ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UNA RED DE TELEFONÍA IP MEDIANTE ASTERISK, CON FUNCIÓN DE VOICEMAIL Y TRANSFERENCIA DE LLAMADAS Y DESARROLLO DE POLÍTICAS DE SEGURIDAD Y MANUAL DE USUARIO DEL SISTEMA PARA SACMIS CÍA. LTDA.

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

DANIEL ALEJANDRO MALDONADO RUIZ
daniel.a.maldonado@ieee.org

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

Quito, Junio 2012

DECLARACIÓN

Yo, Daniel Alejandro Maldonado Ruiz, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

_____

Daniel Alejandro Maldonado Ruiz

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Daniel Alejandro Maldonado Ruiz, bajo mi supervisión.

_____

Ing. Xavier Calderón, M.Sc.
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

- A mis padres, abuelos y demás familiares, por ser siempre un apoyo constante, y una muestra de amor incondicional y siempre perenne.
- A mis hermanas, Arianna Patricia y Andrea Paula, por estar siempre ahí cuando necesitaba un abrazo, un apoyo, una sonrisa, y por ser siempre, sin importar mi mal carácter, mis hermanas.
- A mis amigos, nombrar a unos y no a otros sería una injusticia; a todos ellos, por compartir tantos momentos a mi lado y ser una fuente de conocimiento diferente, y ser siempre una extensión de mi familia.
- A mis maestros, por su paciencia, y su tacto al enseñarme, principalmente todas las cosas que me han causado problemas a través de todos estos años; por no dejarme nunca en la oscuridad, y por siempre, siempre, enseñarme la diferencia entre conocimiento, y sabiduría.
- A cierto tipo de sujetos, conocidos comúnmente por cantantes y escritores; nombrarlos de otra manera convertiría este apartado en un tratado filosófico. A Serrat, Sabina, Delgadillo, Kundera, Benedetti y tantos otros, por ser siempre una inspiración, y una fuente de energía y un afán de ser mejor, de ser siempre el “Mejor de los Conductores Suicidas”.
- A mi guitarra y mi portátil, colchones de mi soledad, por, a pesar de tantísimas cosas, nunca haberme fallado.

DEDICATORIA

Este trabajo está dedicado a aquellas grandes personas que se adelantaron en El Camino, y que en lugar de dejar un vacío, me dejaron toda su enseñanza, su sabiduría y su fuerza de voluntad, para que yo nunca me deje vencer. Que La Fuerza sea con ellos…

Especialmente a mis Abuelos. Gracias, por todo.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación involucra el diseño de un sistema de Telefonía IP con su propio sistema de seguridad y contraseñas de uso para una empresa de Telecomunicaciones, que se complementa con las políticas necesarias para aleccionar a los usuarios de este sistema a proteger su propia privacidad y la de la empresa con el buen uso que se le dé al sistema en su totalidad, empoderándolos y convirtiéndolos en parte activa del sistema de telefonía.

El primer capítulo presenta un resumen de cómo la telefonía ha evolucionado a partir de los primeros diseños que se pusieron en funcionamiento a finales del siglo XIX, a través de todo un siglo de evolución, no solo tecnológica sino también de conceptos y de funcionamiento del sistema, hasta llegar a la fusión de las tecnologías primarias de comunicación: Telefonía e Internet, y todas las posibilidades que nos presenta esta unión.

El segundo capítulo muestra cómo era la infraestructura de red de SACMIS previo a la implementación del sistema de telefonía, y todos los cambios y adiciones que se debieron realizar para que la red física quede funcionalmente apropiada para soportar el sistema de Telefonía IP; no solo en capacidad del sistema, sino en el orden que debe tener un sistema de red físico para que este pueda ser perfectamente escalable y administrable.

El tercer capítulo se centra en el sistema Asterisk, núcleo que hace posible la implementación del servidor de Telefonía IP, y todas las configuraciones y añadiduras necesarias para que pueda el servidor funcionar como fue planteado para esta implementación en particular. Se describen los métodos de decisión para implementar hardware y software del sistema, y que estos cumplan con los parámetros de funcionamiento correspondiente; además del análisis de cómo se da solución a los problemas de comunicación que presentaba SACMIS antes de contar con el servidor de Telefonía, y las formas de proteger al mismo de intrusiones y ataques que puedan producirse.

El cuarto capítulo presenta un pequeño resumen de la evolución del conjunto de normas que conforman la serie 27000, de seguridad de redes informáticas, y el análisis de la norma 27001 para adaptarla de la mejor manera y crear un conjunto de políticas propias para SACMIS, que entrene y conciencie a cada uno de los usuarios de la importancia de la seguridad del sistema de telefonía que utilizan todos los días y que es, en su mayoría, su medio de comunicación con clientes, proveedores, y trabajadores.

El quinto capítulo presenta las conclusiones y las recomendaciones que surgieron de la realización de este proyecto, con un pequeño análisis de cómo se arribó a las mismas.

Finalmente se presentan las referencias bibliográficas de este trabajo, y los anexos complementarios a las explicaciones dadas en la teoría, para que esta pueda ser comprendida de mejor manera.

PRESENTACIÓN

Dentro del mundo de las comunicaciones, la telefonía siempre ha sido uno de los pilares fundamentales y muestra continua de la evolución de la tecnología en función de las necesidades de la humanidad. Sin embargo, con la creación de Internet, las comunicaciones sufrieron un punto de quiebre sin precedentes, a partir de la posibilidad de la transmisión de datos en tiempo real.

La telefonía no podía quedar fuera de este impresionante avance de la tecnología, y como tal, surgió la transmisión de voz sobre paquetes IP, la consabida VoIP, con la cual el desarrollo de servicios de comunicaciones de voz en Internet, complementando y mejorando los servicios existentes en la telefonía tradicional, surgiendo de esta manera una nueva forma de servicios de comunicación: La Telefonía IP, que ofrecía los mismos servicios de la telefonía existente, y otros propios de las comunicaciones por Internet, mientras abarataba costos de comunicaciones y facilidades de acceso a sitios remotos, es decir, una nueva revolución comunicacional.

La seguridad en redes surge como respuesta a la socialización de la Internet y al vertiginoso avance tecnológico. Nunca antes en la historia se volvió imperioso mantener nuestros datos seguros, ya que, las computadoras cada vez toman más el lugar de generadores y procesadores de datos, servidores de aplicaciones, y más que nada, gestionadores de comunicaciones universales. Más allá de la existencia de protocolos de seguridad, claves de encripción y demás algoritmos seguros que la tecnología pueda ofrecernos, la principal barrera que mantiene seguros a los complejos sistemas actuales recae en su mayoría en el componente humano de los mismos. Cada vez más se vuelve necesario generar lo que se ha dado en llamar la seguridad de “Capa 8”, entrenar y concienciar a las personas de su propia seguridad, para mantenerse a sí mismos y a sus sistemas, seguros.

Este Proyecto de titulación aborda ambos campos del estudio de las Redes desde el punto de vista de una aplicación muy puntual: Un Servidor PBX que maneje Telefonía IP con interacción hacia la telefonía tradicional; además del diseño de

políticas de seguridad para este sistema en específico. Las motivaciones de este trabajo van más allá de suplir la necesidad comunicacional de una empresa en crecimiento; se enfocan en que con cualquier sistema computacional, sirva este para comunicaciones en tiempo real o no, debe tener sus propias reglas de Seguridad, basadas en las normas de seguridad de redes Internacionales. Es imperioso que cada usuario tenga conciencia de que los sistemas computacionales no son ya ajenos al este, sino parte integral de su desarrollo y que la seguridad ya no solo compete a técnicos y desarrolladores, sino a todos quienes conforman el entorno de utilización.

Cada loco, con su tema.

Joan Manuel Serrat

Desde los albores de los tiempos, el hombre ha sentido la necesidad de comunicarse con sus similares. Datan de estos intentos las ya conocidas señales de humo, correos corredores, señales mediante antorchas o banderas, y tantas otras qué forman parte ya de la historia de las comunicaciones. Pero no fue hasta 1871 con Antonio Meucci y 1876 con Alexander Graham Bell que las comunicaciones alcanzaron cobertura global a través del teléfono, la más antigua y de las mejores redes WAN del mundo, por cobertura, acceso y posibilidades de migración de tecnología.

Hemos pasado de conexiones analógicas a cores digitales a través de más de un siglo de experimentación continua, y cada vez la telefonía mantuvo su estatus de red masiva global, sin importar el avance tecnológico y se mantuvo como la preponderante en las comunicaciones humanas. Con el desarrollo de Internet y de las redes globales de comunicaciones, se volvió imperioso que la telefonía tome su lugar dentro de las comunicaciones IP.

El presente capítulo realiza un análisis de la evolución de la telefonía IP desde sus inicios, es decir, desde la perspectiva de la telefonía analógica hasta que dio el salto hacia el mundo IP.

CAPÍTULO 1
ANÁLISIS DEL DESARROLLO DE LA TELEFONÍA, DESDE SUS INICIOS HASTA SU DESARROLLO IP, Y SUS DIFERENCIAS CON LA TECNOLOGÍA DE TRANSMISIÓN

1.1 TELEFONÍA ANALÓGICA

La mayoría de ideas grandiosas surgen por dos razones, por accidente o por necesidad. El teléfono es una de estas ideas revolucionarias.

La telegrafía, en su evolución, sentó las bases del desarrollo de la telefonía, al darle la capacidad de transmisión de larga distancia; y haciendo uso de los desarrollos del electromagnetismo y la acústica, el nuevo sistema tuvo el apoyo necesario para los descubrimientos que darían lugar a la invención del teléfono como se lo conoce.

Independientemente de quien lo creó y quien lo patentó primero, no cabe duda que los desarrollos que siguieron a los inventos de Meucci y Bell, sumado a la creación del conmutador automático por parte de Almon B. Strowger hicieron posible el nacimiento de conceptos como ‘llamada telefónica’ y ‘conmutador telefónico’, posibilitando el escalamiento y el crecimiento sostenido de un invento que estaba modificando el modo de vida del mundo.

Este sistema mantuvo una evolución constante durante todo el siglo XX, y sin embargo, los principios básicos de funcionamiento se han mantenido intactos, es decir; la PSTN (*Public Switch Telephone Network* o Red de Telefonía Pública Conmutada) tiene como misión conectar y establecer conexiones entre dos puntos para transmisión de señales de voz. Que este concepto se mantenga ha permitido agregar tecnología y servicios añadidos, mejorando así el sistema telefónico mundial.

Cuando se diseñaron los sistemas telefónicos, primero se debió determinar cuál era el rango de frecuencias que eran escuchadas por los humanos. Si bien los experimentos en acústica determinaron que el oído humano puede registrar el rango de 20 a 20000 [Hz], la mayor parte de sonidos que nos son audibles están entre los 250 y 3400 [Hz]. Esto representaba una reducción del Ancho de Banda necesario para la transmisión de voz a través de la red telefónica, que a pesar de que presentaba cierta pérdida de calidad, especialmente en frecuencias altas, mantenía la inteligibilidad de la comunicación.

La PSTN, para poder llegar hacia nuestras casas, hace uso de cuatro elementos fundamentales: el aparato de comunicación, o 'teléfono', la transmisión, la conmutación y la señalización.

1.1.1 SISTEMA TELEFÓNICO

Engloba mucho más que el simple lazo de finalización del circuito, ya que con el tiempo se han ido agregando varios servicios, como contestadoras automáticas, identificadores de llamadas, y añadidos propios del sistema, como conmutadores, bases telefónicas y un largo etcétera. El teléfono como tal se subdivide, a su vez, en cinco partes que hacen posible su funcionamiento: los sistemas de timbre, teclado de llamado, híbrido (o red), conmutador de colgado y el auricular. Cabe resaltar que los tres primeros pueden funcionar independientemente uno del otro.

- ***Sistema de timbre***

Cuando la oficina central (CO), necesita informar a uno de los terminales que existe una llamada entrante, envía a través del circuito una señal de corriente alterna (AC) de 90 [V]; lo que causa que el timbre que se encuentra integrado oscile produciendo el clásico 'ring' del teléfono. Con este voltaje, en la época actual, no solo se hace funcionar un timbre, que ya es electrónico, sino también luces u otro tipo de señales para alertar de una llamada entrante.

- ***Sistema de teclado de llamada***

Cuando se necesita alertar a la Central Telefónica que se quiere iniciar una llamada telefónica con el extremo lejano, es necesario indicar la dirección del aparato remoto. Al principio, el indicador que se utilizaba eran pulsos secuenciales que se enviaban a través del circuito telefónico y que activaban diferentes conmutadores, para permitir el direccionamiento de la llamada. Esto se hacía con los 'teléfonos de disco', que no eran más que una rueda dentada que enviaba en tiempos definidos el número de pulsos de señalización. Sin embargo, este tipo de señalización volvía lento el proceso de direccionamiento, por lo que se diseñó una nueva forma de direccionar, utilizando tonos que viajen a través del circuito telefónico, siguiendo un patrón, conocido como Doble-tono de multi-frecuencia (*Dual-Tone Multi Frecuency*, o DTMF). El funcionamiento de estos doble-tonos consiste en que cada dígito pertenece a una fila y una columna en una matriz de asignación de frecuencias; cuando se presiona un dígito, la frecuencia de las filas se adiciona a la de las columnas, y estas dos se envían a través del canal. La CO reconoce estos doble-tonos, e identifica el dígito presionado. La distribución de frecuencias se ejemplifica en la tabla 1.1.

	1209 [Hz]	1336 [Hz]	1477 [Hz]	1633 [Hz]
697 [Hz]	1	2	3	A
770 [Hz]	4	5	6	B
852 [Hz]	7	8	9	C
941 [Hz]	*	0	#	D

Tabla 0.1 Distribución de frecuencias de los dígitos del teclado de llamada [3]

Cabe resaltar que la cuarta columna de dígitos no está habilitada en los teléfonos de uso común, aunque el propio teléfono posea la circuitería necesaria para implementarla.

- ***Sistema híbrido***

Es el transformador que existe como parte de la circuitería del teléfono, y que administra las señales que se envían y se reciben a través del par de cobre

utilizado para la conexión. Una de sus funciones principales es la de regular los tonos, es decir, que el sonido que nos llega hasta el parlante tenga un volumen constante, tal como el que se envía a través del micrófono, haciendo la conversación más natural.

- ***El conmutador de colgado***

Es un subsistema del teléfono, que permite cerrar o abrir el circuito de comunicación y así poder establecer una llamada. Además de esta funcionalidad, el conmutador de colgado sirve para enviar señalización a través de la red, el ejemplo más notorio es cuando, en los teléfonos modernos se utiliza la función 'flash', que es una apertura del circuito de comunicación de entre 200 y 1200 milisegundos, y que se utiliza para informar a la red que se está haciendo uso de un servicio.

- ***El auricular***

Es, finalmente, el conjunto de parlantes y micrófonos que permiten realizar la llamada telefónica.

Desde el punto de vista funcional, el teléfono se podría representar como consta en la figura 1.1.

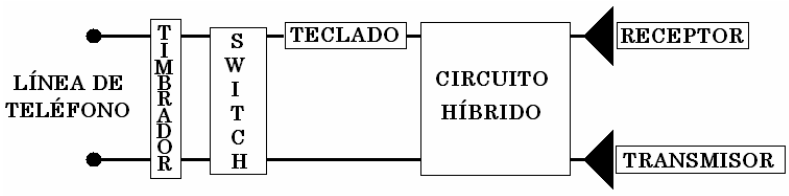


Figura 0.1 Diagrama interno de un aparato telefónico tradicional [29]

El funcionamiento del teléfono analógico está basado en los cambios de corriente que se producen en el aparato y que son detectados por la central, haciendo que el aparato pueda ser visto como un arreglo eléctrico; donde existen dos estados, uno abierto, donde la impedancia del sistema es de 40 [KΩ] y el voltaje de -48[V], lo que hace que a vista de la central, el enlace actúe como circuito abierto. El otro estado, cerrado, hace que el voltaje caiga entre -5[V] y -20[V], la impedancia a 1[KΩ], haciendo que la corriente existente en el circuito, que aumenta a 20 [mA]

pueda alimentar el micrófono y demás circuitería del teléfono. Estos dos estados se presentan en cada aparato telefónico, y las señalizaciones de ocupado se dan cuando la central detecta la impedancia del aparato remoto.

1.1.2 SISTEMA DE TRANSMISIÓN

La transmisión de las señales de voz se da a través de la conversión de las mismas en pulsos eléctricos que viajan por el par de cobre que conforma el enlace de abonado.

Cuando se habla a través del micrófono del teléfono, las vibraciones de la voz son receptadas a través de una zona de presión cubierta por una membrana dentro del micrófono, donde el carbono, que es comúnmente antracita[1] actúa como una resistencia. Esta resistencia, al ser modificada por las vibraciones de la membrana provoca una diferencia de corriente que puede ser transmitida por el enlace telefónico. En el extremo remoto, un proceso inverso hace que las vibraciones pasen a través de un electroimán, convirtiéndolas en vibraciones que el oído humano puede captar.

Sin embargo, las vibraciones producidas en el micrófono no son lo suficientemente fuertes como para viajar sin atenuarse, por lo que el híbrido cumple la función de amplificador:

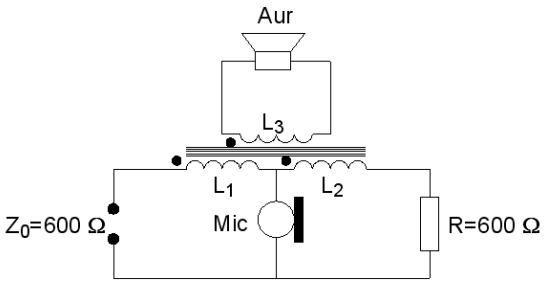


Figura 0.2 Circuito de conversación simplificado [1]

[1] Variedad de carbón mineral con una concentración de 95% de Carbono, y sonoro por percusión.

La impedancia de 600 [Ω] se utiliza para equilibrar el híbrido, que está conformado por las bobinas L1, L2 y L3. La voz que se recepta en el micrófono se distribuye en forma igualitaria entre L1 y L2, la corriente de L1 va hacia la CO, mientras que la de L2 se pierde en la impedancia. L3 recepta estas corrientes de L1 y L2, inducidas en sentido contrario. Esta última bobina hace que las corrientes no se eliminen completamente dejando un rezago de la voz recogida en el micrófono para que se reproduzca en el auricular, efecto conocido como 'sidetone' o efecto local, para que la persona que está hablando no sienta que la línea está muerta.

Además de la transmisión de las señales de voz, en los teléfonos se tienen que transmitir las señales de 'colgado/descolgado', ocupado, y demás señales de control, las mismas que viajan a través del canal telefónico a la par de los mensajes de voz. Este tipo de señalización se conoce como *'in-band'*, y es la que se utiliza en enlaces analógicos.

Al masificarse el uso del teléfono durante el siglo XX, transmitir la información entre troncales de manera 'in-band' se volvió altamente costoso, además de ineficaz. Esta necesidad obligó a multiplexar las señales de voz, utilizando un método conocido como FDM (*Frecuency Division Multiplexation* o Multiplexación por división de Frecuencia).

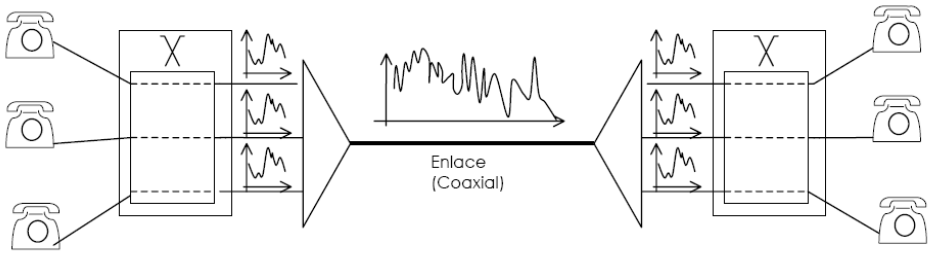


Figura 0.3 Esquema de transmisión con FDM [10]

FDM es una técnica de multiplexación que envía un grupo determinado de mensajes por un solo canal de banda ancha, utilizando para el caso diferentes modulaciones en frecuencia. Cada uno de los mensajes enviados han sido modulados con una sub-portadora de frecuencia diferente a la anterior, lo que

hace que cada mensaje viaje en la frecuencia con la cual fue sub-muestreada, separados una banda de frecuencia para evitar sobrelapamientos, conocida como bandas de guarda. Para que la señal pueda viajar a través del canal de esta forma, es necesario que la voz vaya modulada. Para esta modulación se utilizan portadoras analógicas de 4[KHz][2], con las cuales la señal de voz se puede transmitir sin problemas.

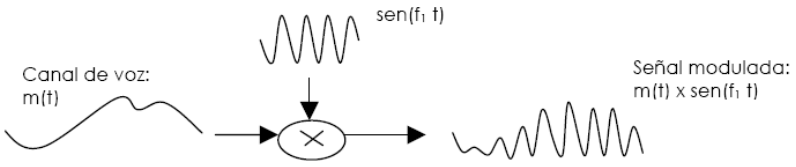


Figura 0.4 Esquema de Modulación [10]

Para que se pueda realizar esta multiplexación en el canal telefónico, una señal en banda base, de 4 [KHz], ocupa un canal de transmisión. 12 canales de 4 [KHz] se multiplexan en uno solo, para crear un grupo. Este grupo cubre las frecuencias de entre 60 y 108 [KHz]. Cinco grupos son multiplexados en lo que se denominó Supergrupo, de entre 312 y 552 [KHz]. El proceso continúa multiplexándose en Mastergrupos (10 Supergrupos) de entre 564 y 3084 [KHz]; y Jumbogrupos (6 Mastergrupos) de entre 564 y 17548 [KHz]; con lo cual se transmiten 3600 canales primarios.

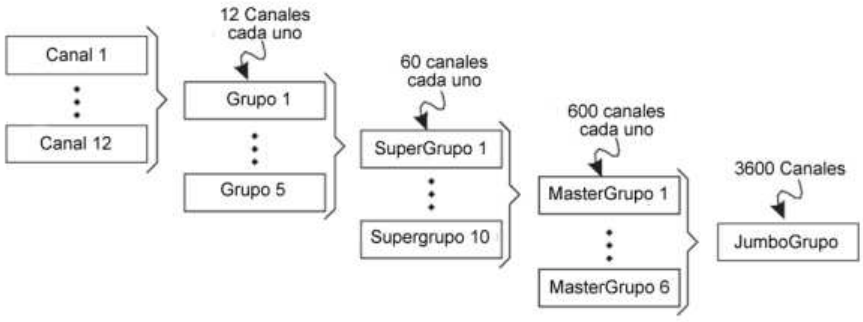


Figura 0.5 Esquema de multiplexación de canales de telefonía analógica [1]

[2] Ancho de Banda definido para transmisión de voz.

Este esquema, propuesto por AT&T, resultó ser el mejor y más eficaz para llevar la información telefónica de una troncal a otra, optimizando las líneas existentes y mejorando la comunicación.

1.1.3 SISTEMA DE CONMUTACIÓN

Se define la conmutación telefónica como la forma de direccionar una llamada hacia el destino remoto, y los pasos que debe seguir la señal para ser transmitida.

El concepto de conmutación telefónica surgió cuando en 1892 Almon B. Strowger, un empresario funerario de Kansas City, diseñó un conmutador automático de llamadas para evitar las 'equivocaciones' de la telefonista local, que era, casualmente, la esposa de su competidor. Este invento, dio pie para la realización de sistemas más complejos que cumplían la misma funcionalidad, enrutar las llamadas hacia su destino de manera automática.

Los siguientes conmutadores siguieron las bases dejadas por Strowger, que funcionalmente conmutaba 100 líneas en un sistema conocido como Paso-a-Paso (*Step-by-Step*); donde la idea funcionaba como un selector único, que no era más que un brazo que se movía de posición en un banco de contactos colocados circularmente, cada uno conectado a una línea de salida; de acuerdo a las señales que recibía desde la línea telefónica. Este circuito se repetía verticalmente hasta conseguir el número completo al que se había marcado.

El conmutador telefónico es el fruto de varios sistemas accionados en serie como:

- **Buscador de Línea:** Utilizado para buscar una línea activa, y conectarla a otra que esté disponible. Se utiliza mayoritariamente para limitar el número de usuarios que pueden utilizar simultáneamente el sistema.

- **Selectores Primarios y Secundarios:** Son los sistemas que realizan la invitación a marcar, y dependiendo del dígito que han recibido,

seleccionando el primer enlace para activar el siguiente selector en secuencia.

- **Selectores Finales:** Siguen los mismos parámetros de los anteriores selectores, y cumplen la función de expansores, para que todos los usuarios puedan acceder a las líneas que se están utilizando.

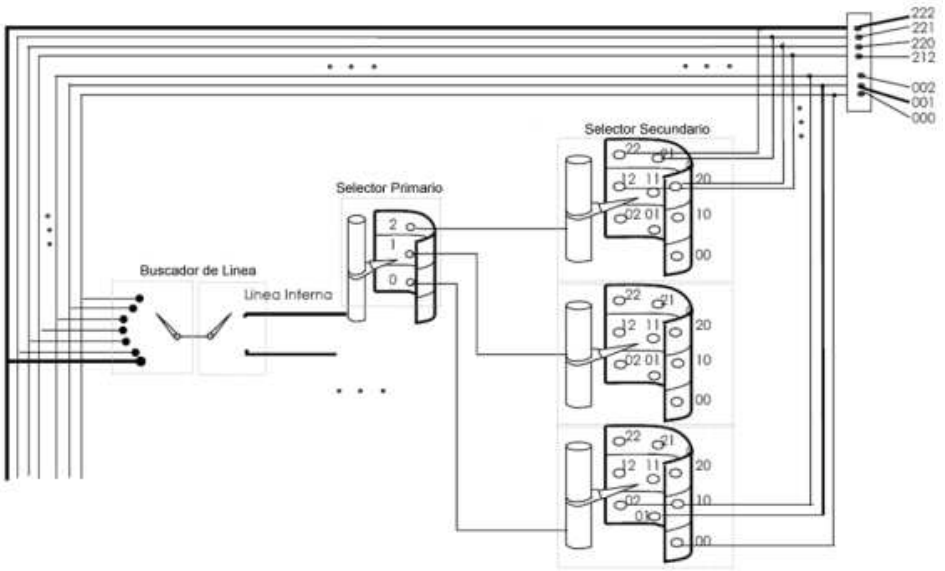


Figura 0.6 Esquema de conmutación Paso-a-Paso [10]

En 1930 aparecen los nuevos conmutadores automáticos conocidos como de matriz, que contenía contactos ubicados en filas y columnas, operadas por barras horizontales y verticales. Las matrices habitualmente contenían 200 cruces (10 filas y 20 columnas).

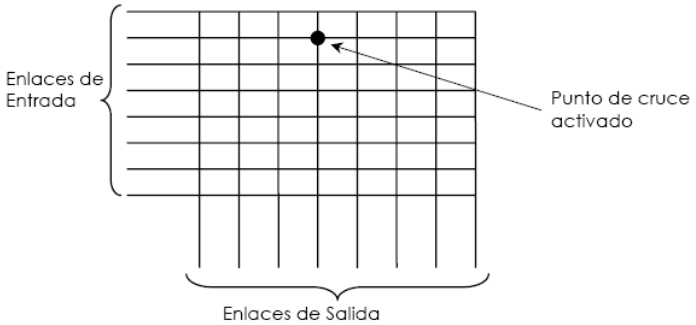


Figura 0.7 Esquema de la conmutación Matricial [10]

Cuando una línea se activa (teléfono descolgado) el sistema detecta esta señal y se dispone a recibir los dígitos en un marcador enlazado a un sistema de registro, que reserva una línea de comunicación. El sistema marcador hace uso de las matrices de conmutación en base a los dígitos marcados. Cuando la llamada se establece, los sistemas marcador y de registro se liberan en espera de una nueva conexión, mientras que el puente de transmisión supervisa la duración de la llamada establecida. Ese tipo de sistema es más simple que los conmutadores S-x-S, estableciendo un control centralizado del sistema de conmutación.

Este tipo de estructuras de conmutación requirió de la creación de oficinas intermedias para la transmisión de la señal telefónica. El tendido que existe entre el abonado y la primera central telefónica u Oficina Central o 'Central Office' (CO) se conoce como enlace de abonado o 'local loop'. A estas centrales las conecta un tipo de conexión diferente, que se conoce como troncal y que es la que transporta las líneas multiplexadas que se explicaron anteriormente. Estas CO son centros de conmutación, que pueden ser de cuatro tipos, los locales, que conectan a los abonados, los primarios, que conectan las centrales locales, los 'tándem' que interconectan los primarias, y los 'tándem' superiores, que interconectan a los anteriores.

Dentro de las ciudades, existen conexiones troncales de interconexión entre centrales locales, y de éstas con las centrales primarias. Cuando se necesita hacer una llamada de mayor distancia, como regional, se utilizan los 'tándems', todos de acuerdo a los dígitos marcados por el usuario.

1.1.4 SISTEMA DE SEÑALIZACIÓN

Se la define como la forma de controlar las señales que viajan a través del medio físico, para administrar las llamadas telefónicas y evitar errores.

En un principio, la señalización de una llamada telefónica requería demasiado del componente humano. Cuando alguien quería iniciar una llamada, al levantar el auricular, enviaba una señal a la central, la cual activaba un pequeño foco,

informando a la operadora del inicio de la comunicación. Este mismo tipo de señalización indicaba a la operadora si la línea destino estaba libre u ocupada, si estaba libre (con el foco apagado) procedía a enviar la señalización de timbre y establecer la comunicación; caso contrario, le decía al origen que la línea estaba ocupada y que espere un momento. La señalización era muy similar cuando se utilizaban troncales, en ese caso, la llamada se pasaba de operador en operador hasta llegar a la Oficina Central que contenga a la línea destino, siendo este último el que establecía la conexión final. La masificación del teléfono volvió a este tipo de señalización un duro trabajo humano, requiriendo cada vez de mayor personal que trabajara con mayor velocidad.

Con el desarrollo de la conmutación telefónica, se requirió otro tipo de señalización para establecer las llamadas. Esta primera señalización mecánica se la realizó en forma '*in-band'* o 'en-banda', es decir, a través del mismo canal de comunicación por donde viajaban los impulsos eléctricos que se convertían en voz. Esta nueva señalización tenía cuatro funciones generales: Alertar, transmitir información de dirección, supervisión y transmisión de voz.

Existen dos grandes señalizaciones distintas, estas son la señalización usuario-Oficina Central y la señalización inter-Oficinas Centrales.

La señalización en el lazo de usuario comienza cuando se levanta el auricular desde el aparato telefónico, causando que se cierre el circuito y se envíe una señal eléctrica hacia la CO, que lo interpreta como un pedido de servicio. La central, al receptar esta señal envía tonos audibles al usuario para indicarle que dispone de servicio para iniciar una llamada telefónica. Esta señalización está conformada por la transmisión simultánea de uno o dos tonos. Si existe este sonido, el usuario se dispone a enviar la señal de direccionamiento. Este número se envía a través pulsos representados como cortes en el circuito telefónico. Estos cortes, que ocurren en una taza de 10 pulsos por segundo son contados por la Central y a través de esta se re direccionaba la llamada. Con el avance de la tecnología estos cortes fueron sustituidos por los doble-tonos de la marcación DTMF. El flujo de corriente se mantiene mientras el auricular esté descolgado, es

decir mientras el teléfono este siendo ocupado; por lo que la señal de DC que se envía a través del lazo de usuario sirve de alerta y de supervisión.

Una vez que los cortes en el circuito telefónico o los doble-tonos han sido registrados, se procede a la habilitación del canal: si la línea está habilitada, se envían tonos de llamada, que para el llamante se oyen como tonos de timbrado, formados por la transmisión de dos tonos simultáneos; si la línea no está disponible se envía hacia el llamante un tono de ocupado, formado por la transmisión de dos tonos simultáneos de diferente frecuencia, distintos a los de los otros tonos. La duración de esta señalización, así como la duración de los mismos varía para cada país, y está definido por la UIT, basados en la recomendación de la UIT-T E.180 de marzo de 1998.

Cuando la línea no está ocupada, para alertar a la persona llamada, mientras al llamante se le envían sus tonos de timbrado, se envía una señal de voltaje de 75 [V_{rms}] con una frecuencia de 20 [Hz] que permite que la campanilla del aparato telefónico funcione. De la misma manera el tiempo de envío de la señal está definido para cada país por la UIT.

La señalización inter-oficinas funciona de manera diferente de la anterior señalización, la más antigua forma de hacerlo es detectando una señal DC entre cada oficina, normalmente detectando cambios de polaridad en la señal.

Los circuitos de larga distancia utilizaban alternadamente señalización AC y DC, mientras que la frecuencia comúnmente utilizada es de 2600 [Hz] para indicar la disponibilidad de las líneas telefónicas, donde esta señal solo se envía a través de troncales libres. Cuando se establece la comunicación, la troncal más cercana establece la comunicación recibiendo el canal de la troncal anterior, y usando su propia señalización, como si la llamada se hubiera producido localmente, para comunicarse con el abonado final. La información de direccionamiento utiliza distintas frecuencias para realizar su cometido, estas son: 700, 900, 1100, 1300, 1500 y 1700 [Hz], combinando dos de estas en cada tipo de señalización. A esta

señalización se la llama MFKP (Multiple-frecuency Key Pulsing o Clave de pulsos de multi-frecuencia)

Todo este tipo de señalización se realizaba, como ya se describió, 'in-band', sin embargo, esta transmisión tenía sus propios problemas, como el hecho de que ciertas compañías telefónicas de forma fraudulenta modificaban las señales para evitar recargas de transmisión, o que cierto tipo de señales durante la conversación podían producir desconexiones accidentales.

1.2 TELEFONÍA DIGITAL

'Analog telephony is almost dead'[3]

La frase anterior resume el camino que está recorriendo la red telefónica, en un mundo tendiente a utilizar recursos digitales en casi cualquier aspecto. La telefonía analógica, si bien poseía de alguna manera alta fidelidad de transmisión, venía embebida con una cantidad de problemas en la misma que impedían que el sistema pudiera tener una calidad de transmisión útil para comunicaciones a larga distancia o en determinados canales sensibles al ruido.

Al ser la voz una onda sinusoidal, si esta señal sufría una distorsión que hacía que su amplitud disminuyera, al aumentar la amplitud en un repetidor, también aumentaba la distorsión, lo que hacía que la voz se escuche con estática, entrecortada, o en el peor de los casos, absolutamente ininteligible.

Cada avance que se producía para corregir estos errores, significaba un nuevo avance en la ciencia y en el modo de concebir la telefonía como tal. Si bien las partes de la telefonía no variaron en su nombre y función, si varió su forma de trabajo, pasando de conmutadores electro-mecánicos a electrónicos, de señalización 'in-band' a ISDN y SS7, de ondas analógicas, a PCM.

[3] "La telefonía analógica casi ha desaparecido". Asterisk, The Future of Telephony, Second Edition. 2007

1.2.1 SISTEMA DE TELÉFONO

La evolución del aparato telefónico se detuvo una vez que los circuitos electrónicos remplazaron a los relés y el DTMF remplazó al direccionamiento mediante pulsos; cada teléfono en el mercado sigue los mismos patrones de funcionamiento, simplemente añadiendo funcionalidades propias del uso que va a tener dicha terminal.

1.2.2 SISTEMA DE TRANSMISIÓN

A pesar que el lazo de abonado o *'local loop'* mantiene la conexión analógica, a partir del sistema de transmisión la voz ya se envía digitalmente. La idea principal de la digitalización es facilitar la reconstrucción de la señal de voz una vez esta haya atravesado el canal de comunicación y llegue al destino.

La digitalización implica una pérdida de fidelidad de la voz, ya que no todas las componentes de frecuencia se muestrean, pero esta pérdida no implica una pérdida de calidad, ya que los componentes principales se digitalizan, haciendo que el usuario final no detecte la diferencia entre la señal analógica y la digital. Además, al digitalizar la voz de da la posibilidad matemática de chequeo y corrección de errores en la señal muestreada, haciendo posible que la señal emitida sea prácticamente igual a la recibida, sin importar la distancia o la cantidad de interferencia que tenga el canal.

Para la digitalización de voz en calidad telefónica se utiliza la técnica conocida como PCM (*Pulse Code Moduation* o Modulación de Pulsos Codificados), que ha demostrado ser la mejor para mantener la calidad de la transmisión de la voz.

La señal de voz transmitida es continua en amplitud y tiempo, y con la digitalización se debe convertirla en una señal discreta, es decir, discontinua en tiempo y amplitud, permitiéndole tomar sólo ciertos valores que pueden ser codificados, mientras más muestras se puedan tomar de una señal analógica,

ésta será más fiel a la original, pero así mismo será mucho más pesada en términos de ancho de banda y por tanto, más difícil de transmitir.

La toma de valores para la señal analógica se la realiza en función de una base regular, según la cual las muestras serán tomadas de la misma manera, o en los mismos intervalos de tiempo. Para ilustrar el proceso se hará un ejemplo, tomando 5 bits para la codificación[4], especificando los efectos que tiene en transmisión y calidad.

Una señal sinusoidal, para su muestreo, se la puede representar tal como muestra la figura 1.8.

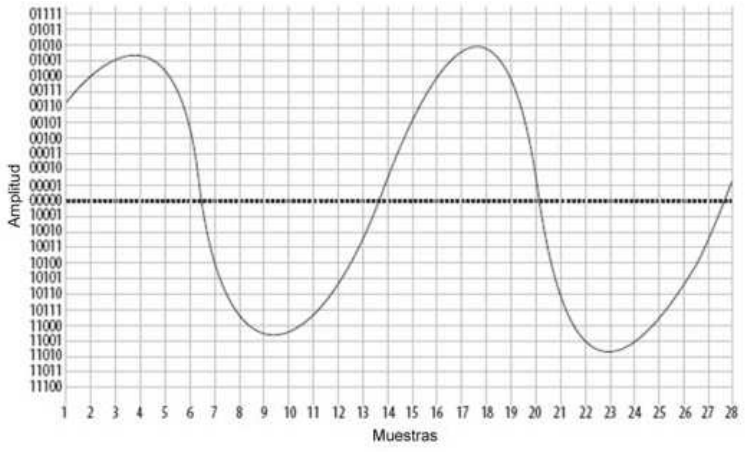


Figura 0.8 Muestreo de la señal utilizando 5 bits [3]

Donde la señal analógica cruza con uno de los valores determinados por 5 bits, o muy cercano a este, se toma una muestra de la señal, dándole un valor único que puede ser transmitible

[4] Para el muestreo de la señal telefónica con PCM se utilizan 8 bits

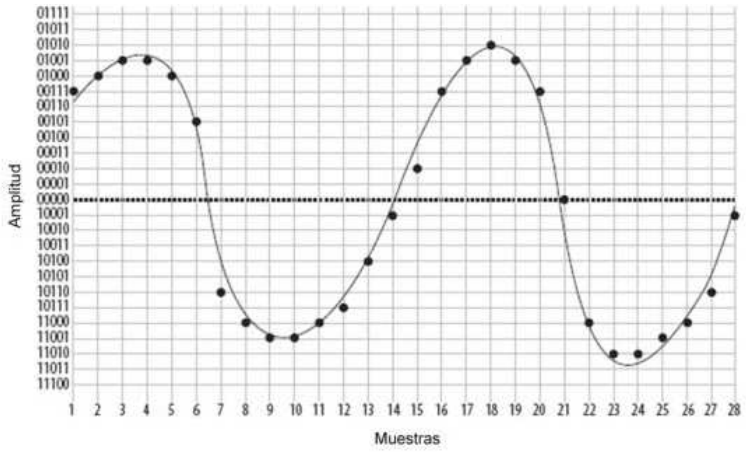


Figura 0.9 Muestras tomadas de la señal original [3]

Una vez que los valores han sido definidos, en el extremo final, se puede reconstruir la señal lo más cercana al original.

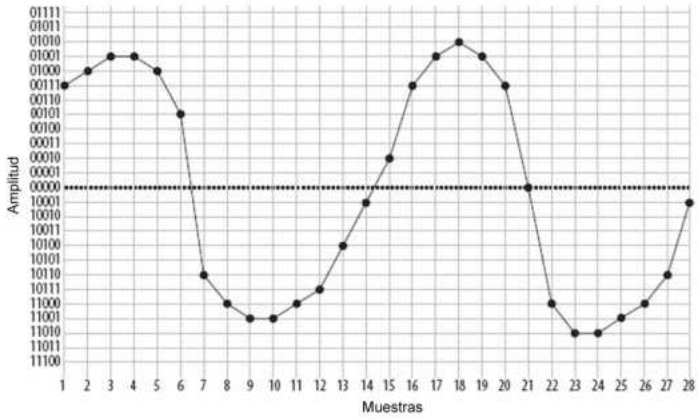


Figura 0.10 Señal reconstruida en el extremo lejano [3]

Sin embargo, es necesario determinar el límite de muestras que se deben tomar de una señal analógica para que su transmisión pueda efectuarse; esta interrogante fue resuelta por Henry Nyquist, ingeniero eléctrico de AT&T/Bell Company, que estableció el teorema que ahora lleva su nombre: *'Cuando una señal es muestreada, la frecuencia de muestreo debe ser de al menos el doble del ancho de banda de la señal original, para que la misma pueda ser reconstruida perfectamente a partir de la original'*

$$f_s \geq 2\, f_m$$

Ecuación 1.1 Definición del Teorema de Nyquist.

Dónde:
f_s es la frecuencia de muestreo, y
f_m es la máxima frecuencia de la señal de voz, o en su defecto, el ancho de banda de la misma.

Como se explicó en las primeras páginas, a pesar de registrar frecuencias de hasta 20000 [Hz], la mayoría de las frecuencias que escucha el oído están en un rango de hasta 3400 [Hz], por lo que se estandarizó que el Ancho de Banda de las señales de calidad telefónica sea de 4000 [Hz]; esto hace que la frecuencia de muestreo adecuada para la voz sea de 8000 [Hz], es decir, de 8000 muestras por segundo.

Esta limitación implica que no se pueden obtener datos precisos con una codificación lineal, por lo que se diseñó la técnica conocida como 'companding'; que mejora el rango de muestreo, para no perder información de precisión de la señal. Trabaja cuantificando las amplitudes mayores con niveles de cuantización mas espaciados, determinados por una función logarítmica, para abarcar mayor cantidad de datos de la señal, manteniendo el valor máximo de frecuencia de muestreo.

Según la UIT-T, en su recomendación G.711 se especifican dos sistemas de 'companding' logarítmica, que operan con el mismo principio de funcionamiento, pero con características diferentes:

- ***Ley A (alaw)***

Usada en Europa, Sudamérica y África. Especifica un cuantizador de 13 segmentos. Para ciertos valores bajo un umbral utiliza una función lineal y sobre esta una función logarítmica, con palabras de 8 bits.

- ***Ley μ (μlaw o ulaw)***

Usada en Estados Unidos, Canadá y Japón. Especifica un cuantizador de 15 segmentos representados por una función logarítmica para toda la señal. De igual manera maneja palabras de 8 bits.

Cada una de estas especificaciones, cabe recalcar, no son compatibles una con la otra.

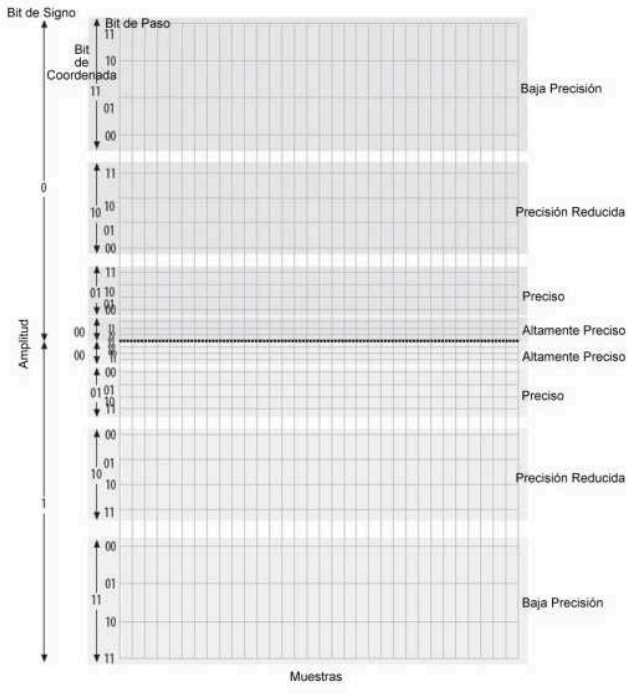


Figura 0.11 Companding con palabras de 5 bits [3]

Como se puede observar en la figura 1.11, mientras más cerca se esté al eje de referencia, las divisiones de cuantización están más cercanas una de la otra, y conforme se va alejando de la misma, las divisiones se van extendiendo, permitiendo abarcar mayores valores de señal.

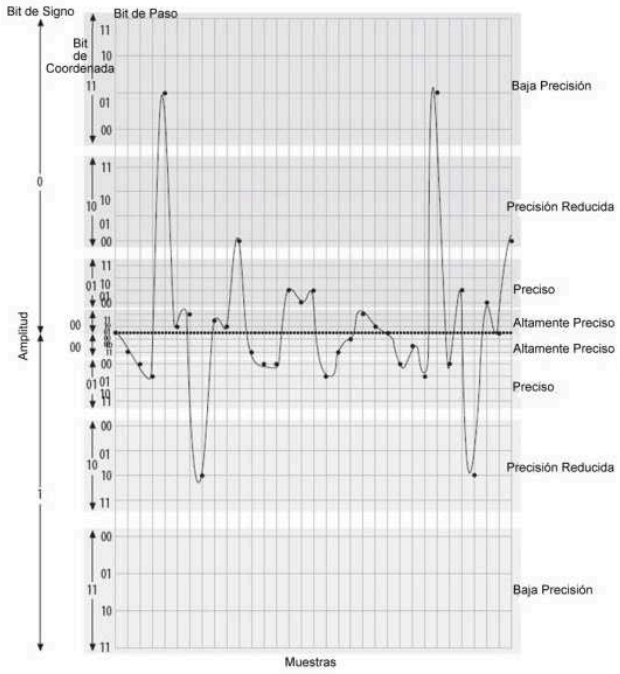


Figura 0.12 Señal muestreada con *companding* de 5 bits [3]

De acuerdo a la UIT-T G.711, ambos métodos utilizan palabras de 8 bits, lo que significa que existen 256 intervalos de cuantización; por lo que la tasa de bit de transmisión vendría a ser:

$$V_t = f_s \cdot n$$

Ecuación 1.2 Calculo de tasa de bit.

Dónde:

fs = frecuencia de muestreo = 8[KHz.]

n = tasa de bit por muestra = 8 $\frac{bits}{muestra}$

Lo que da un resultado de: $8\frac{kbits}{muestra} \cdot 8\frac{muestras}{segundo} = 64\ [kbps]$

Velocidad que se considera de un canal telefónico. [27]

Este tipo de transmisión hizo posible que la multiplexación de señales se pueda hacer digitalmente también. Esta multiplexación se la conoce como de Tiempo o TDM (*Time Division Multiplexing*)

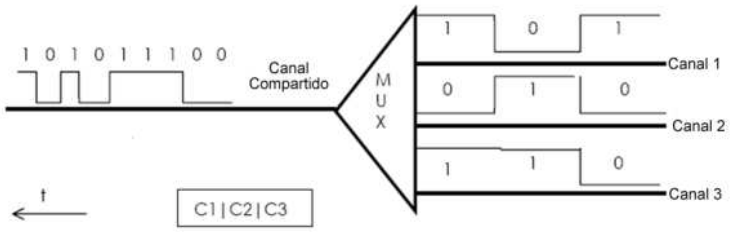


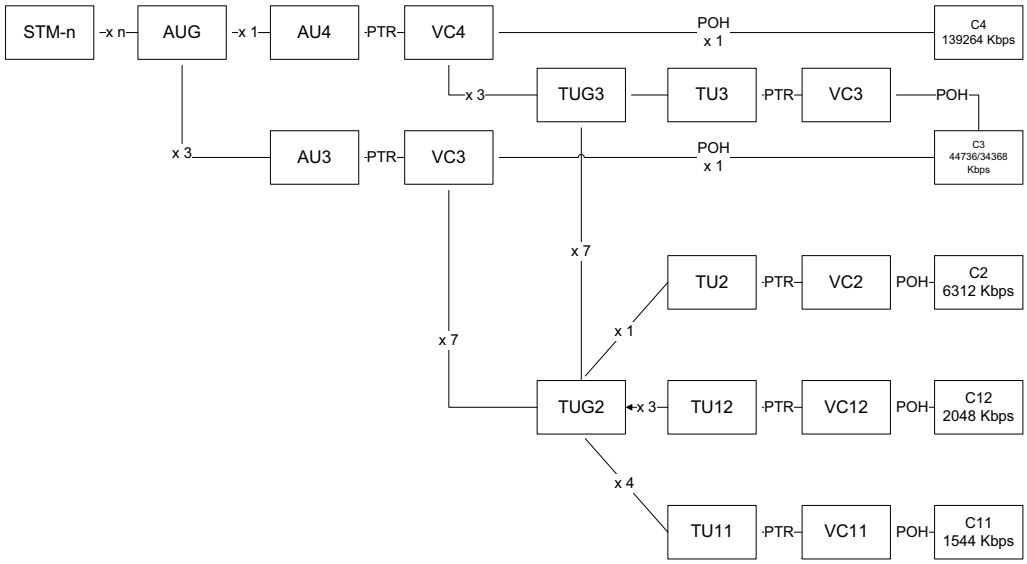
Figura 0.13 Esquema de transmisión con TDM [1]

TDM aparece en 1963 y transmite varias señales PCM simultáneamente, dividiendo el tiempo de transmisión en ranuras, en donde se colocan las muestras de cada canal de comunicación siguiendo un orden específico que pueda ser interpretado por el extremo lejano. Esta estructura de orden específico que se repite en el tiempo se conoce como trama. Al estar los datos de los canales distribuidos, debe existir un ‘‘buffer’’ en el transmisor, que permita la separación de los datos que deben ocupar los *slots* de tiempo, y asimismo, debe existir un *buffer* en el receptor que reorganice los datos recibidos de los canales de comunicación, para formar los mensajes originales.

Esta técnica de multiplexación permitió el avance de sistemas de comunicación cada vez más grandes, permitiendo la transmisión de mayor información en tramas compactas, dando lugar a las Jerarquías Digitales Plesiócronas o PDH y a partir de las anteriores, las Jerarquías Digitales Sincrónicas ó SDH.

Estándar Norteamericano			**Estándar Internacional (UIT-T)**		
Denominación	**Canales de voz**	**Tasa de datos (Mbps)**	**Denominación**	**Canales de voz**	**Tasa de Datos (Mbps)**
DS-1	24	1.544	E1	30	2.048
DS-1C	48	3.152	E2	120	8.440
DS-2	96	6.312	E3	480	34.368
DS-3	672	44.736	E4	1920	139.264
DS-4	4032	274.176	E5	7680	565.148

Tabla 0.2 Tabla de distribución de información de jerarquías PDH [27]



Dónde:

C	Contenedor
VC	Contenedor Virtual
TU	Unidad Tributaria
TUG	Grupo de Unidades Tributarias
AU	Unidad Administrativa
AUG	Grupo de Unidades Administrativas
STM	Módulo de transporte sincrónico
POH	Sobrecarga de trayecto (supervisión)
PTR	Puntero de tributario

Figura 0.14 Esquema de formación de un STM-n [27]

1.2.3 SISTEMA DE CONMUTACIÓN

Con la digitalización, la conmutación telefónica ha hecho uso de distintos sistemas de programación para realizar el direccionamiento, éste sistema, se ha basado, a partir de entonces, en un sistema de conmutación por división de tiempo.

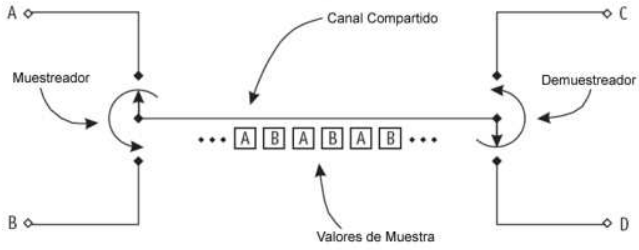


Figura 0.15 Esquema de conmutación por división de tiempo [1]

La conmutación digital enruta conversaciones separadas a través del mismo canal de comunicación, a cada una de estas comunicaciones se le ha asignado una ranura de tiempo. Cada una de estas señales, previamente muestreadas viaja empaquetada en tramas específicas que se separan en el destino y son re-enrutadas con la ayuda de 'buffers' de memoria. Esa es la razón, además de que está optimizada para señales digitales, por la que a la conmutación por división de tiempo se la conoce como conmutación digital.

La conmutación se realiza a través de intercambio de señales digitales entre las ranuras de tiempo, utilizando una técnica llamada *'time-division switching'* o Conmutación por división de tiempo, la cual, a través de intercambio de ranuras de tiempo, le permite al conmutador identificar el destino de cada uno de los canales, enrutando la información hacia su correcto destino.

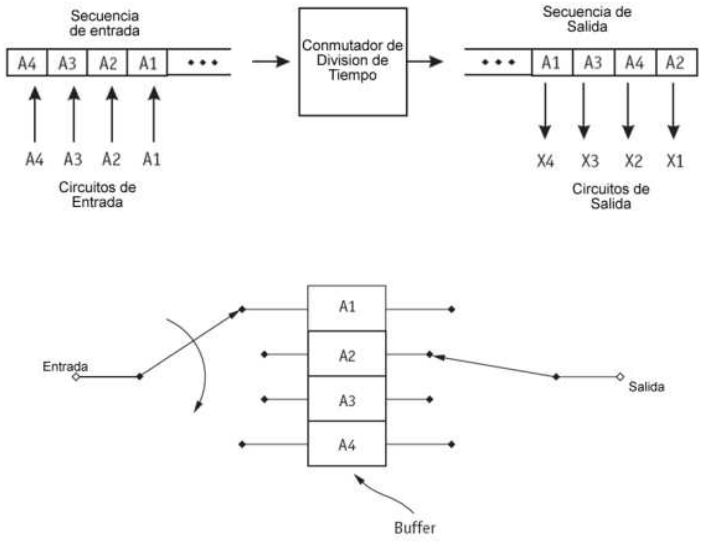


Figura 0.16 Conmutación en tiempo de varios canales [1]

En la entrada de datos, los *buffers* de memoria se van almacenando en orden, según cómo van llegando las tramas, sin embargo, de acuerdo al intercambio de señales, la trama de salida será diferente, según los destinos de cada uno de los canales. En la figura 1.16 se observa gráficamente como se hace este tipo de conmutación. Según el ejemplo, la trama de entrada sería A1, A2, A3, A4; existiendo 4 canales de salida, X1, X2, X3, X4. Según los datos de la conmutación, la trama de salida es A2, A4, A3, A1.

A partir de esta tecnología se desarrolló el concepto de tiempo de lectura/escritura de conmutación, que determina el máximo número de ranuras de tiempo que pueden ser leídas por el conmutador en un determinado tiempo. La información que se almacena en los 'buffers' de memoria espera a ser leída en su totalidad antes de realizar cualquier acción, lo cual contribuye al retardo de conmutación, siendo el máximo retardo el de todas las ranuras, a saber, 1/8000 [s], o 125 [μs].

Dentro de la conmutación digital se tienen varios circuitos distintos, los cuales no pueden estar conectados todos por un sistema digital, ya que muchos de ellos, como troncales y sistemas de larga distancia, están separados espacialmente, por lo que se necesitan sistemas físicos para conectar todos estos multiplexores digitales, por lo que se han desarrollado sistemas que puedan suplir estas dificultades de manera óptima: Sistemas conocidos como TST (Tiempo-Espacio-Tiempo o Time-Space-Time)

Este sistema funciona como combinación de conmutación analógica y digital, estando los conmutadores digitales a los extremos de la comunicación, y en medio de estos, una matriz de comunicaciones, que varía sus rutas en función de la información suministrada en el intercambio de datos.

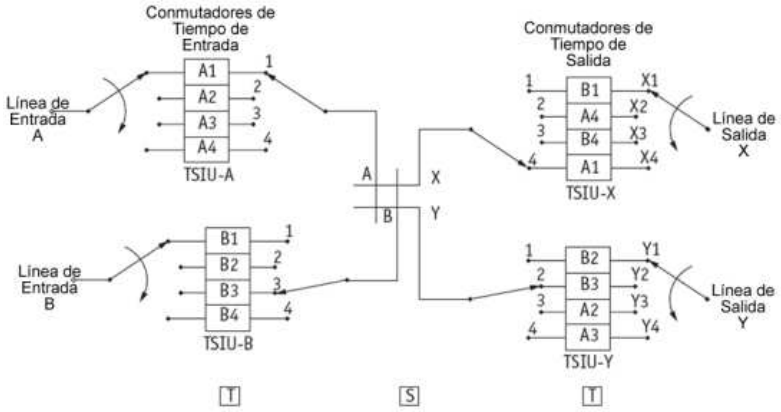


Figura 0.17 Conmutación T-S-T [1]

Las líneas conectadas en A y B se interconectan con X y Y a través de una matriz donde los cuatro transmisores están embebidos, pudiendo realizarse una conexión de cuatro caminos. Según la identificación que reciban los paquetes pueden ir paquetes de A hacia X y Y, lo mismo que B.

El retardo sigue siendo un problema dentro de este esquema, si se considera que se reciben 32000 ranuras de tiempo por segundo, por lo que el retardo total del sistema sería 1/32000 [s] o 31,25 [μs].

A partir de este sistema, se nota que, al aumentar el tamaño de los *buffers* se reduce el retardo de lectura de la información que existe en ellos, por lo que cada vez los sistemas, al aumentar el tamaño del *buffer*, reducen el tiempo de retardo del sistema, y, globalmente, reducen los costos de los sistemas de conmutación digital.

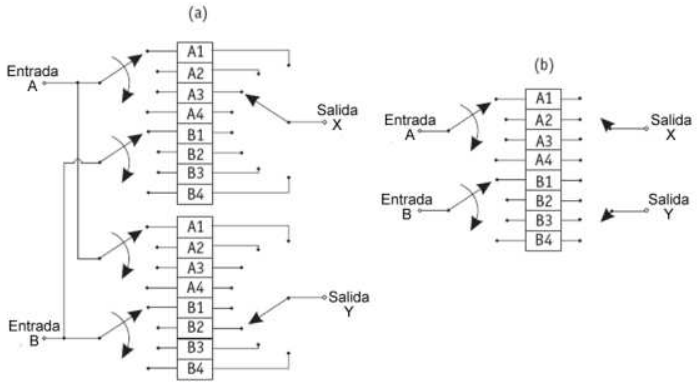


Figura 0.18 (a) Utilización de un 'buffer' de gran tamaño con dos entradas y una salida. (b) Utilización de un 'buffer' de gran tamaño de multi-entrada y multi-salida [1]

1.2.4 SISTEMA DE SEÑALIZACIÓN

La evolución de los sistemas telefónicos exigió que la señalización deje de ser enviada 'in-band', ya que cada señal adicional podía corromper la voz, que ahora viajaba digitalizada, por lo que se optó por enviarla por un canal externo al canal de voz. Esta técnica de señalización apareció en 1976 y se la conoce como CCIS o Señalización de canal común inter-oficinas (*Common Channel Interoffice Signalling*)

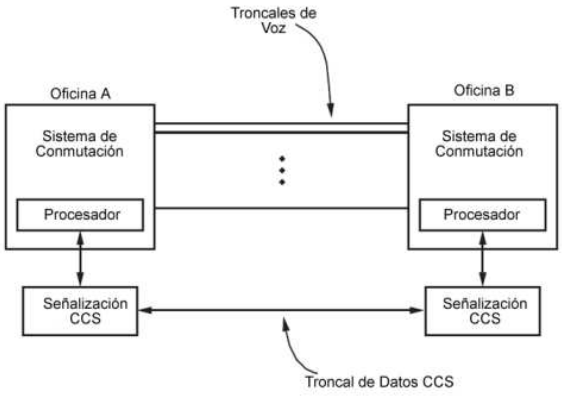


Figura 0.19 Esquema de CCIS en una troncal de voz [1]

A través de este canal se comenzaron a enviar las señales propias de la comunicación telefónica, lo que derivó en la creación de distintos protocolos de señalización Digital:

- ***ISDN (Integrated Services Digital Network o Red Digital de Servicios Integrados)***

Una de las más grandes promesas de integración de comunicación, que lleva en el mercado más de 20 años. Se estructura a través de dos canales para cada uno de los tráficos; la voz se envía a través del canal portador (Bearer Channel o B-Channel), mientras que la señalización se la envía a través de Canales-D.

La falta de una estandarización adecuada hizo que cada fabricante propusiera su propia ISDN, esperando que su idea revolucione el mercado y sea aceptada como estándar de facto; lo que generó la creación de dos tipos de ISDN, volviéndola costosa y de difícil aceptación, aunque muy utilizada en sistemas de troncalizado.

- *ISDN-BRI/BRA*

Basic Rate Interface (o Basic Rate Access): Usualmente conocida solo como ISDN, consiste en dos canales-B de 64 [Kbps] controlados por un canal-D de 16 [Kbps], dando un total de 144 [Kbps] de transmisión. Usado principalmente donde sistemas como DSL no están disponibles o son extremadamente costosos, principalmente en Norteamérica, en Europa, por el contrario ha remplazado casi en su totalidad a los sistemas analógicos, a pesar de que, desde su concepción, tuvo problemas de convergencia de estándares, equipos costosos, y poca documentación sobre el mismo.

- *ISDN-PRI/PRA*

Primary Rate Interface (o Primary Rate Access): Utilizado básicamente para proveer servicio en grandes conexiones. Usa principalmente sistemas PDH T1 (23B+D, en USA) y E1 (30B+D, en Europa). Es mucho más competitivo que BRI.

- ***SS7 (Signalling Service 7 o Servicio de señalización 7)***

Basado en los sistemas de AT&T CCIS. Es el estándar UIT-T de las recomendaciones Q.7XX, es conceptualmente similar a ISDN, y es utilizado en portadoras de red. Es el estándar de señalización para los sistemas telefónicos mundiales, ya que los datos se envían a través de un canal separado,

proporcionando seguridad de acceso a la señalización. Además, proporciona enlaces nativos de tráfico VoIP hacia la PSTN.

1.3 VOZ SOBRE IP (VOICE OVER IP O VOIP)

La evolución de los sistemas de digitalización hizo posible que la transmisión de datos a través de redes no conmutadas se tornara en el estándar de transmisión de información, y en conjunto con la misma, la voz digitalizada. Afirmar cuándo se comenzó a transmitir voz a través de la Internet es bastante arriesgado, ya que los primeros experimentos sobre procesamiento digital de señales datan de principios de los 70's, cuando la DARPA, en su ARPANET investigaba los procesos de transmisión de la que luego sería conocida como Internet.

Este insipiente desarrollo dio pie a que cada vez estos sistemas comiencen a posicionarse en las mentes de los ingenieros hasta que en 1989 se fundó VocalTec Communications. Alón Cohen y Lior Haramaty, graduados del área de telecomunicaciones de las fuerzas de defensa israelí, desarrollaron, a partir de sus conocimientos de paquetización de voz, la primera aplicación de VoIP de la historia, un salto cuantitativo sin precedentes considerando que se dio cuando las computadoras comerciales aún utilizaban pantallas monocromáticas. VocalTec utilizó por primera vez UDP para la transmisión de sus señales de voz a través de una Red Doméstica o de Área Local, aun cuando este protocolo de transmisión no ofrecía la seguridad del recibimiento de la información, lo que podría provocar retardos, además de distorsiones como jitter, propias de los sistemas digitales. Sin embargo, las pruebas de los israelíes demostraron que en una red local, estas distorsiones no se presentaban, sin necesidad de implementar mecanismos de corrección.

Este tipo de tecnología se comenzó aplicando para reducir los costes de llamadas internacionales entre Estados Unidos de América y el Reino Unido. VocalTec además desarrolló la tecnología para presionar a los primitivos módems de los 90's y a los procesadores 486 y enviar la información a través de una canal de 10 [Kbps], dejando libre el CPU para otras aplicaciones. Estos avances les

permitieron crear, en 1995 su aplicación prima, Internet Phone, o iPhone, que se ejecutaba sobre los nodos de comunicación sin necesidad de instalar hardware adicional, además de que presentaba un sistema para prevenir los retardos producidos por jitter y/o pérdida de paquetes. El sistema era simple, se podía llamar a cualquier otro usuario siempre y cuando este haya activado el software en su PC y se haya suscrito al servicio iPhone. Esta revolución, sin embargo, dejaba de lado una cuestión importante: la interoperabilidad.

iPhone no podía llamar a nadie más que no sea a otro iPhone, hacerlo implicaba llegar a un acuerdo con el otro agregado, añadiendo a la comunicación hardware de conversión o software añadido a alguno de los terminales. La propia VocalTec, en conjunto con Daniel Beringer establecieron un sistema global de intercambio de voz mediante IP, conocido como ITXC, poniendo a Internet como el medio para una llamada internacional, además de añadirle al estándar la comunicación con la PSTN, permitiendo al proveedor de VoIP llamar con relativa facilidad a cualquiera que posea un teléfono, sea este físico, o no.

ITXC fue el modelo de Vonage Holdigs Corp. Compañía que luego se posicionaría como el primer proveedor de VoIP en marzo de 2002; un año antes de que Skype haya siquiera presentado su primer beta[5].

[5] Beta se refiere a la primera versión completa de un programa informático, que aún está inacabado, pero que es completamente funcional.

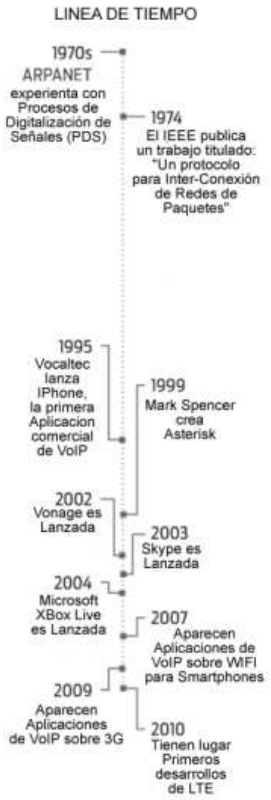


Figura 0.20 Línea de tiempo del desarrollo de VoIP [6]

Paralelamente se fueron desarrollando las redes caseras, y los accesos a Internet mediante DSL. La VoIP se vio enfrentada a tener que atravesar con su protocolo los firewalls de los enrutadores caseros, además de traducir los sistemas NAT[6], por lo que Vonage y otros distribuidores se enfrascaron en discusiones acerca de los términos del estándar que se debía seguir para las comunicaciones. En 2003 Skype, actualmente el mayor proveedor de VoIP del mundo, se saltó esta discusión pasando por alto los estándares y estableciendo su propia tecnología de comunicación.

Skype implementó un sistema de comunicación peer-to-peer, con ruteo descentralizado, proporcionando a cada usuario un canal encriptado y separado de los otros usuarios, y que permitía abrir un túnel que evitaba los firewalls y los direccionamientos de NAT. Además proporcionó un set de códecs de alta

[6] Network Address Translating, sistema de comunicación que utilizan equipos de conectividad para facilitar la comunicación de redes de valores incompatibles.

compresión que permitían entregar un mejor audio que el que la línea telefónica podía manejar.

En resumen, la transmisión de voz paquetizada a través de la red IP, como puede apreciarse en la reseña, no depende solamente de la red como tal, sino de un sistema de protocolos y códecs que permitan que la voz no solo sea enviada a través del canal de transmisión, sino que esta mantenga la calidad y la inteligibilidad de la transmisión vocal analógica.

1.3.1 COMPONENTES Y PROTOCOLOS DE VOIP

Para que la voz pueda ser transmitida a través de la red IP, deben ser encapsuladas sobre un protocolo que soporte el tráfico en tiempo real, que a su vez, se encapsulara directamente sobre UDP. Desde este punto, para la red, la transmisión se vuelve transparente, ya que la trama UDP hace que para las capas inferiores, la trama sea considerada como una mas de datos, para su envío.

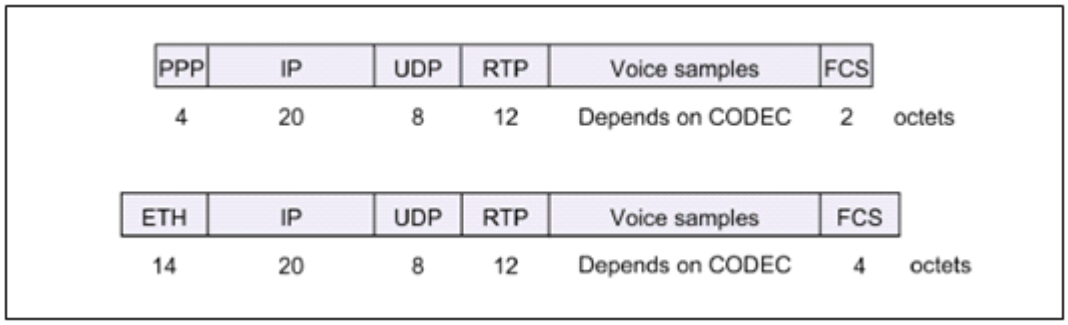


Figura 0.21 Ejemplos de tramas de VoIP sobre diferentes arquitecturas de red [26]

Cada arquitectura de red agregará o disminuirá la carga de cabeceras según sea el caso requerido, para direccionamiento, señalización y enrutamiento; pero mas allá de como se realiza la transmisión a nivel mas bajo, lo que hace que la VoIP sea posible son los protocolos de capas superiores, que definen la transmisión de la voz desde su digitalización.

1.3.1.1 Protocolos de Señalización

1.3.1.1.1 SIP

Session Initiation Protocol (o Protocolo de Inicio de Sesión) es un protocolo a nivel aplicación encargado de, iniciar una sesión de manera interactiva entre dos nodos de comunicación, conocidos como pares. Su fortaleza recae en que el sistema de transacciones se realiza de manera muy similar a como el protocolo HTTP[7] realiza sus transacciones. Además, su configuración también es basada en texto, lo que hace su uso más intuitivo para el programador.

SIP además no funciona de una manera vertical, lo que permite que pueda ser utilizado por otros protocolos de comunicación para formar un sistema multimedia completo. Típicamente, estos protocolos son RTP (*Real-Time Transport Protocol* o Protocolo de Transporte en Tiempo Real) y RTSP (*Real-Time Streaming Protocol* o Protocolo de Transmisión en Tiempo real), además de MGCP *(Media Gateway Control Protocol* o Protocolo de Control de Pasarela de Medios) y SDP (*Session Description Protocol* o Protocolo de Descripción de Sesión), formando un sistema que permite, en este caso, la transmisión de VoIP a través de la red con todas las características propias de la PSTN.

A pesar de estas capacidades, SIP no fue diseñado para proveer un servicio, ni para transmitir tráfico multimedia, además de que no ofrece controles de flujo y control de servicios, sino simplemente administra el inicio de la sesión de transmisión de datos, por medio de sistemas de mensajes, añadiendo seguridad, autenticación, encripción y servicios de privacidad entre el servidor y los pares.

[7] HyperText Transfer Protocol: Protocolo de transmisión de Hiper-Texto, protocolo base de las comunicaciones, base de Internet.

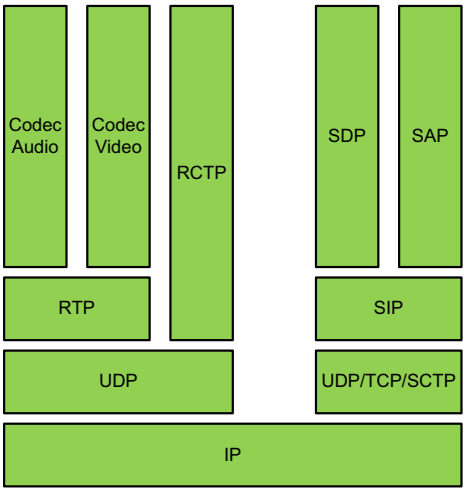


Figura 0.22 Arquitectura del protocolo SIP [4]

Fue definido por la IETF a través del RFC 3261, y sus características principales son:

- **Localización:** Permite la transmisión de información de los usuarios desde cualquier lugar, sin que la movilidad presente un problema.

- **Negociación de parámetros:** A través del intercambio de mensajes, permite gestionar puertos, direcciones IP, tipo de códec, prioridades, etc.

- **Disponibilidad:** Permite determinar si un usuario está disponible antes de comenzar la comunicación.

- **Gestión de comunicación:** Informa de cómo se está desarrollando la comunicación, además de modificar los parámetros durante la sesión activa en función de los requerimientos de red.

Dentro de la comunicación SIP, existen varios elementos o sistemas que intervienen, y que se los conoce como agentes de usuario (User Agents o UA's), los mismos que manejan la señalización para iniciar, o finalizar las comunicaciones, y se dividen en:

- **Cliente (UAC):** Envía las peticiones de registro e inicialización y acepta respuestas a sus peticiones.

- **Servidor (UAS):** Recibe las peticiones de UAC y envía respuestas en función del pedido convenientemente.

Al mismo tiempo un teléfono IP puede ser UAC y UAS, ya que al momento del registro envía peticiones al servidor para poder estar habilitado, y asimismo, acepta peticiones de inicio de una llamada, para establecer las peticiones.

Para que se puedan enviar mensajes, cada dispositivo SIP debe acceder a una dirección otorgada por el servidor, muy similar a las direcciones de correo electrónico, llamadas URI (*Uniform Resourse Identifier* o Identificador Uniforme de Recursos), que se representa como:

sip:usuario@dominio-o-dir-ip[:puerto]

Donde cada dispositivo hace uso de la dirección usuario@dominio-o-dir-ip[:puerto]. El dominio lo asigna el servidor SIP o el Proxy SIP al cual están asignadas las terminales.

Clásicamente una comunicación SIP está determinada por lo que se llama un trapezoide SIP, que no es sino la representación de la comunicación que incluye servidores y terminales, y que simplifica la explicación de los sistemas SIP.

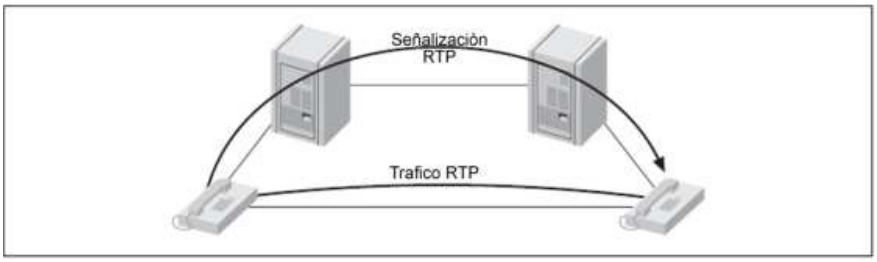


Figura 0.23 Representación del Trapezoide SIP [3]

Los servidores de SIP son de varios tipos y cada uno con funcionalidades diferentes, y se los utiliza dependiendo de su funcionalidad:

- **Servidor Proxy SIP:** hace las veces de un gestionador de mensajes SIP entre los distintos terminales. Almacena la dirección IP desde donde se comunican las terminales para poder enviarles los mensajes según el código de terminal asignado

- **Servidor de registro:** Permite a las terminales registrarse para que puedan ser localizadas por los mensajes SIP que son enviados desde las terminales y desde los servidores.

Cabe recalcar que Asterisk[8] no es un Servidor Proxy SIP, ya que puede actuar como un servidor de registro y, al mismo tiempo, como UAC, en forma de un *softphone*; en ese sentido Asterisk vendría a ser más un B2BUA (*Back-to-Back User Agent* o Agente de Usuario Intermedio), o también llamado Central, ya que para mantener el control de las peticiones SIP y consecuentemente de la llamada, Asterisk se queda en el medio de la misma, mientras que los paquetes RTP pueden ser enviados directamente entre terminales.

Esta funcionalidad de Asterisk le permite funcionar como una pasarela de diferentes tecnologías de comunicación, no solo SIP, sino como H.323, IAX o DAHDI, proporcionando soporte a cada una de ellas.

Como en los procesos de negociación de HTTP, SIP tiene distintos tipos de mensajes para la comunicación, que se dividen en peticiones y respuestas, cada una con su clasificación de acuerdo a su uso final.

[8] Asterisk es el sistema con el que se implementará el sistema de Telefonía IP, y que será explicado en el Capítulo Correspondiente.

Peticiones SIP[9]

Se clasifican en:

- ***Register*:** Es el primer mensaje que un UAC envía hacia la central una vez que ha ingresado a la red, informando su código asignado, su contraseña asignada, la IP desde donde está transmitiendo; para que la central proceda con el registro si los datos están correctos.

- ***Invite*:** Permite inicializar la comunicación entre dos terminales SIP, antes de una llamada, es la primera petición que se envía.

- ***Ack*:** Confirma que se ha recibido el paquete de aceptación 200 OK para el inicio de la comunicación. A partir de este momento, se transmite el tráfico multimedia.

- ***Bye*:** Finaliza la comunicación iniciada con Invite.

- ***Cancel*:** Sirve para cancelar una petición que aún está en curso.

- ***Options*:** Sirve para que el UAC solicite opciones o información sobre el UAS cuando sea requerido.

Respuestas SIP

Cuando se envía una petición SIP, del cliente al servidor o viceversa, inevitablemente se necesitarán mensajes de respuesta para confirmar o denegar un tipo de servicio. Estos mensajes poseen códigos que hacen que su identificación sea más sencilla y manejable por parte de las UA's. Las respuestas SIP se agrupan en:

[9] Estandarizadas en el RFC 3261; existen otras peticiones que se estandarizaron en otros RFC, sin embargo, no son tan comunes con las primeras.

- **Grupo 1XX:** Indican el progreso temporal de la comunicación luego que ha sido enviado el paquete Invite.

- **Grupo 2XX:** Indican el éxito de la negociación de la comunicación, como la 200 OK, como respuesta de Invite.

- **Grupo 3XX:** Informan del re-direccionamiento del paquete en cuestión hacia otro UAS para el establecimiento de la comunicación.

- **Grupo 4XX:** Indican errores de comunicación del cliente SIP.

- **Grupo 5XX:** Indican errores de comunicación del servidor SIP.

- **Grupo 6XX:** Corresponden a cualquier error adicional que pueda producirse.

Para una profundización de los tipos de Respuestas SIP, consultar el anexo H.

1.3.1.1.1.1 Manejo de la comunicación

SIP, como ya se explicó, hace uso de mensajes en forma de peticiones y respuestas que se envían entre terminales y con el servidor.

Cada evento en las comunicaciones SIP está marcado por el envío de estos mensajes, los escenarios más comunes de señalización son:

- ***Registro***

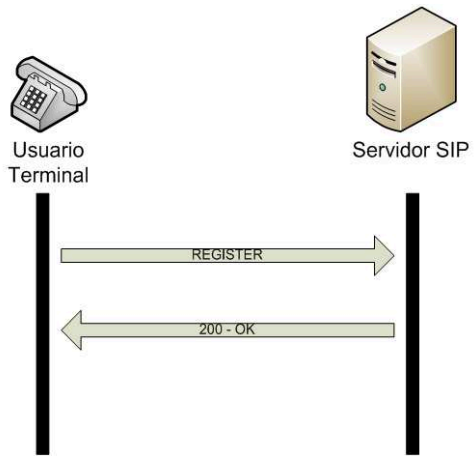


Figura 0.24 Registro sin autenticación

Debe recalcarse que este es un ejemplo puramente didáctico, ya que no debe aplicarse en una implementación real. Cuando un usuario, que no ha sido definido en el servidor con una contraseña, intenta anexarse al sistema, necesita enviar un mensaje de Register, en el cual comprueba su nombre de usuario, el sistema comparara si existe el nombre de usuario requerido, y en caso de existir, enviará un paquete OK, confirmando su registro en el servidor.

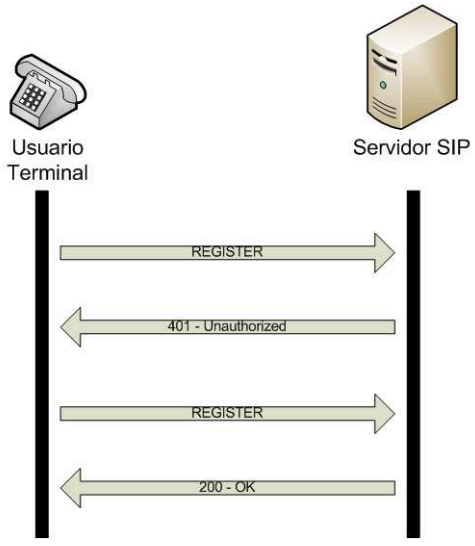


Figura 0.25 Registro con autenticación

Al existir autenticación el sistema no registrará a ningún usuario que no tenga las credenciales correctas, por lo que el envío de un paquete de registro simple será

rechazado, como No-Autorizado, con lo que la terminal deberá enviar un nuevo paquete de registro, pero que contenga los datos completos del sistema, que luego de ser comprobados por el servidor, se procede al registro en el sistema de dicha terminal.

- ***Inicio de sesión***

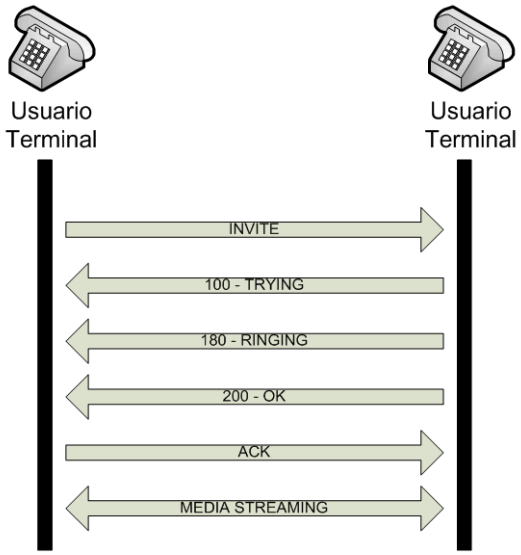


Figura 0.26 Inicio de sesión

Para iniciar una llamada SIP, una vez registrados las terminales, estos pueden comunicarse directamente sin necesidad de una entidad intermedia. Como se puede ver en el gráfico, cuando un usuario necesita iniciar una llamada, envía un mensaje INVITE, para informarle a otro usuario registrado de su situación, para comprobar la comunicación, el receptor enviará un mensaje TRYING, y una vez listo, enviará el mensaje RINGING, que activará el sistema de sonido de señalización en terminal inicial. Cuando se acepte la llamada, se enviará un mensaje ACK, con lo cual la transmisión de media puede dar inicio en ambos sentidos de la transmisión

- ***Finalización de sesión***

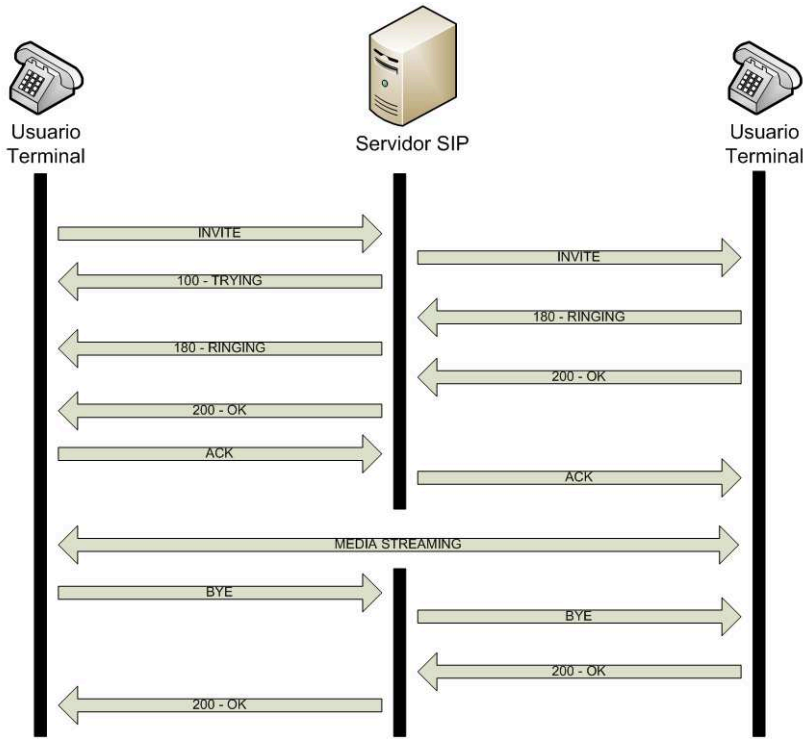


Figura 0.27 Finalización de la llamada

Luego de la transmisión de medios a través de la red, el usuario que desea finalizar la llamada, envía un mensaje BYE, el cual es aceptado de manera inmediata por el otro terminal, el cual sólo tiene opción de enviar un mensaje de OK a la finalización de la sesión.

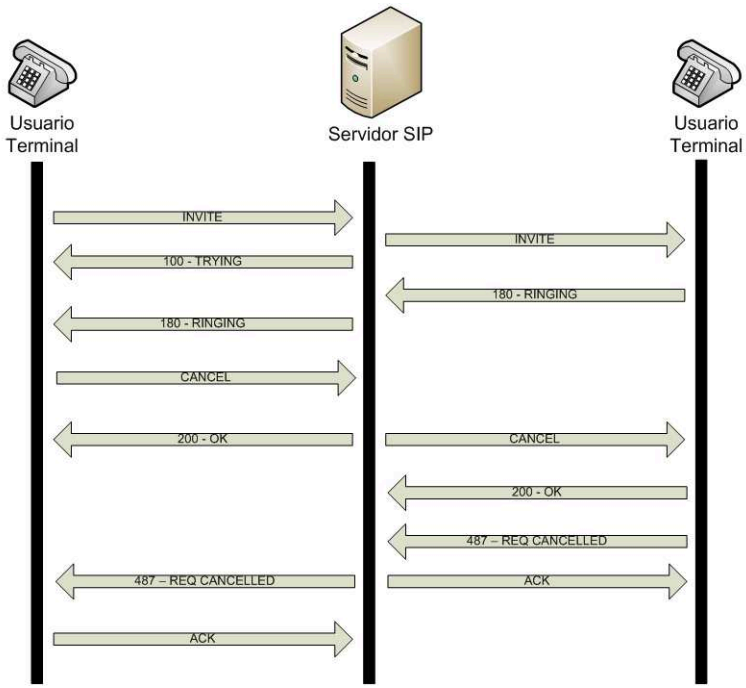


Figura 0.28 Cancelación de la sesión

Al contrario de una finalización de sesión, una cancelación ocurre cuando aún se está enviando mensajes RINGING, por lo que el envío de mensajes de medios nunca fue iniciado. Al enviar el mensaje CANCEL, el terminal receptor sólo puede enviar asimismo un mensaje OK, luego del cual confirmará que la sesión fue cancelada con un mensaje de REQ CANCELLED, confirmando el primer mensaje, tras lo cual, para finalizar la comunicación se enviará un paquete ACK de confirmación.

1.3.1.1.1.2 Seguridad y Enrutamiento

Al utilizar SIP envío de mensajes para autenticar a los usuarios, donde, a partir del mensaje INVITE, y una respuesta 407, se envía un testigo[10] que permite que un usuario sea autenticado, el mayor peligro que corre este protocolo es un ataque DoS (Denial of Service o Denegación de Servicio), que con una inundación de mensajes INVITE inválidos, hacen que el servidor colapse al no poder responder a tantos mensajes incorrectos de manera simultánea. Aunque un

[10] En sistemas de comunicación, un testigo en una porción de código usada para generar un Hash MD5 y aumentar la seguridad de la comunicación.

ataque como el descrito es virtualmente imposible de prevenir, se han implementado varios métodos para minimizar sus efectos, y bloquear cualquier ataque que persiga hacer colapsar al servidor. SIP, como tal, entre sus características puede impedir el acceso al paso de registro a todo aquel mensaje que se identifique como anónimo, es decir, que no haya sido previamente definido en el servidor.

Otro tipo de prevención viene desde el propio sistema operativo, su implementación se explicará más adelante.

Aparte, SIP, para establecer la comunicación entre la terminal y el dominio de llamado, utiliza un mecanismo conocido como Capa de seguridad de transporte, o TLS (Transport Layer Security), con lo que las peticiones se envían de manera segura hacia el servidor, basado principalmente en las seguridades que pueda presentar la red en donde el servicio está corriendo.

El enrutamiento de SIP encuentra en NAT uno de sus puntos débiles, ya que al ser NAT un protocolo de capa baja, la dirección de la información no es modificada automáticamente y muchas veces los paquetes de transmisión no suelen tener el direccionamiento correcto. El avance de la tecnología, sin embargo, ha hecho posible que los nuevos sistemas de borde permitan la traducción del encapsulamiento SIP para permitir la transmisión de datos a través de la red, lo cual ha dado mucha más fiabilidad a la utilización de softphones, sin embargo, SIP y NAT aún son un tema a tener en consideración antes de una implementación.

Además de SIP, que se ha vuelto el rostro visible de las comunicaciones IP por su versatilidad, Asterisk soporta otros protocolos de señalización, cada uno con sus propias virtudes, como son H.323 y IAX

1.3.1.1.2 H.323

El protocolo de comunicaciones de la ITU, diseñado para ser el estándar de audio y video de la Red, especialmente para aplicaciones de videoconferencia. Se diseñó pensando en la simplicidad de la PSTN, para brindar sus servicios mediante un conjunto de protocolos y los componentes necesarios para implementar una transmisión de medios.

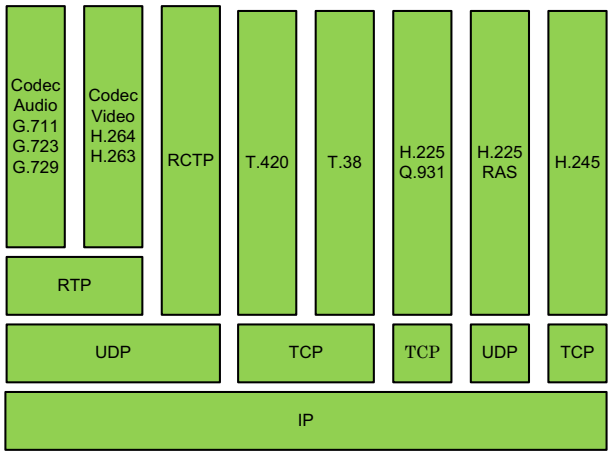


Figura 0.29 Arquitectura del protocolo H.323 [4]

Todo el conjunto de protocolos hicieron de H.323 un protocolo de señalización lo suficientemente robusto para soportar la transmisión de datos Multimedia a través de la red, sin embargo, su falta de modularidad le hizo perder espacio frente a SIP, que es mucho más flexible para su implementación.

1.3.1.1.2.1 Seguridad y Enrutamiento

H.323 es un protocolo relativamente seguro, y las mayores consideraciones de seguridad son las que se puedan aplicar a la red en sí misma, antes que al protocolo. Es por esta razón que H.323, antes que usarse en redes locales, es utilizado para transmisión de datos vía internet o entre ‘carriers’ o portadoras de datos, ya que en estos casos depende únicamente de la seguridad embebida en las conexiones o VPN’s.

Para el enrutamiento, en la recepción de llamadas, requiere del puerto TCP 1720 en cada cliente, además del conjunto de puertos UDP necesarios para la transmisión de medios, puertos determinados según el estándar. Sin embargo, si los clientes están detrás de un dispositivo NAT, se necesita de un gatekeeper que haga las funciones de proxy del sistema, en el cual los usuarios deben registrarse para poder comunicarse, lo cual lo hace complicado para su implementación a baja escala

1.3.1.1.3 IAX

Inter-Asterisk Exchange Protocol, o IAX es un protocolo propietario de Digium, diseñado para la comunicación entre centrales Asterisk. La diferencia más notoria entre este y otros protocolos es que además de utilizar un solo puerto (UDP 4569) para la comunicación de medios y señalización, no utiliza RTP sino su propio medio de transmisión especializado en voz, lo que lo hace mucho más compacto, y en teoría, potencialmente útil para transportar diferentes tipos de medios. Esto hace que el enrutamiento sea más sencillo y que no tenga ningún problema al tratar con equipos que estén atrás de un sistema NAT. IAX, entre sus funcionalidades, permite la troncalización de varias sesiones de datos dentro del canal de comunicación, lo que hace que al ahorro del ancho de banda sea mucho mayor que en otros protocolos, haciéndolo óptimo para sistemas con un alto tráfico de llamadas IP simultáneas.

1.3.1.1.3.1 Seguridad y Enrutamiento

IAX implementa 3 tipos de seguridad, texto plano, Hashes MD5 e intercambio de llaves RSA, los cuales, obviamente, no encriptan los medios que se transmiten, para lo cual es necesario informarle al sistema que lo haga mediante intercambio de llaves variables de longitud determinada por el usuario, lo cual lo vuelve mucho más segura para una transmisión, además de que comúnmente este protocolo se utiliza en VPN’s

Además, como se explicó anteriormente, IAX no tiene problema con NAT, ya que el uso de un solo puerto hace que no sean necesarias traducciones de ninguna clase, con lo que la transmisión se hace de manera transparente.

A pesar de todas las bondades de IAX, su reciente estandarización (al ser propiedad de Digium exclusivamente sólo está disponible para los equipos de esta marca) hace que muchos de los equipos, como teléfonos y servidores no estén soportados, volviéndolo una solución más bien costosa para una implementación de mediana escala. Además, IAX, al hacer uso de un solo puerto, requiere obligatoriamente el paso de información a través de los servidores, aumentando la carga de procesamiento para el mismo.

Se puede notar que en comparación, SIP es el protocolo más simple y, tal vez, menos seguro de los tres que están disponibles, sin embargo, esta sencillez, acompañada de su modularidad y su uso eficiente de puertos, que hace que las transmisiones RTP vayan directamente a los terminales, hizo que su implementación sea la primera en ser elegida por desarrolladores y la industria, en la que, casi todos los teléfonos conocidos, lo soportan nativamente.

1.3.1.2 Protocolos de audio

SIP y H.323 necesitan obligatoriamente de protocolos que permitan el transporte de la voz a través de la red de datos, sin embargo, estos protocolos deben estar provistos de técnicas necesarias para evitar los típicos problemas de la transmisión de los mismos, como jitter o retardos propios del sistema. Para este efecto, IETF desarrollo dos protocolos que cumplen con estas características, y son: RTP (Real-Time Transmition Protocol o Protocolo de Transmisión en Tiempo Real) y RCTP (Real-Time Transmition Control Protocol)

- ***RTP***

RTP esta estandarizado a través del RFC 3550, y es el encargado de la transmisión de voz y video a través de la red, utilizando UDP para el transporte, y un conjunto de herramientas, tales como números de secuencia, marcas de

tiempo, identificación de paquetes en el origen, sincronización, entre otros, para que la transmisión de estos datos pueda darse de una manera fluida. Obviamente por sus características no puede asegurar que la información enviada llegue adecuadamente, pero garantiza que esta llegue, al menos, sincronizada.

- ***RCTP***

RCTP funciona de manera conjunta con RTP, monitoreando su comportamiento dentro de la red, y ofreciendo estadísticas de su uso, que se relacionan con la calidad del servicio prestado. A pesar del monitoreo RCTP no está capacitado para reservar ancho de banda de transmisión o algún sistema de control dentro del canal de comunicación, lo cual lo vuelve simplemente un analizador del funcionamiento, aunque recomendable, de RTP.

- ***SDP***

Adjunto a estos dos protocolos, esta SDP (Session Description Protocol o Protocolo de Descripción de Sesión), que está definido en el RFC 4566 y detalla cómo se realizara el intercambio de paquetes entre los dos terminales, incluidos datos específicos de la comunicación. Este protocolo es muy usado en los inicios de sesión de SIP, donde en el mensaje INVITE, se envían todos los parámetros, como direcciones IP, códecs y puertos por medio de los cuales se va a realizar la comunicación.

1.3.1.3 Códecs

Antiguamente, la definición de Códec se refería al paso de la información analógica a digital (COdificador-DECodificador), pero en un mundo casi completamente digitalizado, donde el ancho de banda de transmisión de información es crítico para aplicaciones, el códec se ha tornado en un sistema de compresión de información para la transmisión de la misma (COmpresor-DECompresor).

El propósito de los códecs en la transmisión de VoIP es la de brindar un equilibrio entre la eficiencia de comunicación (léase menor uso de ancho de banda) y calidad de comunicación (léase fidelidad de transmisión).

Los códecs que son más comúnmente usados para este tipo de trasmisiones ofrecen cada uno sus ventajas, y está en el implementador escoger aquel que esté más acorde con su escenario de trabajo, y son:

- ***G.711***

El códec de telefonía por excelencia. Refiere a la conversión de la información telefónica analógica a digital a través de PCM, con sus variantes μlaw y alaw[11]. Utiliza un Ancho de banda de 8 [KHz.], lo que hace que la tasa de transmisión sea de 64 [Kbps]. Es la base de compresión del resto de códecs que pueden ser utilizados para transmisión, además de que no representa casi carga alguna para el CPU del equipo en cuestión, sea este un teléfono o el servidor de telefonía.

- ***G.726***

Basado en ADPCM (Adaptive Differential Pulse Code Modulation, o Modulación de Pulsos diferencial Adaptivo), lo que hace que pueda trabajar en diferentes tasas de transmisión, menores a las especificadas en G.711, como 16, 24 y 32 [Kbps], aprovechando el uso del ancho de banda de la red. A pesar de aprovechar de mejor manera el ancho de banda, la calidad de la transmisión es muy similar a G.711, y su consumo de CPU no es tan crítico, volviéndolo un códec de mucha utilización.

- ***G.729A***

Único códec disponible para Asterisk que no es libre. Su tasa de transmisión es de 8 [Kbps], ya que utiliza CS-ACELP (Conjugate-Structure Algebraic-Code-Excited Linear Prediction o Predicción Lineal de Estructura conjugada de Código de alteración Algebraica). Su compresión la hace útil para transmisión de VoIP a través de 'carriers' o portadoras de datos, o entre sistemas Asterisk

[11] Explicadas anteriormente

interconectados. Por tener un alto grado de compresión, exige mucho más trabajo de CPU

- ***GSM***

La alternativa libre de G.729A, por su tasa de transmisión de 13 [Kbps], aunque su calidad de sonido este muy por debajo de G.729A.

- ***iLBC***

No es tan popular como los códecs de la ITU, y por tanto no tan compatible con equipos de telefonía IP. Aunque ofrece un equilibrio recomendable entre calidad y eficiencia, su complejo algoritmo y su uso considerable de CPU lo vuelve una alternativa poco atractiva para la implementación.

- ***Speex***

Es un códec de tasa de bit variable, lo que hace que responda a las características de transmisión de la red. Es un códec completamente libre, y su tasa de bit está entre 2,15 y 22,4 [Kbps]

1.4 TELEFONÍA IP, Y SU DIFERENCIA CON LA VOIP

Desde su concepción, la telefonía ha sido el medio para comunicar a dos o más personas que se encuentras alejadas una de la otra, basándose en los principios de funcionamiento de la telegrafía; el paso del tiempo hizo que este sistema evolucione y se fortalezca, pero siempre manteniendo el principio básico de ofrecer un servicio de comunicaciones entre dos puntos físicamente alejados entre si.

Con el surgimiento de los sistemas en tiempo real que funcionan sobre Internet, la ubicuidad de la red como tal, permitió que el transporte de paquetes entre sitios remotos se pueda realizar con un mínimo de perdidas, abriendo las puertas para que nuevas tecnologías de comunicación, en específico voz y video, puedan proliferar en una red convergente.

El hecho de que se pueda transmitir voz digitalizada ha hecho que nuevos sistemas de envío de voz aparezcan facilitando la comunicación (Skype es el más popular), pero llevando a estos sistemas de comunicaciones a un lugar difuso, tanto que muchos usuarios han confundido los servicios de envío de voz a través de la red, con la Telefonía.

La Telefonía IP se define como el conjunto de servicios que se valen de la ubicuidad de internet y de la tecnología aplicada para la transmisión de VoIP, para transmitir señales digitalizadas que originalmente se transmitían a través de una red de circuitos conmutados. Al integrar los servicios telefónicos sobre una red de datos se tiende una plataforma de servicios convergentes que aprovecha las capacidades de ambos mundo, proporcionando un canal exclusivo de comunicación a través del cual los servicios convergentes se envían entre los usuarios a través de una red de paquetes conmutados.

Esta 'fusión' de dos mundos conceptualmente diferentes (el mejor esfuerzo, como concepto de funcionamiento de Internet, no es precisamente la forma de trabajo de un teléfono) ha dado pie para la innovación de los canales de comunicación, volviéndolos más robustos ante ataques, más constantes ante pérdidas de paquetes, más estables frente a la comunicación, lo que ha colaborado al desenvolvimiento de los sistemas de telefonía sobre la red, dándole al teléfono un campo más en el cual desarrollarse.

A pesar de que el concepto de Telefonía IP se manifiesta como un conjunto de servicios, es muchas veces confundido simplemente con la VoIP, que es la tecnología que la hace posible. Este error parte de que se asocia simplemente a la telefonía IP como voz sobre una red de datos, dejando de lado los servicios que ya venían integrados en la telefonía tradicional, además de los nuevos servicios, propios de la red IP.

La principal diferencia entre VoIP y la Telefonía se enmarca en que como tecnología, la VoIP esta orientada a la convergencia sobre WAN, permitiendo transmisión de voz a bajos costes sobre un canal dedicado. La Telefonía IP se

orienta directamente a la convergencia sobre LAN, ya que permite trasladar las facilidades de las centrales tradicionales, pero añadiendo prestaciones, como la fácil escalabilidad y la migración de tecnologías, además de valores añadidos, como QoS y sistemas de verificación de datos, y que al estar en una red local, problemas como jitter, retardos, o perdida de paquetes, se ven casi nulificados por la propia topología de la misma, facilitando así las comunicaciones internas y la fácil migración de las mismas hacia el mundo de la red conmutada.

Mucho de la evolución de las pequeñas y medianas empresas se basa, independientemente en cual sea el foco de su negocio, en su capacidad de comunicación, interna y externa; y de su capacidad de promocionar y posicionar su producto en el mercado. Nada de esto puede realizarse sin un adecuado sistema de comunicaciones.

Cada vez más sectores optan por promocionar sus servicios y dar asistencia a través de interfaces web, y mediante contactos vía correo electrónico. Sin embargo, no se puede obviar la interacción de las personas para la solución de problemas y contactos profesionales.

Este capítulo indica las condiciones en las que se encontraba la empresa SACMIS Cía. Ltda. antes de la implementación de la central, y los cambios que fueron requeridos dentro de la infraestructura de red, para su correcto funcionamiento interno.

CAPÍTULO 2
ESTADO ACTUAL DE LA RED DE SACMIS Y SUS ADECUACIONES

2.1 SACMIS CÍA. LTDA

2.1.1 INTRODUCCIÓN

SACMIS Cía. Ltda. Ingeniería en Electrónica y Telecomunicaciones, es una compañía ecuatoriana fundada en Octubre del 2004, con el objetivo de satisfacer las necesidades tecnológicas de nuestros clientes.

2.1.1.1 Misión

Brindar las mejores alternativas para solucionar las necesidades tecnológicas de nuestros clientes aportando con nuestra experiencia, honestidad y responsabilidad en el cumplimiento de los objetivos y metas propuestas por las empresas que nos necesitan.

2.1.1.2 Visión

Ser una empresa de telecomunicaciones líder y de mayor eficacia en el desarrollo de proyectos con nuestros clientes, demostrando capacidad, profesionalismo y honestidad en todas nuestras actividades y de esta manera aportar con el desarrollo del país.

2.1.1.3 Política

SACMIS comercializa productos y servicios de telecomunicaciones de calidad, basándose en un sistema de gestión de calidad eficaz que permite el mejoramiento continuo de sus procesos, sobre la base de un personal profesional, motivado y comprometido.

2.1.2 SERVICIOS Y SOLUCIONES

Los principales servicios y soluciones que SACMIS Cía. Ltda. ofrece se agrupan en las siguientes categorías:

- ***Diseño, Instalación, Mantenimiento y Soporte de***
  - *Sistemas de telecomunicaciones de alta, media y baja capacidad (PDH, SDH, etc.).*
  - *BTS's, Radioenlaces de Microonda, FO y Sistemas privados de redes Spread Spectrum.*
  - *Líneas de transmisión, sistemas de antena y cableado.*
  - *Enlaces satelitales y su infraestructura.*
  - *Sistemas de energía, Rectificadores y grupos electrógenos.*
  - *Sistema de Fibra Óptica.*

SACMIS dispone de personal capacitado en la instalación y comisionamiento de BTS's Siemens, Nokia, Huawei ya que ha realizado proyectos tanto en Ecuador para CNT, Conecel, Telefónica a nivel nacional e internacional, por lo tanto SACMIS está en capacidad de ofrecer los siguientes servicios:

- *Instalación y mantenimientos de equipos Multiplexores eléctricos y de Fibra Óptica.*
- *Instalación y mantenimiento de BTS NOKIA, BTS's SIEMENS, etc.*
- *Instalación y mantenimiento de equipos de radio PDH Nokia/Siemens.*
- *Instalación y mantenimiento de equipos de radio SDH Siemens.*

- ***Diseño y construcción de redes voz / datos / Internet***
  - *Implementación de Redes LAN / WAN / MAN.*
  - *Redes canalizadas en cobre multipar.*
  - *Redes canalizadas en fibra óptica.*
  - *Soluciones de Cableado Estructurado.*
  - *Integración de Voz, Data, Fax, Vídeo.*

- *Provisión de equipamiento total, desde PC's pasando por Servidores de alta disponibilidad y cualquier tipo de equipo activo necesario para comunicaciones.*
- *Provisión de equipo activo de redes, switches, ruteadores, hubs, etc.*

- ***Soporte técnico***
  - *Monitoreo y mantenimiento preventivo y correctivo de Hardware y Software (24x7).*
  - *Monitoreo y mantenimiento de redes de comunicaciones.*
  - *Entrenamiento y capacitación al cliente.*
  - *Auditoria de redes LAN y WAN.*

- ***Capacitación***

El equipo de Sacmis ha dictado cursos a nivel nacional e internacional en los siguientes temas

- *Sistemas de multiplexación de alta capacidad SDH a nivel eléctrico y óptico y su tendencia a la convergencia de tecnologías (Claro- Perú).*
- *Sistemas de redes gestión, seguridad y análisis de fallas (Honduras)*
- *Sistemas de redes de gestión, seguridad y análisis de fallas (Nicaragua).*
- *Capacitación a Telefónica Ecuador: curso de Ingeniería de Sistemas de transmisión radiante PDH y SDH, sistemas de transmisión y multiplexación en fibra óptica, equipos de medición y forma de uso.*
- *Diseño instalación y mantenimiento de sistemas de radio enlaces SDH de última generación (Colombia).*
- *Diseño instalación y mantenimiento de sistemas de radio enlaces PDH y SDH de última generación (Venezuela).”*[12]

2.2 ESTADO ANTERIOR DE INFRAESTRUCTURA FISICA DE RED

SACMIS actualmente tiene sus oficinas en la Alemania N31-143 y Mariana de Jesús, en el sector de La Carolina, en el centro-norte de Quito. El edificio,

[12] Tomado de las actas constitutivas y definiciones de creación de SACMIS Cía. Ltda.

diseñado para oficinas y lugares de reunión, fue construido con cableado estructurado interno, sin embargo, el uso que la empresa le dio al espacio no se ajustó al cableado existente, por lo que muchos de estos puntos de red quedaron inutilizados.

El edifico mencionado está conformado por dos plantas, que a su vez se subdividen en dos sub-plantas cada una, y están distribuidas de la siguiente manera:

- ***Planta 1***
  - Sub-planta 1: Oficinas de Técnicos de Campo.
  - Sub-planta 2: Bodega y Comedor.

- ***Planta 2***
  - Sub-planta 1: Oficinas Administrativas.
  - Sub-planta 2: Oficina de Gestión de Proyectos.

La Sub-planta 1 de la planta 1 originalmente no tenía ningún punto de red, se conectaba vía inalámbrica a la red central de la empresa.

La sub-planta 2 de la planta 1 tenía un cable llevado fuera de canaleta para la conexión de la computadora de la persona encargada de bodega. Además de esta “conexión” existían puntos de red que están inutilizados por el uso que se le dio al espacio en cuestión.

La Sub-planta 1 de la Planta 2 tenía diversos puntos de red, ubicados en cada oficina de acuerdo como se muestra en el anexo C, siguiendo la siguiente distribución:

- Oficina de Gerencia: 3 puntos de red etiquetados como Voz15/Datos04 (conexión 3) y Datos03 (conexión 4)
- Oficina de Contabilidad y Ventas: 2 puntos de red etiquetados como Voz14/Datos02 (conexión 5)

- Oficina de Recursos Humanos y Sistemas: 5 puntos de red etiquetados como Voz13/Datos01 (conexión 6), Datos12 (conexión 7) y Voz16/Datos11 (conexión 8)
- Recepción: 4 puntos de red etiquetados como Voz18/Datos07 (Conexión 1) y Voz17/Datos06 (conexión 2)

De estos puntos de red, la ocupación se daba de la siguiente manera:

- Voz 14 asignado a Server-Magus (Servidor de Manejo Contable)
- Datos 11 asignado a RR-HH
- Datos 12 asignado a Sistemas
- Datos 07 asignado a Recepción
- Datos 02 asignado a EQC67-Alicia (Ventas)
- Datos 03 asignado a Impresora Xerox
- Datos 01 asignado a Impresora HP
- Voz 15 asignado a la línea CNT de SACMIS
- Voz 13 asignado a Fax de SACMIS

La Sub-planta 2 de la Planta 2 asimismo constaba de distintos puntos de red, este espacio se utiliza exclusivamente para el departamento de Dirección de proyectos, y sus puntos de red, especificados en el anexo C son 4, etiquetados como Voz19 (conexión 9), Datos08 (conexión 10), Datos09 (conexión 11) y Datos10 (conexión 12); siendo la ocupación de los mismos el punto de Voz19, que se usaba como conexión temporal del servidor de Telefonía.

En total, el edificio contaba con 18 puntos de red habilitados, distribuidos como:

Planta		Descripción	Puntos funcionando	Puntos totales
Planta 1	Subplanta 1	Ningún punto	-	-
	Subplanta 2	Conexión de PC de Bodega	-	-
Planta 2	Subplanta 1	Oficinas de Gerencia	2	3
		Oficina de contabilidad y ventas	2	2
		Oficina de Recursos Humanos y Sistemas	4	5
		Recepción	1	4
	Subplanta 2	Dirección de Proyectos	1	4
Total			10	18

Tabla 0.1 Distribución de los puntos de red por espacio de trabajo

Cada una de estas conexiones contaba con una toma de energía para la conexión de los equipos necesarios, y en algunos casos, cajetines ciegos para la administración del paso de cables.

Conexión en el Patch Panel	Conexión referenciada en el plano	Conexión Utilizada en el Conmutador	Uso de la Conexión	Etiqueta de la Conexión
Datos01	Conexión 6	-	Impresora HP	-
Datos02	Conexión 5	-	PC Ventas	-
Datos03	Conexión 4	-	Impresora Xerox	-
Datos04	Conexión 3	-	-	-
Datos05	-	-	-	-
Datos06	Conexión 2	-	-	-
Datos07	Conexión 1	-	PC Recepción	-
Datos08	Conexión 10	-	-	-
Datos09	Conexión 11	-	-	-
Datos10	Conexión 12	-	-	-
Datos11	Conexión 8	-	PC RR-HH	-
Datos12	Conexión 7	-	PC Sistemas	-
Voz13	Conexión 6	-	Fax SACMIS	-

Voz14	Conexión 5	-	Conexión Server-Magus	-
Voz15	Conexión 3	-	Línea CNT-SACMIS	-
Voz16	Conexión 8	-	-	-
Voz17	Conexión 2	-	-	-
Voz18	Conexión 1	-	-	-
Voz19	Conexión 9	-	Conexión Temporal Asterisk	-
Voz20	-	-	-	-
Voz21	-	-	-	-
Voz22	-	-	-	-
Voz23	-	-	-	-
Voz24	-	-	-	-

Tabla 0.2 Distribución de los puntos de red existentes en SACMIS previo a la re-adecuación

2.3 ESTADO ACTUAL MODIFICADO DE LA INFRAESTRUCTURA DE RED FISICA

Para la implementación del proyecto, si bien la infraestructura estaba en condiciones óptimas de conexión, su ubicación y prestaciones hacían inviable la aplicación del proyecto con este sistema, por lo que la re-adecuación se volvió imperiosa.

Para realizar estas modificaciones y re-adecuaciones al sistema de cableado de la empresa, se realizo una interpretación libre de la normas EIA/TIA 568-B, 569, y 606, la misma que cumple los parámetros establecidos en todas estas normas, en cuanto utilización del cableado, conectores y la instalación de la misma, además del etiquetado y la administración del mismo, pero que no es estricta con respecto a la ingeniería de cableado como tal, es decir, la adecuación a realizar se enfoca mas en el funcionamiento del sistema con su respectiva planeación a largo plazo, dejando un poco de lado las certificaciones que exige la norma como tal. Cabe recalcar que, si bien este cableado no podría llamarse estructurado, el

cumplimiento de los requerimientos técnicos hace que fácilmente pueda aprobarse como tal si requiriera el caso.

El porqué de no plantear el cableado como directamente estructurado, a pesar de utilizar sus normas técnicas para la implementación responde a que la situación de la empresa no ameritaba una planeación de tal magnitud, sino simplemente una adecuación que permitiera utilizar el sistema de una manera correcta, adecuada y que permitiera la administración completa del sistema, para su mantenimiento y adecuación, pero no al nivel de certificar cada punto de utilización.

Las modificaciones consisten en reutilizar gran parte del cableado existente y con el mismo implementar nuevos puntos de red, además de realizar un nuevo cableado, y utilizar de mejor manera el equipo activo, a fin de cumplir el requerimiento de transmisión para la compañía.

Tal como demostraron Alón Cohen y Lior Haramaty cuando diseñaron iPhone, las aplicaciones en tiempo real de trafico de voz se podían utilizar en una LAN sin utilizar métodos de corrección, lo que hacia que el canal de transmisión no jugara un papel preponderante en el diseño de la red. Con esa consideración, se decidió mantener en la adecuación la categoría 5e de cableado existente, el cual podía soportar adecuadamente el tráfico de red, incluyendo el tráfico de VoIP.

A partir de la consideración anterior, se determino que con la adecuación de la red, se mantendrían los 18 puntos de red, y se añadirían 5 puntos de red, dando un total de 23 puntos en toda la red física, los cuales quedan distribuidos como se explica en la tabla 2.3.

Planta		Descripción	Puntos para Datos	Puntos para Voz
Planta 1	Subplanta 1	Oficina de Departamento Técnico.	1[13]	1
	Subplanta 2	Bodega	1	-
Planta 2	Subplanta 1	Oficinas de Gerencia	4	1
		Oficina de contabilidad y ventas	3	1
		Oficina de Recursos Humanos y Sistemas	4	1
		Recepción	3	-
	Subplanta 2	Dirección de Proyectos	3	1
Total				23

Tabla 0.3 Distribución de puntos de red luego de la modificación.

Para la ampliación de los 5 puntos nuevos[14], se realizaron cálculos a través del método indirecto para determinar el número de rollos y de corridas por rollo que serian necesarias para la implementación. En base a los esquemas arquitectónicos, y a las mediciones realizadas se tienen los siguientes resultados:

Ubicación de los nuevos puntos[15] y determinación del punto más lejano y del punto más cercano:

- Más cercano: Punto de recepción (SCIP-PD13) a una distancia de 4.5 [m]
- Más lejano: Punto de Departamento Técnico (SCIP-PV05) a una distancia de 13 [m].

A través de estos datos, es posible calcular las corridas necesarias para la ampliación, que resultaría en:

[13] Funciona como una extensión de la red inalámbrica, por lo que no tiene conexión directa a los Switches.

[14] Para el resto de puntos de red, se reutilizara el cableado interno existente y las extensiones requeridas se las especificara de acuerdo a su utilización.

[15] Establecidos en los esquemas de los anexos D y E

Número de Puntos	Punto más Cercano (m)	Punto más Lejano (m)	Distancia Promedio (m)	Corridas disponibles por rollo	Rollos Requeridos
5	4.5	13	12.13	25	1
Total número de rollos de cable					1

Tabla 0.4 Determinación del número de corridas necesarias para la modificación de cableado

Para determinar el número de corridas, se realiza un promedio entre la mayor distancia y la mínima, y a este resultado se le añade una holgura del 10%, y finalmente una holgura de terminación de 2.5 [m] para obtener la distancia promedio de cada corrida.

Con lo que se determina que se necesita un rollo para suplir las necesidades de ampliación como de relocalización de puntos de red.

A partir de estos cálculos, es posible cambiar la administración del cableado, en la cual cada nuevo punto de red recibió un nuevo etiquetado, denominado SCIP-PDXX o SCIP-PVXX, donde:

- SCIP significa SACMIS-IP.[16]
- PD significa cableado de Datos.
- PV significa cableado de Voz; las XX serán los nuevos números de etiquetado.

Según esa asignación, la ubicación de los puntos de red de acuerdo a su ubicación, quedan especificados en los anexos D y E y se nombran:

La Sub-planta 1 de la Planta 1 adquiere dos puntos de red, etiquetados como SCIP-PV05/SCIP-PR01 (Conexión 18), donde PV05 es el punto de telefonía para el Departamento Técnico y PR01 es el punto de extensión para la Red Inalámbrica de SACMIS, aumentando la cobertura de red para la planta baja.

[16] Comúnmente el primer campo informa el número de piso y de rack en el que va el etiquetado, pero como el requerimiento solo hace uso de un rack, se prefirió darle un nombre corporativo al primer campo de la nomenclatura.

La Sub-planta 2 de la Planta 1 modifica la conexión del computador de Bodega, añadiendo un punto de red para la mejor administración del sistema, quedando etiquetado como SCIP-PD14 (conexión 19).

La Sub-planta 1 de la Planta 2 sufre cambios en su infraestructura de red, de la siguiente manera, basada en el anexo E:

- 1: SCIP-PD01; Asignado a computador
- 2: SCIP-PD16/SCIP-PD17; Utilizado para la conexión con la impresora de red Xerox (16) y un punto ocasional si se requiriera.
- 3: SCIP-PV01; Asignado a Teléfono IP físico del departamento de Gerencia.
- 4: SCIP-PD15; Conexión Ocasional, en caso se requiriera un punto adicional en caso de una reunión.
- 5: SCIP-PD02; Asignado a computador.
- 6: SCIP-PD03; Asignado a computador.
- 7: SCIP-PD05; Asignado a computador.
- 8: SCIP-PV06/SCIP-PD08; Asignados a conexión de Fax de SACMIS y Computador
- 9: SCIP-PD09/SCIP-PV03; Asignados a Impresora HP y conexión del Teléfono IP físico del departamento de Sistemas[17].
- 10: SCIP-PD04/SCIP-PV02; Asignados a la conexión del teléfono IP físico del departamento de Ventas y Logística y a Computador.
- 11: SCIP-PD13; Asignado a computador.
- 12: SCIP-PD06; Asignado a Servidor Magus.
- 13: SCIP-PD07; Asignado a computador.

El punto 2 se mantiene y se re-etiqueta, el punto 1 se anula y se cambia por un cobertor de cajetín. Las conexiones asignadas a estos puntos en el patch panel se utilizaran para las nuevas corridas con los q se definen los nuevos puntos 1 y 3 de la oficina de gerencia, donde el punto 3 se convierte en el punto de voz IP. El

[17] Hasta que el teléfono sea necesario, este punto quedará desocupado.

punto 4 se mueve a través de una extensión de 1.75 [m] para servir como punto auxiliar en la oficina de gerencia en caso de una reunión, y se lo ubica donde comúnmente esta situada la silla de los invitados. El anterior punto 3 se separa en los nuevos puntos 5 y 6; donde el punto 6 a través de una extensión de 3.1 [m] para que puedan servir cerca de los escritorios de gerencia. La razón de utilizar la anterior conexión 3, y no dejar que funcione el punto cercano, es que de esta manera se utilizan mejor los recursos, moviendo dos puntos, en lugar de solo tener una extensión larga para el punto ocasional.

El punto 8 se mueve con una extensión de 1,8 [m], junto al fax y al escritorio de Recursos Humanos para que las conexiones entre el punto de red y el equipo no sean demasiado largos, mejorando la administración de los mismos, el punto 7 se mantiene en el mismo lugar y se utiliza para el computador de Sistemas. El punto 6 se transforma en el punto 9, con etiquetación SCIP-PD09/SCIP-PV03, utilizados para la conexión de voz de Sistemas y Recursos Humanos, así como para la conexión del PC del Gestor de Talento Humano de la empresa.

El anterior punto 5 es ahora el punto 10, y que se etiqueta como SCIP-PD04/SCIP-PV02, que es el punto de voz de los departamentos de Contabilidad y Ventas, y Logística, así como la conexión del PC del supervisor de Logística de la empresa.

Del patch panel saldrán 3 nuevos puntos: 11,12 y 13, donde el punto 11 es el punto para la computadora de recepción (SCIP-PD13), mientras que los puntos 12 y 13 serán para contabilidad (12) y ventas (13), llamados SCIP-PD06, SCIP-PD10 y SCIP-PD07, respectivamente.

La Sub-planta 2 de la Planta 2 también realiza cambios en su estructura, referenciando el anexo E:

- 14: SCIP-PD05; asignado a computador.
- 15: SCIP-PD06; asignado a computador, de manera eventual.
- 16: SCIP-PD07; asignado a computador, de manera eventual.

- 17: SCIP-PV03; Asignado a Teléfono IP físico del departamento técnico.

El punto de datos 11 de la enumeración anterior se mueve de posición con una extensión de 4.2 [m] para dar servicio de red ocasional a los Directores de proyectos, para no congestionar la red Inalámbrica, y se renombra con el punto 16; el punto de voz 09 se lo utilizara como punto de datos, con denominación SCIP-PD05, y se lo llamará 14 en el plano final. El Punto de datos 12 se convierte en punto de voz IP SCIP-PV03; este punto se utilizara para el teléfono del departamento de proyectos.

2.3.1 ETIQUETAS DE CABLEADO

Para cada nuevo cable de sección, se especifican nuevas etiquetas que serán colocadas, siguiendo la siguiente numeración[18]:

- SCIP-CPDXX, donde C significa Cable, y XX será el número de denominación del punto en cuestión.
- SCIP-CPVXX, utilizando la misma denominación anterior.
- SCIP-CCDXX, donde la primera C es cable, la segunda C es conexión, y XX será el número de denominación del punto en cuestión; este cable se utiliza para conectar al equipo (computador, fax, etc.) con el punto de red.
- SCIP-CCVXX, utilizando la misma denominación anterior.
- SCIP-CSWXX, donde SW significa Switch, y XX el punto al que numéricamente corresponde el cable en cuestión.

Además de estas etiquetas, existen otras que sirven para marcar los cables de Servidores y conexiones de módems:

- SCIP-PR01: Etiqueta de Flat Panel para Router Inalámbrico Secundario.
- SCIP-CCS01: Etiqueta para el cable de conexión entre switches.

[18] El encabezado de las etiquetas mantiene su significado, explicado previamente.

- SCIP-CCR01: Conexión entre Modem de Internet y el Servidor Proxy y de Correo
- SCIP-CCE01: Conexión del Servidor Proxy y de Correo al Switch
- SCIP-CTF01: Conexión del Servidor de Telefonía al Switch
- SCIP-CRI01: Conexión del Router Inalámbrico y el Switch
- SCIP-CPR01: Conexión entre Routers Inalámbricos
- PCS-XX: Numeración del Patch Panel

Conexión anterior en el Patch Panel	Conexión Actual en el Patch Panel	Conexión en el Plano	Conexión en el Conmutador	Uso de la Conexión	Etiqueta de la Conexión
Datos01	PCS-01	Conexión 1	1	PC Gerencia	SCIP-PD01
Datos02	PCS-02	Conexión 5	2	PC Gerencia	SCIP-PD02
Datos03	PCS-03	Conexión 6	3	PC Gerencia	SCIP-PD03
Datos04	PCS-04	Conexión 7	4	PC Sistemas	SCIP-PD05
Datos05	PCS-05	Conexión 14	5	PC Proyectos	SCIP-PD10
Datos06	PCS-06	Conexión 15	6	PC Proyectos	SCIP-PD11
Datos07	PCS-07	Conexión 16	7	PC Proyectos	SCIP-PD12
Datos08	PCS-08	Conexión 13	8	PC Ventas	SCIP-PD07
Datos09	PCS-09	Conexión 8	9	PC RR-HH	SCIP-PD08
Datos10	PCS-10	Conexión 12	10	PC Server-Magus	SCIP-PD06
Datos11	PCS-11	Conexión 11	11	PC Recepción	SCIP-PD13
Datos12	PCS-12	Conexión 19	12	PC Bodega	SCIP-PD14
Voz13	PCS-13	Conexión 4	13	Eventual Gerencia	SCIP-PD15
Voz14	PCS-14	Conexión 9	14	PC RR-HH	SCIP-PD09
Voz15	PCS-15	Conexión 8	15	FAX	SCIP-PV06

Voz16	PCS-16	Conexión 2	16	Impresora Xerox	SCIP-PD16
Voz17	PCS-17	Conexión 2	17	Eventual Recepción	SCIP-PD17
Voz18	PCS-18	Conexión 3	18	Voz Gerencia	SCIP-PV01
Voz19	PCS-19	Conexión 9	19	Voz Sistemas	SCIP-PV03
Voz20	PCS-20	Conexión 17	20	Voz Sistemas	SCIP-PV04
Voz21	PCS-21	Conexión 18	21	Voz Técnicos	SCIP-PV05
Voz22	PCS-22	Libre	Libre	Libre	Libre
Voz23	PCS-23	Conexión 10	22	PC Logística	SCIP-PD04
Voz24	PCS-24	Conexión 10	23	Voz Logística	SCIP-PV02
-	-	-	24	Conexión con segundo SW	SCIP-CCS01
-	-	-	25	Servidor SACMIS	SCIP-CCE01
-	-	-	26	Servidor Telefonía	SCIP-CTF01
-	-	-	27	Conexión Router Inalámbrico	SCIP-CRI01
-	-	-	40	Conexión con primer SW	SCIP-CCS01

Tabla 0.5 Distribución de los puntos de red en SACMIS luego de la readecuación de la Red

2.4 CAMBIOS EN EL CUARTO DE TELECOMUNICACIONES

Originalmente, el inmueble contaba con un pequeño rack de pared, que contenía un patch panel de 24 posiciones y al que estaban conectados los puntos de cableado interno, a más de esas conexiones, SACMIS contaba con dos switches de 8 puertos de manejo plug'n play, en los cuales la mayoría de las conexiones iban directamente hacia el computador en cuestión, porque no existía una

conexión de punto de red. Todas estas conexiones formaban una clásica 'telaraña' de cables, en los cuales ninguno estaba etiquetado, haciendo casi imposible una labor de mantenimiento

Para la habilitación de la Central, y por tanto de los nuevos puntos de red y sistemas, era necesario un rediseño del cuarto de equipos, en el que el rack de pared fue removido para dar paso a un nuevo rack de piso, el cual debía contener no solo los nuevos equipos de conectividad, sino también los servidores de correo electrónico y de telefonía, además de las acometidas de telefonía e internet. El hecho de que el rack deba contener todos estos elementos, hizo que sea necesario utilizar un rack de 42 U[19], que tiene de altura 1.9 [m], el cual sigue la distribución indicada en la figura 2.1

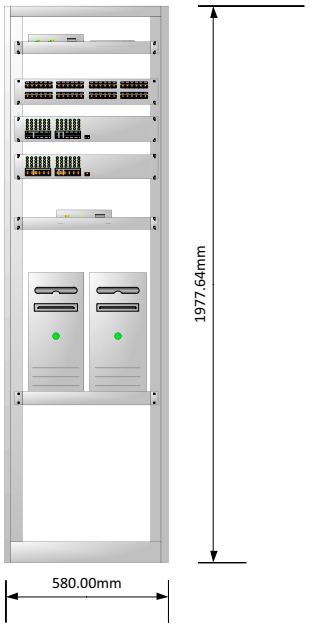


Figura 0.1 Distribución de rack para el cuarto de equipos

Los servidores, así como los módems y los Routers inalámbricos se instalaron en bandejas rígidas, las de los servidores a una altura de 46 [cm], que equivalen a las 18 [in] que recomienda la norma EIA/TIA 568-B para la colocación de face plates, lo cual pone en resguardo a los equipos en caso de una posible

[19] Unidades de Rack, equivalentes a 47.1 [mm]

inundación. Las conexiones eléctricas serán distribuidas en una toma de energía de 8 posiciones para ser instalada en rack, que será colocada en la parte posterior del rack a una altura de 1.5 [m], alejando estas conexiones de las tomas de datos, para evitar cualquier posible interferencia. Cada uno de los cables vienen con las etiquetas diseñadas para la administración del sistema, y los cables vienen organizados mediante un sistema de “peinado”, el cual permite un manejo completo de los cables sin tener que usar un organizador plástico.

Las líneas telefónicas, así como todas las conexiones de internet también llegan a este armario, y son colocadas en bandejas en la parte superior, para facilidad de manipulación por parte del servicio técnico del proveedor, y que este mantenimiento no afecte el cableado de la empresa. Las líneas que vienen desde la acometida de CNT se conectan directamente a la tarjeta transformadora de Telefonía. En el siguiente capítulo se explicará su funcionamiento y utilidad.

Como se expuso el capítulo 1, los grandes inventos son comúnmente fruto de un accidente o de necesidad. Asterisk es una prueba de ello.

Linux Support Services necesitaba comunicarse con el mundo exterior, y necesitaba hacerlo para poder dar soporte técnico a sus clientes en Linux. Las centrales telefónicas digitales e IP propietarias ofrecían sus servicios a costos elevadísimos, por lo que la empresa no podía costear un servicio como tal, así que optó por desarrollar una central de telefonía basada en C para Linux que fuera de arquitectura abierta. Así nació Asterisk. Con el tiempo, el soporte técnico de Linux fue dejado de lado para ofrecer un producto revolucionario: Una Central Telefónica Completamente hecha por Software.

Éste capítulo presenta una breve reseña de la creación de Asterisk, sus usos principales, y de qué parámetros se siguieron para la implementación de la Central Telefónica en SACMIS, su funcionamiento y su potencial de expansión.

CAPÍTULO 3
DISEÑO, IMPLEMENTACIÓN Y EJECUCIÓN DE UN SERVIDOR DE TELEFONÍA IP PARA SACMIS, DE ACUERDO A PARÁMETROS ESTABLECIDOS

3.1 ASTERISK

'*Once upon a time, there was a boy*
...with a computer
...and a phone.
This simple beginning begat much trouble!'[20]

3.1.1 CARACTERÍSTICAS

Asterisk utiliza para su funcionamiento una arquitectura modular, lo que hace posible que al momento de su instalación, sólo los módulos requeridos sean instalados, permitiendo ahorros, tanto de espacio en disco como de recursos de memoria. La característica modular también permite que los desarrolladores puedan implementar nuevos sistemas y adiciones sin modificar el núcleo central o alterar los módulos precedentes, lo que hace a Asterisk un sistema netamente escalable y extensible.

Al instalarse en un sistema Linux, su sistema de directorios es bastante más complejo que un habitual programa binario, cada directorio de Asterisk ejecuta una parte diferente del programa, utilizando los recursos del sistema de mejor manera:

[20] 'Una vez, hubo un muchacho, con una computadora y un teléfono. Este comienzo simple acarreó muchos problemas'. Así definió Mark Spencer la base de la creación de Asterisk. Foreword de Asterisk. The Future of Telephony. Second Edition.2007

El árbol de directorios se compone de:

- **/etc/asterisk/:** contiene los archivos de configuración y dimensionamiento de Asterisk, además del archivo asterisk.conf, que es el que controla a todo el sistema.

- **/usr/lib/asterisk/modules/:** Contiene los módulos binarios de ejecución del programa.

- **/var/lib/asterisk/:** Contiene diversos directorios que ejecutan funciones diferentes dentro de Asterisk. Principalmente contiene el archivo astdb, la base de datos principal del sistema, que almacena los datos y registros propios de Asterisk.

Los directorios que se almacenan en este son:

- **/var/lib/asterisk/agi-bin/:** Contiene los scripts AGI que pueden ser ejecutados desde el dial-plan.

- **/var/lib/asterisk/firmware/:** Contiene archivos de firmware propios de la comunicación de Asterisk con otros sistemas o dispositivos.

- **/var/lib/asterisk/images/:** Contiene imágenes, que pudieran ser transmitidas si el canal lo permitiese.

- **/var/lib/asterisk/keys/:** Almacena las llaves de autenticación RSA si es que el sistema hace uso de las mismas.

- **/var/lib/asterisk/moh/:** Carpeta que contiene la música de espera (music on hold).

- **/var/lib/asterisk/sounds/:** Contiene los sonidos que puede utilizar Asterisk dentro del manejo del dial-plan o de distintas funciones.

- **/var/lib/asterisk/static-http/:** Contiene los elementos web para Asterisk-GUI, si es que estuviera instalado en el sistema.

- **/var/spool/asterisk/:** Contiene directorios que están relacionados con las funciones de entrada/salida del sistema:

  - **/var/spool/asterisk/díctate/:** Contiene los archivos generados por la función Dictate.

  - **/var/spool/asterisk/meetme/:** Contiene los archivos generados por la función MeetMe desde el dial-plan.

  - **/var/spool/asterisk/monitor/:** Contiene los archivos generados por las funciones Monitor y MixMonitor.

  - **/var/spool/asterisk/outgoing/:** Contiene archivos que le permiten al sistema generar llamadas automáticas, de estar configuradas.

  - **/var/spool/asterisk/system/:** Contiene los archivos temporales producidos por la función System.

  - **/var/spool/asterisk/tmp/:** Contiene los archivos temporales de Asterisk antes que sean movidos a otra ubicación o eliminados.

  - **/var/spool/asterisk/voicemail**/: Contiene los archivos generados por la función voicemail, además de las referencias de los buzones de voz.

  - **/var/run/:** En este directorio se almacena en un archivo el PID de funcionamiento de Asterisk.

  - **/var/log/asterisk/:** Contiene los archivos de almacenamiento de eventos del sistema.

3.1.2 HERRAMIENTAS DE LAS QUE DISPONE

Una de las fortalezas de Asterisk, es que implementa todos los sistemas y protocolos de los cuales hace uso la VoIP, lo que hace que su funcionamiento sea totalmente abierto a la implementación de protocolos y códecs estandarizados, que funcionan de manera nativa.

En sí, Asterisk no está diseñada para ser, *per se*, una PBX-IP, sino que es algo parecido a una “caja de herramientas”, que permite realizar, entre otras cosas, una PBX-IP, que además de re-direccionar las llamadas, permite realizar otras funciones como monitoreo, sistemas de grabación y Call-Centers, funciones de SMS y tanto como el usuario se sienta en la capacidad de programar e implementar utilizando el núcleo Asterisk.

Para la transmisión de la VoIP, la parte más importante es la de cómo las llamadas realizan su señalización; para este cometido, Asterisk, utiliza los protocolos que VoIP ha generado desde su aparición, tales como SIP, o IAX. Estos protocolos, que han sido detallados en el Capítulo 1, han permitido extender de una manera segura el uso de la Tecnología, y darle la disposición de servicio para su aplicación.

3.2 REQUERIMIENTOS TÉCNICOS DE LA IMPLEMENTACIÓN

Para su comunicación con el mundo exterior, SACMIS posee dos líneas telefónicas de CNT, de las cuales, una estaba asignada al Fax, y la otra como línea de comunicación como tal. Sin embargo, esta comunicación estaba condicionada al lugar en donde estaba el aparato telefónico, y la persona en cuyo puesto se encontraba el mismo, que en este caso fungía como operadora, literalmente, tenía que correr con teléfono en mano hasta llegar al destinatario.

En vista de esta situación, el uso de una central telefónica se volvió imperativo, sin embargo, las características de comunicación de la misma debían cumplir determinados requisitos:

- Que además de que cada persona tenga su extensión, cada departamento de la empresa tenga su línea específica, además de la línea del operador.

- Que tenga en cuenta la ausencia del llamado, es decir, que si una persona no se encuentra mientras la llamada ha entrado, en lugar de ir directamente al buzón de mensajes, o sencillamente perderse, pueda pasar dando saltos hacia otras extensiones, y en el caso que ninguna conteste, arribar al buzón de la persona llamada originalmente.

- Que el buzón de mensajes envíe un correo electrónico cuando ha recibido un mensaje, adjuntando el mismo: La mayor parte de la plantilla de SACMIS trabaja en campo, por lo que no siempre tendrán su extensión a la mano, sin embargo, a través del correo empresarial, se hará llegar el mensaje de voz a cada persona como adjunto del correo electrónico.

- Que haya prioridades de llamada; es decir, las personas que trabajan en el departamento de proyectos, además de gerencia y recursos humanos, por obvias razones, necesitan llamar al exterior. Esta característica debe habilitarse mediante una clave de acceso, válida únicamente para la extensión en cuestión y que permita acceder a estos privilegios.

- Que se registre cada llamada realizada y recibida, para mantener un control de las mismas, y que permita manejar reportes, semanales o mensuales de cada llamada.

- Que el servicio que se preste a través de la central, sea muy similar a la calidad que ofrece la PSTN para sus comunicaciones, con ausencia de ecos, y un volumen adecuado.

Estos parámetros definirán las características principales con lo que la central debe ser diseñada y programada. Cada uno de los anteriores requerimientos

responden a una necesidad especifica de la empresa, y que con la central telefónica busca solventarse.

3.3 DIMENSIONAMIENTO DEL SERVIDOR

El dimensionamiento de un servidor, como tal, está mucho más *"cerca de ser un arte que una ciencia"*[21]. El dimensionamiento de un servidor de Telefonía IP en gran medida no depende de cuantas extensiones existan, o cuantas troncales se conectarán, sino del número de canales de comunicación simultáneos que va a soportar el servidor. A partir de estas consideraciones, el dimensionamiento del servidor que compete a este estudio queda constituido como:

3.3.1 HARDWARE

Asterisk, al ser un programa de desarrollo libre, posee diferentes versiones según el las necesidades del desarrollador. Sin embargo, para este proyecto se decidió utilizar la versión oficial del paquete de software, proporcionado por el diseñador, a través de la compañía Digium. Para la instalación del paquete oficial, la empresa recomienda determinadas configuraciones de Hardware para que el servidor funcione adecuadamente, tal como se especifica en la tabla 3.1.

Propósito	Número de Canales	Mínimo recomendado
Sistema de Prueba	No más de 5	400 [MHz] x86, 256 [MB] RAM
Sistema SOHO (Small office/home office, o pequeña empresa/domestico)	De 5 a 10	1 [GHz] x86, 512 [MB] RAM
Sistema PYMES	Hasta 25	3 [GHz] x86, 1 [GB] RAM
Sistema Empresarial	Más de 25	CPU's dobles, si es necesario en una arquitectura distribuida

Tabla 0.1 Guía de requerimientos [3]

[21] Ing. Iván Carrera Izurieta. Escuela Politécnica Nacional

Cabe recalcar, que estos “Mínimos recomendados”, cumplen ciertas holguras de trabajo, ya que Asterisk, como tal, puede funcionar en una Netbook de mínimas prestaciones, para un sistema SOHO.

La empresa cuenta con un Gerente General, un Gerente Técnico, un Gerente de Proyectos, un Gerente de Talento Humano; un coordinador de Logística, 4 Líderes de implementación de proyectos y un bodeguero, que, entre si, deben mantener una comunicación constante para manejar adecuadamente los proyectos que SACMIS tiene con sus clientes. Además cada líder de implementación debe mantener comunicación con cada líder de grupo de trabajo previo a la realización de trabajos. Este sistema de comunicación hace que, al menos, en una habilitación de proyecto existan 4 canales simultáneos entre todos estos participantes.

Si a esto sumamos la comunicación que debe existir entre el gerente de Talento Humano, y el Gestor de Talento Humano, y la comunicación entre todas las personas encargadas de contabilidad y ventas, y de estas con las gerencias mencionadas se tienen 3 canales simultáneos más que están todo el tiempo en ejecución.

Finalmente, las salas de reuniones telefónicas se han planificado para que puedan soportar hasta 10 usuarios, lo cual hace que la central maneje al tiempo, 10 canales simultáneos. Como las salas de reuniones no están habilitadas para el área administrativa, además de estos 10 canales se debe considerar los 3 canales del área administrativa.

Esta consideración de 13 canales simultáneos hace que el servidor deba ser diseñado para que al momento de su utilización, no presente fallas de comunicación, y pueda mantener correctamente la interacción de cada uno de estos canales conservando el SLA acordado, además de considerar que en cualquier momento puede necesitar de una ampliación sin que esta afecte a la infraestructura que esta funcionando. Con estas consideraciones se decidió implementar un servidor ‘clon’ ensamblado, siguiendo la recomendación de

Sistema PYMES dada por el fabricante, con lo que el servidor se montó con un Procesador doble de 3.2 [GHz] y dos Slots de 1 [GB] de RAM, además de un disco duro de 240 [GB], y un sistema de energía adecuado, de 600 [W] que le permita al servidor permanecer prendido sin sufrir recalentamientos o problemas similares. Todas estas características se establecieron de esa manera para que el servidor pueda trabajar holgadamente.

Además de las consideraciones de comunicaciones internas, el sistema debía estar dimensionado para que se puedan realizar llamadas hacia CNT, sin que se tuviera problemas de congestión o de llamadas en espera, por lo que se usó para el cálculo de entradas necesarias una calculadora de Erlangs, disponible en Internet, mediante la cual se realizó la estimación de las líneas CNT que serían necesarias para una correcta comunicación con la PSTN, usando los siguientes datos:

Durante el día de trabajo (9 horas)[22] en promedio se reciben alrededor de 25 llamadas, de las cuales, la duración promedio de las mismas es 3 minutos con 12 segundos.

Este dato promedio se lo obtuvo de los siguientes datos obtenidos de manera experimental en el transcurso de 2 semanas (10 días) de uso de las facilidades telefónicas, tal como se muestra en el anexo F. A partir de este valor se debe calcular el número de Erlangs[23], para lo cual se utiliza la formula de la ecuación 3.1 para obtener el valor [28]:

$$A = \frac{1}{T} * (n * m)[Erlang]$$

Ecuación 3.1 Definición del cálculo de Erlangs

[22] 8 horas de trabajo con una hora de almuerzo, en la cual se siguen recibiendo y realizando llamadas.

[23] Valor utilizado en telefónica como medida estadística del volumen de trafico de un canal de comunicación

Dónde:

- A es el número de Erlangs del sistema en cuestión.
- T es el periodo de tiempo (en segundos) dentro de los cuales se realiza el cálculo de muestras.
- n es el número total de llamadas realizadas en el periodo T
- m es la duración promedio de la llamada n

Haciendo el cálculo correspondiente obtenemos:

$$A = \frac{1}{9(3600)} * \left(25 * 3.2(60)\right) = 0.148148 \dots [Erlang]$$

Calculado el número de Erlangs, se recurre a una herramienta en línea, que permite el cálculo del número de canales telefónicos necesarios para la implementación, el cual se encuentra en http://www.erlang.com/calculator/erlb/:

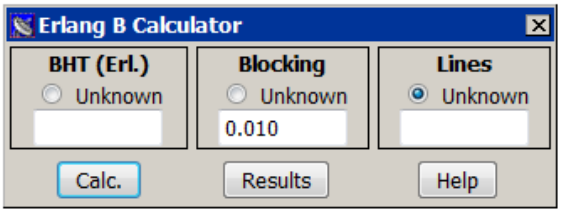


Figura 0.1 Calculadora de Líneas Telefónicas On-line

Dónde:

- BHT es el número de Erlangs, calculado anteriormente
- Blocking es la tasa de bloqueo de llamadas o GOS (Grade of Service o Grado de Servicio). Para un sistema como el estudiado, se asume que la pérdida de llamadas es de 1 por cada 100 llamadas realizadas, por lo que el valor es de 0.01
- Lines es el valor a calcular, en función de los valores anteriores

Utilizando esta herramienta, los valores correspondientes son:

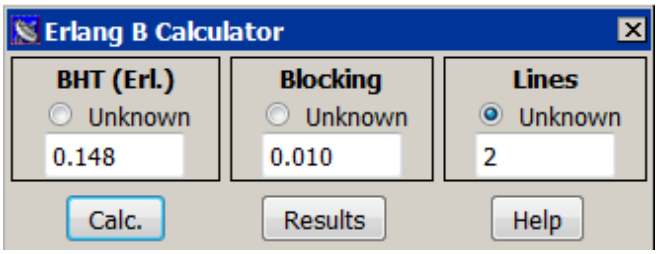


Figura 0.2 Resultados Obtenidos

Lo que nos da una necesidad de dos líneas telefónicas para el correcto uso del sistema.

En el mercado existen 2 tipos de tarjetas controladoras de telefonía para servidores; las proporcionadas directamente por el fabricante del software y un clon de altísimo rendimiento, que, al igual que la original, ofrece compatibilidad absoluta con el sistema, sin embargo, por decisión empresarial, se utilizara la tarjeta original, que es una tarjeta DIGIUM TDM410, que posee dos conexiones FXO para las líneas analógicas externas necesarias, y dos conexiones FXS para conexión de teléfonos analógicos. Además, posee un módulo de supresión de eco, muy útil para poder cumplir con la SLA determinada en los parámetros.

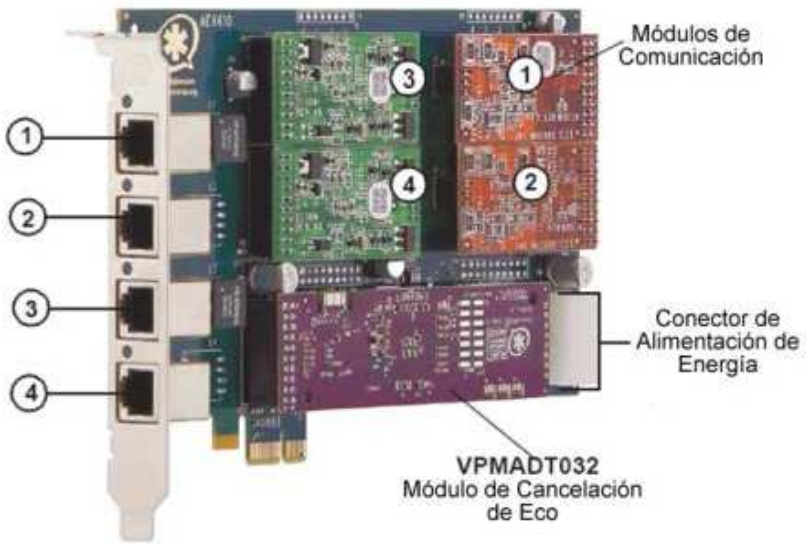


Figura 0.3 Tarjeta DIGIUM TDM410, donde especifica los puerto 1 y 2 para líneas externas (FXO) y 3 y 4 para teléfonos analógicos (FXS), además del supresor de eco [19]

3.3.2 SOFTWARE

Asterisk, como programa, viene soportado para Distribuciones GNU/Linux y MAC, por lo que la elección del software nativo que soportara el sistema, tiene un abanico de posibilidades.

Para la implementación, se escogió la distribución GNU/Linux basada en Red Hat conocida como CentOS, ya que es una distribución conocida y ampliamente soportada por una comunidad entera de desarrolladores; además de que su ejecución utiliza pocos recursos del sistema como tal. Sin embargo, la razón de peso para la elección de este sistema operativo se basa en su kernel[24], que es casi absolutamente estable, por ser una versión anterior a la versión de kernel que está en el mercado, lo que la hace más robusta por todas las pruebas que se le han realizado, y proporciona la estabilidad que necesita la tarjeta DIGIUM para funcionar sin problemas, lo cual es imperantemente necesario para que la comunicación con la PSTN se dé en buenas condiciones, tanto como ofrece la propia red telefónica.

La tabla 3.2 presenta la matriz de decisión que se siguió con los parámetros que se consideraron para la selección del sistema operativo, basados en las recomendaciones del fabricante, de estudiosos y desarrolladores de sistemas Asterisk, de desarrolladores de sistemas operativos basados en Linux, y de implementadores de sistemas Asterisk, cuyos escritos fueron consultados para la realización de este proyecto[25], y que en función de sus estudios se determino los valores que se deben considerar para tomar la decisión al momento de escoger una distribución. A estos valores se asignaron pesos en función de su importancia, medidas cualitativamente entre 0 y 10; además de un grado de importancia por valor, medido cualitativamente entre 0 y 5.

[24] Núcleo de casi todos los sistemas operativos existentes actualmente, en el que se almacenan las librerías necesarias para la conexión de hardware con software de un computador

[25] Textos que pueden ser consultados en la Bibliografía.

Factores	Soporte Técnico		Uso de Licencias		Compatibilidad		Acceso como Usuario Root		Kernel		Repositorios		Total /220
Pesos	8		5		7		7		10		7		
CentOS	3	24	5	25	5	35	5	35	4	40	3	21	180
Red Hat Linux	4	32	3	15	5	35	5	35	3	30	3	21	168
Ubuntu	5	40	5	15	5	35	1	7	2	20	5	35	152

Tabla 0.2 Matriz de decisión para selección de sistema operativo del servidor

Dónde:

- Soporte técnico se refiere a la cantidad de ayuda sobre el Sistema Operativo que se encuentra en Internet o directamente por parte del Proveedor o Distribuidor, y a la velocidad con la que la ayuda puede ser obtenida.
- Uso de Licencias se refiere a si el uso del Sistema Operativo es completamente libre o si en parte o en su totalidad tiene un costo para el usuario.
- Compatibilidad se refiere a la facilidad de instalación del Sistema Operativo en cualquier sistema computacional disponible.
- Acceso como Usuario Root se refiere a si el Sistema Operativo permite, por defecto, trabajar sobre el sistema como SuperUsuario, o guarda restricciones de configuración dentro del sistema para proteger la funcionalidad.
- Kernel se refiere a la fiabilidad y estabilidad del núcleo del sistema para el trabajo de las aplicaciones y del hardware instalado.
- Repositorios se refiere a la facilidad de acceso a paquetes de instalación complementarios para el Sistema Operativo, y que permitan hacer funcionar al Sistema de Mejor Manera.

A través de esta matriz, aseguramos la elección de CentOS como sistema Operativo para la Central, por sus características.

3.3.3 SLA (SERVICE LEVEL AGREEMENT O ACUERDO DE NIVEL DE SERVICIO)

Dentro de los requisitos del sistema, se estableció que las llamadas que se realicen a partir de la central telefónica y las que se reciban deben tener la misma calidad y fiabilidad que tienen las llamadas telefónicas que se producen directamente en la PSTN, por lo que el SLA, gira en torno a esa calidad de transmisión y recepción del sonido. Como se explicará posteriormente, este acuerdo se ve afectado por el uso de softphones, en lugar de teléfonos fijos IP o teléfonos analógicos conectados a la tarjeta de conversión.

3.4 DEFINICIÓN DE FUNCIONES DE LLAMADA Y DIAL-PLAN

Según los requerimientos del sistema de SACMIS, el nuevo sistema telefónico debe integrarse directamente a la red existente, la cual en su configuración consta de una componente cableada y una inalámbrica:

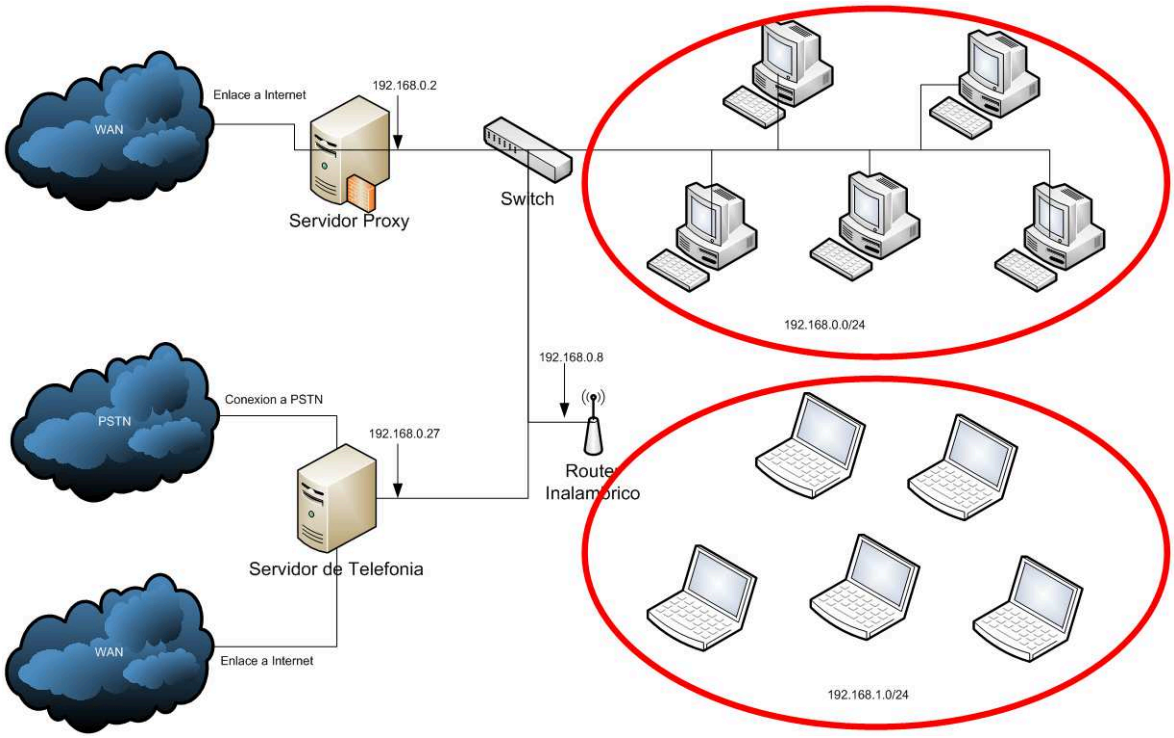


Figura 0.4 Diagrama de la Red de SACMIS

En la parte cableada de la red, se encuentran los servidores de Correo, de Contabilidad y de Telefonía, además de las PC's de Recursos Humanos, de Sistemas y de Ventas, de estos computadores, solo los servidores de correo y de Telefonía no cuentan con una extensión virtual. De la parte inalámbrica todos los computadores cuentan con su propia extensión.

Cada una de estas extensiones virtuales depende de la dirección IP del PC para poder realizar el direccionamiento de llamadas. El direccionamiento IP de la red no es un valor importante a considerar al momento de implementar el sistema de telefonía, ya que solo es necesario que el PC tenga comunicación con el servidor. El acceso al mismo se realiza a través de un definido proceso de acreditación. En este sentido, la limitación de accesos vía asignación de IP's mediante DHCP a las PC's de la red esta a cargo del departamento de Sistemas; y esta basada en las restricciones de seguridad explicadas en el manual de procedimientos de seguridad explicada y desarrollada en el capitulo 4.

Además de las extensiones virtuales, el sistema debe contar con extensiones propias de cada departamento que funcione en la empresa, a saber: Gerencia, Sistemas, Proyectos, Técnico, Contabilidad, Ventas, Recursos Humanos y Logística[26].

El objetivo de tener estos teléfonos departamentales es el de, si la persona llamada no puede contestar, la llamada sea redirigida hacia el teléfono del departamento, donde la persona que se encuentre pueda tomar la llamada. Si, en caso de que ninguno de estos dos teléfonos sean contestados, la llamada será redirigida una segunda vez hacia la operadora del sistema, la cual siempre estará disponible para contestar cualquier llamada entrante. La razón del desarrollo de las transferencias secuenciales es que ninguna llamada realizada al personal de la empresa se pierda y siempre pueda ser contestada. Si, en el peor de los casos la llamada no puede ser contestada por la operadora inclusive, solo en ese

[26] Por cuestiones financieras, los teléfonos de departamentos no se han podido implementar, sin embargo, toda la infraestructura física y de software esta lista para su implementación.

momento la llamada será direccionada al buzón de mensajes de la persona a la que originalmente iba la llamada.

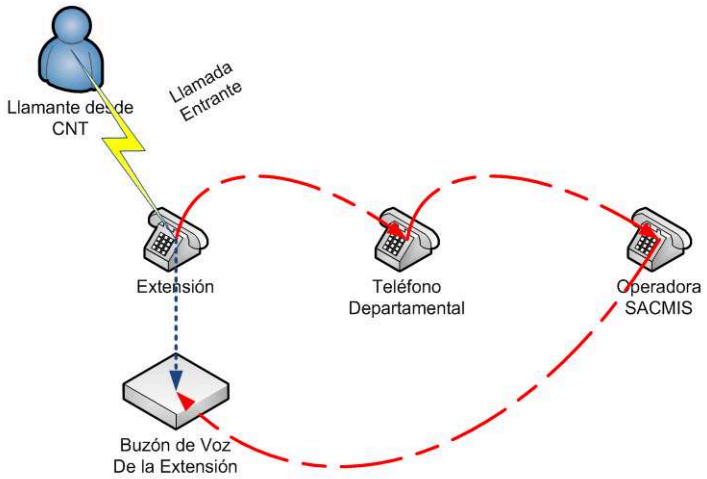


Figura 0.5 Esquema de transferencia de llamadas

El esquema de la Figura 3.5 muestra es funcionamiento de este sistema de transferencia de llamadas, donde con un rayo se representa la llamada que viene desde la PSTN y pasa a través de la central hasta llegar al usuario. Se la ha representado de esta manera, ya que para el usuario final el proceso de acceso a las llamadas se realiza de forma transparente. La flecha de color azul representa el camino natural que siguen las llamadas, es decir, una vez no contestada, ir directamente al buzón de voz. La flecha de color rojo representa como se desarrollan las transferencias secuenciales que se han desarrollado para el sistema de SACMIS.

Si la llamada se realiza hacia un teléfono de departamento, la forma de direccionamiento de llamadas es la misma, se estableció que es necesario que los clientes puedan acceder a los teléfonos de los departamentos, ya que no siempre se conoce la extensión deseada, facilitando la comunicación, y liberando relativamente de carga a la operadora del sistema, como se muestra en la figura 3.6.

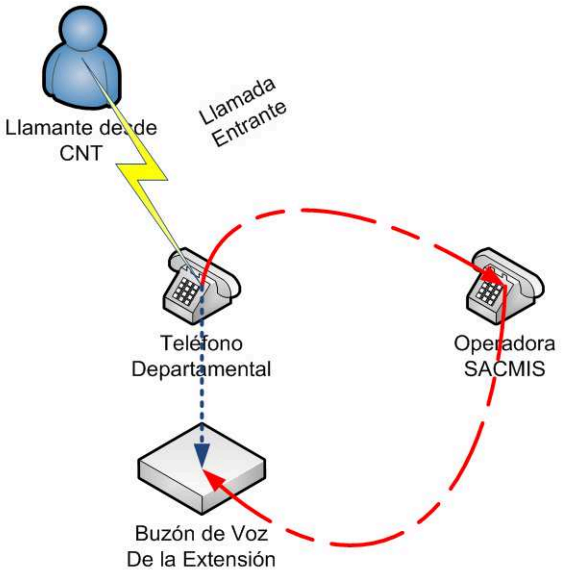


Figura 0.6 Esquema de transferencias de llamadas departamentales

A partir de estas funciones[27], se diseñó el menú de contestación de la central telefónica, que está constituido por dos subsistemas:

El primer subsistema recibe las llamadas de las personas que saben que extensión deben marcar, para lo cual se les ha asignado un tiempo de espera de 5 segundos, tiempo considerado como suficiente en el desarrollo de centrales telefónicas para que el usuario pueda recordar la extensión a la cual necesita acceder. Si en este tiempo la persona que realiza la llamada no ha marcado ninguna extensión, pasará al siguiente subsistema de menú.

El segundo subsistema presenta un menú de opciones, las cuales pueden ser marcadas por el llamante, y están distribuidas por:

- Opción 1: Ventas (Extensión 6020).
- Opción 2: Contabilidad (Extensión 6000).
- Opción 3: Proyectos (Extensión 4000).
- Opción 4: Sistemas (Extensión 3000).
- Opción 5: Técnico (Extensión 5000).

[27] La definición de estas funciones se la realiza en el archivo extensions.conf, que se encuentra en el anexo G.

- Opción 6: Fax (Conectado a un puerto FXS de la tarjeta, asignado como extensión 6500).

En caso de no presionar cualquiera de estas opciones en un tiempo establecido de 5 segundos, automáticamente la llamada pasará a una operadora, que en este caso es la misma extensión 6000.[28]

3.4.1 DIAL-PLAN

Para realizar una llamada externa desde cualquier extensión de la red, las personas deben marcar el número deseado, sea este local, nacional, celular, especial o de emergencias anteponiendo un 9, esto le dice a la central que la llamada será dirigida hacia las líneas troncales para su salida hacia la PSTN. La elección del número 9 se da porque así, se mantiene una diferenciación entre las extensiones internas y los números externos, para que no existan confusiones en las llamadas.

Una vez definidos todos los parámetros de llamada, los números asignados al Dial-plan quedan establecidos de la siguiente manera:

Extensión	Nombre
2000	Departamento de Gerencia
2010	Fernando Aucancela
2020	Christian Casamen
2030	Marcelo Huertas
3000	Departamento de Sistemas
3010	Tania Huertas
3020	Daniel Maldonado
4000	Departamento de Proyectos
4010	Marco Ballesteros

[28] Se acordó que la operadora sea la extensión 6000 por pertenecer al departamento de la Empresa en el que sus integrantes están siempre en la oficina, lo que hace que el teléfono de la operadora siempre sea contestado, evitando de esta manera que la llamada entrante pueda perderse.

4020	Armando Cuzco
4030	Ricardo Espinoza
4040	Fernando Yánez
5000	Departamento Técnico
5010	Carlos Bayas
5020	Danny Checa
5030	Fernando Chicaiza
5040	Esteban Cornejo
5050	Heriberto Dea
5060	Edgar Espinosa
5070	Pablo Espinoza
5080	Pablo Gavilánez
5090	Gabriel Guangaje
5100	Carla Ligña
5110	Javier Nono
5120	Wilson Puruncaja
5130	Paul Quimbita
5140	Diego Ramos
5150	Edwin Sailema
5160	Joselito Salazar
5170	Francisco Singo
5180	Víctor Solís
5190	Francisco Vinueza
6000	Departamento de Ventas y Contabilidad
6010	Daysi Brito
6020	Alicia Casamen
6030	Sandra Ushina
7000	Logística-Bodega

Tabla 0.3 Dial-plan implementado en SACMIS

Cada número de extensión consta de 4 dígitos, de los cuales el primero define el departamento al cual pertenece la extensión, y los siguientes dos números refieren al número que por orden se le ha asignado a cada usuario para su utilización. Se prevé que el personal de SACMIS aumente de acuerdo al número de proyectos permanentes que se negocian con los clientes. El planeamiento de Dial-plan considerando el crecimiento plantea un método de expansión de extensiones sin que afecte al diseño del mismo, el cual considera adicionar un digito al final, lo cual proporciona una ampliación de 90 posibles números

adicionales por departamento, proporcionando la holgura necesaria para aumentar extensiones sin necesidad de modificar el planeamiento de numeración de la Empresa.

3.5 CARACTERÍSTICAS DE LOS USUARIOS

Además de contar con un buzón de correo de voz propio, cada usuario forma parte de dos redes de telefonía distintas, la red interna, a la que tiene acceso sin restricciones, y la salida externa, para la cual necesita una contraseña.

La razón de la existencia de restricciones es económica, ya que, como todo servicio, la PSTN cobra por comunicar a sus suscriptores. Esa es la principal razón de que la salida hacia la PSTN sea monitoreada y restringida. Cada usuario posee una contraseña de 8 dígitos entre 0 y 9[29], que es asignada por extensión. Lo que vuelve a este sistema más seguro es el hecho de que SIP necesita saber la dirección IP desde donde recibirá paquetes, y para que pueda registrarse, esta dirección debe ser fija para cada extensión; lo que hace que la contraseña solo sea válida en un solo teléfono, o en un solo computador con *softphone*, volviendo inútil el robo de contraseñas.

Cada extensión del sistema, para poder registrarse como tal, debe además ingresar en la configuración del *softphone* la contraseña que ha sido definida para cada extensión SIP. Es importante que los usuarios no conozcan esta contraseña, para que no registren más de una extensión, lo que, no solo produciría conflictos en el envío y recepción de paquetes, sino problemas de uso de los teléfonos, que están configurados como fijos.

Según las condiciones de la empresa, cada empleado que trabaja permanentemente en oficina, tiene un computador fijo asignado, parte de los requerimientos era que, para ahorrar costos, en lugar de instalar teléfonos, se

[29] Usar solo números en una contraseña no es lo más seguro ni lo más aconsejable, sin embargo, es la única contraseña que puede aceptar un teléfono.

usen *softphones* en cada computadora, con lo que cada empleado podrá disponer fácilmente de su extensión, sin necesidad de recurrir a más aparataje en las oficinas. Esta solución, aunque es económica, presenta varios problemas en cuanto *drivers*, códecs y conexiones.

Si bien los *softphones*, el momento de que se realiza una llamada reservan memoria de procesamiento para asegurar que los paquetes sean transmitidos correctamente por la red, y recibidos por el otro usuario; los *drivers* de sonido de las computadoras, no siempre son compatibles para esta transmisión de datos en tiempo real, e incluso, los conectores de Auriculares no son compatibles con los auriculares; por lo que la compresión entre los códecs y el procesamiento de estos hace que las llamadas se oigan entrecortadas, con volumen bajo, o que se pierdan sin razón. Cabe recalcar que este tipo de problemas varían de PC a PC, ya que existen computadores donde estas transacciones se realizan sin conflictos, y las llamadas se realizan de manera exitosa en su totalidad.

Cada extensión SIP define las características especificadas en la tabla 3.4

Parámetro	**Definición**
allowguest=no	Deshabilita la recepción de llamadas desde terminales desconocidas ó anónimas.
allowoverlap=no	Deshabilita el *overlapping* de llamadas
bindport=5060	El puerto UDP por defecto que escuchara el servidor de Asterisk
bindaddr=0.0.0.0	Direcciones IP habilitadas para conectarse (0.0.0.0 habilita todas)
srvlookup=yes	Habilita el servidor DNS SRV para llamadas salientes, deshabilitarlo impediría llamadas SIP desde dominios de Internet
videosupport=yes	Habilita el servicio de Video llamada
language=es	Lenguaje por defecto de los sonidos utilizados por el canal
type=friend	Tipo de canal que reconocerá Asterisk, el mismo que le permite realizar y recibir llamadas.
host=dynamic	Dirección IP de cada Terminal
nat=yes	Activa la configuración NAT para la terminal

dmtfmode=RFC2833	Tipo de DMTF de la Terminal, el mismo de los teléfonos analógicos.
codecs=ulaw; h263; h263p	Codecs de Audio y video Habilitados para la terminal

Tabla 0.4 Características de las extensiones SIP habilitadas

3.5.1 CONFIGURACIÓN DE VOICEMAIL

El funcionamiento del sistema de Correo de Voz de SACMIS debe trabajar de manera diferente a como se esta acostumbrado, ya que la mayoría de trabajadores de SACMIS pasa la mayor parte del tiempo realizando trabajos de campo, por lo que no siempre van a tener la oportunidad de revisar su correo de voz desde su extensión telefónica, lo cual haría complicado el manejo de los mensajes, ya que no llegarían a su destinatario en el momento adecuado. Esta es la razón de que cada mensaje de voz que se almacene en el sistema, si su duración es mayor a 5 segundos[30] se almacene en el servidor y se lo envíe a través del cliente de Correo de Asterisk, que ha sido configurado para enviar automáticamente hacia los usuarios un mensaje de correo electrónico a la dirección de correo electrónico empresaria; notificando la recepción del mensaje. En este mensaje de correo se indica el número llamado, la hora y fecha de la llamada y, el número llamante. Asterisk maneja para el almacenamiento de estos mensajes el formato WAV, que puede ser leído en cualquier PC, incluso si no tuviera instalado más que lo básico para su funcionamiento. Además, cada usuario posee un buzón de correo de voz configurable en la central a la cual es posible acceder desde la extensión de cada usuario, y le permite modificar ciertos parámetros de la misma.

Los parámetros del funcionamiento del correo de voz de SACMIS quedan definidos por los parámetros de la tabla 3.5

[30] Se utiliza esta medida ya que comúnmente un mensaje más corto suele ser un mensaje fallido.

Parámetro	Definición
format=wav|gsm	El formato en que se guardaran los mensajes de voz, por defecto se almacenan en formato WAV
attach=yes	Le dice al sistema que en los e-mails, debe adjuntarse una copia de la grabación
maxlogins=3	El numero máximo de oportunidades de acceder que tiene el usuario
servermail=no-responder@SACMIS.com.ec	El servidor de correo para enviar los mensajes a los usuarios
maxmessage=180	Limita el valor máximo en tiempo de un mensaje de voz
minmessage=5	Limita el valor mínimo en tiempo de un mensaje de voz
maxmsg=50	Limita el numero de mensajes por casilla de voz que pueden existir
delete=yes	Especifica que se elimine el mensaje del buzón de correo una vez que ha sido enviado por correo electrónico
fromstring="PBX SACMIS"	Define la cabecera del Asunto de envío de correo
mailcmd=/usr/sbin/sendmail -v -t -f no-responder@sacmis.com.ec	La aplicación que se utilizara para enviar los correos electrónicos
maxsilence=2	Define el máximo tiempo de silencio para considerar el mensaje terminado
silencethreshold=128	Define el valor de sensibilidad del sonido para considerar los silencios
emailsubject=[PBX]: Tienes un nuevo mensaje en tu buzon SACMIS	Define el asunto con el cual el mensaje será enviado.
Estimado ${VM_NAME}:\n\nEl dia ${VM_DATE} recibiste una llamada de ${VM_CALLERID}, quien ha dejado un mensaje al tu no estar disponible. El mensaje de voz esta adjunto a este correo. Si necesitas hacer algún cambio en tu buzón ${VM_MAILBOX} siempre puedes llamar al *333. \nPara servirte. SACMIS PBX. \n"	Define el cuerpo del mensaje que será enviado, el cual contiene las variables necesarias para personalizar el mensaje correspondiente.
emaildateformat=%A, %d/%m/%Y a las %H:%M:%S	Define el formato de fecha del mensaje q será enviado.

Tabla 0.5 Características del buzón de correo de los usuarios.

3.6 SEGURIDADES DE SISTEMA LINUX

La principal seguridad que existe para los sistemas Linux, es que al muy pocas personas saber manejarlos, su uso se convierte en una especie de tabú, proporcionando seguridad de manera sociológica. Cabe recalcar que este miedo, con la cada vez más fuerte intrusión de las tecnologías de la comunicación, se va perdiendo.

Al usar el protocolo SIP para la implementación, y al tener el servidor conectado a Internet, para realización de pruebas de conectividad entre extensiones que se encuentren fuera de la empresa, este se vuelve un blanco para los atacantes. Así, al sistema se lo protege de dos formas, desde la configuración de Asterisk como tal, y a través del cortafuegos iptables.

Para evitar la infiltración de extensiones no autorizadas dentro del sistema, SIP proporciona en su configuración el rechazo del registro de estas comunicaciones anónimas. Sin embargo, los paquetes que puedan seguir llegando mientras se intenta comunicar con la central no se detendrán mientras la IP desde donde se envían sea bloqueada, por lo que es necesaria la configuración del cortafuegos, añadiéndole un pequeño programa de bloqueo conocido como fail2ban.

La configuración de *iptables* debe ser lo más restrictiva posible. En el caso de esta implementación, se habilitan los siguientes puertos:

- TCP 80.
- TCP 22.
- TCP 25.
- UDP 5060.
- UDP 10000:20000 (habilitados los puertos comprendidos entre estos extremos).

Y todos los restantes puertos se encuentran cerrados[31]. A esta configuración se le añade el uso de una contraseña de inicio de sesión robusta y larga, lo que hace que una intrusión SSH sea costosa y difícil.

Como no es posible bloquear IP's, ya que las extensiones pueden loguearse desde cualquier lugar mientras dispongan un cliente SIP y las credenciales necesarias para la autenticación, se necesita una forma de proteger al sistema de ataques de DoS. Para esto, se instaló en el servidor el software fail2ban. Este sistema se integra en el sistema operativo, y lo que hace es leer los registros del sistema de monitoreo (en este caso los registros de Asterisk), y si una dirección IP desconocida ha enviado un determinado número de mensajes infructuosos, en este caso de registro, procede a bloquear la IP añadiendo la regla de bloqueo en iptables de manera automática, lo que hace que dicha IP no pueda volverse a comunicar con el servidor. Este software es el que permite que el servidor pueda estar conectado a Internet, sin problemas, ya que siempre estará bloqueando IP's, mientras el servicio al cual ha sido añadido esté funcionando.

[31] Los puertos SSH (22) y HTTP (80) están abiertos con la finalidad de monitoreo remoto del sistema. Si no se va a realizar dicho monitoreo, es conveniente también cerrarlos.

Cuando se habla de seguridad informática y de comunicaciones, es inevitable pensar en complicados algoritmos de encripción, sistemas de autentificación basados en intercambio de información y contraseñas complicadísimas, sistemas de transferencias de datos con alta seguridad y control de flujo, enlaces dedicados para intercomunicación empresarial, y un muy largo etcétera, fruto de la búsqueda de mantener la información sensible protegida de ataques internos y externos, con mayor o menor éxito.

Sin embargo, todos estos intentos quedan en nada cuando la persona encargada de usar estos sistemas tiene la mala idea de compartir la contraseña de su usuario, por ser 'buena gente', o quedar bien con alguien más. Parte muy importante de estos sistemas es la componente humana, la cual, en conjunto con un sistema de datos, debe ser puesta a punto, para crear conciencia de seguridad más allá de tener un computador fuerte.

Este Capítulo presenta el diseño de Políticas de Seguridad para la red de SACMIS, enfocada en los dominios necesarios para el sistema, además de Políticas de uso del Sistema de Telefonía IP, ambos basados en las normas de la serie 27000, que además de enfocarse en el sistema de red como tal, se enfocan en el usuario, a la persona que, a fin de cuentas, es quien convivirá con el sistema.

CAPÍTULO 4
DISEÑO E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA EL SISTEMA DE RED Y TELEFONÍA, BASADOS EN LAS NORMAS DE LA SERIE 27000

4.1 DESARROLLO DE SGSI Y LA NORMA 27000

Como tal, la norma ISO 27000 existe desde 1995 cuando la BSI (British Standards Institution, o Institución Británica de Estándares) desarrolló la norma BS 7799, para facilitar la implementación de buenas prácticas en gestión de la seguridad de la información en empresas, sean estas británicas o no.

Esta norma se dividió en dos partes, la 7799-1 se centró en ser una guía de buenas prácticas, que no necesitaba de certificación, la cual fue revisada por la ISO y adoptada como la ISO 17799 en 1999.

La norma 7799-2 especificaba normas que podían ser certificables, haciendo que más de 1700 empresas se hayan certificado en esta norma hasta 2005, lo que provocó que la ISO la adoptara como la norma ISO 27001, además de revisar la 17799 y adoptarla como ISO 27002 en 2007, pero manteniendo la fecha de la revisión original. A partir de esta fecha ISO continúa revisando u adoptando nuevas normas a la serie 27000, sin embargo manteniendo la norma 27001 como la única certificable dentro de esta serie.

4.1.1 NORMAS QUE LA COMPONEN

La serie 27000 está compuesta por:

- ***ISO/IEC 27000***

Proporciona un resumen general de los componentes de la norma, además del compendio de términos que se usarán en el resto de normas posteriores y una

pequeña síntesis de los Sistemas de Gestión de Seguridad. Fue publicada en mayo de 2009.

- ***ISO/IEC 27001***

Se presenta como la norma principal de la serie y la única certificable. Contiene los requisitos para la implementación de un SGSI, los cuales están sujetos a auditoría, fue publicada en octubre de 2005.

Esta norma, para su certificación establece 11 dominios que engloban de una manera universal como la normativa de seguridad debe ser establecida. Estos dominios son:

- Políticas de seguridad
- Organización de la Seguridad de la Información
- Administración de los recursos
- Seguridad de Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de Comunicaciones y Operaciones
- Control de Accesos
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes de Seguridad de la Información.
- Gestión de Continuidad del Negocio.
- Cumplimiento

Todos englobados en un solo manual de políticas empresariales.

- ***ISO/IEC 27002***

Procede de la anulada ISO 17799:2005. Describe una guía de buenas prácticas con los objetivos de controles de seguridad recomendados. No es certificable y fue publicada en julio de 2007.

- ***ISO/IEC 27003***

Describe el proceso de implementación de un SGSI, desde el diseño hasta la puesta en marcha, especificando los puntos críticos dentro de esta implementación, además del proceso de obtención de aprobación por parte de la gerencia. Fue publicada en febrero de 2010 y no es certificable

- ***ISO/IEC 27004***

Determina las métricas necesarias para determinar la efectividad de un SGSI según 27001. Fue publicada en diciembre de 2009 y no es certificable.

- ***ISO/IEC 27005***

Proporciona parámetros para gestión de riesgo de seguridad de información y está diseñada para apoyar en la correcta aplicación de los estatutos de la seguridad de información basada en la misma gestión de riesgos. Fue publicada en junio de 2008 y no es certificable.

- ***ISO/IEC 27006***

Especifica los requisitos de la acreditación como auditor y para entidades de auditoría para la certificación de las normas de seguridad. Se basa en la norma EA-7/03, que presenta los requisitos de acreditación de entidades auditoras de SGSI. Sirve principalmente para interpretar los criterios de acreditación de 27001. Fue publicada en marzo de 2007.

- ***ISO/IEC 27007:***

Aún en fase de desarrollo. Presentará una guía de auditoría de SGSI, como complemento a la norma 19011.

- ***ISO/IEC 27008:***

Aún en fase de desarrollo. Presentará una guía de auditoría de controles en el marco de implantación de un SGSI.

- ***ISO/IEC 27010***

Aún en fase de desarrollo. Presentará una norma para la gestión de seguridad en comunicaciones inter-sectoriales.

- ***ISO/IEC 27011***

Especifica una guía de interpretación para la implementación de un SGSI dentro del sector de las telecomunicaciones. Fue publicada en diciembre de 2008.

- ***ISO/IEC 27012***

Aún en fase de desarrollo. Presentará un conjunto de requisitos complementarios a 27001 y 27002 enfocados a empresas de e-Administración.

- ***ISO/IEC 27013***

Aún en fase de desarrollo. Presentará una guía de implementación de 27001 y de 20000-1 (gestión de servicios TI).

- ***ISO/IEC 27014***

Aún en fase de desarrollo. Presentará una guía de gobierno corporativo de la seguridad de la información.

- ***ISO/IEC 27015***

Aún en fase de desarrollo, con publicación prevista en 2012. Consistirá en una guía de SGSI para organizaciones del sector financiero y de seguros.

- ***ISO/IEC 27031***

Aún en fase de desarrollo. Presentará una guía de continuidad de negocio en cuanto a TIC's.

- ***ISO/IEC 27032***

Aún en fase de desarrollo. Presentará una guía relativa a la ciberseguridad.

- ***ISO/IEC 27033***

Norma dedicada a la seguridad en redes, dividida en 7 partes:

- 27033-1, conceptos generales (publicada en Diciembre de 2009)
- 27033-2, directrices de diseño e implementación (aún en desarrollo)
- 27033-3, escenarios de redes de referencia (aún en desarrollo)
- 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways o pasarelas de seguridad (aún en desarrollo)
- 27033-5, aseguramiento de comunicaciones mediante VPN's (aún en desarrollo)
- 27033-6, convergencia IP (aún en desarrollo)
- 27033-7, redes inalámbricas (aún en desarrollo).

- ***ISO/IEC 27034***

Aún en fase de desarrollo. Presentará una guía de seguridad en aplicaciones informáticas.

- ***ISO/IEC 27035***

Aún en fase de desarrollo. Presentará una guía de gestión de incidentes de seguridad.

- ***ISO/IEC 27036***

Aún en fase de desarrollo. Presentará una guía de seguridad de externalización de servicios.

- ***ISO/IEC 27037***

Aún en fase de desarrollo. Presentará una guía de identificación, recopilación y preservación de evidencias digitales.

- ***ISO 27799***

Proporciona directrices para la interpretación de 27002 en el sector sanitario, en tanto datos de salud de pacientes. Al contrario del resto de la serie, esta norma no está desarrollada por el subcomité JTC1/SC27, sino el comité técnico TC 215. Fue publicada en junio de 2008.

Esta serie de normas, en mayor o menor medida están enfocadas a preservar la información de todo ataque interno y externo a través de un SGSI (Sistema de Gestión de Seguridad de Información), pero como en toda norma, se requiere saber que es específicamente la información, la cual está definida como:

"Conocimiento o datos que tienen valor para la organización"[32]

Esta información siempre estará sujeta a ataques, que se definen como:

"Intentos de destrucción, exposición, alteración, inhabilitación, robo, ganar acceso no autorizado o hacer uso no autorizado de la información"

Para prevenir estos ataques es que un SGSI, pilar fundamental y centro de la norma ISO 27000, se constituye.

4.1.2 SGSI

La seguridad de información siempre tendrá un margen de error, un pequeño porcentaje de falla, aun cuando se dispongan de recursos ilimitados y equipos súper potentes. De hecho, en seguridad de información, lo "único seguro es la muerte"[33]. La función de los sistemas de seguridad de información es la de gestionar los recursos existentes de tal manera que ese pequeño margen de error siempre existente se traduzca en un virtualmente improbable ataque hacia un sistema en concreto, mediante la concienciación de los riesgos de seguridad informática, la aceptación de los mismos y a través de este proceso, poder gestionar y minimizar su impacto con un sistema organizado, sistemático, documentado y adaptado a cualquier posible cambio que se dé en la organización.

---

[32] Conceptos extraídos de ISO/IEC 27000.

[33] Dr. Enrique Mafla. Teoría de Seguridad de Redes. Escuela Politécnica Nacional.

Como definición de seguridad, se establece que consiste en la preservación de cuatro cualidades de la información, que son:

- ***Confidencialidad***

La información debe permanecer secreta y no ser distribuida ni ser puesta a disposición de entes no autorizados.

- ***Integridad***

La información debe mantenerse completa, sin fraccionamientos, al igual que sus procesos.

- ***Disponibilidad***

La información, para los entes autorizados, debe estar siempre disponible en su totalidad.

- ***No Repudio***

También conocido como irrenunciabilidad, asegura el origen de la información y que esta no pueda ser negada por el remitente.

Estos términos son considerados como los pilares de la seguridad de la información, y para mantenerlos, se hace uso de procesos que estén sistematizados, documentados y conocidos por toda la organización, siempre tomando en cuenta los riesgos. A esto se conoce como SGSI.

Figura 0.1 Proceso de establecimiento de un SGSI [21]

4.1.3 ESTABLECIMIENTO DE UN SGSI:

Los pasos para establecer un SGSI se basan en los requerimientos del sistema, y son:

4.1.3.1 Plan (Planificar):

Establecer los requerimientos primarios del SGSI: Define el sistema de seguridad, el alcance, las prioridades, los objetivos y los riesgos de un SGSI, todo siempre de acuerdo a como la dirección haya establecido el desarrollo del sistema.

Durante esta fase, se define la metodología de evaluación de los riesgos existentes dentro de la organización, de tal manera que los resultados puedan ser comparables y repetibles, utilizando metodologías existentes, o desarrollando unas propias en base a los requerimientos.

El alcance debe establecer:

- Los objetivos de seguridad y el establecimiento general que deberá cumplir la seguridad en la organización
- Establezca los criterios de evaluación de la seguridad dentro de la organización.
- Identificar los activos y sistemas que formarían parte del SGSI y a sus responsables.
- En relación a los sistemas evaluados, identificar riesgos y vulnerabilidades.
- Analizar las posibilidades reales de que los riesgos se conviertan en amenazas y el impacto en caso de que una amenaza presente un fallo de seguridad.
- Evaluar el impacto de un fallo dentro del sistema y las formas de tratar con el mismo.

Para establecer estos pasos en una normativa diseñada para la aplicabilidad del SGSI, se deben utilizar los objetivos de Control del Anexo A de la norma 27001, y

en general, las buenas maneras estipuladas en la norma 27002, dejando en libertad a los aplicantes para modificar adicionalmente estos requisitos en caso no estén completamente acordes con la necesidad particular de la organización.

4.1.3.2 Do (Hacer)

Implementar y utilizar el SGSI: a partir del alcance establecido, se debe implementar el SGSI de acuerdo a ciertos parámetros definidos:

- Definir e implementar un plan de tratamiento y control de riesgos: a partir del alcance establecido, crear un plan en donde se especifique de una manera clara, los objetivos de control y su forma de implementación.
- Definir un sistema de métricas: al ser necesario que los resultados puedan ser medibles y repetibles, se necesita definir parámetros de evaluación de los resultados de la implementación para determinar su eficacia en el tiempo.
- Gestionar los recursos: para mantener el SGSI funcionando se deben revisar periódicamente los recursos a ser evaluados.
- Implantar controles: para dar una respuesta adecuada a cualquier filtración o ataque hacia el sistema gestionado, se establecen controles que están permanentemente en ejecución sobre el sistema.

4.1.3.3 Check (Verificar)

Mantener un monitoreo permanente del SGSI implementado: Una vez que el SGSI ha sido implementado, la organización está en la obligación de mantener un monitoreo permanente del SGSI, evaluando su actuación, considerando que:

- Se debe detectar errores en los resultados obtenidos en los tiempos adecuados, sin dejar pasar ningún detalle por alto, ya que sería motivo de una vulnerabilidad en el sistema de seguridad.
- Revisar infiltraciones, fallas de seguridad.
- Determinar si los recursos tecnológicos aportan a efectivizar la aplicación del sistema.

Además, se debe permanentemente revisar que tan efectivas fueron las políticas aplicadas y los controles de las mismas, dentro de intervalos de tiempo prudenciales, para comprobar que los objetivos planteados se están cumpliendo, y en caso de presentar alguna falla, estudiar los correctivos necesarios. La evaluación del riesgo, considerando los posibles cambios que se deban aplicar a las políticas y/o los cambios que se han realizado dentro de la infraestructura física o lógica del sistema también debe considerarse, específicamente después de cualquier cambio que sufra la red o la infraestructura social de la empresa. Cada cambio que se plantee, o que se realice debe estar plenamente documentado y registrado, especificando todos los detalles; esto permitirá, en caso de una falla, poder saber que sucedió y como remediarlo.

4.1.3.4 Act (Actuar)

Mejorar el SGSI de acuerdo a los resultados del monitoreo: Una vez que el sistema ha sido evaluado, y los cambios han sido establecidos, el sistema debe ser modificado de acuerdo a los parámetros que dio la experiencia de la implementación, siguiendo los pasos de la cláusula 8 de la norma 27001, y comunicando las actualizaciones a todas las esferas que existan dentro de la organización, para que el cambio sea asimilado de manera completa por cada uno de los miembros la que conforman.

Como se puede apreciar, una vez terminado el cuarto paso se vuelve a iniciar el ciclo de evaluación e implantación, ya que la seguridad es un ente en constante evolución que no debe quedar relegado u olvidado dentro de la organización una vez que ha sido implementado. Es responsabilidad de la dirección de la empresa, y de la rama encargada de la información mantener el SGSI en pleno funcionamiento, más que para cumplir con un estándar, para proteger el activo más importante de su organización: la información.

4.2 REQUERIMIENTOS DE SEGURIDAD DE LA IMPLEMENTACIÓN

Parte del trabajo de SACMIS, como proveedor de servicios de telecomunicaciones, es la completa documentación de los trabajos que se han realizado, no solo para la realización y presentación de informes a los clientes, sino también como respaldos de descargo en caso de existir algún inconveniente con el trabajo realizado. Toda esta información no es solo fotografías, sino además respaldos de configuraciones y calibraciones de los equipos con los que comúnmente se trabaja.

Esta información, para su salvaguardo, se almacena en el servidor de correo electrónico, que también cumple con la función de servidor de archivos y proxy de la red para el acceso a Internet. Sin embargo, esta información se almacena en una carpeta en la que el usuario puede almacenar la suya de la forma que él considere necesario, sin ningún estándar o forma establecida. Esta situación ha causado, más de una vez, la confusión y la pérdida de información importante, principalmente en momentos de apuro frente al cliente.

Aparte de la información técnica, en el servidor de archivos se almacenan la información correspondiente a ciertas actividades administrativas y gerenciales, software de uso común en las terminales de los trabajadores, e informes de proyectos, órdenes de trabajo y demás, propiedades de los administradores de proyectos. Es decir, el servidor de SACMIS es el corazón informático de la empresa, que se complementa con el servidor/estación de trabajo que maneja la contabilidad, la base de datos de inventario de bodega, que esta almacenada en la computadora de sistemas y el servidor de telefonía. Sin embargo, y a pesar de que la política de respaldos existe y se lleva a cabo semanalmente, no está completamente documentada y formalizada, lo que hace que no se lleve a cabo de una manera uniforme.

Los equipos con los que se realizan los trabajos de campo se han uniformizado de manera que todos llevan desde el mismo sistema operativo, hasta las mismas

configuraciones, programas y aplicativos. Esto se debe a que todas las portátiles de la empresa, incluso aquellas que están destinadas a un trabajo más bien administrativo[34] estén listas para ser utilizadas en el trabajo de campo por la persona a la que han sido asignados. Para el trabajo particular, las características propias de los PC's han sido de alguna manera suprimidos para dar paso a una estandarización de la herramienta de trabajo, la cual puedan utilizar todos los técnicos, sin desmedro de que sea, o no, la computadora a él asignado.

Para la realización del manual de políticas de seguridad, estos son los parámetros principales que se consideraran al momento de su realización, en base a los dominios que establece la norma 27001 para la creación de un manual de estas características. En función de estos dominios, se debe realizar un análisis de los recursos y vulnerabilidades del sistema como tal, para establecer los correctivos apropiados, y mejorar la seguridad de la red.

Además, y como se explicó en el capítulo precedente, el sistema físico de Telefonía está bastante bien protegido contra intrusiones externas, además de que el propio sistema, como la implementación realizada no es, en cierto sentido y bajo las circunstancias actuales, muy grande, proporciona su propio sistema de seguridad, encriptando las claves y proporcionando seguridad para el envío de mensajes, lo que deja el punto débil del sistema de Telefonía, en los usuarios y su forma de utilizarlo.

Cuando se trata de telefonía, las consideraciones de la seguridad son diferentes, ya que si las personas no han sido concienciadas en la importancia de la información que están produciendo y/o transmitiendo, no toman la suficiente conciencia de su importancia, principalmente por la falta de sensación de existencia física de la misma, ya que no está en papeles (que son archivados, protegidos y fotocopiados) o cintas magnéticas (donde se almacenaban conversaciones, que podían ser respaldadas y copiadas según sea necesario).

[34] En esta clasificación se excluye el portátil de ventas, la cual nunca ha sido considerada para ningún trabajo que no sea administrativo y contable.

Los requerimientos necesarios de seguridad de la empresa se enfocan principalmente en capacitar y concienciar a los usuarios, que los recursos con los que cuenta la empresa son una herramienta más de trabajo, y, así como existen protocolos de entrada, salida y protección de herramientas, la información que se utiliza para el trabajo diario de SACMIS, y el sistema de Telefonía son igual de útiles, y deben ser protegidos de la misma manera. Cada uno de los activos informáticos del sistema deben siempre ser vistos como una herramienta poderosa de comunicación y desarrollo, o una traba que hará perder activos a la empresa y mermará su desarrollo.

En ese sentido, el establecimiento de procesos, como tales, no se aplicaría de una manera directa en la implementación, sino más bien como un sistema de reglas en función de las vulnerabilidades que sean detectadas; asignando, eso sí, responsables del manejo del sistema de seguridad y una normativa de sanciones si se presentara el caso de un incumplimiento.

4.3 ANÁLISIS DE VULNERABILIDADES DE LA RED DE SACMIS EN FUNCIÓN DE LOS ACTIVOS A ANALIZAR

Los parámetros que van a ser evaluados dentro de SACMIS, están siempre más enfocados en la protección de los intangibles antes que de los equipos como tales. Esto sin embargo no quita que los parámetros de seguridad que vayan a ser establecidos definan también la protección para los equipos físicos, como portátiles y estaciones de trabajo.

Para el establecimiento de las políticas de seguridad, antes se debe evaluar cuáles son las posibles vulnerabilidades que pueden sufrir los activos como tales, tanto físicas como lógicas, y de esta manera decidir si los riesgos que estas toman, pueden ser aceptados (si su existencia no incurre en una brecha de seguridad) o reducidos (si su existencia representa una brecha de seguridad significativa).

A partir de los criterios descritos a continuación, y de los apartados considerados de la norma 27001[35]; se establecerán las políticas necesarias para proteger la red, su información y a los usuarios de telefonía de un posible ataque interno o externo.

4.3.1 ESCALA DE VALORACIÓN DE VULNERABILIDADES

Activos de Información (Confidencialidad)	Clase	Descripción
1	Público	Toda información que puede ser proporcionada a terceros, sean estos clientes o entes de control, y que no afectara el correcto desempeño de las funciones
2	Uso interno no-confidencial	Toda información que puede circular por el interior de la empresa sin que terceros tengan contacto con él. Su distribución a terceros puede ser causa de brechas de seguridad importantes
3	Uso interno confidencial	Toda información que solo puede ser distribuida entre entes autorizados y específicos. Su distribución sin autorización explícita puede ser causa de brechas de seguridad importarte.

Tabla 0.1 Escala de valoración para Confidencialidad

[35] Referidas en el anexo K.

Activos de Información (Integridad)	Clase	Descripción
1	No necesaria	Contenido de solo-lectura, para consultas y descripciones.
2	Necesaria	Si el contenido fuera alterado o modificado, puede incurrirse en brechas de seguridad importante.
3	Imperativa	Si el contenido fuera alterado o modificado, el riesgo para la continuidad del negocio y las operaciones sería muy alto.

Tabla 0.2 Escala de valoración para Integridad.

Activos de Información (Disponibilidad)	Clase	Descripción
1	Bajo	Si la información no llegara a estar disponible, la continuidad del negocio no se vería afectada.
2	Mediano	Si la información no llegara a estar disponible, podría producir retrasos y fallas en la continuidad del negocio, pero sin consecuencias fatales
3	Alto	Si la información no llegara a estar disponible, la continuidad del negocio se vería completamente afectada.

Tabla 0.3 Escala de valoración para Disponibilidad

Activos de Información (No-Repudio)	Clase	Descripción
1	Verificado	Toda la información verificada en su envío y recepción se puede considerar confiable para el desarrollo de las actividades.
2	No Verificado	Si la información no puede ser verificada en su remitente, su contenido no puede considerarse seguro, y su utilización puede ser fuente de brechas de seguridad importante.

Tabla 0.4 Escala de valoración para no-repudio.

Además, la frecuencia temporal de ocurrencia de los eventos también presenta una escala de valoración para amenazas y vulnerabilidades.

Vulnerabilidades (probabilidades)	Clase	Descripción
1	Bajo	La seguridad de los sistemas no son los adecuados, por lo que la vulnerabilidad puede ser explotada
2	Medio	La seguridad no es precisamente la adecuada, pro existen controles de seguridad para evitar la explotación de la vulnerabilidad
3	Alto	La seguridad está establecida y documentada, la explotación de la vulnerabilidad es improbable

Tabla 0.5 Escala de valoración de vulnerabilidades

Amenazas (probabilidades)	Clase	Descripción
1	Bajo	La probabilidad de ocurrencia de un evento es muy baja o muy lejana en el tiempo
2	Medio	La probabilidad de ocurrencia de un evento es moderada, y de igual manera en tiempo
3	Alto	La probabilidad de ocurrencia del evento es alta, o sucede con mucha frecuencia.

Tabla 0.6 Escala de valoración de amenazas

4.3.2 IDENTIFICACIÓN DE ACTIVOS

De acuerdo al estudio de los requerimientos podemos darnos cuenta, que existen dos grupos mayoritarios de activos que serán evaluados, estos son los computadores portátiles del trabajo de campo, los servidores y los equipos de soporte electrónico de los mismos en un grupo, que además incluye software[36] y el sistema de comunicaciones (conexión a internet, telefonía) por un lado, y la información producida por los usuarios en función del uso de los activos físicos y de los trabajos realizados por otro. Cada uno será considerado de modo diferente, ya que, por ejemplo en el sistema de comunicaciones, se debe asegurar la conexión al servidor central, mientras que en la telefonía, el cómo los usuarios deben utilizarla.

4.3.3 IDENTIFICACIÓN DE REQUERIMIENTOS

A partir del reconocimiento de los activos y de la definición de vulnerabilidades, se establecen los siguientes requerimientos:

[36] La mayoría del software usado por los computadores es dado por los propios clientes para los trabajos requeridos. El resto son software no-licenciados, que en este momento no serán contemplados para la creación de las políticas, sin embargo, si la ocasión lo requiriera, serán considerados en un próximo estudio.

- La información que se produce en los trabajos que realiza la empresa no podrá ser divulgada a menos que haya sido previamente revisada y que se haya aprobado su distribución.
- Los equipos de computación portátiles están sujetos a muchos riesgos, ya que por necesidad no pueden estar en un lugar fijo; se debe siempre tener en cuenta la protección de la información que estos contienen debe estar respaldada y protegida, y que los equipos no deben separarse de las personas a las que han sido asignadas.
- Los equipos que dan servicios para la empresa deben cumplir todas las normas de protección física y lógica, y deben ser protegidos ante cualquier tipo de eventualidad.
- Los servicios de administración de archivos, correo electrónico y telefonía deben estar disponibles todo el tiempo para el uso de los empleados.
- Cualquier cambio, de hardware o software a los equipos informáticos solo lo realizara el personal autorizado previa aprobación de la comisión de seguridad de la empresa.
- Los empleados, en el momento de su ingreso a la empresa, conjuntamente con su contrato, recibirán el manual de seguridad de la empresa para que puedan leerlo y asimilarlo, y en el momento de firmar el contrato, aceptan implícitamente conocer sus contenidos y comprometerse a cumplirlos en la manera en la que la empresa lo requiera.
- Todos los empleados de la empresa deben estar conscientes de la necesidad de mantener los sistemas resguardados, y de su total co-responsabilidad en el mantenimiento de la seguridad de la información.

4.3.4 VALORACIÓN DE LOS ACTIVOS

Cada uno de los activos descritos necesitan ser valorados en función del impacto que sufriría el correcto funcionamiento de las operaciones si alguno de los mismos fallara. En función de su valoración se determinara cuales son los activos sin los cuales es imposible mantener la continuidad del negocio, o cuales

mantienen actividad aunque presenten pérdidas en el correcto desenvolvimiento de las actividades.

La tablas 4.7 y 4.8 definen la valoración de cada uno de los activos en función de la escala de valoración de cada posible vulnerabilidad. Cabe recalcar que no se puede aplicar la misma valoración a los equipos físicos que a los intangibles, por lo que se los valora por separado.

Activo	Definición de vulnerabilidad	Valoración de vulnerabilidad	Descripción
Computadores Portátiles	Confidencialidad	3	La información contenida y producida por el PC debe ser solo vista y modificada por el personal autorizado.
	Integridad	3	La información debe ser mantenida integra y sin modificaciones.
	Disponibilidad	2	LA información almacenada en los PC's portátiles debe ser de fácil acceso al personal, sin embargo, no es imperativo acceder desde el mismo si se puede acceder desde el servidor de archivos.
Computadores de Escritorio	Confidencialidad	3	La información contenida y producida por el PC debe ser solo vista y modificada por el personal autorizado.
	Integridad	3	La información debe ser mantenida integra, completa y sin modificaciones.
	Disponibilidad	3	La información debe estar disponible en todo momento para el personal que necesite acceder a ella.
Servidores	Confidencialidad	3	La información contenida y producida por el PC debe ser solo vista y modificada por el personal autorizado.

	Integridad	3	La información debe ser mantenida integra, completa y sin modificaciones.
	Disponibilidad	3	La información debe estar disponible en todo momento para el personal que necesite acceder a ella.
Herramientas y suministros	Confidencialidad	2	El uso de las herramientas será de conocimiento interno empresarial, no debe ser compartida con personal externo.
	Integridad	2	Se debe procurar que las herramientas estén en perfecto estado para su utilización
	Disponibilidad	3	Cada una de las herramientas y suministros deben estar disponibles para todos en todo momento.

Tabla 0.7 Valoración de activos físicos.

La diferencia principal entre los activos físicos y los intangibles, es que la información es directamente sujeta al valor de no-repudio, cosa que no puede ser aplicada a los PC's o Servidores.

Activo	**Definición de vulnerabilidad**	**Valoración de vulnerabilidad**	**Descripción**
Documentación y Registros	Confidencialidad.	3	Los registros de funcionamiento y actas deben permanecer confidenciales para todo personal no autorizado
	Integridad	3	Cada registro debe ser almacenado de tal manera que no pueda ser modificado por nadie.
	Disponibilidad	2	No es imperativo que los registros estén disponibles todo el tiempo.

	No-Repudio	1	Cada registro debe tener una validación de quien lo ingreso y proceso.
Información técnica y de proyectos	Confidencialidad.	2	La información que corresponde a los trabajos de la empresa debe ser conocida por todas las partes, pero protegida de cualquier filtración externa
	Integridad	3	La información no debe ser manipulada o modificada en ningún momento, como respaldo.
	Disponibilidad	3	La información técnica debe estar disponible en todo momento para su consulta y revisión.
	No-Repudio	1	Toda la información tiene que estar asegurada por su generador, para evitar inconvenientes.
Servicios de comunicaciones (Internet)	Confidencialidad	3	Se debe proteger los accesos de internet para que no sean bloqueados o eliminados.
	Integridad	3	Se debe comprobar que la información transmitida o recibida no posea modificaciones o pérdidas.
	Disponibilidad	3	Los servicios de comunicación deben estar disponibles en todo momento.
	No-Repudio	1	La información recibida debe ser verificada y autenticada siempre.

Servicios de comunicaciones (telefonía)	Confidencialidad.	2	Se debe proteger el acceso telefónico para que no sea intervenido y no se produzcan escuchas no autorizadas.
	Integridad	2	No se puede regular por completo la integridad de la información, pero se debe mantener un estándar de utilización del sistema para minimizar fallos.
	Disponibilidad	3	El sistema telefónico de la empresa debe estar disponible en todo momento
	No-Repudio	2	No se puede verificar completamente la información recibida, se debe mantener un estándar de utilización del sistema para minimizar fallos.
Servicios de Correo Electrónico	Confidencialidad.	3	Los correos electrónicos no pueden ser distribuidos a entes no autorizados, so pena de sanción.
	Integridad	3	El sistema de correo electrónico debe mantener la información de cada mensaje sin alterar su contenido.
	Disponibilidad	3	Los mensajes de correo electrónico, así como el acceso al servicio deben estar todo el tiempo disponibles para su utilización.

	No-Repudio	1	Cada mensaje de correo electrónico debe ir con una firma autorizada del remitente, con la que se hace responsable por el mensaje enviado.

Tabla 0.8 Valoración de activos intangibles.

4.3.5 IDENTIFICACIÓN DE RIESGOS EN FUNCIÓN DE LOS ACTIVOS

Los activos siempre serán susceptibles de sufrir ataques, por lo que es parte del SGSI determinar las posibles amenazas que pueden sufrir cada uno de los mismos, para comprobar si estos riesgos se pueden convertir en amenazas para el la red y sus componentes. La tabla 4.9 presenta un resumen de los posibles riesgos a los que están expuestos los activos del sistema.

Riesgo	Amenazas	Afectación	Activos
Desastres Naturales	Inundaciones Incendios Terremotos	Funcionamiento de servidores Acceso a los sistemas de información.	Servidores Computadoras de Oficina Sistemas de información Sistemas de Correo Electrónico
Fallos no humanos	Fallas de suministro eléctrico Fallas de acceso al proveedor de Internet Avería de equipo de trabajo informático. Degradación de Cableado Empresarial.	Funcionamiento de servidores Acceso a los sistemas de información. Uso de computadores portátiles y de escritorio Conexiones a la red empresarial	Servidores Computadoras de Oficina Computadores Portátiles Sistemas de información Sistemas de Correo Electrónico

Fallos humanos no intencionados	Robo de equipos Perdida de equipos Caídas y/o golpes a los equipos Fallas de administración. Daño de dispositivos de almacenamiento Desconocimiento de la normativa vigente Fallas de configuración no contempladas. Virus de computadora.	Uso de computadores portátiles Acceso a los sistemas de información Mal uso de los recursos de comunicación	Computadores Portátiles Sistemas de información Sistemas de Correo Electrónico
Ataques intencionados	Ataques de fuerza bruta y de diccionario al servidor de correo electrónico. Ataques de fuerza bruta al servidor de telefonía. Instalación no autorizada de SW en computadoras de trabajo Suplantación de identidades de usuario. Accesos no autorizados a información sensible Ataques de ingeniería social	Disponibilidad de servicios de comunicaciones Uso de recursos informáticos Cumplimiento de normas de seguridad Identificación de usuarios Acceso a los sistemas de información Mal uso de los recursos de comunicación	Servidores Computadoras de Oficina Computadores Portátiles Sistemas de información Sistemas de Correo Electrónico Infraestructura de comunicación Registros y documentación

Tabla 0.9 Identificación de riesgos para la red.

A partir de estas consideraciones se convino en determinar que todos los riesgos presentados durante la identificación de requerimientos pueden ser reducidos, por lo que de esa forma será diseñado el manual de seguridades.

4.3.6 IDENTIFICACIÓN DE RESPONSABLES

Las responsabilidades de administrar y gestionar el manual de seguridad, aplicarlo, evaluar sus resultados, y establecer los permisos y sanciones necesarias recae directamente en la gerencia técnica de la empresa; compuesta por el Gerente General, el Gerente Técnico, el encargado del área de Sistemas y el encargado de Recursos Humanos, donde:

- El Gerente General y el Gerente Técnico son los responsables de dar el soporte administrativo a las políticas de seguridad y de ejecutoriar las sanciones pertinentes en caso de estas presentarse. Además, al estar más en contacto con los trabajos realizados, definirán como las políticas se aplicaran de mejor manera a los empleados.

- El encargado del área de Sistemas se encarga de revisar continuamente todos los incidentes que puedan producirse con los equipos informáticos, servidores, o software, gestionar los permisos necesarios de uso de los sistemas, evaluar los resultados y presentar las medidas pertinentes tomadas de estos.

- El encargado del área de Recursos Humanos se encargara de gestionar la forma de que todos los empleados estén siempre al corriente del manual de seguridad de la empresa, las obligaciones para con el manual y se encargara de gestionar todos los compromisos de confidencialidad correspondientes al trabajo que se realiza en la empresa.

4.4 SISTEMA DE GESTIÓN DE SEGURIDAD, MANUAL DE PROCEDIMIENTO Y POLÍTICAS DE SEGURIDAD PARA SACMIS CÍA. LTDA.

El sistema de seguridad que será implementado en SACMIS se define mediante un pequeño manual de procedimientos que incluye un análisis general de los

dominios de la norma, aplicados directamente a los activos que serán representados, además del manual de políticas de seguridad que se aplicaran a la red y que es el que, finalmente será llevado hacia el usuario.

Como un punto aparte, se tomara la seguridad de telefonía, directamente enfocada al usuario y a las políticas que debe mantener al momento de usar la red telefónica. El manual de procedimientos también incluye a estas políticas, pero se las considera por separado debido al enfoque.

4.4.1 MANUAL DE PROCEDIMIENTOS DE IMPLEMENTACIÓN DEL SGSI.

4.4.1.1 Políticas de seguridad

Las políticas definidas a continuación se fundamentan en la búsqueda de la protección de la información, activo importante en el desarrollo integral de SACMIS, por lo que su desarrollo va más allá de cumplir un requerimiento o mantenerse a la vanguardia dentro del mercado. Su objetivo principal es crear una cultura organizacional de seguridad entre los componentes de la empresa, para que la seguridad deje de ser una carga, y se transforme en la cotidianidad del trabajo, sea cual sea este el campo de aplicación.

4.4.1.1.1 Objetivo

Determinar la mejor forma de concienciación de usuario de la red de SACMIS, para que este pueda proteger la información que produce y transporta, de amenazas, sean estas internas o externas que puedan presentarse, y convertir a estas en improbabilidades mediante un adecuado sistema de seguridad que venga directamente desde el usuario en forma de una cultura de seguridad.

4.4.1.2 Organización de la Seguridad de la Información

Para garantizar la evaluación y el cumplimiento, a más de la creación de una plantilla de políticas de seguridad, es necesario que desde los mandos superiores de la empresa exista el compromiso de su aplicación y cumplimiento, para que las políticas puedan ser asimiladas de mejor manera, y así mismo, asegure el cumplimiento de las sanciones en caso de que alguna de las normas sea irrespetada.

4.4.1.2.1 Objetivo

Designar y conformar un comité de seguridad que organice, administre, ejecute y evalúe las políticas de seguridad para la empresa, manteniéndolas siempre actualizadas, y designando tiempos de evaluación y sanciones correspondientes en caso que sea necesario.

4.4.1.3 Administración de los recursos

Para la correcta aplicación de una política de seguridad, es imperativo que las organizaciones sepan a ciencia cierta cuáles son sus activos y como proteger los mismos ante cualquier ataque o vulnerabilidad, además de que se ubiquen a cada activo de acuerdo a sus características y aplicabilidad.

4.4.1.3.1 Objetivo

Administrar de manera eficiente cada uno de los activos considerados dentro del análisis de creación de políticas de seguridad, asignándole a cada uno de ellos un nivel de protección apropiado y eficiente de manera que enfrente las vulnerabilidades de manera adecuada.

4.4.1.4 Seguridad de Recursos Humanos

La gestión de seguridad no puede ser aplicada si no se ha concienciado a los usuarios de la red en cómo esta debe ser utilizada y protegida. Todo el personal que conforma la empresa debe tener claro el cómo se debe proteger la red, y la información que circula a través de la misma.

4.4.1.4.1 Objetivo

Minimizar los riesgos que puedan ser producidos por el mal uso de los activos de la red por parte de los usuarios; y establecer compromisos de utilización y confidencialidad de trabajo y divulgación para que los usuarios conozcan todos sus derechos y responsabilidades para con la red y la información en ella contenida.

4.4.1.5 Seguridad Física y Ambiental

Si bien, en un sentido técnico, la información es un intangible, es en espacios físicos en donde esta se almacena y por donde se propaga. El factor ambiental es de vital importancia, porque evitando accesos no autorizados a aéreas sensibles es como, también, se protege la información y la red por sí misma.

4.4.1.5.1 Objetivo

Reducir los riesgos producidos por accesos no autorizados y daños a los sistemas físicos de la empresa que contienen la información y sus medios de transporte. Asignar a cada área sensible sus propias políticas de acceso y limitaciones de manipulación, asignando a cada una de estas un responsable que debe encargarse de mantener estos sitios y facilidades en óptimas condiciones operativas.

4.4.1.6 Gestión de Comunicaciones y Operaciones

Muchas amenazas no solo provienen del mal uso del sistema por parte de los usuarios, sino también de virus, y programas infiltradores que son una amenaza presente e importante, por lo que es imperativo mantener un control acerca de los sistemas de comunicaciones que utiliza la empresa.

4.4.1.6.1 Objetivo

Gestionar de manera adecuada y constante los usos que se les da a los sistemas de comunicaciones y los niveles de permisos y privilegios que deben ser asignados a los empleados para el desarrollo de su trabajo.

4.4.1.7 Control de Accesos

El acceso a los sistemas de SACMIS no debe ser tomado a la ligera, ya que parte de la seguridad de la red implica que el acceso a los servicios de la misma no sea de uso común, sino que tenga las restricciones necesarias para que toda la información contenida en los sistemas y servicios pueda ser protegida; además de que se establezcan responsables del uso de la red en función de los permisos de acceso que tenga cada usuario.

4.4.1.7.1 Objetivo

Impedir accesos no autorizados a los servicios de la red y sistemas de información además de implementar seguridad de accesos y control en los mismos, estableciendo jerarquías de utilización y manteniendo registros de acceso a la red por parte de los usuarios y empleados.

4.4.1.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Los aplicativos de software son sobre los que comúnmente se asienta la información, en forma de bases de datos, gestionadores de archivos y

plataformas de datos, por lo que su uso, implementación y modificación deben estar correctamente gestionados, ya que una mala implementación, o actualización puede hacer peligrar el sistema como tal, con todos los riesgos que esto conlleva.

4.4.1.8.1 Objetivo

Definir los procedimientos de implementación, creación, modificación y eliminación de aplicativos de información, asegurando la integridad de su aplicabilidad y la información a la que este sistema sirve de plataforma; asimismo como los permisos de implementación, creación, modificación y eliminación de aplicativos de información con los que cuenta cada usuario de la red, y las asignaciones correspondientes de responsabilidad en la modificación de sistemas críticos, o programas vitales para la empresa.

4.4.1.9 Gestión de Incidentes de Seguridad de la Información

A pesar de todas las medidas que pudieran tomarse para salvaguardar la seguridad de la información, ningún sistema es lo suficientemente seguro para considerarse libre de eventualidades que comprometan su seguridad y funcionamiento, por lo que tener un sistema de gestión de eventualidades se torna indispensable.

4.4.1.9.1 Objetivo

Generar procedimientos de contingencia en caso de producirse una vulneración a la red o al sistema de información, y documentar cada falla que pueda presentar el sistema de manera que esta pueda ser solventada de manera adecuada y en el menor tiempo posible, según sea determinado por el comité regulador de seguridad.

4.4.1.10 Gestión de Continuidad del Negocio

Cuando se crean procedimientos para solventar cualquier ataque que pueda sufrir la red, es importante también determinar como el trabajo que se estaba realizando continúe en operación sin importar cuán fuerte haya sido el ataque, o cuanto se pueda tardar la recuperación del sistema, siendo la gestión de continuidad del negocio una parte importante a ser considerada.

4.4.1.10.1 Objetivo

Determinar las consecuencias que se podrían producir si la red o el sistema de información sufren un ataque y las maneras en que el sistema de información puede mantenerse funcionando a pesar del ataque, implementando planes de contingencia para restaurar los servicios en el menor tiempo posible.

4.4.1.11 Cumplimiento

Todos los controles que puedan surgir del desarrollo de los objetivos presentados previamente deben tener un sustento legal dentro de la empresa y que no entre en conflicto con la normativa legal ecuatoriana. Cada uno de los usuarios de la red, incluyendo al comité de seguridad deben esta consientes que esta normativa está por encima de cada autoridad, y que su aplicabilidad está por sobre un cargo o gerencia.

4.4.1.11.1 Objetivo

Cumplir y hacer cumplir con la normativa de seguridad diseñada para la empresa, garantizando que todos los entes pertenecientes a la misma sepan de su existencia y se comprometan en su cumplimiento, considerando está a la altura de una norma constitutiva de la empresa.

4.4.2 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.4.2.1 Alcance

Estas políticas se aplicaran a todos los componentes de la empresa y en todos los ámbitos en que los activos determinados sean utilizados dentro del trabajo habitual de la empresa. Con estas políticas se busca brindar instrucciones específicas sobre como la red debe ser utilizada y protegida por parte de los usuarios.

Además, brindará las herramientas necesarias para aplicar sanciones, en caso sea necesario, si algún componente de la empresa incurre en alguna falta que violente a las políticas aquí mencionadas.

4.4.2.1.1 Consideraciones Generales

- Estas políticas se aplicaran a todos los miembros corporativos que pertenezcan a SACMIS Cía. Ltda. Sin excepción, siendo todos sancionables sin importar el cargo que ostenten.
- El comité de Seguridad es el responsables del mantenimiento de la seguridad del sistema, y cualquier cambio o modificación de los permisos adquiridos por defecto, será una decisión del mismo.
- Los nuevos empleados, serán informados de estas políticas de seguridad y, en el momento que firman su contrato, aceptan explícitamente tener conocimiento de las mismas y aceptar las sanciones que puedan proceder de un mal uso del sistema.
- Estas políticas serán revisadas cada 3 meses por parte del Comité de Seguridad, tiempo en el cual las políticas y manual de procedimientos permanecerán en constante evaluación, para buscar mejores formas para mantener la seguridad del sistema.

4.4.2.1.2 Del acceso al servidor y correo electrónico

- Cuando un empleado es contratado, al momento de crear su cuenta de correo electrónico empresarial, se creara también una carpeta dentro del servidor de archivos, a la cual el usuario puede acceder con sus mismos usuario y contraseña de correo electrónico.
- La contraseña asignada en la creación de la cuenta de correo electrónico solo podrá ser usada una vez y deberá ser cambiada inmediatamente por el usuario.
- La contraseña de usuario deberá tener las siguientes características:
  - Tener de 6 a 10 caracteres.
  - Deberá contener letras mayúsculas y minúsculas, además de números y caracteres especiales.
- Las contraseñas de cada usuario son personales e intransferibles, y su divulgación incurre en una falta grave de seguridad.
- Las contraseñas deberán ser cambiadas obligatoriamente cada 30 días, y la nueva contraseña no podrá ser igual a las tres anteriores contraseñas utilizadas.
- La carpeta de archivos personal del empleado solo deberá contener información relativa a la actividad empresarial, y no podrá contener información personal o de características que atenten contra la moral. El comité de seguridad tiene potestad de realizar revisiones de esta información cuando lo considere oportuno.
- Si se detecta que la carpeta personal no es utilizada para los fines que fue creada, se procederá a una amonestación por escrito y a la solicitud de la eliminación de todo el material que incurra en la falta. De reincidir, el comité decidirá la amonestación y eliminara la información en cuestión sin informarle al usuario.
- El correo electrónico empresarial es un bien de la empresa, y su uso está restringido solo a actividades laborales propias del desenvolvimiento del usuario, y no puede ser usado para fines personales.

- La firma del correo electrónico deberá ser estandarizada para todos los miembros de la organización y deberá contener una cláusula de confidencialidad de transmisión de correo electrónico empresarial.
- La distribución de material confidencial a través del correo electrónico empresarial, o en su defecto, su mal uso para el envío de spam o mensajes de índole similar será considerado una falta grave a ser sancionada.
- En tanto no atente contra la privacidad del usuario, el comité de seguridad podrá revisar el uso que se le está dando al correo electrónico empresarial, y en caso de encontrar algún problema, tomara los correctivos necesarios.
- El acceso al servidor solo se realizara desde la red cableada de la empresa, a través de los puntos que están disponibles, o en su defecto, desde un cliente seguro aprobado por el comité de seguridad.
- Los archivos generados por el almacenamiento de correo electrónico deberán ser almacenados en un lugar distinto al que asigna el programa por defecto, de preferencia en una partición diferente y resguardada, para facilitar las labores de respaldo y de recuperación de archivos en caso de un daño catastrófico del sistema.

4.4.2.1.3 Del manejo de la información empresarial

- El jefe de grupo está obligado a reunir toda la información procedente del trabajo de campo en su carpeta personal en el Servidor de Archivos de la empresa.
- El resto de integrantes del grupo, tienen asimismo la obligación de almacenar respaldos, y/o sobrantes de la información extraída en sus respectivas carpetas personales, con un pequeño reporte de que información se está almacenando. Este reporte ira en sus carpetas, para su propia facilidad.
- Cada colaborador deberá tener obligatoriamente un dispositivo de almacenamiento masivo auto-extraíble de al menos 4 [GB] para su uso empresarial. Si el usuario no dispone de este implemento, la empresa debe gestionar su compra, y monitorear su uso.
- Hasta que no se facture un trabajo realizado, los miembros del grupo deberán tenerla información del mismo siempre disponibles en sus dispositivos de

almacenamiento. Cuando el trabajo haya finalizado, esta información será archivada en el Servidor, y Borrada de los Dispositivos.

- El PM debe conocer el itinerario de trabajo de sus colaboradores, la ruta de instalación o revisión y siempre tener a la mano las fechas de los mismos, para evitar contratiempos en la presentación de informes.

4.4.2.1.4 Del manejo de la información en el servidor

- La información será almacenada en las carpetas de cada usuario utilizando el siguiente formato:

  \usuario_de_correo\PM\trabajo_global\fecha\estación.

  En caso de ser un trabajo de E1's o de otro trabajo que requiera almacenamiento de información por rutas, se almacenara con el siguiente formato:

  \usuario_de_correo\PM\trabajo_global\fecha\ruta\estación.

  Ejemplo:

  \dmaldonado\acuzco\E1's 2G Telefonica\260911\Maizal\Maizal

- El dueño de la carpeta tendrá permisos de lectura/escritura y su acceso será registrado por el comité de seguridad.
- El resto de usuarios tendrá permisos de solo lectura sobre la carpeta de un usuario, por motivos de consulta de la información para la realización de informes y demás trabajos relacionados. Los otros usuarios no podrán realizar ninguna modificación a la información de un usuario en particular. Si se presentara el caso, se incurriría en una falta grave que es motivo de sanción.
- Si fuera necesaria la conexión remota hacia el servidor, se realizara a través de un cliente de transmisión seguro, para evitar escuchas no autorizadas.

4.4.2.1.5 De los respaldos

- Los respaldos se clasificaran por semanales y mensuales, siendo esta clasificación considerada en función de la vulnerabilidad de la información.
- Los respaldos serán almacenados fuera del servidor de archivos, en unidades de almacenamiento masivo auto-soportados, que puedan ser soportados y a cuyo acceso se pueda desde cualquier facilidad informática.
- La información que debe respaldarse es:
  - Información de correo electrónico de los usuarios del sistema.
  - Información personal correspondiente a las actividades de la empresa.
  - Información correspondiente a los movimientos contables realizados.
  - Información correspondiente a los movimientos administrativos realizados.
  - Información contenida en el servidor de archivos de los trabajos realizados.
- Los respaldos se realizaran de acuerdo a un horario establecido por el comité y que debe ser acatado por los usuarios de la red.
- Si el caso lo ameritara, a la información respaldada solo se puede acceder con un permiso escrito del comité de seguridad y bajo la supervisión del encargado del área de sistemas.

4.4.2.1.6 De los permisos de Internet

- Para precautelar la seguridad interna de la red[37] todos los dominios, con excepción de los bancarios, estatales y de entidades educativas están bloqueados, solo se puede hacer uso del correo empresarial y de un cliente Skype™ para comunicaciones.
- El uso de Skype™ está reglamentado por la empresa, al ser necesario para la comunicación directa con los clientes. Sin embargo, su mal uso también será sujeto de revisión y de sanción.
- Si se requirieran permisos especiales de acceso a Internet, se debe hacer una solicitud por escrito al encargado del área de Sistemas, el cual, en conjunto

[37] En función de experiencias previas de uso de la red, el dejar habilitados ciertos dominios de internet se convirtió en la causa más probable de infección de virus durante un periodo de trabajo de la red, por lo que se tomó esta decisión.

con el comité de seguridad evaluaran la petición y la aprobaran o denegaran según el caso.

- Cualquier acceso no autorizado a Internet por parte de los usuarios de la red, ser verificada, y si ameritara el caso, se establecerían las sanciones correspondientes.

4.4.2.1.7 De las conexiones externas

- SACMIS, como política de trabajo, no ha contemplado el manejo de conexiones remotas hacia el servidor como un método de trabajo, sin embargo, en ocasiones se ha presentado la necesidad se ha tenido que realizar la conexión.
- Para la conexión remota con el servidor de archivos SACMIS probara y proporcionara un cliente de conexión y transferencia que sea seguro y que pueda realizar la conexión evitando escuchas no autorizadas o accesos restringidos.
- De la misma manera, todo acceso externo será registrado y será controlado su uso, para evitar una fuga de información.

4.4.2.1.8 Del control de las facilidades físicas

- El ingreso al cuarto de equipos solo se realizara por personal autorizado, en caso de alguien necesitar acceso, se realizara con un permiso escrito y con la supervisión del encargado del departamento de Sistemas.
- para realizar cualquier modificación al sistema de cableado estructurado se requerirá un permiso especial detallando cual va a ser el arreglo a realizarse y el tiempo de duración del mismo.
- Cada equipo que conforma el pull de servidores y equipos de red de la empresa deberá tener su respaldo de energía en caso existiera un corte de la misma, para mantener funcionando los servidores, y poder apagarlos de manera apropiada sin que se pierda información al hacerlo.

4.4.2.1.9 Del control de equipos de computación

- Los usuarios son responsables del equipo informático a ellos asignados desde el momento en que se aprobó la transferencia del equipo, hasta que se hace entrega del mismo. Cualquier evento ocurrido durante ese tiempo será de responsabilidad del usuario.
- Ningún usuario tendrá la autorización de instalar software aparte del que ya está instalado en un PC de trabajo, de requerirse la instalación de cualquier paquete, esta se solicitara directamente al encargado del área de sistemas, el cual procederá a evaluar la solicitud, y a aprobarla o negarla según sea el caso. Cualquier modificación realizada será registrada en una bitácora de cambios.
- Si se detecta la instalación de software no autorizado en los equipos de trabajo, la persona responsable será amonestada por escrito, y el software será eliminado de la computadora, para evitar cualquier brecha de seguridad.
- Previo a realizar un cambio de configuración en uno de los equipos, debe realizarse un respaldo de la configuración anterior, en caso de sufrir alguna falla en la nueva configuración.
- Al ser los computadores herramientas de trabajo, están sujetos a eventos más allá de lo contemplado para un computador, por lo que su uso y cuidado fuera de oficina debe ser primordial y de tiempo completo.
- En caso de fallo, perdida de archivos o pérdida del equipo se debe reportar inmediatamente del imprevisto al encargado del área de sistemas, para la evaluación del problema y su pronta solución.
- El acceso al BIOS de las computadoras estará bloqueado mediante contraseña y la utilización de unidades booteables en el sistema estará bloqueado. Cualquier cambio que sea requerido deberá ser aprobado mediante un escrito.

4.4.2.2 Enfoque de las políticas de seguridad de voz

El enfoque dado a las políticas de uso del sistema de telefonía es un tanto diferente al aplicado en el resto de políticas de seguridad, ya que en este caso, se

enfoca en como el usuario produce y maneja la información antes de que esta sea enviada y digitalizada, es decir, cuando el usuario está hablando. Las políticas de uso van más allá de ser simplemente de un componente de la red, se enfocan en que el sistema telefónico es mucho más sensible y por tanto, rubro muy importante, que no debe ser descuidado y que por tanto, su seguridad debe ser aplicada constantemente.

4.4.2.2.1 Políticas de seguridad de Voz

- El sistema de telefonía de SACMIS debe ser de uso únicamente corporativo, y salvo en emergencias, su uso estará restringido para usos personales.
- El proceso de solicitud de habilitación de permisos de llamadas se dará en la misma manera en la que actualmente se solicitan permisos de Internet.
- La asignación de una terminal de llamada, sea esta física o virtual, otorga automáticamente la responsabilidad de su conservación a la persona a la que fue asignada.
- Para cada usuario será asignada una contraseña de 8 dígitos escogidos aleatoriamente, y que será modificada cada cierto tiempo según consideren los entes reguladores.
- La contraseña asignada para la extensión es de uso personal e intransferible y su protección es de total responsabilidad del usuario.
- Los usuarios del sistema de telefonía, desde sus terminales solo pueden tener acceso a los servicios a los cuales han sido habilitados, cualquier violación al sistema para modificar permisos sin autorización, será considerada una contravención grave a estas políticas.
- Las habitaciones en donde se encuentren los servidores y sistemas de comunicaciones deben estar restringidas para el paso no autorizado.
- Los sistemas de telefonía deben estar protegidos ante cortes imprevistos de energía, ataques externos u otro cualquier imprevisto que pueda presentarse.
- En caso de utilizarse las facilidades del sistema en dispositivos móviles, estos están sujetos a las mismas políticas de uso, como las terminales fijas.
- El Departamento de Sistemas monitoreará el sistema constantemente, para prevenir fallas en el mismo y aplicar los correctivos necesarios.

- Asimismo, el uso del sistema por parte de los usuarios será continuamente monitoreado, para evitar incumplimientos de estas políticas de uso.
- El registro de llamadas se considerara como un valor importante para los entes de monitoreo, y su divulgación total o parcial sin previa autorización será considerada una contravención a estas políticas de seguridad.
- Los instaladores de los teléfonos virtuales se podrán distribuir libremente, sin embargo, las contraseñas de registro de terminales serán de propiedad exclusiva del departamento de Sistemas y solo este ente está autorizado a configurar nuevas terminales.
- La habilitación de salas de conferencia para llamadas entrantes solo se creara bajo autorización de los departamentos pertinentes, ya que se puede incurrir en escuchas no-autorizadas por personas ajenas a la información a tratarse.
- Cada usuario está ligado a la información vocal que transmite a través del sistema telefónico, y del cual, al momento de expresarlo queda permanentemente ligado y se hace completamente responsable de él.
- Cada usuario del sistema está llamado al monitoreo del sistema para que no sea mal utilizado, ayudando así al mejor control del sistema.

4.5 MANUAL DE UTILIZACIÓN DEL SISTEMA TELEFÓNICO TOTAL DE SACMIS

4.5.1 PARA REALIZAR UNA LLAMADA

- Al marcar cualquier número externo se debe anteponer el número 9 para salir.
- El sistema de inmediato, le solicitara su clave de usuario que consta de 8 dígitos, al finalizarla, se debe presionar la tecla # (numeral).

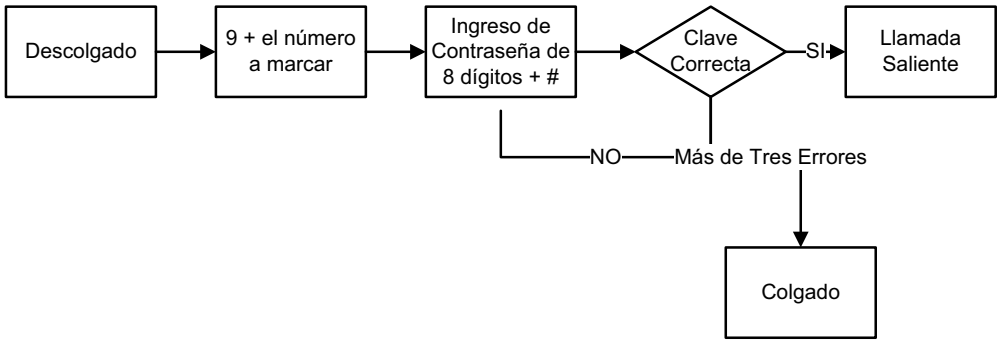


Figura 0.2 Diagrama de Flujo de realización de la llamada

4.5.2 PARA REALIZAR UNA TRANSFERENCIA CIEGA (TRANSFERENCIA DIRECTA)

- Con la llamada activa, se presiona # (numeral), tras lo cual el teléfono volverá al tono de marcado.
- Con tono de Marcado, se digita la extensión a la cual será transferida la llamada; cuando se ha especificado la extensión, el línea se colgara.

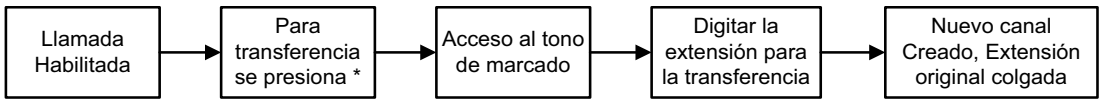


Figura 0.3 Diagrama de flujo de Transferencia Directa

4.5.3 PARA REALIZAR UNA TRANSFERENCIA ASISTIDA (TRANSFERENCIA INDIRECTA)

- Con la llamada activa, se presiona * (asterisco), tras lo cual la central reproducirá el aviso de “Transferencia” y se pasara al tono de marcado.
- Con tono de Marcado, se digita la extensión a la cual será transferida la llamada; lo que dará paso al tono de timbrado.
- Cuando la extensión a ser transferida ha contestado, se cuelga la sesión actual para hacer efectiva la transferencia.
- Si se requiere recuperar la llamada original, se debe presionar * durante el tono de marcado o timbrado, para habilitar el canal original de comunicación.

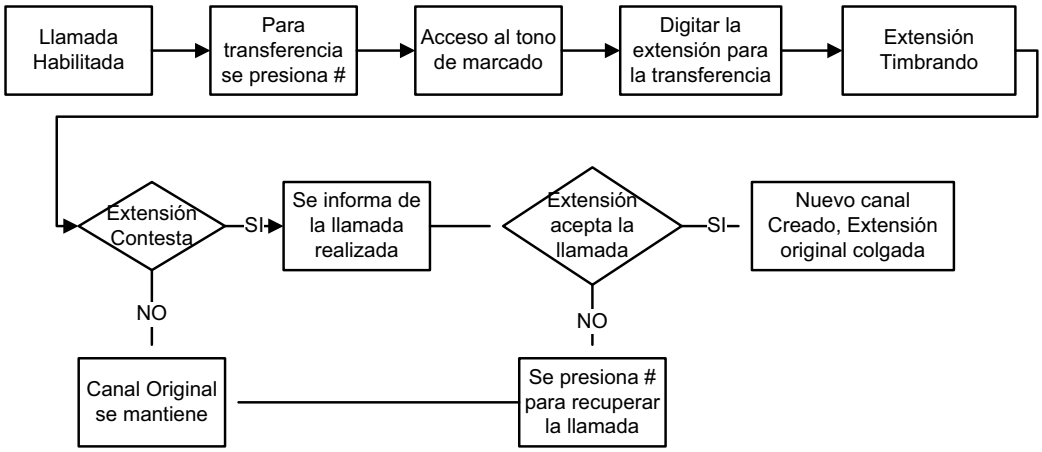


Figura 0.4 Diagrama de Flujo para una transferencia Asistida

4.5.4 PARA HABILITAR LA SALA DE CONFERENCIAS

- Si es necesario que más de dos personas accedan a una conversación, las llamadas serán transferidas a la extensión 8000, que es la sala de conferencias habilitada de la central.
- Cuando un usuario ha ingresado a la sala de conferencias, el sistema le solicitara que se identifique diciendo su nombre, el cual será almacenado en un 'buffer' temporal y servirá para informar al resto de participantes que esa persona ha ingresado o salido de la sala de conferencias.

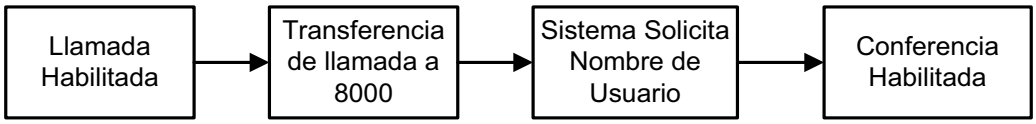


Figura 0.5 Diagrama de Flujo de Habilitación de Sala de Conferencias

4.5.5 PARA HABILITAR EL FAX

- Cuando un usuario necesita hacer uso del fax, y no hizo uso de la opción del menú, la llamada debe ser transferida a la extensión 6500, asignada para el fax analógico.

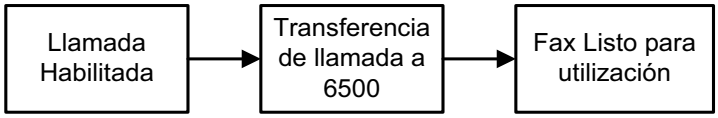


Figura 0.6 Diagrama de Flujo de Habilitación de Fax

4.5.6 PARA REVISAR LAS CARACTERÍSTICAS DEL BUZÓN DE VOZ

- Si bien los mensajes de voz se graban y se envían por correo electrónico, para revisar las características que posee el sistema, se debe marcar la extensión *333. La contraseña por defecto es 1234, y se recomienda que en el primer uso se la cambie.

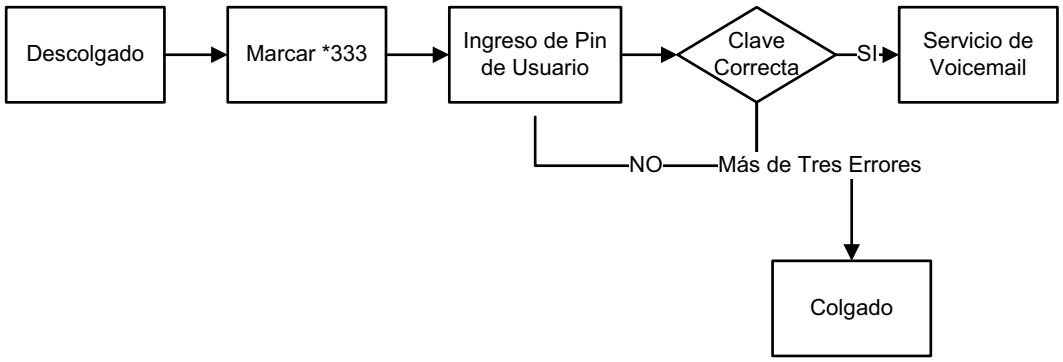


Figura 0.7. Diagrama de Flujo de acceso a Voicemail

4.5.7 RECOMENDACIONES

- Recuerde que su contraseña es personal e intransferible.
- Los permisos asignados pueden ser cambiados previa aprobación de la Gerencia de la Compañía
- Asimismo, los permisos asignados pueden ser revocados si se observa mal comportamiento por parte de la Gerencia.
- Recuerde que el Teléfono es una herramienta de trabajo, que debe ser correctamente aprovechada y no desperdiciada.

Al final de cada trabajo realizado, es importante destacar cada uno de los conocimientos adquiridos, y meditar acerca de cómo el mismo pudo haberse realizado de mejor manera. Es importante realizar siempre conclusiones apropiadas para ayudar al entendimiento del mismo.

Este capítulo presenta las conclusiones y recomendaciones a las que se ha arribado luego de la realización del proyecto.

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- **SIN TELEFONÍA ANALÓGICA, NO EXISTIRÍA TELEFONÍA IP**

Las necesidades que marcaron el desarrollo de la telefonía, permitieron el desarrollo de la Telefonía IP. Cada avance que se dio desde los inicios de la telefonía permitió que al migrar la tecnología al mundo IP se pueda prever el alcance real de la misma, y el como facilitaría las comunicaciones. Sin los primeros descubrimientos y primeras aplicaciones, la telefonía no se hubiera vuelto digital, y mucho menos IP

- **NO TODA VOIP ES TELEFONÍA IP, PERO TODA TELEFONÍA IP ES VOIP**

Diferenciar la VoIP como tecnología, de la Telefonía IP como servicio y darles como tal un espacio de convergencia donde se puede apreciar esta diferencia permite notar que la Telefonía IP hace uso de la VoIP para su funcionamiento en una LAN, y como la VoIP permite unir servidores remotos y clientes de voz remotos. A pesar de que la Telefonía depende de la tecnología, la VoIP, por si sola, no tiene las características necesarias para ser considerada como Telefonía.

- **EL PASO DE UNA PBX DE HARDWARE A SOFTWARE MARCÓ UN QUIEBRE EN LAS COMUNICACIONES**

En el pasado, la constitución de una central se la realizaba a partir de módulos de expansión, lo que hacía que pensar en una expansión requiriera toda una nueva circuitería para el sistema, que muchas veces, se traducía en un desembolso de fondos muy grande. La constitución de Asterisk como PBX permite que las expansiones sean realizadas vía software, poniendo la escalabilidad del sistema en tanto uso, en manos del usuario.

- **UN ÚNICO CABLE LARGO, NO ES A LA LARGA ADMINISTRABLE**

Si bien en redes, principalmente hogareñas y de pequeña empresa, no se utiliza cuarto de equipos por facilidad y la red es bastante simple, nunca un cable entre equipos activos llegará a ser administrable, ya que, por muy bien hecho que esté, siempre presentara mayor probabilidad de daño, rotura o avería mientras más largo sea, y por tanto, mientras más expuesto esté. Además de que esta forma de utilización del cableado forza a los cables a sus límites, lo que hace que su capacidad de transmisión especifica se vea afectada.

- **NO TODO EQUIPO ACTIVO ES ÚTIL EN TODAS LAS OCASIONES**

Por concepto, siempre se recomienda que los equipos activos de conectividad de red deban ser administrables, para habilitar o deshabilitar seguridades y puertos, sin embargo, estos equipos pueden resultar demasiado sobredimensionados para redes pequeñas o redes tipo prototipo, mientras que equipos sencillos de características moderadas pudieran ser más óptimos, con el mismo desempeño que necesita la red en cuestión.

- **TODA INSTALACIÓN DEBE SER AMIGABLE CON EL AMBIENTE**

Cada vez se nota que todo tipo de trabajo que se realiza a nivel de ingeniería debe, por obligación, considerar formas de realización que no produzcan un impacto al ecosistema del planeta. En una instalación de SCE, o una re-adecuación, esta política se manifiesta utilizando los recursos necesarios, dando prioridad al reciclaje mientras sea posible.

- **EN TODO SISTEMA DE CABLEADO, ES VITAL UNA BITÁCORA DE INSTALACIÓN Y ETIQUETADO**

Lo que vuelve completamente administrable a un sistema de Cableado, es que se tenga debidamente registrado todo el etiquetado y todos los cambios que se han realizado a un sistema, a fin de, si en caso existiera una falla, siempre tener un procedimiento de corrección.

- **LA ESTRUCTURA MODULAR DE ASTERISK SOPORTA SU EVOLUCIÓN**

Como sistema, Asterisk, al ser *Open-Source*, siempre tendrá adiciones y cambios proporcionados por los usuarios que lo usen de acuerdo a sus requerimientos, esto es posible gracias a que el núcleo del sistema permanece y solo se le van añadiendo nuevos módulos y variaciones, lo que a la larga, se traduce en una evolución continua del mismo, sin necesidad de modificar el código base, lo que permite no tener varias versiones incompatibles, sino versiones evolucionadas altamente compatibles.

- **EL SOPORTE NATIVO DE PROTOCOLOS PROPORCIONA FLEXIBILIDAD DE IMPLEMENTACIÓN**

Siempre que se lleve a cabo una implementación, el hecho de contar con sistemas soportados y probados nativamente, proporciona, más que facilidad de implementación, seguridad de que el sistema será sólido y sin fallas. Principalmente en software, las incompatibilidades y 'parches' en un sistema siempre lo volverán vulnerable, por lo que los soportes nativos son muy importantes. Además de que permite experimentar con los sistemas, volviéndolos flexibles de acuerdo a cada necesidad.

- **SIP SE VOLVIÓ EL PROTOCOLO DE VOIP POR SU FACILIDAD Y FLEXIBILIDAD**

A pesar de que puede proporcionar ciertas fallas de seguridad, y problemas de traducción de direcciones, SIP es un protocolo muy flexible para implementar, porque proporciona facilidades para las extensiones que se ponen a funcionar sin mayor complicación.

- **CADA PROTOCOLO Y CÓDEC TIENE SUS BENEFICIOS**

A pesar de que SIP se ha ganado su lugar dentro de las implementaciones de VoIP, cada protocolo tiene sus beneficios y en el momento de implementar cualquier diseño se debe considerar cuales son requerimientos reales, y no dejarse llevar por un estándar.

- **LA SEGURIDAD DEL SISTEMA ES PRIMORDIAL**

Siempre que se implemente cualquier diseño, se debe tener muy en cuenta como el sistema será protegido de ataques, internos y externos, y de cómo esta seguridad se replica en el rendimiento de la implementación, y se debe buscar siempre el equilibro entre rendimiento y seguridad.

- **LA ESTANDARIZACIÓN DE PROTOCOLOS ES PARTE DEL DISEÑO**

Principalmente cuando se va a utilizar dispositivos que funcionen con la implementación, se debe escoger aquellos que tengan compatibilidad nativa con el protocolo que se está utilizando, ya que de una incompatibilidad de dispositivos puede proporcionar fallas de comunicación, y más que todo, puede encarecer los costos del diseño en cuestión, lo cual no es eficiente.

- **LOS REQUERIMIENTOS SON ÚNICOS PARA CADA ESTUDIO**

Cuando se hace un diseño, es importante reconocer que los requerimientos de un sitio siempre será diferentes de cualquier otra posible implementación, porque las características que se implementaran son únicas y funcionan solamente para quien ha sido diseñado. Esto es fruto de la personalización de los sistemas, que, finalmente, es lo que se busca al realizar un diseño.

- **LOS PEQUEÑOS DETALLES SON IMPORTANTES EN UN DISEÑO**

Cuando se está diseñando un nuevo sistema, principalmente en telefonía, se debe tomar en cuenta aquellos pequeños detalles que pueden complicar el funcionamiento real del sistema. Si bien al momento de diseñar se consideran los sistemas básicos, pero las comunicaciones también cuentan con números especiales, por citar un ejemplo, sin los cuales el funcionamiento se vería seriamente mermado.

- **LA SEGURIDAD ES, HOY EN DÍA, PARTE FUNDAMENTAL DE LAS REDES DE INFORMACIÓN**

Con el auge de las telecomunicaciones y los sistemas real-time, la seguridad informática se va posicionando como un apartado a tomar en cuenta cuando se

utilizan este tipo de servicios, ya que la privacidad del usuario es un rubro vital que debe ser protegido de manera adecuada y eficiente.

- **EN UN SISTEMA, EL EQUILIBRIO ENTRE RENDIMIENTO Y SEGURIDAD ES PRIMORDIAL**

Todo sistema de seguridad proporcionara siempre molestias a los usuarios, ya que, al no ser intuitiva la idea de seguridad, los necesarios bloqueos siempre serán una molesta para la utilización de un sistema asegurado. Sin embargo, el exceso de seguridad de un sistema, que lo vuelva lento y poco manejable tampoco es de utilidad, por lo que el equilibrio es primordial, y principalmente, la cantidad de seguridad va en función de lo que se deba proteger.

- **EL USUARIO DEBE ESTAR CORRECTAMENTE INFORMADO EN TEMAS DE SEGURIDAD**

Los cada vez más innovadores sistemas de seguridad no serán útiles si el usuario no se prepara para manejarlos y utilizarlos de la mejor manera posible; y la responsabilidad de la concienciación es compartida entre los entes que ofrecen servicios y el propio usuario, que debe ser motivado a interesarse en su propia seguridad.

- **NO TODOS LOS SISTEMAS DE SEGURIDAD SON ÚTILES PARA TODAS LAS REDES**

La cantidad de sistemas de seguridad debe estar en función de la información a proteger, en ese sentido, una PC personal no ameritara tanta seguridad como un servidor de aplicaciones, cada sistema debe ser evaluado previamente de una manera objetiva antes de ser implementada la seguridad, para evitar excesos en seguridad, que obedezcan más a la moda del momento que a los requerimientos reales.

- **LA SEGURIDAD DE "CAPA 8" AÚN NO ES CORRECTAMENTE EXPLOTADA**

Aún muchos sistemas y servicios consideran que el usuario es un ente ajeno al sistema y que su seguridad debe ser "recomendada" por parte de los proveedores

de servicios, lo que hace que el usuario se preocupe menos de su propia seguridad. Esta política se sustenta en que el usuario desconoce cómo protegerse a sí mismo. Los nuevos sistemas de seguridad están en la obligación de modificar esta conducta para una correcta explotación de la seguridad por parte del usuario

- **CADA NUEVO DISEÑO DE RED DEBE CONTAR CON SU PROPIO SISTEMA DE SEGURIDAD**

Desde el diseño de un nuevo sistema de comunicaciones deben ir implícitos los algoritmos y las reglas y normas de seguridad que serán contempladas en el mismo, para que la seguridad evolucione a la par del nuevo sistema dando lugar a un servicio integral de cara al usuario y al proveedor.

5.2 RECOMENDACIONES

- **SE DEBE REALIZAR MANTENIMIENTO PERIÓDICO A LA RED:**

Cada red tiene su propia utilización, y por tanto, su propia degradación, por lo que el monitoreo constante es importante, para evitar fallas, y realizar un mantenimiento adecuado cada cierto tiempo determinado por la utilización que se le dé a la red.

- **EN CASO DE CRECIMIENTO, SE DEBEN AGREGAR EQUIPOS DE CONECTIVIDAD:**

En la implementación presentada, la mayoría de conexiones se da vía inalámbrica, por lo que no se requirió más equipos, sin embargo, en caso de una reingeniería, se deban añadir tantos equipos como sean necesarios, en función de las nuevas prioridades.

- **PREVIO A TODA INSTALACIÓN, SE DEBE REVISAR LOS MATERIALES DE PISOS, PAREDES Y TECHO:**

Al ser cada instalación diferente, no se puede estandarizar que tipo de sujeción deben llevar canaletas, mangueras y pasadores, por lo que previo a la instalación se debe tener un completo conocimiento de la estructura y los materiales que la

componen, para que cada conexión y encaminamiento quede completamente asegurado.

- **EN LA INSTALACIÓN SE DEBEN UTILIZAR IMPLEMENTOS DE SEGURIDAD:**

Siempre, por las características de las instalaciones, pueden ocurrir accidentes, así como se debe determinar las infraestructuras, con las mismas se debe utilizar herramientas e implementos de seguridad, que eviten caídas, cortaduras y lesiones, asignando la prioridad correspondiente la seguridad de las personas que están instalando el sistema.

- **SE DEBE, EN LO POSIBLE, MEJORAR LA DISPONIBILIDAD DEL SERVIDOR:**

Si bien las necesidades del servidor hacen que el hardware implementado sea suficiente para garantizar un correcto desempeño, no debe descuidarse que la tecnología avanza y siempre es posible mejorar los sistemas, volviéndolos redundantes y con disponibilidad aumentada. En este sentido no se debe descuidar las protecciones eléctricas.

- **LAS CONTRASEÑAS DEBEN SER CAMBIADAS CADA TRES MESES, POR SEGURIDAD:**

Cada contraseña, como todo producto, tiene su tiempo de caducidad, ya que el uso prolongado de la misma la pone en peligro frente a ataques de ingeniera social, por lo que se debe cambiar la contraseña periódicamente, para evitar cualquier inconveniente posterior.

- **EN TANTO SEA POSIBLE, SE DEBE UTILIZAR TELÉFONOS FÍSICOS EN LUGAR DE SOFTPHONES:**

Como se explicó, el uso de softphones condiciona mucho el sistema de telefonía a los recursos y compatibilidades que posea un PC en el cual se instalen los teléfonos virtuales, lo que no siempre asegurará una comunicación fluida, que siempre, por el contrario, estará presente en un teléfono físico, ya que su diseño ha sido creado para tal función.

- **PARA UNA IMPLEMENTACIÓN DE TELEFONÍA MÓVIL, SE DEBEN CONFIGURAR LOS CODECS ADECUADOS:**

A pesar de que la señalización sea mucho más sencilla en SIP para localización, se debe considerar los canales que se ocupan para la transmisión de información, ya que muchas veces el ancho de banda no es suficiente y se debe utilizar códecs que primordien el rendimiento en detrimento de la fidelidad. Como en la mayoría de los casos, 'todo depende'.

- **SE DEBE REVISAR LOS ARCHIVOS DE CONFIGURACIÓN DEL SISTEMA CON REGULARIDAD:**

Siempre es necesario que los archivos de configuración sean revisados, porque en la creación y revisión se puede pasar por alto detalles que podrían ser importantes y/o críticos para el sistema, y que pueden ser visualizados con más calma, en una revisión posterior de los archivos.

- **LOS SISTEMAS DE SEGURIDAD DEBEN SER REVISADOS Y EVALUADOS PERIÓDICAMENTE:**

Las evaluaciones periódicas a los sistemas de seguridad permiten corregir errores y ampliar campos de seguridad para la correcta protección de la información.

- **CONFORME AVANCE LA RED Y EL SISTEMA TELEFÓNICO, SE DEBE MODIFICAR LAS POLÍTICAS DE SEGURIDAD:**

El sistema de telefonía de SACMIS aún tiene mucho por crecer, en base a los requerimientos propios del trabajo; con cada avance que se realice para ampliar la capacidad de red telefónica, las políticas diseñadas para su implementación deben ser revisadas para que contemplen las nuevas adicciones, los nuevos sistemas, y los nuevos usuarios.

- **SE DEBEN ESTABLECER SANCIONES POR ESCRITO PARA LAS CONTRAVENCIONES A LAS NORMAS DE SEGURIDAD:**

Cada acción en contra de las buenas prácticas de seguridad por parte de los usuarios debe ser sancionada, para desanimar a otros usuarios de realizar la

misma u otras faltas similares. La Gerencia debe determinar las sanciones pertinentes siempre acogiéndose al reglamento interno y a las políticas de seguridad diseñadas.

- **SI UN COMPUTADOR NO ES DE USO CONTINUO NO DEBE ASIGNARSE UNA EXTENSIÓN:**

Dentro del sistema de trabajo, las computadoras que se utilizan, si no están asignadas a una persona en específico, a esta PC no debe ser asignada una extensión, ya que la información de contactos y llamadas, así como la información personal del usuario se verá vulnerable a cualquier filtración o ingreso no autorizado, violando la privacidad del usuario.

BIBLIOGRAFÍA

LIBROS, TEXTOS Y PUBLICACIONES

[1] **NOLL**, A. Michael. INTRODUCTION TO TELEPHONES AND TELEPHONE SYSTEMS. Artech House. USA. 1999. Third Edition. ISBN 1-58053-000-1

[2] **Carpenter**, Colman; **Duffett**, David; **Middleton**, Nik; **Plain**, Ian. ASTERISK 1.4: THE PROFESSIONAL'S GUIDE. Packt Publishing Ltd.2009. First Edition. ISBN 978-1-847194-38-1.

[3] **Van Meggelen**, Jim; **Madsen**, Leif; **Smith**, Jared. ASTERISK: THE FUTURE OF TELEPHONY. O'Reilly Media, Inc. 2007. Second Edition. ISBN-13 978-0-596-51048-0.

[4] **Gómez López**, Julio; **Gil Montoya**, Francisco (Editores). VOIP Y ASTERISK: REDESCUBRIENDO LA TELEFONÍA. Alfaomega Grupo Editor. 2009. Primera Edición. ISBN 978-607-7686-08-8.

[5] **Durkin**, James F. VOICE-ENABLING THE DATA NETWORK: H.323, MGCP, SIP, QOS, SLAS, AND SECURITY. Cisco Press. 2010. First Edition. ISBN 1-58714-287-2.

[6] Spectum Magazine. Enero 2011, Publicaciones IEEE

[7] RCF 3261: Definición de SIP

[8] Normas ISO-IEC 27000, 27001, 27002

PÁGINAS WEB

[9] http://www.saber.golwen.com.ar/htelefono.htm

[10] http://trajano.us.es/~rafa/ARSS/apuntes/tema4.pdf;
http://trajano.us.es/~rafa/ARSS/apuntes/tema5.pdf;
http://trajano.us.es/~rafa/ARSS/apuntes/tema6.pdf
Apuntes de clase de Arquitectura de Redes, Sistemas y Servicios. Dr. Rafael Estepa Alonso. Universidad de Sevilla.

[11] http://es.wikipedia.org/wiki/Tel%C3%A9fono

[12] http://es.wikipedia.org/wiki/Micr%C3%B3fono_de_carb%C3%B3n

[13] http://es.wikipedia.org/wiki/Antracita

[14] http://proton.ucting.udg.mx/temas/comunicaciones/ulloa/index.html

[15] http://web.educastur.princast.es/ies/sanchezl/organiza/depart/electronica/Web/tema9.htm

[16] http://www.monografias.com/especiales/telefoniaip/index.shtml

[17] http://www.uberbin.net/archivos/rants/voip-no-es-telefonia-ip.php

[18] http://www.cudi.edu.mx/primavera_2005/presentaciones/rodolfo_castaneda.pdf

[19] http://docs.digium.com/TDM410/analog410series_manual.pdf

[20] http://www.3cx.es/voip-sip/sip-responses.php

[21] www.iso27000.es: La Página en español de la norma ISO-IEC 27000

[22] https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/es/n/non_repudiation.htm

[23] http://es.wikipedia.org/wiki/Session_Initiation_Protocol

[24] http://es.wikipedia.org/wiki/Session_Description_Protocol

[25] http://www.fiuba6662.com.ar/6648/presentaciones/2006/Informe%20SIP.pdf

[26] http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml

APUNTES ESCOLÁSTICOS

[27] Apuntes de clase y Folleto teórico de Teoría de Comunicaciones. Ing. Ma. Soledad Jiménez. Ingeniería Electrónica y Redes de Información. Facultad de Ingeniería Electrónica. Escuela Politécnica Nacional.

PROYECTOS DE TITULACIÓN

[28] **Rodríguez Hoyos**, Ana Fernanda. DESARROLLO DE UN SISTEMA DE TELEFONÍA IP DISTRIBUIDO MEDIANTE LA IMPLEMENTACIÓN DE UN MECANISMO DE DESCUBRIMIENTO DE RUTAS DE LLAMADAS, EN BASE AL SISTEMA OPERATIVO LINUX. Tesis de Grado de Ingeniería Electrónica y Redes de Información. Escuela Politécnica Nacional. Octubre 2010.

[29] **Méndez Esquivel**, Carlos. INBOUND PARA ENLACES PSTN CON VOIP. Tesis de Licenciatura en Ingeniería en Electrónica y Comunicaciones. Universidad de las Américas Puebla. Mayo 2005.

[30] **Álvarez Zurita**, Flor María; **García Guzmán**, Pamela Anabel: IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA LA INTRANET DE LA CORPORACIÓN METROPOLITANA DE SALUD. Tesis de Grado de Ingeniería Electrónica y Redes de Información. Escuela Politécnica Nacional. Octubre 2007.

- **OTROS**

[31] Currículo Empresarial SACMIS Cía. Ltda.

[32] Capturas de tráfico del sistema de telefonía utilizando en paquete computacional Wireshark.

ANEXOS

A. DIFERENTES TONOS UTILIZADOS EN LAS REDES TELEFÓNICAS NACIONALES[1]

A.1. CANADÁ

Tono	Frecuencia (Hz)	Cadencia (seg)
Tono de ocupado	480+620	0.5 on 0.5 off
Tono de congestión	480+620	0.25 on 0.25 off
Tono de invitación a marcar	350+440	continuo
Tono de llamada	440+480	2.0 on 4.0 off
Tono de indicación de llamada en espera	440	2x(0.3 on 10.0 off)

A.2. COLOMBIA (REPÚBLICA DE)

Tono	Frecuencia (Hz)	Cadencia (seg)
Tono de ocupado	425	0.25 on 0.25 off
Tono de congestión	425	0.10 on 0.25 off 0.35 on 0.25 off 0.65 on 0.25 off
Tono de invitación a marcar	425	continuo
Tono de abonado inaccesible	425	0.65 on 0.25 off 0.20 on 0.60 off
Tono de pago	50/12000/16000	0.15 on
Tono de llamada	425	1.0 on 4.5 off

[1] Que tienen referencia con los usados en Ecuador

Tono especial de información	950/1400/1800	3x0.333 on 1.0 off

A.3. ECUADOR

Tono	Frecuencia (Hz)	Cadencia (seg)
Tono de ocupado	425	0.33 on 0.33 off
Tono de congestión	425	0.33 on 0.33 off
Tono de invitación a marcar	425	continuo
Tono de llamada	425	1.2 on 4.65 off
Tono de indicación de llamada en espera	425	0.2 on 0.6 off

A.4. ESPAÑA

Tono	Frecuencia (Hz)	Cadencia (seg)
Tono de ocupado – I	425	0.2 on 0.2 off
Tono de ocupado – II	425	0.5 on 0.5 off
Tono de congestión – I	425	2x(0.2 on 0.2 off) 0.2 on 0.6 off
Tono de congestión – II	425	0.25 on 0.25 off
Tono de invitación a marcar	425	continuo
Tono especial de invitación a marcar – I	425	1.0 on 0.1 off
Tono especial de invitación a marcar – II	425	0.5 on 0.05 off

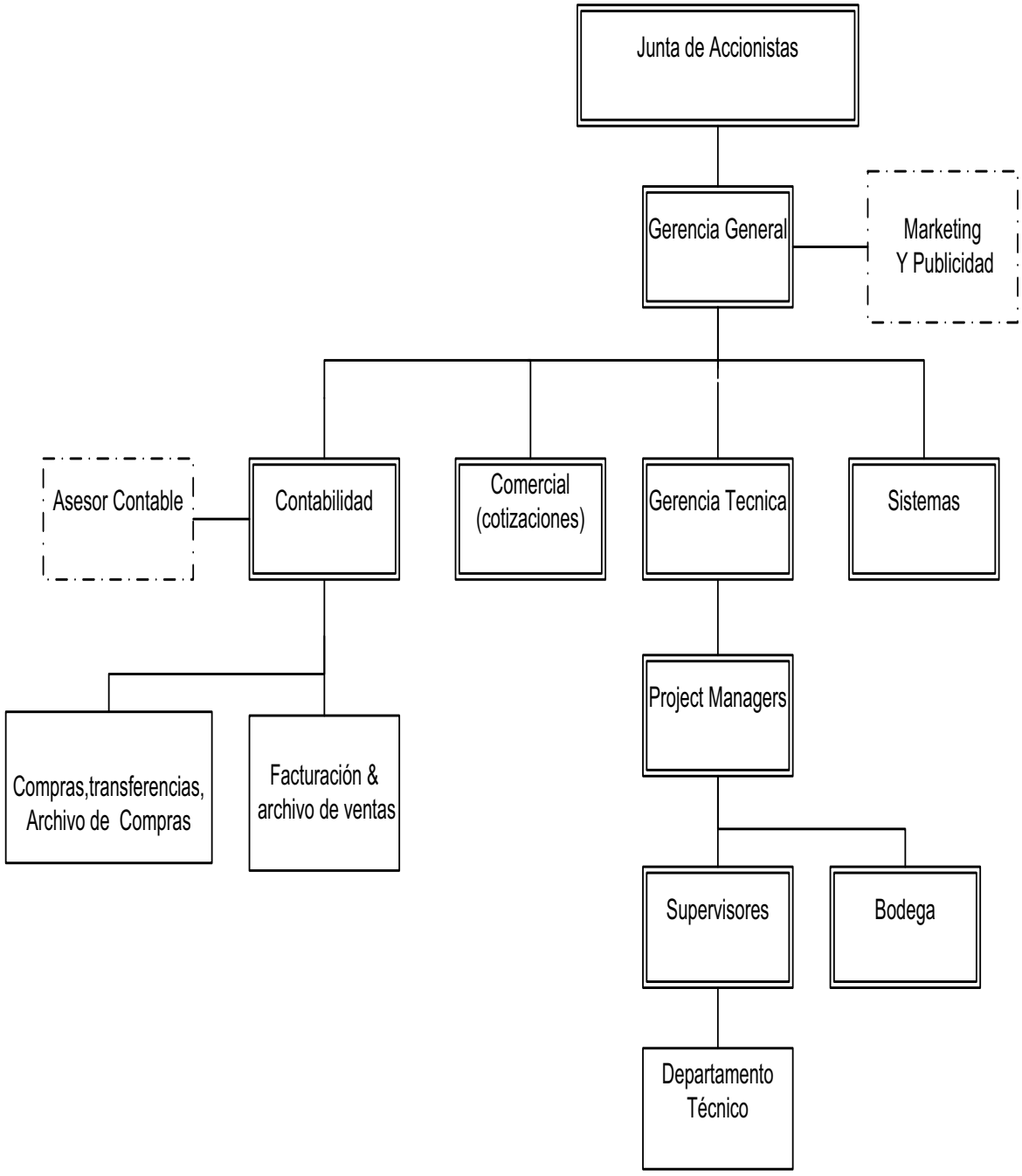
Tono de abonado inaccesible – I	425	0.2 on 0.2 off 0.2 on 0.6 off
Tono de abonado inaccesible – II	425	0.5 on 2.5 off
Tono de identificación de teléfono de previo pago – I	1600	0.05 on 0.05 off 0.05 on 1.5 off
Tono de identificación de teléfono de previo pago -II	1600	0.05 on 0.05 off 0.05 on 0.05 off 0.05 on 1.5 off
Tono de llamada – I	425	1.5 on 3.0 off
Tono de llamada – II	425	1.0 on 4.0 off
Tono especial de información	950/1400/1800	3x0.33 on 1.0 off
Tono de aviso - intervención de la operadora	1400	0.4 on 5.0 off
Tono de indicación de llamada en espera	425	0.175 on 0.175 off 0.175 on 3.5 off

A.5. ESTADOS UNIDOS DE AMÉRICA

Tono	**Frecuencia (Hz)**	**Cadencia (seg)**
Tono de ocupado	600x120//600x133//600x140//600x160//480+620	0.5 on 0.5 off
Tono de confirmación	350+440	3x(0.1 on 0.1 off)
Tono de invitación a marcar	600x120//600x133//600x140//600x160//350+440	continuo
Tono de repetición de invitación a marcar	350+440	3x(0.1 on 0.1 off) + continuo

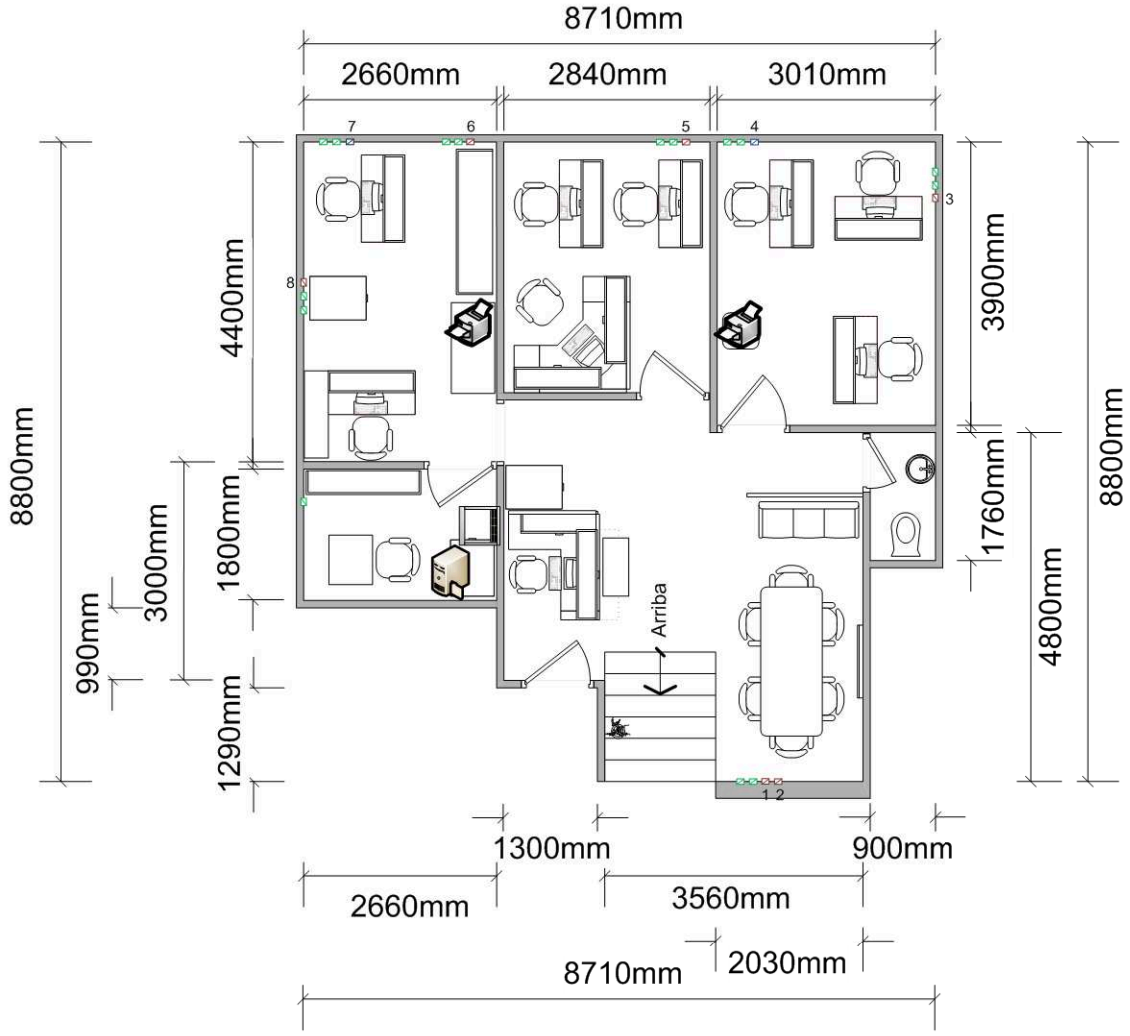
Tono de intervención	600x120//600x133//600x140//600x160//480+620	0.5 on 0.5 off
Tono de abonado inaccesible	200//400	0.5 on 6.0 off
Tono de señal permanente	480//400//500	continuo
Tono de grabación	440	0.5 on 5.0 off
Tono de llamada	420x40//500x40//440+480	2.0 on 4.0 off
Tono de re-llamada	600x120//600x133//600x140//600x160//480+620	0.3 on 0.2 off
Tono de aviso - mensaje (4)	1400	0.5 on
Tono de indicación de llamada en espera	440	2x(0.3 on 10.0 off)

B. ORGANIGRAMA INSTITUCIONAL DE SACMIS CÍA. LTDA. [31]



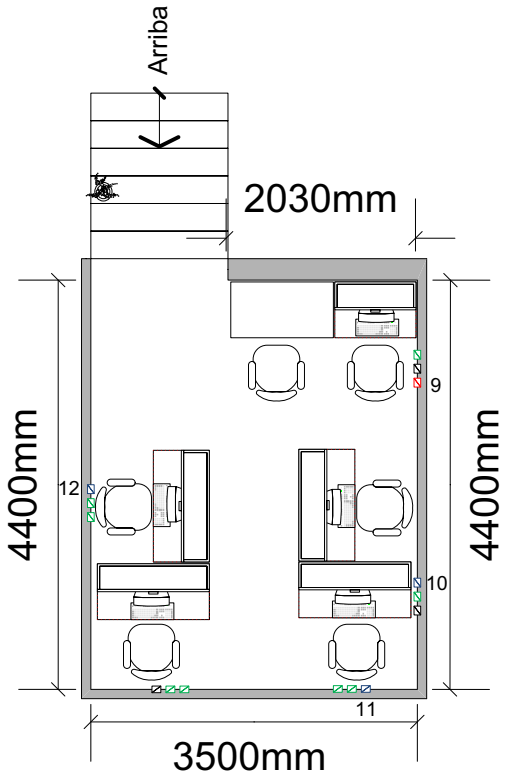
C. PLANO DE PLANTA ALTA PREVIO A LA RE-ADECUACIÓN[1]

C.1. SUBPLANTA 1



[1] El plano de la planta baja solo se adjuntó en la re-adecuación, ya que no se hicieron cambios, sino que se instaló la infraestructura desde un inicio

C.2. SUBPLANTA 2

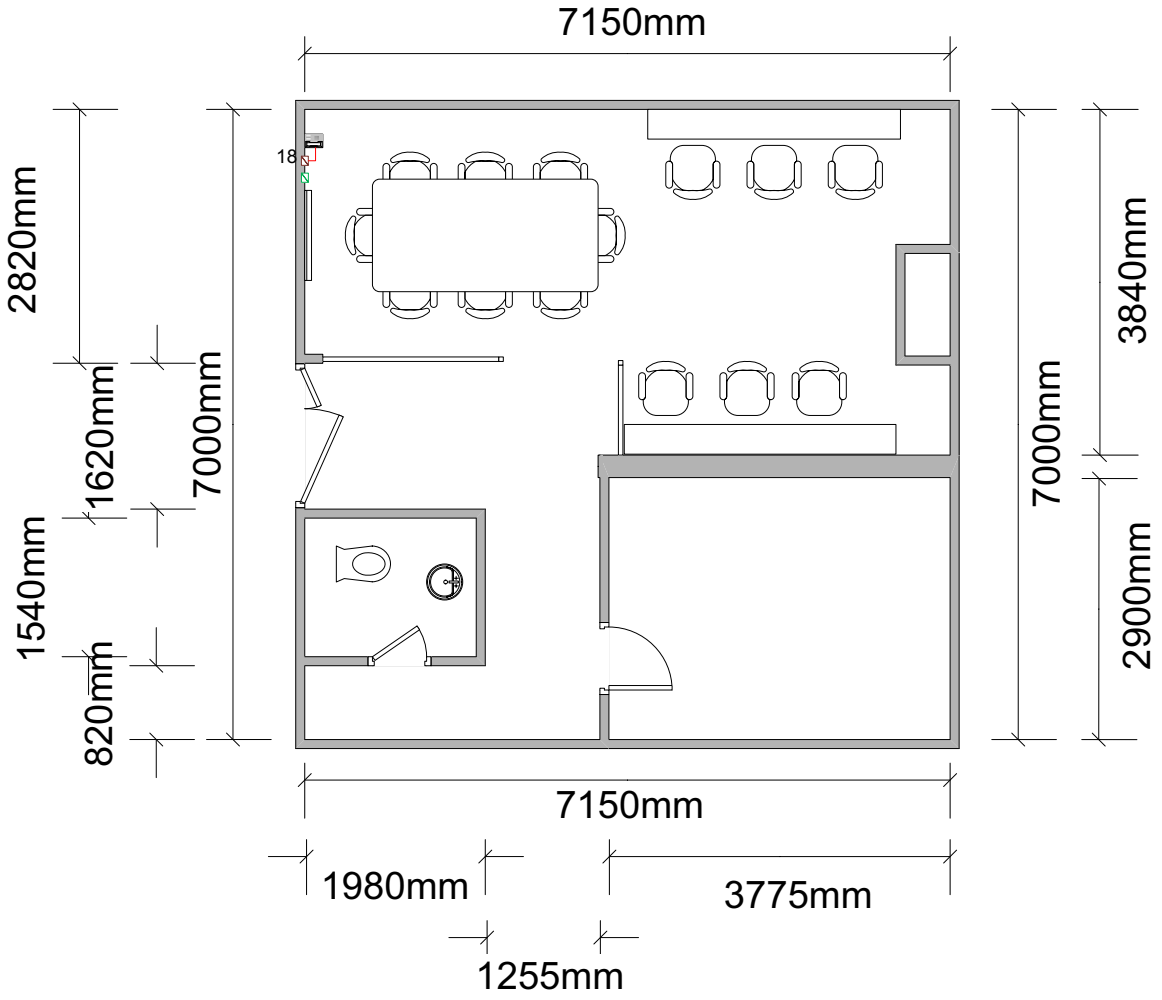


Donde:

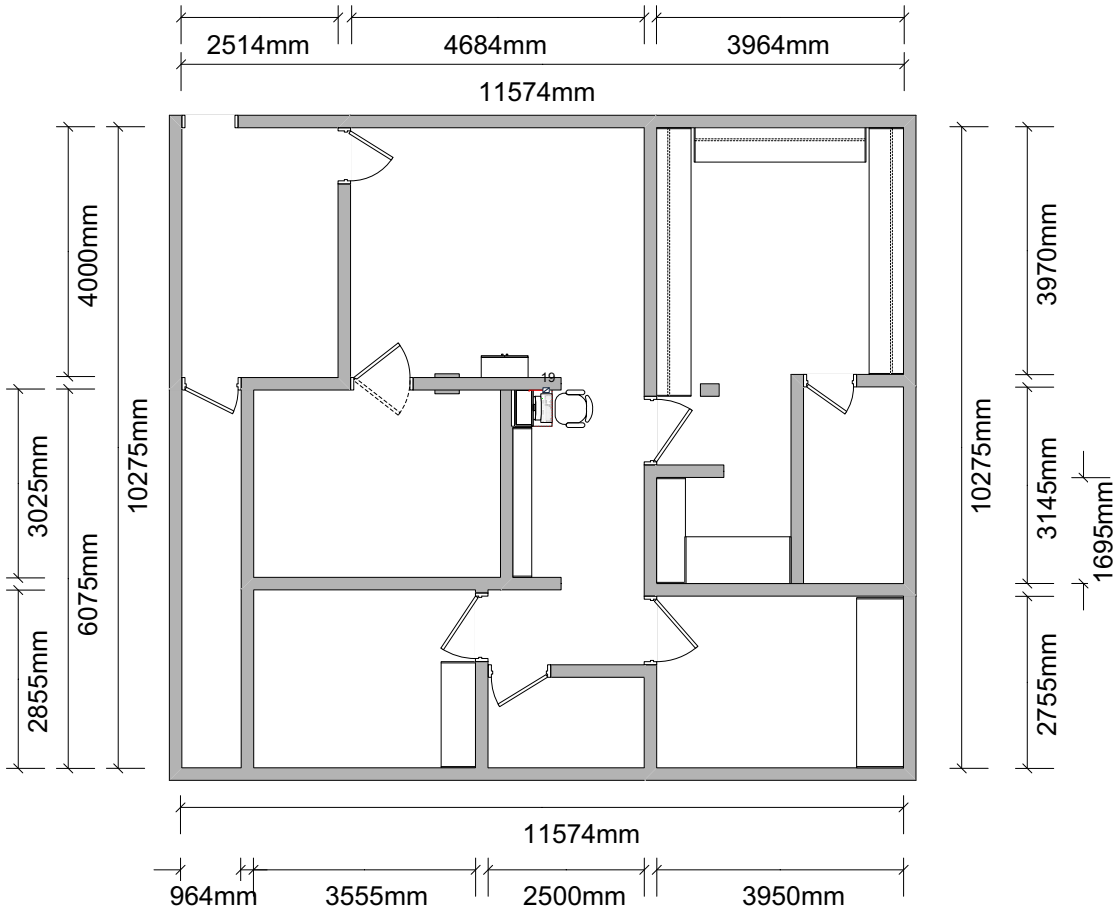
- Toma de Voz
- Toma de Datos
- Toma de Energía
- Toma Ciega

D. PLANO DE PLANTA BAJA LUEGO DE LA RE-ADECUACIÓN

D.1. SUBPLANTA 1



D.2. SUBPLANTA 2

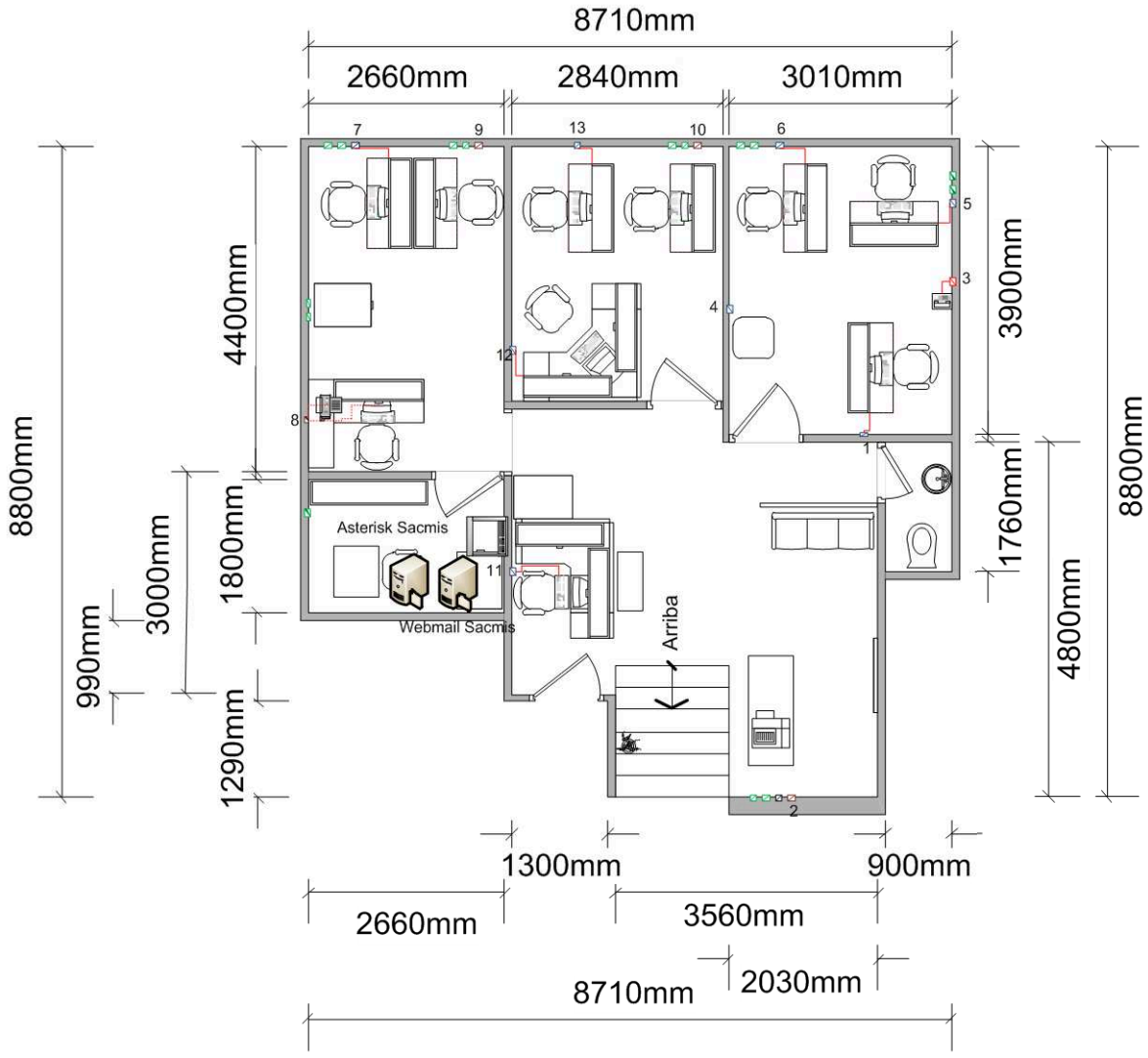


Donde:

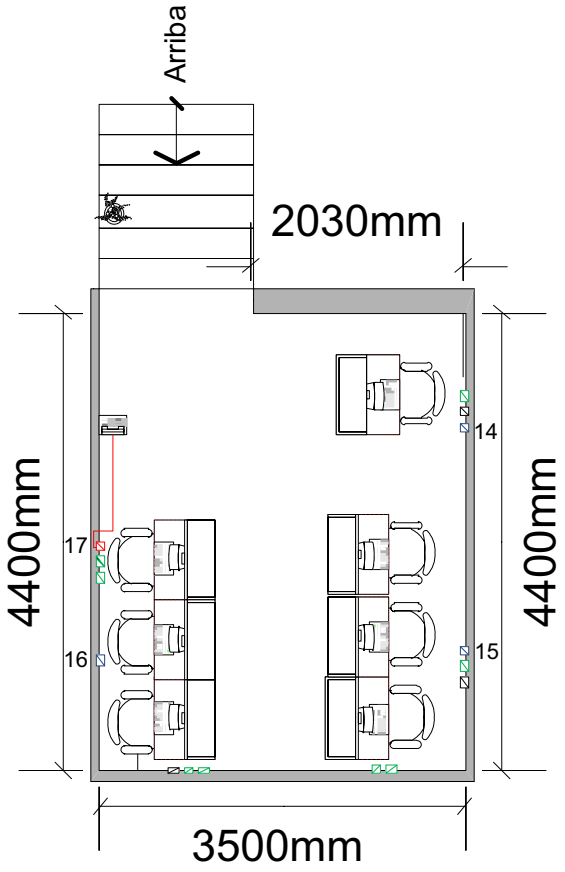
- Toma de Voz
- Toma de Datos
- Toma de Energía
- Toma Ciega

E. PLANO DE PLANTA ALTA LUEGO DE LA RE-ADECUACIÓN

E.1. SUBPLANTA 1



E.2. SUBPLANTA 2



Donde:

- Toma de Voz
- Toma de Datos
- Toma de Energía
- Toma Ciega

F. VALORES DE LLAMADAS REALIZADAS/RECIBIDAS PARA EL CÁLCULO DE LOS VALORES DE TRAFICO PARA EL SERVIDOR DE TELEFONIA[1]

F.1. SEMANA 1

Día	Hora	Numero de llamadas	Duración Promedio de llamada (segundos)
Lunes	09:00-10:00	3	130
	10:00-11:00	4	215
	11:00-12:00	3	250
	12:00-13:00	5	175
	13:00-14:00	2	155
	14:00-15:00	3	270
	15:00-16:00	2	292
	16:00-17:00	3	280
	17:00-18:00	2	210
Promedio			220
Martes	09:00-10:00	2	95
	10:00-11:00	4	145
	11:00-12:00	3	167
	12:00-13:00	2	200
	13:00-14:00	2	115
	14:00-15:00	4	180
	15:00-16:00	5	195
	16:00-17:00	3	230
	17:00-18:00	4	200
Promedio			170
Miércoles	09:00-10:00	2	75
	10:00-11:00	4	180
	11:00-12:00	6	290
	12:00-13:00	1	175
	13:00-14:00	1	78

[1] Estas llamadas incluyen las transferencias que se realizan via fax

	14:00-15:00	4	178
	15:00-16:00	5	215
	16:00-17:00	3	260
	17:00-18:00	1	230
Promedio			195
Jueves	09:00-10:00	1	75
	10:00-11:00	3	195
	11:00-12:00	2	170
	12:00-13:00	2	132
	13:00-14:00	1	89
	14:00-15:00	3	215
	15:00-16:00	3	225
	16:00-17:00	1	145
	17:00-18:00	2	210
Promedio			178
Viernes	09:00-10:00	2	125
	10:00-11:00	3	245
	11:00-12:00	1	95
	12:00-13:00	3	270
	13:00-14:00	2	190
	14:00-15:00	4	255
	15:00-16:00	3	235
	16:00-17:00	4	320
	17:00-18:00	4	280
Promedio			210
Promedio Semanal		192 (3 min 12 seg)	

Semana 2

Día	**Hora**	**Numero de llamadas**	**Duración Promedio de llamada (segundos)**
Lunes	09:00-10:00	3	160
	10:00-11:00	4	240
	11:00-12:00	3	250
	12:00-13:00	5	195
	13:00-14:00	2	155

	14:00-15:00	3	270
	15:00-16:00	2	260
	16:00-17:00	3	290
	17:00-18:00	2	193
Promedio			224
Martes	09:00-10:00	2	130
	10:00-11:00	4	195
	11:00-12:00	3	230
	12:00-13:00	2	200
	13:00-14:00	2	116
	14:00-15:00	4	180
	15:00-16:00	5	185
	16:00-17:00	3	230
	17:00-18:00	4	240
Promedio			190
Miércoles	09:00-10:00	2	75
	10:00-11:00	4	180
	11:00-12:00	6	135
	12:00-13:00	1	175
	13:00-14:00	1	140
	14:00-15:00	4	178
	15:00-16:00	5	136
	16:00-17:00	3	260
	17:00-18:00	1	75
Promedio			150
Jueves	09:00-10:00	1	75
	10:00-11:00	3	270
	11:00-12:00	2	170
	12:00-13:00	2	132
	13:00-14:00	1	125
		3	245
	15:00-16:00	3	225
	16:00-17:00	1	145
	17:00-18:00	2	210
Promedio			177
Viernes	09:00-10:00	2	125
	10:00-11:00	3	120

	11:00-12:00	1	130
	12:00-13:00	3	270
	13:00-14:00	2	190
	14:00-15:00	4	275
	15:00-16:00	3	235
	16:00-17:00	4	330
	17:00-18:00	4	260
Promedio			215
Promedio Semanal		191 (3min 11 seg)	

G. ARCHIVOS DE CONFIGURACIÓN DEL SERVIDOR

G.1. SIP.CONF

```
; Define los parámetros que deberán tener todas las canales SIP del
sistema.

[general]
context=phones          ; El contexto por defecto, su configuración se
establecerá en extensions.conf
allowguest=no
allowoverlap=no         ; Deshabilita el overlapping de llamadas
bindport=5060           ; El puerto UDP por defecto que escuchara el
servidor de Asterisk
bindaddr=0.0.0.0  ; Direcciones IP habilitadas para conectarse (0.0.0.0
habilita todas)
srvlookup=yes           ; Habilita el servidor DNS SRV para llamadas
salientes, deshabilitarlo impediria llamadas SIP desde dominios de
Internet
;externip = 186.69.167.170
;externrefresh=8
;localnet=192.168.0.0/255.255.255.0
videosupport=yes  ; Habilita el servicio de Videollamada
;dtmfrelax=yes
language=es       ; Lenguaje por defecto de los sonidos utilizados por el
canal

; Plantilla de definición de canales SIP

[planSACMIS](!)         ; El simbolo (!) junto al nombre define la
plantilla para usarla dentro del archivo
type=friend       ; Tipo de canal que reconocera Asterisk
host=dynamic            ; Direccion IP de cada Terminal
nat=yes                 ; Activa la configuracion NAT para la terminal
dmtfmode=RFC2833  ; Tipo de DMTF de la Terminal
videosupport=yes  ; Habilita el servicio de Videollamada
disallow=all            ; Deshabilita codecs anteriores
;allow=alaw       ; Habilitacion de codecs
allow=ulaw
;allow=gsm
;allow=h261
allow=h263
allow=h263p

[planSACMISCel](!)
type=friend
host=dynamic
compactheaders=yes
nat=yes
dmtfmode=RFC2833
disallow=all
allow=ulaw
;allow=gsm

; Canales SIP, definidos para la configuracion
```

```
; Departamento de Gerencia

[2000](planSACMIS)
callerid="Departamento de Gerencia" <2000>
secret=gerndp2000
context=phones-pass
mailbox=2000@SACMIS

[2010](planSACMIS)
callerid="Fernando Aucancela" <2010>
secret=gernfa2010
context=phones-pass
mailbox=2010@SACMIS

[2011](planSACMISCel)
callerid="Fernando Aucancela" <2011>
secret=gernfa2011
context=phones-pass
mailbox=2011@SACMIS

[2020](planSACMIS)
callerid="Christian Casamen" <2020>
secret=gerncc2020
context=phones-pass
mailbox=2020@SACMIS

[2021](planSACMISCel)
callerid="Christian Casamen" <2021>
secret=gerncc2021
context=phones-pass
mailbox=2021@SACMIS

[2030](planSACMIS)
callerid="Marcelo Huertas" <2030>
secret=gernmh2030
context=phones-pass
mailbox=2030@SACMIS

[2031](planSACMISCel)
callerid="Marcelo Huertas" <2031>
secret=gernmh2031
context=phones-pass
mailbox=2031@SACMIS

; Departamento de Sistemas

[3000](planSACMIS)
callerid="Departamento de Sistemas" <3000>
secret=sistdp3000
context=phones-pass
mailbox=3000@SACMIS

[3010](planSACMIS)
callerid="Tania Huertas" <3010>
secret=sistth3010
context=phones-pass
mailbox=3010@SACMIS

[3020](planSACMIS)
callerid="Daniel Maldonado" <3020>
```

```
secret=sistdm3020
context=phones-pass
mailbox=3020@SACMIS

; Departamento de Proyectos

[4000](planSACMIS)
callerid="Departamento de Proyectos" <4000>
secret=proydp4000
context=phones-pass
mailbox=4000@SACMIS

[4010](planSACMIS)
callerid="Marco Ballesteros" <4010>
secret=proymb4010
context=phones-pass
mailbox=4010@SACMIS

[4011](planSACMISCel)
callerid="Marco Ballesteros" <4011>
secret=proymb4011
context=phones-pass
mailbox=4011@SACMIS

[4020](planSACMIS)
callerid="Armando Cuzco" <4020>
secret=proyac4020
context=phones-pass
mailbox=4020@SACMIS

[4021](planSACMISCel)
callerid="Armando Cuzco" <4021>
secret=proyac4021
context=phones-pass
mailbox=4021@SACMIS

[4030](planSACMIS)
callerid="Ricardo Espinoza" <4030>
secret=proyre4030
context=phones-pass
mailbox=4030@SACMIS

[4031](planSACMISCel)
callerid="Ricardo Espinoza" <4031>
secret=proyre4031
context=phones-pass
mailbox=4031@SACMIS

[4040](planSACMIS)
callerid="Fernando Yanez" <4040>
secret=proyfy4040
context=phones-pass
mailbox=4040@SACMIS

[4041](planSACMISCel)
callerid="Fernando Yanez" <4041>
secret=proyfy4041
context=phones-pass
mailbox=4041@SACMIS
```

```
; Departamento Tecnico

[5000](planSACMIS)
callerid="Departamento Tecnico" <5000>
secret=techdp5000
context=phones-pass
mailbox=5000@SACMIS

[5010](planSACMIS)
callerid="Carlos Bayas" <5010>
secret=techcb5010
mailbox=5010@SACMIS

[5020](planSACMIS)
callerid="Danny Checa" <5020>
secret=techdc5020
mailbox=5020@SACMIS

[5030](planSACMIS)
callerid="Fernando Chicaiza" <5030>
secret=techfc5030
mailbox=5030@SACMIS

[5040](planSACMIS)
callerid="Esteban Cornejo" <5040>
secret=techec5040
mailbox=5040@SACMIS

[5050](planSACMIS)
callerid="Heriberto Dea" <5050>
secret=teched5050
mailbox=5050@SACMIS

[5060](planSACMIS)
callerid="Edgar Espinosa" <5060>
secret=techee5060
mailbox=5060@SACMIS

[5070](planSACMIS)
callerid="Pablo Espinoza" <5070>
secret=techpe5070
mailbox=5070@SACMIS

[5080](planSACMIS)
callerid="Pablo Gavilanez" <5080>
secret=techpg5080
mailbox=5080@SACMIS

[5090](planSACMIS)
callerid="Gabriel Guangaje" <5090>
secret=techgg5090
mailbox=5090@SACMIS

[5100](planSACMIS)
callerid="Carla Ligna" <5100>
secret=techcl5100
mailbox=5100@SACMIS

[5110](planSACMIS)
callerid="Javier Nono" <5110>
```

```
secret=techjn5110
mailbox=5110@SACMIS

[5120](planSACMIS)
callerid="Wilson Puruncaja" <5120>
secret=techwp5120
mailbox=5120@SACMIS

[5130](planSACMIS)
callerid="Paul Quimbita" <5130>
secret=techpq5130
mailbox=5130@SACMIS

[5140](planSACMIS)
callerid="Diego Ramos" <5140>
secret=techdm5140
mailbox=5140@SACMIS

[5150](planSACMIS)
callerid="Edwin Sailema" <5150>
secret=teches5150
mailbox=5150@SACMIS

[5160](planSACMIS)
callerid="Joselito Salazar" <5160>
secret=techjs5160
mailbox=5160@SACMIS

[5170](planSACMIS)
callerid="Francisco Singo" <5170>
secret=techfs5170
mailbox=5170@SACMIS

[5180](planSACMIS)
callerid="Victor Solis" <5180>
secret=techvs5180
mailbox=5180@SACMIS

[5190](planSACMIS)
callerid="Francisco Vinueza" <5190>
secret=techfv5190
mailbox=5190@SACMIS

; Departamento De Ventas y Contabilidad

[6000](planSACMIS)
callerid="Departamento De Ventas y Contabilidad" <6000>
secret=vcontdp6000
context=phones-pass
mailbox=6000@SACMIS

[6010](planSACMIS)
callerid="Daysi Brito" <6010>
secret=vcontdb6010
context=phones-pass
mailbox=6010@SACMIS

[6020](planSACMIS)
callerid="Alicia Casamen" <6020>
secret=vcontac6020
```

```
context=phones-pass
mailbox=6020@SACMIS

[6030](planSACMIS)
callerid="Sandra Ushina" <6030>
secret=vcontsu6030
context=phones-pass
mailbox=6030@SACMIS

; Departamento de Logistica

[7000](planSACMIS)
callerid="Logistica" <7000>
secret=logjl7000
mailbox=7000@SACMIS
```

G.2. EXTENSIONS.CONF

```
; Define los parametros de funcionamiento de la central

[general]
autofallthrough=yes

[globals]
operadora=DAHDI/2
trunkCNT=DAHDI/G0
fax=DAHDI/1

[menu-incoming]
exten => s,1,Answer()
;exten => s,n,Set(CONTADOR=0)
exten => s,n,Set(TIMEOUT(digits)=4)
exten => s,n,Set(TIMEOUT(response)=5)
exten => s,n,PlayBack(/root/sonidos-SACMIS/bienvenida)
exten => s,n(menu),Background(/root/sonidos-SACMIS/menu1)
;exten => s,n,NoOp(${CONTADOR})
exten => s,n,WaitExten()

exten => _2XXX,1,Macro(buzon3,${EXTEN},2000)
exten => _3XX0,1,Macro(buzon1,${EXTEN},3000)
exten => _4XXX,1,Macro(buzon3,${EXTEN},4000)
exten => _5XX0,1,Macro(buzon1,${EXTEN},5000)

exten => 6000,1,Dial(${operadora},45,Ttm)
exten => 6000,n,Voicemail(6000@SACMIS)
exten => 6000,n,Hangup()

exten => _60[1-9]0,1,Macro(buzon4,${EXTEN})
exten => _6[1-9]X0,1,Macro(buzon4,${EXTEN})

exten => _7XX0,1,Macro(buzon2,${EXTEN})

exten => i,1,Playback(/root/sonidos-SACMIS/invalida)
exten => i,n,Goto(s,menu)

exten => t,1,Goto(submenu-incoming,s,1)
```

```
[submenu-incoming]
exten => s,1,Set(TIMEOUT(digit)=3)
exten => s,n,Set(TIMEOUT(response)=5)
exten => s,n,BackGround(/root/sonidos-SACMIS/menu2)
exten => s,n,WaitExten()

exten => 1,1,Macro(buzon2,6020)

exten => 2,1,Dial(SIP/6010,45,Ttm)
exten => 2,n,Voicemail(6010@SACMIS)
exten => 2,n,Hangup()

exten => 3,1,Macro(buzon2,4010)
exten => 4,1,Macro(buzon2,3010)
exten => 5,1,Macro(buzon2,7000)

exten => 6,1,Dial(${fax},45)
exten => 6,n,Hangup()

exten => i,1,Playback(/root/sonidos-SACMIS/invalida)
exten => i,n,Goto(menu-incoming,s,menu)

exten => t,1,Dial(${operadora},45,Ttm)
exten => t,n,Hangup()

[internal]
exten => _2XXX,1,macro(llamadaSACMIS,${EXTEN},2000)
exten => _3XX0,1,macro(llamadaSACMIS,${EXTEN},3000)
exten => _4XXX,1,macro(llamadaSACMIS,${EXTEN},4000)
exten => _5XX0,1,macro(llamadaSACMIS,${EXTEN},5000)
exten => _60[1-9]0,1,macro(llamadaSACMIS1,${EXTEN})
exten => _6[1-9]X0,1,macro(llamadaSACMIS1,${EXTEN})

exten => 7000,1,Dial(SIP/${EXTEN},45,Ttm)
exten => 7000,n,Voicemail(7000@SACMIS)
exten => 7000,n,Hangup()

exten => 7010,1,Dial(SIP/${EXTEN},45,Ttm)
exten => 7010,n,Voicemail(7010@SACMIS)
exten => 7010,n,Hangup()

exten => _[2-5]000,1,macro(departamentosSACMIS,${EXTEN})

exten => 6000,1,Dial(${operadora},45,Ttm)
exten => 6000,n,Voicemail(6000@SACMIS)
exten => 6000,n,Hangup()

exten => 6500,1,Dial(DAHDI/1,45,Ttm)
exten => 6500,n,Hangup()

exten => 8000,1,Answer()
exten => 8000,n,Meetmecount(8000,CONFCOUNT)
exten => 8000,n,Gotoif($[${CONFCOUNT}<=10]?meetme:conf_full,1)
exten => 8000,n(meetme),Meetme(8000,icaMps)
exten => conf_full,1,Playback(conf-full)

exten => *333,1,Answer()
exten => *333,n,VoiceMailMain(${CALLERID(num)}@SACMIS)
exten => *333,n,HangUp()
```

```
[locales]
exten =>
_9[2356]XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT
})
;exten => _9[2356]XXXXXX,n,Hangup()
exten =>
_9100,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})

[nacionales]
exten => _90[3-
7]XXXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
;exten => _90[3-7]XXXXXXX,n,Hangup()

[emergencia]
exten => _910[124-6],1,Dial(${trunkCNT}/${EXTEN:1})
exten => _910[124-6],n,Hangup()
exten => 9131,1,Dial(${trunkCNT}/${EXTEN:1})
exten => 9131,n,Hangup()
exten => 9911,1,Dial(${trunkCNT}/${EXTEN:1})
exten => 9911,n,Hangup()
exten => 9140,1,Dial(${trunkCNT}/${EXTEN:1})
exten => 9140,n,Hangup()

[especiales]
exten => _91[7-
9]00XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
;exten => _91[7-9]00XXXXXX,n,Hangup()

[porta]
exten => _9082[5-
9]XXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
exten =>
_908[568]XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCN
T})
exten => _9089[027-
9]XXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
exten =>
_909[01347]XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunk
CNT})
exten => _9092[0-
4]XXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
exten => _9099[13-
6]XXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})

[movistar]
exten =>
_9084XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
exten => _9087[0-
2]XXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
exten => _9092[5-
9]XXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
exten =>
_909[58]XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT
})
exten => _9099[027-
9]XXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})

[alegro]
```

```
exten => _9082[0-
4]XXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
;exten => _9082[0-4]XXXXX,n,Hangup()
exten =>
_9096XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:4:4},${trunkCNT})
;exten => _9096XXXXXX,n,Hangup()


[celulares]
include => porta
include => movistar
include => alegro

[CNT]
include => locales
include => nacionales
include => especiales

[fax]
exten =>
_9[2356]XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:6},${trunkCNT})

[analogico]
include => internal
include => emergencia
exten =>
_9[2356]XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:6},${trunkCNT})
exten => _90[3-
7]XXXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:6},${trunkCNT})
exten => _91[7-
9]00XXXXXX,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:6},${trunkCNT})
exten => _9100,1,macro(llamadasegura,${EXTEN:1},${CHANNEL:6},${trunkCNT})

[phones]
include => internal
include => emergencia

exten => 100,1,Goto(menu-incoming,s,1)


[phones-pass]
include => phones
include => celulares
include => CNT



[macro-buzon1]
exten => s,1,Dial(SIP/${ARG1},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado:nodisponible)

exten => s,n(nodisponible),Playback(/root/sonidos-SACMIS/no-disponible)
exten => s,n,Dial(SIP/${ARG2},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado1:nodisponible1)
exten => s,n(nodisponible1),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado2:nodisponible2)
exten => s,n(nodisponible2),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,u)
exten => s,n,Hangup()
```

```
exten => s,n(ocupado2),Goto(nodisponible2)
exten => s,n(ocupado1),Goto(nodisponible1)

exten => s,n(ocupado),Playback(/root/sonidos-SACMIS/ocupado)
exten => s,n,Dial(SIP/${ARG2},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado3:nodisponible3)
exten => s,n(nodisponible3),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado4:nodisponible4)
exten => s,n(nodisponible4),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,b)
exten => s,n,Hangup()
exten => s,n(ocupado2),Goto(nodisponible4)
exten => s,n(ocupado1),Goto(nodisponible3)

[macro-buzon2]
exten => s,1,Dial(SIP/${ARG1},30,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado:nodisponible)

exten => s,n(nodisponible),Playback(/root/sonidos-SACMIS/no-disponible)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado1:nodisponible1)
exten => s,n(nodisponible1),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,u)
exten => s,n,Hangup()
exten => s,n(ocupado1),Goto(nodisponible1)

exten => s,n(ocupado),Playback(/root/sonidos-SACMIS/ocupado)
exten => s,n,Dial(${operadora}DAHDI/2,45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado2:nodisponible2)
exten => s,n(nodisponible2),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,b)
exten => s,n,Hangup()
exten => s,n(ocupado2),Goto(nodisponible2)

[macro-buzon3]
exten => s,1,Dial(SIP/${ARG1},45,Ttm)
exten => s,n,Dial(SIP/${ARG1:-4:3}1,30,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado:nodisponible)

exten => s,n(nodisponible),Playback(/root/sonidos-SACMIS/no-disponible)
exten => s,n,Dial(SIP/${ARG2},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado1:nodisponible1)
exten => s,n(nodisponible1),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado2:nodisponible2)
exten => s,n(nodisponible2),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,u)
exten => s,n,Hangup()
exten => s,n(ocupado2),Goto(nodisponible2)
exten => s,n(ocupado1),Goto(nodisponible1)

exten => s,n(ocupado),Playback(/root/sonidos-SACMIS/ocupado)
exten => s,n,Dial(SIP/${ARG2},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado3:nodisponible3)
exten => s,n(nodisponible3),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado4:nodisponible4)
exten => s,n(nodisponible4),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,b)
```

```
exten => s,n,Hangup()
exten => s,n(ocupado2),Goto(nodisponible4)
exten => s,n(ocupado1),Goto(nodisponible3)

[macro-buzon4]
exten => s,1,Dial(SIP/${ARG1},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado:nodisponible)

exten => s,n(nodisponible),Playback(/root/sonidos-SACMIS/no-disponible)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado1:nodisponible1)
exten => s,n(nodisponible1),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado2:nodisponible2)
exten => s,n(nodisponible2),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,u)
exten => s,n,Hangup()
exten => s,n(ocupado2),Goto(nodisponible2)
exten => s,n(ocupado1),Goto(nodisponible1)

exten => s,n(ocupado),Playback(/root/sonidos-SACMIS/ocupado)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado3:nodisponible3)
exten => s,n(nodisponible3),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado4:nodisponible4)
exten => s,n(nodisponible4),Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,b)
exten => s,n,Hangup()
exten => s,n(ocupado2),Goto(nodisponible4)
exten => s,n(ocupado1),Goto(nodisponible3)


[macro-llamadaSACMIS]
exten => s,1,Dial(SIP/${ARG1},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado:nodisponible)

exten => s,n(nodisponible),Playback(/root/sonidos-SACMIS/no-disponible)
exten => s,n,Dial(SIP/${ARG2},45,Ttm)
exten => s,n,Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,u)
exten => s,n,Hangup()

exten => s,n(ocupado),Playback(/root/sonidos-SACMIS/ocupado)
exten => s,n,Dial(SIP/${ARG2},45,Ttm)
exten => s,n,Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,b)
exten => s,n,Hangup()

[macro-llamadaSACMIS1]
exten => s,1,Dial(SIP/${ARG1},45,Ttm)
exten => s,n,GotoIf($["${DIALSTATUS}" = "BUSY"]?ocupado:nodisponible)

exten => s,n(nodisponible),Playback(/root/sonidos-SACMIS/no-disponible)
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,u)
exten => s,n,Hangup()

exten => s,n(ocupado),Playback(/root/sonidos-SACMIS/ocupado)
```

```
exten => s,n,Dial(${operadora},45,Ttm)
exten => s,n,Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS,b)
exten => s,n,Hangup()

[macro-departamentosSACMIS]
exten => s,1,Dial(SIP/${ARG1},45,Ttm)
exten => s,n,Playback(/root/sonidos-SACMIS/no-linea)
exten => s,n,Voicemail(${ARG1}@SACMIS)
exten => s,n,Hangup()

[macro-llamadasegura]
exten => s,1,Authenticate(/etc/asterisk/passwords/pass-${ARG2},a)
exten => s,n,Dial(${ARG3}/${ARG1})
exten => s,n,Hangup()
```

G.3. VOICEMAIL.CONF

```
; Archivo de configuracion de correo de voz de Asterisk

; Parametros generales

[general]

format=wav|gsm                      ; El formato en que se guardaran los
mensajes de voz
attach=yes                    ; Le dice al sistema que en los e-mails,
debe adjuntarse una copia de la grabacion
maxlogins=3                   ; El numero maximo de oportunidades de
accesar que tiene el usuario
servermail=no-responder@SACMIS.com.ec    ; El servidor de correo para
enviar los mensajes a los usuarios
maxmessage=180                      ; Limita el valor maximo en tiempo de
un mensaje de voz
minmessage=3                        ; Limita el valor minimo en tiempo de
un mensaje de voz
maxmsg=50                     ; Limita el numero de mensajes por casilla
de voz que pueden existir
delete=yes                    ; Especifica que se elimine el mensaje del
buzon de correo una vez que ha sido enviado por correo electronico
searchcontext=no              ; Busca los buzones en todos los contextos
definidos en el archivo
fromstring="PBX SACMIS"             ; Define la cabecera del Asunto de
envio de correo
mailcmd=/usr/sbin/sendmail -v -t -f no-responder@SACMIS.com.ec        ;
La aplicacion que se utilizara para enviar los correos electronicos
maxsilence=2                        ; Define el maximo tiempo de silencio
para considerar el mensaje terminado
silencethreshold=128                ; Define el valor de sensibiliada del
sonido para considerar los silencios



; Formato de e-mail que recibira el usuario cuando tenga un mensaje

emailsubject=[PBX]: Tienes un nuevo mensaje en tu buzon SACMIS
```

```
emailbody=Estimado ${VM_NAME}:\n\nEl dia ${VM_DATE} recibiste una llamada
de ${VM_CALLERID}, quien ha dejado un mensaje al tu no estar disponible.
El mensaje de voz esta adjunto a este correo. Si necesitas hacer algun
cambio en tu buzon ${VM_MAILBOX} siempre puedes llamar al *333. \nPara
servirte. SACMIS PBX. \n"

emaildateformat=%A, %d/%m/%Y a las %H:%M:%S



; Contexto general donde se almacenaran las definiciones de los buzones
de SACMIS

[SACMIS]

;Definicion de los buzones del departamento de Gerencia
2000 => 1234,Departamento de
Gerencia,SACMIS@SACMIS.com.ec,,sayduration=yes
2010 => 1234,Fernando Aucancela,faucancela@SACMIS.com.ec,,sayduration=yes
2011 => 1234,Fernando Aucancela,faucancela@SACMIS.com.ec,,sayduration=yes
2020 => 1234,Christian Casamen,ccasamen@SACMIS.com.ec,,sayduration=yes
2021 => 1234,Christian Casamen,ccasamen@SACMIS.com.ec,,sayduration=yes
2030 => 1234,Marcelo Huertas,mhuertas@SACMIS.com.ec,,sayduration=yes
2031 => 1234,Marcelo Huertas,mhertas@SACMIS.com.ec,,sayduration=yes

; Definicion de los buzones del departamento de sistemas
3000 => 1234,Departamento de
Sistemas,SACMIS@SACMIS.com.ec,,sayduration=yes
3010 => 1234,Tania Huertas,thuertas@SACMIS.com.ec,,sayduration=yes
3020 => 1234,Daniel Maldonado,dmaldonado@SACMIS.com.ec,,sayduration=yes

; Definicion de los buzones del departamento de proyectos
4000 => 1234,Departamento de
Proyectos,SACMIS@SACMIS.com.ec,,sayduration=yes
4010 => 1234,Marco
Ballesteros,mballesteros@SACMIS.com.ec,,sayduration=yes
4011 => 1234,Marco
Ballesteros,mballesteros@SACMIS.com.ec,,sayduration=yes
4020 => 1234,Armando Cuzco,acuzco@SACMIS.com.ec,,sayduration=yes
4021 => 1234,Armando Cuzco,acuzco@SACMIS.com.ec,,sayduration=yes
4030 => 1234,Ricardo Espinoza,respinoza@SACMIS.com.ec,,sayduration=yes
4031 => 1234,Ricardo Espinoza,respinoza@SACMIS.com.ec,,sayduration=yes
4040 => 1234,Fernando Yanez,fyanez@SACMIS.com.ec,,sayduration=yes
4041 => 1234,Fernando Yanez,fyanez@SACMIS.com.ec,,sayduration=yes

; Definicion de los buzones del departamento tecnico

5000 => 1234,Departamento Tecnico,SACMIS@SACMIS.com.ec,,sayduration=yes
5010 => 1234,Carlos Bayas,cbayas@SACMIS.com.ec,,sayduration=yes
5020 => 1234,Danny Checa,dcheca@SACMIS.com.ec,,sayduration=yes
5030 => 1234,Fernando Chicaiza,fchicaiza@SACMIS.com.ec,,sayduration=yes
5040 => 1234,Esteban Cornejo,ecornejo@SACMIS.com.ec,,sayduration=yes
5050 => 1234,Heriberto Dea,hdea@SACMIS.com.ec,,sayduration=yes
5060 => 1234,Edgar Espinosa,eespinosa@SACMIS.com.ec,,sayduration=yes
5070 => 1234,Pablo Espinoza,pespinoza@SACMIS.com.ec,,sayduration=yes
5080 => 1234,Pablo Gavilanez,pgavilanez@SACMIS.com.ec,,sayduration=yes
5090 => 1234,Gabriel Guangaje,gguangaje@SACMIS.com.ec,,sayduration=yes
5100 => 1234,Carla Ligna,cligna@SACMIS.com.ec,,sayduration=yes
5110 => 1234,Javier Nono,jnono@SACMIS.com.ec,,sayduration=yes
```

```
5120 => 1234,Wilson Puruncaja,wpuruncaja@SACMIS.com.ec,,sayduration=yes
5130 => 1234,Paul Quimbita,pquimbita@SACMIS.com.ec,,sayduration=yes
5140 => 1234,Diego Ramos,dramos@SACMIS.com.ec,,sayduration=yes
5150 => 1234,Edwin Sailema,esailema@SACMIS.com.ec,,sayduration=yes
5160 => 1234,Joselito Salazar,jsalazar@SACMIS.com.ec,,sayduration=yes
5170 => 1234,Francisco Singo,fsingo@SACMIS.com.ec,,sayduration=yes
5180 => 1234,Victor Solis,vsolis@SACMIS.com.ec,,sayduration=yes
5190 => 1234,Francisco Vinueza,fvinueza@SACMIS.com.ec,,sayduration=yes

; Definicion de los buzones del departamento de Ventas y contabilidad

6000 => 1234,Departamento de Ventas y
Contabilidad,SACMIS@SACMIS.com.ec,,sayduration=yes
6010 => 1234,Daysi Brito,dbrito@SACMIS.com.ec,,sayduration=yes
6020 => 1234,Alicia Casamen,acasamen@SACMIS.com.ec,,sayduration=yes
6030 => 1234,Sandra Ushina,sushina@SACMIS.com.ec,,sayduration=yes

; Definicion de los buzones de Logistica

7000 => 1234,Bodega,bodegaSACMIS@SACMIS.com.ec,,sayduration=yes
```

G.4. CHAN_DAHDI.CONF

```
[channels]

relaxdtmf=no
answeronpolarityswitch=no
hanguppolarityswitch=no
echocancel=yes
;rxgain=-5.0
;txgain=8.0
busydetect=yes
busycount=3
;busypattern=350,350
callprogress=no
language=es
;callerid=Llamada Externa
usecallerid=yes

context=menu-incoming
relaxdtmf=yes
echocancel=yes
busydetect=yes
busycount=3
rxgain=8.0
txgain=5.0
callerid="SACMIS Cia. Ltda." <2554746>
usecallerid=yes
signalling=fxs_ks
group=0
channel => 3,4

inmediate=no
context=fax
signalling=fxo_ks
rxgain=-6.0
txgain=8.0
```

```
group=1
channel => 1

inmediate=no
context=analogico
signalling=fxo_ks
rxgain=-8.0
txgain=4.0
group=2
channel => 2
```

G.5. FAIL2BAN/JAIL.CONF

```
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
#
# $Revision: 617 $
#

# The DEFAULT allows a global definition of the options. They can be
override
# in each jail afterwards.

[DEFAULT]

# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban
will not
# ban a host which matches an address in this list. Several addresses can
be
# defined using space separator.
ignoreip = 127.0.0.1 192.168.0.0 186.69.167.170

# "bantime" is the number of seconds that a host is banned.
bantime  = 600

# A host is banned if it has generated "maxretry" during the last
"findtime"
# seconds.
findtime  = 600

# "maxretry" is the number of failures before a host get banned.
maxretry = 3

# "backend" specifies the backend used to get files modification.
Available
# options are "gamin", "polling" and "auto". This option can be
overridden in
# each jail too (use "gamin" for a jail and "polling" for another).
#
# gamin:   requires Gamin (a file alteration monitor) to be installed. If
Gamin
#          is not installed, Fail2ban will use polling.
# polling: uses a polling algorithm which does not require external
libraries.
# auto:    will choose Gamin if available and polling otherwise.
backend = auto
```

```
# This jail corresponds to the standard configuration in Fail2ban 0.6.
# The mail-whois action send a notification e-mail with a whois request
# in the body.

[ssh-iptables]

enabled  = false
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
           sendmail-whois[name=SSH, dest=you@mail.com,
sender=fail2ban@mail.com]
logpath  = /var/log/sshd.log
maxretry = 5

[proftpd-iptables]

enabled  = false
filter   = proftpd
action   = iptables[name=ProFTPD, port=ftp, protocol=tcp]
           sendmail-whois[name=ProFTPD, dest=you@mail.com]
logpath  = /var/log/proftpd/proftpd.log
maxretry = 6

# This jail forces the backend to "polling".

[sasl-iptables]

enabled  = false
filter   = sasl
backend  = polling
action   = iptables[name=sasl, port=smtp, protocol=tcp]
           sendmail-whois[name=sasl, dest=you@mail.com]
logpath  = /var/log/mail.log

# Here we use TCP-Wrappers instead of Netfilter/Iptables. "ignoreregex"
is
# used to avoid banning the user "myuser".

[ssh-tcpwrapper]

enabled     = false
filter      = sshd
action      = hostsdeny
              sendmail-whois[name=SSH, dest=you@mail.com]
ignoreregex = for myuser from
logpath     = /var/log/sshd.log

# This jail demonstrates the use of wildcards in "logpath".
# Moreover, it is possible to give other files on a new line.

[apache-tcpwrapper]

enabled  = false
filter       = apache-auth
action   = hostsdeny
logpath  = /var/log/apache*/*error.log
           /home/www/myhomepage/error.log
maxretry = 6
```

```
# The hosts.deny path can be defined with the "file" argument if it is
# not in /etc.

[postfix-tcpwrapper]

enabled  = false
filter   = postfix
action   = hostsdeny[file=/not/a/standard/path/hosts.deny]
           sendmail[name=Postfix, dest=you@mail.com]
logpath  = /var/log/postfix.log
bantime  = 300

# Do not ban anybody. Just report information about the remote host.
# A notification is sent at most every 600 seconds (bantime).

[vsftpd-notification]

enabled  = false
filter   = vsftpd
action   = sendmail-whois[name=VSFTPD, dest=you@mail.com]
logpath  = /var/log/vsftpd.log
maxretry = 5
bantime  = 1800

# Same as above but with banning the IP address.

[vsftpd-iptables]

enabled  = false
filter   = vsftpd
action   = iptables[name=VSFTPD, port=ftp, protocol=tcp]
           sendmail-whois[name=VSFTPD, dest=you@mail.com]
logpath  = /var/log/vsftpd.log
maxretry = 5
bantime  = 1800

# Ban hosts which agent identifies spammer robots crawling the web
# for email addresses. The mail outputs are 'buffer'ed.

[apache-badbots]

enabled  = false
filter   = apache-badbots
action   = iptables-multiport[name=BadBots, port="http,https"]
           sendmail-'buffer'ed[name=BadBots, lines=5, dest=you@mail.com]
logpath  = /var/www/*/logs/access_log
bantime  = 172800
maxretry = 1

# Use shorewall instead of iptables.

[apache-shorewall]

enabled  = false
filter   = apache-noscript
action   = shorewall
           sendmail[name=Postfix, dest=you@mail.com]
logpath  = /var/log/apache2/error_log
```

```
# This jail uses ipfw, the standard firewall on FreeBSD. The "ignoreip"
# option is overridden in this jail. Moreover, the action "mail-whois"
defines
# the variable "name" which contains a comma using "". The characters ''
are
# valid too.

[ssh-ipfw]

enabled  = false
filter   = sshd
action   = ipfw[localhost=192.168.0.1]
           sendmail-whois[name="SSH,IPFW", dest=you@mail.com]
logpath  = /var/log/auth.log
ignoreip = 168.192.0.1

# These jails block attacks against named (bind9). By default, logging is
off
# with bind9 installation. You will need something like this:
#
# logging {
#     channel security_file {
#         file "/var/log/named/security.log" versions 3 size 30m;
#         severity dynamic;
#         print-time yes;
#     };
#     category security {
#         security_file;
#     };
# }
#
# in your named.conf to provide proper logging.
# This jail blocks UDP traffic for DNS requests.

[named-refused-udp]

enabled  = false
filter   = named-refused
action   = iptables-multiport[name=Named, port="domain,953",
protocol=udp]
           sendmail-whois[name=Named, dest=you@mail.com]
logpath  = /var/log/named/security.log
ignoreip = 168.192.0.1

# This jail blocks TCP traffic for DNS requests.

[named-refused-tcp]

enabled  = false
filter   = named-refused
action   = iptables-multiport[name=Named, port="domain,953",
protocol=tcp]
           sendmail-whois[name=Named, dest=you@mail.com]
logpath  = /var/log/named/security.log
ignoreip = 168.192.0.1

# This jail blocks traffic for Asterisk

[asterisk-iptables]
```

```
enabled  = true
filter   = asterisk
action   = iptables-allports[name=ASTERISK, protocol=all]
           sendmail-whois[name=ASTERISK, dest=dmaldonado@SACMIS.com.ec,
sender=fail2ban@local.local]
logpath  = /var/log/asterisk/messages
maxretry = 5
bantime = 259200
```

G.6. DAHDI/SYSTEM.CONF

```
# Autogenerated by /usr/sbin/dahdi_genconf on Fri Feb  4 10:36:24 2011
# If you edit this file and execute /usr/sbin/dahdi_genconf again,
# your manual changes will be LOST.
# Dahdi Configuration File
#
# This file is parsed by the Dahdi Configurator, dahdi_cfg
#
# Span 1: WCTDM/0 "Wildcard TDM410P Board 1" (MASTER)
fxoks=1
echocanceller=mg2,1
fxoks=2
echocanceller=mg2,2
fxsks=3
echocanceller=mg2,3
fxsks=4
echocanceller=mg2,4

# Global data

loadzone    = us
defaultzone = us

#alaw = 1-4
```

H. RESPUESTAS SIP [4]

1xx Respuestas informativas	
100	Tratando
180	Teléfono sonando
181	Llamada está siendo re direccionada
182	Encolada
183	Progreso de sesión
2xx Respuestas de éxito	
200	OK
202	aceptada: Utilizada por referidos
3xx Respuestas de redirección	
300	Múltiples opciones
301	Movido permanentemente
302	Movido temporalmente
305	Utiliza Proxy
380	Servicio alternativo
4xx Errores de solicitud	
400	Solicitud errónea
401	No autorizado: Utilizado solamente por registradores. Proxy's deben utilizar autorización proxy 407
402	Pago requerido (Reservado para uso futuro)
403	Prohibido
404	No Encontrado: Usuario no encontrado
405	Método no permitido
406	No Aceptable
407	Autenticación Proxy Requerida
408	Expiración de solicitud: No pudo encontrar al usuario a tiempo
410	Ido: El usuario existió una vez, pero ya no está disponible aquí.
413	Solicitud de entidad muy larga
414	Solicitud URI muy larga
415	Tipo de medio no soportado
416	Esquema URI no soportado
420	Mala extensión: Mala extensión de protocolo SIP utilizada, no entendida por el servidor
421	Extensión requerida
423	Intervalo muy corto
480	Temporalmente no disponible

481	Llamada/Transacción no existe
482	Lazo detectado
483	Muchos saltos
484	Dirección incompleta
485	Ambiguo
486	Ocupado acá
487	Solicitud terminada
488	No aceptable acá
491	Solicitud pendiente
493	No descifrable: No pudo desencriptar la parte del cuerpo S/MIME
5xx Errores de servidor	
500	Error interno del servidor
501	No Implementado: La solicitud / método SIP no está implementado aquí.
502	Pasarela errónea
503	Servicio no disponible
504	Expiración de servidor
505	Versión no soportada: El servidor no soporta esta versión del protocolo SIP
513	Mensaje demasiado largo
6xx Errores globales	
600	Ocupado en todas partes
603	Declinación
604	No existe en ninguna parte
606	No Aceptable

I. SCRIPT DE INSTALACIÓN DE ASTERISK PARA SERVIDORES

```
#!/bin/bash
#
#Script para la instalacion de Asterisk en CentOS 5
#
#
echo "Instalacion de la ultima version de Asterisk 1.4 en CentOS, se
recomienda cerrar otras aplicaciones antes de continuar"
sleep 5
#Ingreso a la carpeta de fuentes
echo "Ingreso a la Carpeta de Fuentes /usr/src/"
cd /usr/src
#Creacion de la carpeta contenedora de los paquetes
echo "Creacion de la carpeta asterisk"
mkdir asterisk
#Ingreso a la carpeta
cd Asterisk
sleep 4
#Instalación de los paquetes esenciales para el uso de Asterisk
echo "Instalacion de paquetes necesarios para el servidor"
yum -y install gcc libtermcap-devel gcc-c++ newt-devel mysql-connector-
odbc perl-DBD-ODBC unixODBC* libtool make e2fsprogs-devel keyutils-libs-
devel krb5-devel libogg libselinux-devel libsepol-devel libxml2-devel
libtiff-devel gmp php php-pear php-pear-DB php-gd php-mysql php-pdo
ncurses-devel audiofile-devel bison bison-devel libogg-devel gtk+* mysql-
devel zlib zlib-devel perl-DateManip iksemel* kernel-devel openssl-devel
httpd postfix cyrus-sasl-lib cyrus-sasl cyrus-sasl-plain openssl-perl
openssl-devel xmlsec1-openssl openssl openssl097a sox spandsp perl-CGI-
SpeedyCGI httpd perl-libwww-perl.noarch fontconfig freetype dejavu-lgc-
fonts.noarch lame phpmyadmin
#Descarga de los paquetes de instalacion de Asterisk
echo "Descarga de los paquetes de Asterisk"
wget http://downloads.digium.com/pub/asterisk/asterisk-1.4-current.tar.gz
sleep 2
wget http://downloads.digium.com/pub/asterisk/asterisk-addons-1.4-
current.tar.gz
sleep 2
wget http://downloads.asterisk.org/pub/telephony/dahdi-linux-
complete/dahdi-linux-complete-current.tar.gz
sleep 2
wget http://downloads.digium.com/pub/libpri/libpri-1.4-current.tar.gz
sleep 2
for pkg in *.tar.gz; do tar -xvzf $pkg; done
sleep 1
#Instalacion de Asterisk
echo "Inicio de la instalacion"
vlibpri=`tar -tf libpri-1.4-current.tar.gz | head -n 1`
echo "Se Ingresa a la carpeta" $vlibpri
cd $vlibpri
sleep 2
make
sleep 2
make install
sleep 2
```

```
echo "Saliendo de" $vlibpri
cd ..
vdahdi=`tar -tf dahdi-linux-complete-current.tar.gz | head -n 1`
echo "Se Ingresa a la carpeta" $vdahdi
cd $vdahdi
sleep 2
make
sleep 2
make install
sleep 2
make config
sleep 2
echo "Saliendo de" $vdahdi
cd ..
vasterisk=`tar -tf asterisk-1.4-current.tar.gz | head -n 1`
echo "Se Ingresa a la carpeta" $vasterisk
cd $vasterisk
sleep 2
make distclean
sleep 2
make clean
sleep 2
./configure
sleep 2
#make menuselect
#sleep 2
make
sleep 2
make install
sleep 2
make samples
sleep 2
make config
sleep 2
echo "Saliendo de" $vasterisk
cd ..
vaddons=`tar -tf asterisk-addons-1.4-current.tar.gz | head -n 1`
echo "Se ingresa a la carpeta" $vaddons
cd $vaddons
sleep 2
./configure
sleep 2
make
sleep 2
make install
sleep 2
make samples
sleep 2
echo "Saliendo de" $vaddons
cd ..
echo "Configurando el servicio para su inicio con el sistema"
chkconfig asterisk on
echo "Iniciando Asterisk"
service asterisk start
echo "Reiniciando el servidor, Instalacion completa"
sleep 1
echo "Reiniciando…"
sleep 3
reboot
```

J. DIÁLOGOS UTILIZADOS EN LA CENTRAL

Además de los mensajes propios del sistema (en español), se han utilizados estos mensajes personalizados para el sistema.

MENSAJES PERSONALIZADOS:

- Bienvenida: Bienvenido, Ud. Se ha comunicado con SACMIS, Electrónica y Telecomunicaciones.
- Menú 1: Si conoce el número de extensión, márquelo ahora, sino, espere un momento.
- Menú 2: Para Comunicarse con Ventas, presione 1; Contabilidad, presione 2 Departamento de Proyectos, presione 3; Departamento de Sistemas, presione 4, Bodega, presione 5, Para enviar un fax, presione 6. O espera en la línea, que una operadora lo atenderá.
- No-disponible: Al parecer la línea que Ud. necesita no está disponible en este momento, espere, su llamada está siendo redirigida.
- no-línea: Al parecer, las líneas están ocupadas, espere por favor, su llamada está siendo redirigida,
- Ocupado: Al parecer la línea que Ud. necesita está ocupada en este momento, espere, su llamada está siendo redirigida.
- Adiós: Gracias por llamar a SACMIS Electrónica y Telecomunicaciones, que tenga un buen día.

K. ARTÍCULOS DE LA NORMA UTILIZADOS PARA LA CREACIÓN DE LAS POLÍTICAS DEL USUARIO.

Si bien la norma utiliza sus propias divisiones y conceptualizaciones para el establecimiento del manual de seguridad, para el establecimiento de las políticas de usuario de SACMIS podría tomarse como una relación bastante vaga para ser considerada como parte de un solo apartado o dominio. La selección de los apartados que fueron considerados exhaustivamente para la creación de las políticas de seguridad de SACMIS se escogieron luego de una lectura profunda del Anexo completo, considerando todas las necesidades posibles de seguridad en función del alcance que se determinó para estas primeras políticas de seguridad.

Estos apartados son:

Política de seguridad de información
- Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes
- Documentar política de seguridad de información: La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
- Revisión de la política de seguridad de la información: La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.

Organización de la seguridad de la información:
- Asignación de responsabilidades de la seguridad de la información: Se deben definir claramente las responsabilidades de la seguridad de la información.

- Proceso de autorización para los medios de procesamiento de información: Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
- Acuerdos de confidencialidad: Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.

Responsabilidad por los activos:
- Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.
- Inventarios de activos: Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
- Propiedad de los activos: Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' de una parte designada de la organización.
- Uso aceptable de los activos: Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.

Clasificación de la información
- Objetivo: Asegurar que a información reciba un nivel de protección apropiado.
- Lineamientos de clasificación: La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.

Seguridad de los recursos humanos

Antes del empleo
- Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.

- Roles y responsabilidades: Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
- Selección: Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
- Términos y condiciones de empleo: Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información

Durante el empleo

- Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.
- Gestión de responsabilidades: La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
- Capacitación y educación en seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
- Proceso disciplinario: Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.

Terminación o cambio del empleo

- Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.

- Responsabilidades de terminación: Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.
- Devolución de activos: Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.
- Eliminación de derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.

Seguridad física y ambiental

Áreas seguras
- Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.
- Perímetro de seguridad física: Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
- Controles de entrada físicos: Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
- Seguridad de oficinas, habitaciones y medios: Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
- Protección contra amenazas externas y ambientales: Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
- Trabajo en áreas seguras: Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
- Áreas de acceso público, entrega y carga: Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar

de los medios de procesamiento de la información para evitar un acceso no autorizado.

Seguridad del equipo

- Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
- Ubicación y protección del equipo: El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
- Servicios públicos: El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
- Seguridad en el cableado: El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
- Mantenimiento de equipo: El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
- Seguridad del equipo fuera-del-local: Se debe aplicar seguridad al equipo fuera-del-local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
- Eliminación seguro o re-uso del equipo: Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.
- Traslado de Propiedad: Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.

- Segregación de deberes: Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
- Separación de los medios de desarrollo y operacionales: Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.

Planeación y aceptación del sistema

- Objetivo: Minimizar el riesgo de fallas en los sistemas.
- Gestión de capacidad: Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
- Aceptación del sistema: Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.

Respaldo (back-up)

- Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.
- Back-up o respaldo de la información: Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.

Gestión de seguridad de redes

- Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
- Controles de red: Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
- Seguridad de los servicios de red: Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.

- Seguridad de documentación del sistema: Se debe proteger la documentación de un acceso no autorizado dentro de una organización y con cualquier entidad externa.

- Procedimientos y políticas de información y software: Se deben establecer política, procedimientos y controles de intercambio formales para proteger el

intercambio de información a través del uso de todos los tipos de medios de comunicación.

- Mensajes electrónicos: Se debe proteger adecuadamente los mensajes electrónicos.

Monitoreo

-Objetivo: Detectar actividades de procesamiento de información no autorizadas.

- Registro de auditoría: Se deben producir registros de las actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.

- Uso del sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.

- Protección de la información del registro: Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.

-Registros del administrador y operador: Se deben registrar las actividades del administrador y operador del sistema.

- Registro de fallas: Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.

- Sincronización de relojes: Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.

Control de acceso

Requerimiento comercial para el control del acceso

- Objetivo: Controlar acceso a la información

- Política de control de acceso: Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.

- Gestión de la clave del usuario: La asignación de claves se debe controlar a través de un proceso de gestión formal.

Responsabilidades del usuario
- Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.
- Uso de clave: Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.

- Política sobre el uso de servicios en red: Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
- Autenticación del usuario para conexiones externas: Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.

- Control de conexión de redes: Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales

- Sistema de gestión de claves: Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.

- Aislamiento del sistema sensible: Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).

- Computación móvil y comunicaciones: Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.

- Análisis y especificación de los requerimientos de seguridad: Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.

- Análisis y especificación de los requerimientos de seguridad: Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.

- Control de software operacional: Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.

- Control de acceso al código fuente del programa: Se debe restringir el acceso al código fuente del programa.

- Revisión técnica de las aplicaciones después de cambios en el sistema operativo: Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
- Restricciones sobre los cambios en los paquetes de software: No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
- Filtración de información: Se deben evitar las oportunidades de filtraciones en la información.

- Control de vulnerabilidades técnicas: Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.

- Identificación de legislación aplicable: Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.

- Protección de data y privacidad de información personal: Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.

- Prevención de mal uso de medios de procesamiento de información: Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.

- Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.
- Cumplimiento con las políticas y estándares de seguridad: Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
- Chequeo de cumplimiento técnico: Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.

L. ANÁLISIS DE PAQUETES SIP Y RTP EN UNA COMUNICACIÓN VOIP PARA TELEFONÍA [32]

El protocolo SIP para el envío de mensajes a través de la red, hace uso de un paquete similar al utilizado por SMTP, que se compone de mensajes que son leídos por el servidor.

El protocolo SIP contiene un encabezado primario que indica si el mismo es petición o respuesta, además de encabezados secundarios, con diferentes campos, como direcciones, dominios y datos encriptados propios del sistema. El cuerpo del mensaje comúnmente va vacío, a menos que se comience una petición de llamada, en cuyo caso se lo utiliza bajo el formato del protocolo SDP.

L.1. SOLICITUD DE REGISTRO:

Cuando el cliente (192.168.1.144) necesita conectarse con el servidor (192.168.0.12) envía un paquete de este tipo[1]:

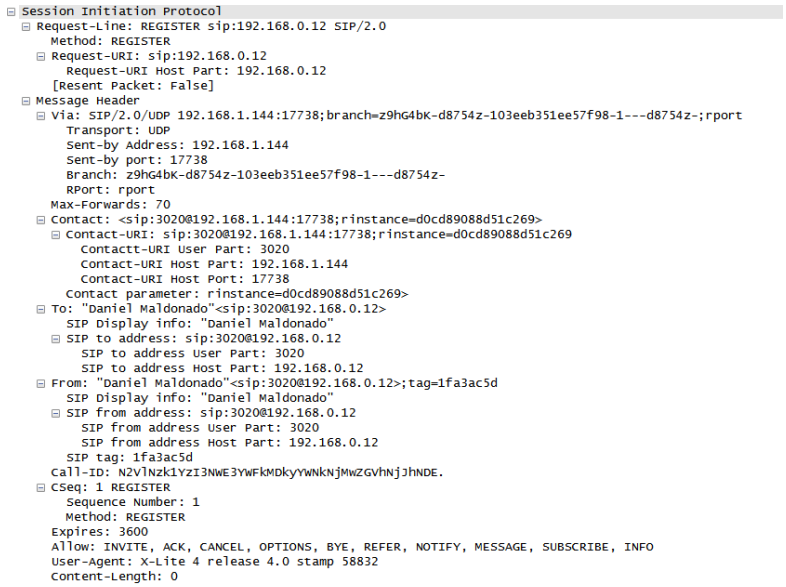


Figura L.1.a. Solicitud de registro del cliente

[1] Todos estos mensajes van encapsulados en tramas UDP normales, que a su vez están encapsuladas en paquetes IP y a su vez en tramas Ethernet para su envío.

En la figura L.1.a. se observa que la línea principal especifica el tipo de mensaje que se está enviando, y el método que se usará para leer el mensaje; mientras que la cabecera del paquete contiene varios campos en los que se especifican:

- Protocolo de transmisión, dirección de origen y puerto de origen del mensaje, además de reportes
- Dirección de origen del mensaje, tal como va a ser recibida por la central
- Dirección de recepción del mensaje, tal y como será leída por la central
- Número de secuencia del mensaje enviado, así como los mensajes permitidos y el nombre de la UA con la que se está haciendo contacto, el tiempo de expiración del mensaje

Luego de estos valores va el cuerpo del mensaje, que en este caso va vacio.

Figura L.1.b. Mensaje intermedio del servidor de intento de conexión

A partir de que la comunicación se ha establecido, en un registro solo cambian los valores del primer campo de la cabecera. Como el registro se realiza con autenticación, la central impide el mismo al primer intento, ya que el primer paquete enviado por el cliente no contiene la contraseña encriptada de registro, sino simplemente un pedido de registro, como se muestra en la figura L.1.c.

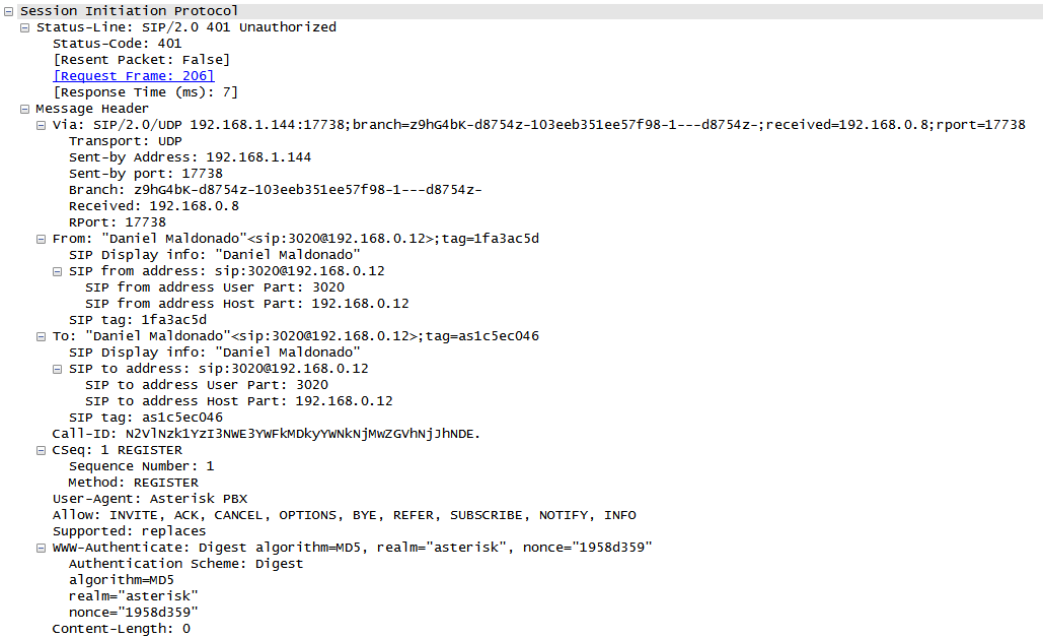


Figura L.1.c. Mensaje de desautorización del Servidor por falta de parámetros de inicio

En esta figura se añade un quinto y sexto campos al mensaje SIP, uno de ellos se añade luego del campo de protocolos y que especifica la dirección asignada al cliente dentro del servidor, para que los demás clientes puedan encontrarlo y realizar llamadas, conocido como el Contact-URL. El sexto campo agregado al final de la cabecera contiene los valores de autenticación necesarios para dar como válido el registro del cliente en la central. Una vez que el servidor ha enviado el mensaje de desautorización, el nuevo mensaje de solicitud de registro contendrá este quinto campo (figura L.1.d.), llamado Authorization, en el cual se especifican nombres, nounces, contraseñas y algoritmos necesarios para el registro.

Figura L.1.d. Reenvío de mensaje de registro del cliente con los parámetros de inicio

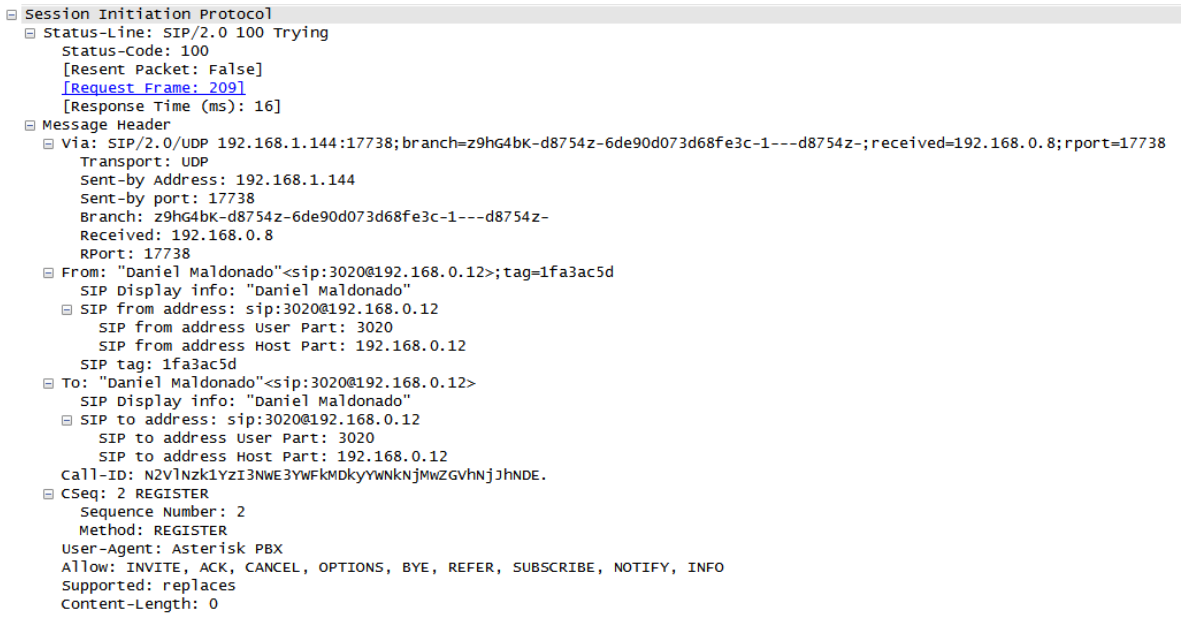


Figura L.1.e. Mensaje intermedio del servidor de intento de conexión

Antes de dar paso al registro como tal, la central envía un mensaje que le dice al cliente que su solicitud está siendo atendida, para que el cliente no pierda el hilo de comunicación (figura L.1.e.).

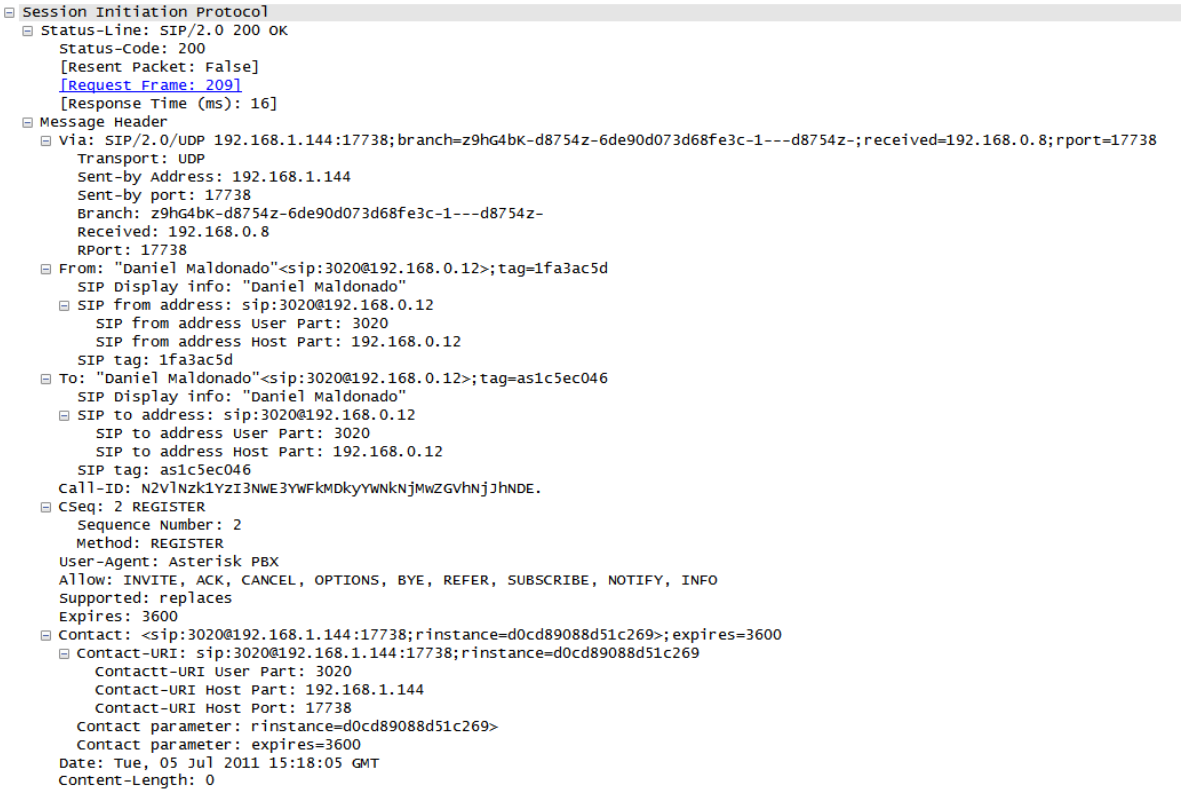


Figura L.1.f. Mensaje de aprobación de registro del servidor.

Finalmente la central envía el mensaje 200/OK al cliente (figura L.1.f.), con lo cual el cliente ha quedado registrado de manera satisfactoria en la central. En este mensaje se sustituye el campo de Autenticación por el de datos de Contacto, para especificar la dirección a la cual responderá el cliente de ahora en adelante

L.2. REALIZACIÓN DE UNA LLAMADA; ACCESO VÍA TELÉFONO AL SERVICIO DE VOICEMAIL:

Cuando se va a iniciar una llamada, el cliente envía la petición INVITE en la línea inicial del paquete, indicando el Contatc-URI del destino de la llamada; además de que en el campo de Contacto donde se especifica el Contac-URI de la parte que solicita la comunicación y los campos conocidos de Origen, Destino y valores de secuencia.

En estos paquetes SIP, el cuerpo del mensaje contiene los valores del protocolo SDP (RFC 2327) que especifican los valores con los cuales la llamada será

establecida, según los protocolos y códecs de los cuales dispone cada parte para comunicarse.

Los valores que SDP puede tomar son:

Descripción de la sesión

v= (Versión del protocolo)

o= (Origen e identificador de sesión)

s= (Nombre de sesión)

i=* (Información de la sesión)

u=* (URI de descripción)

e=* (Correo electrónico)

p=* (Número telefónico)

c=* (Información de conexión)

b=* (Cero o más líneas con información de ancho de banda)

Una o más líneas de descripción de tiempo (Ver abajo "t=" y "r=")

z=* (Ajustes de zona horaria)

k=* (Clave de cifrado)

a=* (Cero o más líneas de atributos de sesión)

Cero o más descripciones de medios

Descripción de tiempo

t= (Tiempo durante el cual la sesión estará activa)

r=* (Cero o más veces de repetición)

Descripción de medios, si está presente

m= (Nombre de medio y dirección de transporte)

i=* (Título)

c=* (Información de conexión)

b=* (Cero o más líneas con información de ancho de banda)

k=* (Clave de cifrado)

a=* (Cero o más líneas de atributos de sesión)

En los cuales el sistema se basara para negociar la comunicación, tal como establece la figura L.2.a.

```
Session Initiation Protocol
  Request-Line: INVITE sip:*333@192.168.0.12 SIP/2.0
    Method: INVITE
    Request-URI: sip:*333@192.168.0.12
      Request-URI User Part: *333
      Request-URI Host Part: 192.168.0.12
    [Resent Packet: False]
  Message Header
    Via: SIP/2.0/UDP 192.168.1.144:17738;branch=z9hG4bK-d8754z-db15b166ce91283c-1---d8754z-;rport
      Transport: UDP
      Sent-by Address: 192.168.1.144
      Sent-by port: 17738
      Branch: z9hG4bK-d8754z-db15b166ce91283c-1---d8754z-
      RPort: rport
    Max-Forwards: 70
    Contact: <sip:3020@192.168.0.8:17738>
      Contact-URI: sip:3020@192.168.0.8:17738
        Contactt-URI User Part: 3020
        Contact-URI Host Part: 192.168.0.8
        Contact-URI Host Port: 17738
    To: <sip:*333@192.168.0.12>
      SIP to address: sip:*333@192.168.0.12
        SIP to address User Part: *333
        SIP to address Host Part: 192.168.0.12
    From: "Daniel Maldonado"<sip:3020@192.168.0.12>;tag=b6ffdd11
      SIP Display info: "Daniel Maldonado"
      SIP from address: sip:3020@192.168.0.12
        SIP from address User Part: 3020
        SIP from address Host Part: 192.168.0.12
      SIP tag: b6ffdd11
    Call-ID: MGZhOWEzNTc5N2MxY2FjODZmYmE5M2JhMTY5MDgwY2E.
    CSeq: 1 INVITE
      Sequence Number: 1
      Method: INVITE
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
    Content-Type: application/sdp
    Supported: replaces
    User-Agent: X-Lite 4 release 4.0 stamp 58832
    Content-Length: 410
  Message Body
    Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): - 12954352868908260 1 IN IP4 192.168.1.144
        Owner Username: -
        Session ID: 12954352868908260
        Session Version: 1
        Owner Network Type: IN
        Owner Address Type: IP4
        Owner Address: 192.168.1.144
      Session Name (s): CounterPath X-Lite 4.0
      Connection Information (c): IN IP4 192.168.1.144
        Connection Network Type: IN
        Connection Address Type: IP4
        Connection Address: 192.168.1.144
      Time Description, active time (t): 0 0
        Session Start Time: 0
        Session Stop Time: 0
      Session Attribute (a): ice-ufrag:420b5b
        Session Attribute Fieldname: ice-ufrag
        Session Attribute Value: 420b5b
      Session Attribute (a): ice-pwd:67390524f33dd59efe64ea6ee72d3076
        Session Attribute Fieldname: ice-pwd
        Session Attribute Value: 67390524f33dd59efe64ea6ee72d3076
      Media Description, name and address (m): audio 59304 RTP/AVP 107 0 8 101
        Media Type: audio
        Media Port: 59304
        Media Protocol: RTP/AVP
        Media Format: DynamicRTP-Type-107
        Media Format: ITU-T G.711 PCMU
        Media Format: ITU-T G.711 PCMA
        Media Format: DynamicRTP-Type-101
      Media Attribute (a): rtpmap:107 BV32/16000
        Media Attribute Fieldname: rtpmap
        Media Format: 107
        MIME Type: BV32
        Sample Rate: 16000
      Media Attribute (a): rtpmap:101 telephone-event/8000
        Media Attribute Fieldname: rtpmap
        Media Format: 101
        MIME Type: telephone-event
        Sample Rate: 8000
      Media Attribute (a): fmtp:101 0-15
        Media Attribute Fieldname: fmtp
        Media Format: 101 [telephone-event]
        Media format specific parameters: 0-15
      Media Attribute (a): sendrecv
      Media Attribute (a): candidate:1 1 UDP 659136 192.168.1.144 59304 typ host
        Media Attribute Fieldname: candidate
        Media Attribute Value: 1 1 UDP 659136 192.168.1.144 59304 typ host
      Media Attribute (a): candidate:1 2 UDP 659134 192.168.1.144 59305 typ host
        Media Attribute Fieldname: candidate
        Media Attribute Value: 1 2 UDP 659134 192.168.1.144 59305 typ host
```

Figura L.2.a. Mensaje de invitación a establecimiento de llamada, adjuntando los parámetros posibles de establecimiento

En este ejemplo, el cliente establece la comunicación con el servidor para acceder a los servicios de voicemail; sin embargo, el sistema de comunicación se da de la misma manera entre dos clientes. Antes de establecer la comunicación el servidor solicita al cliente que envía el paquete INVITE se identifique con el servidor, especificando su nombre de usuario, contraseñas, algoritmos de encripción y nounces, para comprobar que el cliente es legítimo (figura L.2.b.), tras lo cual el cliente vuelve a enviar el paquete INVITE con los valores solicitados en los campos específicos, para que la comunicación pueda establecerse (figura L.2.d)

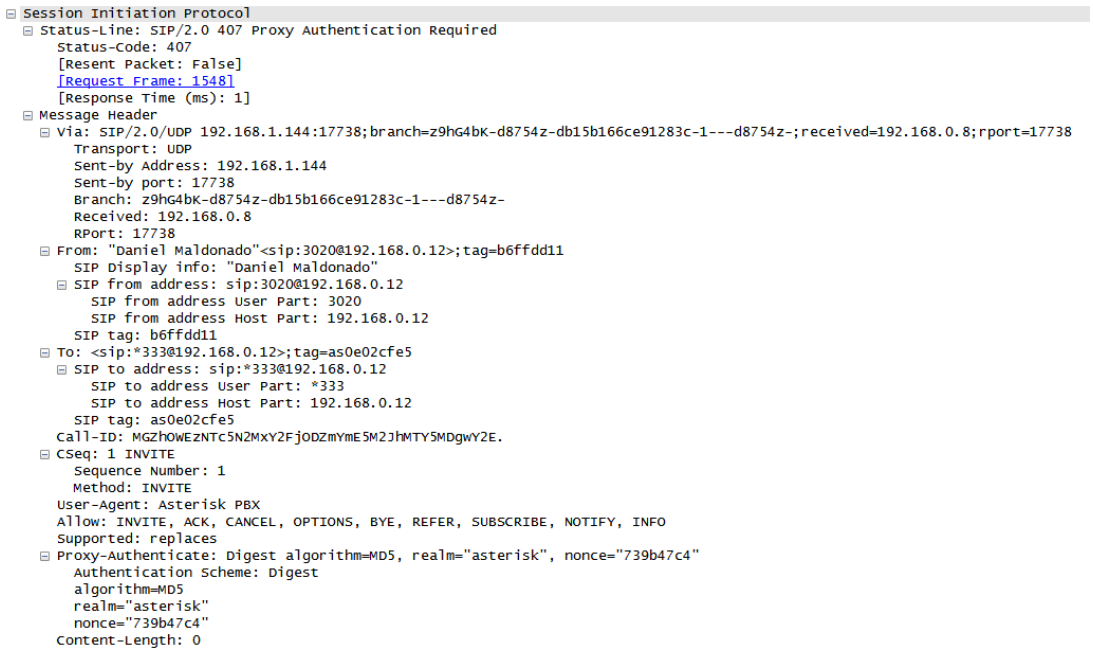


Figura L.2.b. Solicitud del servidor de autenticación para el establecimiento de la llamada

El cliente tanto al recibir el mensaje de autenticación como el mensaje de 200/OK, envía un ACK de confirmación al servidor de que los mensajes fueron recibidos satisfactoriamente. Estos mensajes solo contienen los campos básicos de origen y destino, además de la secuencia (figuras L.2.c. y L.2.j.)

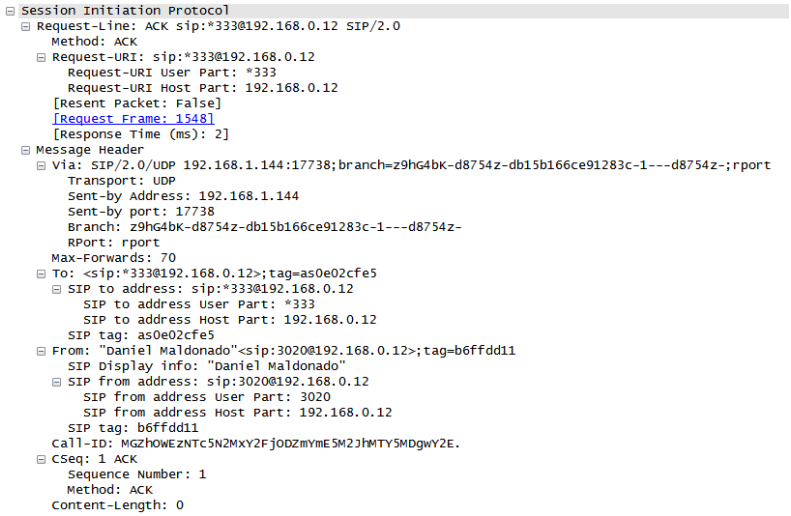


Figura L.2.c. ACK de la solicitud enviado por el cliente

Figura L.2.d.Envío de nueva solicitud de establecimiento de llamada adjuntando valores de autenticación al servidor

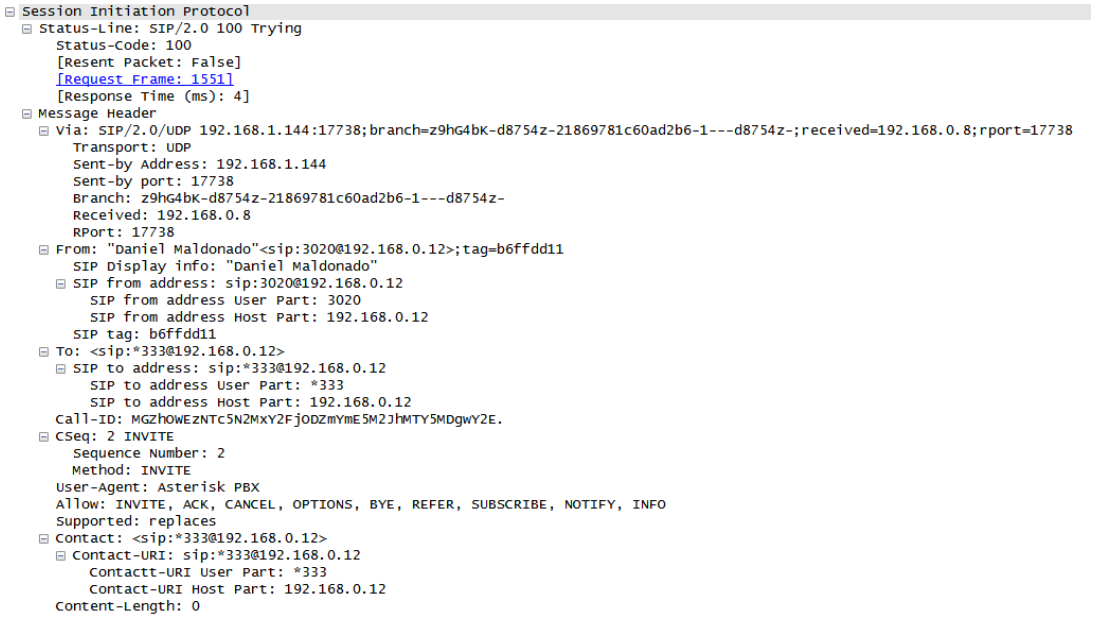


Figura L.2.e. Mensaje intermedio del servidor de intento de conexión

El servidor siempre envía, entre comunicaciones, un paquete TRYING para informarle al servidor que la solicitud está siendo procesada, para que no se pierda el hilo de comunicación (figura L.2.e.). Los mensajes INVITE anteriores contenían en los campos del protocolo SDP todos los valores posibles con los cuales se puede iniciar una comunicación, como por ejemplo todos los códecs que su cliente soporta (para el caso PCMU y PCMA); en el paquete 200/OK, los campos del paquete SDP ya especifican todos los valores negociados por las partes, para que la comunicación se dé en las mismas condiciones (figura L.2.f.)

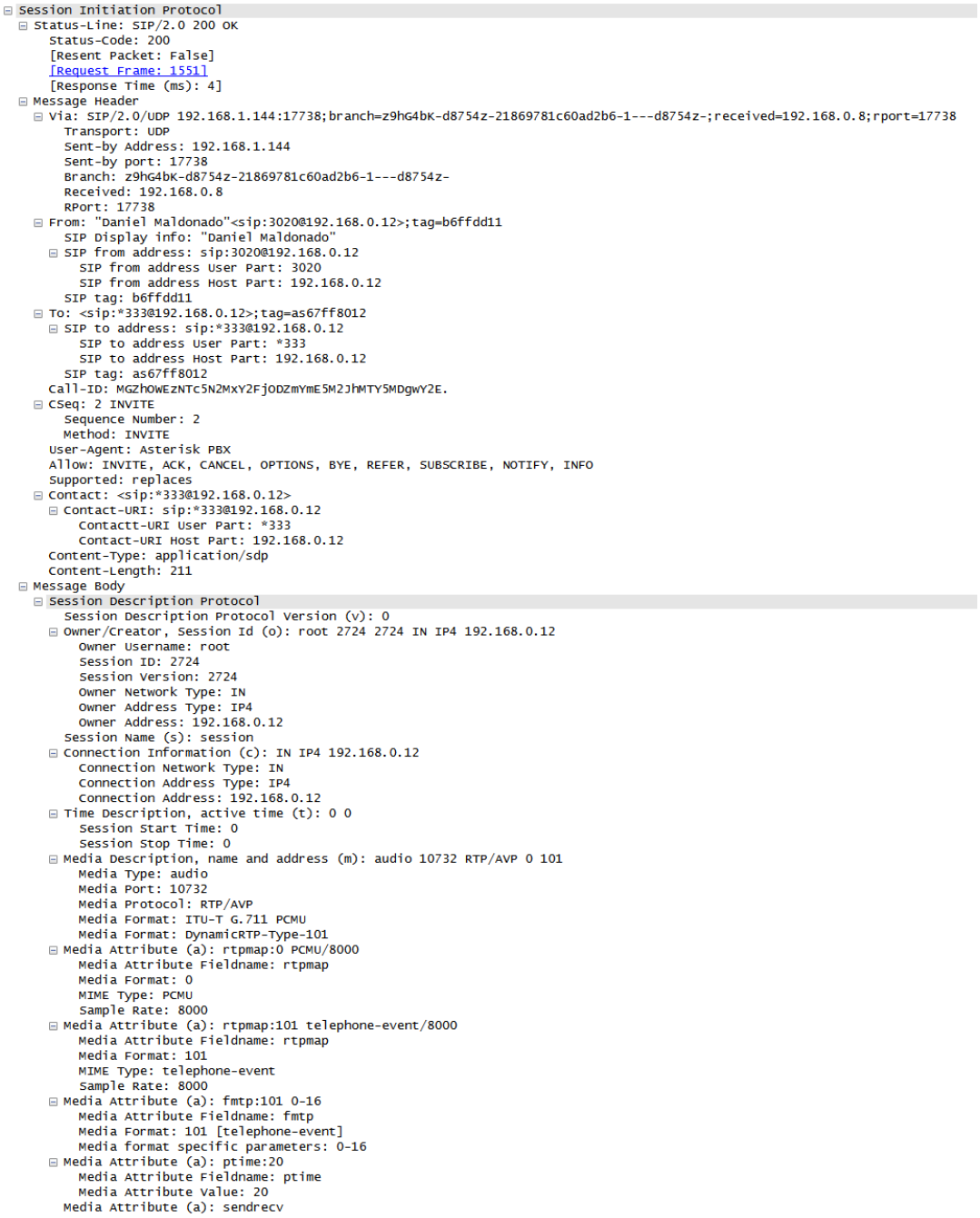


Figura L.2.f. Mensaje del servidor de aceptación de la solicitud de llamada, con los valores se sesión establecidos.

A partir de este punto, se transmiten únicamente paquetes RTP de comunicación, los cuales se ejemplifican en las figuras L.2.g., L.2.h. y L.2.i.

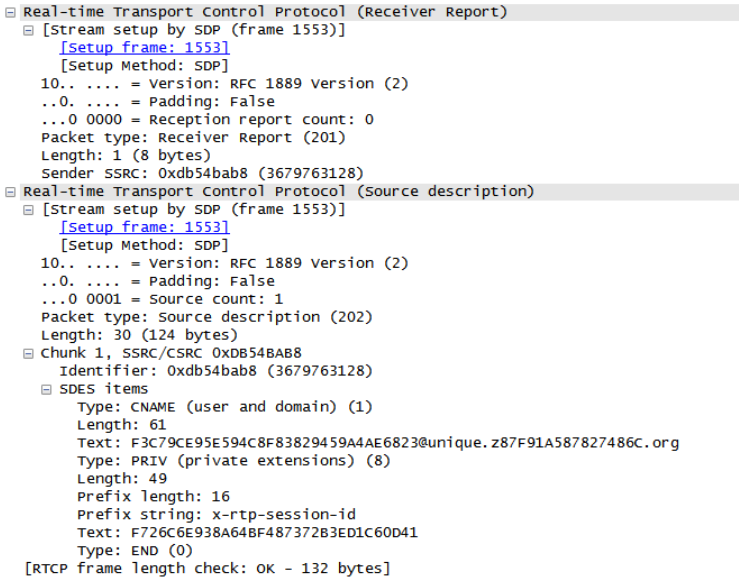


Figura L.2.g. Reportes de envío y recepción de paquetes RTP entre cliente y servidor

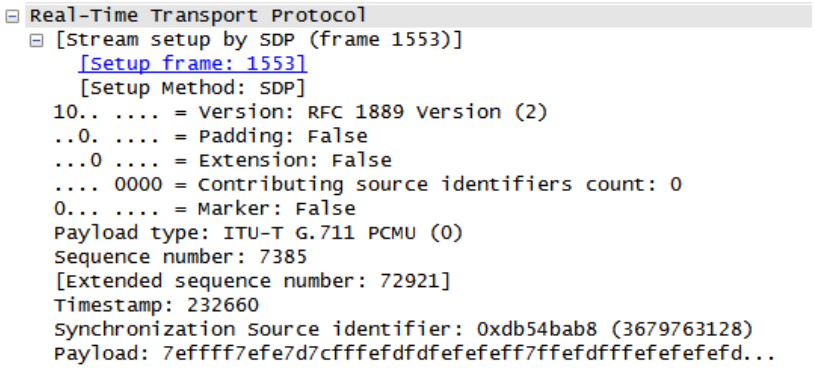


Figura L.2.h. Mensaje RTP en sentido cliente-servidor

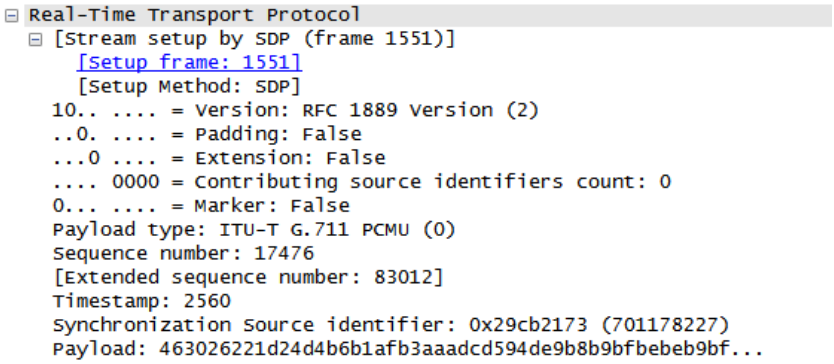


Figura L.2.i.Mensaje RTP en sentido servidor-cliente

Figura L.2.j. ACK de confirmación de comunicación por parte del cliente

Cuando un cliente (en este caso el servidor a una orden del cliente de finalización de la comunicación) quiere finalizar la comunicación, envía al servidor un mensaje BYE, este mensaje no es necesario que envíe la autenticación correspondiente, ya que el enlace ya ha sido efectuado, por lo que solo tiene que cancelarlo. En este mensaje, en la cabecera, se añaden dos campos con valores propios del sistema Asterisk que le indican al sistema cual es la causa del envío de BYE, para monitorear si la llamada ha sido cancelada por el usuario o por agentes externos, o a su vez por fallas en la comunicación (figura L.2.L.).

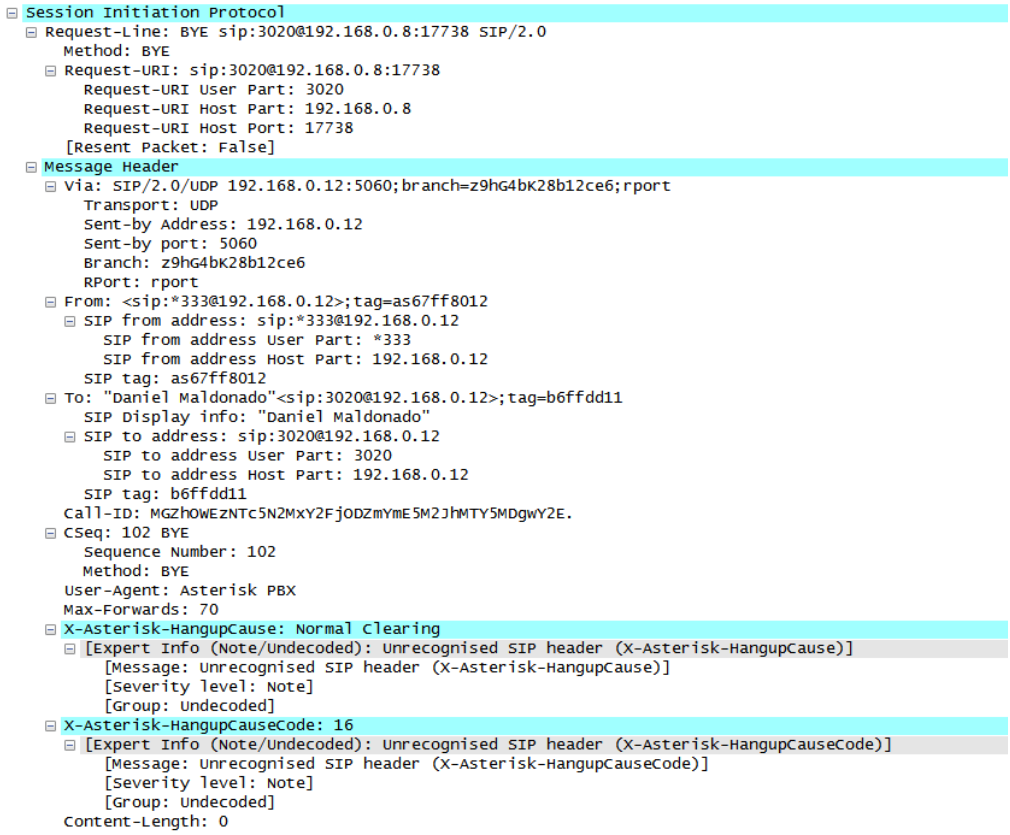


Figura L.2.L. Envío por parte del servidor del mensaje de finalización de la comunicación

A una petición de BYE, el cliente no tiene más opción que enviar un mensaje 200/OK, ya que la una parte ha finalizado la comunicación (figura L.2.l.).

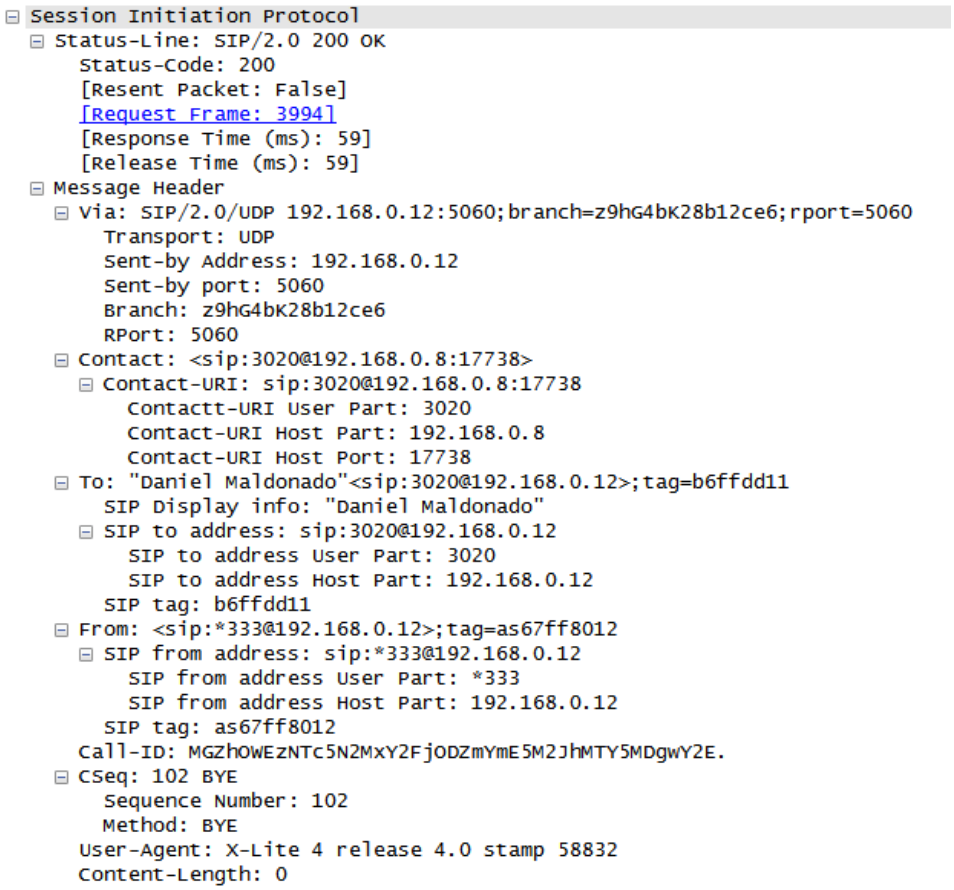
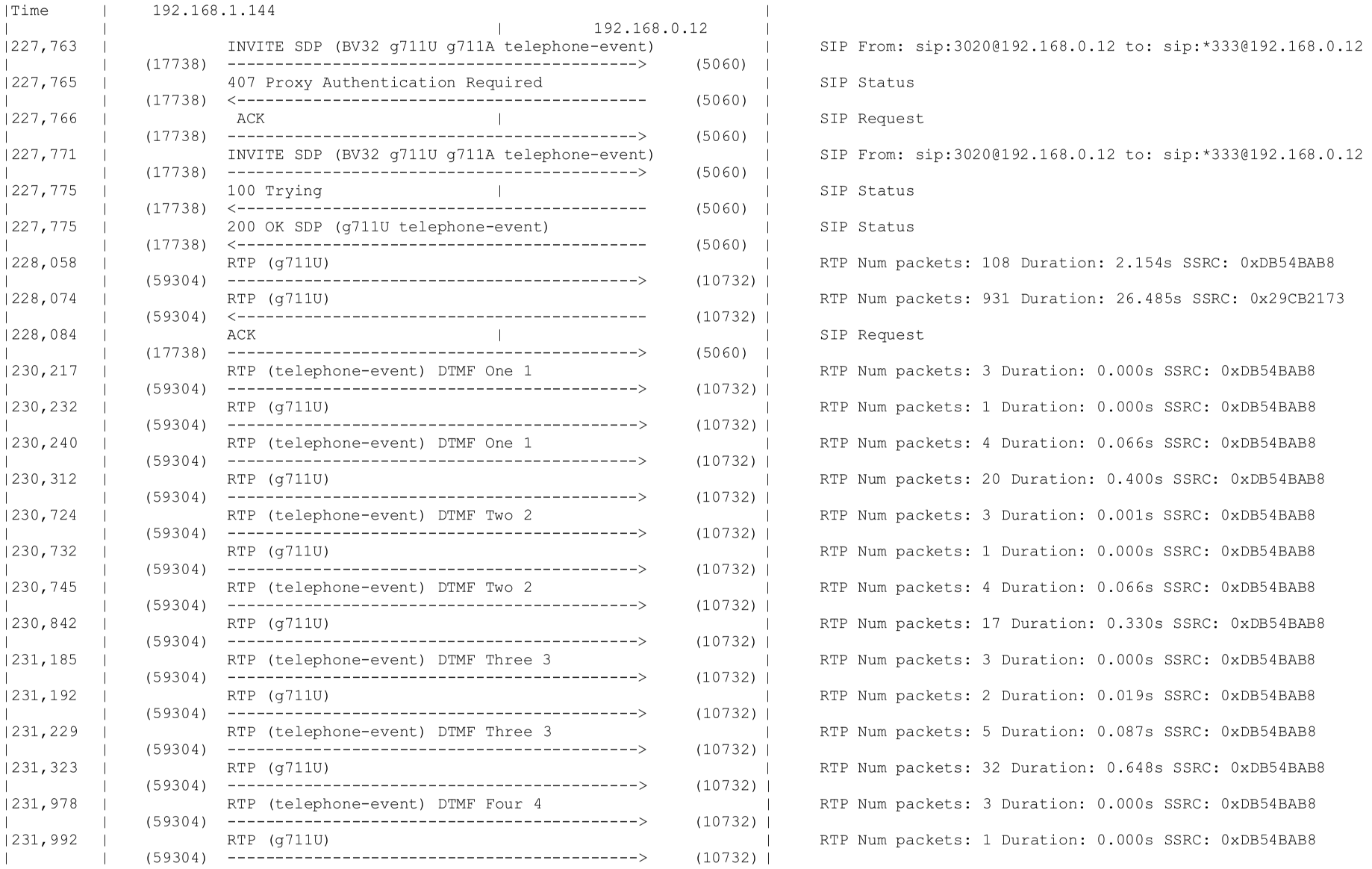
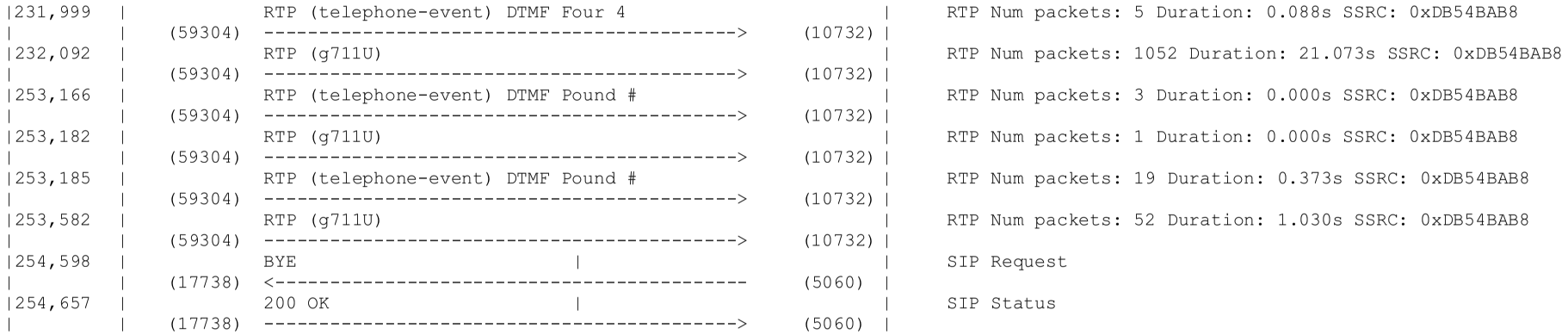


Figura L.2.I. Mensaje de aceptación de finalización enviado por el cliente.

El siguiente esquema ejemplifica de una manera gráfica como se da la transmisión de paquetes entre el cliente y el servidor, especificando los puertos que se utilizan, tanto para la transmisión de paquetes SIP como para la transmisión de paquetes RTP.


Time
192.168.1.144
192.168.0.12
227,763 INVITE SDP (BV32 g711U g711A telephone-event) SIP From: sip:3020@192.168.0.12 to: sip:*333@192.168.0.12
(17738) (5060)
227,765 407 Proxy Authentication Required SIP Status
227,766 ACK SIP Request
227,771 INVITE SDP (BV32 g711U g711A telephone-event) SIP From: sip:3020@192.168.0.12 to: sip:*333@192.168.0.12
227,775 100 Trying SIP Status
227,775 200 OK SDP (g711U telephone-event) SIP Status
228,058 RTP (g711U) RTP Num packets: 108 Duration: 2.154s SSRC: 0xDB54BAB8
(59304) (10732)
228,074 RTP (g711U) RTP Num packets: 931 Duration: 26.485s SSRC: 0x29CB2173
228,084 ACK SIP Request
230,217 RTP (telephone-event) DTMF One 1 RTP Num packets: 3 Duration: 0.000s SSRC: 0xDB54BAB8
230,232 RTP (g711U) RTP Num packets: 1 Duration: 0.000s SSRC: 0xDB54BAB8
230,240 RTP (telephone-event) DTMF One 1 RTP Num packets: 4 Duration: 0.066s SSRC: 0xDB54BAB8
230,312 RTP (g711U) RTP Num packets: 20 Duration: 0.400s SSRC: 0xDB54BAB8
230,724 RTP (telephone-event) DTMF Two 2 RTP Num packets: 3 Duration: 0.001s SSRC: 0xDB54BAB8
230,732 RTP (g711U) RTP Num packets: 1 Duration: 0.000s SSRC: 0xDB54BAB8
230,745 RTP (telephone-event) DTMF Two 2 RTP Num packets: 4 Duration: 0.066s SSRC: 0xDB54BAB8
230,842 RTP (g711U) RTP Num packets: 17 Duration: 0.330s SSRC: 0xDB54BAB8
231,185 RTP (telephone-event) DTMF Three 3 RTP Num packets: 3 Duration: 0.000s SSRC: 0xDB54BAB8
231,192 RTP (g711U) RTP Num packets: 2 Duration: 0.019s SSRC: 0xDB54BAB8
231,229 RTP (telephone-event) DTMF Three 3 RTP Num packets: 5 Duration: 0.087s SSRC: 0xDB54BAB8
231,323 RTP (g711U) RTP Num packets: 32 Duration: 0.648s SSRC: 0xDB54BAB8
231,978 RTP (telephone-event) DTMF Four 4 RTP Num packets: 3 Duration: 0.000s SSRC: 0xDB54BAB8
231,992 RTP (g711U) RTP Num packets: 1 Duration: 0.000s SSRC: 0xDB54BAB8


231,999
RTP (telephone-event) DTMF Four 4
(59304)
(10732)
RTP Num packets: 5 Duration: 0.088s SSRC: 0xDB54BAB8
232,092
RTP (g711U)
(59304)
(10732)
RTP Num packets: 1052 Duration: 21.073s SSRC: 0xDB54BAB8
253,166
RTP (telephone-event) DTMF Pound #
(59304)
(10732)
RTP Num packets: 3 Duration: 0.000s SSRC: 0xDB54BAB8
253,182
RTP (g711U)
(59304)
(10732)
RTP Num packets: 1 Duration: 0.000s SSRC: 0xDB54BAB8
253,185
RTP (telephone-event) DTMF Pound #
(59304)
(10732)
RTP Num packets: 19 Duration: 0.373s SSRC: 0xDB54BAB8
253,582
RTP (g711U)
(59304)
(10732)
RTP Num packets: 52 Duration: 1.030s SSRC: 0xDB54BAB8
254,598
BYE
(17738)
(5060)
SIP Request
254,657
200 OK
(17738)
(5060)
SIP Status