

RAE

1. **TIPO DE DOCUMENTO:** Trabajo de grado para optar por el título de INGENIERO(A) DE TELECOMUNICACIONES.
2. **TITULO:** DISEÑO DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES PARA LA OPERACIÓN DE UN IP CONTACT CENTER PARA LA UNIVERSIDAD DE SAN BUENAVENTURA - COLOMBIA
3. **AUTORES:** Guillermo Alfonso Nuñez y Jairo David Mesa
4. **LUGAR:** Bogotá, D.C
5. **FECHA:** Marzo del 2014
6. **PALABRAS CLAVE:** IP Contact Center, Central Telefonica, Asterisk, Servidores, Comunicaciones por Voz IP, Software Libre, Linux Centos, IVR, LAN, Dispositivos Administrativos de LAN's.
7. **DESCRIPCION DEL TRABAJO:** El objetivo principal de éste proyecto es diseñar la infraestructura de telecomunicaciones para la operación de un IP Contact Center para la Universidad De San Buenaventura – Colombia. El proyecto se fundamenta en contribuir al diseño de nuevas estrategias y soluciones TIC's que incrementen los recursos de telecomunicaciones para ampliar ventajas y canales de comunicación como lo son (voz, datos, chat, E-mail, etc) con los estudiantes, profesores, miembros franciscanos y la comunidad en general.
8. **LINEAS DE INVESTIGACION:** Tecnologías actuales y sociedad. Sub línea de investigación: tecnologías de información y comunicaciones. Campo de investigación: convergencia y gestión de TIC.
9. **CONTENIDOS:** Análisis y especificación de los requerimientos funcionales y no funcionales de la Universidad San Buenaventura - Colombia con respecto a sus necesidades de comunicación y mercadeo para identificar los recursos de Telecomunicaciones esenciales para la operación de un IPCC. Diseño de la arquitectura física y lógica del IPCC de acuerdo con los requerimientos establecidos, Dimensionamiento de los recursos tecnológicos, para la operación y gestión del IPCC con base en las mejores prácticas establecidas en el mercado y por ultimo simulación de aplicaciones que proporcionan funcionalidades de una central telefónica (PBX) del mercado actual de acuerdo con el dimensionamiento calculado y los requerimientos establecidos.
10. **METODOLOGIA:** Investigación empírico-analítica ya que el diseño propuesto conlleva a toda una serie de procedimientos basados en teorías aplicadas y estudios de pruebas, con los cuales se desarrollará el diseño de una infraestructura de telecomunicaciones para la operación de un IP Contact Center para dar solución a la pregunta trazada a lo largo de éste.
11. **CONCLUSIONES:**

Un IP Contact Center es una solución eficiente que integra varios servicios, y por medio de una infraestructura económica se puede contar una solución que ayude a la universidad a contar con una estrategia adicional para el manejo de contacto con los clientes. Un IP Contact Center es una solución eficiente que integra varios servicios, y por medio de una infraestructura económica se puede contar una solución que ayude a la universidad a contar con una estrategia adicional para el manejo de contacto con los clientes. La plataforma de comunicaciones vía telefónica (3COM NBX 100-V3000) con la que cuenta la universidad para contactar a sus clientes puede ser mejorada con una solución de voz sobre IP como lo es Asterisk, ya que con esta ahorrarían costos, se contaría con escalabilidad y flexibilidad en la parte de gestión de las llamadas. El IVR propuesto ayudara a que los clientes naveguen de una forma cómoda , fácil y en un diferente idioma como lo es el de la opción de inglés, además brindara la unificación de la información entre las diferentes sedes en Colombia , fortaleciendo el nombre al nivel nacional y al nivel internacional para aquellos estudiantes que vienen del exterior.

DISEÑO DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES PARA LA
OPERACIÓN DE UN IP CONTACT CENTER PARA LA UNIVERSIDAD DE SAN
BUENAVENTURA - COLOMBIA

GUILLERMO ALFONSO NUÑEZ
JAIRO DAVID MESA

UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2014

DISEÑO DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES PARA LA
OPERACIÓN DE UN IP CONTACT CENTER PARA LA UNIVERSIDAD DE SAN
BUENAVENTURA - COLOMBIA

GUILLERMO ALFONSO NUÑEZ
JAIRO DAVID MESA

PROYECTO DE GRADO PRESENTADO PARA OPTAR PARA EL TITULO DE
INGENIERÍA DE TELECOMUNICACIONES

TUTOR
INGENIERO ANDRES TORRES

UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2014

Nota de Aceptación

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D. C. Enero 18 del 2014

AGRADECIMIENTOS

Agradecer primero y siempre a Dios por apoyarme en el entendimiento, aprendizaje y entrega en esta parte de mi vida académica, también para aquellos que plantaron en mí, esa voz de enseñanza y apoyo en toda esta marcha académica.

Guillermo Nuñez

Le agradezco a Dios por haberme guiado en este camino, a mis padres Jairo Mesa y Beatriz Helena por siempre apoyarme en todo momento, a mi hermana Lina Mesa por cada consejo de fuerza que en su momento me dio, a mi novia Carolina Gomez por ayudarme con la voces y sobre todo por impulsarme siempre alcanzar mis metas, por ultimo a los profesores que hicieron parte de este trabajo por su tiempo y aportes para que este trabajo cumpliera con los objetivos planteados.

Jairo David Mesa

TABLA DE CONTENIDO

I.	Introducción.....	15
1.	Planteamiento del problema.....	16
1.1.	Descripción y formulación del problema	16
1.2.	Justificación	18
1.3.	Objetivos de la investigación.....	19
1.3.1.	Objetivo general.....	19
1.3.2.	Objetivos específicos.....	19
1.4.	Alcances y delimitaciones del proyecto	20
2.	Marco referencial	21
2.1.	Marco teórico y conceptual	21
2.2.	Teoría general del ip contact center.....	21
2.3.	Funcionamiento de un contact center	22
2.4.	Componentes de un contact center	22
2.5.	Tecnologías involucradas en un contact center	23
2.6.	CRM o customer relationship management.....	24
2.7.	Voz sobre ip	24
2.8.	Ventajas de la voz sobre ip	24
2.9.	Servicios de voz por ip	24
2.10.	Calidad de servicio y seguridad de la voz sobre ip	25
2.11.	Voz sobre ip y las comunicaciones unificadas	25
2.12.	TMO (acdttime+holdtime+acwtime/acdcalls)	27
2.13.	Numeración ani.....	28
2.14.	Asterisk como central telefónica	28
2.15.	Conceptos, configuración y arquitectura de asterisk.....	29
2.16.	Programas de complemento para asterisk.....	31
2.17.	Marco legal	32
3.	Metodología	33
3.1.	Enfoque de la investigación	33
3.2.	Línea de investigación	34

4.	Desarrollo ingenieril.....	34
4.1.	Requerimientos funcionales y no funcionales para la operación de un ipcc en la usb bogotá	34
4.1.1.	Análisis de los requerimientos	37
4.1.2.	Identificación de recursos esenciales	39
4.1.2.1.	Requerimientos tecnológicos físicos	39
4.1.2.2.	Requerimientos lógicos	40
4.1.2.3.	Servicios.....	41
4.2.	Diseño de la arquitectura física y lógica del ip contact center.....	42
4.2.1.	Generalidades	42
4.2.2.	Estrategia de diseño lógico del ipcc.....	43
4.2.3.	Diseño dispositivos de acuerdo a los requerimientos establecidos	46
4.2.3.1.	Router.....	46
4.2.3.2.	Media gateway	46
4.2.3.3.	Switch core.....	47
4.2.3.4.	Firewall.....	47
4.2.3.5.	Proxy	50
4.2.3.6.	File server.....	51
4.2.3.7.	Gestión de servidores linux centos con ssh y webmin	55
4.2.3.8.	Controlador de dominio y directorio activo	57
4.2.3.9.	Configuración estación tele operador (agente).....	59
4.2.4.	Diseño de arquitectura física	59
4.2.4.1.	Diseño cableado estructurado.....	60
4.2.4.2.	Diseño direccionamiento ip	61
4.2.4.3.	Diseño rack de comunicaciones.....	61
4.3.	Dimensionamiento de los recursos tecnológicos para la operación del ip contact center.....	62
4.3.1.	Tamaño	63
4.3.2.	Caso de uso:.....	64
4.3.3.	Capacidad de la infraestructura.....	64
4.3.4.	Soluciones tecnológicas	65

4.3.5.	Solución utilizando la central telefónica administrada con asterisk.....	65
4.3.6.	Dispositivos físicos del ipcc usb bogota.....	66
4.3.7.	Enlaces.....	67
4.3.8.	Estudio de llamadas	67
4.3.9.	Análisis de operación-campaña blend	68
4.3.10.	Estudio de ancho de banda de internet.....	69
4.3.11.	Análisis de operación:	70
4.3.12.	Cálculo del ancho de banda.....	71
4.3.13.	Selección de proveedores.....	73
4.3.14.	Enlaces a contratar	75
4.3.15.	Equipos e instalaciones-mantenimiento concurrente	75
4.4.	Simular aplicaciones que proporcionen funcionalidades de una central telefónica (pbx).....	79
4.4.1	Instalación y configuración de asterisk 1.8	79
4.4.2	Simulación y configuración en asterisk de una central telefónica.	81
4.4.3	Implementación de aplicaciones para la central telefónica.....	92
4.4.4	Análisis de códec y llamadas.....	96
ii.	Conclusiones.....	102
iii.	Bibliografía	104
iv.	Anexos	106

INDICE DE FIGURAS

Figura 1 Número de estudiantes matriculados	17
Figura 2 Número de estudiantes matriculados en las diferentes sedes de la USB .	17
Figura 3 Servicios del IPCC	22
Figura 4 Conexión Digital E1	26
Figura 5 Esquema Conceptual y arquitectura base de Asterisk	29
Figura 6 3Com NBX100 Phone System	36
Figura 7 Diseño de entrada de tráfico del IP CONTACT CENTER USB-BOG	43
Figura 8 Arquitectura <i>Ip Contact Center</i> con LAN actual USB-BOG	44
Figura 9 Entorno SSH Client	56
Figura 10 SSH Client.....	56
Figura 11 Ingreso al servidor por webmin	56
Figura 12 Entorno grafico de Webmin	57
Figura 13 Diagrama de Flujo Controlador de Dominio	58
Figura 14 Diseño de Cableado estructurado	60
Figura 15 Diseño Direcccionamiento IP	61
Figura 16 Diseño RACK de comunicaciones	62
Figura 17 Creación de la máquina virtual en Oracle VM VirtualBox.....	79
Figura 18 Selección de los módulos a instalar	80
Figura 19 Diseño de la simulación de aplicaciones en Asterisk	82
Figura 20 Configuración del archivo <i>Sip.conf</i>	83
Figura 21 Configuración del archivo <i>extensions.conf</i>	83
Figura 22 Configuración del archivo <i>voicemail.conf</i>	84
Figura 23 Configuración del archivo <i>meetme.conf</i>	84
Figura 24 Configuración del archivo <i>extensions.conf</i>	84
Figura 25 IVR simulado	85
Figura 26 Configuración en <i>extensions.conf</i> del IVR y de <i>queues.conf</i> para colas.	86
Figura 27 Configuración del archivo <i>Agents.conf</i>	86
Figura 28 Configuración de los estados de los Agentes.	87
Figura 29 Base de Datos en asterisk	89
Figura 30 Configuración del archivo <i>jail.conf</i>	91
Figura 31 Comando iptables –L para ver las direcciones bloqueadas	91
Figura 32 Consola de monitoreo	93
Figura 33 Consola CDR	94
Figura 34 Comando MixMonitor	94
Figura 35 Comparación en ancho de banda de una llama GSM y otra 729	98
Figura 36 Simulación de llamada entrante hasta llegar al agente	99
Figura 37 Ancho de banda de la llamada	99
Figura 38 Análisis de la llamada.....	100
Figura 39 Pista de la llamada	101

INDICE DE TABLAS

tabla 1 Principales componentes de un contact center	23
tabla 2 Tecnologías involucradas en un contact center.....	23
tabla 3 Dispositivos del ip contact center usb bog-col	45
tabla 4 Firewall tipo hardware.....	48
tabla 5 Firewall tipo software	49
tabla 6 Licenciamiento pago.....	57
tabla 7 Análisis de operación.....	71
tabla 8 Comparación de los diferentes proveedores isp.....	75
tabla 9 Servicios de los diferentes proveedores respecto a la banda ancha	77
tabla 10 Dispositivos administrativos ipcc usb bogotá.....	78
tabla 11 Tabla de encuesta	96
tabla 12 Comparación códec gsm vs 729	97

INDICE ANEXOS

Anexo 1 Carta de autorización para la información de USB	106
Anexo 2 Formato de consulta de información técnica USB	108
Anexo 3 Formato diligenciado de la información técnica USB	109
Anexo 4 Especificaciones técnicas de la PBX 3COM NBX100	111
Anexo 5 Configuración completa de switch core cisco.....	112
Anexo 6 Configuración completa de switch Core Cisco	114
Anexo 7 Configuración del Squid para que el proxy haga las veces de filtrado	115
Anexo 8 Configuración de Sistema Operativo para Agente Tele operador	117
Anexo 9 Equipo Agente Tele Operador.	120
Anexo 10 Dispositivo SW-CORE IPCC USB Bogotá.	121
Anexo 11 Central ASTERISK IPCC USB Bogotá.....	122
Anexo 12 Firewall IPCC USB Bogotá.....	123
Anexo 13 File server y proxy server IPCC USB Bogotá	124
Anexo 14 IDS IPCC USB BOGOTA	125
Anexo 15 Servidor controlador de dominio y directorio activo IPCC USB Bogotá	126
Anexo 16 Planta eléctrica diesel 437-DE16SS.....	127
Anexo 17 Pila de puertos aceptados en reglas del Firewall	128
Anexo 18 ficheros del Firewall.....	129
Anexo 19 Pasos para el diseño del Firewall.....	132
Anexo 20 Diseño y configuración de controlador de dominio y AD	139
Anexo 21 Instalación Flash Operator Panel 2 (FOP2)	146
Anexo 22 Instalación de la aplicación Asterisk-stat.....	150

LISTA DE ABREVIATURAS

AGI	Asterisk Gateway Interface
AMI	Asterisk Manager Interface
ANI	Automatic Number Identification
BRI	Basic Rate Interface
BW	BandWidth
CLIP	Calling Line Identification Presentation
CRM	Customer Relationship Management
CSTA	Computer-Supported Telecommunications Applications
CTI	Computer Telephony Integration
DDI	Direct Dial-In
DECT	Digital Enhanced Cordless Telecommunications
DISA	Direct Inward System Access
DNAT	Destination Network Address Translation
DSP	Digital Signal Processor
DTMF	Dual Tone Multi-Frequency
ERP	Enterprise Resource Planning
EVM	Entry Voice Mail
FMC	Fixed Mobile Convergence / Fixed Mobile Convenience
GPL	General Public License
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPCC	IP Contact Center
ISP	Internet Service Provider
ISPBX	Integrated Services Private Branch exchange
ITSP	Internet Telephony Service Provider
ITU	International Telecommunication Union
IU	Interfaz de Usuario
IVR	Interactive Voice Response
LAN	Local Area Network

LCR	Least Cost Routing
LDAP	Lightweight Directory Access Protocol
LIM	Line Interface Module
MoH	Music on Hold
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
OA	Operadora Automática
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PC	Personal Computer
PoE	Power over Ethernet
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PYME	Pequeña Y Mediana Empresa
QoS	Quality of Service
QSIG	Q Signaling
RDSI	Red Digital de Servicios Integrados
RFC	Request For Comments
RSM	Real Time Service Manager
RTB	Red Telefónica Básica
RTP	Real-time Transport Protocol
RTPC	Red Telefónica Pública Conmutada
SAI	Sistema de Alimentación Ininterrumpida
SDSL	Symmetric Digital Subscriber Line
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TAPI	Telephony Application Programming Interface
TCP	Transmission Control Protocol

TI	Tecnologías de la Información
UDP	User Datagram Protocol
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

I. INTRODUCCIÓN

El contacto con el cliente es una oportunidad de fortalecer la relación entre él y la empresa, además de mejorar la imagen corporativa en los procesos de preventa, venta y posventa. El proceso de asignar personal adecuado al cliente concreto en el momento apropiado es de vital importancia para tener una relación exitosa con él. Si se gestionan correctamente las estrategias de mercadeo hacia los clientes, estos estarán más satisfechos generando fidelización entre ellos, lo cual es mucho más rentable que conseguir otros nuevos.

Lo anterior se puede llevar a cabo con la implementación de un adecuado sistema de gestión de contactos y servicios. Dicha implementación puede ser *In-House* o *Outsourcing* por medio de los servicios de un *Contact Center*, el cual permite que las empresas gestionen eficazmente la interacción con sus clientes y proveedores para generar mejores niveles de aceptación, recordación y entre ellos así como mayor productividad para la empresa.

En este proyecto se diseñó una plataforma de telecomunicaciones para la operación de un *ip Contact Center In-House*, que responde a las necesidades de admisión y PQRS (preguntas, quejas, reclamos y sugerencias) de la Universidad de San Buenaventura – Colombia. El término *In-House* en este contexto significa que dicho *Contact Center* es de propiedad de la universidad y funcionará, seguramente, dentro de sus instalaciones. En el presente documento se encontrará un estudio de cómo adaptar un diseño de una infraestructura física de un *ip Contact Center* en la universidad San Buenaventura sede Bogotá.

La universidad es en sí misma una empresa que al igual que las demás también tiene necesidades en el área comercial o de mercadeo. Mientras una empresa mantiene procesos de preventa, la universidad requiere fortalecer sus campañas de admisión de estudiantes. Por su parte, la gestión que una empresa común haría en el proceso de venta, equivale en la universidad por ejemplo a los procesos de

matrícula e inscripción de materias, entre otros. Finalmente, el proceso de posventa de una empresa se puede homologar a los requerimientos de la universidad para la atención de estudiantes en diferentes áreas, incluyendo por ejemplo la solicitud y expedición de todo tipo de certificaciones y atención de PQRS, etc.

Además de implementar agresivas campañas de mercadeo para la incorporación de nuevos estudiantes a la universidad y apoyo a diferentes proyectos de investigación institucional, un *Contact Center* también permite prestar servicios tercerizados a diferentes clientes entre los cuales se encuentra la comunidad franciscana de Colombia, empresas particulares, generando una nueva fuente de ingreso de gran rentabilidad.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA

La universidad de San Buenaventura sede Bogotá cuenta actualmente con 4.454 estudiantes, la cual no es una cifra muy grande comparada con otras universidades que se consideran en el mismo nivel de competencia por precios, calidad y prestigio. Universidades como la universidad Piloto de Colombia, el Politécnico Grancolombiano, la universidad Jorge Tadeo Lozano y la universidad Militar Nueva Granada que cuentan con 6.596, 13.000, 8.650 y 11.957 estudiantes respectivamente¹, muestran un rezago evidente en la captación de estudiantes para los programas académicos Bonaventurianos. Los datos de matriculados para primer semestre de éstas y otras universidades, entre 2008 y 2011, se encuentran en la Figura 1, y la comparación de los matriculados en las diferentes sedes en la Figura 2.

¹ <http://www.mineducacion.gov.co>, <http://universidades.universia.net.co>

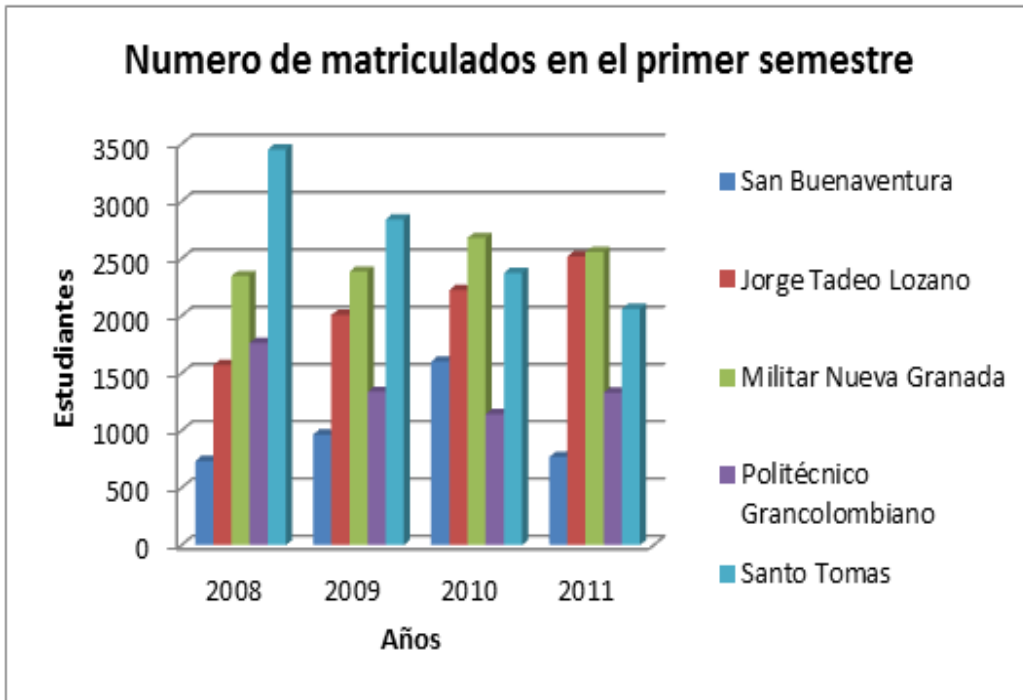


Figura 1 Número de estudiantes matriculados²

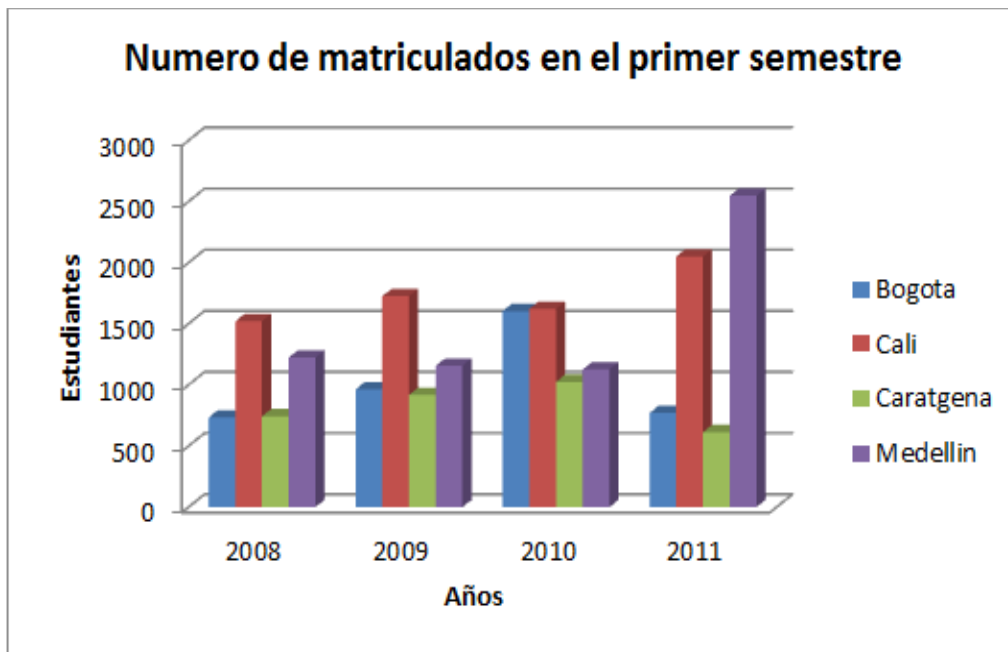


Figura 2 Número de estudiantes matriculados en las diferentes sedes de la USB²

² <http://www.mineducacion.gov.co>, <http://universidades.universia.net.co>

Esta situación ha impulsado al interés de mejorar la calidad institucional para alcanzar los objetivos de crecimiento, posicionamiento y competitividad.³

Para ello se requiere de la implementación de planes de mercadeo más agresivos que ayuden a captar la atención de los estudiantes que están próximos a graduarse de su formación de educación media y sus familias, así como otros aspirantes que están interesados en algún programa académico a nivel de tecnologías, pregrados y posgrados ofrecidos en las diferentes sedes de la universidad.

Una de las más efectivas herramientas para el mercadeo es la atención personalizada en procesos clave para aspirantes, estudiantes y egresados a través de diversos canales de comunicación bidireccional e interactiva como llamadas telefónicas, fax, e-mail, chat, mensajería instantánea, video conferencia, redes sociales, etc. Dicha solución de telecomunicaciones puede ser provista por un *ip Contact Center* que pueda aportar y apoyar al aumento de estudiantes matriculados a los programas educativos de la universidad San Buenaventura-Colombia.

Con todo lo anterior se pretende resolver la siguiente pregunta de investigación:
¿Cuál es la infraestructura de telecomunicaciones necesaria para la *operación In-House* de un *ip Contact Center* que atienda las necesidades de comunicación y sus relaciones con los clientes de la universidad de San Buenaventura Colombia?

1.2. JUSTIFICACIÓN

El interés de este proyecto está dado por la necesidad de buscar nuevas estrategias de telecomunicaciones que ayuden y promuevan cada uno de los programas académicos logrando así una mayor relación y aceptación de los estudiantes en los planteles estudiantiles.

³ <http://usbcartagena.edu.co/index.php/la-universidad/plugins/system/documentos/images/documents/plugins/system/noticias/272-reunion-direccion-de-mercadeo-corporativo>

Los beneficios del proyecto se basan en incrementar los recursos de telecomunicaciones que permitan agregar nuevos canales de comunicación como lo son (voz, datos, chat, E-mail, videoconferencias, redes Sociales, etc) por medio de comunicación Unificada (UC) con los estudiantes, profesores, miembros franciscanos y la comunidad en general.

La utilidad de este proyecto ayudará a la reducción de costos que invierte la universidad anualmente direccionados a la parte de publicidad.

Este proyecto aportará planes de acción para futuros proyectos de investigación, ya que programas académicos como los son Administración de empresas, Ingenierías de Sistemas, Electrónica entre otras, aporten proyectos de desarrollo en sus campos, complementado el *ip Contact Center* para hacerlo eficiente y eficaz para los fines de la Institución. También se podrá prestar el servicio tercerizado logrando una fuente de ingresos extra para la universidad.

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo General.

Diseñar la infraestructura de telecomunicaciones para la operación de un *IP Contact Center* para la Universidad de San Buenaventura – Colombia.

1.3.2. Objetivos Específicos.

- Analizar y especificar los requerimientos funcionales y no funcionales de la Universidad San Buenaventura - Colombia con respecto a sus necesidades de comunicación y mercadeo para identificar los recursos de telecomunicaciones esenciales para la operación de un *IP Contact Center*.

- Diseñar la arquitectura física y lógica del *IP Contact Center* de acuerdo con los requerimientos establecidos.
- Dimensionar los recursos tecnológicos, para la operación y gestión del *IP Contact Center* con base en las mejores prácticas establecidas en el mercado.
- Simular aplicaciones que proporcionen funcionalidades de una central telefónica (PBX) del mercado actual de acuerdo con el dimensionamiento calculado y los requerimientos establecidos.

1.4. ALCANCES Y DELIMITACIONES DEL PROYECTO

El presente proyecto se limita a, diseñar y dimensionar la arquitectura física y lógica de la infraestructura de telecomunicaciones requerida para la operación de un *ip Contact Center* a partir de la identificación, análisis y especificación de las necesidades de canales de comunicación de las relaciones con los clientes de la USB Colombia. Por lo tanto, no hace parte del alcance de este trabajo de grado la implementación de la totalidad o de alguna de las partes o recursos incluidas en el mencionado diseño. Tampoco se contempla el diseño e implementación de campañas y/o estrategias de mercadeo para la USB o sus clientes.

El análisis y especificación de los requerimientos funcionales y no funcionales de la USB Colombia con respecto a sus necesidades de comunicación y mercadeo, así como el diseño de la arquitectura y el dimensionamiento de la infraestructura tecnológica depende necesariamente de la posibilidad de acceso oportuno a la información relacionada con estos aspectos. De no contar con dicha información el proyecto deberá ser realizado con base en supuestos sustentados adecuadamente.

En caso de tener acceso a información de circulación restringida, los autores, el director y los jurados evaluadores del presente proyecto adquieren y aceptan irrevocablemente la obligación de mantener bajo absoluta reserva de confidencialidad cualquier dato suministrado por la Universidad. La publicación y/o

divulgación de dicha información no se podrá realizar sin la autorización expresa de la institución.

Con respecto a las necesidades de mercadeo, este proyecto se centrará únicamente en aquellas que pueden ser resueltas a través del uso de los servicios de un *ip Contact Center* como recurso para la Gestión de Relaciones con los Clientes (CRM).

Una vez diseñada la solución, se propondrá un plan de implementación modular que permita programar los gastos e inversiones necesarios en un plazo de tiempo mayor para intentar ajustarse a posibles restricciones presupuestales.

Debido a la complejidad de realizar una simulación general de un *ip Contact Center* por la interacción de todo un conjunto de soluciones de Hardware y de Software, el presente trabajo realizará una simulación de aplicaciones de Licencia Libre como GPL (Licencia Pública General) vigentes en el mercado de *ip Contact Centers* como lo es Asterisk.

2. MARCO REFERENCIAL

2.1. MARCO TEÓRICO Y CONCEPTUAL

2.2. Teoría general del *IP Contact Center*

Contact Center: El nombre de Centro de Contacto quiere hacer énfasis en el uso de múltiples canales de comunicación que se puede tener con el cliente. Es una aplicación que opera como un *Call Center*, pero utilizando las últimas facilidades de internet (*Call-Back, Chat, E-mail, VoIP, Web Collaboration, etc.*).

Ello permite centralizar en un único repositorio toda la Información de los canales que actualmente se estén utilizando en la empresa. En la Figura 3 se muestra como los diferentes medios de comunicación se Integran en el *Contact Center* y éste se relaciona con las diferentes áreas de la empresa.



Figura 3 Servicios del IPCC⁴

2.3. Funcionamiento de un *Contact Center*

Cuando una llamada llega desde la PSTN (*Public Switched Telephone Network*) pasa a través del *Gateway ip* que convertirá la señal telefónica en paquetes *ip* (protocolos SIP, H.323 entre otros) que serán transferidos a la Centralita *ip*. Si el cliente accede por otros canales, realizará una conexión con el servidor respectivo. El *Contact Center Server* identificará a cada uno de los contactos que han ingresado, así como el medio de comunicación empleado para luego determinar el agente calificado que atenderá a un determinado cliente. Una vez tomada la decisión, se establece la comunicación entre el cliente y el agente pero al mismo tiempo el *Contact Center Server* almacena los datos de la transacción y envía la información del cliente al agente y supervisor respectivo.

2.4. Componentes de un *Contact Center*

Los principales componentes de un *Contact Center* son:

⁴ Diseño propio Autores

Gateway VoIP	Dispositivo que realiza la conversión de la señal de voz tradicional de las llamadas provenientes de la PSTN en paquetes IP (SIP, H.323) y viceversa.
IP-PBX o Centralita IP	Dispositivo hardware o software que se encarga de conmutar el tráfico telefónico de VoIP.
Web Server	Servidor que administra las aplicaciones web y maneja las sesiones de agentes, supervisores y administradores.
Contact Center Server	Software gestor de contactos que selecciona el mejor método para distribuir a los contactos en los grupos de agentes
File Server	Dispositivo que almacena archivos físicos como grabaciones, scripts de emails, sesiones de chat, etc.
Database Server	Dispositivo que contiene una extensa base de datos del sistema, sus configuraciones, y la data histórica de los clientes
Gateway Análogo	Dispositivo que nos permite reutilizar la telefonía tradicional POTS.
IP-Phones o / SoftPhones:	Terminales de los agentes para la realización o recepción de llamadas que pueden ser hardware o software.

Tabla 1 Principales componentes de un *Contact Center*⁵

2.5. Tecnologías involucradas en un *Contact Center*

Universal Queueing	Tecnología por la cual todos los canales y medios de contacto (telefonía, fax, web, mjs, entre otros) son integrados en una misma cola para un procesamiento y manejo estandarizado.
Automatic Call Distributor (ACD)	Sistema diseñado para procesar eficientemente grandes cantidades de llamadas entrantes y asegurar que sean atendidas en un tiempo determinado.
Interactive Voice Response (IVR)	Sistema automático de procesamiento de llamadas programado para responder con mensajes de voz preestablecidos a entradas DTMF del teléfono del cliente. Los IVRs permitirán que el cliente pueda navegar y seleccionar la información deseada.
Speech Recognition	Proceso de convertir un mensaje hablado en texto, con el uso de un sistema capaz de extraer la información lingüística de las emisiones de un ser humano.
Dialers	Sistema que automatiza el inicio y discado de llamadas en un Outbound Contact Center y las conectan a los agentes.

Tabla 2 Tecnologías involucradas en un *Contact Center*

⁵<http://es.scribd.com/doc/43555155/Diseo-e-Implementacion-de-Un-Sistema-Experto-Para-Una-ma-de-Contact-Center>

2.6. CRM o Customer Relationship Management

Básicamente consiste en centrar un modelo de negocio en el cliente y dotar a la empresa de herramientas técnicas que permitan prestar un servicio y comunicación a los usuarios. Es una estrategia de negocio orientada a la fidelización de clientes. Permite a todos los empleados de una empresa disponer de información actualizada sobre los mismos, con el objetivo de optimizar la relación entre empresa/cliente.

2.7. Voz sobre IP

La voz sobre *ip* e Internet Protocol (*IP*) cada vez son más populares entre las empresas y los consumidores. La voz sobre *ip* proporciona una serie de soluciones donde se puede encontrar aplicaciones de comunicaciones unificadas más avanzadas

2.8. Ventajas de la voz sobre IP

La voz sobre *ip* y las comunicaciones unificadas permiten:

- Reducir los gastos de desplazamiento y formación, mediante el uso de videoconferencias y conferencias en línea.
- Permite actualizar el sistema telefónico.
- Tener un número de teléfono que suena a la vez en varios dispositivos.
- Reducir gastos telefónicos.
- Utilizar una sola red de voz y datos, reduciendo costos.
- Acceder a las funciones de su sistema telefónico desde cualquier lugar.⁶

2.9. Servicios de voz por IP

Las funciones de voz sobre *ip* están disponibles en una variedad de servicios, algunos servicios básicos y gratuitos de voz sobre *ip* requieren que todas las partes

⁶http://www.cisco.com/web/ES/solutions/es/voice_over_ip/index.html

estén en sus ordenadores para recibir llamadas. Otros admiten llamadas desde un aparato telefónico tradicional e incluso de un teléfono móvil a cualquier otro teléfono.

2.10. Calidad de servicio y seguridad de la voz sobre IP

La mayoría de los servicios de voz sobre *ip* para el consumidor utilizan Internet pública para realizar llamadas. Pero muchas empresas utilizan voz sobre *ip* y comunicaciones unificadas a través de sus redes privadas. Eso se debe a que las redes privadas proporcionan una seguridad más robusta y una mejor calidad de servicio que Internet.

2.11. Voz sobre IP y las comunicaciones unificadas

Los sistemas de comunicaciones unificadas ofrecen más funciones y beneficios que la voz sobre *ip*. Reúnen todas las formas de comunicación independientemente de su ubicación, de la hora o del dispositivo. Los faxes, correo electrónico y correo de voz se entregan todos en la misma bandeja de entrada. Puede integrar sus sistemas de gestión de relaciones con clientes (CRM) y sus sistemas telefónicos para mejorar el servicio al cliente y mucho más.

Conexión digital E1

La mayoría de las PBX admiten también la conexión a la red pública a través de servicios E1, los que proveen 30 canales de voz o datos de 64 kb/s y un canal de señalización de 64 kb/s.⁷

⁷ *Conceptos de Telefonía Corporativa*-Ing. José Joskowicz - Instituto de Ingeniería Eléctrica, Facultad de Ingeniería - Universidad de la República Montevideo, URUGUAY

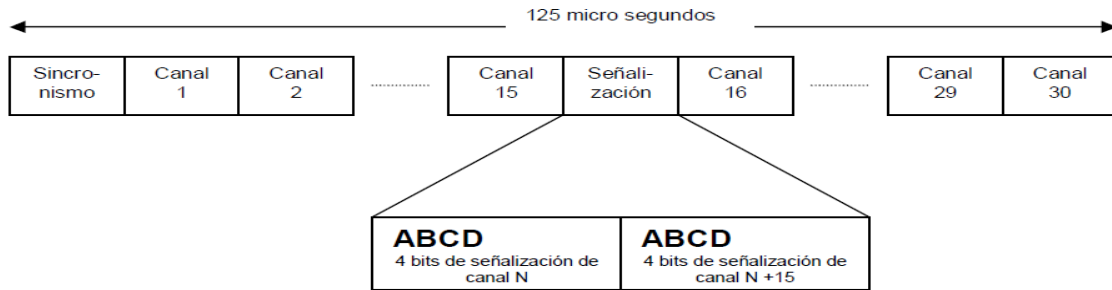


Figura 4 Conexión Digital E1⁸

Cada canal tiene asociado 4 bits (conocidos como bits ABCD) que se utilizan para la señalización de línea (básicamente emulan la señal de campanilla y la corriente de bucle del canal). Cada trama incluye la señalización correspondiente a 2 canales. Cada canal, por tanto, refresca su señalización cada 16 tramas ($125 \mu s \times 16 = 2 \text{ ms}$)

Cada trama es unidireccional, por lo que un enlace E1 cuenta con 2 tramas, una de ida y otra de vuelta.

Los bits ABCD de señalización se utilizan para indicar el estado de la línea. Por ejemplo, cuando el canal N se encuentra libre, los bits ABCD asociados al canal N toman los valores 1011, tanto en la trama de ida como en la de vuelta. Cuando la PBX quiere iniciar una llamada por el canal N, cambia el valor de sus bits ABCD correspondientes al canal N al valor 0011 (Seizure) en la trama de ida. La central pública reconoce la toma de línea con los valores 0011 (Seizure Acknowledge) en la trama de vuelta.

Una vez tomado un canal, la PBX debe discar el número deseado. Esto es realizado mediante la señalización de registro R2 (MFC-R2). Esta señalización consiste en el intercambio de tonos, a través del canal de audio, entre la PBX y la central pública.

⁸ *Conceptos de Telefonía Corporativa*-Ing. José Joskowicz - Instituto de Ingeniería Eléctrica, Facultad de Ingeniería - Universidad de la República Montevideo, URUGUAY

2.12. TMO (acdtime+holdtime+acwtime/acdcalls)

Este dato es de suma importancia en la Gestión diaria de un *Contact Center* ya que es una de las premisas utilizadas para realizar el dimensionamiento, por ende una desviación del TMO puede traer como consecuencia inmediata el incumplimiento de los Niveles de Servicio.

- Acctime: Es el total del tiempo que duran los ejecutivos conversando con los clientes sin contar el Hold.
- Holdtime: Es el total del tiempo que los ejecutivos colocaron al cliente en espera.
- Acwtime: Es el total del tiempo empleado por los ejecutivos posteriores a la llamada (llenar planillas, Encuestas Etc.)
- Acdcalls: Total de llamadas recibidas o llamadas que entraron al ACD y se atendieron. (Leer sobre medición del Nivel de Servicio)⁹

La Suma del ACD+HOLD se denomina Tiempo de Conversación

Para verlo de un Modo más sencillo podemos usar la siguiente fórmula simplificada:

$TMO = ACD + HOLD + ACW$ (si aplica) / Total de Llamadas Atendidas. O

$TMO =$ Total tiempo de conversación / Llamadas Atendidas

Dependiendo del Software que se utilice para el manejo del tráfico de los Call Center (Avaya, Genesys, Software Libre, entre otros) hay muchas opciones para extraer reportes para el manejo de los indicadores.

Algunos reportes traen de una vez calculado el TMO, sin embargo, es sumamente importante conocer de dónde vienen los valores y como se calculan para poder gestionar efectivamente el indicador.

⁹<http://gestiondecallcenter.com/2012/01/31/medicion-de-tmo/>

2.13. Numeración ANI

ANI es el número de teléfono que se envía a la red pública para identificar al llamante. En enlaces digitales se puede seleccionar más de un número para el mismo enlace. El número ANI progresa a través de las distintas centrales hasta llegar al teléfono destino, que podrá identificar el origen de la llamada gracias al ANI. El ANI solo progresa si está en el rango de numeración asignado por la operadora de telefonía.

2.14. Asterisk como central telefónica

Asterisk es una plataforma de código abierto para construir aplicaciones de comunicaciones, funciona como *PBX IP*, *Gateways VoIP*, servidores de conferencia y otras soluciones personalizadas. Actualmente es una de las soluciones más utilizadas en el mercado de las comunicaciones en el sector empresarial, centros de llamadas, el sector de transportes, agencias gubernamentales siendo tentativa por su alcance, robustez y economía.

Hoy en día esta plataforma puede convertirse en la base para un sistema completo de telefonía de una empresa, o ser utilizado para mejorar o ampliar un sistema existente. El proyecto Asterisk comenzó en 1999, cuando Mark Spencer libero el código inicial bajo la licencia de código abierto GPL. Desde entonces, se ha mejorado y probado por una comunidad global de miles de personas. Asterisk brinda una ventaja para construir aplicaciones de comunicaciones, implementar sistemas de teléfono de la empresa (también conocido como PBX), distribuidores de llamadas, puertas de enlace VoIP y puentes de conferencia Asterisk incluye diferentes componentes de bajo y de alto nivel que simplifican considerablemente el proceso de construcción de estas aplicaciones complejas.¹⁰

Asterisk es de código abierto, lo que significa que este puede ser desarrollado, evaluado y mejorado para las necesidades abiertas del mercado de *open source*.

¹⁰ <http://www.asterisk.org/>

2.15. Conceptos, configuración y arquitectura de Asterisk

Las figuras a continuación ilustran el esquema conceptual y la arquitectura base de Asterisk, en la primera se puede observar los protocolos de telefonía ip, tarjetas de comunicación y líneas Digitales. En la segunda, cada uno de los drivers que tiene Asterisk para su correcto funcionamiento.

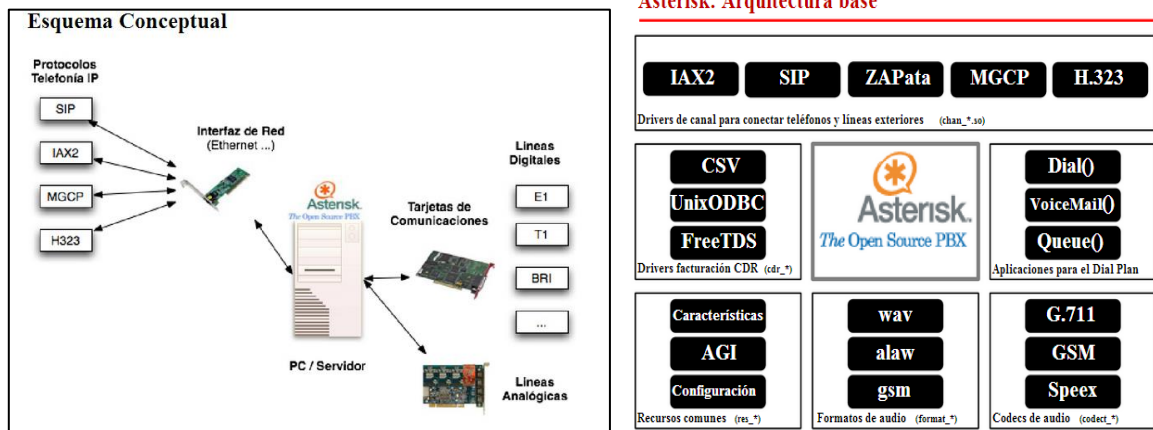


Figura 5 Esquema Conceptual y arquitectura base de Asterisk¹¹

Los archivos más importantes de configuración son los siguientes:

- Asterisk.conf, Sip.conf, lax.conf, Chan_dahdi.conf, Extensions.conf

Para el manejo de las colas en Asterisk se tienen varias estrategias que pueden ser utilizadas.

Ringall: Timbra a todos los canales disponibles hasta que alguno conteste

Leastrecent: Timbra a la interface que hace menos tiempo le colgó la cola

Fewestcalls: Timbra a la interface que menos llamadas ha completado

Random: Timbra aleatoriamente a los miembros de la cola.

¹¹ www.asterisk.org

En la configuración del plan de marcado se tiene que tener en cuenta:

Contextos

- Permiten dividirlo en múltiples segmentos independientes
- Sintaxis: [nombre-del-contexto]
- Permite tener múltiples funciones y que se pueda realizar lo siguiente:
 - 1) Incluir contextos dentro de otros
 - 2) Incluir contextos dependiendo el horario del día
 - 3) Saltar entre contextos

Extensiones

- Una extensión es un conjunto de acciones con nombre
- No necesitan estar atadas a extremos físicos.
- Los identificadores pueden ser numéricos (como una PBX tradicional) o nombres (valores alfanuméricos).

Prioridades

- Dentro de cada extensión, a cada paso le es dada una prioridad numérica (ósea un numero de secuencia).
- Las extensiones pueden estar formadas por muchas prioridades
- En vez de setear las prioridades manualmente, se pueden usar la prioridad 'n' para que la numeración sea asignada de forma automática se cargue el archivo extensions.conf

Aplicaciones

- Cada prioridad en el *dialplan* invoca una aplicación.
- Las aplicaciones realizan el trabajo real:
 - 1) Reproducir sonidos
 - 2) Conectar un teléfono con otro

2.16. Programas de complemento para Asterisk

FLASH OPERATOR PANEL 2 (FOP2)

Asterisk NO cuenta nativamente con un panel que permita ver la actividad del sistema. Por esta razón se recurre a esta herramienta. El panel le permite ver la actividad detallada PBX, como quién está hablando, duración de llamadas, llamadas en espera, llamadas en cola, etc Esto le permite controlar el teléfono y realizar transferencias, hacer un llamado espionaje y susurro, la actividad de cola de pantalla y mucho más¹².

Esta herramienta la pueden utilizar

- Para recepcionistas
- Desarrollado con una recepcionista en mente. Todas las acciones están disponibles en dos clics del ratón.
- Ver quién está disponible o no.
- Transferir directamente a la extensión destino, correo de voz o números externos.
- Capacidad para teléfonos sonando recogida.

Para los supervisores de *Call Center*

- No sólo se puede ver el estado de la extensión, sino también una rápida visión de las colas.
- Ver agentes conectados a una cola.
- Ver estado del agente (en pausa, cierra la sesión, no es válido).
- Vea todas las llamadas en espera en la cola con su temporizador.
- Gestione agentes: añadir, eliminar o miembros colas pausa.
- Lista de extensiones de filtro solo para los miembros de cola con un solo clic.

¹² <http://www.fop2.com/about.php>

FAIL2BAN

Fail2ban es una aplicación escrita en Python para la prevención de intrusos en un sistema, que se basa en la penalización de conexión (bloquear conexión) a los orígenes que intentan accesos por fuerza bruta. Se distribuye bajo la licencia GNU¹³.

2.17. Marco legal

En la parte de *Contact Centers* el conjunto de acciones emprendidas desde la parte legal para el desarrollo de Contact Centers en Colombia, sobresalen por una parte estatus legales que regulan el sector de acuerdo con la agremiación como lo es la Asociación Colombiana de *Call Center* (<http://www.acdecc.org/>), de cierta forma esta asociación presenta prácticas comerciales y operativas de los Contact Centers en adelante (CC) y empresas de tercerización de procesos en adelante (BPO) consideradas como usos y costumbres, moral y éticamente aceptadas dentro del sector.

Lo dispuesto en este Código de políticas¹⁴ fija la pautas sobre las cuales una empresa establecerá su propio código de ética, el cual regirá el ejercicio profesional y socialmente responsable de los servicios directos, agregados y conexos de sus actividades como CC y BPO.¹⁵

Por otro lado la regulación dependerá del tipo de servicio y de campaña que se preste con respecto a si este es de tipo financiero, servicios de telecomunicaciones entre otros.

¹³ <http://www.fail2ban.org>

¹⁴ http://www.acdecc.org/esp/pdf/Codigo_etica.pdf

¹⁵ <http://www.acdecc.org/esp/congreso/programa.php>: Capitulo 1 al 7

3. METODOLOGÍA

3.1. ENFOQUE DE LA INVESTIGACIÓN

Investigación empírico-analítica ya que el diseño propuesto conlleva a toda una serie de procedimientos basados en teorías aplicadas y estudios de pruebas, con los cuales se desarrollará el diseño de una infraestructura de telecomunicaciones para la operación de un *ip Contact Center* para dar solución a la pregunta trazada a lo largo de éste proyecto.

Para el desarrollo inicial del proyecto, se consultará información básica acerca de las herramientas tecnológicas en operación de *Contact Centers* y el uso de estrategias de comunicaciones que utilizan actualmente en las Universidades de San Buenaventura-Colombia para atraer estudiantes a sus programas académicos.

Esta investigación se realizará por medio de cada una de las páginas web, internet, citas agendadas con los encargados los de las áreas de comunicaciones, también por vía e-mail o vía telefónica, para posteriormente acceder y analizar la información solicitada para este proyecto.

Con este análisis e información recolectada se realizará un dimensionamiento basado en los recursos tecnológicos de información y comunicaciones para saber cuántos clientes, equipos, capacidad, canales, se tienen en las instalaciones de la Universidad. El análisis de estos datos utilizará la teoría del telegráfico para así identificar los equipos requeridos y posteriormente realizar un mejor diseño de la arquitectura física y lógica.

La simulación se hará basándonos en el ejercicio de Piloto de Prueba, evaluando y validando las configuraciones realizadas en la Central Telefónica (PBX), además se brindará información del performance de solución PBX para soportar y adaptarse en la realidad a la necesidad de la universidad San Buenaventura Colombia.

3.2. LÍNEA DE INVESTIGACIÓN

LÍNEA DE INVESTIGACIÓN: Tecnologías Actuales y Sociedad.

SUBLINEA DE INVESTIGACIÓN: Tecnologías de información y comunicaciones.

CAMPO DE INVESTIGACIÓN: Convergencia y Gestión de TIC

4. DESARROLLO INGENIERIL

El diseño de la infraestructura de telecomunicaciones será una red de área local paralela a la LAN de la sede de la Universidad San Buenaventura sede Bogotá, por lo tanto esta estará dentro de las instalaciones pero tendrá una administración, gestión y control aparte de la LAN de la USB Bogotá, claro está siguiendo estrictamente las directrices en gestión de contenidos y políticas que requiera la Universidad San Buenaventura.

El diseño contará con la conexión entre la LAN del IPCC y la LAN USB por medio de una VPN, para el direccionamiento y gestionamiento de información del *ip Contact Center*, por lo tanto esta estará mencionada pero estará disponible como opción para hacer parte de una infraestructura de la USB Bogotá (ver Figura 8 Arquitectura *ip Contact center* con LAN actual USB-BOG)

4.1. REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES PARA LA OPERACIÓN DE UN IPCC EN LA USB BOGOTÁ

Como primera opción es necesario analizar y especificar los requerimientos funcionales y no funcionales de la Universidad San Buenaventura con respecto a sus necesidades de comunicación y mercadeo para identificar los recursos de telecomunicaciones esenciales para la operación de un *ip Contact Center*.

Para el desarrollo de esta actividad es creado un formato 001(ver Anexo 3 Formato diligenciado de la información técnica de la infraestructura de comunicaciones con

el cliente de USB Bogotá)¹⁶ y una carta donde se solicita un permiso para poder generar un planteamiento de preguntas de especificaciones básicas y concretas al jefe de soporte de tecnología de la Universidad San Buenaventura Bogotá, estas preguntas abordan temas específicos como el de la arquitectura de red y especificaciones de cómo funcionan los equipos de red actualmente en el servicio de la recepción y salida de llamadas telefónicas internas y externas de la universidad para la gestión de PQRS por parte de los clientes, cuerpo estudiantil y cuerpo docente de la universidad.

Es importante recolectar dicha información, ya que por medio de esta se puede identificar que es posible plantear y aportar una solución de telecomunicaciones que impulse por medio de herramientas TIC's, la comunicación de la universidad San Buenaventura con sus clientes que en si sería todo el cuerpo estudiantil, además de todo un cuerpo Docente y todo una comunidad que requiera consultar información acerca de la Universidad. Toda esta información recolectada estará bajo confidencialidad y será parte del estudio del proyecto de investigación que se está trabajando.

4.1.1. Escenario Actual de la USB BOG

Parte del levantamiento de información del escenario actual de la LAN de la USBBOG se centró especialmente en las soluciones que soportan la parte de dispositivos de comunicaciones que tiene actualmente la universidad, debido a que la infraestructura de IPCC será paralela en la parte de dispositivos de red con los de la Universidad.

La universidad cuenta actualmente con una plataforma de recepción y salida de llamadas telefónicas de 250 extensiones internas¹⁷, donde las llamadas locales de entrada y salida que no pasan directamente a la extensión son recibidas por la recepción. La salida de llamadas a números especiales, nacionales, internacionales

¹⁶ Formato 001-anexos –preguntas básicas sobre arquitectura de red

¹⁷ Dato 22 de Abril del 2013 formato 001

y celular salen por Recepción. A su vez en campañas especiales se dan permisos específicos a promoción, admisiones y a las Facultades.

La Universidad San Buenaventura sede Bogotá cuenta actualmente con un dispositivo hardware PBX de referencia 3COM NBX 100-V3000. El sistema telefónico NBX 3Com 100¹⁸, ofrece los beneficios de la voz sobre IP (VoIP) y mensajería de voz avanzado - sin los altos costos y la complejidad operativa de TDM PBX o sistemas de propiedad intelectual. Dentro de sus especificaciones técnicas más importantes se encuentran:



Figura 6 3Com NBX100 Phone System¹⁹

Sistema operativo Wind River VxWorks y Soporta hasta 250 dispositivos.
Entre sus aplicaciones principales están: correo de voz, operadora automática, grupos de llamadas, trasferencias, correo electrónico.
Compatible con una amplia gama de 3Com y productos de terceros.

En la parte de troncales de líneas se cuenta con 1 Troncal E1 y 4 celufijos, tipo de entradas PSTN con tipo E1, en la producción del dispositivo actual no se cuenta con VoIP por lo tanto este proyecto de investigación aporta favorablemente la solución en caso de que en el futuro se integre una Solución de VoIP el IP Contact Center.

El dispositivo hardware no posee un ACD Automatic Call Distributor (Distribuidor Automático de Llamadas) desde el punto de vista de la telefonía como su nombre lo indica, realiza el enrutamiento de la llamada entrante hacia los terminales correspondientes que utilizan los operadores. El módulo ACD es una herramienta que al tener por función el enrutamiento de las llamadas, es perfecto para centrales telefónicas o PBX que manejen amplio caudal de llamadas entrantes, como lo es

¹⁸http://www.3comphones.com/3com_nbx100.htm

¹⁹http://www.3comphones.com/3com_nbx100.htm

en este caso el IP Contact Center. En realidad, la situación ideal para emplear el módulo ACD es aquella en que el cliente que llama no necesita hablar con alguien en particular, sino simplemente requiere asesoramiento de cualquiera de los múltiples agentes que trabajen en la misma plataforma y para el mismo servicio, situación básica que puede cubrir el IP Contact Center.

Actualmente la universidad NO cuenta con un sistema de grabación, en respaldo de este cuenta solo con grabación para mensajes de voz, el estudio de este proyecto brinda soluciones de módulos de grabación donde cada llamada será grabada, si se realiza por otra clase de servicios se hará un constante manejo de reportes de respaldo por medio de un servidor de tickets como por ejemplo en el caso de una solicitud vía chat, o mensajes por correo.

4.1.1. Análisis de los requerimientos

Luego de obtener la información del departamento de soporte tecnológico, el Formato 001(ver Anexo 3 Formato diligenciado de la información técnica de la infraestructura de comunicaciones con el cliente de USB Bogotá) nos ayuda a identificar los recursos TIC esenciales y los requerimientos funcionales y no funcionales que se adaptarán para el diseño de la infraestructura física y Lógica del *ip Contact Center*.

El formato 001 brinda la posibilidad de adaptar paralelamente el diseño de una infraestructura de Telecomunicaciones que ayude e impulse el contacto por medio de soluciones TIC's a los clientes de la universidad. El acompañamiento telefónico, correo, chat, redes sociales para la formulación de requerimientos o necesidades que generalmente presenta el estudiante y el interesado en el día a día del proceso de formación académica.

De acuerdo a la baja cantidad de estudiantes en comparación a las otras universidades (ver Figura 1 Número de estudiantes matriculados), la USB Bogotá

deberá aumentar la demanda de estudiantes matriculados a sus programas académicos; actualmente la Universidad no cuenta con una infraestructura dedicada exclusivamente y con el rol específico en impulsar la atención y el contacto a los clientes (estudiantes, Docentes- interesados).

El proceso de investigación adaptará requerimientos funcionales que actualmente son importantes para la universidad, como son los siguientes:

- La información de contenidos como lo son programas académicos, admisiones, apoyo académico, y portal Universitario todo ello por medio de las páginas de la universidad y por medio de llamadas telefónicas como se hace actualmente.
- Es de vital importancia que la Universidad siga contando con su cuerpo o departamento de desarrollo de aplicaciones que complementara el trabajo de los tele operadores el cual alimentarán la base de datos por medio de los registros creados en cada llamada o solicitud realizada por cada medio ya sea por correo, chat, redes sociales o siendo de prioridad la parte del contacto telefónico.
- La base de datos y la información donde se ven reflejados los atributos de todo su cuerpo estudiantil activo y no activo de todo su historial académico en todos los diferentes programas de pregrado, posgrado entre otros.
- Pagos en línea por medio de las páginas de la universidad.
- Seguimiento de PQRS donde los estudiantes activos, envían correos para la solución de inconvenientes esenciales, como lo son Aulas virtuales, creación de contraseñas para medios interactivos, correos entre otros.
- Biblioteca en Línea es una opción funcional que hará parte de las opciones del estudiante, donde el podrá por medio de la página, correo, chat o una llamada solicitar material de consulta para sus necesidades académicas.
- Él envió de mensajes de correo donde se informa actividades de la agenda estudiantil.

4.1.2. Identificación de recursos esenciales

Se identificaron recursos físicos y lógicos esenciales donde el diseño de la infraestructura de telecomunicaciones puede aportar en ampliar servicios que complementen y ayuden a la apropiada asistencia de PQRS de los clientes de la Universidad, estos son los siguientes:

4.1.2.1. Requerimientos Tecnológicos Físicos

Para la operación de un IPCC es importante identificar cuáles son los requerimientos funcionales físicos, para ello parte del análisis de necesidades fue especificar y proponer una infraestructura modular, donde se tuviera en cuenta cada dispositivo físico en su diseño para ello también se identificó la importancia de cada una de estas soluciones de telecomunicaciones y se propuso su dimensionamiento en el diseño de infraestructura, a continuación se identifica las soluciones físicas más representativas en las redes LAN convencionales utilizadas para la parte de Contact Center :

- a) Router: dispositivo referenciado por el ISP para encaminamiento de la información.
- b) Switch: requerimiento necesario para la segmentación de la red LAN.
- c) Firewall: requerimiento necesario para bloquear acceso no autorizado a la LAN.
- d) Proxy: requerimiento necesario para la interceptación de conexiones de la red LAN.
- e) Controlador de Dominio- Directorio Activo: requerimiento necesario para asignar dominio de la LAN, asignación de usuarios, perfiles y políticas necesarias para brindar seguridad en la parte local de la LAN.
- f) File Server: requerimiento necesario para que se deposite e interactúe información confidencial de asignación de tareas definidas por roles, DB, entre otros y sean almacenados según perfiles y permisos.

- g) Central Telefónica (PBX): requerimiento necesario para la gestión de llamadas entrantes y salientes del IPCC.
- h) IDS: requerimiento necesario para la identificación de intrusos en la LAN
- i) Rack: requerimiento necesario para almacenar dispositivos físicos necesarios para la operación del IPCC.
- j) Planta Eléctrica: requerimiento necesario para brindar respaldo eléctrico a la operación del IPCC.
- k) Computadores: requerimiento necesario para operación de usuarios finales
- l) Diademas (headsets): requerimiento necesario para la atención al cliente.

4.1.2.2. Requerimientos lógicos

Para la operación de un IPCC es importante identificar cuáles son los requerimientos funcionales lógicos que harán parte del diseño de la infraestructura, para ello parte del análisis de necesidades fue especificar y proponer soluciones de bajo costo y de software libre que actualmente se implementen en el mercado empresarial, además también de identificar la importancia de cada una de estas soluciones de telecomunicaciones y su configuración que es abordada en el segundo objetivo del proyecto de Investigación; a continuación se identifica las soluciones lógicas más representativos en las redes LAN convencionales utilizadas para la parte del IP Contact Center :

- a) Sistema Operativo: requerimiento lógico necesario para el funcionamiento de los dispositivos administrativos como proxy, firewall, file server, IDS, central telefónica entre otros, estas soluciones lógicas están basadas en sistemas operativos derivados de distribuciones de Linux como y que en virtud de estas son de distribución libre, pero totalmente viables para el propósito empresarial como lo sería el caso del IPCC.
- b) Sistema de PQRS basada en tickets ya que nos brinda una lectura real del tiempo de solución de inconvenientes que requiere el cuerpo estudiantil, docentes entre otros vitales para el día a día en las tareas de la Universidad.

- c) Canal de internet de voz (E1): requerimiento necesario para la parte de voz del IPCC garantizando calidad de servicio en la parte de Voz.
- d) Canal de internet dedicado (datos): requerimiento necesario para trabajar y garantizar la parte de datos(Internet, mail, chat, redes sociales, intranet)
- e) Herramientas de monitoreo, control y administración para gestionar de una apropiada forma el funcionamiento del IPCC. Ejemplo: pingplotter, fileserver, syslog, Cisco Network Assistance.
- f) Sofphone para que el tele operados realice o reciba las llamadas
- g) Licencias de Antivirus para seguridad local de estaciones
- h) Software de monitoreo o Supervisión para verificar control y estadísticas de llamadas del IPCC. Llamadas.
- i) Editores de texto para verificación de contenidos y entrega de informes: ejemplo: openoffice

4.1.2.3. Servicios

- a) La adaptación de servicio de solicitud en línea donde el estudiante no tenga que dirigirse a pedir personalmente un salón o un periférico, si no que en solución a este lo haga por medio del IP Contact Center, donde existirán diferentes servicios disponibles para que esta solicitud se agende.
- b) El contacto telefónico será el fuerte de este diseño, ya que estará acondicionado para llevar a cabo campañas de marketing que promuevan los programas académicos de la Universidad.
- c) Servicio de línea inteligente (IVR) para que el interesado elija la opción donde desea realizar las PQRS.
- d) Servicio de Grabación de llamadas para hacer control de calidad en la asistencia al cliente.
- e) Servicio de encuestas para desarrollo de estadísticas de mercado.
- f) Servicio vía telefónica para ayuda de pagos en líneas de cualquier eventualidad de pago que requiera hacer el estudiante.
- g) El IPCC adaptara servicio en paralelo de actualización de inquietudes e información de actividades de agenda estudiantil por las diferentes opciones de redes sociales que se trabajan actualmente.
- h) Servicio de línea inteligente para consulta de información. Ejemplo: clave del aula virtual.

El departamento de Soporte tecnológico, el departamento de desarrollo de aplicaciones estarán asociados y serán importantes para retroalimentación de la información y la incorporación de las soluciones unificadas donde se construirá un resultado satisfactorio a cualquier necesidad del solicitante sin importar su perfil.

4.2. DISEÑO DE LA ARQUITECTURA FÍSICA Y LÓGICA DEL IP CONTACT CENTER.

4.2.1. Generalidades

Para el desarrollo de este objetivo es primordial ya haber indagado información útil acerca de la Universidad, de cómo esta gestiona la atención al cliente, de qué es funcional y qué no lo es, de cómo se puede introducir paralelamente una infraestructura que trabaje de la mano con la universidad gestionando la información unificadamente, y de cómo este proyecto puede tener una disposición de telecomunicaciones que cumpla con el objetivo de un diseño que contenga toda una infraestructura y que cumpla el perfil de *Contact Center* para la atención a los clientes de la Universidad.

Como principal medida, se describe como sería el encaminamiento de una llamada, de cómo cada dispositivo administrativo va hacer parte de un conjunto de soluciones para garantizar la integridad de la información y de cómo este puede responder a la demanda de contactos por los diferentes medios con los clientes.

Para conocer más puntualmente cual será el recorrido de una llamada podemos tomarlos de la siguiente forma: Cuando una llamada llega desde la PSTN pasa a través del Media Gateway IP que convertirá la señal telefónica en paquetes IP (protocolos SIP, H.323 entre otros) en el caso del proyecto será el adoptado SIP o Protocolo de Inicio de Sesiones. Estos paquetes por ultimo serán transferidos a la PBX o Central Telefónica donde se llevara a cabo un orden de llegadas de llamadas a lo que se llama en la teoría “colas o encolamiento de llamadas”.

La central telefónica identificará a cada uno de los contactos que han ingresado, y en su momento el IVR hará la introducción del *script* para dar encaminamiento a la llamada hacia su destino, así como el medio de comunicación empleado para luego determinar el agente calificado que atenderá a un determinado cliente. Una vez tomada la decisión, se establece la comunicación entre el cliente y el agente pero al mismo tiempo la central telefónica almacenará los datos de la transacción y enviará la información del cliente al agente y supervisor respectivo.

Para el diseño de la arquitectura física y lógica del *ip Contact Center* se tendrán en cuenta los siguientes requerimientos establecidos: estrategia de diseño lógico del IPCC, Diseño Lógico de Dispositivos y por último Diseño de Arquitectura Física. El *ip Contact center* estará paralelamente a la parte de la red LAN de la Universidad, pero este contará con su propia arquitectura en la parte física y en la parte Lógica a continuación se abordará la estrategia de Diseño del IPCC:

4.2.2. Estrategia de diseño lógico del IPCC

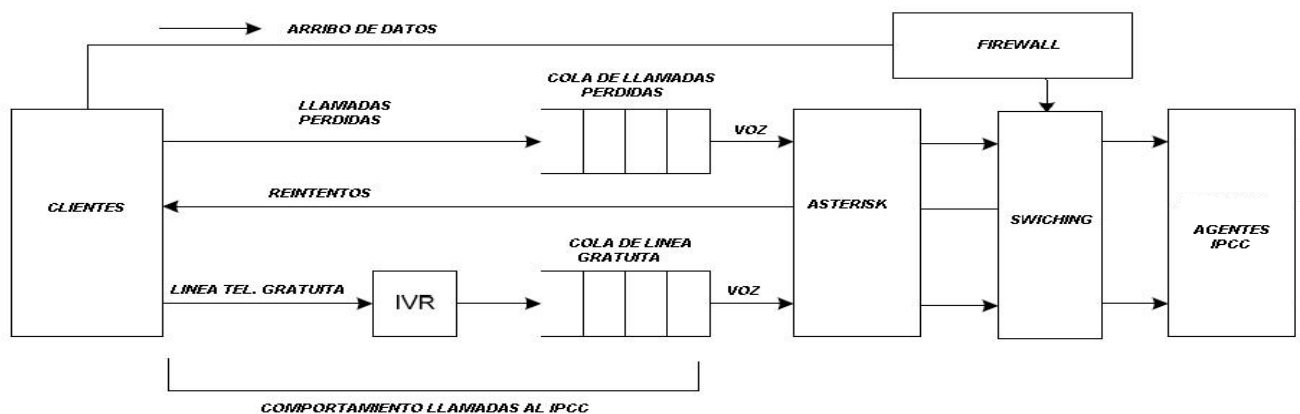


Figura 7 Diseño de entrada de tráfico del IP CONTACT CENTER USB-BOG²⁰

La grafica de diseño de entrada de tráfico nos ilustra el encaminamiento del tráfico de voz pasando desde el cliente, luego pasando por el IVR y el comportamiento de las colas por los respectivos dispositivos que se encargan de la gestión para que

²⁰ Grafica elaborada por Guillermo Nuñez y Jairo Mesa

estas lleguen a los agentes quienes son las personas encargadas de atender este tráfico de voz.

En la Figura 8 se puede observar la RED LAN de la Universidad San Buenaventura en la parte izquierda exponiéndola como un ejemplo de red y al lado derecho de esta está el diseño de la arquitectura de red del IPCC de la Universidad San Buenaventura, como lo muestra la Figura 8:

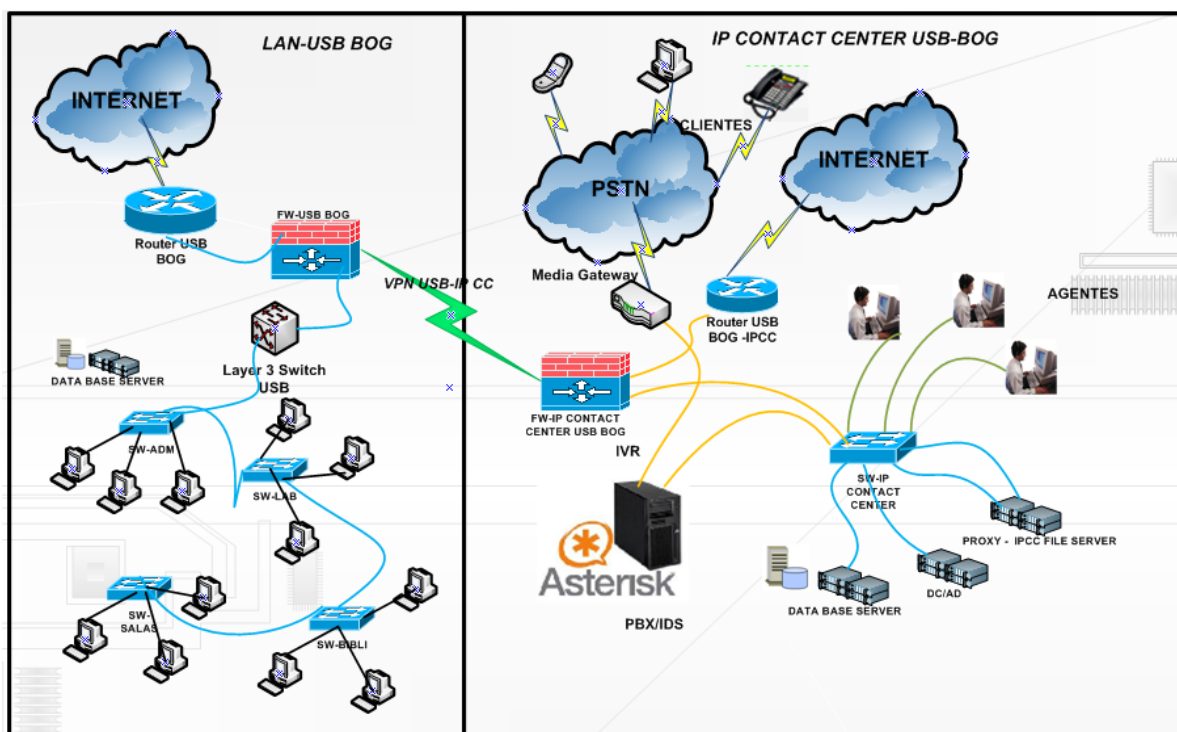


Figura 8 Arquitectura *Ip Contact Center* con LAN actual USB-BOG²¹

Se tomarán en cuenta los siguientes dispositivos administrativos que harán parte de la infraestructura del IPCC, y que en la actualidad son utilizados para el mercado de *Contact Center* que son necesarios, para brindar flexibilidad, calidad, respaldo, seguridad e integridad a la información.

²¹ Grafica elaborada por Guillermo Nuñez y Jairo Mesa

Dispositivos administrativos IPCC USB Bogotá			
Dispositivo	Función	Características	Observaciones de Funcionamiento
Router	Encargado de enrutar los paquetes de datos y Voz	Dispositivo arrendado por el ISP, gestionado por el ISP	Este SO o IOS es gestionado por el ISP con algunas condiciones técnicas del cliente
Media Gateway	Dispositivo de traducción o servicio que convierte secuencias de medios digitales entre las redes dispares como PSTN, SS7, Next Generation Networks (redes 2 G, 2.5g y 3 G radio acceso) o PBX	Dispositivo arrendado por el ISP, gestionado por el ISP	OS según el Propietario
Switich Core	Encargado de la conectividad de los servidores u usuarios por medio de VLAN´s	Dispositivo CISCO , gestionado por el administrador de red por SSH	IOS Cisco V12.2
Central Telefónica Asterisk	Central telefónica del IPCC , encargada de recibir el tráfico de Voz y gestionar sus directrices	Equipo HP Proliant ML110 G7 Gestionado por el Administrador con conocimientos en Asterisk	OS Linux , Asterisk
Firewall	Encargado de la seguridad del IPCC y de establecer VPN a la LAN de la USB	Equipo HP Proliant ML110 G7	OS Linux , Centos
File Server	Encargado de almacenamiento de datos del IPCC	Equipo HP Proliant ML110 G7	OS Linux , Centos +webmin
IDS Server	Encargado de la detección de intrusos y detectar accesos no autorizados la red del IPCC	PC Desktop HP Compaq Pro 6000	OS Linux , Centos +webmin
DC/AD Server	Encargado de gestionar el controlador de Dominio y el directorio activo , importante para la gestión de políticas para los usuarios del IPCC	Equipo HP Proliant ML110 G7	Licencia Microsoft Server 2008 st/ 2012 st+ Licencias Cal
PROXY Server	Encargado de interceptar las conexiones de red hacia un servidor destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.	Equipo HP Proliant ML110 G7	OS Linux , Centos +webmin
Data Base Server	Encargado de gestionar y ejecutar datos privados de la USB correspondientes al uso de un aplicativo por ejemplo un CMR	Equipo HP Proliant ML110 G7	OS Linux , Centos +webmin

Tabla 3 Dispositivos del Ip Contact Center USB BOG-COL

4.2.3. Diseño dispositivos de acuerdo a los requerimientos establecidos

A continuación se relaciona los dispositivos administrativos que harán parte del diseño de la infraestructura del IPCC que son necesarios para la infraestructura del IPCC y que en su selección para el diseño fueron seleccionados para que cada uno de ellos brinde un trabajo específico en la operación de la LAN:

4.2.3.1. Router

Dispositivo de capa 3 esencial para toda empresa que requiere trabajar con contenidos de internet o que en su finalidad sea trabajar con Voz IP; Es primordial este dispositivo en el diseño ya que el canal de datos serán conectado a este dispositivo por alguna de sus interfaces y será útil para el encaminamiento de los paquetes en la red. La configuración de este dispositivo está gestionada por el proveedor de servicios de Internet y el recomendará cual es el equipo a disposición para el servicio, generalmente son de marca CISCO.

El IPCC requiere su segmento de 4 direcciones IP donde se garantice cumplimiento de 99.6% de estabilidad de los servicios en ultimo 4 de milla y cumplimiento de fallas en el menor brevedad no mayor a 1 hora.

4.2.3.2. Media Gateway

Dispositivo que se encarga de la traducción o conversión de secuencias de medios digitales entre las redes como PSTN, SS7, o redes de nueva generación como redes 2 G, 2.5g y 3 G radio acceso o PBX. Estará encargado de distribuir la comunicación por el protocolo SIP a la Central Telefónica, permitiendo también la comunicación de los diferentes tipos de redes, uno de sus principales funciones es convertir entre diferente transmisión y codificación técnicas o también llamado *transcoding*, este dispositivo será gestionado en su instalación por el proveedor de servicios de internet ISP.

4.2.3.3. Switch Core

Dispositivo de capa 2 o capa 3 , gestionado por el administrador de la LAN del IPCC importante para el IPCC ya que en este se realizarán labores de configuración de las *Vlan*'s, para segmentar dominios entre diferentes perfiles como lo será, el tele operados, el supervisor, BackOffice entre otros de staff administrativo, este tendrá configuración de troncales para los servidores, y su gestión se hará por SSH para fortalecer su seguridad, su configuración por su extensión paso a paso se encuentra en el Anexo #5.

4.2.3.4. Firewall

El firewall es un dispositivo importante hoy en día para las redes LAN de las compañías, ya que este dispositivo controla los datos que entran y salen en la red, además de configuraciones de Filtrado de paquetes de datos, Filtrado por aplicación, Reglas de filtrado, VPN's, VoIP, QoS, Security, Gateway Filtering, entre otros. Su ubicación siempre es recomendable que sea entre la red externa (WAN) y la red interna (LAN), además de saber que alcance y seguridad nos puede brindar el firewall es necesario saber cómo se gestionara , en la actualidad se encuentran en el mercado dos tipos de firewall, estos son los de tipo software y los de tipo hardware llamados también (Appliances), el mercado de los firewall de hardware son una buena opción porque ellos brindan entornos amigables para el administrador , son granulares y flexibles a la hora de configurarlos pero sus costos son la desventaja, a continuación se nombrara firewall's representativos del mercado que hacen parte de la familia SOHO (small office/home office) que pueden ser adaptables al IPCC pero que en su costo representan una desventaja para el presupuesto del diseño que se planteara:

<i>Firewall Hardware (Appliance)</i>	<i>Vendor</i>	<i>Arquitectura</i>	<i>Valor Aprox (USD)</i>
Sonicwall XPRS2	Sonicwall	Filtrado de paquetes/ Dual-Homed Host/ Screened Host Screened Subnet (DMZ)	620
VPN Firewall Brick 20	Lucent Technologies	Filtrado de paquetes/ Dual-Homed Host	810
Contivity 600	Novel Networks	Filtrado de paquetes/ Dual-Homed Host/	710
Firebox 1000/2500	Watchguard Technologies	Filtrado de paquetes/ Dual-Homed Host/ Screened Host Screened Subnet (DMZ)	720
FireWall-1 de CheckPoint Software	CheckPoint Software	Filtrado de paquetes/ Dual-Homed Host/ Screened Host Screened Subnet (DMZ)	810

Tabla 4 Firewall tipo Hardware

Por el lado de la familia de Firewall de tipo Software se encuentran los integrados a los sistemas operativos como en sistemas operativos licenciados como es en su caso Windows (Xp, W7, etc), pero también se encuentran en el mercado competitivo los firewall tipo software libres embebidos en sistemas operativos como lo puede en distribuciones o modificaciones de Unix y Linux. Para la realización del proyecto de investigación el firewall que se planteara estará bajo un diseño de tipo software libre sin pago; ya que las soluciones de la infraestructura estarán basadas en bajo costo pero de igual forma competitiva en el mercado, esto implica también que sean modulares, flexibles y principalmente cómodos para la primera inversión de presupuesto.

La decisión de seleccionar software de distribución libre depende en gran medida la seguridad que se quiere conseguir también, por lo que hay que tener gran cantidad de factores en cuenta, desde el nivel de seguridad que se quiere alcanzar realmente, hasta el tiempo que se puede emplear en la puesta en marcha del sistema y en el caso de poner uno de pago, también hay que tener en cuenta el presupuesto disponible.

Los Firewall de software pago tienen el defecto de que si se descubre una vulnerabilidad en lo cual no es nada normal, tarda bastante en resolverse, mientras que los software libres están en continuo testeo y reparación, con ello podemos

concluir que lo más viable para este proyecto es un firewall de software libre NO pago, a continuación se presenta un cuadro de las clase de Firewall tipo software:

Sistema Operativo	Distribución	Maquina	Tipo	Licenciamiento
GNU/Linux	Centos ,Mandriba, Osuse,Ubuntu,ClearOS, Gibraltar, IPCop, Zentyal, SmoothWall,FreeBSD, etc.	Dedicada	TORRE SERVIDOR	libre
Unix(modificación)	Unix	Dedicada	TORRE SERVIDOR	pago

Tabla 5 Firewall tipo Software

La propuesta de diseño para el firewall del IPCC está basada en las siguientes características:

- Se aplicará una maquina dedicada tipo torre (Servidor) (ver capítulo de dimensionamiento de infraestructura).
- La solución de Firewall estará Basadas en: GNU/Linux: CentOS modo básico (gestión por consola de comandos)para la optimización de recursos
- Firewalls direccionado al filtrado de paquetes sobre la pila de protocolos TCP/IP.
- Su objetivo será filtrar las comunicaciones en ambos sentidos entre su interfaz interna que es la que se conecta a la red LAN y la externa que conectará a la WAN.
- El tráfico de voz no pertenecerá a la inspección del firewall por lo tanto esta será regla de excepción.
- Se agregará complemento NAT (Traducción de Dirección de Red) ya que el ISP entrega una direccionamiento IP público restringido en 4 IP´s, y el IPCC requiere direccionamiento interno para su funcionamiento y el inspeccionamiento de tráfico entrante y saliente.
- Se utilizará el complemento IPTABLES utilizando Shorewall, trabajando principalmente argumentos ACCEPT, REJECT y DROP, respectivamente.
- El mecanismo de funcionamiento para realizar este filtrado es a través de una lista de reglas. Las reglas, pueden ser de dos tipos; de aceptación y de

rechazo, éste última se descompone en dos subtipos, es decir, en términos de aceptación, rechazo y denegación.

- La lista de reglas de entrada del exterior hacia la red LAN interna es totalmente independiente de la lista de reglas de filtrado de salida de la red hacia WAN.

Para observar configuración de Ficheros de Firewall y pasos de instalación y diseño ver Anexo 18 y 19.

4.2.3.5. Proxy

El proxy es necesario para interceptar las conexiones de red, bloquear contenidos, control de tráfico y aceptación de filtrado por URL que se determinan según los perfiles, estos son por ejemplo el de los administrativos y uno general para los tele operadores, el proxy realizara la tarea de autenticación y/o validación de uno o varios equipos para permitir o bloquear la salida hacia internet.

Para el diseño del proxy se tendrá en cuenta al igual que el diseño del firewall la disposición de sistema operativo de distribución libre y se implementara en una maquina dedicada tipo torre-servidor, donde se seguirán los siguientes pasos:

1. Instalación de distribución de Linux "Centos 6.4" basada en Red Hat Enterprise.
2. Con el medio de instalación (cd) se inicia el sistema como prioridad de inicio.
3. Luego se seleccionará el idioma del Sistema Operativo y del teclado.
4. Después descargar todos los archivos de configuración saldrá un aviso como "Congratulations, your CentOS installation is complete", en donde se seleccionar Reboot, para reiniciar el sistema.
5. se ingresará con el usuario *root*, con las respectivas credenciales.
6. Se actualiza el sistema operativo con el comando "yum -y update". Luego se instalara el módulo de squid con el comando "yum -y install squid" .

7. Después de instalado el módulo de squid, se debe ingresar al fichero de configuración con el comando: "vim /etc/squid/squid.conf"
8. Después de ingresar al fichero de configuración del Squid hay que realizar una serie de modificaciones para que el proxy haga las veces de filtrado como se ilustra en el Anexo 7.
9. Después de modificar el fichero de squid.conf se procede a iniciar el servicio.
10. Por último para configurar el proxy por definición para los tele operadores del IPCC se hará por medio del Servidor de directorio Activo definiéndolo en las políticas de servidor proxy para que este quede aplicado por política.

Para la administración y gestión de los servidores es recomendable usar ssh Client apuntando a su dirección IP, pero configurando un puerto diferente al 22 que es el *Default* además de configurar el servicio de Openssh-server en el servidor proxy, el firewall y el IPCC File-server que están bajo distribución de Linux con Centos; para ello se tiene que digitar el siguiente comando luego de estar por consola localmente el usuario *root*:

- nano/etc/ssh/sshd_config

Luego de este se elige el puerto que se configurara que no sea el 22, en este caso puede ser el 5011.

- port 5011

Luego de esto se reinicia el servicio ssh con el siguiente comando:

- /etc/init.d/ssh restart

4.2.3.6. File Server

El file server será una solución que brindara el resguardo de información por autenticación, compartición de datos por asignación y reposo de datos. Para la instalación del File server se debe tener en cuenta que esta estará configurado bajo el mismo dispositivo físico dedicado tipo torre donde se encuentra configurado el PROXY, por lo tanto este estará bajo la línea de comandos o si es preferible

también se puede configurar con ambiente gráfico, con la opción de ser administrado remotamente por medio del protocolo https seguro y de modo grafico por el módulo webmin puerto 10000.

Para agregar el módulo de servidor de archivos se agregará una interface más o tarjeta NIC funcionará como se mencionó anteriormente para almacenar y compartir documentos bajo un mismo entorno, además con la opción de compartir impresoras, para esto se debe tener en cuenta los siguientes pasos:

Luego de realizar la configuración de centos como se indicó en la configuración del Proxy, se verificara en la consola de comando los siguientes módulos a instalar:

- `etc / samba / smb.conf`

Luego de realizar la instalación por comando se reiniciara el servicio con el siguiente comando:

- `service smb restart`

Como el servidor samba estará bajo un grupo de usuarios de Windows o más bien este hará parte de un dominio, se debería modificar las líneas siguientes líneas de comando:

- `etc / samba / smb.conf`
- `workgroup=ipccusb.bog`
- `server string = brief comment about server # Este seria opcional ##`

Para crear un directorio compartido samba en un entorno Linux, se debe proceder a editar el `smb.conf` y modificar una información según las necesidades que se debe aplicar al servidor de Archivos como lo requiera el IPCC, estos son los siguientes:

```
[Nombre de recurso compartido] ## Aquí se modificara al nombre de share-  
ipccusb##  
Comment = Inserte un comentario aquí  
Path = /home/share/share-ipccusb  
Válida usuarios = agente01 agente02  
Pública = no  
Writable = sí  
Printable = no
```

El ejemplo anterior permite a los usuarios agente01 y agente02 leer y escribir en el directorio /home/share/share-ipccusb, en el servidor samba, desde un cliente samba.

Configuración de Contraseñas Encriptados

Las contraseñas encriptadas son activadas por defecto por motivos de seguridad en el caso de Windows XP que será el sistema operativo a utilizar por los tele operadores requiere contraseñas encriptadas.²²

Para la configuración de contraseñas encriptadas se debe crear un archivo de contraseñas separado para samba configurando ejecutar este comando:

- `cat / etc / passwd | mksmbpasswd.sh> / etc / samba / smbpasswd`

Si el sistema utiliza NIS se debe escribir el siguiente comando:

- `ypcat passwd | mksmbpasswd.sh> / etc / samba / smbpasswd`

Luego se debe seguir los siguientes pasos en el directorio samba:

El archivo mkssmbpasswd.sh está instalado en el directorio /usr/bin con el paquete samba

Se debe cambiar los permisos del archivo de contraseñas para que solo el usuario *root* tenga permiso de lectura y escritura con el siguiente comando:

- `chmod 600 / etc / samba / smbpasswd`

²² <http://www.centos.org/docs/4/html/rhel-sag-en-4/s1-samba-configuring.html>

El script no copia las contraseñas el Nuevo archivo, y el usuario samba no puede estar activo hasta que no se establece una contraseña para el usuario. Para mayor seguridad se recomienda que el la contraseña samba sea diferente a la de sistema del usuario.

Para ello el Webmin será una herramienta entendible donde se convertirá los usuarios samba a usuarios del sistema para que los usuarios finales puedan en el servidor leer y escribir archivos en el en el file compartido.

Para establecer la contraseña para cada usuario samba se utiliza el siguiente comando:

- `smbpasswd agente01`

Las contraseñas deben estar habilitadas, puesto que están activadas de forma predeterminada, para ello se debe verificar que la siguiente line de exista:

- `cifrar contraseñas = sin`

Si la línea no existe pero esta comentada con un punto y coma por favor omite la línea con `##`.

Para activar específicamente las contraseñas encriptados en el fichero de configuración agregue las siguientes líneas a la siguiente línea `etc/samba/smb.conf`.

- `encrypt passwords = sí`
- `smb passwd file = /etc/samba/smbpasswd`

Luego de este paso es recomendable reiniciar el servicio smb con el siguiente comando:

- `service smb restart`

Inicio y detención del servicio.

Siempre es necesario que el servicio samba en el servidor este en ejecución, para ver el estado del servicio samba se debe verificar con este comando:

- /Sbin / service smb status

Para iniciar y detener el servicio samba se ejecuta los siguientes comandos:

- /Sbin / service smb start ### para iniciar el servicio###
- /Sbin / service smb stop

Para iniciar el servicio en el momento de arranque del servidor se utiliza el siguiente comando:

- / Sbin / chkconfig - level 345 smb

4.2.3.7. Gestión de servidores Linux Centos con ssh y webmin

Como se comentaba anteriormente es importante que por facilidad en el momento de gestionar remotamente los servidores bajo entorno de consola Linux centos se recomienda por motivos de seguridad hacerlo por SSH Client igual al momento de crear backups hacerlo por SSH Secure File Transfer Client, para ello se debe seguir los siguientes pasos:

Paso 1

Descargar el cliente en la estación de administración en el caso del IPCC USB el administrador lo hará por medio de entorno Windows para ello primero se debe descargar el paquete.

Paso 2

Luego de descargar el paquete ssh se instala y se ejecuta de la siguiente forma para ingresar a la consola de comando de los servidores de forma segura por medio del usuario *root* o el usuario con privilegios que agreguemos:

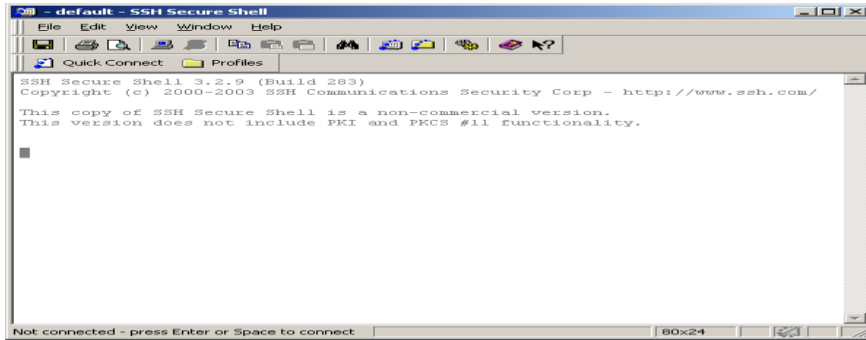


Figura 9 Entorno SSH Client

Para ello damos click en Quick Connect e ingresamos los datos del servidor, en este caso todos los servidores que están bajo distribución de Linux incluido los Dispositivos Switch pueden ser administrados y operados por SSH esto lo haría más seguro y preventivo:

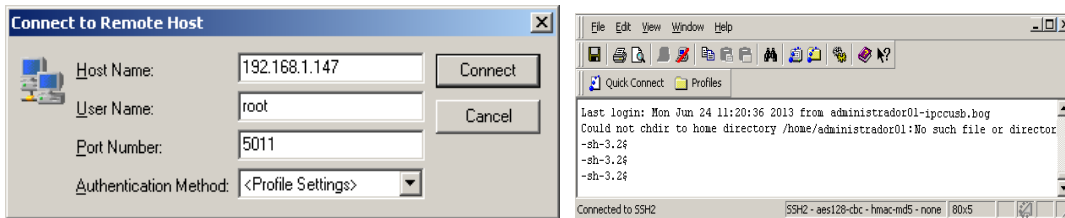


Figura 10 SSH Client

Ingreso al servidor por webmin:

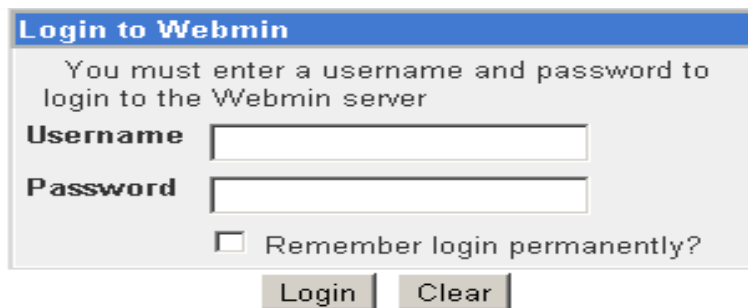


Figura 11 Ingreso al servidor por webmin

Entorno grafico de Webmin para gestionar acl para los usuarios.

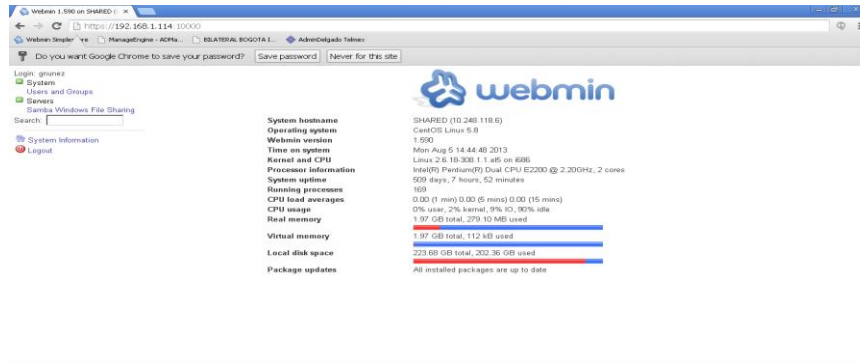


Figura 12 Entorno grafico de Webmin

4.2.3.8. Controlador de dominio y Directorio Activo

Es importante para el IPCC incorporar un diseño de controlador de dominio y directorio Activo, este ayudará a que la red base su estructura jerárquica en un dominio que será nombrado con el nombre de dominio IPCCUSB.BOG, se involucra protocolos importantes como LDAP, DNS, KERBEROS etc. Permitiendo mantener una serie de objetos relacionados con componentes de una red, esto se hace también para mayor seguridad de los usuarios de una red y para adaptar políticas de seguridad y gestión para usuarios. Dicho proceso es recomendable hacerla con entorno Windows Server en este caso puede ser con SERVER 2008 ST el cual es licenciado por compra y debe ser adquirido por medio de un distribuidor autorizado por Microsoft, para ello se debe tener en cuenta la licencias cal que también tendrán el mismo comportamiento de compra como el de la licencia de server, en este caso son 12 estaciones por lo tanto se debe realizar la inversión de 12 cal, una por usuario u estación.

A continuación se presentan costos para tener en cuenta en el momento de adquirir licenciamiento con Microsoft para la instalación del Servidor controlador de Dominio y Directorio Activo para el IPCC:

Producto	Cantidad	Costo Unitario
Windows Server standard	1	\$ 888.15
Cals Windows Server	12	\$ 29.41

Tabla 6 Licenciamiento Pago

Las razones del por qué un controlador de Dominio con directorio activo, es para crear una funcionalidad de grupo de trabajo pero bajo un enfoque jerárquico y de seguridad, ya que un dominio además de ser una agrupación de equipos y usuarios también facilita la administración de los mismos, administra políticas, contraseñas, perfiles de usuario parase aplicados a los perfiles de cada tele operador, el supervisor y el analista Bakcoffice. Los servidores de Windows en este caso el server 2008 ST comparten un usuario base de cuenta y seguridad de datos, lo que permite a cada usuario tener una única cuenta, un único ID y una única contraseña intransferible e igual bajo el entorno.

A continuación se puede observar el diagrama de flujo de la operación del controlador de dominio y directorio activo:

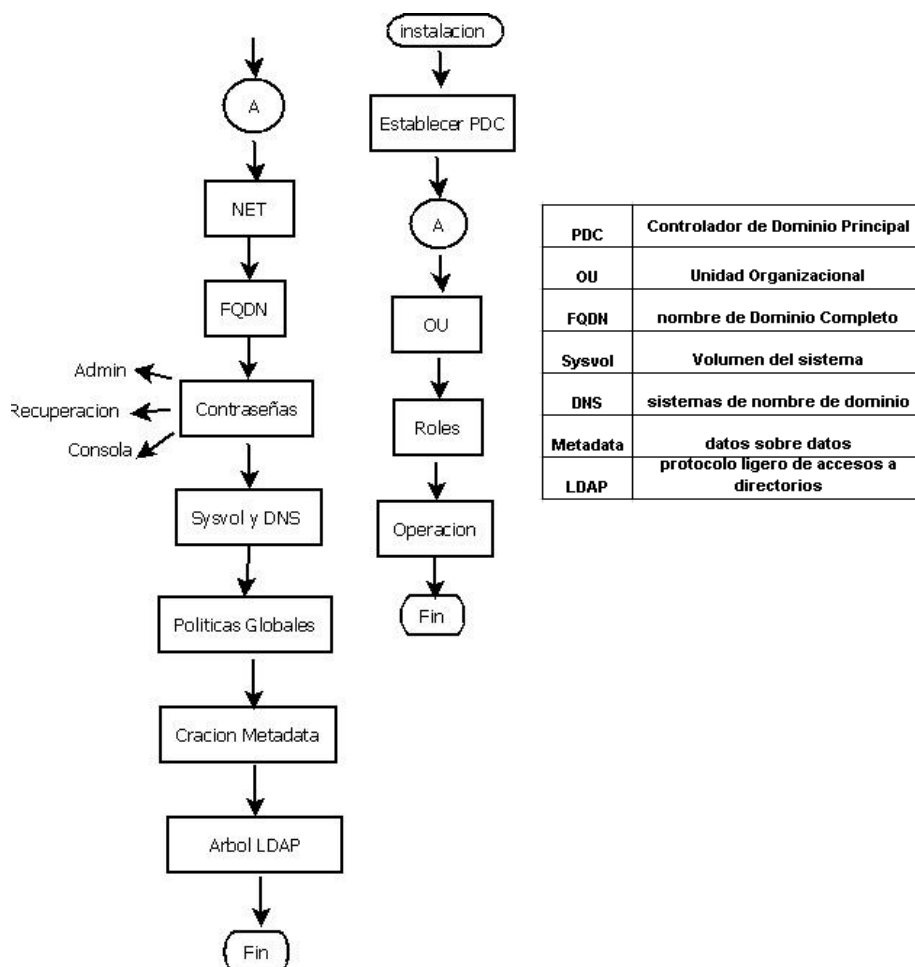


Figura 13 Diagrama de Flujo Controlador de Dominio

Para observar pasos de diseño, desarrollo y configuración del Servidor Controlador de Dominio con Directorio Activo ver Anexo 20

4.2.3.9. Configuración estación tele operador (Agente)

La configuración de las estación de los tele operadores se hará con Windows XP Professional SP3 ya que brinda estabilidad para las aplicaciones web y las del *Softphone*, para ello se debe tener en cuenta que cada computador debe tener una licencia obtenida con un distribuidor autorizado.

Como primer paso se debe hacer la instalación del sistema operativo por cualquier tipo de medio, en el ejercicio del proyecto en curso se realizó por medio de un CD, para observar todo el procedimiento de configuración por favor ver Anexo 8.

4.2.4. Diseño de arquitectura física

- Diseño parte eléctrica y respaldo Eléctrico

El diseño de la parte eléctrica es fundamental para la regulación de consumo de carga eléctrica que se llevara a cabo dentro de las instalaciones de la Universidad para ello se deberá tomar en cuenta los siguientes:

- Acometida Eléctrica 110v/120v 60Hz
- Caja de Circuitos de 6 posiciones
- 2 Breakers de 15 A para Líneas
- 1 carrete Cable Eléctrico 12
- Toma Eléctrica Doble para cada Posición

Como opción se recomienda Planta Eléctrica, para respaldo eléctrico cuando el fluido Eléctrico esté ausente que se muestra en Anexo 16²³.

²³ <http://www.wesimportaciones.com/index.php/agro/generacion/generadores-diesel/8-agro/218-ficha-tecnica-437-de16ss>

4.2.4.1. Diseño cableado estructurado

Para la parte de cableado estructurado se define UTP categoría 5e, como recomendación se recomienda los siguientes materiales para su tendido:

- Canaleta Metálica 10 x 4 cms
- Cable UTP cat 5e marca Quest
- Conectores RJ45
- Conector Hembra RJ45
- Patch Panel 48 pts
- Gabinete de piso metalico 150cmts Alto , 100 cmts Ancho y 100cmts de profundida
- Patch Core 1.50 cms
- Toma doble

A continuación se presenta diseño de cableado estructurado

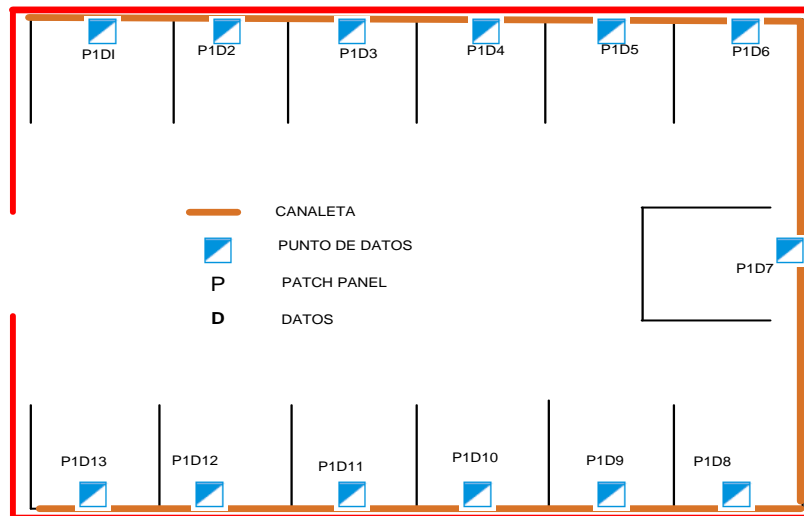


Figura 14 Diseño de Cableado estructurado

4.2.4.2. Diseño direccionamiento IP

Como se mencionó anteriormente el IPCC estará basado bajo direccionamiento IPv4, donde se recibirá una IP Publica donde se pedirá al ISP configuración DHCP dentro de su enrutamiento para la parte interna:

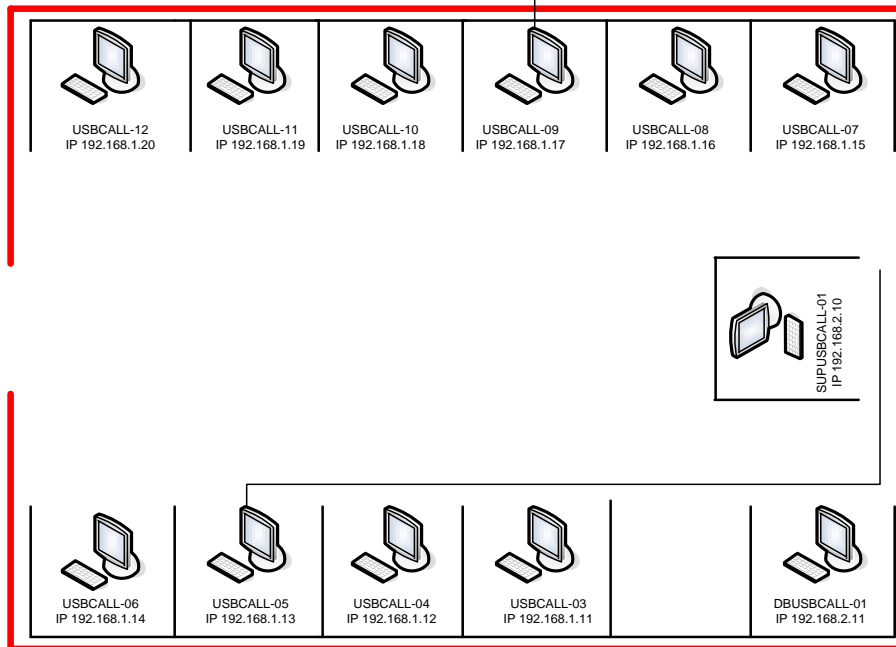


Figura 15 Diseño Direccionamiento IP

4.2.4.3. Diseño RACK de comunicaciones

A continuación se tiene la arquitectura que se instalará en el rack de Comunicaciones o Cuarto de Servidores.

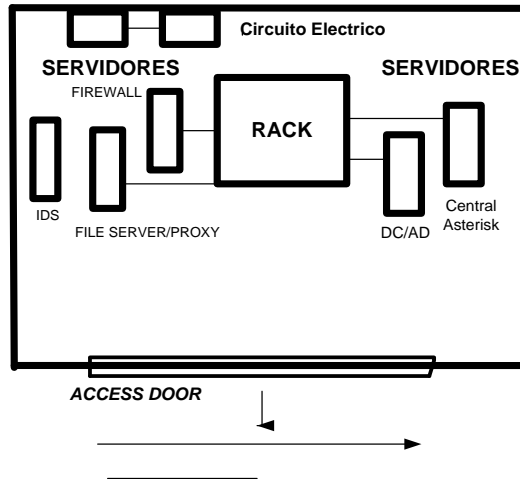


Figura 16 Diseño RACK de comunicaciones

4.3. DIMENSIONAMIENTO DE LOS RECURSOS TECNOLÓGICOS PARA LA OPERACIÓN DEL IP CONTACT CENTER.

Hoy en día el servicio de un *ip Contact Center* sería una herramienta tecnológica apropiada para brindar a la universidad un mejor servicio a sus estudiantes activos e impulsar el número de matriculados a los programas académicos.

El dimensionamiento de los recursos tecnológicos es vital para el funcionamiento apropiado dentro de las necesidades de la Universidad, contando con que actualmente la Universidad no cuenta con un sistema de gestión de Servicio al cliente estructurada.

El dimensionamiento del *Ip Contact Center* será modular, esto quiere decir que su plataforma tecnológica física y lógica se puede implementar en diferentes pasos para su estructura dependiendo de la demanda, su escalabilidad será amigable y adecuada, para llevar a cabo estos pasos modulares abarcaremos los siguientes teorías, tecnologías, dispositivos y soluciones basadas en prácticas reales de *IP Contact Centers* en el mercado actual:

- ✓ Tamaño
- ✓ Capacidad de la infraestructura
- ✓ Soluciones Tecnológicas

4.3.1. Tamaño

Para recurrir y dimensionar el tamaño del *IP Contact Center*, se recurrirá a la teoría de colas y la teoría de teletráfico, contando claramente con el caso actual de las necesidades de comunicaciones de La Universidad San Buenaventura con el cuerpo estudiantil activo, cuerpo Docente y posibles nuevos estudiantes, para ello es importante aclarar que el proyecto de Investigación propondrá un diseño de una infraestructura del *IP Contact Center*, no un plan de mercadeo o figura de negocio el cual no hace parte del mismo por lo tanto se propondrá un dimensionamiento basado en teoría y tomando en cuenta el caso actual, para hallar el tamaño de la infraestructura tomando las siguientes necesidades de la Universidad San Buenaventura:

- La Universidad puede aumentar su cuerpo estudiantil en las diferentes sedes²⁴
- La Universidad puede brindar un contacto más apropiado con los alumnos para crear fidelización de los estudiantes con la Universidad
- La Universidad puede mejorar el tiempo de solución de inconvenientes a los estudiantes, profesores y clientes de la Universidad.
- La Universidad puede aumentar más los canales de comunicación en la parte de publicidad y ventajas de estudiar en la universidad.
- La Universidad cuenta con una planta telefónica Básica de 250 extensiones en uso con un máximo de crecimiento a 250 por lo tanto vemos que para su escalabilidad en el futuro el dispositivo o la solución requiere ser cambiada.
- Las llamadas locales de entrada y salida que no pasan directamente a la extensión son recibidas por la recepción donde se puede presentar un abandono de llamadas que pueden ser importantes para la Universidad.
- La salida de llamadas a números especiales, nacionales, internacionales y celular salen por Recepción. Este procedimiento puede ser escalado al *IP Contact Center*

²⁴ <http://usbcartagena.edu.co/index.php/la-universidad/plugins/system/documentos/images/documents/plugins/system/noticias/272-reunion-direccion-de-mercadeo-corporativo>

para que por medio de tareas o procesos se genere una efectividad de contacto con los destinatarios requeridos.²⁵

4.3.2. Caso de uso:

El análisis que se plantea es el siguiente:

- Tipo de campaña del *IP Contact Center* BLEND (llamadas entrantes y salientes)
- Número de estaciones del IPCC: 12
- Número de Agentes u operadores en Piloto: 10
- Número de personal de supervisión: 2 (1 supervisor)(1 BackOffice y TI)
- El IP Contact Center estará disponible en operaciones en jornada de 8:00 am a 4:00 pm

4.3.3. Capacidad de la infraestructura

La infraestructura estará soportada sobre direccionamiento IPV4, por lo tanto se acordara arrendamiento de un servicio E1 para la parte de Voz y un canal de internet para gestionar la parte de datos el cual se dimensionara en el punto de estudio de ancho de banda de internet que esta propuesto más adelante; Esta gestión se hará con el proveedor de Servicios de Internet que se escoja en el momento de implementar el proyecto. El IPCC contara con cableado estructurado UTP categoría 5e , y su parte de voz con tecnología VoIP, basada en la conmutación de paquetes es decir, se elimina completamente la utilización de elementos basados en circuitos conmutados; Se propondrá además un sistema de grabaciones, reportes de llamadas, interacciones de respuesta de voz (IVR), historiales, etc.

Por la parte eléctrica el IPCC requiere de una acometida para línea de 110v con un Breaker totalizador para carga de 50A y caja de circuitos de 12 posiciones, junto a los anclajes para la parte de cableado eléctrico.

²⁵ Formato 001. Anexo 2

Las posiciones de los operadores junto a los supervisores trabajaran con extensiones softphone eyeBeam, esta clase de herramienta se han vuelto popular últimamente por ser los más apropiados para el ahorro de inversión en dispositivos físicos y el ahorro cuanto mayor número de extensiones se tengan; Existirá la posibilidad de que las extensiones del IPCC puede transferir llamadas o la posibilidad de establecer conferencias con extensiones del staff de la Universidad por medio de una VPN ; A continuación se expone modularmente el dimensionamiento del diseño de la infraestructura que tendrá además en su arquitectura un respaldo eléctrico por si este se requiere:

4.3.4. Soluciones tecnológicas

Se utilizara una gama de soluciones tecnológicas basadas en *Opensource* o distribución libre que serán configuradas para, la central telefónica, Firewall, Servidores de datos, Servidor de Correos, proxy, IDS ; en la parte e software licenciado se utilizara Servidores con Windows server para controladores de Dominios, Directorios Activos, WSUS, también se adhieren servicios unificados como mensajería chat , servicios de redes sociales.

En la parte de plataformas de Seguridad se propone sistemas de control de accesos, sistemas de circuitos de cámaras de seguridad.

En la parte de respaldo eléctrica se propone, caja de trasferencia eléctrica, planta eléctrica, banco de Baterías, UPS's, y además sistema de aire acondicionado para Rack de Comunicaciones o (data center).

4.3.5. Solución utilizando la central telefónica administrada con Asterisk

Actualmente existen varias alternativas en el mercado actual, una de las más llamativas económicas y apropiadas para el dimensionamiento de la infraestructura del IPCC es ASTERISK; esta es una aplicación para controlar y gestionar

comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP mediante todos los protocolos VoIP que implementa²⁶.

Asterisk es una aplicación OpenSource basada en licencia GPL y por lo tanto con las ventajas que ello representa, lo que lo hace libre para desarrollar sistemas de comunicaciones profesionales de gran calidad, seguridad y versatilidad.

Poco a poco, esta aplicación se ha convertido en la evolución de las tradicionales centralitas analógicas y digitales permitiendo también integración con la tecnología más actual: VoIP. Asterisk se convierte así en el mejor, más completo, avanzado y económico sistema de comunicaciones existente en la actualidad.

Otro aliciente es su capacidad de ser programada, permitiendo realizar labores que hasta el día de hoy lo llevaban realizando sistemas extremadamente costosos y complicados y, gracias a Asterisk, esta misma labor se realiza de una forma más económica lo que fomenta el uso de sistemas libres como Linux y estándares abiertos como SIP, H323 o IAX.

Una de las ventajas más interesantes es su posibilidad como sistema híbrido, ya que permite gestionar comunicaciones telefónicas tradicionales (analógicas, digitales, móviles,...) como comunicaciones IP mediante el uso de los protocolos estándar de VoIP.

4.3.6. Dispositivos físicos del IPCC USB BOGOTA

Cada uno de los dispositivos Administrativos y sus características físicas utilizados en el diseño del IPCC de la universidad San Buenaventura están dimensionados para cumplir las necesidades de la campaña, para observar sus dimensiones físicas y de rendimiento se encuentran en los Anexos 9, 10, 11, 12, 13, 14 y 15.

²⁶http://comunidad.asterisk-es.org/index.php?title=Introduccion_a_Asterisk

4.3.7. Enlaces

Para el dimensionamiento del diseño es importante saber cuáles y cuantos serán las tecnologías que interconectaran los servicios del IPCC, el acceso vía telefónica o vía internet de los clientes desde las diferentes redes públicas hacia el IPCC es lo más importante, por lo tanto el requerimiento es obtener un servicio E1, que trabajará la parte de voz, permitiendo escalabilidad para que en el momento de aplicar campañas de alta demanda esté disponible; El otro servicio a contratar será un canal de internet el cual nos servirá para gestionar la parte de datos del IPCC. Se realiza el siguiente análisis para el dimensionamiento de 12 estaciones que trabajaran en la atención de los servicios que brinda el IPCC:

- ✓ El tipo de campaña del IPCC será blend (Inbound y outbound)por lo tanto será 12 por el número de extensiones activas que va tener el IPCC
- ✓ El E1 consta en 32 divisiones (time slots) 30 líneas, más 2 canales de señalización.
- ✓ 2 DID Línea Gratis de fácil recordación para clientes local o al nivel nacional (la facturación del servicio de estas líneas estará a cargo por el IPCC).
- ✓ 1 Canal de Internet de 10M a 12M, para uso aplicativos web de consulta y conexión a contenidos de Internet.

4.3.8. Estudio de llamadas

El TMO ($acdtime+holdtime+acwtime/acdcalls$) de cada Servicio o Campaña es una tarea de Planificación fundamental. Este dato es de suma importancia en la gestión diaria ya que es una de las premisas utilizadas para realizar el dimensionamiento de una campaña, por ende una desviación del TMO puede traer como consecuencia inmediata el incumplimiento de los Niveles de Servicio.

A continuación se hace un ejercicio real para el dimensionamiento:

4.3.9. Análisis de operación-campaña Blend

Como se mencionó anteriormente el desarrollo del dimensionamiento del IPCC será un complemento a las necesidades de la universidad , pero también será una solución disponible para el desarrollo de diferentes campañas en las que el IPCC respalde los requerimientos Futuros de la Universidad, como también perfilarse como herramienta Tecnológica de subcontratación de campañas a terceros, para ello el proyecto de investigación , parte de un análisis de un tipo de campaña como lo es la Blend , de allí la importancia de dimensionar la operación de campaña Inbound y la campaña Oubound; se relaciona a continuación el siguiente análisis:

Hora de Operación: 8 horas

Tiempo de Almuerzo: 45 minutos

Descanso 1: 15 Minutos c/u

Tiempo de llamada estimada: 5 minutos Max o Aprox

Agentes Inbound: 8

Agentes Outbound: 2

Agente Supervisor: 1

Analista BackOffice-TI: 1

Análisis Agentes llamadas Inbound

- ✓ $8 \text{ horas} * 60 \text{ minutos} = 480 \text{ minutos}$
- ✓ $480 \text{ minutos} - 60 \text{ minutos} = 420 \text{ minutos}$ -tiempo de productividad por jornada
- ✓ $420 \text{ minutos} / 5 \text{ minutos (acdTime)} = 84$ llamadas recibidas de 5 minutos Aprox por agente en una jornada.
- ✓ $84 \text{ llamadas} * 8 \text{ agentes} = 672$ llamadas de 5 minutos Aprox en la operación de 8 horas por los agentes disponibles del IPCC.

- ✓ Tiempo intervalo: 15 minutos
- ✓ TMO= X

- ✓ After call (ACW Time) = 30 segundos (1/10 del TMO)
- ✓ HOLDTIME (3%) = 9 segundos
- ✓ ACDDTime= 5minutos= 300 segundos
- ✓ 30 llamadas en el intervalo de 15 Minutos
- ✓ $30 * 5\text{minutos}(\text{ACDDTime})=150$ minutos
- ✓ $150\text{minutos}/15$ minutos tiempo intervalo=10 Agentes
- ✓ Cada 80% (0.8) (30 s en contestar una llamada)
- ✓ 10 agentes $*0.8 = 8$ agentes
- ✓ 15 tiempo intervalo $* 1.2$ factor de seguridad = 18 líneas
- ✓ Total=18 líneas
- ✓ 8 puestos de trabajo

TMO= ACD + HOLD + ACW (si aplica) / Total de llamadas Atendidas.

TMO= $300\text{s} + 9\text{s} + 30\text{s} / 150 = 2.26$ segundos en un intervalo

Análisis Agentes Outbound

- ✓ 2 agentes $* 2.5$ líneas = 5 líneas
- ✓ 18 líneas + 5 líneas = 23 líneas
- ✓ 23 líneas $* 1.3$ FACTOR DE SEGURIDAD = 29.9 Líneas
- ✓ 1 E1 = 30 LINEAS APROX
- ✓ ANI =LOCAL –NACIONAL

4.3.10. Estudio de ancho de banda de internet

El Ancho de banda de internet es de vital importancia para el IPCC, es una medida de recursos disponibles para transmitir la parte de datos ya que en la parte de voz tendremos el servicio del E1; También es una medida que se usa para definir la velocidad de Internet o, de forma más precisa, la velocidad de la conexión de Internet que tendrá el IPCC.

Se puede usar para referirse a capacidad o a consumo. Se mide en bits por segundo (bits/s), en kilobits por segundo (kbit/s), megabits por segundo (Mbit/s) o algún otro múltiplo. Para entrar en el dimensionamiento del ancho de banda de internet para la parte de datos primero tenemos que saber con qué aplicativos de Internet contara cada Agente o tele operador y además de esto el supervisor y el analista BackOffice; a continuación se nombraran las variables más importantes y básicas que deben tenerse en cuenta al calcular el tráfico de red, teniendo en cuenta que con el tiempo puede cambiar por lo tanto se tiene que contar con la escalabilidad del servicio, como el del número de usuarios simultáneos a internet:

- ✓ El número de equipos en uso a internet simultáneamente
- ✓ El rendimiento del software del explorador de Internet
- ✓ La capacidad de las conexiones y los segmentos de red asociados a cada equipo
- ✓ La topología de la red del IPCC y la capacidad de los distintos elementos del hardware de red.

4.3.11. Análisis de operación:

IPCC USB	Hora de Operación: 8 horas # De usuarios conectados a Internet Simultáneamente: 12
Aplicativos Agentes o tele operadores	Cuenta de Correo Accesos a páginas web Universidades San Buenaventura Acceso a consultas Intranet Universidad Operación de pagos bancarios Chat Acceso redes sociales Descarga de reporte o tickets

<p>Aplicativos Supervisor</p>	<p>Cuenta de Correo Accesos aplicativos de supervisión Acceso a reportes de central aplicativo PBX Accesos a páginas web Universidades San Buenaventura Acceso a consultas Intranet Universidad Operación de pagos bancarios Chat Acceso redes sociales Descarga de reporte o tickets Otros</p>
<p>Aplicativos Analista BackOffice</p>	<p>Cuenta de Correo Accesos aplicativos de supervisión Accesos aplicativos de monitoreo de red Accesos a servicios de control y gestión de red Acceso a reportes de central aplicativo PBX Accesos a páginas web Universidades San Buenaventura Acceso a consultas Intranet Universidad Operación de pagos bancarios Chat Acceso redes sociales Descarga de reporte o tickets Otros</p>

Tabla 7 Análisis de operación

4.3.12. Cálculo del ancho de banda

Para calcular el ancho de banda para gestionar los datos como el ingreso a páginas de internet, envío y recepción de correos, soportes en línea entre otros , se realiza un cálculo matemático donde se debe tener en cuenta las siguientes variables :

N = cantidad de usuarios

La fórmula utilizada es la siguiente:

$$AB = G * C$$

Donde:

AB = Ancho de banda a contratar

N = Cantidad de usuarios que utilizan Internet en el IPCC.

G = Ancho de banda a garantizar por usuario.

C = Concurrencia de las personas (cantidad de personas que utilizan Internet simultáneamente).

El valor G es un valor muy importante. Al bajar un archivo cuanto ancho de banda quiero que consuma. Un valor puede ser 1Mbps, el valor G también puede depender del tipo de aplicativo que este implementando el IPCC en el momento.

El valor C puede variar en momentos entre los usuarios, no todos los usuarios utilizaran el Internet al mismo tiempo, pero parte de este proyecto quiere llegar al punto de que este sea utilizado al mismo tiempo por los 12 usuarios para garantizar seguridad y calidad del servicio para el IPCC.

CASO DE USO

$N=12$ (usuarios con Internet disponible en la oficina)

$G=1024Kbps$ (ancho de banda "garantizado" por usuario)

$C = 12$ personas (Estimamos que 12 personas del IPCC estarán conectado simultáneamente al enlace de Internet)

$$AB=G*C$$

$$AB=12*1024Kbps=12288Kbps.$$

Es decir, 12 Mbps para el servicio de Internet del IPCC, este sería viable por medio de un servicio ADSL o como se le llama comúnmente canal de internet de banda ancha, ya que un servicio de enlace dedicado que se quiera obtener puede ser

bastante costoso en su mensualidad y no se justificaría, es viable que luego de tercerizar campañas de alta demanda de tráfico podría ser una buena opción.

Para los 12 usuarios donde se estiman que navegan 12 personas simultáneamente, se puede garantizar un ancho de banda de 1Mbps para la parte de datos en el IPCC que se concluye en una conexión de descarga apropiada.

4.3.13. Selección de proveedores

Para dichos enlaces (o circuitos) existen en Colombia 5 ISP que sobresalen en el mercado de servicios de Telecomunicaciones, estos son Telmex (claro), IFX, Telefónica, ETB, UNE

Se requiere de uno de estos proveedores locales o también llamado proveedor de última milla para el arrendamiento de los enlaces o medios que conectaran los clientes con el IPCC.

Se deben tener en cuenta con el proveedor de servicios de Internet (ISP) los siguientes factores en el momento de realizar arrendamiento de los servicios, teniendo en cuenta que IPCC cuenta con un centro de cómputo, cuarto de Racks o Data-center como bien se le llama:

- ✓ La conexión de los servicios se debe hacer en la Universidad San Buenaventura sede Bogotá Carrera 8 H n.º 172-20
- ✓ Se debe llegar con los servicios listos a conexión al data center ubicado en la Universidad San Buenaventura sede Bogotá Carrera 8 H n.º 172-20
- ✓ Cualquier obra civil debe ser asumida por el ISP
- ✓ La obra civil no debe afectar de ningún modo la arquitectura física de las instalaciones de la Universidad

A continuación se realiza la actividad de Indagación y análisis con respecto a la contratación de la renta del E1 y el canal de Internet con los diferentes proveedores o ISP:

PROVEEDOR DE SERVICIOS	SERVICIO E1 (30 canales de 64 kbps)2048 kbps		
	especificaciones técnicas	servicios adicionales	Precio
CLARO	<ul style="list-style-type: none"> • cuenta con 30 canales de 64 kbps, con un ancho de banda de 2048 Red de Fibra Óptica extremo a extremo (30 llamadas simultaneas) 	DIDS para llamadas directas a sus extensiones: Teléfono Virtual , Fax a e-mail, IP Centrex, PBX Distribuido	\$1.400.000 (10-abril-2013)
TELEFONICA	<ul style="list-style-type: none"> • cuenta con 30 canales de 64 kbps, con un ancho de banda de 2048 ANI (identificación del número llamante) a pedido del PABX. • Se llega por el anillo de fibra óptica metropolitano, utilizando cobre para la última milla 	<ul style="list-style-type: none"> • Sobre el PRI se puede configurar numeración directa a través de MDE's (Marcación directa a extensiones) o DID (direct inward dialing). Se pueden configurar hasta 100 números DID. • Comunicación de datos en 30 x 64 Kbps, 15 X 128 kbps, 8 X 256 kbps, etc, mediante el PRI a través de la plataforma de telefonía pública básica conmutada. • Se pueden manejar simultáneamente voz, datos e imagen. • Se pueden establecer videoconferencias. 	\$2.100.000(10-abril-2013)
IFX	<ul style="list-style-type: none"> • cuenta con 30 canales de 64 kbps, con un ancho de banda de 2048 kbps • Telefonía Local • Condición necesaria: Para la utilización de códec G729 verificar que su planta IP-PBX lo soporte • Telefonía (LDN) Larga distancia Nacional • Telefonía Celulares • Telefonía (LDI) Larga distancia Internacional • Numeración Local e Internacional 	<ul style="list-style-type: none"> • Numeración entrante Toll free • Interfaz web y reportes online 	\$1.600.000 (02-Mayo-2013)

ETB	RDSI PRI cuenta con 30 canales de 64 kbps, con un ancho de banda de 2048 kbps. • 30B+D. Canal B: canal básico de 64 Kbps. Canal D: canal de 64 Kbps de señalización. Canal H: es un canal que permite la transferencia de información de usuario a velocidades superiores a 64 Kbit/s. Existen varios tipos de canal H: canal H0 de 384 Kbit/s, canal H10 de 1920 Kbit/s, etc. • ANI (identificación del número llamante) a pedido del PABX.	• ANI (identificación del número llamante) a pedido del PABX. • Interfaz web y reportes online	\$1.600.000(10-Mayo-2013)
UNE	• Optimización en el manejo del tráfico, puesto que la conexión se hace directamente a la red de conmutación de la central sin pasar por la etapa de concentración de abonado. • Reducción de los requerimientos de infraestructura telefónica del cliente ya que cada enlace E1-PABX ocupa sólo una conexión física por cada 30 conexiones del PBX normal.	• ANI (identificación del número llamante) ha pedido del PABX. • Interfaz web y reportes online	\$1.700.000 (10-Mayo-2013)

Tabla 8 Comparación de los diferentes proveedores ISP

4.3.14. Enlaces a contratar

Después de realizar el análisis respectivo por costos y por respaldo en su infraestructura el proveedor de servicios CLARO ofrece la alternativa más apropiada para la renta del canal de Internet y el arrendamiento del enlace E1, además del servicio que ofrece si se renta el canal de internet con ellos y el servicio del E1, nos brinda la línea de fácil recordación nacional y local junto con el paquete de minutos.

4.3.15. Equipos e instalaciones-mantenimiento concurrente

Generalmente los proveedores ofrecen dentro de sus servicios algunos equipos como el Router, Gateway, mediaconverters, convertidores ATA ,equipos de comunicación Del servicio del E1 que son de un costo alto y en solución como valor agregado los proveedores los ofrecen dentro de la renta de los canales.

Partiendo de esta ventaja se hará el requerimiento al proveedor de servicios de los siguientes dispositivos dentro de la renta de los servicios de Internet y servicio de E1 entre otros.

PROVEEDOR DE SERVICIOS	SERVICIO DE INTERNET BANDA ANCHA PARA DATOS					
	Ancho de banda	Velocidad de descarga	Sistemas administrados	Llegada en Fibra Óptica	Velocidad de carga	Precio
CLARO	12M	12.000 Kbps	<ul style="list-style-type: none"> • WEB Hosting o Disco Duro Virtual de 1000 Megas. • Gratis el dominio que elija con el nombre de su empresa • 40 cuentas incluidas con espacio de correo de 40 Gigas • 5 direcciones IP incluidas • Soporte Técnico Soporte técnico 7x24 	SI	6.000 Kbps	\$500.000(10-abril-2013)
TELEFONICA	10M	10.000 Kbps	<ul style="list-style-type: none"> • Gratis el dominio que elija con el nombre de su empresa • 20 cuentas incluidas con espacio de correo de 40 Gigas • 4 direcciones IP incluidas • Soporte Técnico Soporte técnico 7x24 	SI	5.000 Kbps	\$400.000(22-abril-2013)
IFX	12M	12.000 Kbps	<ul style="list-style-type: none"> • Simetría del canal: El canal se puede diseñar manera simétrica o asimétrica • Optimización del ancho de banda • Tipo de interfaces: Ethernet, FastEthernet, Gigabit Ethernet, E1/T1 Fraccional, V.35 y STM / OC-N • Tecnología de Backbone • No incluye Dominio -no cuentas de correo • 6 direcciones IP 	SI	6.000 Kbps	\$600.000(02-Mayo-2013)
ETB	12M	12.000 Kbps	<ul style="list-style-type: none"> • Llegada últimas millas se refiere (Fibra, cobre, radio). • Conectividad directa al NAP Colombia, al NAP de las Américas •permite realizar monitoreo a nivel de servicio: HTTP, POP3, SMTP, DNS y que se puede visualizar en tiempo real. • 20 cuentas incluidas con espacio de correo de 40 Gigas • 4 direcciones IP incluidas • La disponibilidad es nacional, previo estudio técnico • Soporte Técnico Soporte técnico 7x24 	SI	6.000 Kbps	\$450.000(14-Mayo-2013)

UNE	12M	12.000 Kbps	<ul style="list-style-type: none"> • Llegada en fibra Óptica • Gratis el dominio que elija con el nombre de su empresa • 20 cuentas incluidas con espacio de correo de 40 Gigas • 2 direcciones IP incluidas Soporte • Técnico Soporte técnico 7x24 	SI	6.000 Kbps	\$500.000(14-Mayo-2013)
-----	-----	-------------	--	----	------------	-------------------------

Tabla 9 Servicios de los diferentes proveedores respecto a la banda ancha

Dispositivos administrativos IPCC USB Bogotá				
Dispositivo	Cantidad	Referencia	Característica	VALOR U-PC
Router	1	Cisco	N/A	N/A
Switich Core	1	Cisco Catalyst 2950	Tipo de dispositivo Conmutador - 24 puertos - Gestionado Tipo incluido Montaje en rack - 1U Puertos 24 x 10/100/1000 + 4 x SFP Power Over Ethernet (PoE) PoE Rendimiento Capacidad de conmutación: 176 Gbps Rendimiento de reenvío (64 bytes tamaño del paquete): 41,7 Mpps Tamaño de tabla de dirección MAC 8K de entradas Protocolo de gestión remota SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH Cumplimiento de normas IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q 802.3ab, IEEE, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP), IEEE 802.3at Poder CA 120/230 V (50/60 Hz) Garantía del fabricante Garantía limitada de por vida	\$5.580.000
Central Telefónica Asterisk	1	HP Proliant ML110 G7	VER TABLA #3 ESPECIFICACIONES TECNICAS HP Proliant ML110	\$2.400.000
Firewall	1	HP Proliant ML110 G7	VER TABLA #3 ESPECIFICACIONES TECNICAS HP Proliant ML110	\$2.400.000
File Server Y PROXY Server	1	HP Proliant ML110 G7	VER TABLA #3 ESPECIFICACIONES TECNICAS HP Proliant ML110	\$2.400.000

IDS Server	1	PCs Desktop HP Compaq Pro 6000	Procesadores: AMD Quad-Core A10-5800B con gráficos Radeon HD 7660D (3,8 GHz, 4 MB de caché L2) Chipset: AMD A75 Factor de forma: Microtorre Memoria máxima 32 GB 1600 MHz SDRAM DDR3 Ranuras de memoria: 4 DIMM Unidad interna: 250 GB Unidad óptica: DVD-ROM SATA Puertos: 4 USB 3.0 Alimentación: Eficiencia estándar de 320 W, PFC activo; 320 W, 90% de eficiencia energética, PFC activo Interfaz de red Broadcom NetXtreme Gigabit Ethernet BCM 5761 (estándar)	\$1.400.000
DC/AD Server	1	HP Proliant ML110 G7	VER TABLA #3 ESPECIFICACIONES TECNICAS HP Proliant ML110	\$2.400.000
Data Base Server	1	HP Proliant ML110 G7	VER TABLA #3 ESPECIFICACIONES TECNICAS HP Proliant ML110	\$2.400.000
Computadores de Operación	12	MINI TORRE DELL OPTIPLEX 380	Tarjeta de red: Broadcom® Integrated Gigabit Networking (BRCM 57780)- puertos: 8 USB 2.0 ports, 2 front, 6 rear, Telcado y mouse Opticos 1 RJ-45 Optional PS2 dongle 1 VGA, 1 Serial, 1 Parallel 2 Line-in (stereo/microphone) 2 Line-out (headphone/speaker) 1 low-profile PCIe x16 2 low-profile PCI (Optional riser converts the PCIe and PCI into full height slots) monitor: Dell G-Series and Entry Standard and Widescreen Flat Panel Analog: Dell G2210	\$2.400.000

Tabla 10 Dispositivos administrativos IPCC USB Bogotá

4.4. SIMULAR APLICACIONES QUE PROPORCIONEN FUNCIONALIDADES DE UNA CENTRAL TELEFÓNICA (PBX)

En este capítulo se simuló una central telefónica basada en Asterisk 1.8 mostrando cada una de sus funcionalidades, la configuración básica y su ejecución. Seguidamente se realizó una captura de tráfico de una llamada, se observó los códec de audio y el ancho de banda utilizado.

4.4.1 Instalación y configuración de Asterisk 1.8

Para esta simulación de una central telefónica se descargó Oracle VM VirtualBox que es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana Innotek GmbH. Actualmente es desarrollado por *Oracle Corporation* como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual.

Lo primero fue crear una máquina virtual donde se instaló Linux para posteriormente instalar la distribución Centos 5

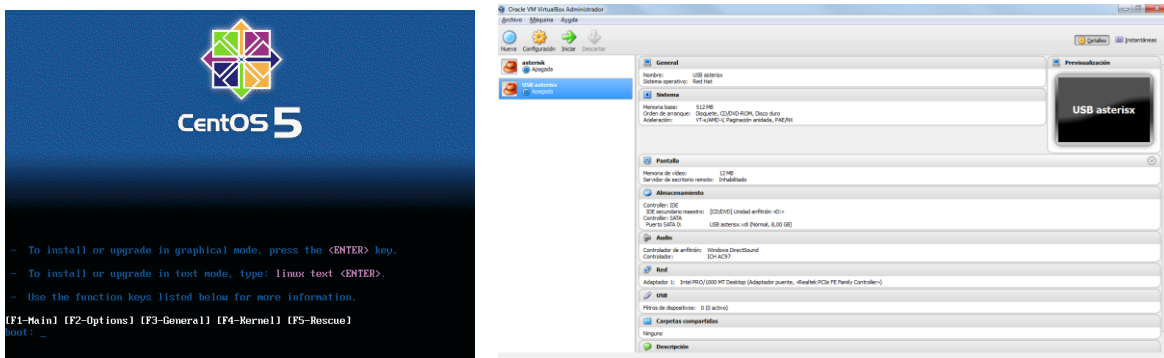


Figura 17 Creación de la máquina virtual en Oracle VM VirtualBox

Se creó una máquina virtual de nombre USB Asterisk con 512 de procesador y un disco duro de 8 Gigas. Posteriormente se instaló Asterisk 1.8.

Primo se Comprobó las dependencias a utilizar de la siguiente forma:

```
# yum check-update # yum -C list ncurses-devel openssl
# yum -y update # yum -C list zlib zlib-devel curl
```

Se Instaló cada una de las dependencias como *Zlib*, *Curl*, *Sendmail* entre otras. Se instaló la rama base para el funcionamiento de Asterisk desde la página de asterisk.org.

LibPRI, *Dahdi*, Asterisk-1,8 colocando el comando *wget* y la página.

<http://downloads.asterisk.org/pub/telephony/libpri/libpri-1.4-current.tar.gz>

<http://downloads.asterisk.org/pub/telephony/dahdi-linux-2.6.2-rc1.tar.gz>

<http://downloads.asterisk.org/pub/telephony/dahdi-tools/dahdi-tools-2.6.1.tar.gz>

<http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-1.8-current.tar.gz>

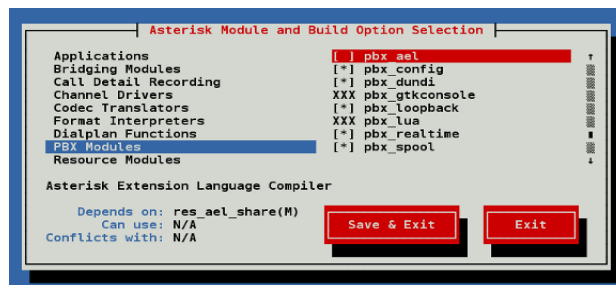


Figura 18 Selección de los módulos a instalar

Se descomprimió cada una de las librerías con el comando *tar -zxvf* y se instaló cada una de ellas con *Make Clean* seguidamente *Make* para copilar y por último *Make Install*. Al finalizar se abrió una ventana donde se seleccionó solo los módulos que se utilizaron y se oprimió *reboot* para reiniciar la máquina virtual.

Al iniciar de nuevo la máquina virtual ya quedo instalado asterisk 1.8 y cada uno de los módulos necesarios para el funcionamiento de la central telefónica.

4.4.2 Simulación y configuración en Asterisk de una central telefónica.

Para esta simulación se tuvieron en cuenta los siguientes parámetros:

5 departamentos (Tesorería, Tecnología, Préstamos, Decano y Director de telecomunicaciones), dos agentes, uno para programas académicos y admisiones y el otro para las peticiones, quejas, reclamos y sugerencias (PQRS).por último se contó con un administrador de la central telefónica. La simulación contó con un total de 10 extensiones dedicadas a usuarios como se muestra a continuación.

Las extensiones fueron las siguientes:

100 La extensión de un teléfono *ip* del Decano, para este ejemplo Guillermo Nuñez

101 La extensión de un *Sofphone* que se encuentra en tesorería

102 La extensión del director de telecomunicaciones Jairo Mesa

103 La extensión de la directora de tecnología Querli Chacón

104 La extensión en un *Sofphone* del departamento de reservas de auditorios

110 La extensión del agente encargado de programas académicos y admisiones

111 La extensión del agente encargado de PQRS

112 La extensión del administrador de *ip Call Center*.

113 Se Utilizaron como otros usuarios para las diferentes pruebas

114 Se utilizaron como otros usuarios para las diferentes pruebas

En la siguiente figura se puede observar el diseño que se utilizó para la simulación de la central telefónica, las extensiones 113 y 114 no se muestra, ya que las utilizaremos como usuarios para realizar diferentes pruebas de las aplicaciones del IPCC.



Figura 19 Diseño de la simulación de aplicaciones en Asterisk

Aquí se tuvo en cuenta que solo el decano, el directo de telecomunicaciones y de tecnología contarán con buzón de voz. Por otra parte todas las extensiones podrán ser monitoreadas por el administrador menos la del decano que contará con un permiso exclusivo para realizar las llamadas deseadas sin necesidad de ser supervisado por el administrador. El administrador podrá escuchar, recoger, transferir cualquier llamada, llevar un control de las colas de los agentes y así establecer el mejor servicio para la central telefónica. Todas las llamadas del exterior las recibirá un DID, el cual en este caso será el 0180005200534 y las direccionará al IVR de la universidad.

❖ Cuenta de usuarios

Para la configuración de cada cuenta de usuario se realizó en el archivo *sip.conf* donde se especificaron cada uno de los usuarios y troncales como se observa en la figura 20.

```
;DECLARACIONES DE REGISTRO|  
  
;FRIENDS, USERS Y PEERS DEBAJO DE ESTA LINEA  
  
[100]; telefono ip del DECANO (Guillermo Nunez)  
type=friend  
host=dynamic  
secret=100  
context=users  
mailbox=100@buzon  
  
[101]; Tesoreria  
type=friend  
host=dynamic  
secret=101  
context=users
```

Figura 20 Configuración del archivo *Sip.conf*

Después de esta configuración se configuro el plan de marcado (*dialplan*) donde asigno que va hacer cada extensión, este archivo contiene la tarea que va realizar cuando se marca cada número. En la figura 21 se observa que la cuenta 100 se le asigno la ext 100 y se le adiciono un comando (*voicemail*) para que tenga buzón de voz mientras que la ext 101 no tendrá el servicio.

```
[users]  
  
exten=>100,1,dial(SIP/100,20,Ttk) ;telefono ip (DECANO)  
Guillermo Nunes  
exten=>100,n,Voicemail(100@buzon) ; buzón de voz ( configurara  
en sip y en voicemail.conf las cuentas)  
  
exten=>101,1,dial(SIP/101,20,Ttk) ;pc 1 (TESORERIA)
```

Figura 21 Configuración del archivo *extensions.conf*

❖ Buzón de voz

Para asignar un buzón de voz, en este caso al Director de Telecomunicaciones, Decano y Directora de Tecnología se realizó en el archivo *voicemail.conf*, en donde escribimos la extensión, la clave de ingreso, y el e-mail de la persona como se observa en la siguiente figura.

```
[buzon]
100=> 100,Guillermo Nunez,jairodmesa@gmail.com
102=> 102,Jairo Mesa,jairodmesa@gmail.com
103=> 103,querli Chacon,jairodmesa@gmail.com
```

Figura 22 Configuración del archivo *voicemail.conf*

❖ Sala de conferencia

Para crear una sala de conferencia donde puedan entrar varias personas a debatir algún asunto, se realizó en el archivo *meetme.conf*, donde se configuro la sala para posteriormente configurar en el archivo *extensions.conf*, el número de ingreso que en este caso fue 300 y la clave fue 2222 como se puede ver en la Figura 23.

```
[rooms]
conf => 100|,2222
```

Figura 23 Configuración del archivo *meetme.conf*

❖ Transferencia y estacionamiento

Para configurar la trasferencias y estacionamiento de las llamadas se realizó en el archivo *features.conf*, donde en este caso se configuro # para trasferir, *2 para poder llamar a otra y pedir algún tipo de información y volver a recogerla y por último #700 para dejar estacionada y recogerla por cualquier persona. Para realizar estos cambios se debió agregar las siguientes letras (Ttk) en el contexto *users* del archivo *extensions.conf* como se puede ver Figura 24.

```
[users]
exten=>100,1,dial(SIP/100,20,Ttk)
```

Figura 24 Configuración del archivo *extensions.conf*

❖ Configuración del IVR, Agente y colas de llamadas

Para realizar el IVR se estableció primero la necesidad de la universidad y como podía mejorar para el cliente un plataforma como estas. En el siguiente diagrama de flujo se muestra paso a paso el proceso por el cual, el usuario puede navegar en el plan de marcado.

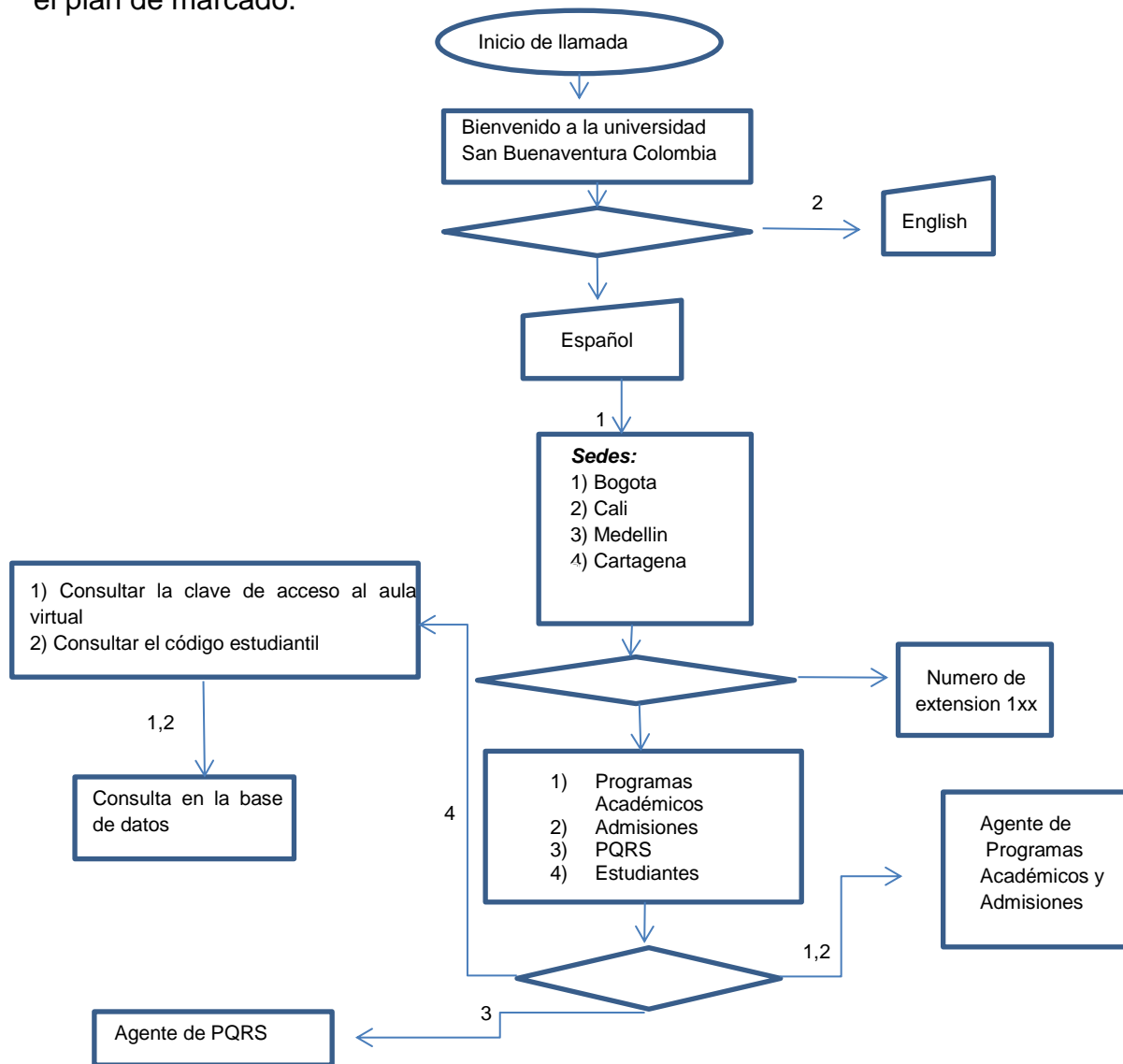


Figura 25 IVR simulado

Para la configuración del IVR se realizó en el archivo *extensions.conf* como se observa en la primera imagen, aquí se escribió comando como responder llamada

(*answer*), colgar (*hangup*), reproducir un sonido(*playback*), ir a contexto diferente (*go*) entre otros.

En la segunda imagen se creó los parámetros para tener en cuenta en las colas del *ip Contact Center* que se realizaron en el archivo *queues.conf*, aquí se contó con opciones como el tiempo de timbres al agente (*timeout*), música de fondo (*musiconhold*), estrategia (*strategy*) entre otros.

<pre>[ivr] exten=>s,1,answer() exten=>s,n,wait(1) exten=>s,n,background(bienvenida) exten=s,n,waitexten(5) exten=>i,1,playback(pbx-invalid); si oprime alguna tecla invalida exten=>i,n,goto(s,1); devuelve al menu exten=1,1,Goto(espagnol,s,1) exten=2,1,Goto(ingles,s,1)</pre>	<pre>[INFORMACIONU] monitor-format=wav announce=anuncio-informacionu strategy=ringall musiconhold=default timeout=15 weight=1 member=>users/110@users,0,Lina Maria,SIP/110 member=>Agent/2001</pre>
--	---

Figura 26 Configuración en *extensions.conf* del IVR y de *queues.conf* para colas.

En este archivo se le dio el nombre de cada agente y tipo de cola que deseamos que tenga en nuestro IPCC. Seguidamente se fué a el archivo *agents.conf* donde asignamos la clave de cada agente para ingresar a recibir llamadas.

```
[general]

[agents]

agent => 2001,9999,Agente2001
agent => 2002,9999,Agente2002
```

Figura 27 Configuración del archivo *Agents.conf*

En este caso para ingresar cada agente marca 555 se registra con número de agente (2001, 2002) y su clave 9999.

Para configurar un estado de DISPONIBLE o NO DIPONIBLE se creó en el archivo *extensions.conf* de la siguiente manera:

```

; Disponible o Desconectado de los Agentes

exten=>620,1,answer()
exten=>620,n,addqueuemember(informacionu)
exten=>620,n,goto(${AQMSTATUS},1)
exten=>620,n,hangup()

exten=>621,1,answer()
exten=>621,n,removequeuemember(informacionu)
exten=>621,n,goto(${RQMSTATUS},1)
exten=>621,n,hangup()

exten=>630,1,answer()
exten=>630,n,addqueuemember(PQRS)
exten=>630,n,goto(${AQMSTATUS},1)
exten=>630,n,hangup()

exten=>631,1,answer()
exten=>631,n,removequeuemember(PQRS)
exten=>631,n,goto(${RQMSTATUS},1)
exten=>631,n,hangup()

exten=>ADDED,1,playback(agente-conectado)
exten=>MEMBERALREADY,1,playback(agente-ya-conectado)
exten=>NOSUCHQUEUE,1,playback(la-cola-no-existe)

exten=>REMOVED,1,playback(agente-desconectado)
exten=>NOTINQUEUE,1,playback(no-conectado)
exten=>NOSUCHQUEUE,1,playback(la-cola-no-existe)

```

Figura 28 Configuración de los estados de los Agentes.

❖ CDR y registros en tablas de *Mysql*

Asterisk no cuenta por si misma con una interfaz web para ver los CDR (registro detallados de llamadas), por esta razón se utilizó una herramienta llamada asterisk-stat que nos convierte los registros que tenemos en una tabla en mysql a una interfaz web, donde pudimos filtrar por fechas o duración de las llamadas.

Lo primero que se hizo fue crear una base de datos y una tabla en mysql de la siguiente forma:

Nos ubicamos en el directorio `cd /usr/src/` y descargamos `esquema-cdr.sql`, el cual contiene la tabla para guardar nuestros cdr. Iniciamos el servicio `mysql` y nos aseguramos que inicie automáticamente cuando arranque nuestro sistema operativo.

```
# service mysqld start
#chkconfig mysqld on
```

Asignamos una contraseña al usuario `root` de MySQL. En este se utilizó `mysqlroot`

```
#mysqladmin -u root password 'mysqlroot'
```

Ahora cargamos el script ejecutando el siguiente comando:

```
# mysql -u root -p <esquema-cdr.sql
```

Ahí nos pidió una contraseña, la cual es `mysqlroot` anteriormente asignada. Verificamos la correcta creación de la base de datos y la tabla con los siguientes comando:

```
# mysql -u root -p
# mysqlroot
```

```
Mysql> USE asteriskcdrdb;
```

```
Mysql> DESC cdr;
```

Y veremos la tabla creada de la siguiente forma:


```
mysql> desc cdr;
+-----+-----+-----+-----+-----+-----+
| Field      | Type      | Null | Key | Default      | Extra |
+-----+-----+-----+-----+-----+-----+
| accountcode | varchar(20) | NO   | MUL |              |       |
| src         | varchar(80) | NO   |     |              |       |
| dst         | varchar(80) | NO   | MUL |              |       |
| dcontext    | varchar(80) | NO   |     |              |       |
| cliid       | varchar(80) | NO   |     |              |       |
| channel     | varchar(80) | NO   |     |              |       |
| dstchannel  | varchar(80) | NO   |     |              |       |
| lastapp     | varchar(80) | NO   |     |              |       |
| lastdata    | varchar(80) | NO   |     |              |       |
| calldate    | datetime   | NO   | MUL | 0000-00-00 00:00:00 |       |
| start       | datetime   | NO   |     | 0000-00-00 00:00:00 |       |
| answer      | datetime   | NO   |     | 0000-00-00 00:00:00 |       |
| end         | datetime   | NO   |     | 0000-00-00 00:00:00 |       |
| duration    | float(7,4) | NO   |     | 0.0000         |       |
| billsec     | float(7,4) | NO   |     | 0.0000         |       |
| disposition | varchar(45) | NO   |     |                |       |
| amaflags    | varchar(45) | NO   |     |                |       |
| userfield   | varchar(255) | NO   |     |                |       |
| uniqueid    | varchar(32) | NO   |     |                |       |
| linkedid    | varchar(32) | NO   |     |                |       |
| peeraccount | varchar(32) | NO   |     |                |       |
| sequence    | varchar(32) | NO   |     |                |       |
+-----+-----+-----+-----+-----+-----+
22 rows in set (0.01 sec)
```

Figura 29 Base de Datos en asterisk

Ahora configuramos Asterisk para que registre los CDR en la tabla creada. A continuación re direccionar todos los CDR a la tabla creada, nos ubicamos en `cd /etc/asterisk/`. Editamos el archivo `cdr_mysql.conf` y habilitamos la sección `[global]` (se habilita quitando el punto y coma que tiene al frente de este comando).

Recargamos el archivo

```
# rasterisk
CLI> module reload cdr_mysql.so
CLI> cdr mysql status
```

De ahora en adelante todos los CDR de Asterisk quedaran registrados en tabla que se creó como se puede ver a continuación.

Con todas estas configuraciones antes mencionada ya la central telefónica debe estar lista para ponerse en marcha, teniendo una dirección IP 192.168.1.15 donde se encuentra el servidor Asterisk, con cada una de las extensiones ya mencionadas y con cada una de las aplicaciones que paso a paso se configuraron.

❖ Fail2Ban

Por último se instaló y configuro el software Fail2Ban el cual nos sirvió como seguridad en nuestra central. Para el correcto funcionamiento es necesario contar con el soporte de Python y Jwhois en nuestro servidor

```
# yum -y install python jwhois
```

A continuación se descargó el código fuente y se instaló la aplicación:

```
# cd /usr/src/  
# wget http://hivelocity.dl.sourceforge.net/project/fail2ban/fail2ban-stable/fail2ban-0.8.4/fail2ban-0.8.4.tar.bz2  
# tar xvfj fail2ban-0.8.4.tar.bz2  
# cd fail2ban-0.8.4  
# python setup.py install
```

Con los siguientes comandos se configuro el inicio automático de la aplicación.

```
Vim /etc/rc.local  
/usr/bin/fail2ban-client-start
```

Ahora configuraremos el archivo *jail.conf* que se encuentra en *cd /etc/fail2ban*, aquí se puso la cantidad de errores que podría tener una persona al registrarse, si supera este número de intentos automáticamente se bloqueara el tráfico que vendría de esta dirección ip.

```
[asterisk-iptables]

enable =true
filter= asterisk
action: iptables-allports [name=ASTERISK,protocol=all]
mail-whois [name=ASTERISK-CLIENTE,
dest=jairodmesa@gmail.com,
send=fail2ban@mail.com]
logpath= /var/log/asterisk/full
maxretry=3
bantime=86400
```

Figura 30 Configuración del archivo *jail.conf*

Por último, en esta imagen con el comando *iptables -L* se pudo ver las direcciones bloqueadas. En la imagen se puede observar que se ejecutó el comando y no hay nada bloqueado, después se intentó registrar desde cualquier dispositivo tres veces incorrectamente y se vio cómo nuevamente ejecutando el comando se muestra que el tráfico de la dirección 192.168.1.5 fue bloqueado.

```
[root@localhost fail2ban]# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
fail2ban-ASTERISK all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination

Chain fail2ban-ASTERISK (1 references)
target    prot opt source                destination
RETURN    all  --  anywhere              anywhere

Chain fail2ban-SSH (0 references)
target    prot opt source                destination
RETURN    all  --  anywhere              anywhere
[root@localhost fail2ban]# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
fail2ban-ASTERISK all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination

Chain fail2ban-ASTERISK (1 references)
target    prot opt source                destination
DROP     all  --  192.168.1.23          anywhere
RETURN    all  --  anywhere              anywhere
```

Figura 31 Comando *iptables -L* para ver las direcciones bloqueadas

Plan de marcado (*Dialplan*)

Llamadas que entrar a la central por el 0180005200534 ingresan al IVR.
Ingresar al buzón de voz se hace por la ext 1234 y la clave es la misma de la ext
Para el ingreso a la sala de conferencias se marca 300 y clave de la sala 2222
Para el ingreso al directorio de la USB se marca 512
Para que un agente este en línea listo para atender se marca 555 y su número de agente en este caso creamos uno 2001 para programas académicos y 2002 para las PQRS, y la clave que es 9999.
Para los agente información (2001)620 para conectarse rápidamente directamente a su celular y 621 para desconectarse
Para los agente PQRS (2002)630 para conectarse rápidamente directamente a su celular y 631 para desconectarse
462 para transferir a la encuesta
= para transferir - #700 = llamada estacionada
*2 = poder estacionar la llamada mientras se llama a otra persona
192.168.1.15/fop2 para que el administrador controle cada una de las llamadas
192.168.1.15/asterisk-stat/ para mirar los CDR.

4.4.3 Implementación de aplicaciones para la central telefónica

- Flash Operator Panel 2(FOP)

Asterisk no cuenta nativamente con un panel que permita ver la actividad del sistema, por consiguiente se utilizó una aplicación llamada FLASH OPERATOR PANEL 2(FOP) para que cualquier usuario autorizado pueda observar la actividad de la central telefónica, por ejemplo quien está hablando y con quien está hablando, duración de las llamadas activas, llamadas en espera, llamadas en cola, etc. La aplicación permite controlar su teléfono, realizar transferencias, lanzar monitoreos/susurros, supervisar las colas de llamadas y ver hasta dos líneas por teléfono configurado entre otras funcionalidades, para mayor información www.fop2.com. En la siguiente figura se puede observar la interfaz web que tiene esta aplicación, lo interesante es poder configurar los botones que necesitamos, las extensiones y las troncales que deseamos monitorear o llevar control. Esta

herramienta es un requerimiento esencial para IPCC. En el anexo #21 se puede observar la instalación y la configuración de cada una de las opciones que permite este programa.



Figura 32 Consola de monitoreo

- Registro de los CDR (registro detallados de llamadas) utilizando ASTERISK STAT

La herramienta asterisk-stat, proporciona diferentes reportes y gráficos, permiten a un administrador de Asterisk analizar rápidamente y fácilmente el tráfico de llamadas que pasan por Asterisk. Esta herramienta recogerá los cdr que se encuentran registrados en la tabla asteriskcdrdb creada en la instalación de la central telefónica, ahí los consultara y por medio de una interfaz web mostrara esta información de una manera más amigable para el usuario. En la siguiente figura podemos apreciar la interfaz que nos presenta esta aplicación, para ver la instalación de esta herramienta se puede dirigir al anexo #22 donde se explica paso a paso como es la debida instalación.

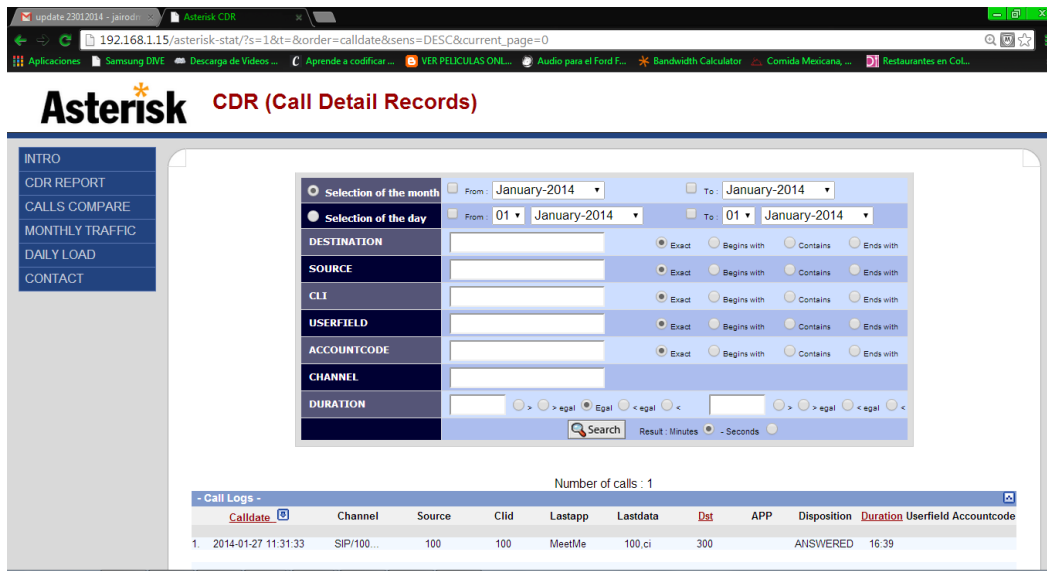


Figura 33 Consola CDR

- Sistema de grabación de llamadas en el IPCC

Como se analizó en el primero capítulo un sistema de grabado es esencial en un IPCC, ya que se puede tener un registro de audio de cada llamada, se puede evaluar la calidad que prestan nuestros agentes hacia los clientes y así ofrecer el mejor servicio, recordando que cada agente habla en nombre de la empresa.

Con el comando MixMonitor se puede grabar las llamadas de una extensión específica, de la cola, salientes o simplemente todas las llamadas realizadas como se realizó en este caso. A continuación se realiza una llamada a nuestra central donde en la siguiente grafica se puede observar el comando MixMonitor y la sucesión de la llamada.

```

=== Using SIP RTP CoS mark 5
-- Executing [0180005200534@users:1] Set("SIP/100-00000000", "calltime=20140313015416") in new stack
-- Executing [0180005200534@users:2] MixMonitor("SIP/100-00000000", "/home/JAIRO/llamadasentrantesIVR/X20140313015416X100X0005200534X.gsm") in new stack
-- Executing [0180005200534@users:3] Goto("SIP/100-00000000", "ivr,s,1") in new stack
-- Goto (ivr,s,1)
-- Executing [s@ivr:1] Answer("SIP/100-00000000", "") in new stack
=== Begin MixMonitor Recording SIP/100-00000000
-- Executing [s@ivr:2] Wait("SIP/100-00000000", "1") in new stack
-- Executing [s@ivr:3] Background("SIP/100-00000000", "bienvenida") in new stack
<SIP/100-00000000> Playing 'bienvenida.gsm' (language 'es')
-- Executing [i@ivr:1] Goto("SIP/100-00000000", "espanol,s,1") in new stack
-- Goto (espanol,s,1)
-- Executing [s@espanol:1] Answer("SIP/100-00000000", "") in new stack
-- Executing [s@espanol:2] Background("SIP/100-00000000", "ivr") in new stack
<SIP/100-00000000> Playing 'ivr.gsm' (language 'es')
=== Spawn extension (espanol, s, 2) exited non-zero on 'SIP/100-00000000'
=== MixMonitor close filestream
=== End MixMonitor Recording SIP/100-00000000
localhost*CLI>

```

Figura 34 Comando MixMonitor

Primer comando set, donde se graba la fecha y seguidamente el comando MixMonitor encargado de grabar la llamada. Este comando se realiza en el archivo *extensions.conf* de la siguiente forma:

MixMonitos(Nombre del archivo y lugar de grabado)

- Encuesta de calidad en las llamadas

En un *Call Center* el agente habla por la empresa, en este caso la universidad, por consiguiente para prestar el mejor servicio se realizó unas cortas preguntas de calidad al finalizar las llamadas.

Se realizó una encuesta de 5 preguntas para validar si se dio una solución a la inquietud y si ha sido amable el agente que lo atendió.

Para realizar esta encuesta se diseñó una tabla con las 5 preguntas donde nos muestra cada una las respuestas de los usuarios. En este caso la tabla se realizó con ayuda de un script default realizado en MySQL, donde se puede observar la integridad de Asterisk con diferentes programas, las utilidades y aplicaciones que se pueden integrar. Esta encuesta se configura en la ext 462.

Preguntas Realizadas:

- 1 ¿Fueron los agentes amables?
- 2 ¿Obtuvo una respuesta rápida?
- 3 ¿Recibió información útil?
- 4 ¿Ha llenado las expectativas por las cuales usted escogió el servicio?
- 5 ¿En general, como califica el servicio?

Tabla que nos muestra Asterisk

	Fecha	Rt1	Rt2	Rt3	Rt4	Rt5
Usuario 1	15012014	5	5	5	5	5
Usuario 2	15012014	3	3	4	2	3

Tabla 11 Tabla de encuesta

- Consulta base datos vía telefónico.

Asterisk dentro de todas funcionalidades tiene la opción de consultar tablas dentro una base de datos creada en MYSQL, lo primero que se realiza es crear una base de datos y diferentes tablas para que Asterisk pueda llamarlas.

En la siguiente aplicación se configura y se crea una tabla llamada asteriscdrdb donde se crean dos tablas, para la consulta. Una de ellas es tcodigou (tabla del código de la universidad) y la segunda tclaveaula (clave de la aula virtual), en estas tablas se pide la cedula y seguidamente se consulta el código universitario o la clave para el ingreso a los cursos virtuales. Con esta aplicación se podría tener una base de datos que se esté actualizando constantemente por el departamento de sistemas o cada uno de los departamentos para brindar información vía telefónica.

4.4.4 Análisis de códec y llamadas.

Wireshark es una herramienta utilizada para capturar trafico red, con ella se puede ver a detalle que protocolos y ancho de banda estamos utilizando en cada una de las llamadas. Para esta simulación se tuvo en cuenta la figura 45, donde se especifica las extensiones, los nombre y funcionamiento de cada una de ellas.

En este capítulo podremos analizar los códec de audio GSM y 711 que son lo más utilizado, ya que del formato de audio con que se realiza la llamada es esencial para calcular el ancho de banda y calidad en el servicio, también se realizará una llamada pasando desde la red PSTN hasta llegar hacer atendida por el agente, se

analizará los dispositivos por los cual tiene que pasar la llamada, lo que se realiza en cada paso y el ancho de banda que se consumió.

Como primer paso se muestra la tabla de comparación de los códec:

	Códec G.711	Códec G 723	Códec GSM	Códec G.729
Velocidad de transmisión (Kbps)	64	5,3/6,6	13	8
Tamaño carga útil (Payload)(Bytes)	160	24	32.5	20

Tabla 12 Comparación códec GSM vs 729

Como se puede observar teóricamente el códec G.711 tiene un mayor consumo que el códec GSM.

Para comprobar esta teoría, se realizó dos llamadas, una utilizando GSM y la segunda G.711 y se procedió analizar el ancho de banda.

Se configuro la central para recibir cualquier códec, se procede a configurar cada sofphone con GSM y otro con G.711 y se realizan las llamadas. En wireshark, se dirige hacia la opción de gráfica, ahí se filtra solo le consumo de voz RTP de la siguiente forma `rtp and ip.dst==192.168.1.12` y se analiza las llamadas.

En la siguiente figura mostro que efectivamente la primera llamada (GSM), consumió menos ancho de banda pero la calidad no fue la mejor, mientras en la segunda (G.711) consume un poco más pero la calidad es superior, Por consiguiente tiene que tener muy claro qué tipo de códec utilizar dependiendo el ancho de banda y la calidad que requiramos para el IPCC. Hay que recordar que existen muchos tipos de códec de voz, los más utilizados son los anteriormente mencionados, pero existen de licencia gratis y otros pagos como el G.729 utilizado por Skype.

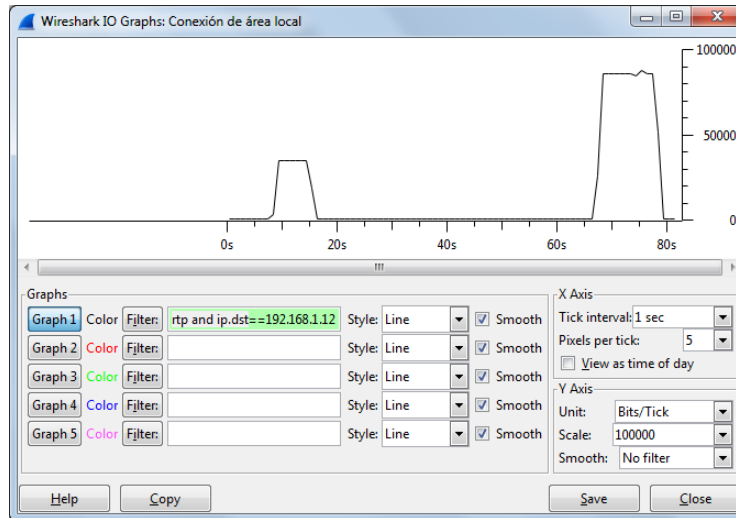


Figura 35 Comparación en ancho de banda de una llamada GSM y otra 729

- Análisis de toda una llamada.

En esta simulación se realizó una llamada desde un teléfono móvil, hasta el IVR de la central telefónica para finalmente ser atendida y solucionada por un agente. En la siguiente grafica se ilustra el recorrido que debió realizar la llamada.

Inicialmente la llamada empezó en una red móvil desde cualquier lugar con cobertura, seguidamente realizó su comunicación con la red PSNT ya que estamos comunicándonos a un teléfono fijo (analógico), llega a la casa, donde es recibido por Gateway (*grandstream*) que como ya se ha mencionado hace el cambio de analógico al digital, pasa por un IDS, el cual rectifica que no sea un intruso y posteriormente llega a la central donde es captada por el IVR de la universidad San Buenaventura. Por último, es llevada al agente encargado para resolver la inquietud, quien finalizada la llamada enviado al cliente a la encuesta de calidad.

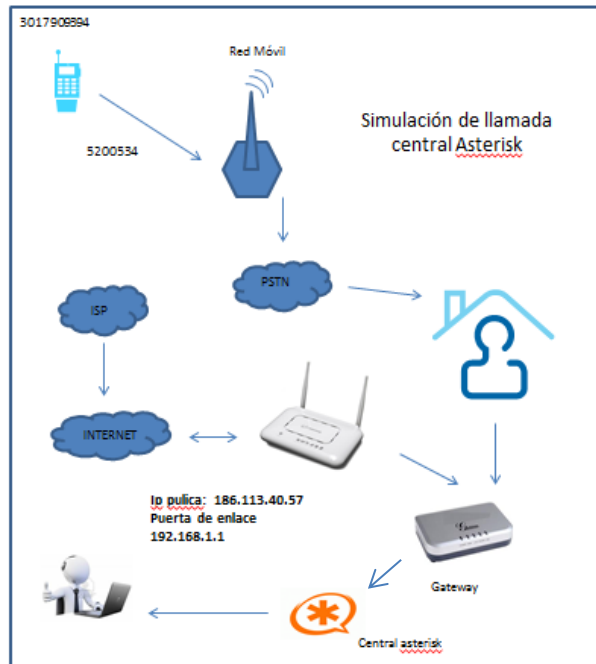


Figura 36 Simulación de llamada entrante hasta llegar al agente

La llamada dura: 2 minutos 41 segundos. En la siguiente figura se observa que empezó a consumir ancho de banda del segundo 80 al 110, donde se estableció la comunicación con el agente, desde el segundo 0 hasta el 80 y del segundo 110 hasta 145 donde entra el IVR y la encuesta, se observa el bajo consumo de ancho de banda. La línea roja muestra el consumo de diferentes protocolos que no fueran RTP.

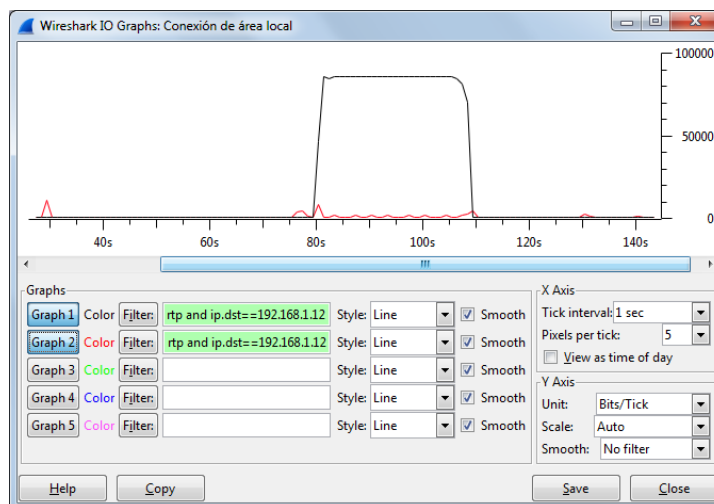


Figura 37 Ancho de banda de la llamada

En el siguiente grafico se puede observar la llamada en detalle, como se muestra en teoría.

Los mensajes más comunes son:

- **INVITE.** Tipo Request. Para establecer una sesión entre agentes de usuario.
- **ACK.** Para la confirmación de un establecimiento de sesión.
- **OPTION.** Un Request o solicitud de información de capacidades
- **BYE.** Se usa para la liberación o terminación de una sesión establecida.
- **CANCEL.** Cancela una petición pendiente sin influir en la sesión o llamada.

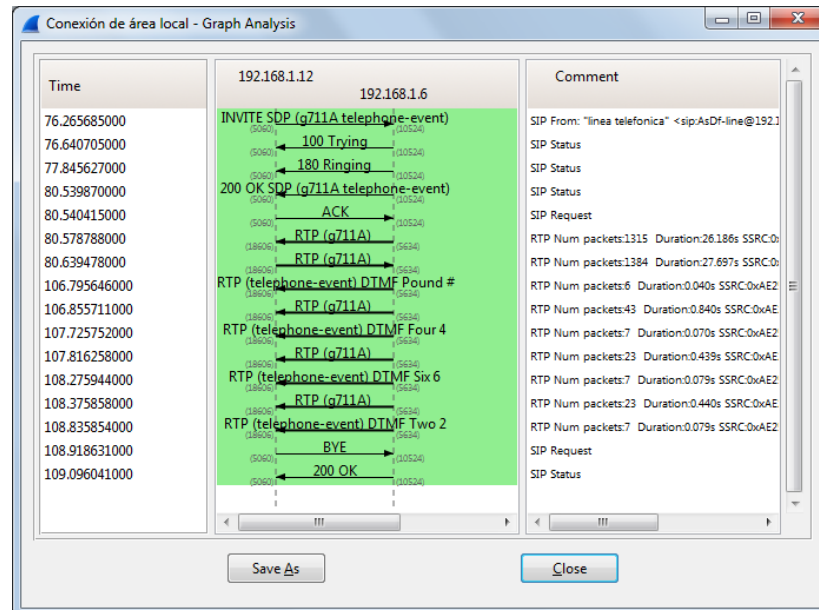


Figura 38 Análisis de la llamada

Wireshark también tiene la opción de decodificar la llamada para poderla escuchar, aquí nos pone un jitter búfer de 100ms, pero es modificable, dependiendo el receptor se puede perder o captar más datos.

En la siguiente Figura podemos observar dos pistas de audio, la cual corresponde a cada uno de los usuarios, en la llamada se puede observar la duración cuando se realiza ya la comunicación con el agente.

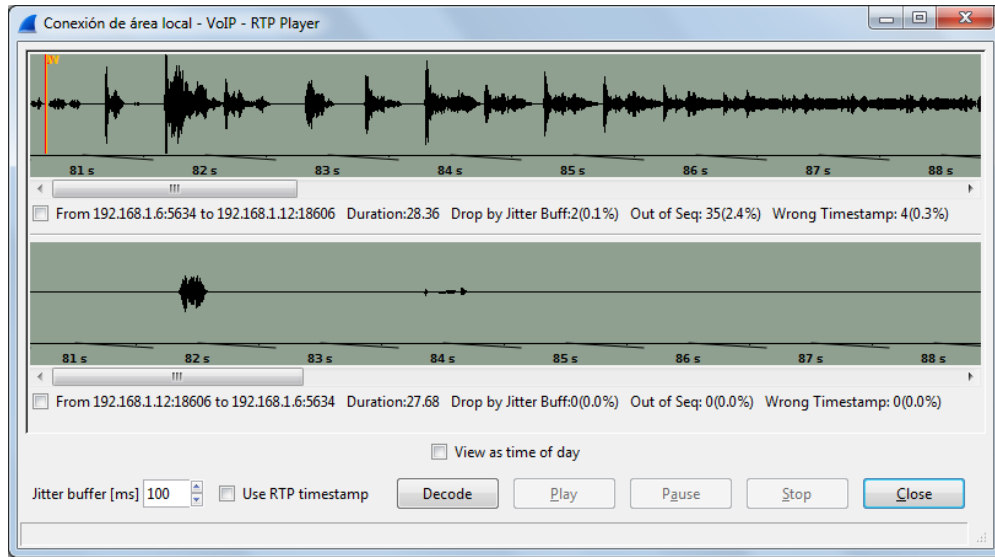


Figura 39 Pista de la llamada

Como se puede observar en un IPCC center se tiene que tener en cuenta muchas variables, las cuales indican el número de personas, propósito del *Call Center*, calidad, dispositivos, software, entre otros. Como ya se ha mencionado este proyecto es modular en donde se puede escalar y modificar a las necesidades que requieran la universidad o empresa y cambios posteriores que se puedan llegar a realizar.

II. CONCLUSIONES

Un *IP Contact Center* es una solución eficiente que integra varios servicios, y por medio de una infraestructura económica se puede contar una solución que ayude a la universidad a contar con una estrategia adicional para el manejo de contacto con los clientes.

El estudio del proyecto de investigación permitió identificar claramente que las plataforma como Asterisk, Distribucion linux (Centos) pueden convivir con plataformas licenciadas como Windows sever 2008, y además contar con un buen respaldo en la seguridad de la información como por ejemplo lo puede ser el firewall y el proxy.

La plataforma de comunicaciones vía telefónica (3COM NBX 100-V3000) con la que cuenta la universidad para contactar a sus clientes puede ser mejorada con una solución de voz sobre IP como lo es Asterisk, ya que con esta ahorrarían costos, se contaría con escalabilidad y flexibilidad en la parte de gestión de las llamadas.

Los dispositivos administrativos como lo son router , switch, firewall y servidores son parte primordial para el diseño de la infraestructura del IPCC de la universidad, ya que brindan una arquitectura estructurada y modular para su gestión.

El diseño propuesto muestra una forma factible y modular para la implementación de IPCC en la Universidad San Buenaventura, teniendo en cuenta las diferentes variables como la seguridad, precios de los proveedores de servicios (ISP), equipos, marcas y por supuesto un favorable presupuesto gracias a que la mayoría de software utilizados están bajo la plataformas de licencia libre *Open Source(Centos)*.

El IVR propuesto ayudara a que los clientes naveguen de una forma cómoda , fácil y en un diferente idioma como lo es el de la opción de inglés, además brindara la unificación de la información entre las diferentes sedes en Colombia , fortaleciendo el nombre al nivel nacional y al nivel internacional para aquellos estudiantes que vienen del exterior.

Asterisk es una herramienta flexible que puede convivir con diferentes módulos de programación como mysql, php, python, http brindando así aplicaciones como la consulta de clave del aula virtual en una base de datos vía telefónico, o la interfaz gráfica web para la visualización de los registros de llamadas.

La aplicación wireshark utilizada en el proyecto de investigación fue de gran ayuda ya que se pudo observar y analizar el tráfico de una llamada entrante , los protocolos utilizados y el ancho de banda utilizado, aparte los *códecs* que se utilizaron para la parte de voz (trafico RTP).

III. BIBLIOGRAFÍA

Ministerio de Educación Nacional de Colombia: 2011 Disponible en Internet: <http://www.mineducacion.gov.co/1621/propertyvalue-37666.html>

Ministerio de Educación Nacional de Colombia: 2011 Disponible en Internet: <http://www.mineducacion.gov.co/buscandocolegio/>

Colegio Fray Rafael de La serna: 2011 Disponible en Internet: <http://www.colegiofrayrafaeldelaserna.edu.co/>

Aldo Javier Lovera Raffo: diseño e implementación de un Sistema experto para una plataforma De *contact center* 2008 Disponible en Internet: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/202/LOVERA_ALDO_DISENO_SISTEMA_EXPERTO_PARA_PLATAFORMA_CONTACT_CENTER.pdf?sequence=2

Iván Enrique Puerto Parra plan de negocios para crear una empresa de servicios de *Contact center* utilizando el CRM para mejorar la gestión Comercial de las empresas pyme en la ciudad de Bogotá. 2008 Disponible en Internet: <http://www.javeriana.edu.co/biblos/tesis/economia/tesis238.pdf>

Nikolai Tchernitchin Lapin: Diseño e implementación de un *IP Contact Center* distribuido, en base a elementos de bajo costo, y con elementos modulares, que permitan mostrar las partes de ella en forma sencilla y de manera docente 2007 Disponible en Internet:

<http://www.pioxii.edu.co/12/index.php/en/134-pio12carrusel/180-medellin>

German Capdehourat : Análisis y Diseño de *Call Centers* 2006 Disponible en Internet:

http://iie.fing.edu.uy/~gcapde/trabajos/perfo/trabajo_perfo.pdf

German Riaño Mendoza: *Call Center* Modelos de Investigación de Operaciones 2005 Disponible en Internet: http://elavio2005.uniandes.edu.co/MiniCursosTutoriales/Riano_P.pdf

CISCO *IP Contact Center*. Construyendo el *Contact Center* 2012 Disponible en Internet: http://84.113.22.230:8980/archiv/doku/cisco/Mobile_Avvid_Vol%202/dokumente/Produkte/Call_Centers/IPCC/DS_IPCC.pdf

Internet: <http://www.fdi.ucm.es/profesor/jcgutierrez/Tema%20/02UML-1.pdf>

J. Joskowicz. *Conceptos De Telefonía Corporativa*. Montevideo, Uruguay. Versión 10. Julio 2013.

Curso Voz Sobre Ip Y Asterisk v1.0 (Disponible en: <http://dc388.4shared.com/doc/G7uemS10/preview.html>. Consultado el 25 julio 2013)

Asterisk (Disponible en: <http://www.asterisk.org/get-started>. Consultada el 4 Julio 2013)

Flash Operator Panel 2 (Disponible en: <http://www.fop2.com/documentation-installation-getting-started.php>. Consultado el 15 de agosto 2013)

Call Analytics Solution (Disponible en: <http://www.cdr-stats.org>. Consultada el 20 de agosto 20 2013)

Curso de Asterisk Special Edition.(27:08:2013:Bogotá) dictado por Netsecurity.

IV. ANEXOS

Anexo 1 Carta de autorización para la información de USB

CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, DE INFORMACION TECNICA DE LA RED DE COMUNICACIONES DE LA UNIVERSIDAD SANBUENAVENTURA BOGOTA.

Bogotá 5 de Marzo del 2013

Ingeniera
QUERLI CAÑAS CHACÓN
Jefe Unidad de Soporte Tecnológico
Universidad San Buenaventura
Ciudad

Asunto: Proyecto de Grado “Diseño de la infraestructura de telecomunicaciones para la operación de un *IP contact center* para la Universidad de San Buenaventura – Colombia”

Reciba un cordial saludo.

Por medio de la presente Guillermo Alfonso Nuñez Arciniegas con código estudiantil 20071236035 y Jairo David Mesa código estudiantil 20071236030 estudiantes activos de la Universidad San Buenaventura Bogotá, del programa de Ingeniería de Telecomunicaciones de 10 semestre, nos dirigimos a usted con el fin de solicitar muy amablemente información técnica relacionada con la Unidad de tecnología en el área de comunicaciones; para adelantar el proyecto de grado “Diseño de la infraestructura de telecomunicaciones para la operación de un *IP contact center* para la Universidad de San Buenaventura – Colombia”, el cual fue aprobado a finales del segundo periodo del 2012 por el nodo de profesores de Ingeniería de telecomunicaciones.

En el formato adjunto se especifican los datos requeridos para el inicio del proyecto. Este formato cuenta con el visto bueno de nuestro tutor la Ingeniera Diana C. Contreras y el respectivo Director de Programa Ingeniería de Telecomunicaciones Nelson Felipe Rosas, luego de su estudio y aprobación. La información suministrada por la Unidad de Tecnología se utilizará solo para los fines y objetivos del proyecto, los cuales son los siguientes:

OBJETIVO GENERAL:

Diseñar la infraestructura tecnológica de información y comunicaciones (TIC) para la operación y gestión de un *IP Contact Center* para la Universidad de San Buenaventura - Colombia

OBJETIVOS ESPECÍFICOS:

- Analizar y especificar los requerimientos funcionales y no funcionales de la Universidad San Buenaventura - Colombia, con respecto a sus necesidades de comunicación y mercadeo para identificar los recursos de TIC esenciales para la operación y gestión de un IP Contact Center.
- Dimensionar los recursos tecnológicos, de información y comunicaciones, para la operación y gestión del IP Contact Center con base en las mejores prácticas establecidas en el mercado y la teoría del teletráfico.
- Diseñar la arquitectura física y lógica del *IP Contact Center* de acuerdo con los requerimientos establecidos y el dimensionamiento calculado.
- Validar el diseño planteado, de acuerdo con el dimensionamiento calculado y los requerimientos establecidos.

Agradecemos la atención a la presente y en espera de una pronta y positiva respuesta.

Cordialmente;

GUILLERMO NUÑEZ ARCINIEGAS
Estudiante

JAIRO DAVID MESA
Estudiante


Anexo: Formato para su diligenciamiento en dos (2) Folios.

VoBo: Tutor Trabajo de Grado Ingeniera Diana C. Contreras Jáuregui

VoBo: Director Ingeniería de Telecomunicaciones Nelson Felipe Rosas

Anexo 2 Formato de consulta de información técnica USB

FORMATO 01: FORMATO DE CONSULTA DE INFORMACION TECNICA DE LA RED DE COMUNICACIONES DE LA UNIVERSIDAD SANBUENAVENTURA BOGOTA.

	FORMATO:001	fecha: / /	PROGRAMA: Ingeniería Telecomunicaciones		
	ESTUDIANTES	Guillermo Nuñez Arciniegas cod: 20071236035 Jairo David Mesa cod: 20071236030		Observaciones:	Desarrollo de Investigación Proyecto de Grado
Descripción de la Actividad	RECOLECCION INFORMACION DE ESPECIFICACIONES TECNICAS RED LAN UNIVERSIDAD SAN BUENAVENTURA BOGOTÁ COLOMBIA PARA EL PROYECTO DE GRADO "DISEÑO DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES PARA LA OPERACIÓN DE UN IP CONTACT CENTER PARA LA UNIVERSIDAD DE SAN BUENAVENTURA - COLOMBIA"				
Resumen de la Actividad					
	PREGUNTAS	Si	No	Comentarios	
	La Universidad cuenta Actualmente con un sistema o plataforma de recepcion y salida de llamadas Telefónicas ?				
	Existe un departamento o dependencia que realice la labor de recepcion y salida de llamadas telefónicas ?				
	La Universidad cuenta Actualmente con un dispositivo(hardware) central que administre o gestione la recepcion y salida de llamadas telefónicas ?				
	Cual es la Marca del Dispositivo (Hardware)?				
	Tipo de troncales de líneas o troncales ?				
	Tipo de entrada PSTN ?				
	Cuenta con voz sobre IP para los Usuarios internos PBX ?				
	Tiene modulo ACD?				
	Cuenta con disparadores CTI ?				
	Cuentan con sistemas de grabacion ?				
	De tener VozIP que codec utiliza, cuentas extensiones tiene ?				
	Se tiene un modulo de administracion ?				
	Respeto la arquitectura o-lan /e-lan?				
	Cuenta con tarjeta FXS FX0 o TRANSCODIN ?				
	Cuantos e1 se tiene para entrada PSTN ?				
	La Universidad cuenta con Dispositivos Switch de cape 3? si es si que Marca y Modelo?				
	Que Clase de Topología Utiliza La Universidad en su Area de recepcion de llamadas?				
	Que clase de direccionamieto Maneja Actualmente la Universidad en la red?				

Anexo 3 Formato diligenciado de la información técnica USB

FORMATO 01: FORMATO DILIGENCIADO POR EL DEPARTAMENTO DE SOPORTE TECNOLÓGICO DE LA UNIVERSIDAD SAN BUENAVENTURA SEDE BOGOTÁ, CONTIENE INFORMACIÓN TÉCNICA DE LA RED DE COMUNICACIONES DE LA UNIVERSIDAD SANBUENAVENTURA BOGOTÁ.

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ, D.C.	FORMATO:001	fecha: 22 / 04 / 2013	PROGRAMA: Ingeniería de Telecomunicaciones	
	ESTUDIANTES	Guillermo Nuñez Arciniegas cod: 20071236035 Jairo David Mesa cod: 20071236030	Observaciones:	Desarrollo de Investigación Proyecto de Grado
Descripción de la Actividad	RECOLECCION INFORMACION DE ESPECIFICACIONES TECNICAS RED LAN UNIVERSIDAD SAN BUENAVENTURA BOGOTÁ COLOMBIA PARA EL PROYECTO DE GRADO			
Resumen de la Actividad*	Recolectar información básica sobre la infraestructura de comunicaciones de las universidades San Buenaventura.			
	PREGUNTAS	Si	No	Comentarios
	La Universidad cuenta actualmente con un sistema o plataforma de recepción y salida de llamadas telefónicas.	X		
	Existe un departamento o dependencia que realice la labor de recepción y salida de llamadas telefónicas.	X		Las llamadas locales de entrada y salida que no pasan directamente a la extensión son recibidas por la recepción. La salida de llamadas a números especiales, nacionales, internacionales y celular salen por Recepción. A su vez en campañas especiales se dan permisos específicos a Promoción y Admisiones y a las Facultades.
	La Universidad cuenta actualmente con un dispositivo (hardware) central que administre o gestione la recepción y salida de llamadas telefónicas	X		Planta telefónica básica
	¿Cuál es la Marca del Dispositivo (Hardware)?	En producción actual: 3COM NBX 100 y 3COM		

	NBX V3000 En dos meses aproximadamente se cambiará por una nueva solución basada en Asterisk
Tipo de troncales de líneas o troncales	Troncal E1 y 4 celufijos
Tipo de entrada PSTN	E1
Cuenta con voz sobre IP para los Usuarios internos PBX	En producción actual: Solución digital, pero no VoIP Con nueva solución: VoIP
Tiene módulo ACD	En producción actual: No posee ACD Con nueva solución: Tiene un módulo básico de Call Center
Cuenta con disparadores CTI	No tenemos información al respecto
Cuentan con sistemas de grabación	Las grabaciones solo se aplican para buzones de voz.
De tener VozIP ¿qué códec utiliza, cuentas extensiones tiene?	El códec es nativo de 3COM. Las extensiones en uso son de 250 con un máximo de crecimiento a 250
Se tiene un módulo de administración	Incorporado en la NBX V3000
Respeto la arquitectura c-LAN /e-LAN?	No tenemos información al respecto
Cuenta con tarjeta FXS FX0 o TRANSCODIN?	En producción actual: Para los 4 celufijos se tiene entradas análogas y 3 que salen a través de extensión telefónica (ATA) Con nueva solución: Se tendrá FXO para los 4 celufijos
Cuantos e1 se tiene para entrada PSTN?	Un E1 en funcionamiento actual y un E1 adicional para implementar con la nueva solución
La Universidad cuenta con Dispositivos Switch de cape 3. Si es sí que Marca y Modelo	Sí. Marca 3COM en varios modelos desde 4228 hasta 5500G
¿Qué Clase de Topología de red utiliza la Universidad en su Área de recepción de llamadas?	No es clara la solicitud para dar respuesta
¿Qué clase de direccionamiento IP Maneja actualmente la Universidad en la red?	Direccionamiento privado, segmentado por VLANS

Anexo 4 Especificaciones técnicas de la PBX 3COM NBX100

Com NBX 100 Phone System

The 3Com NBX 100 Phone System, the first commercially available IP PBX product, introduced the world to the value of networked telephony in 1998. The most popular IP-PBX system in the world, it delivers exceptional investment assurance.

The 3Com NBX 100 supports up to 200 devices/100 PSTN lines. It connects your remote workers directly through their Internet router, and reliably connects multiple intra-company sites - across town or around the globe - with low-cost IP virtual tie lines. Adding locations and capacity is easy: the 3Com NBX 100 and Super Stack 3 NBX telephony solutions both use the same system software.

The award-winning 3Com NBX 100 phone system delivers crystal-clear, toll-quality voice communications. It brings 10/100 Mbps performance to users' worktops, and is radically simple to use. It delivers the benefits of voice-over-IP (VoIP) and advanced voice messaging - without the high costs and operational complexity of TDM PBX or proprietary IP systems.

- Supports up to 200 devices, including up to 100 central office (CO) lines
- Ensures high system availability with the Wind River VxWorks real-time operating system (also used in pacemakers and artificial hearts), so server and PC downtime does not impact your telephone service
- Has powerful call-processing features built in: voice mail, automated attendant, hunt/call groups, call detail reporting, computer telephony integration (CTI), PC-based visual voice mail/email clients (IMAP4), and more
- Easily integrates a wide range of off-the-shelf applications, including customer relationship management (CRM), call centers, and speech recognition; 3Com NBX Solution Providers Program delivers a broad range of productivity-enhancing applications for use with 3Com voice solution platforms
- Software-based 3Com NBX WAV application ports make TAPI/WAV CTI affordable
- Simplifies voice mail message exchange between sites with optional 3Com NBX VPIM Multisite Messaging Exchange
- Offers an extensive range of multisite voice networking options: 3Com NBX IP Virtual Tie Lines, NBX ConneXtions H.323 gateway software, and T1/E1 PRI/Q.SIG
- Supports telecommuters and remote access users with optional 3Com NBX IP licenses
- Simplifies day-to-day operation with Web-based administration and user programming
- Can eliminate the cost and administrative overhead of two separate networks for data and voice
- Offers a wide range of worktop options: 3Com NBX business phones—the 1102 (shared 10 Mbps port), the second generation 2102 (switched 10/100 port), the 2102-IR (switched 10/100 Mbps with infrared beaming port), and the 2101 (basic phone set with 10/100 Mbps port)—plus NBX Attendant Console (with up to 100 available functions), NBX pcXset (softphone client), and legacy analog phone and fax devices (2500 series compatible)
- Compatible with a range of 3Com and third-party products, including the optional 3Com NBX Call Center application and 3Com NBX Unified Communications
- Available in any one of 10 languages/dialects
- Compatible with other 3Com networked telephony solutions, easing growth to larger systems and preserving your telephony investments

Anexo 5 Configuración completa de switch core cisco

- SWITCH CORE

```
hostname SW_CORE
boot-start-marker
boot system bootflash:cat4500-ipbasek9-
mz.150-2.SG4.bin
boot-end-marker
enable secret 5
$1$p4ft$Y1U69f.qPhb0OQxulaawN/
username adminbilateral password 7
052315577406593F494F4647
no aaa new-model
ip subnet-zero
ip domain-name USB IPCC.BOG
ip vrf mgmtVrf
vtp mode transparent
power redundancy-mode redundant
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
vlan 20-25 // 20 admon 25 agentes
vlan 60
name VOZ
vlan 500
name transit
ip ssh time-out 30
ip ssh version 1
interface FastEthernet1
ip vrf forwarding mgmtVrf
no ip address
speed auto
duplex auto
!
interface FastEthernet 1/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet /2
switchport trunk encapsulation dot1q
switchport mode trunk
speed 100
duplex full
!
interface FastEthernet /3
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet 1/4
switchport access vlan 25
speed 100
duplex full
!
```

```
interface FastEthernet 1/5
switchport access vlan 25
speed 100
duplex full
spanning-tree portfast
!
interface FastEthernet 1/6
switchport access vlan 25
speed 100
duplex full
spanning-tree portfast
!
interface FastEthernet 1/7
switchport access vlan 25
switchport mode access
!
interface FastEthernet 1/8
switchport access vlan 25
switchport mode access
!
interface FastEthernet 1/9
switchport access vlan 20
switchport mode access
!
interface FastEthernet 1/10
switchport access vlan 25
switchport mode access
!
interface FastEthernet 1/11
switchport access vlan 25
switchport mode access
!
interface FastEthernet 1/12
switchport access vlan 25
switchport mode access
!
interface FastEthernet 1/13
switchport access vlan 25
switchport mode access
!
interface FastEthernet 1/14
switchport access vlan 25
switchport mode access
!
interface FastEthernet /15
switchport access vlan 20
switchport mode access
!
interface FastEthernet 1/16
switchport access vlan 20
switchport mode access
!
interface FastEthernet 1/17
```



```
shutdown
!  
interface FastEthernet 1/18  
shutdown  
!  
interface FastEthernet 1/19  
shutdown  
!  
interface FastEthernet 1/20  
switchport access vlan 500  
shutdown  
speed 100  
duplex full  
!  
interface FastEthernet 1/21  
switchport access vlan 500  
!
```

```
shutdown  
speed 100  
duplex full  
!  
interface FastEthernet 1/22  
switchport access vlan 500  
shutdown  
speed 100  
duplex full  
!  
interface FastEthernet 1/23  
shutdown  
!  
interface FastEthernet 1/24  
shutdown
```

Anexo 6 Configuración completa de switch Core Cisco

COTIZACIÓN HP ProLiant ML 310 G8



*Tintas *Tóneres *Accesorios *Portátiles
*Redes *Ups *Wireless *Computadores
*Alquiler Computadores *Impresoras

COTIZACION

713-3169

DIA	MES	AÑO
16	08	2013

EMPRESA :				e-mail:			
CONTACTO:	GUILLERMO NUÑEZ			TEL/CEL	3015062438		
DIRECCION:				CIUDAD:	BOGOTÁ		
DESCRIPCION	CANT	VR.UNITARIO	VR. TOTAL				
SERVIDOR HP ProLiant ML310e Gen8 serie SATA (Reemplazo del ML110 G7) - LFF Intel® Xeon® Quad-Core E3-1220v2 - 3.1GHz, 8MB L3 Cache, 4GB RAM, 1 Procesador, Disco Duro de 1TB, DVD-RW, iLO Management Engine Standard, Formato Torre, convertible a 4U para RACK mediante opcional que lo habilita, Procesador Intel® Xeon™ Quad-Core E3-1220v2 de 3.1 GHz, 8MB Level 3 cache - 69 Watts, E3-1200 Series. Posee de fabrica 1 Procesador. Crecimiento soporta para un procesador (1 socket, hasta 4 cores) Chipset Intel C204. Familia de procesadores E3-1200v2 / Procesador de 69 Watts. Memoria RAM Estándar 4GB (1x4GB) UDIMM, Máximo 32 GB. Soporta sólo UDIMM. Más Información: www.hp.com/go/DDR3memory-configurator Controlador estándar Modelo 689063-001 posee estándar B120i/Zero Memory. Soporta RAID 0/1/1+0 (sólo SATA), Capacidad de discos máximo estándar: 12TB SATA Non-Hot-Plug (4 x 3TB SATA), con discos opcionales. Incluye unidad óptica (DVD-RW), Máximo opcional: 12TB Hot-Plug LFF (4 x 3TB SAS o SATA LFF) u 8TB Hot-Plug SFF (8 x 1TB SAS o SATA SFF) con el reemplazo del cajón de discos duros y su respectiva controladora SAS adicional. Slot de ampliación 4 PCI-Express slots estándar: Un PCIe 3.0 x16 (velocidad x8); Un PCIe 3.0 x8 (velocidad x8); Un PCIe 2.0 x8 (velocidad x4) y Un PCIe 2.0 x4 (velocidad x1). Controlador de red (2) dos puertos de 1Gb - HP 330L 1Gb Full Duplex RJ45 con soporte para velocidades 10/100/1000 Mb/s, Puertos externos: Serial: 1, Video: 1, Network RJ-45: 2, ILO 4: 1 (opcional), USB 2.0: 10 (4 frontales, 4 traseros, 2 Internos), 1 Internal SD Slot. Fuente de poder y refrigeración, Estándar una fuente de poder de 350Watts no removible en caliente. Dos ventiladores no removibles en caliente, no redundantes. (Garantía 1AÑO)	1	1,825,000	1,825,000				
SERVIDOR LENOVO THINK SERVER TS130 - INTEL XEON 4C E3-1225v2 77W, OSL_no preload, 500GB SATA 6Gb/s, 3.5" Thermal Kit, 4GB 2RX8 PC3-10600E ECC-UDIMM DDR3-1333 2GBIT, DVD Burner/CD-RW Rambo 8 (SATA), 280W 85+ PSU, No HDD Cable, No FDD, RAID 0/1 Setup by customer. AMT 7.0 completamente gratis precargado en el equipo, 3 años On site	1	1,982,758	1,982,758				
SERVIDOR IBM i1 NUEVO MODELO M4 2582EHU!! Express x3100 M4, Xeon 4C E3-1220v2 69W 3.1GHz/1600MHz/8MB, 1x4GB, SS 3.5In SATA, SR C100, Multi-Burner, 350W p/s, Tower 1 AÑO DE GARANTIA 5X9 - NO INCLUYE DISCOS	1	1,219,827	1,219,827				
DISCO PARA SERVIDOR IBM 39M4514 500 GB S-ATA Simple-swap 3Gb/s HDD	1	474,113	474,113				
Licencia para servidor Win Svr Std 2012 x64 SPA 1pk DSP OEI DVD 2CPU/2VM parte P73-05338	1	1,698,275	1,698,275				
			SUBTOTAL			7,199,973	
			IVA			1,151,996	
			TOTAL			8,351,969	

FORMA DE PAGO: TRANSFERENCIA EFECTIVO

DISPONIBILIDAD: INMEDIATA

BLANCA CASTAÑO
Asesor Comercial
TEL. 6112247-6221436
7030910-7030883

CRA 16 N. 79-20 OF 713 Telefax : +67 (1)6112247 Cel:3124506043 Oficina +67 (1) 6 221436 -7030910-7030883

e-mail : ventas@allware.com.co / Bogota D.C. Colombia www.allware.com.co

Anexo 7 Configuración del Squid para que el proxy haga las veces de filtrado

```
##### DEFINICION ACL #####
acl red_local src 10.248.119.0/24-10.248.118.0/24-10.249.49.0/24-10.249.50.0/24-
10.249.48.0/26
acl permitidas dstdom_regex www.usbbog.edu.co 10.249.48.144
#Recommended minimum configuration:
#acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80 # http
#acl Safe_ports port 21 # ftp
acl Safe_ports port 8080-8585 # https
#acl Safe_ports port 70 # gopher
#acl Safe_ports port 210 # wais
acl CONNECT method CONNECT
#acl Safe_ports port 1025-65535 # unregistered ports
#acl Safe_ports port 280 # http-mgmt
#acl Safe_ports port 488 # gss-http
#acl Safe_ports port 591 # filemaker
#acl Safe_ports port 777 # multiling http
acl apache rep_header Server ^Apache
acl QUERY urlpath_regex cgi-bin \?
```

La siguiente es la definición de las ACL y/o objetos que más adelante serán llamados.

Acá se definen las reglas de acceso a internet

```
http_access allow permitidas
http_access allow localhost
http_access deny all
#####
#####
visible_hostname PROXY
##### REGLAS PARA PAGINAS
#####
icp_access allow all
#####
#####
```

```

##### PUERTO ASIGNADO
#####
http_port 8080
#####
#####
hierarchy_stoplist cgi-bin ?
#####
#####
cache_dir ufs /var/spool/squid 2048 16 256
#####
#####
access_log /var/log/squid/access.log squid
#####
#####
cache deny QUERY

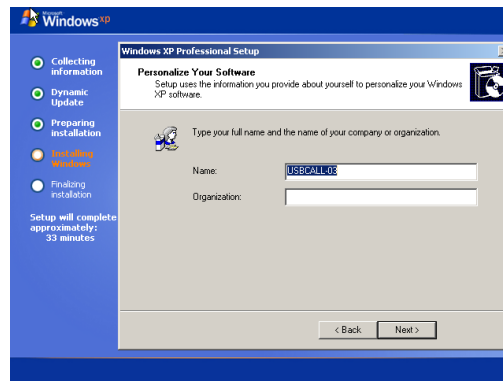
#####
#####
refresh_pattern ^ftp:          1440 20% 10080
refresh_pattern ^gopher:      1440 0% 1440
refresh_pattern .              0 20% 4320
#####
#####
#broken_vary_encoding allow apache
#####
#####
coredump_dir /var/spool/squid
#####
#####

```

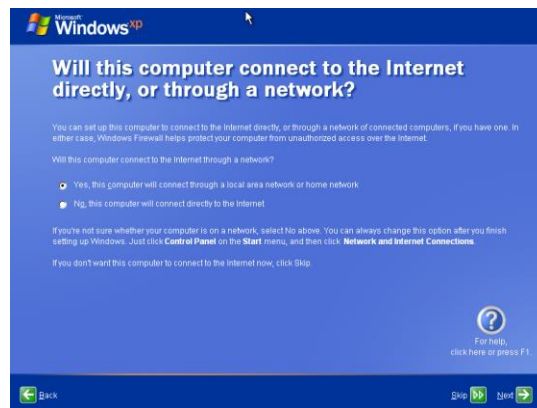
Anexo 8 Configuración de Sistema Operativo para Agente Tele operador

El sistema operativo configurado en las estaciones de tele operador es Windows XP Profesional SP3, con actualizaciones críticas a la fecha.

Es importante nombrar a los equipos en la red, además de configurar estáticamente las direcciones IP. En este caso el administrador elige la forma de hacerlo. Como se procede en el siguiente ejemplo:



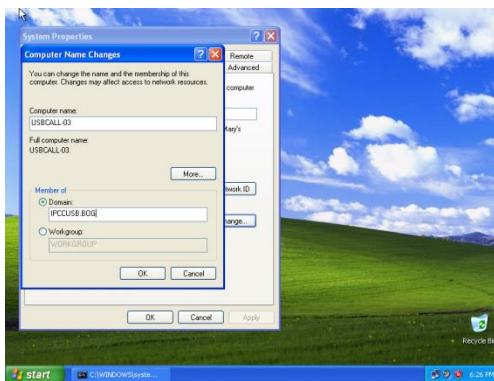
Se realizan las respectivas configuraciones como zona horaria, configuración de interconexión entre otras. Por último registramos la maquina ante Microsoft.



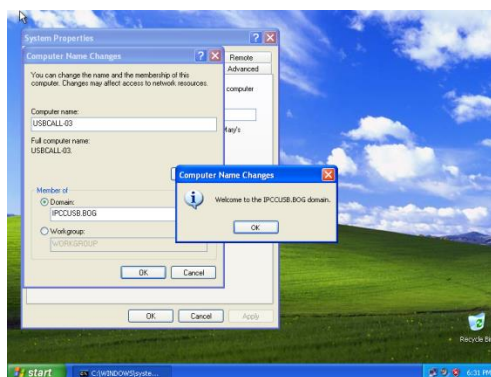
Luego de esta lista, y de haber hecho la instalación de todo el software es necesario para la operación cambiar la contraseña del administrador y luego agregar la estación al dominio como se ilustra a continuación:



Se configura el nombre de la máquina y se agrega la estación como miembro del dominio en este caso es IPCCUSB.BOG



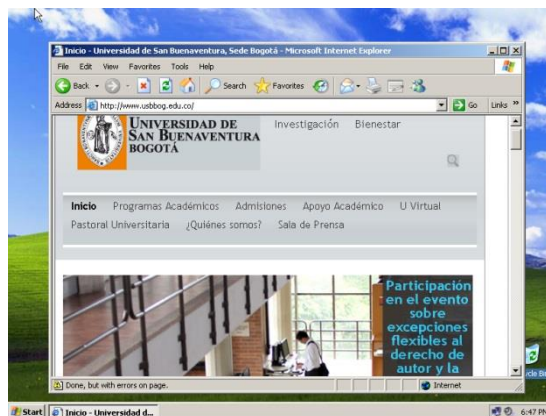
El sistema solicitará autenticación del usuario con privilegios del dominio. En este caso será el administrador01 con su respectiva contraseña, y luego se oprime ok y se reinicia la estación.



Como se puede observar ya la estación hace parte del dominio, para ello entonces se autentica el usuario con las credenciales correspondientes como: el nombre del usuario y la respectiva contraseña.



El servidor se encargará de aplicar las políticas configuradas por el administrador de red en gestión de políticas GPO y en herramientas administrativas del servidor controlador de dominio.



Anexo 9 Equipo Agente Tele Operador. .

EQUIPO	Optiplex 380
PANORAMA	
Computadora de Operaciones: producción	Ubicación: IPCC USB BOGOTA Modelo: Minitorre Sistema Operativo: Windows XP SP3 CPUs: intel Core 2 duo @ 2.93GHz Memory: 1GB RAM Total Disk: 160 GB Entorno de Sistema: Entorno Windows System Serial #: 13Z9MM1 DNS: 10.249.48.67 - 10.249.48.68 Rango Dir IP: 192.168.0.1-192.168.0.100 otro: NA
Contactos	
Proveedor de Hardware	DELL
Propietarios del sistema	Administrador IPCC
Propietario de Bases de Datos	NA
Propietario de Aplicaciones	Soporte Técnico
Proveedor de Software	Microsoft
Estrategia de Respaldo para el Sistema	
Diario	NA
Mensual	OK
Trimestral	NA
PROCEDIMINETO DE RECUPERACION DE DESASTRES	
<u>Escenario 1</u> La pérdida Total de Datos	Se restaura una de las imágenes que se tendrá de apoyo
<u>Escenario 2</u> La pérdida total del disco	La parte afectada es cambiada y luego se verifica su correcto funcionamiento

Anexo 10 Dispositivo SW-CORE IPCC USB Bogotá.

EQUIPO	Cisco Catalyst 2950
PANORAMA	
Dispositivo de Producción	<p>Ubicación: IPCC USB BOGOTA</p> <p>Modelo: Cisco Catalyst 2950</p> <p>Sistema Operativo: cat2900-IPBASEK9-M</p> <p>Puertos: 24 x 10/100/1000 + 2 x SFP</p> <p>Protocolo de Gestion: IGMP</p> <p>Protocolo de Gestion Remota: SNMP 1, SNMP 2, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH-2</p> <p>Cumplimiento de Normas: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q 802.3ab, IEEE, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)</p> <p>Sistema de Manejo : SSH-HTTP</p> <p>Fuente de Poder: CA 120/230 V(50/60 Hz)</p> <p>DNS: N/A</p> <p>IP Address: VLAN ADMON 192.168.1.X</p> <p>Other: NA</p>
Contactos	
Proveedor de Hardware	Cisco
Propietarios del sistema	Administrador IPCC
Propietario de Bases de Datos	NA
Propietario de Aplicaciones	Soporte Técnico
Proveedor de Software	Microsoft
Estrategia de Respaldo para el Sistema	
Diario	NA
Mensual	OK
Trimestral	NA
PROCEDIMINETO DE RECUPERACION DE DESASTRES	
<u>Escenario 1</u> La pérdida Total de Datos	se copia el archivo de configuración IOS y se reestablece
<u>Escenario 2</u> La pérdida total del disco	Se solicita garantía del equipo al constructor

Anexo 11 Central ASTERISK IPCC USB Bogotá.

EQUIPO	HP Proliant ML 310 G8
---------------	------------------------------

PANORAMA	
Servidor de producción	Ubicación: IPCC USB BOGOTA Modelo: Tipo-Torre Sistema Operativo: Linux Centos CPUs: Intel(R) Xeon(R) CPU X3430 @ 2.40GHz [1 core(s) x86] Memoria: 4 GB RAM Total Disk: 1.25 T Sistema de Manejo: SSH-HTTP Entorno de Sistema: Asterisk Sistema Serial #: MX211600CE DNS: x.x.x.x Dirección IP : 192.168.1.x Otro: NA
Contactos	
Proveedor de Hardware	HP-Hewlett Packard
Propietarios del sistema	IPCC USB
Propietario de Bases de Datos	NA
Propietario de Aplicaciones	Soporte Técnico
Proveedor de Software	http://www.asterisk.org/

Estrategia de Respaldo para el Sistema	
Diario	NA
Semanal	OK
Mensual	NA

PROCEDIMINETO DE RECUPERACION DE DESASTRES	
<u>Escenario 1</u> La pérdida Total de Datos	Se carga los archivos de copia de seguridad contenidas en el Back up y se inicia los servicios de configuración
<u>Escenario 2</u> La pérdida total del disco	La parte afectada es cambiada y luego se verifica su correcto funcionamiento y estabilidad del sistema.

Anexo 12 Firewall IPCC USB Bogotá.

EQUIPO	HP Proliant ML 310 G8
---------------	------------------------------

PANORAMA	
Servidor de producción	Ubicación: IPCC USB BOGOTA Modelo: Tipo-Torre Sistema Operativo: Linux Centos CPUs: Intel(R) Xeon(R) CPU X3430 @ 2.40GHz [1 core(s) x86] Memoria: 4 GB RAM Total Disk: 1.25 T Sistema de Manejo : SSH-HTTP Entorno de Sistema: Webmin-Linux Centos Sistema Serial #: MX211600CE DNS: x.x.x.x Dirección IP-LAN: 192.168.1.1 Dirección IP-WAN: ASIGNADO POR EL ISP Otro: NA
Contactos	
Proveedor de Hardware	HP-Hewlett Packard
Propietarios del sistema	IPCC USB
Propietario de Bases de Datos	NA
Propietario de Aplicaciones	Soporte Técnico
Proveedor de Software	http://www.centos.org/

Estrategia de Respaldo para el Sistema	
Diario	NA
Semanal	OK
Mensual	NA

PROCEDIMINETO DE RECUPERACION DE DESASTRES	
<u>Escenario 1</u> La pérdida Total de Datos	Se carga los archivos de configuración contenidas en back up, inicio del servicio y verificar estado de la configuración.
<u>Escenario 2</u> La pérdida total del disco	La parte afectada es cambiada y luego se verifica su correcto funcionamiento y estabilidad del sistema.

Anexo 13 File server y proxy server IPCC USB Bogotá

EQUIPO	HP Proliant ML 310 G8
---------------	------------------------------

PANORAMA	
Servidor de producción	Ubicación: IPCC USB BOGOTA Modelo: Tipo-Torre Sistema Operativo: Linux Centos CPUs: Intel(R) Xeon(R) CPU X3430 @ 2.40GHz [1 core(s) x86] Sistema de Manejo : SSH-HTTP Memoria : 4 GB RAM Total Disk: 1.25 T Entorno de Sitema: Webmin-Linux Centos System Serial #: MX211600CE DNS: x.x.x.x IP Address INT-01: 192.168.1.x / PROXY IP Address INT-02: 192.168.1.x/ FILE SERVER
Contactos	
Proveedor de Hardware	HP-Hewlett Packard
Propietarios del sistema	IPCC USB
Propietario de Bases de Datos	NA
Propietario de Aplicaciones	Soporte Técnico
Proveedor de Software	http://www.centos.org/

Estrategia de Respaldo para el Sistema	
Diario	NA
Semanal	OK
Mensual	NA

PROCEDIMINETO DE RECUPERACION DE DESASTRES	
<u>Escenario 1</u> La pérdida Total de Datos	Se carga los archivos de configuración contenidas en back up, inicio del servicio y verificar estado de la configuración.
<u>Escenario 2</u> La pérdida total del disco	La parte afectada es cambiada y luego se verifica su correcto funcionamiento y estabilidad del sistema.

Anexo 14 IDS IPCC USB BOGOTA

EQUIPO	PCs Desktop HP Compaq Pro 6000
---------------	---------------------------------------

PANORAMA	
Servidor de producción	Ubicación: IPCC USB BOGOTA Modelo: Tipo-Torre Sistema Operativo: Linux Centos CPUs: AMD Quad-Core A10-5800B Memoria: 4 GB RAM Total Disk: 250 GB Entorno de Sistema: Webmin Sistema Serial #: MX6000 Sistema de Manejo : SSH-HTTP DNS: x.x.x.x Dirección IP INT-01: 192.168.1.x Dirección IP INT-02: 192.168.1.x
Contactos	
Proveedor de Hardware	HP-Hewlett Packard
Propietarios del sistema	IPCC USB
Propietario de Bases de Datos	NA
Propietario de Aplicaciones	Soporte Técnico
Proveedor de Software	http://www.centos.org/

Estrategia de Respaldo para el Sistema	
Diario	NA
Semanal	NA
Mensual	OK

PROCEDIMINETO DE RECUPERACION DE DESASTRES	
<u>Escenario 1</u> La pérdida Total de Datos	Se carga los archivos de configuración contenidas en back up, inicio del servicio y verificar estado de la configuración.
<u>Escenario 2</u> La pérdida total del disco	La parte afectada es cambiada y luego se verifica su correcto funcionamiento y estabilidad del sistema.

Anexo 15 Servidor controlador de dominio y directorio activo IPCC USB Bogotá

EQUIPO	HP Proliant ML 310 G8
PANORAMA	
Servidor de producción	Ubicación: IPCC USB BOGOTA Modelo: Tipo-Torre Sistema Operativo: Microsoft Windows Server 2008 R2 Standard Edition CPUs: Intel(R) Xeon(R) CPU X3430 @ 2.40GHz [1 core(s) x86] Memoria: 8 GB RAM Total Disk: 1.25 T Entorno de Sistema : Windows Server 2008 st Sistema Serial #: MX211600CE DNS : x.x.x.x Dirección IP : 192.168.1.x Otro: NA
Contactos	
Proveedor de Hardware	HP-Hewlett Packard
Propietarios del sistema	IPCC USB
Propietario de Bases de Datos	NA
Propietario de Aplicaciones	IPCC USB BOGOTA
Proveedor de Software	http://www.microsoft.com/es-co/default.aspx

Estrategia de Respaldo para el Sistema	
Diario	NA
Semanal	NA
Mensual	OK

PROCEDIMINETO DE RECUPERACION DE DESASTRES	
<u>Escenario 1</u> La pérdida Total de Datos	se restaura configuración back Up , dicho Back Up debe ser configurado desde un Disco Externo de Almacenamiento y tenerlo disponible para eventuales fallas
<u>Escenario 2</u> La pérdida total del disco	la parte afectada es cambiada y luego se verifica su correcto funcionamiento

Anexo 16 Planta eléctrica diesel 437-DE16SS

MODELO	437-DE16SS
	ALTERNATOR // ALTERNADOR
Type // Tipo	Single Phase // Monofásico
Prime Power (kVA) // Salida Continua (Kva.)	15.5
Max. Output (kVA) // Salida Máxima (Kva.)	17
Power Factor // Factor de Potencia	1
Rated Frequency (Hz) // Frecuencia Nominal (Hz)	60
Rated Voltage (V) // Voltaje Nominal (V)	120 / 240
Rated Current (A) // Amperaje (Amp)	129.2 / 64.6
Max. Current Per Phase (A) // Amperaje Máx. x Fase	N/A
	CHARACTERISTICS // CARACTERÍSTICAS
Type // Tipo	Super Silent Cabin // Cabinada Super Silenciosa
Noise Level (7m) dB(A) // Nivel de Ruido en dB(A) 7m	53
Excitation Mode // Modo de Generación	Self-Excitation and Constant Voltage (AVR) // Autoexcitación y Voltaje Continuo (AVR)
Fuel Tank Capacity (L) // Cap. Tanque Combustible (L)	65
Fuel Tank Capacity (gal) // Cap. Tanque Combustible (gal)	17
Autonomy (h) // Autonomía (hr)	9
Lube Oil Type // Tipo de Aceite de Lubricación	SAE15W40
	TECHNICAL SPECIFICATIONS (MOTOR) // ESPECIFICACIONES TECNICAS (MOTOR)
Motor Model // Modelo Motor	437-488G
Motor Type // Tipo Motor	YANMAR 4TNV88
Power (hp) // Potencia (hp)	26.28
Power [Kw] // Potencia [Kw]	19.6
Displacement (c.c.) // Desplazamiento (c.c.)	2190
Rotational Speed (rpm) // Velocidad (rpm)	1800
Starting System // Tipo arranque	Electrico // Eléctrico
Motor Type // Tipo motor	4 Stroke Naturally Aspirated // 4 Tiempos Aspiración Natural
Number of Cylinders // Número de Cilindros	Inline 3 Cylinder // 3 en Línea
Cooling System // Refrigeración	Water Cooled // Enfriado por Agua

Anexo 17 Pila de puertos aceptados en reglas del Firewall

Puerto/protocolo	Descripción
20/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - datos
21/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - control
22/tcp	SSH, scp, SFTP
25/tcp	SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)
43/tcp	nickname
53/tcp	DNS Domain Name System (Sistema de Nombres de Dominio)
53/udp	DNS Domain Name System (Sistema de Nombres de Dominio)
69/udp	TFTP Trivial File Transfer Protocol (Protocolo Trivial de Transferencia de Ficheros)
80/tcp	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (WWW)
85/tcp	Puerto de informacion
88/tcp	Kerberos Agente de autenticación
110/tcp	POP3 Post Office Protocol (E-mail)
445/tcp	Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)
445/udp	Microsoft-DS compartición de ficheros
514/udp	syslog usado para logs del sistema
1433/tcp	Microsoft-SQL-Server
1434/tcp	Microsoft-SQL-Monitor
1434/udp	Microsoft-SQL-Monitor
1512/tcp	WINS Windows Internet Naming Service
2049/tcp	NFS Archivos del sistema de red
2086/tcp	Web Host Manager puerto por defecto
2427/udp	Cisco MGCP
3128/tcp	HTTP usado por web caches y por defecto en Squid cache
3128/tcp	NDL-AAS
3306/tcp	MySQL sistema de gestión de bases de datos
5000/tcp	Universal plug-and-play
5060/udp	Session Initiation Protocol (SIP)
6000/tcp	X11 usado para X-windows
8080/tcp	HTTP HTTP-ALT ver puerto 80. Tomcat lo usa como puerto por defecto.
10000/tcp	Webmin (Administración remota web)

Anexo 18 ficheros del Firewall

```
#####
##### zones #####
[root@FIREWALL ~]# /etc/shorewall/zones
#
# Shorewall version 3.4 - Sample Zones File for three-interface configuration.
# Copyright (C) 2006 by the Shorewall Team
#
# This library is free software; you can redistribute it and/or
# modify it under the terms of the GNU Lesser General Public
# License as published by the Free Software Foundation; either
# version 2.1 of the License, or (at your option) any later version.
#
# See the file README.txt for further details.
#-----
# For information about entries in this file, type "man shorewall-zones"
#
# For more information, see http://www.shorewall.net/Documentation.htm#Zones
#
#####
#ZONE TYPE  OPTIONS          IN          OUT
#          OPTIONS          OPTIONS
fw  firewall
net  ipv4
loc  ipv4
vpn  ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
#####
##### interfaces #####

#ZONE INTERFACE  BROADCAST  OPTIONS
net  eth1      detect    tcpflags,dhcp,routefilter,nosmurfs,logmartians
loc  eth0      detect    tcpflags,detectnets,nosmurfs
-    ppp+      -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
#####
##### masq #####
[root@FIREWALL ~]# /etc/shorewall/masq

eth1      192.168.0.0/24    IP PUBLICA ASIG POR ISP
eth1      192.168.1.0/24    IP PUBLICA ASIG POR ISP
eth1      192.168.2.0/24    IP PUBLICA ASIG POR ISP
#ppp+     192.168.0.0/24    IP PUBLICA ASIG POR ISP
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
#####
##### nat #####
[root@FIREWALL ~]# /etc/shorewall/nat

#EXTERNAL INTERFACE  INTERNAL  ALL  LOCAL
#          INTERFACES
```

```

##IP-ASIGNADO POR ISP   eth1 192.168.1.1 yes no
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
#####
##### rules #####
[root@FIREWALL ~]# /etc/shorewall/rules

#ACTION      SOURCE      DEST      PROTO DEST  SOURCE      ORIGINAL  RATE      USER/
#           PORT  PORT(S)  DEST  LIMIT  GROUP
#           PORT  PORT(S)  DEST  LIMIT  GROUP
#
#   Accept DNS connections from the firewall to the network
#
DNS/ACCEPT   $FW        net
#
#   Accept SSH connections from the local network for administration
#
SSH/ACCEPT   loc        $FW
SSH/ACCEPT   net        $FW
SSH/ACCEPT   vpn        $FW
#
#   Allow Ping from the local network
#
Ping/ACCEPT  loc        $FW
Ping/ACCEPT  loc        loc
Ping/ACCEPT  vpn        loc
#
POP3/ACCEPT  loc        all
SMTP/ACCEPT  loc        all
# Reject Ping from the "bad" net zone.. and prevent your log from being flooded..
#

Ping/ACCEPT  net        $FW
ACCEPT       $FW        loc        icmp
ACCEPT       $FW        net        icmp
ACCEPT       $FW        vpn        icmp
#REDIRECT    loc        8080      tcp      80
#####
ACCEPT       loc        net        tcp 20,21,22,43,53,80,85,443,1024:65535,8080
ACCEPT       loc        net        udp 43,53,123,443,1024:65535
ACCEPT       loc        $FW        udp 80,4550,5550,85,3650,85,8080
ACCEPT       net        $FW        tcp 10000
ACCEPT       net        $FW        tcp 80,4550,5550,85,3650,85,8080
ACCEPT       net        loc        tcp 80,4550,5550,85,3650,85,8080
ACCEPT       net        loc        tcp 4050
ACCEPT       $FW        vpn        47
ACCEPT       vpn        $FW        tcp 1723
ACCEPT       vpn        $FW        47
ACCEPT       net:DNS ASIGNADO POR ISP all
ACCEPT       net:DNS ASIGNADO POR ISP all
DROP        net        loc        tcp 135,139
#####
DNAT         net        loc:192.168.1.1 tcp 1:2000 - IP-ASIGNADO POR ISP
DNAT         net        loc:192.168.1.1 udp 1:30000 - IP-ASIGNADO POR ISP
DNAT         net        loc:192.168.1.1 tcp 1720 - IP-ASIGNADO POR ISP

```

```

DNAT    net      loc:192.168.1.99 udp 80,4550,5550,85,3650,85,8080 - IP-ASIGNADO POR ISP
DNAT    net      loc:192.168.1.99 tcp 80,4550,5550,85,3650,85,8080 - IP-ASIGNADO POR ISP
#####
#####
DNAT    net      vpn:192.168.0.1 tcp 1723    - IP-ASIGNADO POR ISP
DNAT    net      vpn:192.168.0.1 47 -      - IP-ASIGNADO POR ISP
DNAT    net      loc:192.168.0.1 tcp 1:2000  - IP-ASIGNADO POR ISP
DNAT    net      loc:192.168.0.1 udp 1:30000 - IP-ASIGNADO POR ISP
DNAT    net      loc:192.168.0.1 tcp 1720   - IP-ASIGNADO POR ISP
#####
#DNAT   net      loc:192.168.1.99 udp 1:20000 - 190.144.156.39
#####
#REDIRECT  loc      8080      tcp 80
#####
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
#####
##### routestopped #####
[root@FIREWALL ~]# /etc/shorewall/routestopped
#####
#INTERFACE  HOST(S)
#eth1      -
#eth2      -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE

```

Anexo 19 Pasos para el diseño del Firewall

1. Se procede a descargar Shorewall 3.4.6-2. formato RPM
2. Se descarga CentOS 5.9 desde la página oficial en la sección de descargas en <http://www.shorewall.net>
3. Se instala rpm -Uvh shorewall-3.4.6-2.noarch.rpm
4. Se copian los archivos de configuración desde /usr/share/doc/shorewall/default-config a /etc/shorewall.
5. Quedando de esta forma en raíz:
 - a. cd /usr/share/doc/shorewall/default-config
 - b. cp * /etc/shorewall/
6. Se debe tener en cuenta que los ficheros que se configuran se encuentran en el directorio /etc/shorewall, y los que se configuraran serán los siguientes: **zones, interfaces, policy, NAT, rules, routestopped.**
7. En CentOS se configurará el shorewall.conf en la siguiente raíz /etc/shorewall/shorewall.conf
8. Se define principalmente en CentOS el parámetro STARTUP_ENABLED, este sirve para activar Shorewall, en el vamos a encontrar NO por default, y este debe ser activado en la línea STARTUP_ENABLED=Yes con este se puede proceder a que el Shorewall funcionara.
9. Otro parámetro opcional a tener en cuenta es CLAMPMSS, ya que si se cuenta con un enlace tipo PPP se debe cambiar el No por Yes, se utiliza en conexiones tipo PPP (PPTP o PPPoE) y sirve para limitar el MSS (acrónimo de Maximum Segment Size que significa Máximo Tamaño de Segmento).
10. Paso importante (**Zones**): con ella se definen las zonas que se administraran del firewall. La zona fw está definida en zones, por lo tanto ya no tendremos que ponerla ni borrarla, ahora procedemos a registrar las zonas de Internet (net) y Red Local (loc):

```
#####  
#ZONE          DISPLAY          OPTIONS
```

```

fw firewall      (firewall predefinida, esta se dejara)
net ipv4         (zona de internet WAN )
loc ipv4         (zona local LAN )
#LAST LINE — ADD YOUR ENTRIES BEFORE THIS ONE — DO NOT REMOVE
#####

```

11. Paso importante (**interfaces**): con la configuración en este fichero se establecen las interfaces de las zonas a ser tomadas en cuenta por el firewall. Se establecen las interfaces que corresponden a la de Internet y Red Local. En el caso de este diseño se recomienda que se tenga en cuenta la interfaz eth1 para acceder hacia Internet WAN, y una interfaz eth0 para acceder hacia la LAN y en todas se solicita que se calcule automáticamente la dirección de transmisión (Broadcast). Además, se identifican ciertas propiedades respecto a la interpretación de los paquetes que ingresan o salen por esa interfaz:

```

#####
#ZONE INTERFACE  BROADCAST  OPTIONS
net  eth1        detect      tcpflags,dhcp,routefilter,nosmurfs,logmartians
loc  eth0        detect      tcpflags,detectnets,nosmurfs
-    ppp+        -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
#####

```

12. Se tendrá en cuenta el siguiente parámetro para que en la interfaz de Internet (net) eth1 se adhiera a blacklist, con lo que se tendrá la opción de que si en algún momento se observa en los registros de logs del sistema que alguna IP está intentando ingresar sin permiso al servidor, Firewall se podrá bloquear por completo editando en el fichero /etc/shorewall/blacklist la IP correspondiente de dicho intruso.

13. Paso importante (**policy**): Este fichero establece las políticas por defecto para paquetes que viajan entre una zona hacia otra:

```

#####
#SOURCE DEST POLICY LOG LIMIT: BURST
# LEVEL
net all DROP info
all all REJECT info

```

#LAST LINE — ADD YOUR ENTRIES BEFORE THIS ONE — DO NOT REMOVE

#####

14. Con la configuración de la anterior se bloqueará todo el tráfico desde donde sea a donde sea. Esta naturaleza es recomendable, ya que estando el Firewall en marcha, se identificará cuales serán los segmentos IP destinos que se trabajaran en el IPCC y se definirán, teniendo las siguientes alternativas en la configuración:

- a. fw net ACCEPT: Si se desea permitir al propio firewall acceder hacia la zona de Internet.
- b. loc net ACCEPT: Si se desea dar una salida a los equipos de la LAN sin restricción de puertos hacia la WAN
- c. obteniendo el fichero del siguiente modo:
loc net ACCEPT
net all DROP info
all all REJECT info

15. Con la configuración del punto 14 no se especifica ningún puerto. Por lo consiguiente los equipos del IPCC navegaran y podrán salir a cualquier lado. Caso contrario que no se desee esta política, se podrá configurar como está con el fichero de rules que es especificado más adelante.

16. También es posible tener otras configuraciones como la siguiente, en el momento que lo requiera la operación del IPCC:

ACCEPT: Se acepta la conexión.

DROP: Se ignora la conexión.

REJECT: Se rechaza explícitamente la conexión.

QUEUE: Envía el pedido a una aplicación con la target QUEUE.

CONTINUE: Dejar que el pedido de conexión continúe para ser procesado por otras reglas.

NONE: Se asume que esta conexión no puede darse y no se generan reglas al respecto.

17. Paso importante (**NAT-masq**): Este fichero se utiliza para definir enmascaramiento o NAT. Es primordial, ya que el ISP entregará IP publicas fijas, y para la configuración de la LAN del IPCC debe existir un segmento para asignamiento de roles y reglas para ciertos dispositivos, además de los motivos de seguridad perimetral que se deben tener en cuenta, por lo que es útil con la red privada, donde se requiere navegar a través de un Proxy. Con el fichero de **masq** se definirá las VLAN que sería ADMON y AGENTS y SERVERS. En el siguiente sería el procedimiento para aplicar el enmascaramiento para la interfaz eth0 (Red LAN), la cual sale por medio de la interfaz eth1 que es nuestra IP Pública:

```
##### nat #####
#EXTERNAL   INTERFACE   INTERNAL   ALL       LOCAL
#
#           INTERFACES
IP-ASIGNADO POR ISP   eth1  192.168.1.1  yes  no
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

```
##### masq #####
#INTERFACE   SUBNET   ADDRESS   PROTO  PORT(S) IPSEC
eth1         192.168.0.0/24   IP PUBLICA ASIG POR ISP
eth1         192.168.1.0/24   IP PUBLICA ASIG POR ISP
eth1         192.168.2.0/24   IP PUBLICA ASIG POR ISP
#ppp+       192.168.0.0/24   IP PUBLICA ASIG POR ISP
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
#####
```

18. Paso importante (**rules**): Este es el fichero de configuración más importante de Shorewall, ya que aquí se definen las reglas que permitirán o denegarán el acceso a servicios y puertos desde y hacia zonas o el firewall. También se puede definir las reglas DNAT y registro de ciertos paquetes. Antes de configurarlo hay que tener en cuenta que las políticas por defecto son DROP, por lo tanto nada pasa a ningún lugar y no se podrá navegar ni siquiera el mismo Firewall. Por lo tanto el procedimiento a seguir es ir

abriendo y permitiendo el acceso a varios puertos según como sean los requerimientos en el momento de la implementación del IPCC.

En Shorewall no solo se puede configurar con las numeraciones de los puertos, este permite también configurar los puertos según sea su nombre o servicio que ofrece (DNS, FTP, POP3, MySQL, SSH, VNC, etc) y se propone la siguientes configuraciones:

DNS/ACCEPT loc fw

Con esta regla, se está permitiendo que la red local haga consultas de DNS al firewall, para la numeración de puerto a los DNS el cual corresponde la numeración 53, con esta regla se abrirá la parte de TCP como en UDP por que con esta bastaría para que se abra el puerto DNS.

Si se requiere permitir las consultas de DNS desde el Internet (net) hacia el Firewall (fw), lo tendríamos que hacer así:

DNS/ACCEPT net fw

19. Se aceptaran las conexiones por SSH(22) solamente desde una IP especifica en la parte local, ya que la gestión, monitoreo y control se hará por SSH por seguridad:

```
SSH/ACCEPT 192.168.1.x $FW
SSH/ACCEPT net $FW
SSH/ACCEPT vpn $FW
```

20. Se aceptara solicitudes de ping desde la LAN hacia el Firewall, para verificar estados de fallas.

```
# Allow Ping from the local network
#
Ping/ACCEPT loc $FW
Ping/ACCEPT loc loc
```



```
Ping/ACCEPT  vpn      loc
```

21. Luego se dará permisos a la red LAN (loc) para que se pueda conectar a la WAN Internet (net), se pueden definir los puertos que se requieran , en el caso del IPCC este contará con un dominio de cuentas de correo que será @usb.edu.co por lo tanto hay que dar el permiso a los servidores SMTP(servidor de salida p=25)y POP (servidor de entrada p=110) De la misma forma, también es recomendable para mayor seguridad a la VLAN de AGENTS denegar a que usuarios de operación puedan salir a puertos como el , 5800(VNC conexión por http), 5900(VNC conexión por normal), 1-1023, ya que son puertos de riesgos.

```
#####  
POP3/ACCEPT  loc      all  
SMTP/ACCEPT  loc      all  
# Reject Ping from the "bad" net zone. and prevent your log from being flooded..  
#  
Ping/ACCEPT  net      $FW  
ACCEPT      $FW      loc      icmp  
ACCEPT      $FW      net      icmp  
ACCEPT      $FW      vpn      icmp  
#REDIRECT   loc      8080     tcp      80  
#####  
ACCEPT      loc      net      tcp 20,21,22,43,53,80,85,1024:65535,8080  
ACCEPT      loc      net      udp 43,53,123,443,1024:65535  
ACCEPT      loc      $FW      udp 80,4550,5550,85,3650,85,8080  
ACCEPT      net      $FW      tcp 10000  
ACCEPT      net      $FW      tcp 80,4550,5550,85,3650,85,8080  
ACCEPT      net      loc      tcp 80,4550,5550,85,3650,85,8080  
ACCEPT      net      loc      tcp 4050  
#####
```

La anterior configuración de reglas ilustra con ACCEPT que se están aceptando desde la net, cuando es desde internet en la parte (loc) si es local LAN y si (\$fw) si esta es aceptado por el firewall. Luego en las líneas, se puede observar que tipo de protocolo se aceptará TCP o UDP en la parte de transporte.

Se debe tener en cuenta que en la línea red local (loc) se debe permitir hacer peticiones al Puerto 53 hacia el Internet. Es recomendable configurar un DNS cache para la LAN en donde se encuentran los servidores, pero también se debe

tener en cuenta que al mismo tiempo el ISP proporciona unos DNS que son de gran ayuda para navegar. Para estos DNS se deben tener en cuenta para el diseño del controlador de Dominio, de esta forma nuestro DNS local podrá resolver un dominio pasará a utilizar el DNS secundario, asignado por la LAN en la parte local.

Es importante tener en cuenta los siguientes puertos para la operación, y en el despliegue de operación se agregaran según los requeridos por el administrador de red, en el Anexo 17 se referencian los más necesarios.

22. Paso importante (**routestopped**): con este fichero se puede definir que direcciones IP o redes podrán continuar accediendo cuando el firewall este detenido o cuando este se encuentra en proceso de reinicio para que se genere una excepción sobre la configuración de las IP y las interfaces que se determinen. Se puede definir en formato separado por comas indicando la red o la IP de la siguiente forma:

```
#####  
#INTERFACE HOST(S) OPTIONS  
Eth0 IP que se requiera /mascara de red  
eth1 -  
#LAST LINE — ADD YOUR ENTRIES BEFORE THIS ONE — DO NOT REMOVE  
#####
```

Anexo 20 Diseño y configuración de controlador de dominio y AD

- ✓ Teniendo el dispositivo listo se realiza la instalación por medio del CD Win Server 2008 ST siguiendo las directrices referenciadas en la siguiente URL: [http://technet.microsoft.com/en-us/library/cc755116\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc755116(v=ws.10).aspx)
- ✓ Se selecciona el Idioma a instalar y se acepta los términos de licenciamiento ya que la figura es empresarial, para ello se debe cumplir con una documentación física y virtual de la compra de la licencia.
- ✓ Se realiza una configuración personalizada y se elige el medio de almacenamiento donde quedará el sistema operativo. Se procede a configurar las contraseñas de administrador como primer paso. Luego se realizará el proceso de complementos para administración del servidor, para ello se da clic en herramientas administrativas y se elige administrador del servidor como lo indica las imágenes a continuación:



Figura Gestión de Server 2008

Luego se agregan funciones al servidor, para ello se debe recordar que recomendable primero hacer un ambiente de prueba.

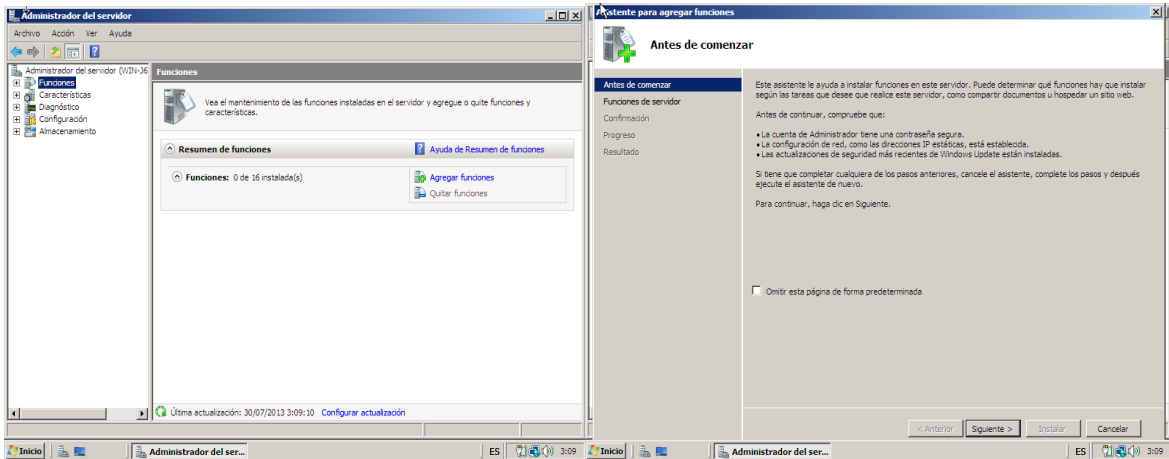


Figura Administración del Servidor

- ✓ Selección de función de servicios de dominio de Active Directory y luego se realiza la instalación.

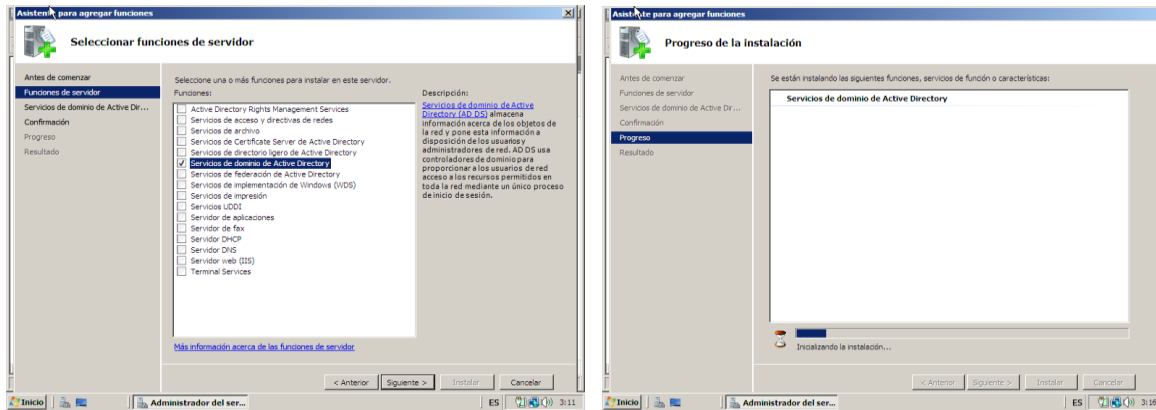


Figura Selección de Funciones del Servidor

- ✓ Para crear la funcionalidad de controlador de dominio se debe instalar el completamente dcpromo.exe como función y luego es recomendable cambiar de nombre al servidor en este caso se le nombra como IPCCUSB01.

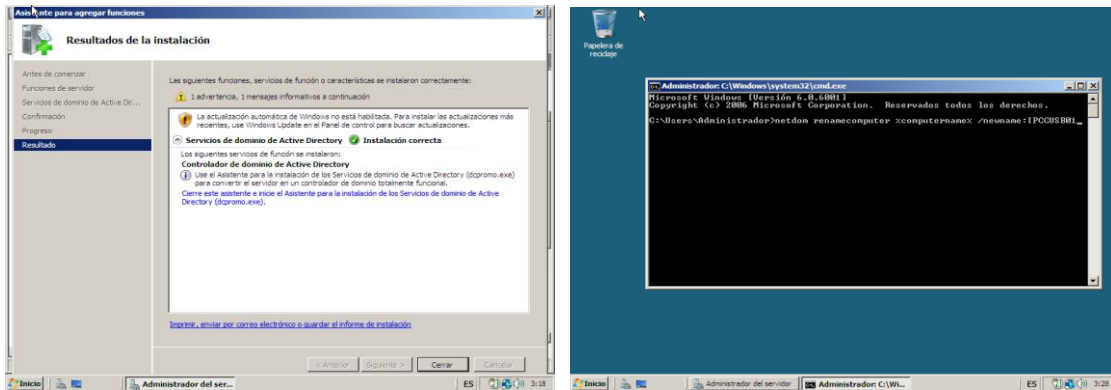


Figura Instalación del dcpromo.exe

- ✓ Se ejecuta la letra S para continuar, luego es recomendable reiniciar el servidor.
- ✓ Ahora instala la función dcpromo.exe para agregar la funcionalidad de controlador de dominio. A continuación se hará la instalación del asistente de los servicios de dominio y seguidamente se ilustra la compatibilidad del sistema operativo eligiendo el siguiente

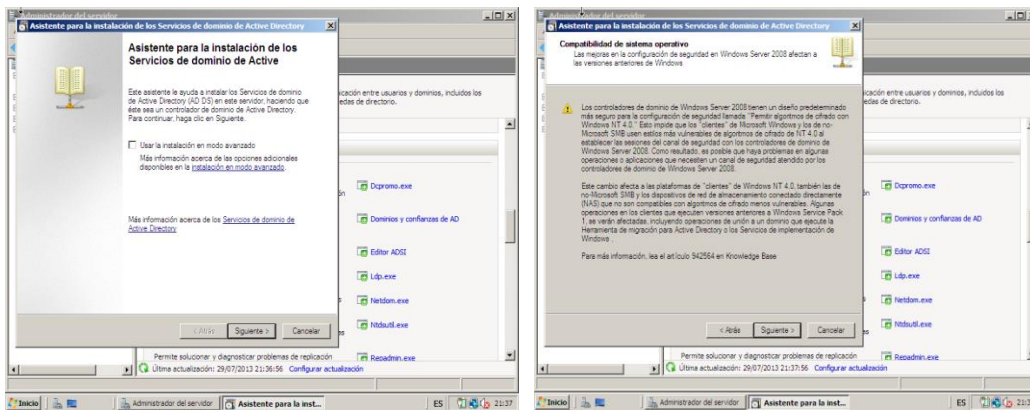


Figura Asistente de Instalación de servicios

- ✓ Ahora se asigna el nombre al dominio raíz. En este caso será IPCCUSB.BOG y luego se elige crear un dominio nuevo en un bosque nuevo:

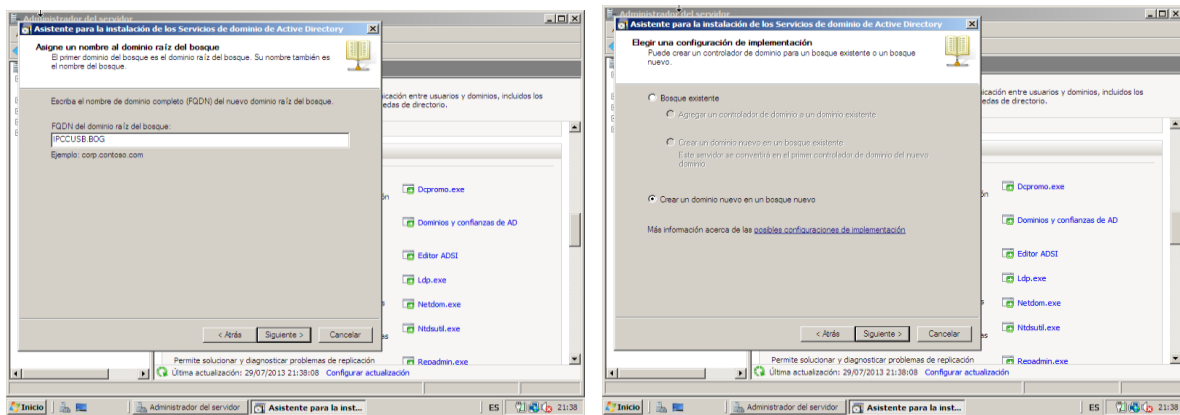


Figura Asignación del Bosque raíz

- ✓ Se establece ahora el nivel funcional. En este caso aplica para Win Server 2008 y se elige la ruta donde quedará la base de datos, el archivo de registro y la carpeta SYSVOL, los cuales son importantes para el funcionamiento de los servicios.

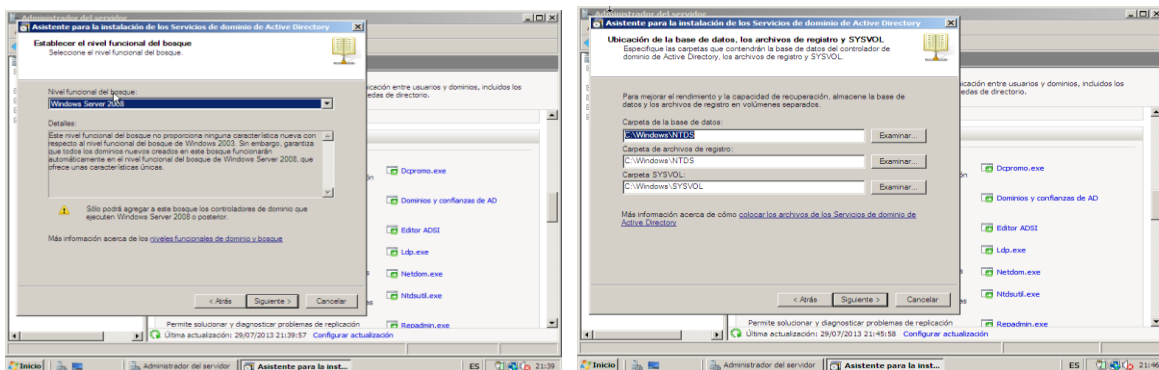


Figura Nivel Funcional del Bosque

- ✓ Por último, se crea una contraseña para restauración de servicios por parte de un administrador del servidor y luego un resumen de la configuración hecha en el proceso de configuración de los servicios de dominio.

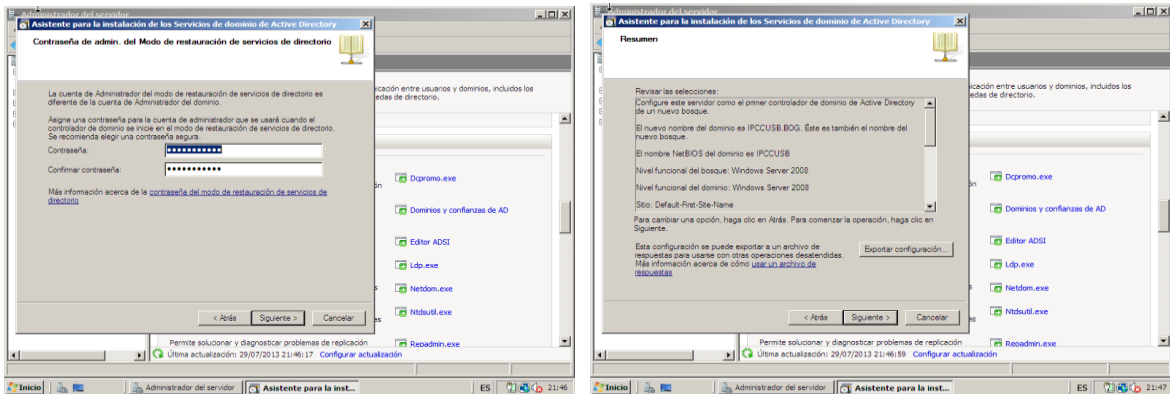


Figura Instalación de Servicios del Dominio

- ✓ Ahora el pazo a realizar es crear la unidad organizativa donde se aplicará todas las políticas que el administrador quiera ejercer sobre el árbol raíz, para ello se debe crear la unidad organizacional, los grupos y los usuarios que harán parte de los grupos.
- ✓ Se elige de nuevo herramientas administrativas, luego usuarios y los equipos de Active Directory. Se elige la carpeta raíz, da clic derecho sobre él y se elige nuevo seguido de Unidad organizativa.
- ✓ Luego se crean los objetos en este caso se crean carpetas que serán distinguidas en este caso por agentes que serán los tele operadores, los supervisores y el administrador del directorio activo, quien tendrá las credenciales válidas para administrar el servidor.

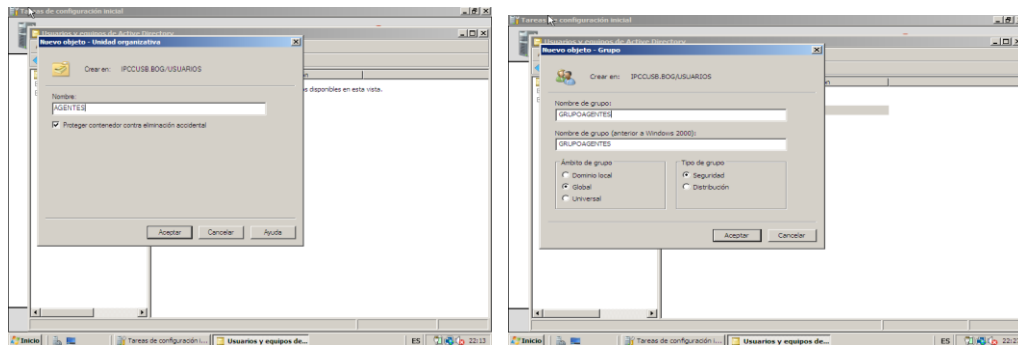


Figura Objetos del Dominio

- ✓ Ahora se elige la creación de grupos de la misma forma, pero ahora se hace click sobre nuevo y grupo, y se nombran los grupos. En este caso es

administrador, agentes inbound y agentes outbound, Por último, se hace las creación de usuarios dependiendo a que grupo pertenece, el siguiente es un ejemplo aplicado a agente inbound

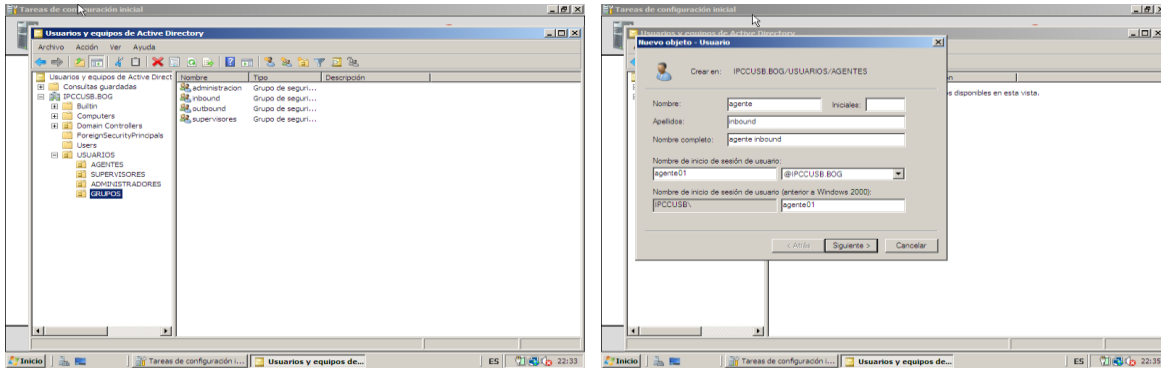


Figura Información del usuario

- ✓ El nombre del usuario se le llamará agente1 y luego se asignará una contraseña al objeto, esta será de conocimiento del administrador y del usuario final en este caso la tele operador, no tendrá por qué saberla otro que no sea el poseedor del usuario.

✓

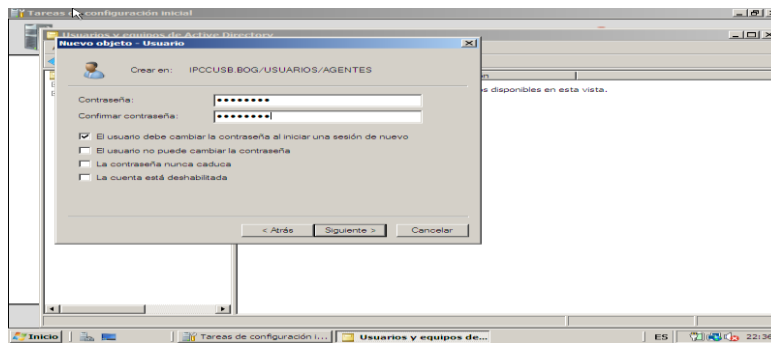


Figura Configuración Password

- ✓ Luego este es agregado al grupo a donde pertenece en este caso se asigna al agente 01 al grupo de agentes inbound como lo indica la imagen. Y Para el mismo caso aplica para los supervisores.

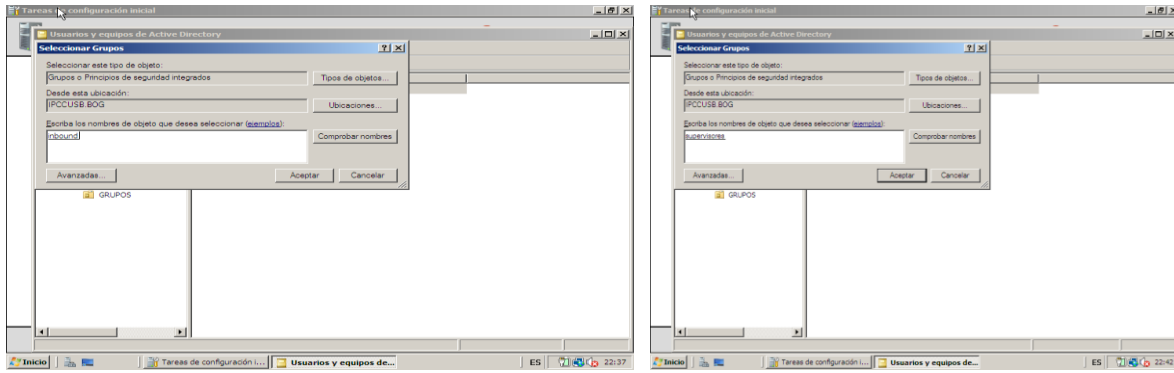


Figura Asignación a grupo

Anexo 21 Instalación Flash Operator Panel 2 (FOP2)

Lo primero que tenemos que hacer es habilitar el AMI en Asterisk, AMI vienen de Asterisk Manager Interface, el cual es el modulo que nos permite que Asterisk se comuniquen con nuestra aplicación FOP. Para habilitar, entramos al archivo manager.conf.

```
Cd / etc/asterisk/  
Vim manager.conf
```

Y lo configuramos de la siguiente manera:



```
root@dhcpc13/etc/asterisk  
[general]  
enabled=yes  
port=5038  
bindaddr = 127.0.0.1  
  
;este el usuario valido para conectarnos  
[usuariofop]  
secret= foppassword  
deny = 0.0.0.0/0.0.0.0  
permit=127.0.0.1/255.255.255.0  
read=system,call,command,agent,user,originate  
write=system,call,command,agent,user,originate
```

Figura Habilitar el AMI en Asterisk

Con la configuración realizada, creamos un usuario llamado usuariofop con una contraseña foppassword, el cual la aplicación FOP2 podrá conectarse a Asterisk mediante AMI y tendrá permisos de system,call,command,agent,user,originate.

Por último, se habilita el inicio automático del servidor WEB y se arranca con:

```
#chkconfig httpd on  
#service httpd start
```

Ejecutamos los siguientes comandos para descargarlo

```
# cd /usr/src/                                # cd fop2/  
# wgethttp://www.fop2.com/file.php?file=20    # make install  
# tar -zxvf fop2-2.26-centos5-i386.tgz
```

Luego ingresamos a buttons.cfg, para configurar cada uno de los botones que queremos que aparezcan en nuestra interfaz gráfica.

```
[SIP/101]  
type=extension  
extension=101  
context=users  
label=TESORERIA  
  
[SIP/104]  
type=extension  
extension=104  
context=users  
label=PRESTAMOS  
  
[SIP/103]  
type=extension  
extension=103  
context=users  
label=TECNOLOGIA  
  
[SIP/troncalALO]  
type=trunk  
label=TRONCAL ALO  
  
[QUEUE/informacionu]  
type=queue  
label=COLA PROGRAMA Y ADMISIONES  
context=features  
extension=1000
```

Figura Configuración de Buttons.cfg para los botones en FOP2

Ahora editaremos el archivo principal fop2.cfg y actualizaremos los siguientes parámetros:

```
Manager_host=localhost                        Manager=user=usuariofop  
Manager_port=5038                            Manager_secret=foppassword
```

Y se agregará las siguientes líneas donde se pondrán a los usuarios, clave y permisos permitidos.

Sin olvidar poner el archivo de botones, el cual fue configurado. En este caso se escribiría:

Buttonfile=buttons.cfg

```
user=112:1234:all
buttonfile=buttons.cfg
```

188,1 Final

Figura Permisos de los usuarios para FOP2

A continuación, para iniciar la aplicación se realizará de la siguiente forma

```
# service fop2 start
```

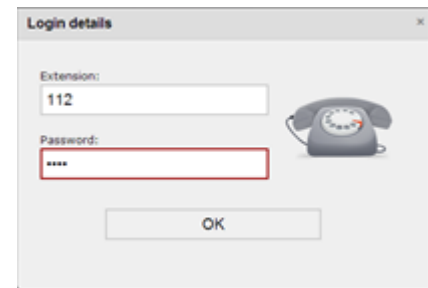
Una vez ejecutado el comando anterior puede abrir en un explorador de internet la URL <http://x.x.x.x/fop2> y autenticarse con alguno de los usuarios creados en el paso 3 (x.x.x.x es la dirección ip de su servidor Asterisk)

En este caso la dirección de nuestro servido es la 192.168.1.15

Figura Autenticación FOP2

Nos autenticamos con el administrado 112 y la clave anteriormente puesta que en este caso es la 1234

Nos mostrará un panel como el siguiente:



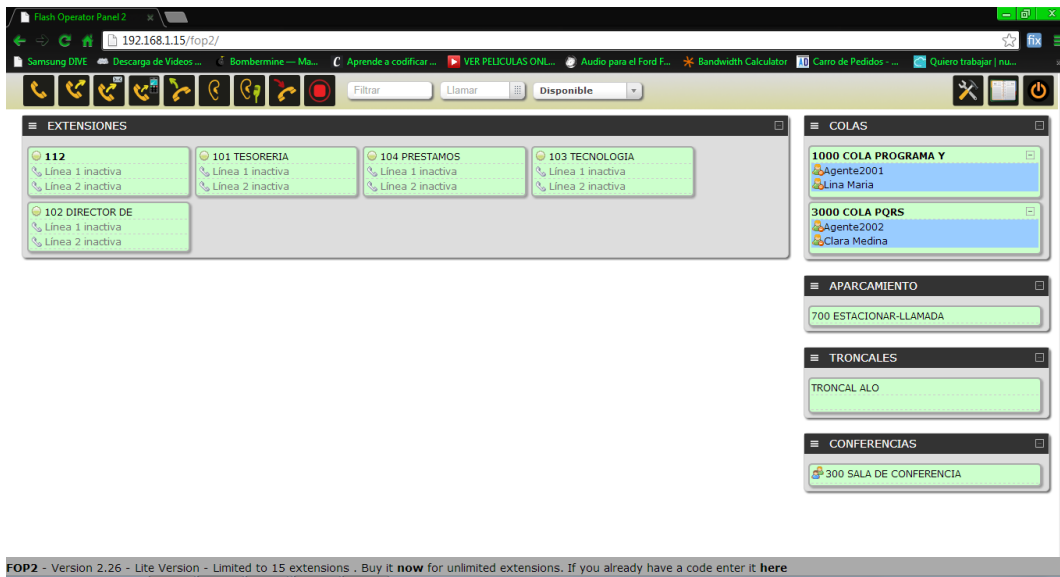


Figura Panel de administración de FOP2

En este panel encontramos todos botones creados, las cuentas de nuestros usuarios, las colas de nuestros agentes, la sala de conferencia y también adicionalmente se creó una troncal con un proveedor de minutos llamado ALOglobal.

En este panel el administrador podrá monitoria cada llamada, recogerla, transferirla y en algunos casos específicos hasta espiar la llamada con algunos usuarios con debidos permisos antes configurados.

Anexo 22 Instalación de la aplicación Asterisk-stat

La herramienta Asterisk-stat, va proporcionar diferentes reportes y gráficos, que van a permitir a un administrador de Asterisk analizar rápidamente y fácilmente el tráfico de llamadas que pasan por este.

Para todos los gráficos que genera el analizador vamos a instalar la librería GD

```
# yum install php-gd
```

Ahora instalamos el código fuente de la herramienta así:

```
# cd /var/www/html/  
# wget http://areski.net/asterisk-stat-v2/asterisk-stat-v2_0_1.tar.gz  
# tar -zxvf asterisk-stat-v2_0_1.tar.gz
```

Se configurará la herramienta de la siguiente manera:

```
# mv asterisk-stat-v2 asterisk-stat  
# cd asterisk-stat/  
# vim lib/defines.php
```

En este archivo vamos a establecer cuál es el equipo donde va a funcionar la herramienta y los datos de conexión a la base datos MySQL.

```

<?php

define ("WEBROOT", "http://localhost/asterisk-stat/");
define ("FSROOT", "/var/www/html/asterisk-stat/");

define ("LIBDIR", FSROOT."lib/");

define ("HOST", "localhost");
define ("PORT", "3306");
define ("USER", "cdruser");
define ("PASS", "cdrpassword");
define ("DBNAME", "asteriskcdrdb");
define ("DB_TYPE", "mysql"); // mysql or postgres

```

Figura Conexión con base de datos de MySQL

Ahora ya se probará la herramienta ingresando al explorador y digitando: www.192.168.1.15/asterisk-stat y veremos nuestra herramienta funcionando.

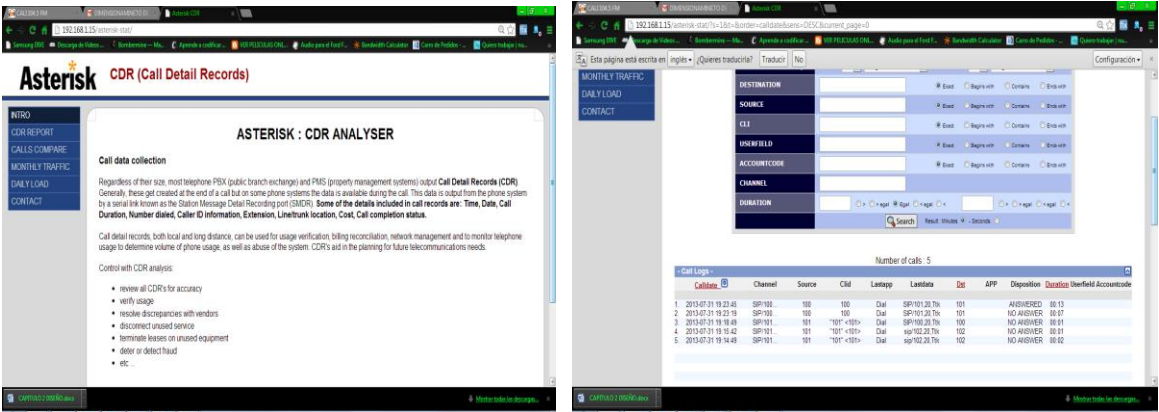


Figura Herramienta Asterisk-stat