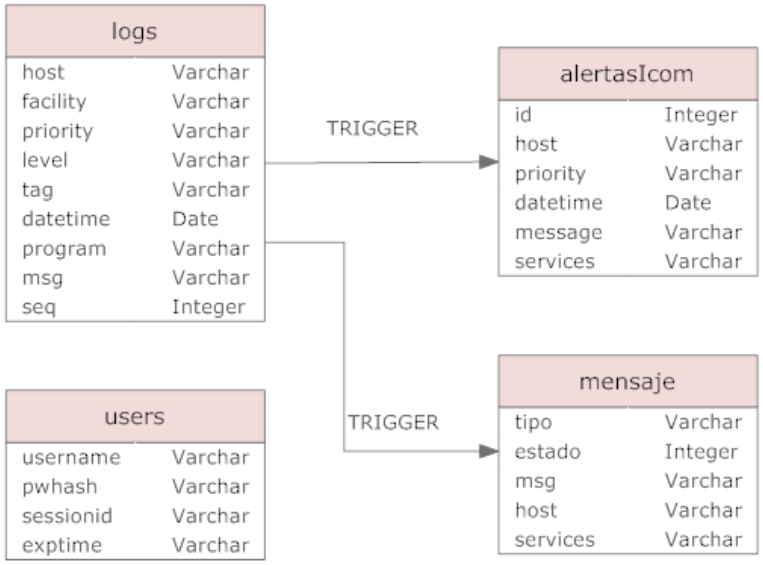

Figura 16. Esquema de la Base de Datos de Agente.

A continuación se explicara cada una de las tablas que conforman la base de datos:

logs: Esta tabla se crea a partir de la configuración de syslog-NG, es la encargada de recibir toda la información proveniente del icom Centrex IP y por ende la más importante, ya que contiene todos los log que se generen en el sistema, además a partir de ésta se crean las otras tablas que conforman la base de datos, está conformada por 9 columnas que se distribuyen de la siguiente manera:

- **host:** Es el lugar de donde se origina el mensaje.
- **facility:** Es el servicio que está generando el mensaje.
- **priority:** Es la prioridad o nivel de alerta que tiene el mensaje.

- **level:** Similar a proirity.
- **tag:** Es la etiqueta del mensaje.
- **datetime:** Es la hora en la que se origino el mensaje.
- **program:** Es el programa que genera el mensaje.
- **msg:** Contiene la información detallada del mensaje.
- **seq:** Es la secuencia con la cual se van generando los mensajes del sistema.

alertasIcom: Esta tabla se crea a partir de la tabla logs utilizando trigger (mas adelante se explicara este tema), trigger es un disparador que permite que una vez llegue la información requerida a la tabla de logs este crea y actualiza la tabla "alertasIcom" con la información capturada llenando todos los campos requeridos.

La creación de esta segunda tabla permite que se pueda tener de forma separada las alertas del sistema iCom Centrex IP del resto de mensajes generados en el mismo, como por ejemplo mensajes de reinicio, configuración, etc. La tabla contiene 6 columnas distribuidas así:

- **id:** Es el identificador del mensaje que llega.
- **host:** Lugar de donde se origina el mensaje.
- **services:** Servicio del Centrex donde se origino la falla, para efectos del presente proyecto solo puede tener tres valores: establecimiento, transferencia y grabación de llamada.
- **priority:** Prioridad de alerta que tiene el mensaje, puede ser, Warning, Alert, Error y Emerg.
- **datetime:** Fecha y hora en la que ocurrió la falla.
- **message:** Da información explícita sobre el tipo de falla ocurrida.

Mensaje: esta tabla también se crea a partir de trigger, pero tiene la particularidad de que esta es la que permite saber el momento exacto en el que ha ocurrido una falla, es decir, esta tabla contiene un campo llamado estado, el cual tiene valor por defecto cero (0), pero una vez que se genere una falla en el Centrex este estado cambiara a uno (1), logrando que el sistema de gestión genere un alarma de acuerdo a la prioridad que este tenga y una vez esta alarma sea atendida el estado volverá a cero en busca de otra falla.

Esta tabla permite al gestor de la aplicación, conocer en tiempo de ejecución las fallas sin necesidad de realizar operaciones como hacer click en un botón o en un enlace. A continuación se describen los campos que conforman a la tabla:

- **Id:** Identificador del mensaje.
- **Host:** Origen del mensaje.
- **Estado:** Indicador de ocurrencia de la falla, toma valores cero y uno depende cual sea la situación.
- **Mensaje:** Mensaje relacionado con la falla generada.
- **Servicio:** Servicio que origino la alerta.

users: esta tabla se crea a partir de la configuración de syslog-NG, y contiene la información sobre las cuentas de usuario que pueden acceder a la aplicación de gestión. Está conformada por 4 columnas que se distribuyen de la siguiente manera:

- **username:** Nombre de usuario. Por defecto contiene el valor “admin”.
- **pwhash:** Contraseña asignada al usuario.
- **sessionid:** Identificador de la sesión que ha iniciado el usuario. Esta sesión normalmente es iniciada vía Web.
- **exptime:** Tiempo que dura la sesión de usuario desde que se establece hasta que finaliza.

Trigger: son objetos relacionados con tablas y almacenados en la base de datos que se ejecutan o se muestran cuando sucede algún evento sobre sus tablas asociadas [30]. Los eventos pueden ser las sentencias INSERT, DELETE, UPDATE que modifican los datos de una tabla.

Los triggeres se pueden ejecutar antes (BEFORE) y/o después (AFTER) de que sean modificados los datos. Los triggers tienen dos palabras clave, OLD y NEW que se refieren a los valores que tienen las columnas antes y después de la modificación. Los INSERT permiten NEW, los DELETE sólo OLD y los UPDATE ambas.

Son usados para mejorar la administración de la Base de datos, sin necesidad de contar con que el usuario ejecute la sentencia de SQL. Además, pueden generar valores de columnas, previene errores de datos, sincroniza tablas, modifica valores de una vista, etc. Permite implementar programas basados en paradigma lógico (sistemas expertos, deducción).

En el caso del proyecto, su principal función es la de generar tablas diferentes que se usan explícitamente para la gestión de fallas, permitiendo que la información pueda almacenarse de una forma más segura y confiable, lo que va de la mano de la gestión de seguridad.

La estructura básica de un trigger es:

- **Llamada de activación**: es la sentencia que permite “disparar” el código a ejecutar.
- **Restricción**: es la condición necesaria para realizar el código. Esta restricción puede ser de tipo condicional o de tipo nulidad.
- **Acción a ejecutar**: es la secuencia de instrucciones a ejecutar una vez que se han cumplido las condiciones iniciales.

Estos trigger permiten que una vez sea generada algún tipo de falla en el sistema actualice los campos de las tablas que están relacionados con ellos, para que el sistema de gestión se dé cuenta de que ocurrió una falla, de que tipo es, que servicio la origino, cual es la prioridad que tiene y cuál es el origen. Todo esto es capaz de realizarlo en tiempo de ejecución.

3.3.4.2 GESTOR DEL SISTEMA DE GESTIÓN.

La figura 17 muestra cómo está compuesta la parte gestora del sistema.

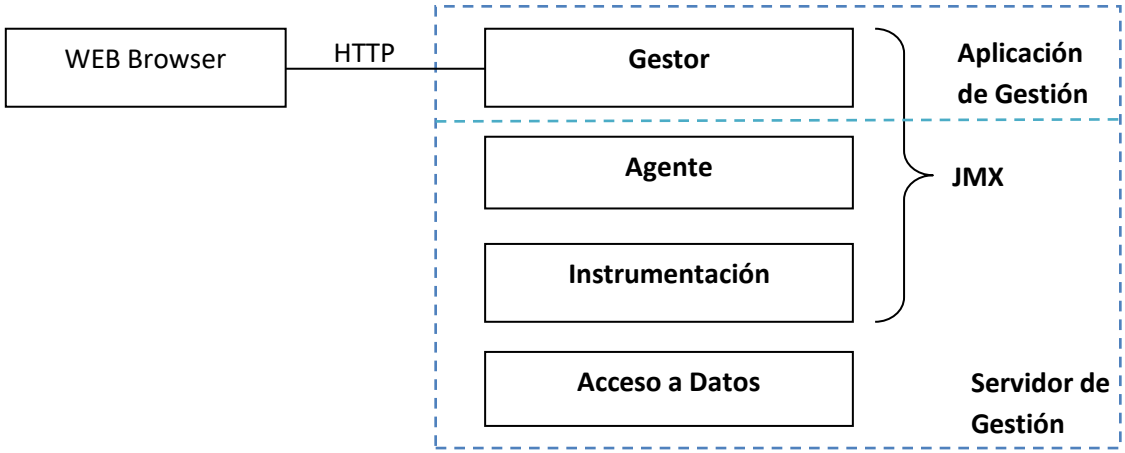

Figura 17. Servidor de Gestión.

La parte del servidor de gestión la conforman tres niveles (Acceso a Datos, Instrumentación y Agente) y la parte de la aplicación de gestión se constituye como la aplicación cliente que accede a la información expuesta desde el servidor. Los tres niveles superiores de la parte del gestor del sistema de gestión propuesto en el presente proyecto son las capas definidas en la arquitectura JMX.

Con respecto al último nivel, el de acceso a datos, es el que permite que el sistema de gestión puede capturar la información necesaria que se origina en el agente, es decir en la base de datos. Esta es la primera etapa que tienen que pasar los mensajes de error antes de que puedan ser procesados por la aplicación de gestión, para poder así darle una solución definitiva a estas fallas que puedan presentarse en el sistema.

En la figura se contempla también el WEB Browser, que representa la interfaz web de gestión, es decir, es el resultado final de la aplicación de gestión, que muestra de una manera grafica y sencilla todo lo que pase en el sistema de gestión. Gracias a que JMX tiene en su último nivel (Gestor) un interpretador http para poder realizar la comunicación con la aplicación de gestión, en la aplicación se pueden manejar tanto los diferentes usuarios que tendrán acceso a la aplicación como las peticiones realizadas por los usuarios del sistema de gestión.

Además de los roles de los usuarios del sistema, que garantiza que solo el administrador podrá realizar cambios en la configuración del sistema de gestión, existe un nivel de seguridad transparente para cada usuario, que es la seguridad inherente de JMX, de DAO, y de la Base de Datos de Gestión.

3.4 DESARROLLO DEL SISTEMA DE GESTIÓN.

El sistema de gestión planteado en este proyecto, como se puede observar en el diagrama de clases (Figura 18), al igual que en la arquitectura del sistema (Figura 12), contiene ciertas características en su diseño que lo hacen un sistema fácilmente escalable y con la capacidad de integrarse y operar con diferentes sistemas de monitoreo y gestión.

Estas características específicamente pueden ser ubicadas en la clase IcomInstrument y la clase Agent. La primera es la que implementa la interfaz que instrumenta los recursos, y por ende, la información de gestión; aquí se puede de una forma sencilla y sin necesidad realizar grandes cambios al diseño, agregar tanto algunas operaciones que implementen las funcionalidades de gestión y/o definir nuevas clases que complementen las funcionalidades definidas originalmente en dicha clase.

La segunda, la clase Agent, permite el descubrimiento de los recursos gestionados y los hace disponibles a diferentes aplicaciones de gestión. Es esta parte del sistema la que nos otorga la capacidad de poder interactuar con diferentes tipos de clientes, ya sea que estos utilicen JMX o no. Es esta parte el núcleo del sistema, y su implementación es realmente sencilla, ya que solo recibe la información lista para ser gestionada y la despliega de acuerdo a ciertos parámetros que establezcan las partes.

Finalmente, como parte fundamental del sistema planteado, la clase Manager se constituye en la lógica de la aplicación de gestión y es la que permite que la información de gestión sea vista de forma agradable y fácil de entender para los administradores del sistema.

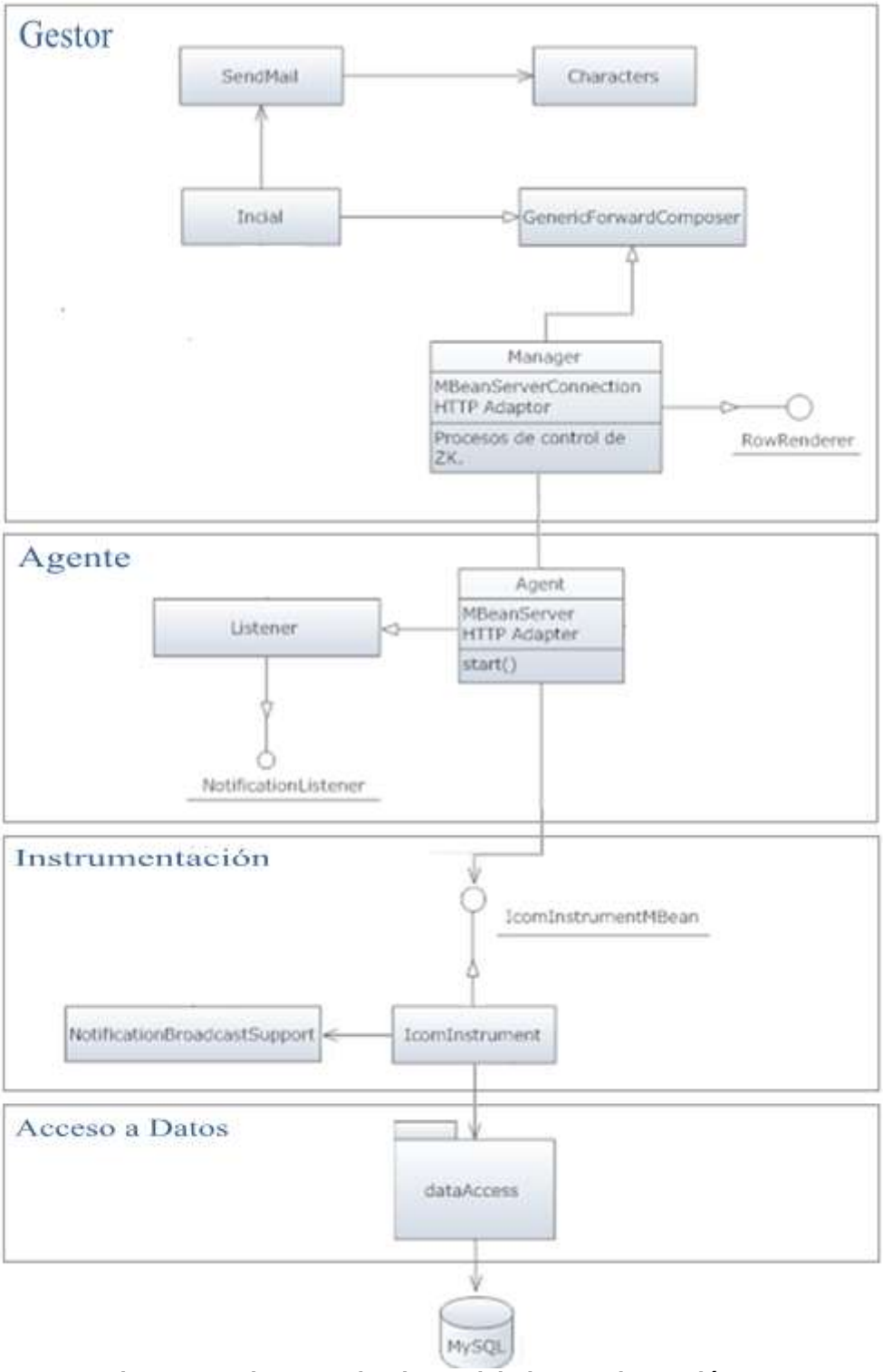

Figura 18. Diagrama de Clases del Sistema de Gestión.

4 PRUEBAS

El presente capítulo muestra una serie de pruebas que corroboran el correcto funcionamiento y cumplimiento de las condiciones planteadas en el diseño del sistema.

Se presentan una serie de imagines donde se muestra el funcionamiento de la aplicación de gestión, desde el ingreso a la misma, hasta la llegada de alguna falla en especial.

4.1 PRUEBAS DE LA FUNCIONALIDAD SEGURIDAD.

4.1.1 INGRESO FALLIDO A LA APLICACIÓN.

Inicialmente se probara la seguridad del sistema donde se simulara el ingreso de un usuario no autorizado y lo que sucede al tercer intento fallido.

A continuación se presenta la pantalla inicial de la aplicación de gestión:

Figura 19. Pantalla inicial

La siguiente imagen muestra el ingreso de un usuario no autorizado al sistema:

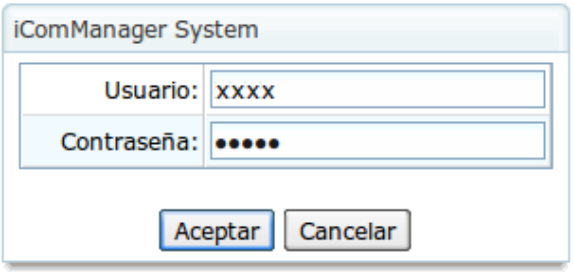

Figura 20. Ingreso Fallido

Una vez se introduzca el usuario no autorizado por primera vez la aplicación muestra lo siguiente:

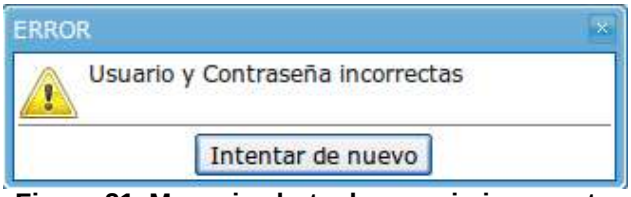

Figura 21. Mensaje alerta de usuario incorrecto

El usuario tendrá hasta tres intentos para ingresar la contraseña correcta, de lo contrario el sistema se bloqueara y enviara una notificación al correo electrónico del administrador donde le indica que un usuario no autorizado está intentado ingresar al sistema:

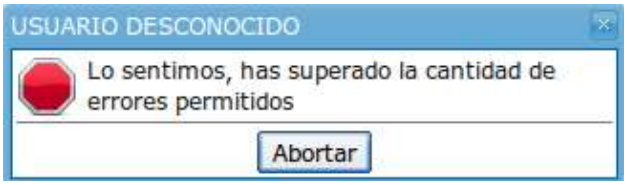

Figura 22. Mensaje error de usuario

4.1.2 INGRESO PERMITIDO A LA APLICACIÓN.

Una vez se ha probado el ingreso fallido, se muestra el ingreso a la aplicación por parte del administrador del sistema de gestión.

Se está en la pantalla inicial de la aplicación, ver figura 19, ahora el administrador ingresa su nombre de usuario y contraseña para acceder a la aplicación:

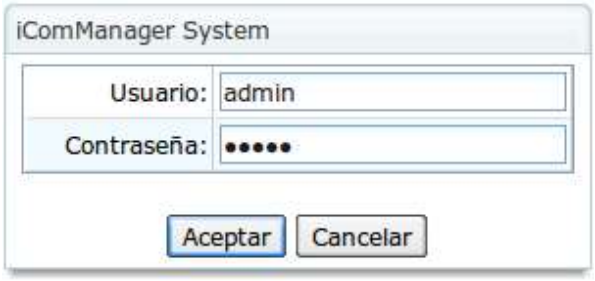

Figura 23. Ingreso Administrador

Una vez se halla ingresado el usuario permitido el resultado será el ingreso a la aplicación del sistema de gestión:

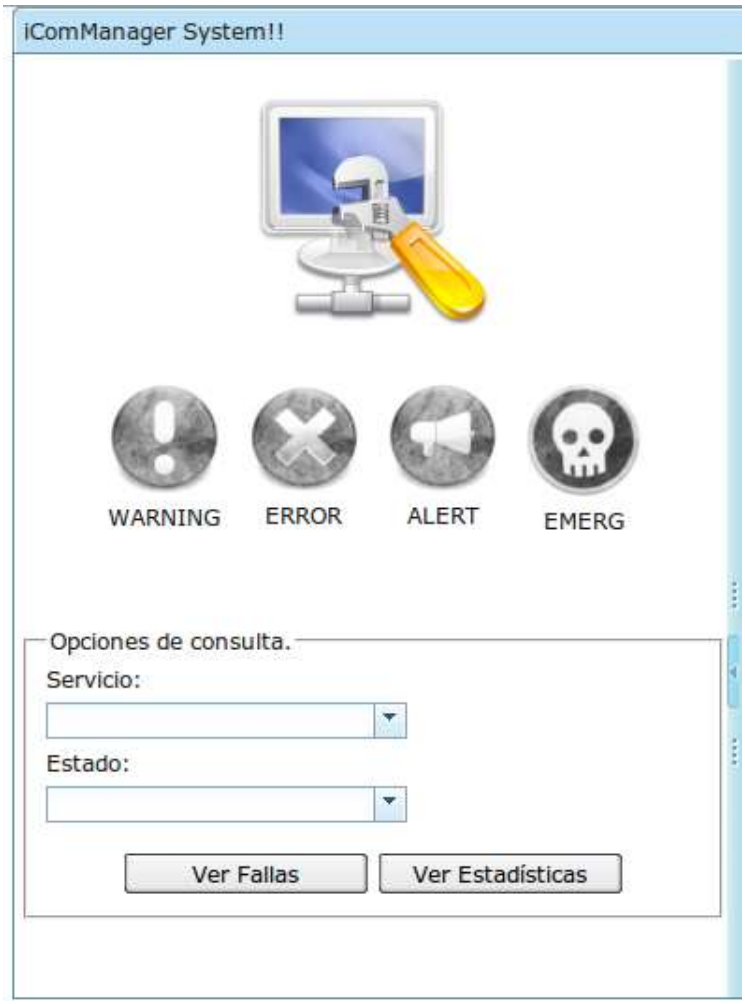

Figura 24. Aplicación de gestión

4.1 PRUEBAS DE LA FUNCIONALIDAD DE FALLAS

4.1.1 RECOLECCIÓN DE ALARMAS

En esta parte de la interfaz, se tiene acceso a las diferentes funcionalidades del sistema. Los servicios gestionados son los que se muestran en la figura 25, a cada uno de ellos se le puede consultar información más precisa sobre el tipo de fallas presentado, como se muestra en la figura 26.

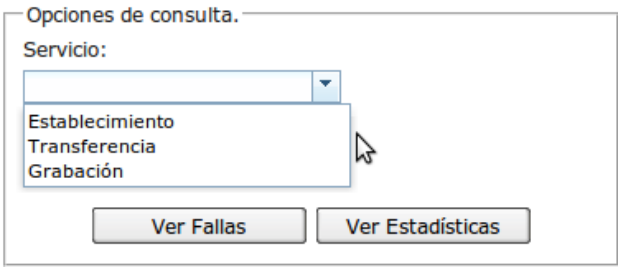

Figura 25. Menú Servicio

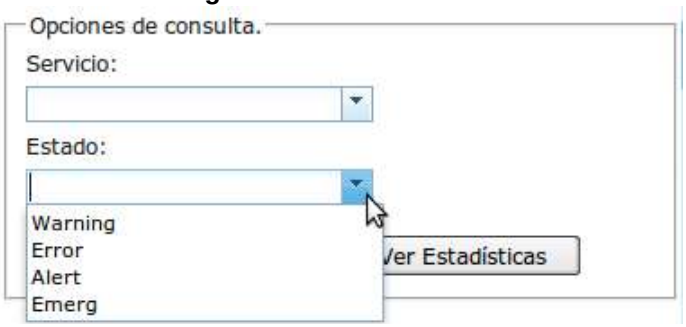

Figura 26. Menú buscar

Si se desea consultar las fallas que se han presentado en determinado servicio, se debe seleccionar el servicio y hacer click en el botón “Ver Fallas”. El resultado se muestra en a figura 27.

Figura 27. Ver Fallas

Estando en esta parte el administrador puede filtrar estos mensajes, para esto el menú estado despliega los diferentes tipos de falla que presenta el sistema y por el cual se desea filtrar:

Una vez se seleccione la opción que se desee, en este caso es warning, se desplegara la información seleccionada mostrando todas las alarmas del tipo warning que se han generado para el servicio seleccionado en el sistema de gestión, ver figura28.

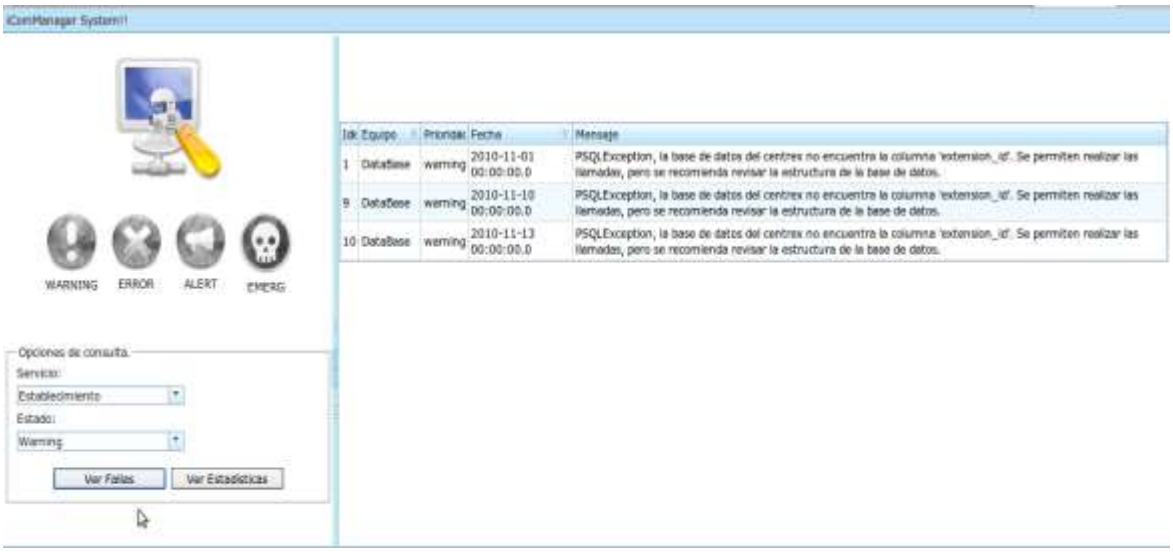

Figura 28. Selección de la búsqueda

4.1.2 ESTADÍSTICAS

Además la aplicación cuenta un botón que permite ver de manera grafica la ocurrencia de las fallas, esto se logra haciendo click en “ver estadísticas” el cual muestra la cantidad de fallas que han ocurrido por cada servicio:

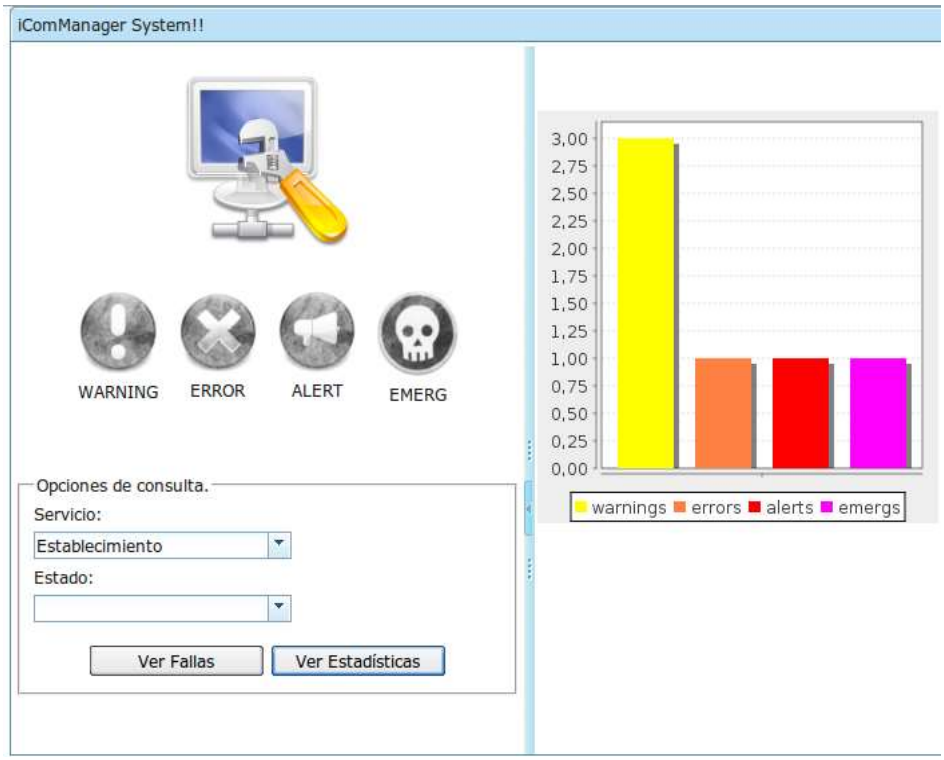

Figura 29. Estadísticas

4.1.3 DETECCIÓN DE LA FALLA.

En el capítulo anterior se explicó cómo debe ser el funcionamiento del sistema de gestión en el momento de que ocurra una falla, a continuación se mostrara de forma grafica como responde la aplicación ante las mismas.

Inicialmente el sistema se encuentra en la pantalla principal de la aplicación de gestión (ver figura 24). Cuando en el sistema iCom Centrex IP ocurra una falla de cualquier tipo, la aplicación detecta la falla y según el tipo que tenga lo mostrara en la aplicación de la siguiente manera:

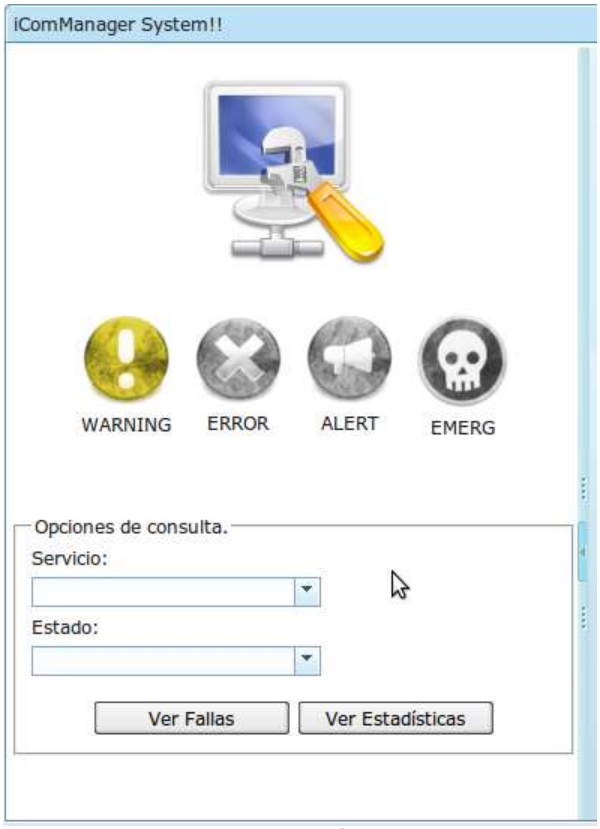

Figura 30. Detección de la falla

Esta alerta mantendrá este color hasta que el administrador revise la falla, para revisarla basta con hacer click sobre la alerta generada para que la aplicación responda de la siguiente manera:

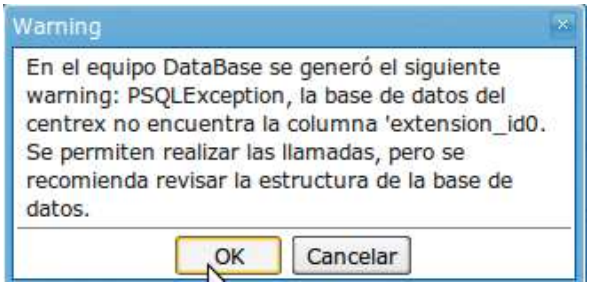

Figura 31. Revisión de la falla

Una vez el administrador presione OK la aplicación retornara a su pantalla principal en la espera de una nueva falla.

A continuación se presenta como responde el equipo para las diferentes fallas que presenta el sistema:

Figura 32. Tipo de falla (Error)

Figura 33. Tipo de falla (Alert)

Figura 34. Tipo de falla (Emerg)

El manejo de las fallas es igual para todas y siguen el mismo procedimiento anteriormente descrito en este capítulo.

4.1.4 DETECCIÓN DE DOS O MÁS FALLAS

Anteriormente se describió el proceso para atender una falla, ahora se verá cómo responde la aplicación cuando ocurren dos o más fallas.

Inicialmente la aplicación se encuentra en modo de espera de fallas o en su pantalla principal (ver figura 24). En el momento en que ocurren dos tipos diferentes de fallas la aplicación responde como se observa en las figuras 35 y 36.

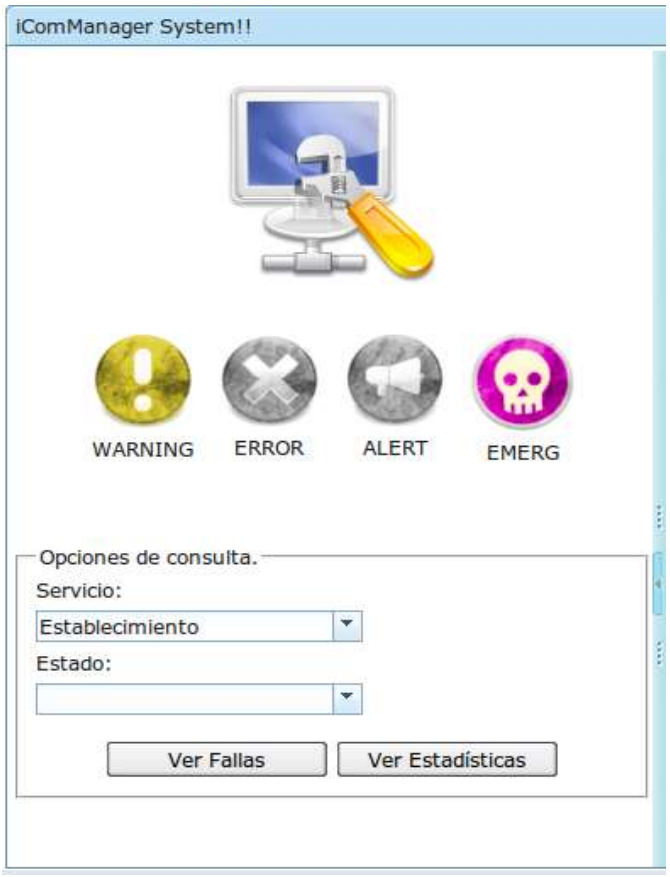

Figura 35. Ocurrencia de 2 fallas

Figura 36. Dos fallas al tiempo

Estas dos fallas se quedaran en estado encendido hasta que sean atendidas por el administrador. Primero se atenderá el warning (ver figura 37), mientras se realiza esta operación la otra falla que se presento se mantiene en su estado encendido, una vez se atienda la falla warning la aplicación muestra la figura 38, en donde se deberá realizar un procedimiento similar al explicado en la sección 4.3.

Figura 37. Atención de una falla

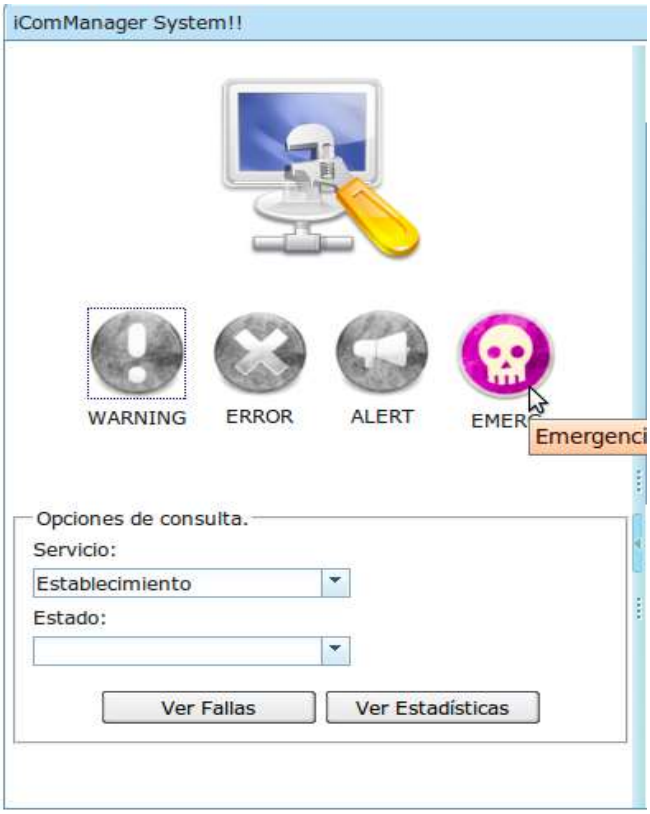

Figura 38. Falla atendida y una pendiente

5 CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

5.1 CONCLUSIONES

- El sistema de gestión aquí desarrollado permite optimizar el rendimiento y aumentar las funciones del proyecto iCom Centrex IP el cual no contaba inicialmente con un módulo o subsistema para la gestión.

- La arquitectura de instrumentación de gestión que plantea JMX es lo suficientemente potente como para ser considerada por cualquier proyecto de gestión. Esto se debe a que JMX permite trabajar de forma independiente a los protocolos de comunicación, se puede realizar una gestión de servicios, sistemas o cualquier recurso, y, por ser un desarrollo en el lenguaje de programación de Java, se cuenta con suficiente apoyo y material.

- La gestión de NGN es una necesidad constante en el contexto actual de las telecomunicaciones, por lo que proyectos como el desarrollado en este trabajo de grado se convierten en una guía de estudio y referencia, tanto en el diseño de sistemas de gestión como en su implementación.

- Es de suma importancia poder contar con la documentación adecuada, instaladores y demás recursos que se necesitan en la entrega de un proyecto, con el fin de evitar retrasos que perjudique el buen desarrollo del proyecto, problema con el que nos encontramos en este proyecto, ya que el sistema iCom Centrex IP había sido desmontado de los servidores que lo contenían y el grupo de trabajo de dicho proyecto no tenía un repositorio con los archivos de configuración, archivos desplegables y bases de datos de la versión final del mismo. Esto último se tradujo inevitablemente en un considerable retraso en la finalización del presente proyecto, pero a la vez se convirtió en una oportunidad de aprendizaje sobre configuración, montaje, funcionamiento y desarrollo de sistemas Centrex IP.

- El diseño e implementación del sistema de gestión del presente proyecto permite que se pueda completar las funcionalidades de gestión para todos los servicios del iCom Centrex IP, teniendo la posibilidad de realizar esto tanto en la misma aplicación de gestión desarrollada como en diferentes aplicaciones sin que esto implique un gran impacto en el diseño de este sistema.

- El esfuerzo invertido en su desarrollo, ha implicado la obligación de familiarizarse con una serie de tecnologías y herramientas como JMX, ZK, AGI, syslog-NG, manejo de bases de datos, que han consumido parte del tiempo de desarrollo, pero que su potencia y vigencia las hace muy merecedoras de esta dedicación por parte de los desarrolladores, logrando así, ampliar la base de conocimientos de los mismos.

- La utilización del framework ZK para la interfaz de usuario, redujo considerablemente el desarrollo del mismo gracias a su fácil manejo y completa documentación, además de que es un software de código abierto.

- Si bien el presente proyecto planteaba en sus objetivos la construcción de una solución de gestión y no una arquitectura, el estudio realizado tanto de la teoría de gestión como de diferentes arquitecturas y modelos, ayudó a determinar las características funcionales necesarias con las que debe contar un sistema de gestión, haciendo de este trabajo una referencia para la construcción de una arquitectura de gestión.

- El diseño de la aplicación permite implementar otras formas de acceder a ella, no solo mediante un navegador web. El hecho de poder trabajar con la vista de forma independiente a todo lo demás, nos permite pensar en nuevas implementaciones para la gestión a través de un teléfono IP o un PDA por ejemplo.

- Se logró incursionar con éxito en el desarrollo de aplicaciones de gestión utilizando la tecnología JMX en un ambiente “Open Source”.

- La utilización de una metodología para el desarrollo, la programación orientada a objetos y la aplicación de patrones de diseño son una gran ayuda para el desarrollo de proyectos de calidad, con altos niveles de eficiencia y bajo un cronograma controlado.

- Los sistemas operativos basados en Linux proporcionan un mejor rendimiento que cualquier otro sistema operativo basado en software privativo porque son sistemas sostenidos por una comunidad confiable y capaz de ofrecer un desarrollo y actualización constante del sistema.

- Es importante acudir a los foros especializados existentes en la red, ya que éstos pueden ofrecer un soporte importante y válido al momento de solucionar problemas que surjan en las diferentes fases del proyecto, en particular en el desarrollo del mismo.

- El sistema desarrollado tiene por característica principal una gran escalabilidad debido a que se usaron tecnologías abiertas, lo que se traduce en mayores facilidades a la hora de añadir funcionalidades que lo complementen.

- A la hora de desarrollar un proyecto, es importante asegurarse de que las tecnologías a manejar sean lo suficientemente maduras para una adecuada y rápida ejecución del proyecto, así como un dimensionamiento correcto en cuanto al tiempo de terminación del proyecto.

5.2 RECOMENDACIONES

- A través del proceso de desarrollo de la aplicación de gestión es muy importante tener en cuenta las limitaciones y capacidades de los equipos que se tienen, ya que el despliegue de interfaces y las características de rendimiento no son completamente visibles en todos los equipos que se encuentran en el mercado. El no tener en cuenta esta recomendación podría prolongar el proceso de desarrollo al tener que hacer modificaciones considerables en el código de la aplicación para que se ajuste a las características técnicas de los equipos reales.

- Se recomienda agregar un módulo de help desk al sistema aquí desarrollado para dar soporte a los usuarios del iCom Centrex IP.

- Un factor importante en cualquier sistema de telecomunicaciones es la seguridad, por ende se recomienda ampliar la seguridad del sistema a los servicios ofrecidos y mensajes que pasan a través del iCom Centrex IP.

- Debido el sistema desarrollado no ofrece las 5 áreas funcionales que se presentan en un sistema de gestión, se recomienda implementar las tres áreas funcionales faltantes con el fin de mejorar el rendimiento del mismo.

- En caso de tener acceso a la versión final del sistema iCom Centrex IP se recomienda complementar el presente desarrollo para que la gestión pueda cubrir todas las necesidades del iCom Centrex IP, desde la configuración de usuarios, servicios, hasta la puesta en marcha de los mismos.

- Se recomienda seguir utilizando tecnologías abiertas, las cuales ofrecen libertad al usuario para su manejo, ejecución, distribución y modificación (aspectos esenciales para un buen desarrollo de software), sin preocupaciones de que en cualquier momento termine la licencia de ejecución y por ende su trabajo.

5.3 TRABAJOS FUTUROS

- Dado que los servicios que ofrece el sistema iCom Centrex IP se desarrollaron en un ambiente IMS, se puede tomar el presente proyecto como base para la implementación de sistemas de gestión de diferentes proyectos que se desarrollen en dicho ambiente, por ejemplo el proyecto de Televisión Digital Interactiva que actualmente se está desarrollando en la Universidad del Cauca

- Actualmente las redes están migrando para un terreno móvil, por lo que se puede pensar en una aplicación de gestión para dispositivos móviles con el fin de que el administrador no tenga que estar siempre detrás de un escritorio pendiente de un equipo en especial sino que tenga mayor movilidad.

- Dado que la versión final del sistema iCom Centrex IP se encuentra en funcionamiento en la compañía AVATAR LTDA, se podría realizar y complementar el presente proyecto con la realización de una arquitectura de gestión en un ambiente real de telecomunicaciones.

- Viendo como está avanzando la tecnología hoy en día, se puede realizar un centrex con todas las funcionalidades que este presenta, pero para la telefonía móvil, el cual pueda interactuar con los usuarios de las actuales compañías de telefonía móvil que se encuentran en funcionamiento en nuestro país.

- El proyecto que se realizo solo cubre la parte de la gestión de los servicios, como trabajo futuro se puede pensar en la implementación de un sistema que pueda realizar la facturación de los servicios contratados o realizar un sistema de log en el que todas las operaciones que los usuarios realizan queden reflejadas (para su posterior análisis).

6 BIBLIOGRAFÍA

[1] Barba, A., *Gestión de red,* Edicions UPC. Barcelona, Septiembre de 1999.

[2] Koontz, H.; Weihrich, H., *Administración, una prospectiva global,* McGraw-Hill. México, 1998.

[3] Hegering, H.; Abeck, S.; Neumair, B., *Integrated Management of Networked Systems: Concepts, Architectures, and Their Operational Application,* Morgan Kaufmann, 1999.

[4] Sayman, T.; Magedanz, T., *From Networks and Network Management Into Service and Service Management.,* Journal of Network and Systems Management, Vol.4, No.4, 1996.

[5] Antonio, M.; de Mora, C., *Los Estándares De Gestión De Redes De Telecomunicaciones.* Sevilla, 2002.

[6] Unión Internacional de Telecomunicaciones,"*MARCO DE GESTIÓN PARA LA INTERCONEXIÓN DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT", Recomendación X.700.* Septiembre de 1992.

[7] *ISO, "Information technology -- Open Systems Interconnection -- Management Information Services -- Structure of management information: Management Information Model", Recomendacion ISO/IEC 10165-1:1993.* 1993.

[8] *CCITT, "TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – ESTRUCTURA DE LA INFORMACIÓN DE GESTIÓN: MODELO DE INFORMACIÓN DE GESTIÓN", Recomendacion X.720.* 1992

[9] Unión Internacional de Telecomunicaciones*, "Protocolo de Informacion de Gestion Comun", Recomendación X.711.* 1997

[10] Unión Internacional de Telecomunicaciones*, "Principios para una red de gestión de las telecomunicaciones", Recomendación M.3010.* Febrero de 2000.

[11] Pras, A.; Beijnum, V.; Bert, J.; Sprenkels, Ron., *Introduction to TMN.* s.l. : CTIT Technical Report 99-09, University of Twente. Holanda, 1999.

[12] Case, J., *"A Simple Network Management Protocol (SNMP)" RFC 1157.* Mayo de 1990.

[13] Centro de Investigacion Imaginar, *Estudio integral de Redes de Nueva Generacion y convergencia.* Junio de 2007

[14] Union Internacional de Telecomunicaciones, *"Vision general de las redes de proxima generacion", Recomendación ITU-T Y.2001.* Diciembre de 2004

[15] Union Internacional de Telecomunicaciones, *"Requisitos y arquitectura funcional de las redes de próxima generación", Recomendación ITU-T Y.2012.* 2006.

[16] Unión Internacional de Telecomunicaciones, *"Principios generales y modelo de referencia general de las redes de próxima generación", Recomendación ITU-T Y.2011.* Octubre de 2004.

[17] Blum, N.; Magedanz, T.; Schreiner, F., *"Management of SOA based NGN service exposure, service discovery and service composition, Integrated Network Management.* 2009.

[18] Union Internacional de Telecomunicaciones, *"Principios para la Gestion de Redes de Nueva Generación", Recomendación ITU-T M.3060/Y.2401.* Marzo de 2006.

[19] Tejedor, R., *IP Multimedia Subsystem. Convergencia total en IMS.* Millán. 2006.

[20] Fundación Orange, *IMS: IP Multimedia Subsystem. La evolución de las redes móviles.*, Agosto de 2007. Disponible en Web. http://www.fundacionorange.es/areas/25_publicaciones/Nota_18_DEF.pdf. [Citado el: 20 de Agosto de 2010.]

[21] Znaty, S.; Dauphin, J.; Geldwerth, R., *IP Multimedia Subsystem: Principios y Arquitectura.*

[22] de Vergara, L., *Análisis y comparativa de las alternativas propuestas para la Gestión Basada en Web.* Universidad Politécnica de Madrid. 2001.

[23] Sun Microsystem, Inc. *Java Management Extensions (JMX) Specification, version 1.4.* Noviembre de 2006.

[24] Agredo, G.; Maya, N.; Maya, E.; *Selección de herramientas para realizar gestión basada en WBEM en la Red de Datos de la Universidad del Cauca.* 2003.

[25] Caicedo, J.; Rios, C.; Hermida, V.; *iCom_Centrex_IP-SAT-RT-5-V1.1Arquitectura_de_Referencia.* Popayan : Universidad del Cauca, 30 de noviembre 2009.

[26] Pagina de inicio de syslog-NG. Disponoble en web: http://www.balabit.com/products/syslog_ng/. [Citado el: 30 de octubre de 2010.]

[27] *ISO, "Information technology - Security techniques - Information security management systems – Requirements", Recomendacion ISO/IEC 27001.* 2005.

[28] affiliates, Oracle Corporation and/or its. Core J2EE Patterns - Data Access Object. 2010 Disponible en web: http://java.sun.com/blueprints/corej2eepatterns/Patterns/DataAccessObject.html. [Citado el: 05 de 11 de 2010.]

[29] Reuter, Stefan. asterisk-java. Disponible en web: http://asterisk-java.org/development/tutorial.html. [Citado el: 05 de 11 de 2010.]

[30] Widenius, M.; *MySQL 5.0 Reference Manual.* Oracle and/or its affiliates, 2010.