Denwa UC&C 4.0.1

- Manual de Uso

Versión: 46

Manual de instalación, configuración y uso de Denwa UC&C 4.0.1

Revisado por: Nicolás Saravia Vivas
Córdoba, Argentina - 24 de junio de 2021
Páginas Totales: 243
Área de Ingeniería
Denwa Technology Corp.
GlobalThink Technology S.A.

Denwa UC&C 4.0.1

Manual de Uso

Área de Ingeniería
GlobalThink Technology S.A.
Córdoba, Argentina - 24 de junio de 2021
Versión: 46

Marcas

GlobalThink Technology y **Denwa** son marcas registradas por **Global Think Technology S.A.**, Córdoba, Argentina. Otras marcas utilizadas en este documento son propiedad de sus respectivos dueños.

Versión

Manual de instalación, configuración y uso de Denwa UC&C 4.0.1

Revisión: 46
Fecha: 24 de junio de 2021

Información de la Empresa

SALES OFFICE
1000 N.W. 57th Court Suite 1040
Miami, FL 33126 (Blue Lagoon)

I+D Department
Humberto Primo 843 Piso 6
X5000FAQ - Córdoba, Argentina

Argentina: +54 (11) 5129 6905 +54 (351) 571 6300
USA: +1 (305) 433 6166 +1 (305) 5872453
Ecuador: +593 4 390 1463
Chile: +56 (22) 938 1742

Sección 1

Información del documento

1.1. Propósito

El propósito del presente documento es el proporcionar información necesaria para la correcta configuración de **Denwa UC&C 4.0.1** .

1.2. Alcance

La documentación aquí proporcionada puede ser utilizada en cualquiera de las versiones del sistema Denwa UC&C, esto exceptúa al dispositivo denominado como Denwa SOHO, así como a los Gateways de Telefonía y SoftSwitches.

1.3. Simbología

En caso de ser necesario se utilizará la siguiente simbología, a fin de facilitar la comprensión del contenido:

- Recuadros: Su propósito es el incluir una nota informativa respecto a la funcionalidad específica que se esté desarrollando en el texto, puede poseer distintos 4 niveles de importancia:
  - **Informativo**: Color gris.

    Ejemplo de cuadro gris

    Contenido informativo

  - **Bajo**: Color verde. Puede afectar a los usuarios de la plataforma.

    Ejemplo de cuadro verde

    Puede afectar a los usuarios de la plataforma.

  - **Medio**: Color amarillo. Puede afectar la operación del cliente.

    Ejemplo de cuadro amarillo

    Puede afectar la operación del cliente.

  - **Alto**: Color rojo. Puede afectar la operación de toda la plataforma.

Ejemplo de cuadro rojo

Puede afectar la operación de toda la plataforma.

- **Transcripción**: Entre brackets. Transcripción de un documento externo

Nombre o ubicación del documento a citar

Contenido
Continúa el contenido

- **Consola o archivo de sistema**: En recuadro con líneas numeradas

```
1 Visualización de la consola
2 o contenido de algún archivo del sistema
```

- Tipografías: Se emplean tipografías específicas para referirse a botones, texto y distintos elementos de la interfaz de usuario.

Apartado I

Preparativos

Sección 2

Proceso de instalación

Actualmente existen dos (2) archivos de ISO para la instalación de Denwa UC&C 4.0.1 , los cuales fueron diseñados para ambientes completamente diferentes:

- Instalación común, con conexión directa a la Internet.
- Instalación en un ambiente cerrado, con repositorios locales o alcanzables por medio de la red MAN del distribuidor.

En cualquiera de los ambientes, el proceso de instalación es el mismo, con la única salvedad de que será necesario declarar el servidor que opera como Proxy de Aplicaciones o Repositorio.

Sin embargo, sin importar el entorno en el que se fuere a realizar la instalación, se requerirá conocer previamente el número de la licencia de instalación y el de la licencia de activación.

Obtención de licencias

En caso de no conocer el número de las licencias de instalación y/o activación, estos pueden ser solicitados al área de Soporte de Denwa Technology Corp. , proporcionando el número de serie del equipo en el cual se realizará la instalación.

2.1. Archivos ISO disponibles

Al momento de publicar este manual, las versiones liberadas de estos archivos ISO se encuentran disponibles en los siguientes enlaces:

- **Con conexión a internet:** `http://dendown.denwaip.com/dendown/downloads/src/DenwaUC-4.0.1.20200212.iso`
- **Por medio de Proxy:** `http://dendown.denwaip.com/dendown/downloads/src/DenwaUC-4.0.1.20200903-TECO-proxy.iso`

2.2. Disponibilización a USB

Una vez descargado el archivo ISO adecuado al entorno en el cual se encuentra el equipo a instalar, es necesario disponer de el software apropiado para su traspaso a un dispositivo de almacenamiento USB, esto puede variar según el sistema operativo del computador que se utilice.

2.2.1. Linux

2.2.1.1. Modo GUI

2.2.1.1.1. Basado en Debian En el caso de sistemas operativos basados en Debian, tales como: Ubuntu, Deepin, Linux Min, Kali Linux, SteamOS y similares; es posible utilizar la aplicación ***Startup Disk Creator***, en caso de no encontrarse en el sistema, es posible instalarla desde la Terminal mediante el siguiente comando:

```
apt install usb-creator-gtk
```

Una vez instalada, la puede localizar tecleando las palabras "Crear disco de arranque" o «*Create Startup Disk*» en el menú de actividades de GNOME, o en el menú de inicio de la distribución que esté utilizando.

Una vez abierta la aplicación, verá que la interfaz es realmente sencilla. De hecho, el procedimiento se explica prácticamente solo. Posee dos apartados, uno en el que deberás seleccionar la imagen ISO que quiere grabar, y otra en la que se indica el dispositivo USB.

Lo primero es seleccionar la imagen ISO; para ello, debajo de la caja de imagen de disco de origen, debe hacer clic en el botón Ötro...", esto abrirá el explorador de archivos y le permitirá localizar y seleccionar el fichero.

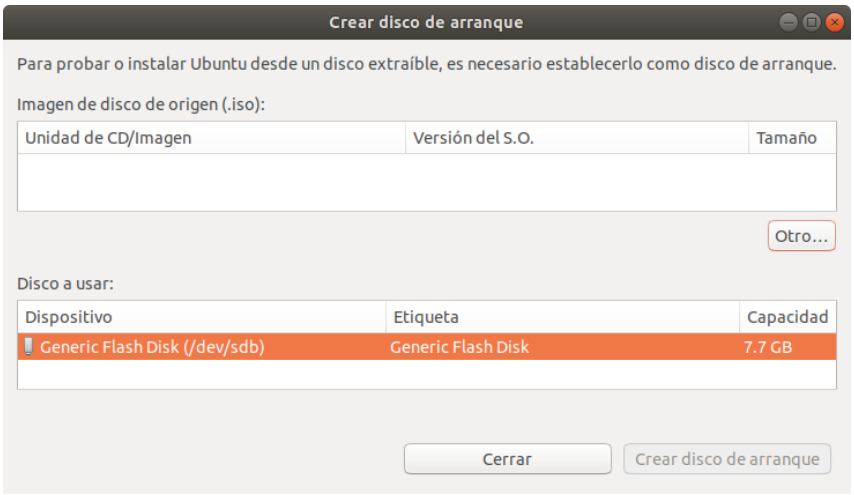

Figura 2.1: Interfaz del Creador de Discos de Arranque

Una vez seleccionada la imagen a quemar, el siguiente paso es seleccionar el dispositivo a utilizar. Ahí debe seleccionar el dispositivo USB que desea que le sirva como disco de arranque (previamente debe estar conectado)

En caso de visualizar varios dispositivos, debe tener más de un volumen conectado a su sistema a través de un puerto USB; por lo que deberá seleccionar el adecuado y listo. Tenga en cuenta que este procedimiento borrará todo el contenido que se encontraba anteriormente en el dispositivo.

Hecho esto, tan solo queda marcar el botón de «Crear disco de arranque» para que empiece el proceso de grabar la imagen y preparar el volumen.

En cuestión de unos minutos (dependiendo de la velocidad del puerto y el tipo de dispositivo USB seleccionado) deberá tener preparado el USB de arranque con el instalador de Denwa UC&C 4.0.1

2.2.2. Windows

En nuestro caso, recomendamos el uso de Rufus para la creación de discos de inicio. Para descargar Rufus, puede ir a la página oficial del proyecto (`https://rufus.ie`) y descender un poco hasta el apartado de descagas. Ahí verá que tiene principalmente dos opciones: instalable o portable.

El uso de Rufus es realmente muy simple. Una vez abierta la aplicación (si te has descargado la versión portable, tan solo debes ejecutar el fichero descargado) verás una ventana con varias opciones.

El primer paso es seleccionar el dispositivo USB. En un cuadro desplegable se listarán todos los dispositivos USB conectados a su sistema. Debs asegurar bien la elección, dado que en el proceso se borrarán todos los datos contenidos en él. En la imagen que se muestra a continuación, se ha seleccionado un dispositivo de 8 GB, en el que previamente se encontraba grabada una imagen de Ubuntu 18.04 LTS.

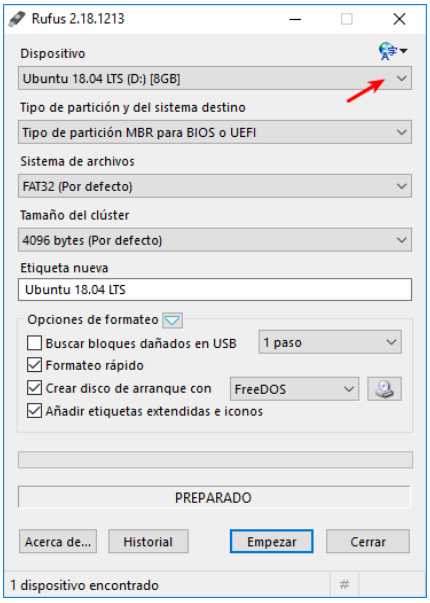

Figura 2.2: Interfaz de Rufus

No es necesario formatear previamente del dispositivo seleccionado, ya que Rufus ya formatea la unidad, previamente a crear el nuevo disco de arranque. Incluso, en opciones de formateo, se encuentra marcada la casilla de formateo rápida.

Hecho esto, el siguiente paso es seleccionar la imagen de Denwa UC&C 4.0.1 (no olvides comprobar su integridad antes), para generar el disco de arranque. Para ello, tiene que pulsar sobre el botón señalado en la siguiente imagen.

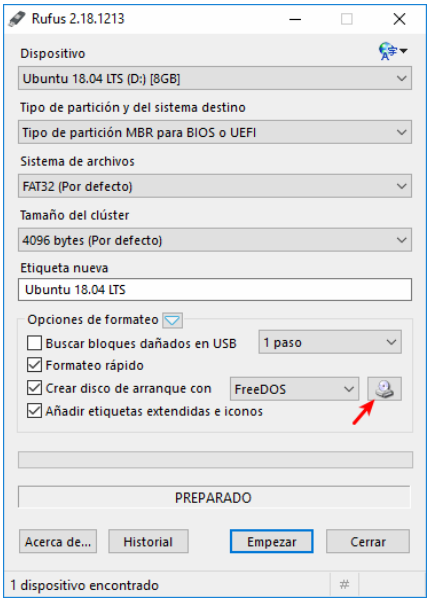

Figura 2.3: Interfaz de Rufus: Selección de ISO

Al seleccionar la imagen, hay varias opciones que cambian de acuerdo a la configuración más adecuada. Puede modificar algunas opciones, como la etiqueta del volumen, pero lo

mejor es dejar todas las opciones tal y como se encuentran por defecto iniciar con el proceso.

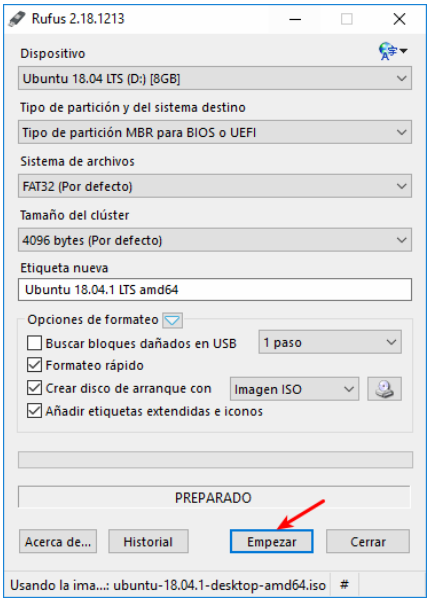

Figura 2.4: Interfaz de Rufus: Inicio de la grabación

Una vez finalizado el proceso, el dispositivo USB se encuentra listo para utilizarse en la instalación de Denwa UC&C 4.0.1 .

2.3. Instalación del sistema operativo base

Primeramente es necesario configurar la forma en la que se iniciará el equipo, para ello deberá ingresar a la BIOS del equipo y seleccionar como disco de inicio al dispositivo USB generado en la sección anterior. Adicionalmente se deberá colocar **UEFI** como modo de arranque.

Configuración de inicio

Debido a que el sistema Denwa UC&C 4.0.1 es compatible con equipos de distintas generaciones, la forma de acceder a la BIOS puede ser diferente en cada caso.

Una vez que el equipo haya iniciado con el dispositivo USB, se mostrará una pantalla en la que se podrá seleccionar el idioma utilizado para la visualización de las opciones de instalación, recomendamos utilizar siempre el Inglés, ya que toda nuestra documentación utiliza como referencia dicha lengua.

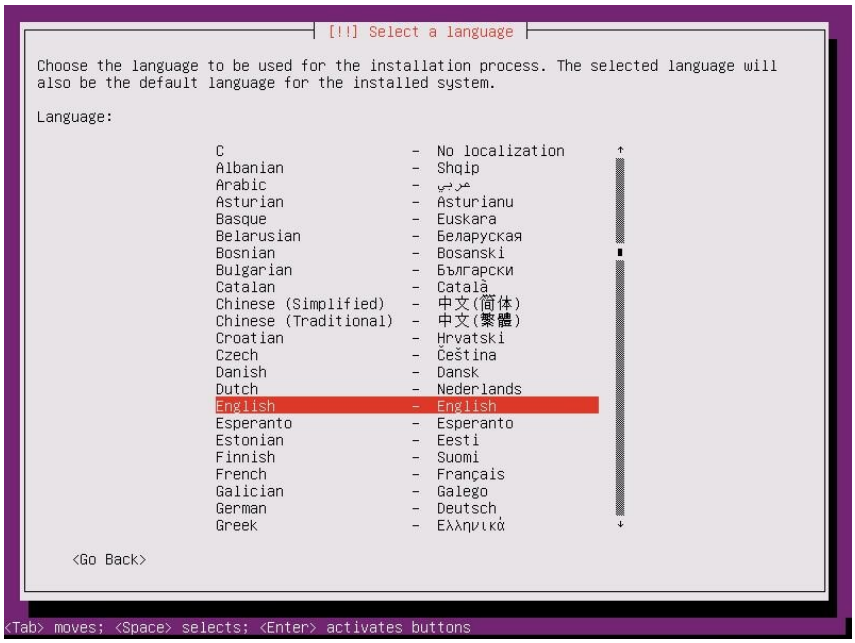

Figura 2.5: Instalación del sistema operativo: selección de idioma del instalador

En la siguiente pantalla es necesario seleccionar la opción «*Install Denwa UC*» para utilizar el particionamiento automático, o bien, «*Install Denwa UC Manual Partition*» para dimensionar de forma diferente las particiones del sistema; y pulsar la tecla «Enter».

Particionamiento manual

La instalación de algunos módulos, características propias de resguardo local de los CDR, registros masivos a los logs del sistema, discos secundarios o alineaciones con RAID, pueden requerir la personalización de las particiones del sistema.
Ante la duda consulte al área de Soporte de Denwa Technology Corp. .

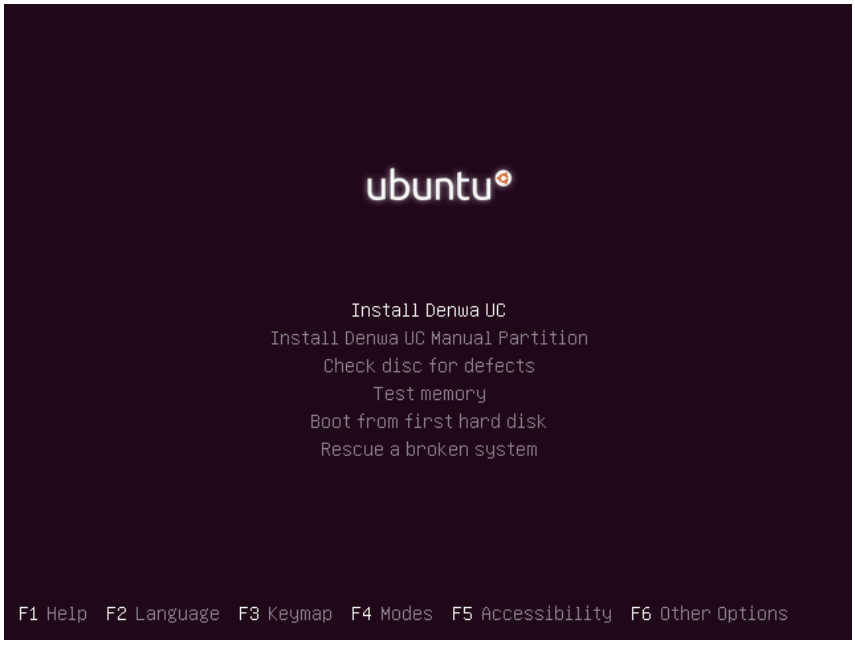

Figura 2.6: Instalación del sistema operativo base

Luego habrá que seleccionar el idioma de instalación del sistema operativo base; una vez

más recomendamos utilizar siempre el Inglés, porque toda nuestra documentación utiliza como referencia dicha lengua.

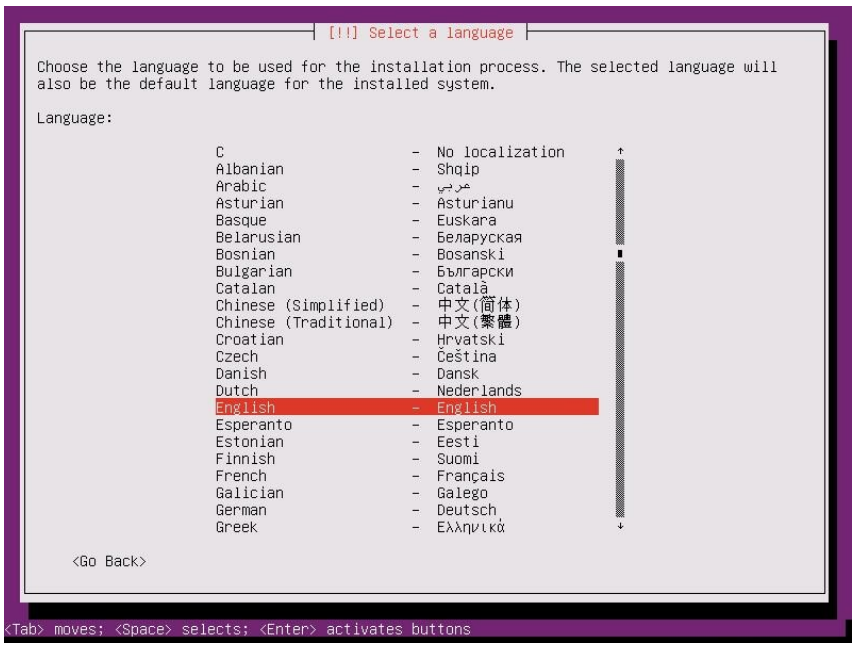

Figura 2.7: Instalación del sistema operativo: selección de idioma del sistema operativo

En el siguiente paso se seleccionará la ubicación, seleccione la ciudad, región o país que corresponda.

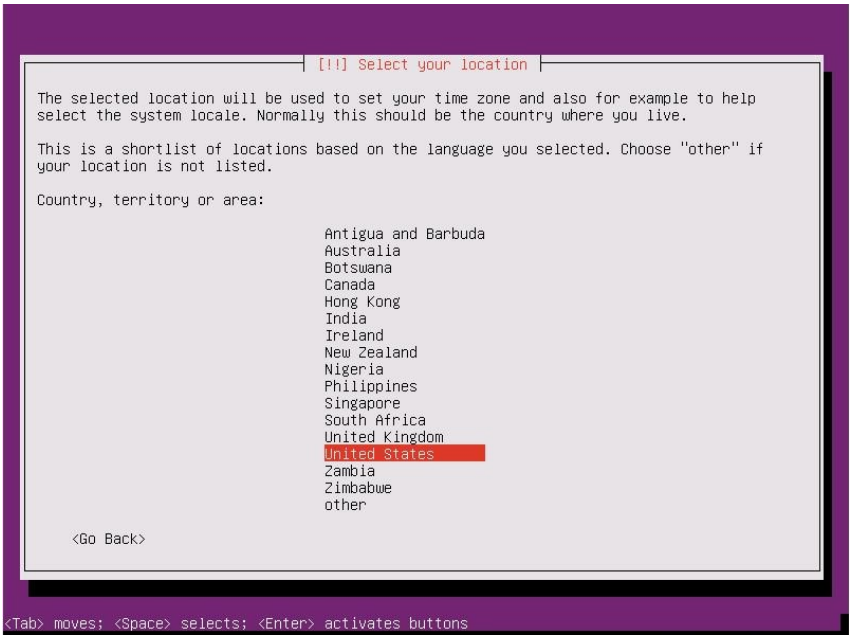

Figura 2.8: Instalación del sistema operativo: selección ciudad, región o país

A continuación se le consultará si desea ejecutar el asistente de distribución de teclado, es nuestra recomendación que lo ejecute, ya que con presionar unas pocas teclas, se evitará muchos problemas cuando deba ingresar al equipo mediante monitor y teclado.

Figura 2.9: Instalación del sistema operativo: asistente de distribución de teclado

Caso contrario se le presentará el listado de todas las distribuciones de teclado posibles, para que seleccione uno de la lista. Por defecto se encuentra seleccionada la opción de «Inglés de Estados Unidos» ("*English (US)*").

Figura 2.10: Instalación del sistema operativo: lista de idiomas y países

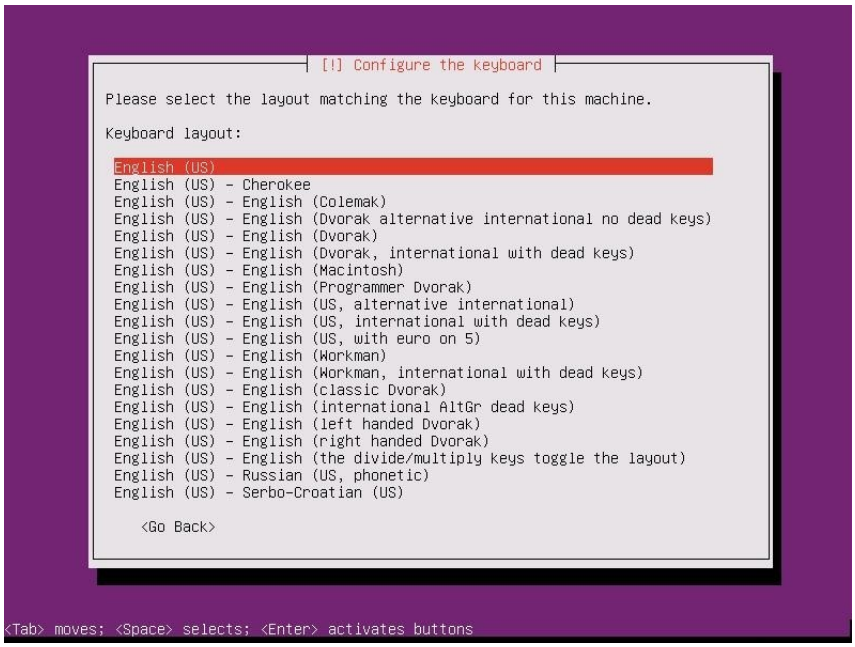

Figura 2.11: Instalación del sistema operativo: lista de distribuciones de teclado para el idioma y país seleccionado

Luego, en caso de que el equipo cuente con una conexión activa a internet, se detectará de forma automática la zona horaria en la cual se realiza la instalación, bastará con pulsar «Yes» para validar la zona horaria detectada o «No» para seleccionarla desde un listado.

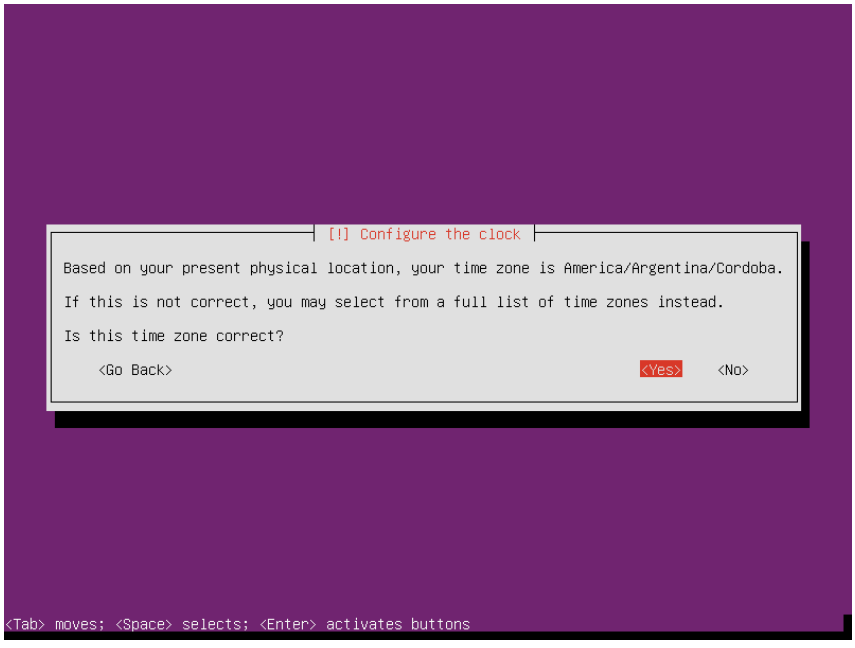

Figura 2.12: Instalación del sistema operativo: confirmación de zona horaria

Una vez hecho esto iniciará la detección de discos y el particionamiento de los mismos, en caso de haber seleccionado la opción de «*Install Denwa UC*» bastará con seleccionar la opción «Guided - use entire disk». Se solicitará confirmación sobre el disco en el que se realizará el particionado.

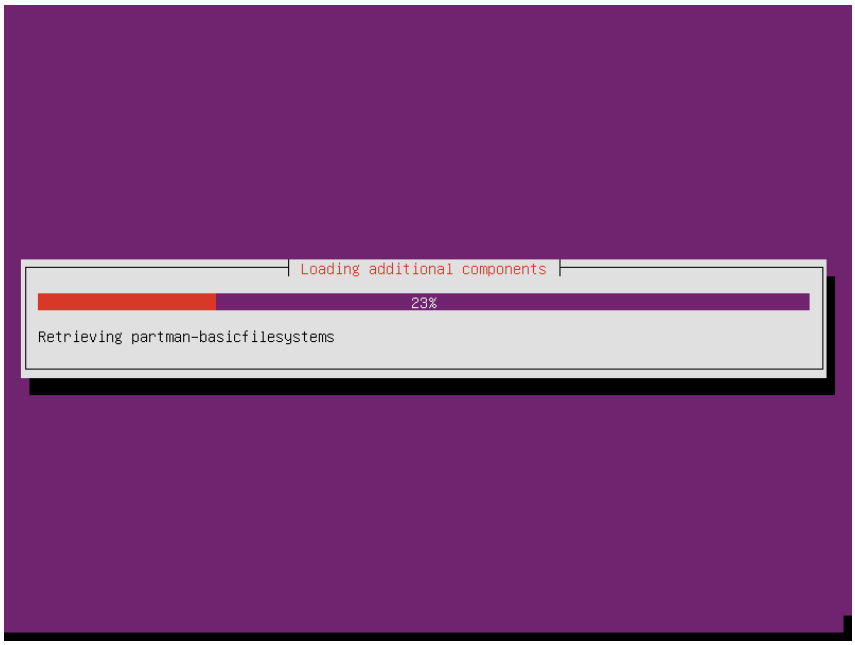

Figura 2.13: Instalación del sistema operativo: detección de discos

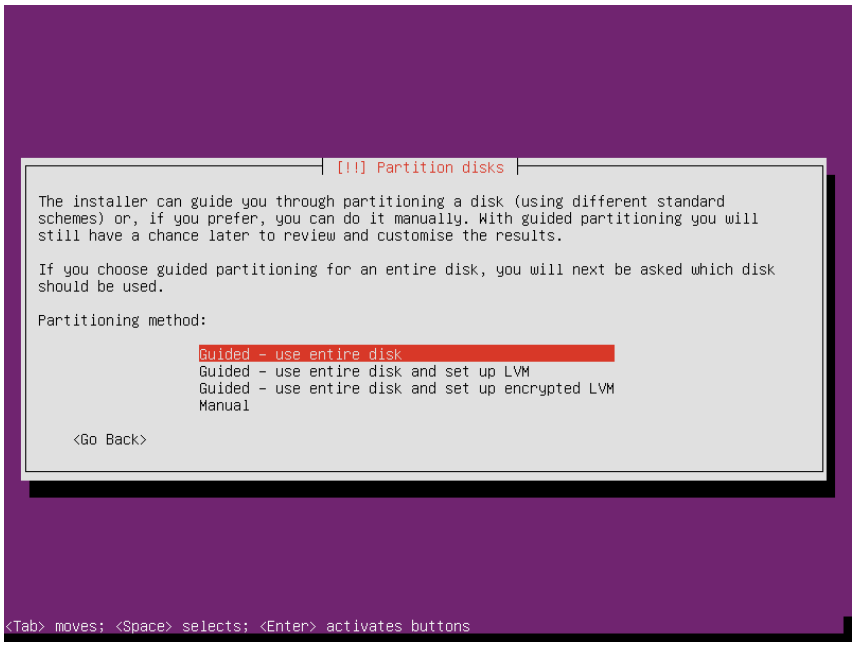

Figura 2.14: Instalación del sistema operativo: método de particionamiento

Particionamiento personalizado

En caso de haber seleccionado la opción de particionamiento personalizado, se deberá tener las siguientes consideraciones:

- Todas las particiones, excepto la «swap», deben ser del tipo «ext4»
- Se debe crear al menos las siguientes particiones:
  - «**boot**» en el disco de estado sólido, para los archivos de arranque del sistema
  - «\» en el disco de estado sólido, para el Sistema Operativo base (20GB mínimo, 30GB recomendado), para:
    - Sistema Operativo
    - Logs del sistema
    - Carpetas de usuarios de Sistema Operativo («pbxadmin», «Soporte Denwa»)
    - Archivos de módulos
  - «**swap**» en el disco de estado sólido, se recomienda de 2GB a 8GB según el equipo. (consultar al área de Soporte de Denwa Technology Corp.)
  - «**denwa**» en el disco de estado sólido, para todos los procesos asociados al motor de telefonía
    - Motor de Telefonía
    - Bases de Datos
    - Interfaz Web
    - Grabaciones por transferirse al FTP Server (si lo hubiese)
  - «**persistent**» en el disco mecánico (si lo hubiese) para el almacenamiento local de la grabación de las llamadas

Solamente restará con aguardar unos minutos para que la instalación finalice, pudiendo ser posible (en caso de que la instalación se realice por medio de un pendrive booteable) la selección del disco donde se implementará el cargador de arranque. Recomendamos seleccionar el mismo dispositivo del paso anterior.

Esta parte del proceso finalizará cuando se le solicite reiniciar el equipo y remover el medio de instalación extraible.

2.4. Instalación del sistema de comunicaciones unificadas

Luego del reinicio, ingrese nuevamente al equipo con las credenciales:

- **Usuario:** pbxadmin
- **Contraseña:** pbxadmin

No hay Prompt

En caso de que una vez reiniciado el equipo, no visualice el prompt del sistema, deberá presionar las teclas Control, Alt y alguna de las de función, por ejemplo:

```
Ctrl + Alt + F2
```

Una vez iniciada la sesión se deberá ejecutar un comando para iniciar el proceso de instalación del sistema de comunicaciones unificadas:

```
install-uc
```

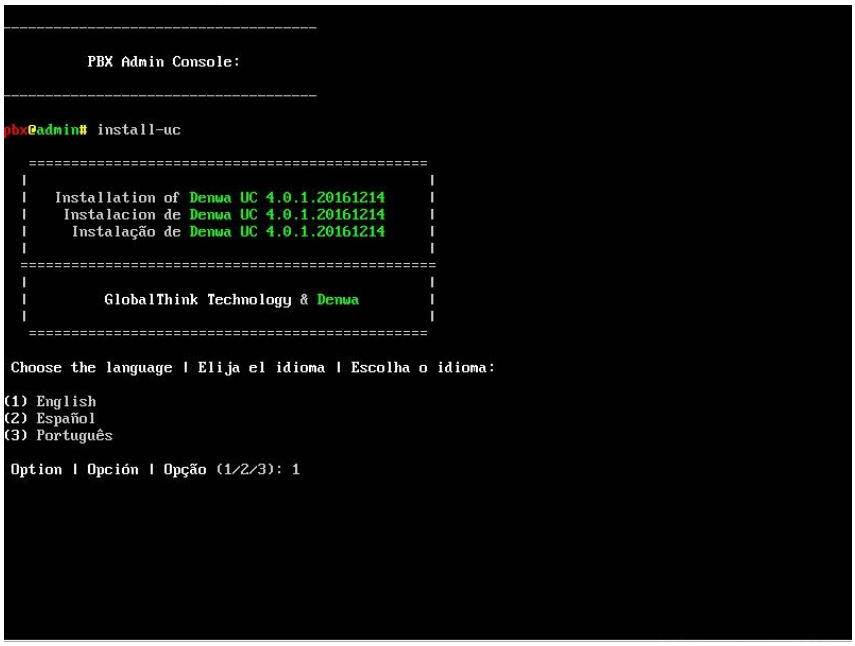

Figura 2.15: Instalación del sistema de comunicaciones unificadas: idioma de instalación

En la primera parte se consultará por el idioma de instalación del sistema de comunicaciones unificadas (idioma a visualizarse en la interfaz web y por medio del acceso por SSH) y, después de validar la conectividad hacia los repositorios de Denwa Technology Corp. (ya sean por la internet o por el repositorio local del distribuidor), se solicitará el la licencia de instalación.

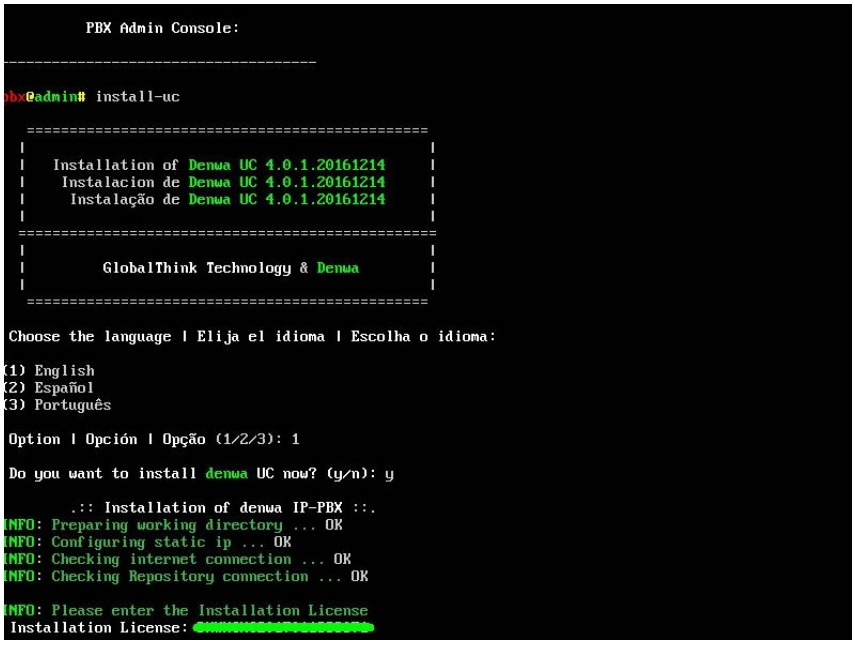

Figura 2.16: Instalación del sistema de comunicaciones unificadas: licencia de instalación

Ahora bien, al instalar el sistema de comunicaciones unificadas sobre un equipo físico, el siguiente paso no será necesario; sin embargo en entornos virtuales, se nos consultará la versión o la familia del procesador.

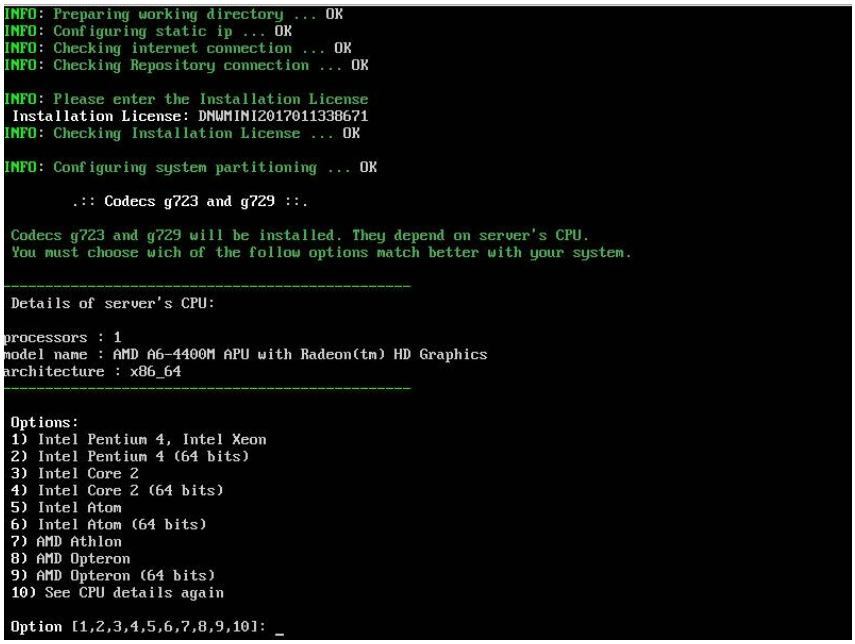

Figura 2.17: Instalación del sistema de comunicaciones unificadas: familia del procesador

A partir de este instante, solamente resta aguardar a que finalice la descarga, instalación y configuración de los distintos paquetes de software necesarios para el sistema de comunicaciones unificadas. Al terminar, bastará con presionar la tecla «Enter» para que el equipo se reinicie.

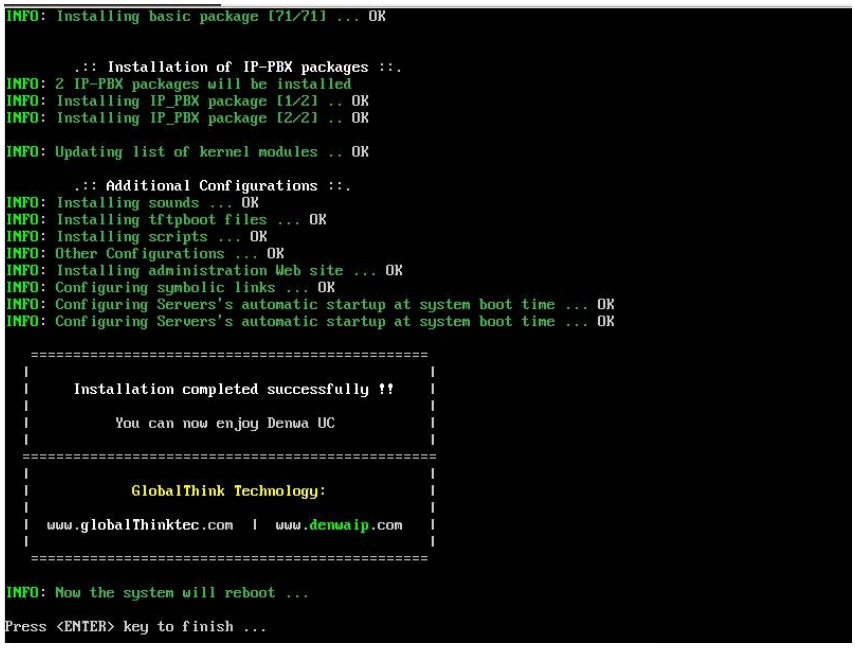

Figura 2.18: Instalación del sistema de comunicaciones unificadas: instalación finalizada

2.5. Activación del sistema de comunicaciones unificadas

Ahora bien, el siguiente paso debe ser ejecutado desde la interfaz web del sistema de comunicaciones unificadas, por lo que es necesario conocer la dirección IP que posee el equipo, en caso de no conocerla (por haber sido configurada por DHCP al momento de instalar el sistema operativo base), es posible ingresar empleando dos métodos diferentes:

- Consultando en la consola del equipo
  1. Ingrese por medio de la consola con el usuario pbxadmin
  2. Ejecute el comando

```
ifconfig
```

  3. Observe la dirección IP que el servidor DHCP de su red le ha asignado al equipo
  4. Utilizando el navegador web, ingrese a la dirección IP obtenida
- Utilizando la IP predeterminada del sistema
  1. Configure en su computador cualquier IP en la red 10.10.10.0/24, excepto la 10.10.10.10
  2. Utilizando el navegador web, ingrese a `http://10.10.10.10`

Una vez que haya finalizado la carga de la página de inicio de sesión, ingrese utilizando los siguientes datos:

- **Usuario:** admin
- **Contraseña:** admin
- **Perfil:** Administrador

Al ingresar se le mostrará una pantalla como la siguiente

Figura 2.19: Activación del sistema de comunicaciones unificadas: pantalla de inicio

Bastará con presionar el único botón de la pantalla para que se muestre un formulario en donde se solicitará información de contacto y la licencia de activación. Luego de completar todos los datos, se procederá a validar el estado de la licencia y, en caso de encontrarse vigente y contar con descargas disponibles, se activará e iniciará la descarga de las actualizaciones publicadas hasta la fecha.

Apartado II

Acceso Web

Sección 3

Interfaz del Administrador

La forma de ingresar a la interfaz de administración de la PBX, es por medio de un navegador web, como lo puede ser: Mozilla Firefox, Google Chrome, Edge, Opera o Internet Explorer. Sin embargo, nuestra recomendación es utilizar Google Chrome, versión 79 o superior.

3.1. Pantalla de Login

Una vez abierto el navegador web, en la barra de direcciones deberá colocar la dirección IP del sistema de comunicaciones unificadas y la palabra «admin», por ejemplo: `http://192.168.0.1/admin`. Dependiendo del último update instalado la pantalla de login podría cambiar.

Figura 3.1: Pantalla de login: Updates 001 a 004

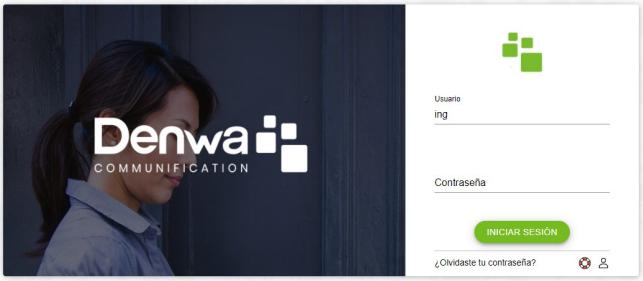

Figura 3.2: Pantalla de login: Updates 005 en adelante

Las credenciales predeterminadas son:

- **Usuario**: admin
- **Contraseña**: admin

No existe límite a la cantidad de usuarios administradores que se pueden crear y que pueden acceder en forma simultánea

Cantidad de administradores

Se recomienda tener una cantidad limitada de administradores y con accesos diferenciados, como se podrá observar en la sección Administradores, en la página 97.

3.1.0.1. Recuperación de Contraseña

El caso de que cuente con un usuario tipo administrador y que haya olvidado su contraseña, es posible recuperarla; sin embargo es necesario que se cumplan dos (2) condiciones:

- Que el sistema de comunicaciones unificadas tenga su servidor de correo debidamente configurado (ver sección Pestaña Servidor de Correo en la página 92)
- Que el usuario tipo administrador (que desea recuperar su contraseña) tenga una dirección de correo electrónico asociada

Con ambas condiciones cumplidas, al pulsar sobre el texto «¿Olvidaste tu contraseña?» y colocar el nombre de usuario de administración, se enviará un correo electrónico que contendrá el código necesario para recuperar la contraseña.

Figura 3.3: Pantalla de login: Recuperación de contraseña

3.1.0.2. Conexión a la VPN de Soporte

Además, se agrega la posibilidad de conectar el sistema de comunicaciones unificadas a soporte sin necesidad de los accesos del Administrador, siempre y cuando Denwa UC&C 4.0.1 tenga acceso a Internet.

Haciendo clic sobre el ícono con forma de salvavidas, ubicado bajo el botón de inicio de sesión en la página de login, del administrador se abrirá la siguiente ventana:

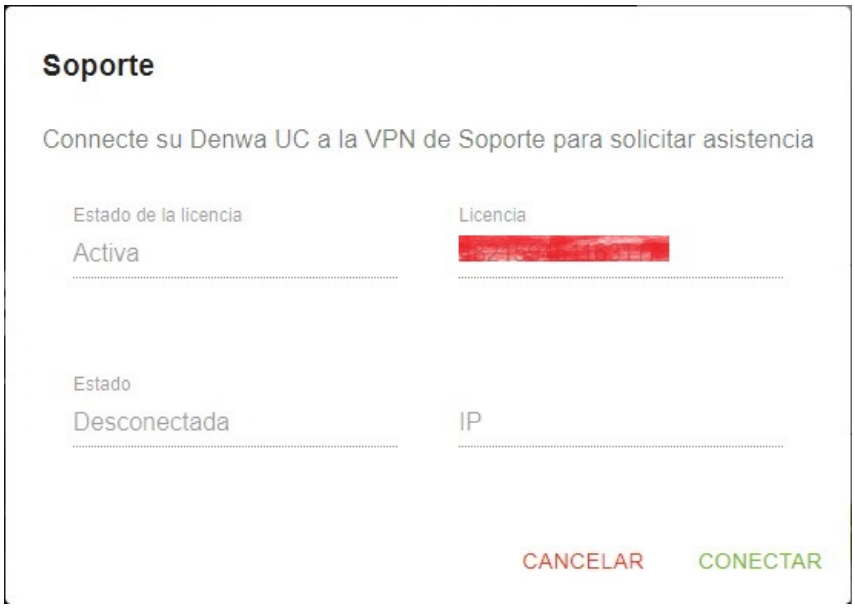

Figura 3.4: Pantalla de login: Conexión a VPN de Soporte

En esta ventana es posible observar información relevante que, el área de Soporte de Denwa Technology Corp. , le solicitará para dar curso a su solicitud por medio del sistema de tickets `http://support.denwaip.com`, a saber:

- **Estado de la licencia**: Indica si el equipo cuenta con un contrato de soporte y actualizaciones activo
- **Licencia**: Número de la licencia de activación del equipo
- **Estado**: Estado de la conexión a la VPN de Soporte de Denwa Technology Corp.
- **IP**: Dirección IP asignada dentro de la VPN de Soporte

En caso de que el campo llamado «Estado» indique que Denwa UC&C 4.0.1 se encuentra «Desconectada», deberá pulsar sobre el botón «Conectar» y aguardar unos segundos para obtener una dirección IP que proporcionarle al área de Soporte de Denwa Technology Corp.

3.2. Pantalla de Inicio

De forma predeterminada se visualizará el tablero del sistema de comunicaciones unificadas, el cual será abordado a continuación.

Opciones a visualizar

Es posible que el usuario tipo administrador que le ha sido asignado no pueda visualizar todos los elementos de menú que se describirá a continuación. En caso de que considere que, por sus funciones y aptitudes, deba contar con mayores privilegios, solicíteselo al administrador de su Denwa UC&C 4.0.1 .

3.2.1. Tablero

Muestra información relevante del sistema en formato de tarjetas, indicando:

- **Tiempo**: Parámetros propios del sistema operativo base utilizado por Denwa UC&C 4.0.1
  - Fecha del sistema
  - Tiempo de actividad del sistema

- **Estado de las actualizaciones**: Muestra si todos los elementos de Denwa UC&C 4.0.1 se encuentran actualizados a su versión más reciente; en caso contrario la línea inferior se mostrará en otro color, indicando que se requiere ejecutar una acción sobre el sistema.
    - Actualizaciones Denwa UC
    - Actualizaciones de firmware de los dispositivos
- **Llamadas activas**: Muestra un gráfico representando las cantidad de llamados en curso de los últimos veinte (20) minutos.
- **Clasificación de las llamadas entrantes**: Por medio de un gráfico de barras apilables muestra la cantidad total de llamados de los últimos ocho (8) días, discriminándolas por:
    - Atendidas
    - No atendidas
- **Estado de las particiones**: Representa el estado de ocupación en cada una de las particiones de Denwa UC&C 4.0.1
    - **Sistema**: Normalmente ubicado en el disco de estado sólido, para el Sistema Operativo base, y contiene:
        - Sistema Operativo
        - Logs del sistema
        - Carpetas de usuarios de Sistema Operativo («pbxadmin», «Soporte Denwa»)
        - Archivos de módulos
    - **Aplicaciones**: Habitualmente el disco de estado sólido, para todos los procesos asociados al motor de telefonía, es decir:
        - Motor de Telefonía
        - Bases de Datos
        - Interfaz Web
        - Grabaciones por transferirse al FTP Server (si lo hubiese)
    - **Datos**: Únicamente en el disco mecánico (si lo hubiese) para el almacenamiento local de la grabación de las llamadas

      Disponibilidad de las particiones

      De acuerdo al modelo del equipo y la cantidad de dispositivos de almacenamiento disponibles, los gráficos se encontrarán activos o inactivos.
- **Nivel de seguridad de las contraseñas**: En caso de contar con contraseñas vulnerables indica la cantidad de ellas.
- **Estado de los servicios**
    - Telefonía
    - Información
    - DHCP
    - SNMP
    - NTP
    - Mensajería
- **Uso de los dispositivos de almacenamiento por tipo de datos**: En esta tarjeta se sumariza el espacio utilizado en disco según el tipo de dato.
    - Base de datos
    - Logs

- Copia de seguridad
- Grabaciones
- Transferencias al FTP
- Buzón de voz
- Capturas de red

- **Estado de las políticas de *Firewall***: Las políticas son la respuesta predeterminada a cualquier conexión que no cumpla con los criterios que hayan sido declarados como «excepciones».

- **Estado de los servicios de *Firewall***

  - ***Firewall***: Servicio de *Firewall*
  - **Intentos fallidos**: Servicio que bloquea el acceso desde un origen que haya errado en sus credenciales para cualquier tipo de conexión en un periodo de tiempo definido (ver «Firewall», en la página 116)
  - **Escaneo de puertos**: Servicio que bloquea el acceso desde un origen desde donde haya provenido un intento de escaneo de puertos sobre Denwa UC&C 4.0.1 (ver «Firewall», en la página 116)

- **Estado de habilitación del HTTPS**

- **Cantidad de llamados de los últimos tres (3) meses**

3.2.2. Usuarios

Muestra el listado de todos los usuarios de Denwa UC&C 4.0.1 , indicando:

- **General**: Nombre brindado al usuario
- **Móvil**: Número de teléfono móvil del usuario
- **Extensión**: Número de interno en Denwa UC&C 4.0.1
- **Modo**:

3.2.3. Interfaz Avanzada

Este elemento es un acceso directo a la versión anterior de la interfaz web de administración de Denwa UC&C 4.0.1 . Puede consultar todo su contenido en la sección Interfaz Avanzada, a partir de la página 27.

3.2.4. Cerrar sesión

3.3. Interfaz Avanzada

Opciones a visualizar

Es posible que el usuario tipo administrador que le ha sido asignado no pueda visualizar todos los elementos de menú que se describirá a continuación. En caso de que considere que, por sus funciones y aptitudes, deba contar con mayores privilegios, solicíteselo al administrador de su Denwa UC&C 4.0.1 .

3.3.1. Inicio

Al ingresar con el perfil de Administrador, se observa la pestaña Inicio de configuración de la interfaz web de la PBX. Se pueden encontrar datos sobre el estado del servidor, información de los servicios activos, estadísticas del uso de discos y más puntuales de Denwa UC&C 4.0.1 .

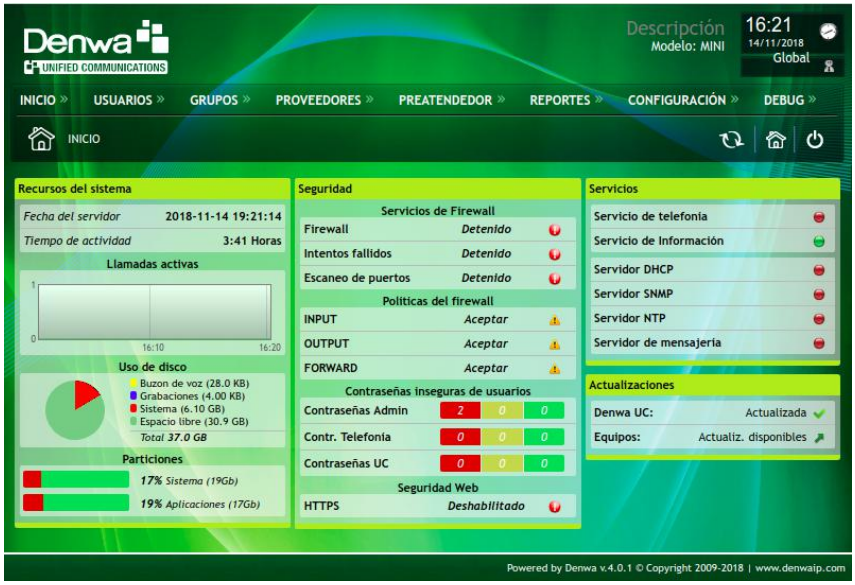

Figura 3.5: Interfaz avanzada: Pantalla de inicio

Esta página ofrece la siguiente información expresada en recuadros.

- **Recursos del sistema**: Para mas detalle se puede dirigir a Reportes >Recursos del Sistema, o a la sección Recursos del sistema en la página 85.
  - **Fecha del servidor**: fecha y hora actual de la central.
  - **Tiempo de actividad**: tiempo transcurrido desde la última vez que se encendió el equipo.
  - **Llamadas activas**: permite visualizar de manera gráfica las llamadas cursadas en los últimos 20 minutos.
  - **Uso de disco**: buzón de voz, grabaciones, sistema, espacio libre y total.
  - **Particiones**: Porcentaje de uso de las particiones del sistema.
- **Seguridad**: Indicador y alerta de los estados en los esquemas de seguridad en el Denwa UC
  - **Servicios de Firewall**: muestra el estado del firewall, intentos fallidos y escaneo de puertos.
  - **Políticas del Firewall**: INPUT, OUTPUT y FORWARD.
  - **Contraseñas inseguras de usuarios**: muestra mediante un código de colores el estado de las contraseñas de administrador, telefonía y UC.
  - **Seguridad Web**: muestra el estado de HTTPS.
- **Servicios**: Indicador de estado de los servicios (En verde si estan activos, y en rojo si estan desactivados)
  - Servicio de telefonía
  - Servicio de Información
  - Servidor DHCP
  - Servidor SNMP

- Servidor NTP
- Servidor de mensajería

- Actualizaciones
  - **Denwa UC**: indica si existen actualizaciones disponibles para Denwa UC&C 4.0.1 (Configuración >Soporte)
  - **Equipos**: indica si existen actualizaciones disponibles para los equipos de telefonía homologados (Configuración >Equipos >Modelos)

Alertas por ocupación de disco

Cuando la capacidad del disco llega a un 70 %, el sistema envía un correo electrónico a los usuarios de tipo administrador de la plataforma, informando que una o más de las particiones del sistema ha sobrepasado el umbral (esta tarea la realiza una vez cada hora). Para el correcto funcionamiento de estas alertas, se debe configurar previamente el servidor de correo electrónico en Configuración >General >Servidor de Correo (ver sección Pestaña Servidor de Correo en la página 92).

3.3.2. Usuarios

Desde la pestaña Usuarios se pueden seleccionar diversas acciones, que serán explicadas a continuación.

3.3.2.1. Ver Usuarios

Esta opción permite observar la lista completa de los usuarios creados, junto con su Nombre, Apellido, Email, Extensión, Modo y Estado de Registro. En caso de que la extensión se encuentre registrada, ubicando el mouse sobre el círculo verde se visualiza el número IP del teléfono asociado.

Además es posible eliminar y editar los usuarios individualmente de forma directa. Para eliminar un usuario sólo es necesario ejecutar un clic sobre el ícono con forma de equis (✖). Mientras que para editarlo se debe hacer clic en el Nombre del usuario deseado.

Figura 3.6: Interfaz avanzada: Ver usuarios

3.3.2.1.1. Edición múltiple También es factible realizar una selección múltiple de usuarios. Para ello es necesario seleccionar al menos dos usuarios (hacer clic en los casilleros que se encuentran a la izquierda del nombre del usuario). Luego se debe acceder al menú Acciones, el cual se ubica en la esquina inferior izquierda de la pantalla.

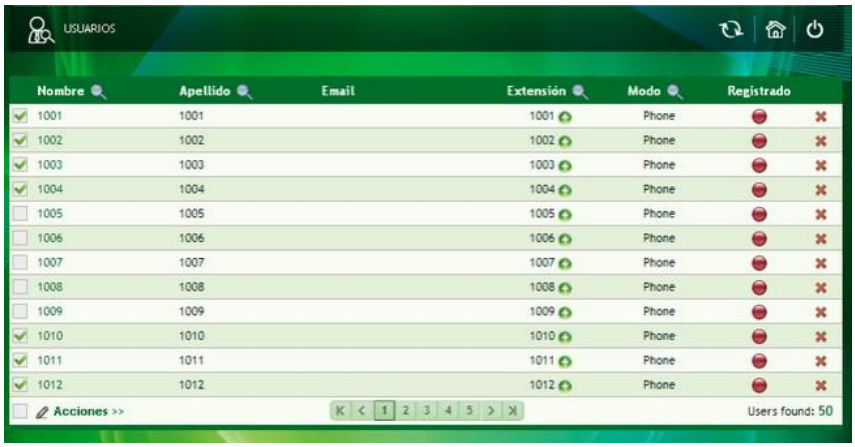

Figura 3.7: Interfaz avanzada: Ver usuarios, selección múltiple

En la ventana emergente, se muestran las configuraciones de los usuarios seleccionados, las cuales son una versión reducida de lo que se puede encontrar en la opción Nuevo Usuario.

Figura 3.8: Interfaz avanzada: Ver usuarios, edición múltiple

3.3.2.1.2. Asignación de números de acceso Además se pueden asignar los DIDs (números de acceso) a las extensiones haciendo clic en el ícono de suma (⊕), al lado derecho del número de extensión. Esta acción desplegará una ventana como la siguiente:

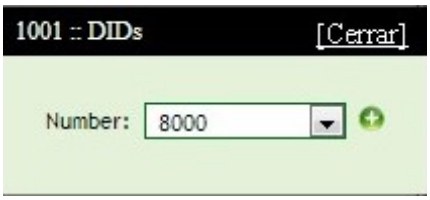

Figura 3.9: Interfaz avanzada: Ver usuarios, asignación de números de acceso

Luego de seleccionarlo, se asociará a la extensión presionando sobre el en el ícono de suma (⊕). Por otro lado, si lo que se desea es borrar la relación, se deberá pulsar sobre el símbolo de resta (−). Todos los cambios serán guardados al oprimir en «[Cerrar]».

3.3.2.2. Buscar Usuarios

Desde esta opción se pueden realizar búsquedas de usuarios por: nombre, apellido, extensión, tipo y DID (número de acceso). También, permite buscar a tanto a los usuarios re-

gistrados como a los no registrados; o por algún texto indicativo o prefijo en particular. Esta herramienta simplifica las tareas cuando se dispone de gran número de internos.

Figura 3.10: Interfaz avanzada: Buscar usuarios

Búsqueda de usuarios

La búsqueda de usuarios también puede realizarse desde la pantalla donde se listan todos los usuarios (ver sección Ver Usuarios en la página 29), haciendo clic sobre el ícono 🔍 que se encuentra en el encabezado de la tabla.

El resultado de la búsqueda se observa en el panel derecho. Desde aquí también se pueden realizar la configuraciones de los usuarios, es decir editar, borrar y/o agregar un DID.

3.3.2.2.1. Modificar permite editar la configuración del usuario, al pulsar sobre esta opción se muestra la ventana de Modificar Usuario. Esta ventana es idéntica (excepto por que ya cuenta con información) a la de alta de usuarios (ver sección Nuevo Usuario en la página 32) a esta pantalla también se puede acceder pulsando sobre el nombre del usuario en el listado de Ver Usuarios de la página 29.

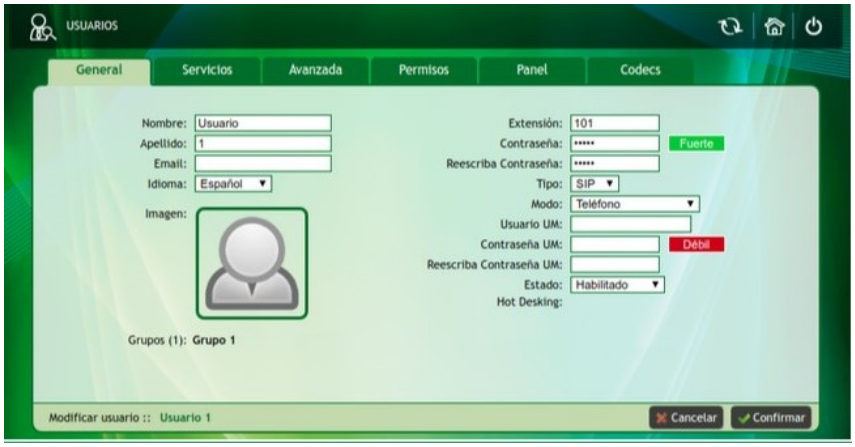

Figura 3.11: Interfaz avanzada: Modificar usuario

3.3.2.2.2. Borrar permite eliminar los usuarios. Luego de presionar sobre este ítem se visualiza la ventana de Ver Usuarios.

3.3.2.3. Nuevo Usuario

El menú Nuevo Usuario permite generar una nueva extensión, y realizar las configuraciones pertinentes.

Límite de usuarios

Aunque teóricamente no existe límite para la cantidad de usuarios, es nuestra recomendación no sobrepasar la cantidad indicada en las distintas Hojas Técnicas de los productos, las cuales han sido estimadas de forma estadística, considerando la relación existente entre llamadas activas (entrantes, salientes y entre internos) y la cantidad de usuarios de la plataforma.
Ante cualquier duda consulte al área de Preventa de Denwa Technology Corp. .

3.3.2.3.1. Pestaña General de Nuevo Usuario La ventana que se visualiza permite crear o modificar los nuevos usuarios. Los datos a ingresar son los siguientes:

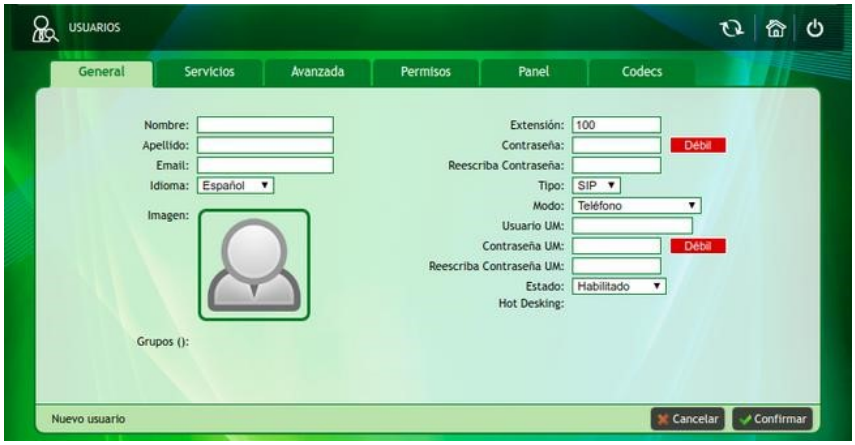

Figura 3.12: Interfaz avanzada: Nuevo usuario, pestaña general

- Datos personales del usuario
  - **Nombre**: nombre del usuario asignado a la extensión.
  - **Apellido**: apellido del usuario asignado a la extensión.
  - **Email**: dirección de correo electrónico del usuario asignado a la extensión. En caso de que extensión no responda la llamada, allí se enviaran los de voicemails.
  - **Idioma**: se selecciona el idioma para el usuario.
  - **Imagen**: se puede incorporar una imagen de perfil desde el Denwa Desktop.
  - **Grupo**: Muestra los grupos a los cuales pertenece el usuario.
- Se define el número de extensión junto con la contraseña del mismo y su modo. Para una extensión simple se usa modo teléfono ; para los agentes de call center tambien se utiliza el modo teléfono.
  - **Extensión**: se define la extensión para el usuario. No hay límite con la cantidad de dígitos para la numeración interna
  - **Contraseña**: se define la contraseña del usuario. La misma debe ser fuerte, por lo cual debe estar compuesta por mayúsculas, minúsculas, números y caracteres especiales.
  - **Reescriba contraseña**: se confirma la contraseña del usuario.
  - **Tipo**: permite seleccionar el tipo de extensión, las opciones son SIP, FXS o IAX2.

Extensión FXS

Si se elige FXS, se debe seleccionar el puerto asociado a la extensión. Para ello es necesario hacer un clic sobre el ícono ⚙.

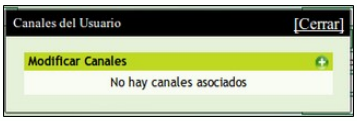

Figura 3.13: Interfaz avanzada: Usuario tipo FXS, canales del usuarios

Luego, bastará con un clic en el signo de suma (⊕) para realizar la asociación del canal.

Figura 3.14: Interfaz avanzada: Usuario tipo FXS, canales disponibles

- **Modo**:

  - **Teléfono**: extensión VoIP para ATA, Softphone o IPPhone.
  - **Teléfono con Video**: Teléfono con pantalla de video incorporada.
  - **FAX**: extensión VoIP para ATA con soporte de FAX.
  - **FAX to Email**: este modo posibilita la recepción de FAXs desde el portal Denwa Desktop de los usuarios asociados o las casillas de correo electrónico de los mismos. Para ello, se debe crear un usuario con el modo FAX to Email; la extensión de éste es virtual, debido a que no se registrará (en Ver Usuario se visualiza un círculo rojo en Registrado). Luego, es posible asignar usuarios desde la Pestaña Avanzada de Nuevo Usuario. Esta asignación es la que permite la recepción de los FAXs, además de en la casilla de correo de la extensión virtual, en la de los usuarios asignados y sus portales de Denwa Desktop.
  - **Conferencia**: permite la conexión multimedial entre dos o más usuarios. Para lo cual es necesario crear un usuario con modo Conferencia; esta extensión es virtual por esta razón no se registrará (en Ver Usuario se visualiza un círculo rojo en Registrado). Una vez que se crea el usuario, en la opción Ver Usuario junto al modo conferencia se visualiza . Al hacer clic sobre este icono se debe definir el PIN. Luego de discar la extensión, el usuario debe marcar este código para incorporarse a la conferencia. No existe un límite para crear extensiones tipo conferencia, y la cantidad de usuarios por sala de conferencia se remite a la cantidad de llamadas simultáneas.

Figura 3.15: Interfaz avanzada: Usuario modo Conferencia

- **Grupo**: permite realizar llamadas a un conjunto de usuarios reunidos en un grupo de acuerdo a la configuración de este, dirigirse a Ver Grupo. Para lo que se debe crear una extensión virtual (en Ver Usuario se visualiza un círculo rojo en Registrado). Una vez que se crea el usuario, en la opción Ver Usuario junto al modo Grupo se visualiza . Al ejecutar un clic sobre este icono se debe seleccionar el grupo al cual se le asignará la extensión y Confirmar.

Figura 3.16: Interfaz avanzada: Usuario modo Grupo

- **Visitante**: posibilita el uso de los equipos registrados en la red a personas no pertenecientes a ella, es decir es una extensión que se genera para poder realizar llamadas desde cualquier equipo. Para ello al crear el usuario en este modo, es necesario establecer un PIN de seguridad. Para realizar una llamada se debe validar la identidad llamando al *65,luego se ingresa el PIN de seguridad y por último la extensión a llamar.
- **Parking**: permite almacenar llamadas entrantes. Al crear un usuario parking es necesario asignar un grupo de extensiones a las cuales se transferirán las llamadas que no se puedan atender en el momento. El número de extensiones que se le asignan al modo, son la cantidad de llamadas que pueden almacenarse. Para que se pueda realizar este proceso, es necesario tomar la llamada entrante y luego transferirla. Cuando se termina la llamada en curso, la PBX llama al usuario y le avisa en que extensión de parking se guardó la llamada. Para responder la llamada, solo se debe discar la extensión de parking en la que se guardó.
- **Portero**: permite gestionar las llamadas a la puerta en la que se encuentra el portero eléctrico. Para esto es necesario crear un nuevo usuario con modo Portero y confirmar. Luego se debe ingresar a Ver Usuarios, hacer clic sobre la extensión portero, en la Pestaña servicios se debe configurar la extensión teléfono que sonará cuando se llame al portero. El aprovisionamiento del equipo se debe realizar, luego de creada la extensión.
- **Intercomunicador**: permite configurar una extensión con este modo. Luego, tildando en la Pestaña Permisos de Nuevo Usuario la opción Habilitar Intercomunicador se dispone de esta funcionalidad. Este tipo de extensión puede recibir llamada y realizar la auto atención de la línea con una sola vía de audio. Esta vía es desde la extensión que llama. Es utilizada para realizar anuncios o ubicar personal. Se accede al marcar *59 + EXT. DEL INTERCOM + SEND.
- **Call Center**: permite configurar una extensión para integrar Call Center de terceros. El call center se registra usando este tipo de extensión, el tráfico de llamadas entrantes se balancearan entre los distintos equipos.

- **Dispatcher**: se generar una extensión tipo dispatcher se implementa para el envío masivo de mensajes de Voz, FAX, Video y SMS.
- **Video Security**: permite asignar equipos de seguridad a una extensión.Además se puede realizar llamadas desde teléfonos con video a estas extensiones y visualizar la actividad en el lugar conectando en modo promiscuo o bien con audio de dos vías.
- **Preatendedor**: permite crear una extensión que funcione como preatendedor.
- **Aplicación**: este modo permite llamar a una aplicación para su ejecución. Para ello se debe seleccionar el ícono ⚙. La pantalla emergente posibilita elegir la aplicación deseada. Luego, se debe presionar Confirmar y Cerrar.

Figura 3.17: Interfaz avanzada: Usuario modo Aplicación

- **Teléfono compartido**: se crea una extensión que puede llamar a cualquier extensión normalmente, pero cuando se quiere realizar otro tipo de llamada (externa por ejemplo), se solicita un código de discado remoto. Este código es único para cada uno de los usuarios. El usuario que desee utilizar un teléfono compartido debe ingresar su código de discado remoto. Las configuraciones se realizan en la Pestaña de Servicios (ver sección Pestaña Servicios de Nuevo Usuario en la página 35)o desde el portal Denwa Desktop (ver sección **??** en la página **??**).
- **Teléfono público**: esta opción permite crear una extensión que puede llamar normalmente, pero se solicita al usuario un código de discado remoto. Este código es único para cada uno de los usuarios. El usuario que desee utilizar un teléfono público debe ingresar su código de discado remoto. Las configuraciones se realizan en la Pestaña de Servicios (ver sección Pestaña Servicios de Nuevo Usuario en la página 35)o desde el portal Denwa Desktop (ver sección **??** en la página **??**).

- Configuraciones para Denwa Desktop (ver sección **??** en la página **??**) y estado de esta extensión.
  - **Usuario UM**: nombre de usuario de UM (Mensajeria Unificada).
  - **Contraseña UM**: contraseña de UM. La misma debe ser fuerte, por lo cual debe estar compuesta por mayúsculas, minúsculas, números y caracteres especiales.
  - **Reescriba Contraseña UM**: reescribir para confirmar la contraseña de UM.
  - **Estado**: se asigna un estado a la extensión
    - Habilitado: se pueden realizar llamadas dentro y fuera de Denwa UC&C 4.0.1 .
    - Suspendido: sólo se pueden realizar llamadas dentro de Denwa UC&C 4.0.1 , pero permite recibir llamadas fuera de ella.
    - Deshabilitado: no se pueden realizar y recibir ningún tipo de llamadas sea cual sea su destino.

3.3.2.3.2. Pestaña Servicios de Nuevo Usuario Desde esta pestaña se deben determinar los servicios de llamada. Aquí se puede configurar la línea del usuario de acurdo a los servicios que se le desea habilitar.

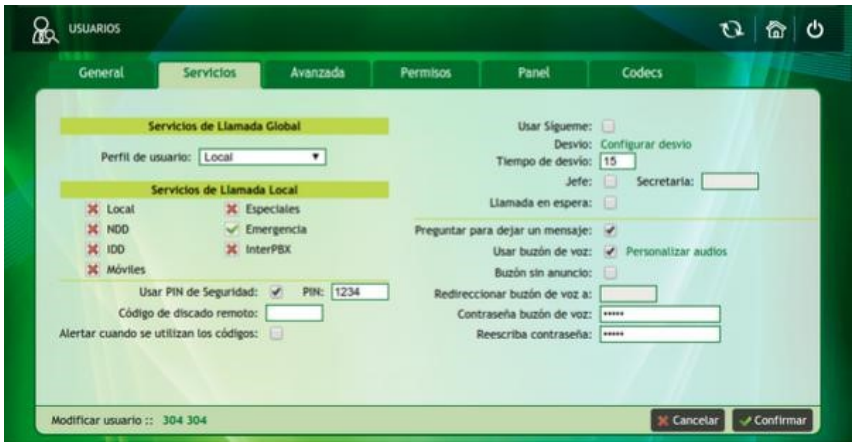

Figura 3.18: Interfaz avanzada: Nuevo usuario, pestaña servicios

Los campos que se pueden administrar son los siguientes.

- **Servicios de Llamada Global**: permite asignar un perfil al usuario, es decir se puede establecer un conjunto de características comunes a varios usuarios; estos pueden ser configurados en Perfiles de usuario (ver sección Perfiles de Usuario en la página 48). En caso de que no exista ningún perfil creado, por defecto se ofrece el perfil Local, es decir: se pueden realizar llamados los 7 días de la semana, las 24 horas del día.
- **Servicios de Llamada Local**: permite gestionar los permisos para realizar diversos tipos de llamadas. Pueden encontrarse habilitados o permitidos (✔), denegados (✖) o protegidos por el Pin de Seguridad (🔒). En el caso de que se desee que todos los servicios de llamada se encuentren protegidos por Pin de Seguridad, se recomienda tildar en Usar PIN de Seguridad. Para configurar los prefijos que corresponden con cada tipo de llamada se debe acceder a Servicios de Llamadas (ver Servicio de llamadas en la página 120).
  - Local: llamadas locales
  - NDD: larga distancia nacional
  - IDD: larga distancia internacional
  - Móviles: llamadas a móviles
  - Especiales: llamadas a servicios especiales, tales como los 0800, 0810 y 0600, por ejemplo
  - Emergencia: números de emergencia
  - InterPBX: llamadas a otra central telefónica conectada por un troncal interconn

Sip interconn

Los troncales tipo interconn permiten la interconexión de dos equipos de telefonía, permitiendo que los usuarios de ellas puedan comunicarse entre sí como si en un mismo equipo se encontrasen, además de compartir sus demás troncales. Por ejemplo:
En caso de que hubiese dos (2) centrales 200 y 300 conectadas a través de un troncal interconn, los usuarios de 200 pueden cursar llamados hacia el exterior utilizando los troncales de 300, y viceversa.

- **Usar PIN de Seguridad**: se usa un PIN para que cada una de las llamadas realizadas por el usuario soliciten autorización. Se tienen dos casos de empleo, para los cuales el usuario deberá marcar su PIN para realizar una llamada:
  1. Al colocar en los servicios de llamadas, no hace falta hacer clic en el checkbox correspondiente a «Usar PIN de Seguridad».

2. Se requiere colocar en cada servicio de llamada y luego hacer clic en el checkbox «Usar PIN de Seguridad».

- **PIN (Personal Identification Number)**: este código numérico es elegido por el administrador, que se debe marcar cuando se lo solicite.

- **Código de discado remoto**: este código se utiliza para realizar llamadas salientes de Denwa UC&C 4.0.1 desde un teléfono compartido. Este código es único para cada usuario.

- **Alertar cuando se utilizan los códigos**: se envía un email a la dirección de correo electrónico que el usuario tiene registrado en Pestaña General de Nuevo Usuario (ver Pestaña General de Nuevo Usuario en la página 32) cuando estos códigos son utilizados.

- **Usar sígueme**: Luego de crear el usuario, en esta pestaña se permite habilitar la opción de activar Sígueme. Para ello se debe hacer clic en el checkbox, esto habilita la configuración del mismo.

    - Tipos de sígueme:
        - **Alternado + Anuncio**: se sigue una secuencia de timbrado, una operadora permite que el llamante se anuncie.
        - **Simultaneo + Anuncio**: timbran todas las extensiones al mismo tiempo y una operadora permite que el llamante se anuncie.
        - **Alternado**: describe la forma en la que timbran en las extensiones, en este caso es siguiendo una secuencia de a una por vez.
        - **Simultaneo**: con esta opción timbran todas las extensiones al mismo tiempo.
        - **Alternado + Silencioso**: se sigue una secuencia de timbrado y no existe operadora. La llamada se transfiere automáticamente a la siguiente tipo de extensión.
        - **Simultaneo + Silencioso**: timbran al mismo tiempo y no existe operadora.
    - Pulsando el botón con el ícono de suma (⊕) se agrega la regla de sígueme.
    - En los campos que están debajo se puede configurar las extensiones o números que se asocian a dicho usuario. También se puede establecer el tiempo de ring. Para que la acción se concrete se debe hacer clic sobre el ícono de suma (⊕).

Figura 3.19: Interfaz avanzada: Usuario configuración de sígueme

- **Desvio**: En esta sección, también se permiten configurar desvíos.

    - **Desde**: permite seleccionar el origen de las llamadas que llegan a la extensión. En el menú desplegable se visualizan las siguientes opciones: internas, externas y todas.
    - **Causa**: es el motivo que da origen a la ejecución a la regla de desvío. En este menú se puede seleccionar dentro de las opciones: ocupado, sin respuesta y siempre.
    - **Acción**: aquí se indica el curso que tomará la llamada, dentro de éstas se puede seleccionar: desvío, desconectar y buzón de voz. Número: se activa esta opción siempre que en la acción correspondiente no se hubiese seleccionado la opción desconectar. Esto es debido a que es necesario colocar el número al cual se realizará el desvío o el buzón de voz.

- Pulsando el botón con el ícono de suma (⊕) se agrega la regla de desvío.

Figura 3.20: Interfaz avanzada: Usuario configuración de desvío

- **Tiempo de desvío**: se define el tiempo a esperar antes de realizar el desvío de la llamada.
- **Jefe**: se obliga a que todas las llamadas entrantes a su interno primero se redireccionen a la Secretaria. Para ello se debe seleccionar la opción «Jefe» y colocar la extensión de la «Secretaria».
- **Llamada en espera**: en caso de estar habilitado, si el usuario se encuentra en un llamado telefónico e ingresa otro llamado, reproducirá un tono alertando el nuevo llamado, permitiéndole al usuario atender el segundo, en tanto que deja en pausa el primero
- **Preguntar para dejar un mensaje**: se aplica para llamadas externas, es decir cuando se reciba una llamada, la cual en primera instancia es atendida con un preatendedor puede disponer de esta opción.
- **Usar buzón de voz**: si se desea utilizar un buzón de voz en el interno, sólo se debe marcar la casilla correspondiente al buzón. Una vez hecho esto se habilita la posibilidad de personalizar los mensajes de audio. Para ello es posible hacer un clic sobre ⬆ y cargar algún archivo de audio o presionar sobre 🎤 y grabar el audio desde su extensión.

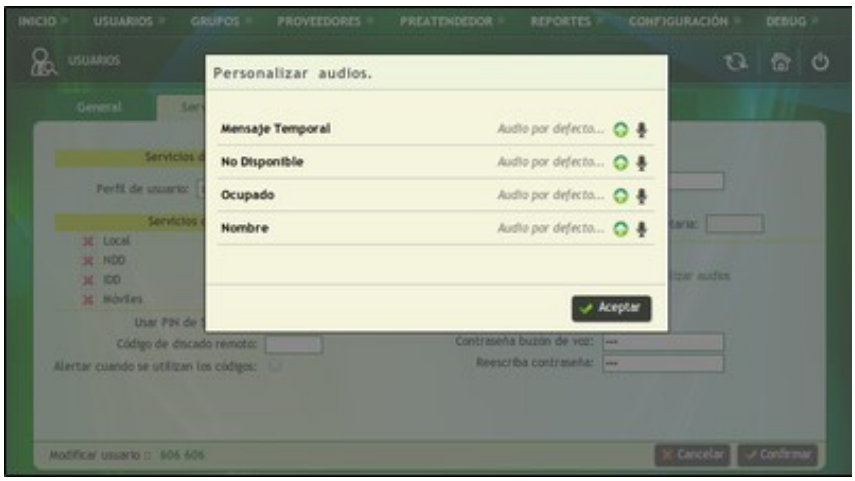

Figura 3.21: Interfaz avanzada: Usuario: Personalización de audios

- **Buzón sin anuncio**: con esta opción se habilita o deshabilita el anuncio de buzón de voz.
- **Redireccionar buzón de voz a**: para poder usar esta opción se debe deshabilitar el Buzón de voz. Luego de esto se carga la extensión a la que se redirecciona el buzón de voz.
- **Contraseña buzón de voz**: se establece una contraseña para acceder a los mensajes guardados desde el dispositivo telefónico.
- **Reescriba contraseña**: debe coincidir con la contraseña, para poder completar el proceso.

3.3.2.3.3. Pestaña Avanzada de Nuevo Usuario Desde esta pestaña se pueden configurar funciones extras a cada usuario.

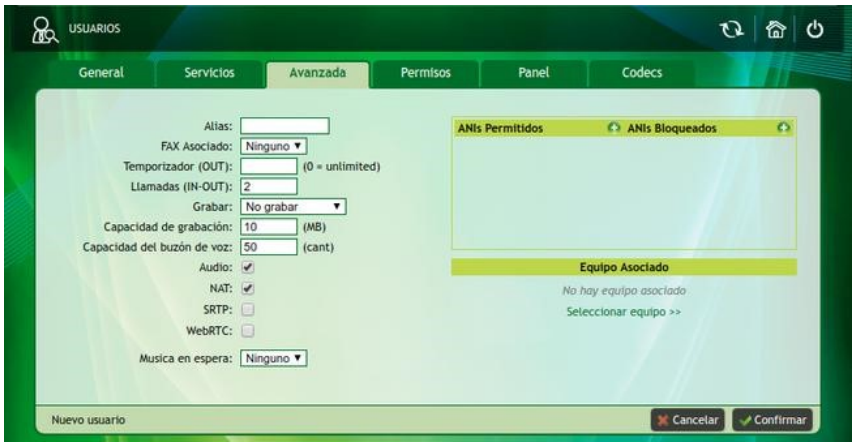

Figura 3.22: Interfaz avanzada: Usuario configuración avanzada

- **Alias**: permite crear un número y asociarlo al usuario. Con esto las llamadas entrantes pueden discar dicho número y comunicarse con la extensión deseada.
- **FAX Asociado**: se otorga la posibilidad de asociar un usuario tipo FAX, o FAX to Email a la extensión, y de este modo, se reciben los mensajes en el Desktop o en la casilla de correo electrónico.
- **Temporizador (OUT)**: permite añadir un temporizador el cual limita la duración de las llamadas salientes.
- **Llamadas (IN-OUT)**: permite determinar la cantidad de llamadas simultaneas que puede realizar o recibir cada usuario.
- **Grabar**: permite grabar llamadas salientes, entrantes o ambas, de forma aleatoria o continua.
  - **No grabar**: No graba ninguna llamada
  - **All-Continuo**: Graba todas las llamadas, entrantes o salientes
  - **All-Aleatorio**: Graba algunas llamadas, tanto entrantes como salientes
  - **In-Continuo**: Graba todas las llamadas entrantes
  - **In-Aleatorio**: Graba algunas llamadas entrantes
  - **Out-Continuo**: Graba todas las llamadas salientes
  - **Out-Aleatorio**: Graba algunas llamadas salientes
- **Capacidad de grabación**: se limita el espacio en MB disponible para la grabación de llamadas. Cuando el espacio sea excedido, las grabaciones más antiguas comenzarán a borrarse, en caso de que desee conservarlas, será necesario configurar un servidor de respaldo desde Pestaña Respaldo de General (ver Pestaña Respaldo en la página 92) para almacenar dichas grabaciones.
- **Capacidad del buzón de voz**: se establece la cantidad de voicemails que se pueden almacenar localmente en Denwa UC&C 4.0.1 . Si se configura un un servidor de respaldo desde Pestaña Respaldo de General(ver Pestaña Respaldo en la página 92), los voicemails excedentes se guardarán en el mismo; caso contrario, serán eliminados.
- **Audio**: esta casilla se encuentra activa de forma predeterminada y es necesaria para poder realizar grabaciones; sin embargo al desmarcarla, disminuye el procesamiento de Denwa UC&C 4.0.1 al enviar unicamente paquetes de señalización por ella, en tanto que los de *media* se envían de equipo a equipo.

Media de punto a punto

En el caso de que el audio y/o video se envíen de extremo a extremo (sin pasar por Denwa UC&C 4.0.1), será necesario que ambos equipos utilicen los mismos *Codecs*; caso contrario la comunicación no se establecerá, ya que la función de *Transcoding* la realiza el sistema de comunicaciones unificadas.

- **NAT (*Network Address Translation*)**: es un mecanismo utilizado para intercambiar paquetes entre dos redes que asignan direcciones incompatibles. Esta opción es necesaria para incorporar a la red equipos que lo requieren.
- **SRPT (*Secure Real Time Transport Protocol*)**: define un perfil de RTP, con el que se proporciona cifrado, autentificación del mensaje e integridad, y protección contra reenvíos a los datos en aplicaciones unicast y multicast.
- **Música en espera**: se elige la música en espera para cuando el usuario deja un llamada en espera. Para elegir, la música, primero debe estar cargada en la sección de Configuración >Anuncios >Música en Espera (ver sección Música en Espera en la página 125).

Características de los archivos de audio para la música en espera

Los archivos de audio deben ser WAV con una taza de bits de 128Kbps, el tamaño de su muestra de audio debe ser de 16 bits, de un único canal (mono) taza de muestra de 8 KHz en formato PCM.

- **WebRTC**: al habilitar esta casilla se brinda soporte de protocolo webRTC a la extensión, es decir que podrá utilizar las credenciales SIP a través de la web.
- **ANIs Permitidos**: con esta opción se crea una lista de ANIs (*Automatic Number Identification*) de los cuales se pueden recibir llamadas. Si en este recuadro no hay ningún ANI, no hay restricciones de llamadas entrantes, si en cambio existen ANIs permitidos sólo se pueden recibir llamadas de estos. Para ello se debe hacer clic sobre el ícono de suma (⊕).

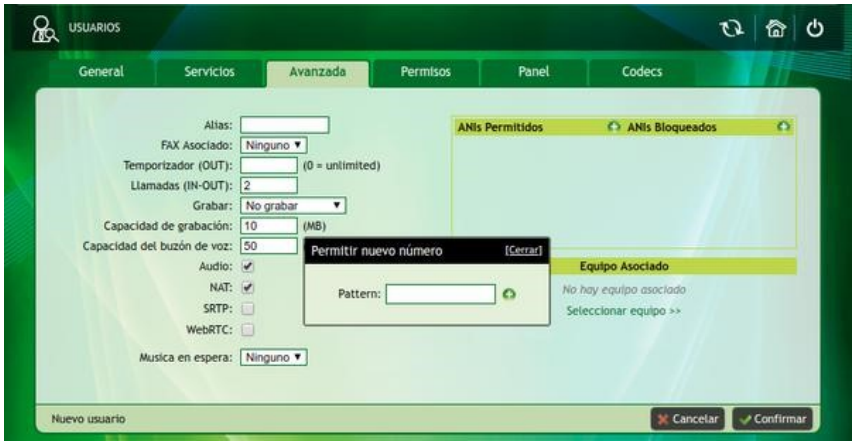

Figura 3.23: Interfaz avanzada: Usuario, lista blanca

ANIs Permitidos en configuración Jefe - Secretaria

En el caso de que se configure en la Pestaña Servicios de Nuevo Usuario la opción Jefe- Secretaria, la extensión de la secretaria se encontrará en este listado. Además, todos aquellos ANIs permitidos, podrán comunicarse de forma directa con el «Jefe» sin necesidad de pasar por la «Secretaria».

- **ANIs Bloqueados**: se crea una lista de ANIs de los cuales no se pueden recibir llamadas.

Usuarios IAX2

Para algunos telefonos con que registran con protocolo IAX2 no se debe solicitar token para su registro. Se agrego la opción de configurar el parametro RCT cuando los internos tienen configurado el protocolo IAX2.

Figura 3.24: Interfaz avanzada: Usuario, permisos del nuevo usuario

3.3.2.3.4. Pestaña Permisos de Nuevo Usuario Desde la pestaña de permisos se puede configurar las siguientes opciones:

- **Permisos de telefonía**
  - **Supervisión de llamadas**: se habilita al usuario a intervenir llamadas, marcando *49 + número de extensión a intervenir. Existen tres formas de realizar esta acción:
    - Presionando el número 4 se puede escuchar la conversación, pero sin poder interactuar con ninguno de los agentes.
    - Presionando el número 5 se puede escuchar la conversación, mientras se interactúa con el usuario intervenido.
    - Presionando el número 6 se puede realizar la comunicación normalmente como en una conferencia.
  - **Habilitar Voceo**: es semejante a un intercomunicador, solo que se aplica a un grupo. Para realizar un voceo a un grupo, se debe marcar *58 + número de extensión (extensión configurada como grupo).
  - **Habilitar Intercomunicador**: se pueden realizar anuncios a una extensión sin necesidad de que el receptor atienda. Esto se logra marcando *59 + número de extensión.
  - **Ocultar Identificador**: permite ocultar la identificación de la extensión en llamadas salientes. Para ello se debe discar el código *36 + Número a marcar.
  - **Rellamar en ocupado**: Cuando el usuario tiene esta opción habilitada, y se realiza una llamada a otro usuario (interno) que se encuentra ocupado, se escucha una notificación acerca de esta situación y la llamada finaliza. En el momento en que el usuario receptor se desocupe, Denwa UC&C 4.0.1 gestiona la comunicación entre ambos usuarios llamándolos a ambos.
  - **Devolver llamada en transferencia**: se genera que la extensión destino de la transferencia desatendida devuelva la llamada al transferente en caso de que la misma no sea contestada.
  - **Llamar desde la red pública**: permite a la extensión llamar desde una red externa a la red privada.

- **Tomar llamadas**: Con esta opción se habilita o no *88 (Tomar llamada Grupo), *89 (Tomar llamada Todos) en cada usuario, la cual permite la toma de llamadas. Las diferentes opciones para tomar llamadas son:
  - Todas
  - Mis Grupos
  - Directo Extensión
  - Ninguna

Figura 3.25: Interfaz avanzada: Usuario, tomar llamadas

- **Permisos UC**
  - **Habilitar Extensión en el Desktop**: se habilita la opción de registrar la extensión en el Denwa Desktop. Este es un software de comunicaciones unificadas que permite desde una única interfaz multi-plataforma acceder a los diferentes servicios.
  - **Habilitar Extensión en el Móvil**: se habilita la opción de registrar la extensión en el móvil. El usuario se debe registrar desde su teléfono móvil mediante el Softphone Denwa agregando a su número de extensión la letra m por delante (por ejemplo, m100). Es necesario, configurar desde el Denwa Desktop la manera en que se desea realizar y recibir las llamadas. Las opciones son Todos, Principal, Web y M óvil.
  - **Habilitar envío de SayIts**: se habilita al usuario a escribir en las Noticias Corporativas. Esto es un servicio dentro del Denwa Desktop, es una red social empresarial que impulsa las comunicaciones internas y construye una forma más robusta de compartir noticias e información.
  - **Habilitar Mensajería Instantánea**: permite a la extensión utilizar la mensajería unificada de Denwa Desktop. Con la mensajería instantánea (IM), se pueden enviar y recibir mensajes multi-usuarios y servicio de soporte online.
  - **Permitir envío de SMS**: se habilita la posibilidad de enviar SMS.
  - **Permitir envío de FAX**: se habilita la posibilidad de enviar FAX.
  - **Generar llamada desde Outlook**: permite la utilización de TAPI SP. Esta opción nos permite monitorear la extensión desde una aplicación Windows como por ejemplo dialer.exe. Los pasos son:
    1. Habilitar la extensión para generar la llamada desde Outlook.
    2. Descargar e instalar setupDenwaTSP (version 32 y 64 bits).
    3. Configurar en la aplicación IP de la central extensión y password de la extensión a monitorear (la extensión a la que le habilitamos TAPI SP).
    4. Configurar dialer.exe, y desde ese software accederemos a varias funcionalidades. Transferencia de llamadas, contactos para ser llamados automaticamente, etc.
  - **Perfil de acceso a módulos**: Existen módulos adicionales adaptados para Denwa UC&C 4.0.1 , cada uno de estos módulos permite asignar un perfil a cada usuario. En el siguiente ejemplo, vemos que esta PBX Denwa tiene instalado el módulo de Hoteles y de Contact Center. Por lo cual a este usuario se le asigna un perfil de Agente.

Figura 3.26: Interfaz avanzada: Usuario, permiso de acceso a módulos

3.3.2.3.5. Pestaña Panel de Nuevo Usuario En la pestaña Panel, se puede asignar usuarios a monitorear al nuevo usuario.

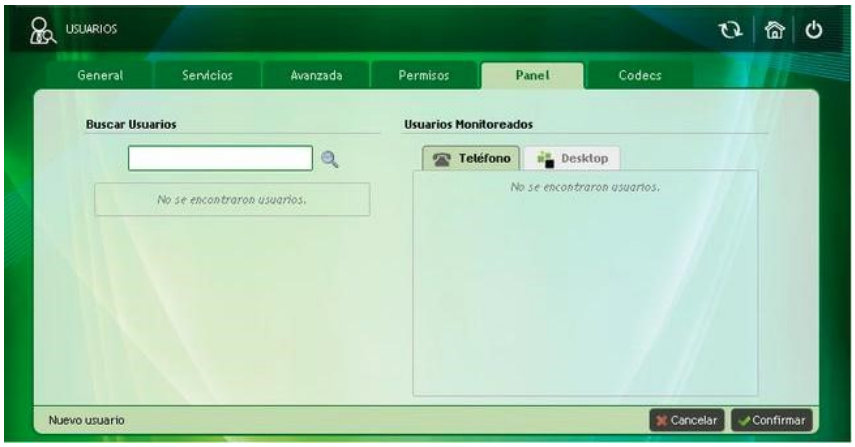

Figura 3.27: Interfaz avanzada: Usuario, panel de usuario

Para iniciar una búsqueda se debe ingresar algún dato referente al usuario a monitorear (nombre, extensión,etc) y luego presionar el botón . En la imagen siguiente se puede observar que se ingresó juan, se presionó el botón de búsqueda, y con eso fue suficiente para encontrar al usuario Juan Perez.

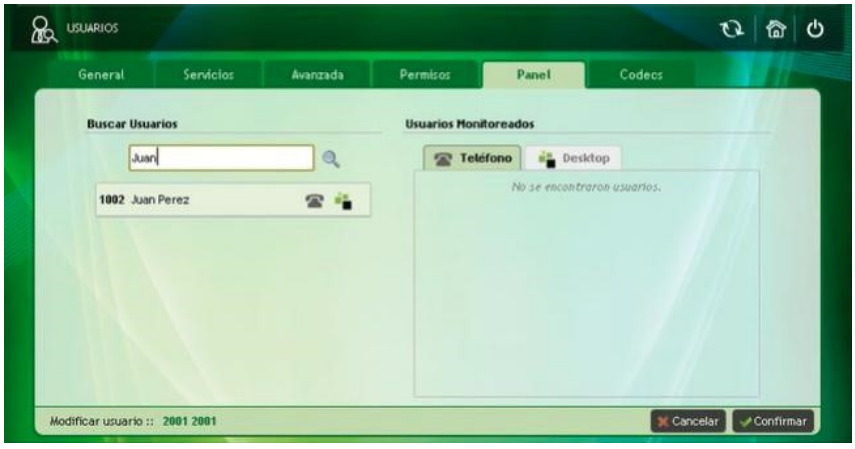

Figura 3.28: Interfaz avanzada: Usuario, panel de usuario (ejemplo)

Luego, para permitir el monitoreo del usuario se debe mediante el botón para el BLF del teléfono, y el botón para el monitoreo en el denwa Desktop seleccionar el deseado.

En el sector derecho de la pantalla se observan dos listas de los usuarios que serán monitoreados, en la pestaña «Teléfono» se encuentran todos los BLF y en la pestaña «Desktop» la lista de los usuarios monitoreados en el Denwa Desktop.

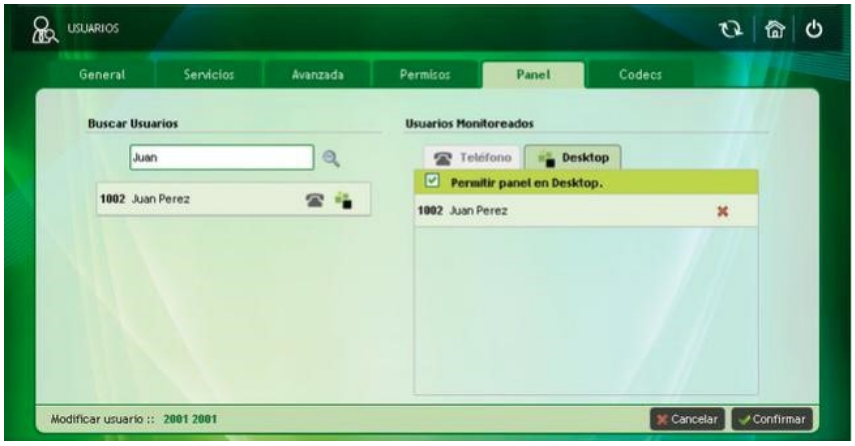

Figura 3.29: Interfaz avanzada: Usuario, panel de usuario: activación de panel en Denwa Desktop

Se puede Permitir panel en el Desktop al aplicar un tilde en la casilla correspondiente, lo que genera que se disponga de una nueva pestaña donde se pueden observar los usuarios monitoreados en el Desktop.

3.3.2.3.6. Pestaña Codecs de Nuevo Usuario Desde esta pestaña se pueden elegir los codecs de audio y video que se le asignarán al usuario. También, se permite seleccionar el modo DTMF y el modo FAX deseado.

Es conveniente, que se selecciones al menos los siguientes codecs:

- **G.729**: es un algoritmo de compresión de datos de audio para voz que comprime audio de voz en trozos de 10 milisegundos. Los tonos tales como los DTMF o de fax no pueden ser transportados confiablemente con este códec. Por lo cual, se debe utilizar así G.711 o métodos de señalización fuera de banda para transportar esas señales. Se recomienda utilizarlo cuando las comunicaciones son salientes de Denwa UC&C 4.0.1 .

- **G.711**: es un estándar de la ITU-T para la codificación de audio. El codificador G.711 proporciona un flujo de datos de 64 Kbit/s. Para este estándar existen dos métodos principales, el μ-law (usado en Estados Unidos y Japón) y el A-law (usado en Europa y el resto del mundo). Este códec se recomienda para comunicaciones entre las extensiones pertenecientes a una misma PBX Denwa (los usuarios conectados a la LAN de la central).

- **H.264**: es una norma que define un códec de vídeo de alta compresión. Este estándar es capaz de proporcionar una buena calidad de imagen con tasas binarias inferiores a los estándares previos.

Figura 3.30: Interfaz avanzada: Usuario, codecs

Los modos DTMF (*Dual-Tone Multi-Frequency*): son señales analógicas necesarias al hacer las llamadas telefónicas.

- **RFC 2833**: se envía las señales DTMF fuera del audio. Se debe evitar utilizarlo con el codecs G.711 ya que en este caso quedarán distorsionados.

- **IN BAND**: los tonos DTMF pueden ser enviados en banda (codificados como el audio). Sólo se puede realizar si la codificación utilizada no emplea ningún tipo de compresión, es el caso de G.711.

- **INFO**: no se recomienda para la entrega de DTMF, debido a que no permite generar la señalización de los dígitos en sincronía con el audio, por lo cual produce desplazamientos temporales.

Los modos FAX: son protocolos que describe cómo enviar y recibir faxs sobre una red de datos.

- **T38**: el fax se convierte en una imagen, luego es necesario que se envíe a otro dispositivo de fax T38 y por último se convierte nuevamente en una señal análoga de fax.

- **T38 Redundancy**: se ofrece una alternativa de T38 para eliminar los efectos de la pérdida de paquetes a través de la redundancia de datos. Es decir se envíanmas de una vez los paquetes; esto aumenta el ancho de banda que se utiliza, pero sigue siendo menor que no usar T38.

- **Pass Through**: cuando se conecta un FAX analógico directamente a una toma FXS, los faxs entran y salen de forma automática, para ello se usa una serie de mecanismos de gestión interno.

3.3.2.4. Importar Usuarios

Es posible importar usuarios desde un archivo en formato .csv simplemente haciendo clic en «Seleccionar archivo», seleccionando el archivo y haciendo clic en «✔ Importar».

Figura 3.31: Interfaz avanzada: Importar Usuarios

Además, es posible generar una versión propia del archivo .csv; para facilitar esta tarea se cuenta con la posibilidad de descargar unas plantillas (haciendo clic en «Plantilla básica» o «Plantilla avanzada»). La diferencia entre ellas es la posibilidad de configuración que presentan: la plantilla básica requiere pocos datos y presenta una configuración limitada; en cambio la plantilla avanzada, permite acceder a todas las configuraciones para crear un nuevo usuario.

- Plantilla básica users_basic.csv:
  - Extensión
  - Contraseña
  - Nombre
  - Apellido
  - Email
  - Número de desvío
  - Tiempo de desvío
  - Idioma
  - Estado (0 deshabilita,1 habilita, 2 suspende)
  - Usuario UM
  - Contraseña UM
  - Tipo
  - Modo
  - Local (0 deshabilita,1 habilita)
  - NDD (0 deshabilita,1 habilita)
  - IDD (0 deshabilita,1 habilita)
  - Mobiles (0 deshabilita,1 habilita)
  - Specials (0 deshabilita,1 habilita)
  - Emergency (0 deshabilita,1 habilita)
  - InterPBX (0 deshabilita,1 habilita)
- Plantilla avanzada users_advanced.csv:
  - Extensión
  - Contraseña
  - Nombre
  - Apellido

- Email
- Número de desvío
- Tiempo de desvío
- Idioma
- Estado (0 deshabilita,1 habilita, 2 suspende)
- Usuario UM
- Contraseña UM
- Tipo
- Modo
- Local (0 deshabilita,1 habilita)
- NDD (0 deshabilita,1 habilita)
- IDD (0 deshabilita,1 habilita)
- Mobiles (0 deshabilita,1 habilita)
- Specials (0 deshabilita,1 habilita)
- Emergency (0 deshabilita,1 habilita)
- InterPBX (0 deshabilita,1 habilita)
- Tipo de grupo (simultáneo, alternado o balanceado)
- Perfil de usuario
- Dispositivo
- Temporizador (OUT)
- Grabar
- Capacidad Buzón Voz
- Capacidad de grabación
- Audio
- NAT
- Llamada desde red pública
- Alias
- Usar PIN de seguridad
- PIN de seguridad
- Usar buzón de voz
- Redireccionar buzón de voz a
- Secretaria
- Permitir envío SMS
- Permitir envío FAX
- Codecs de Audio y Video
- Modo DTMF
- Modo FAX

Se recomienda editar los campos de las plantillas y luego corroborar que el formato no se haya modificado.

3.3.2.5. Generación de Usuarios

Esta funcionalidad permite crear usuarios por lotes, es decir, en un solo paso se puede crear una cantidad determinada de usuarios, con el mismo perfil y opciones de servicios de llamada local.

Figura 3.32: Interfaz avanzada: Generación de usuarios

Para la creación de lote de usuarios se debe:

1. Ingresar el rango de extensiones (desde, hasta) que se desea generar
2. Seleccionar el perfil adecuado para los usuarios, o los servicios de llamada local (ver Perfiles de Usuario en la página Perfiles de Usuario)
3. Hacer clic en «✔ Crear»

En el recuadro inferior: «Progreso de la creación de usuarios» todos los usuarios generados.

3.3.2.6. Perfiles de Usuario

Esta funcionalidad permite que se creen diferentes perfiles para luego poder asignarlos a las extensiones. Estos perfiles permiten limitar el uso telefónico por días, horarios y asignar servicios de llamadas. También es posible configurar que rutas son permitidas para cada uno de los perfiles.

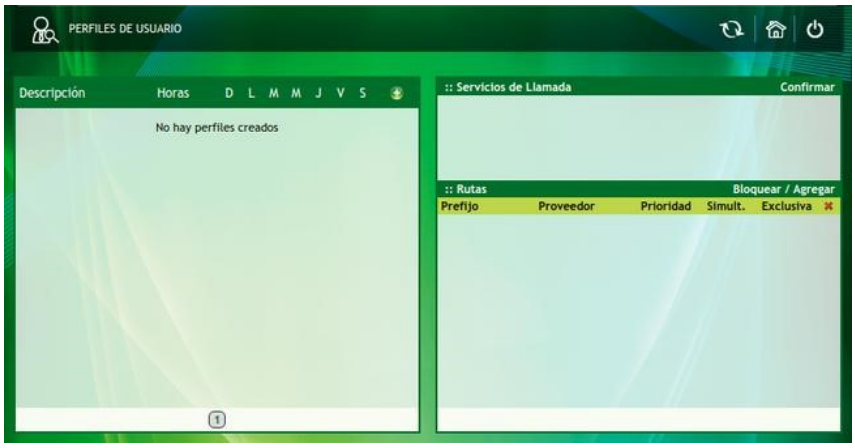

Figura 3.33: Interfaz avanzada: Perfiles de usuario

3.3.2.6.1. Creación de perfil Para comenzar con la creación del perfil, se debe hacer clic en el signo ✚, con ello se mostrará una ventana emergente.

- **Descripción**: Nombre descriptivo del nuevo perfil
- **Desde hora**: Horario al cual iniciará el perfil
- **Hasta hora**: Horario en el que finalizará el perfil
- **Día de la semana**: Seleccionar los días de la semana en los cuales operará el horario antes definido, debe habilitarse la casilla de correspondiente.

Figura 3.34: Interfaz avanzada: Perfiles de usuario, nuevo perfil

Luego se debe presionar «Confirmar» para visualizar el nuevo perfil en el listado.

3.3.2.6.1.1. Modificación del horario Se puede modificar el horario pulsando sobre el ícono ⚙ correspondiente a su fila, esto mostrará una ventana similar a la utilizada para crear el perfil.

3.3.2.6.1.2. Eliminación del perfil Es posible eliminar el perfil pulsando sobre el ícono ✖ correspondiente a su fila.

3.3.2.6.2. Modificación de perfil La modificación de perfil abarca tanto la edición de perfiles de usuario ya existentes, como la configuración inicial de los perfiles recientemente creados.

3.3.2.6.2.1. Administración: Servicios de Llamada Se puede establecer los servicios de llamada asociados al perfil en el cuadro derecho superior de la pantalla. Permite gestionar los permisos para realizar diversos tipos de llamadas.

Pueden encontrarse habilitados o permitidos (✔), denegados (✖) o protegidos por el Pin de Seguridad (🔒); también es posible indicar la cantidad de segundos permitidos para cada uno de los distintos prefijos, en caso de desear que sea ilimitado el valor debe ser de cero (0).

Configuración de los Servicios de llamada

Los prefijos que corresponden con cada tipo de llamada se deben ser configurados en Servicios de Llamadas (ver Servicio de llamadas en la página 120).

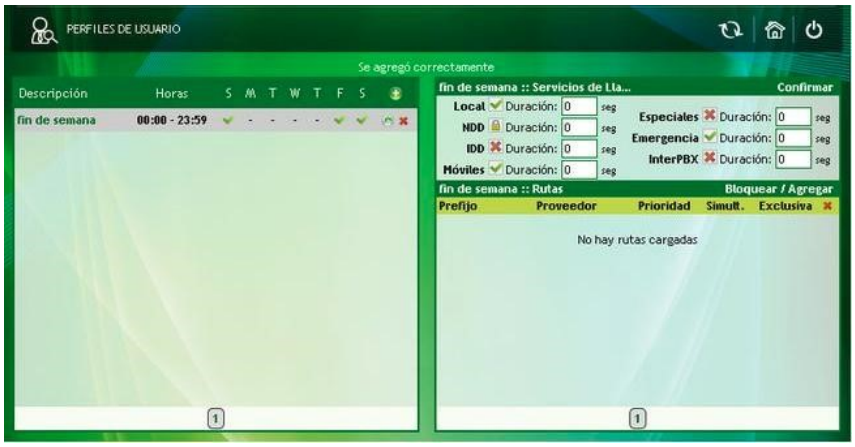

Figura 3.35: Interfaz avanzada: Perfiles de usuario, servicios de llamada

Una vez realizada la configuración deseada, es necesario hacer clic en «Confirmar».

3.3.2.6.2.2. Administración: Rutas Es posible (y necesario) agregar rutas para el perfil, para ello:

- Se debe hacer clic en «Agregar» (ubicado en el recuadro de Rutas).
- Luego se busca una ruta, esto se puede realizar por prefijo y/o por proveedores.
- Cuando se encuentran las rutas, se seleccionan con tildes en los las casillas de la derecha, se asignan las prioridad y cantidad de llamadas simultáneas, para que sea de uso ilimitado debe colocarse un cero (0)

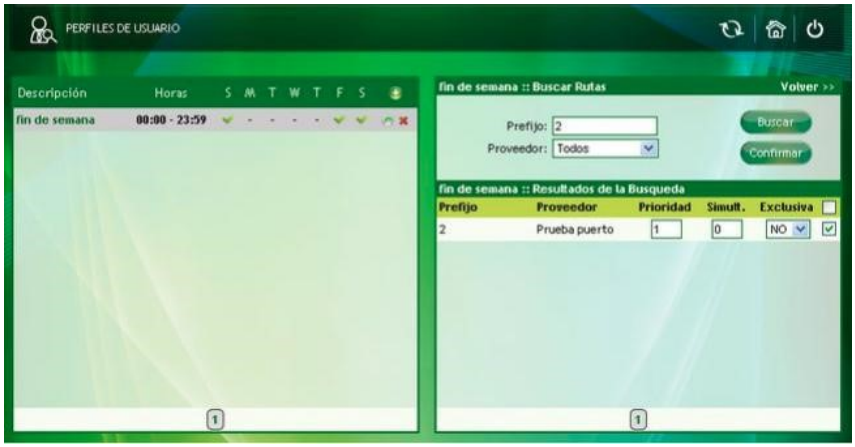

Figura 3.36: Interfaz avanzada: Perfiles de usuario, rutas

Una vez que se haya seleccionado y configurado las rutas, bastará con pulsar sobre el botón «Confirmar». En caso de no desear guardar los cambios, se debe pulsar sobre el texto «volver».

Del mismo modo es posible restringir el uso de un proveedor, pulsando sobre «Bloquear» en lugar de «Agregar».

3.3.2.7. Directorio Corporativo

Con el directorio corporativo, se pueden subir listas de contactos para utilizarlas en usuarios que dispongan del Denwa Desktop.

Figura 3.37: Interfaz avanzada: Directorio Corporativo

3.3.2.7.1. Pestaña Buscar En esta pestaña se observa la lista de los contactos disponibles en el Directorio Corporativo. La búsqueda se puede realizar por Nombre, Email o Número, pulsando sobre el ícono 🔍 en el encabezado de la tabla. También se encuentra información respectiva a su dirección.

En caso de necesitar trabajar con la lista de contactos, se puede exportar el directorio con el botón «📥 Exportar», el cual generará un archivo en formato .csv.

Figura 3.38: Interfaz avanzada: Directorio Corporativo, descarga de CSV

Además se cuenta con la posiblidad de borrar todo el directorio coorporativo pulsando sobre el botón «✖ Borrar»; eliminar un único contacto, haciendo clic en el ícono ✖ en su fila correspondiente, o editar un contacto al hacer clic sobre su nombre.

Figura 3.39: Interfaz avanzada: Directorio Corporativo, edición de contacto

3.3.2.7.2. Pestaña Importar Con la Plantilla básica se puede descargar el archivo contacts_basic.csv que servirá como guía al diseñar la lista de contactos del directorio corporativo. Una vez que los contactos deseados fueron ingresados a la planilla, se pulsa sobre el botón «Seleccionar archivo» para buscarlo entre los directorios del ordenado y luego, presionando

el botón «✔ Importar» iniciará el proceso de importación. En caso de existir problemas con alguna entrada del directorio, se mostrará con una ✖.

Figura 3.40: Interfaz avanzada: Directorio Corportativo, importar contactos

3.3.3. Grupos

Desde la pestaña Grupos se puede realizar el manejo y la administración de los mismos. Se pueden crear grupos de usuarios que se pueden utilizar como:

- Grupos de llamadas.
- Grupos para luego asignarles ciertas características y relaciones con los demás, aunque no sea un grupo destinado a recibir llamadas.

3.3.3.1. Ver Grupos

Permite visualizar y editar todos los grupos creados, así como sus características.

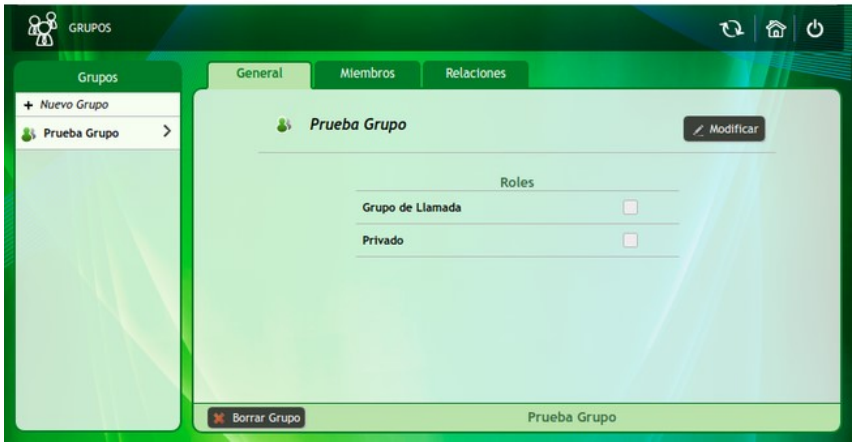

Figura 3.41: Interfaz avanzada: Ver Grupos

En el listado de grupos aparecen los nombres de todos los grupos creados en la PBX en cuestión. Al hacer clic sobre el nombre de un grupo se pueden realizar modificaciones en las distintas pestañas

3.3.3.1.1. Pestaña General

- **Modificar**: permite realizar cambios tanto en el nombre del grupo como en el icono del mismo.

- **Roles**: refieren al comportamiento que tendrán las llamadas del grupo.
  - **Grupo de Llamada**: sólo los grupos que cumplan este rol pueden formar parte del preatendedor. Además, activa las llamadas entre los usuarios del mismo grupo, también con usuarios que no pertenezcan al mismo. Al tildar en el checkbox, para optar por esta opción, se despliega la siguiente ventana.

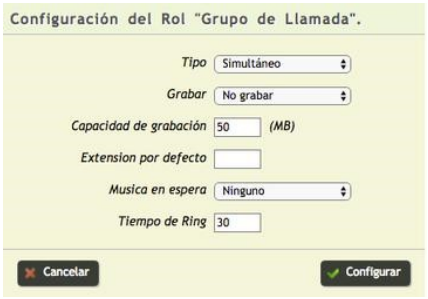

Figura 3.42: Interfaz avanzada: Configuración del grupo de llamada

  - **Tipo**: indica el curso que debe seguir cada una de las llamadas entrantes al grupo. Las opciones que brinda el menú desplegable son
    - **Simultáneo**: al ingresar una llamada al grupo suenan todos los teléfonos que pertenezcan a él; cuando uno de ellos atiende la llamada los demás teléfonos dejan de sonar.
    - **Alternado**: este modo utiliza el orden lista de Miembros del grupo (ver siguiente figura); es decir, que al ingresar una llamada suena el teléfono del primer miembro de dicha lista, la segunda llamada va con destino al segundo miembro y así sucesivamente.
    - **Balanceado**: al igual que el modo anterior, este modo utiliza la lista de Miembros del grupo (ver siguiente figura), es capaz de analizar quien ha recibido la menor cantidad de llamadas. Para luego, asignarle a éste la nueva llamada entrante.
  - **Grabar**: permite grabar (o no) las llamadas entrantes y salientes. Este menú desplegable brinda las siguientes opciones:
    - **No grabar**: tal como lo indica su nombre, este modo no graba ninguna llamada, ni entrante ni saliente.
    - **TODOS - Continuo**: se graban todas las llamadas; es decir la de todos los miembros del grupo, tanto entrantes como salientes.
    - **TODOS - Aleatorio**: sólo se graban algunas llamadas de cualquier miembro que pertenezca al grupo.
  - **Capacidad de grabación**: es la capacidad para almacenar las grabaciones de las llamadas, por defecto es de 10MB pero es posible cambiar este valor directamente desde el recuadro. Cuando esta capacidad (o cuota) llega a su máximo pueden ocurrir dos cosas: la primera es que se comiencen a sobrescribir las grabaciones más antiguas con las recientes y la segunda es tener creado un cliente FTP (Protocolo de Transferencia de Archivos) al cual se exportan las grabaciones una vez que se llego al máximo de la cuota. Para configurar el cliente FTP es necesario ver Pesta ña Respaldo de General (Configuración >General >Respaldo).
  - **Extensión por defecto**: refiere a la extensión, que no pertenece al grupo, que suena en caso de que la llamada no haya sido respondida por los integrantes correspondientes al grupo.
  - **Música en Espera**: Se elige la música en espera que se reproduce cuando las extensiones del grupo están sonando. Sólo aplica para la estrategia en Simultáneo y para elegir la música, previamente se debe cargar en la sección de Configuración >Anuncios >Música en Espera (ver Música en Espera en la página 125).

- **Tiempo de Ring**: indica el tiempo que suena el teléfono, la unidad que se utiliza es «segundos».

- **Privado**: corta las relaciones del grupo en cuestión con el resto, al efectuar clic en su checkbox se abre la ventana que se muestra a continuación, para aceptar este rol es necesario hacer clic en Configurar

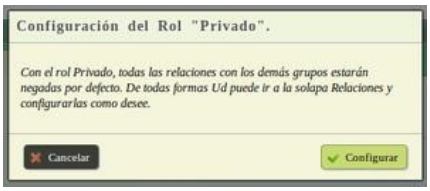

Figura 3.43: Interfaz avanzada: Configuración del grupo privado

3.3.3.1.2. Pestaña Miembros Se brinda la opción de eliminar miembros del grupo con sólo hacer un clic en el ícono ✖ situado a la derecha de cada uno de ellos. También es posible incorporar usuarios desde «✪ Agregar miembros», con ello se abre una ventana como la siguiente:

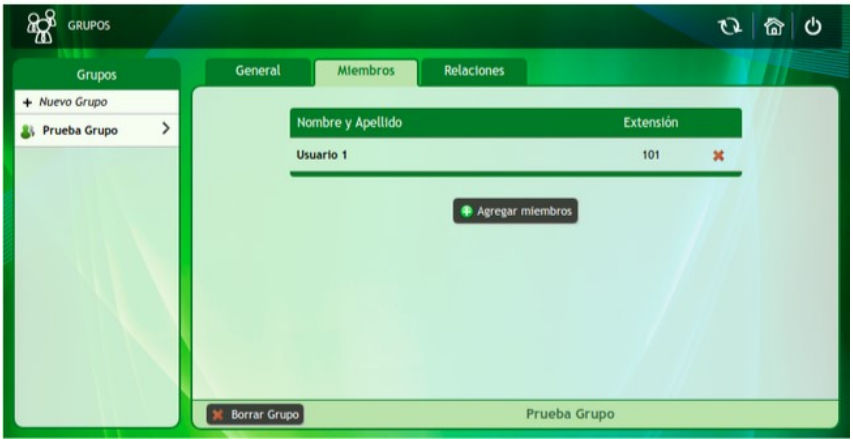

Figura 3.44: Interfaz avanzada: Configuración de miembros

En ella se deberá escribir el nombre de usuario en el recuadro blanco, actualizándose automáticamente el listado en la parte inferior de la ventana. Es posible agregarlos al grupo haciendo clic en ✚, usuario a usuario. Finalmente se guardan los cambios, pulsando en «✔ Agregar miembros».

Figura 3.45: Interfaz avanzada: Agregar miembros

3.3.3.1.3. Pestaña Relaciones Se relacionan las funciones generales y de Desktop entre dos grupos, el grupo en cuestión con el grupo que se seleccione. Las flechas que indican los permisos que tiene un grupo para con el otro, cambian de color (habilitando o deshabilitando) con sólo hacer clic sobre ellas.

- **Mensajería Instantánea**: son aquellos mensajes que se pueden enviar desde un grupo a otro.
- **Calendario**: permite compartir entre grupos las actividades de la agenda, tales como eventos, tareas, llamadas, reuniones, aniversario y notas.
- **Conversaciones**: incluye las funciones de envío de mensajes, SMS y Fax. El envío de mensajes llega tanto al Desktop como a la dirección de email de cada miembro del grupo.
- **Monitoreo de llamadas**: habilita la oportunidad de supervisar o no llamadas de un grupo en particular, para ello se debe activar el permiso de Supervisión de Llamadas (Pestaña Permisos de Nuevo Usuario) a todos los usuarios del grupo que puede realizar esta acción. En este ejemplo, los usuarios integrantes del grupo 1, deben tener permiso de supervisión de usuario y relación de monitoreo de llamadas activada para monitorear a un usuario perteneciente al grupo 2. La acción se realiza discando *49 + Número de extensión a monitorear.

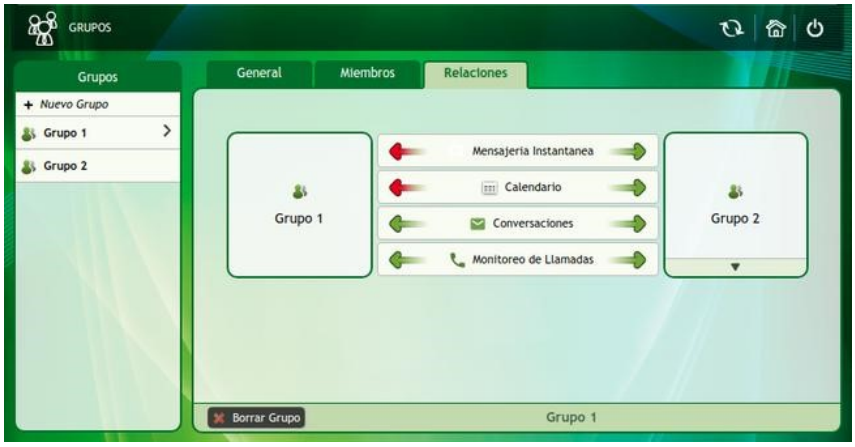

Figura 3.46: Interfaz avanzada: Relaciones de grupos

Una vez que la relación entre ambos grupos se encuentre de la manera deseada, los cambios serán guardados al pulsar sobre «✔ Aplicar cambios»; en caso de desear reestablecerlo a un estado previo (si aún no se ha guardado), se deberá pulsar sobre «↺ Deshacer cambios».

3.3.3.1.4. Nuevo grupo Adicionalmente, pulsando sobre «⊕ Nuevo Grupo» (columna a la izquierda de la pantalla) muestra una ventana en donde se solicita el nombre e icono del grupo, tal como lo muestra en la siguiente figura. Para confirmar estos cambios se debe hacer clic en «✔ Crear». En esta instancia el grupo ha sido creado, por lo que en la columna Grupos se visualiza el mismo.

3.3.3.2. Nuevo Grupo

Esto conduce a una ventana que solicita el nombre e icono del grupo, tal como lo muestra en la siguiente figura (Fig. A.). Para confirmar estos cambios se debe hacer clic en Crear. En esta instancia el grupo ha sido creado, por lo que en la columna Grupos se visualiza el mismo.

3.3.3.3. Centro de costos

La opción Centro de costos permite asignar costos a las llamadas, discriminando los tipos de llamadas, los destinos y los usuarios.

Figura 3.47: Interfaz avanzada: Centro de costos

En primera instancia, se debe crear un nuevo centro de costos. Para lo cual es necesario completar los campos que se muestran a continuación y posteriormente hacer clic en «✔ Confirmar»:

- **Descripción**: se completa con una breve descripción o nombre de este nuevo centro de costos.
- **Día de recarga**: refiere al día del mes en que efectúa la carga para hacer llamadas.
- **Monto**: es la capacidad disponible para efectuar llamadas, siendo este monto la cantidad de pesos que se asignan a esa cuenta hasta la nueva recarga del mes siguiente. El saldo no es acumulable con el monto del nuevo mes.

Una vez que se tiene generado el centro de costos, es momento de asignar el monto por minuto de los distintos tipos de llamadas (ver Servicio de llamadas en la página 120)

Figura 3.48: Interfaz avanzada: Centro de costos y tipos de llamado

Por supuesto que se puede utilizar la opción «modificar / borrar» para efectuar cambios en el centro de costos o eliminarlo directamente.

Ahora es el momento de incorporar usuarios al centro de costos, para lo cual es necesario hacer clic en «Agregar». Luego, se abre una ventana que presenta un menú desplegable sencillo; el cual permite buscar usuarios por extensión, nombre o apellido. Si este campo se deja en blanco y se presiona Buscar, muestra una lista con todos los usuarios de la PBX y se

pueden seleccionar los usuarios que se quieran agregar al centro de costos directamente desde esta lista.

Figura 3.49: Interfaz avanzada: Adición de usuarios al centro de costos

Configuración de Centro de costos

Estos procedimientos se deben hacer para cada uno de los centros de costos existentes.

3.3.4. Proveedores

Los proveedores sirven para crear vínculos virtuales, mediante el uso de diversos troncales (trunks). Es decir, que los troncales sirven para crear conexiones con otras centrales PBX, operadores VoIP y con el mundo externo PSTN. Entre los distintos tipos de troncales se encuentran: TDM, SIP, DenwaPBX InterConn, Asterisk InterConn, entre otros.

Cada troncal tiene definidos códigos de países y áreas donde se pueden enviar y/o recibir llamadas; por ejemplo: 1786 Miami (USA) ó 54351 Córdoba (Argentina), a éstas se las llaman rutas.

Un troncal puede usar el método de registro para intercambiar credenciales de seguridad con el operador, en ese caso sólo permite enviar y recibir llamadas con ese operador siempre que esté registrado.

3.3.4.1. Ver Proveedores

Desde este menú se observa la lista de proveedores o troncales (ver siguiente figura), que brinda la siguiente información:

- **Descripción**: refiere simplemente al nombre del troncal.
- **IP**: es aquella dirección IP de destino de del troncal; por ejemplo, se tienen dos centrales, A y B, al configurar A se coloca la dirección IP de B y viceversa.
- **Tipo**: en esta columna se detalla si el enlace es:
  - **OUT**: sólo se pueden realizar llamadas, pero no existe llamas entrantes.
  - **IN**: no es posible realizar llamadas ya que solamente existen llamadas entrantes.
  - **INOUT**: esta habilitado tanto para realizar llamadas, como para recibirlas.
- **Protocolo**: permite visualizar de manera rápida el protocolo que utiliza el troncal en cuestión (ver Pestaña General de Nuevo Proveedor).
- **Registrado**: esta columna expone si Denwa UC&C 4.0.1 esta registrada o no como cliente del proveedor, en caso que el mismo lo solicite.
- **Acción**: presenta las opciones para directamente eliminar al proveedor (✖) o para modificarlo (🖉). Esta última opción permite editar las opciones que tiene un nuevo proveedor (ver Nuevo Proveedor en la página 60).

3.3.4.1.1. Configuración de proveedor Al realizar clic sobre el nombre descriptivo que se ha seleccionado para el troncal (en la primer columna) se muestra la ventana de configuración, desde ella es posible definir: las rutas, los números de acceso y planes de discado.

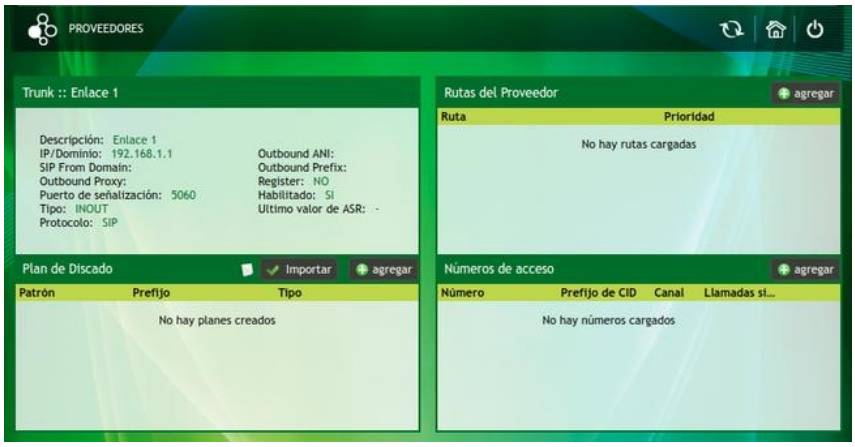

Figura 3.50: Interfaz avanzada: Configuración del proveedor

Se observan cuatro recuadros, que se explican a continuación.

- **Trunk**: se permite verificar los detalles del enlace.
- **Prefijos del proveedor**: al realizar clic en «⊕ agregar» se despliega la siguiente ventana:

Figura 3.51: Interfaz avanzada: Prefijos del proveedor

  - Ruta: aquellos dígitos que se designen como ruta son los que saldrán por el troncal en cuestión.
  - Prioridad: se permite asignar un orden de prioridades del 1 al 9, para el caso que existan distintos caminos para cursar la llamada. Por ejemplo:
    Si la ruta es 4 entonces coincide con todas aquellas llamadas que comiencen con 4. En cambio, si la ruta es 567, cursará las llamadas que comiencen con 567. Se debe tener en cuenta que la cantidad de dígitos que van a continuación de los que refieren a las rutas es indistinto.
    Al finalizar se debe pulsar «✔ Confirmar», para guardar la nueva ruta.

Sobre la seguridad de los proveedores

Se ofrecerá más información para su configuración en el apartado de Seguridad (ver Ruta de proveedores en la página 168)

- **Números de acceso** : Este ítem refiere al número de ingreso que tiene asociado el troncal (que puede ser más de uno); o sea, se asigna el número de acceso para poder recibir llamadas desde el mismo proveedor. Para agregarlos se debe hacer clic en «⊕ agregar» y agregar la siguiente información en la ventana emergente:

Figura 3.52: Interfaz avanzada: Números de acceso

- **Número**: refiere a la línea, analógica o digital, que brinda el proveedor para tener conexión con la PSTN. Se pueden usar los campos «Desde» y «Hasta», si se tiene más de una línea y con numeración consecutiva.
- **Llamadas simultáneas**: permite seleccionar la cantidad de llamadas entrantes simultaneas que podrá cursar el troncal para las líneas del ítem anterior. Por defecto es el 0 que indica la posibilidad que las llamadas sean ilimitadas.
- **Prefijo de CID**: es el prefijo (por supuesto numérico) de llamada entrante. Para el caso que el proveedor no brinde este servicio, se puede establecer un prefijo para diferenciar de que proveedor es la llamada entrante.
- Finalmente se debe pulsar «✔ Confirmar» con el objetivo de aceptar estos cambios.

- **Plan de discado**: Este plan es sólo para llamadas de salida del troncal, tiene el objetivo de dirigir las llamadas de manera simple y correcta. Existen dos formas de agregar un Plan de Discado:

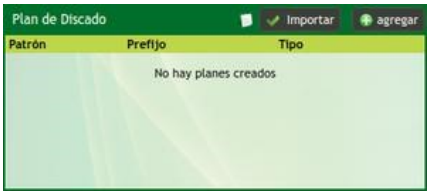

Figura 3.53: Interfaz avanzada: Plan de discado

1. La primera de ellas es necesario realizar clic en «⊕ agregar» se despliega la siguiente ventana

Figura 3.54: Interfaz avanzada: Nuevo plan de discado

2. La segunda de ellas es necesario realizar clic en «✔ Importar», allí seleccionaremos el archivo con los planes de discado que deseemos agregar. Para facilitar la creación del archivo se cuenta con la posibilidad de descargar una plantilla realizando clic en el botón 🗋. Hay que tener en cuenta que el archivo a importar sea de formato .csv y se recomienda editar los campos de las plantillas y luego corroborar que el formato no se haya modificado.

En ambos casos se deberá completar la siguiente información:

- **Patrón**: son los dígitos de referencia para los números salientes de la central. Ambos se comparan y si son coincidentes se puede modificar o quitar.
- **Prefijo**: depende del proveedor. Si los patrones son coincidentes el prefijo reemplaza al patrón; pero si el prefijo esta vacío directamente se quita el patrón.
- **Tipo**: el plan de discado siempre es para las llamadas salientes de la central.

Por ejemplo:

Patrón	Prefijo	Coincide con	Se reemplaza por
471T ó 471*	54351471	471xxxxxx	54351471xxxxxx
471555555	54351478666666	471555555	54351471666666
21.3T ó 21_3*	552193	21x3xxxxxx	552193xxxxxx
47.555555 ó 47_555555	54351478666666	47x555555	54351478666666

3.3.4.2. Nuevo Proveedor

Para generar un nuevo proveedor o troncal, debe ingresar a la opción Nuevo Proveedor y completar los datos que muestra la pantalla.

Figura 3.55: Interfaz avanzada: Nuevo Proveedor

Al confirmar dispondrá de cuatro (4) pestañas que serán detalladas a continuación.

3.3.4.2.1. Pestaña General de Nuevo Proveedor La primer pestaña es General, desde aquí es posible realizar la configuración básica del troncal, llenando los campos que se observan en la siguiente figura.

Figura 3.56: Interfaz avanzada: Configuración general del proveedor

- **Descripción**: refiere al nombre que se selecciona para el enlace troncal.
- **Protocolo**: se define un protocolo para el troncal que se esta creando. En el listado de protocolos es posible localizar los TDM; que emplean tanto placas analógicas como digitales. Además, existe TDM Premium que, como su nombre lo indica, se incluye sólo en el modelo Denwa Premium. Se debe tener en cuenta que todos aquellos protocolos InterConn se aplican para vincular dos centrales PBX.
  - SIP
  - TDM
  - TDM Khomp

- DenwaPBX InterConn
- SIP Microsoft ICS
- SIP Microsoft Lync
- SIP Lotus Domino
- SIP Skype for Business
- SIP with SMS
- SIP - Argentina - Metrotel
- SIP - Costa Rica - ICE
- SIP - Peru - Globalbackbone
- SIP - Panama - CableAndWireless
- SIP - Mexico - Alestra
- SIP - Mexico - Movistar
- SIP - México - Izzi
- SIP - México - Axtel
- SIP - México - Axtel - Broadsoft
- Asterisk InterConn
- TDM InterConn
- H323.

Versiones de SIP

Del ítem anterior, el protocolo más común utilizado para señalización entre los extremos conectados es SIP. El resto de los protocolos SIP que se observan en el listado anterior se han personalizado para algún cliente en particular. También se encuentra en dicho listado Asterisk InterConn que, a diferencia del resto, utiliza el protocolo IAX (Inter-Asterisk eXchange).

- **Protocolo de transporte**: permite elegir la señalización entre TCP o UDP. De los protocolos del listado anterior, sólo SIP Microsof Lync utiliza TCP; mientras que el resto utiliza UDP.
- **Utilizar SBC**: al hacer clic en su checkbox se habilita el SBC (Session Border Controller) en el troncal. Esta opción se encuentra disponible sólo en el modelo Denwa Premium.
- **IP/Dominio**: refiere a la dirección IP o dominio del equipo conectado en el otro extremo del troncal. Para el caso de un troncal tipo TDM, Denwa utiliza el localhost.
- **SIP From Domain**: se utiliza para aquellos operadores que solicitan el cambio en el campo From del encabezado del paquete SIP.
- **Puerto de Señalización**: indica el puerto donde el troncal atenderá los requerimientos SIP; por defecto es el puerto 5060.
- **Tipo**: el troncal se puede configurar para sólo realizar llamadas, sólo recibirlas o ambas. Para ello se tienen las opciones OUT, IN e INOUT, respectivamente.
- **Aceptar nombre a mostrar**: al dar clic en el checkbox correspondiente, cuando se recibe una llamada se visualiza el nombre de quien llama (Display Name) si el proveedor brinda este servicio.
- **Es interconn**: permite realizar llamadas directamente a extensiones configuradas en DenwaUC sin DIDs y utilizar las rutas configuradas en otros proveedores.
- **Estado**: esta opción posibilita habilitar o deshabilitar el troncal.

- **Outbound Proxy**: este recuadro se debe completar si el proveedor lo requiere; ya que se coloca automáticamente en el campo Proxy del encabezado SIP. Es decir, que si se habilita esta opción todas las llamadas se envían a este IP o dominio y el IP o dominio del troncal solo se usa para registro.
- **Outbound ANI**: si el proveedor lo solicita el ANI (Automatic Number Identification) puede ser siempre el mismo. Completando este recuadro, queda fija la información en el campo ANI del encabezado SIP.
- **Outbound Prefix**: es el prefijo que se antepone a cada llamada saliente. Sólo se completa este campo si el proveedor lo requiere para autenticar la llamada. Esta opción agrega el prefijo sin necesidad de hacer un plan de discado.
- **Registrar**: si se tilda en el checkbox correspondiente se habilitan los tres campos siguientes.
  - **Usuario**: es la identificación que el troncal utiliza para autentificarse en el servidor de destino, generalmente el número telefónico asignado a este troncal.
  - **Usuario de Autenticación**: es para una doble autenticación, para así brindar mayor seguridad.
  - **Contraseña**: es la clave para autenticación durante el registro.

Disponibilidad de campos

Dependiendo del protocolo que se seleccione se podrá disponer o no de la totalidad de las opciones mencionadas anteriormente. Esta variación es debida a las características del protocolo. Estos protocolos están definidos AQUÍ.

Proveedores y *Firewall*

Cuando se crea un trunk o se modifica su IP, se agregan las mismas a las reglas de alta prioridad de usuario en el firewall. Esto se aplica a proveedores SIP, DENWAPBXIC y H323. Se generarán automáticamente dos reglas por proveedor, una para protocolo SIP y otra RTP.

3.3.4.2.2. Pestaña Avanzada de Nuevo Proveedor

Luego de crear el troncal o proveedor es necesario asignar canales. Esta asignación se realiza dependiendo del protocolo utilizado, tal como se muestra a continuación.

3.3.4.2.2.1. SIP y DenwaPBX InterConn

En el caso de interconexión SIP simplemente es necesario definir la cantidad de canales que se pueden utilizar. Lo mismo ocurre cuando se utilizan troncales DenwaPBX InterConn.

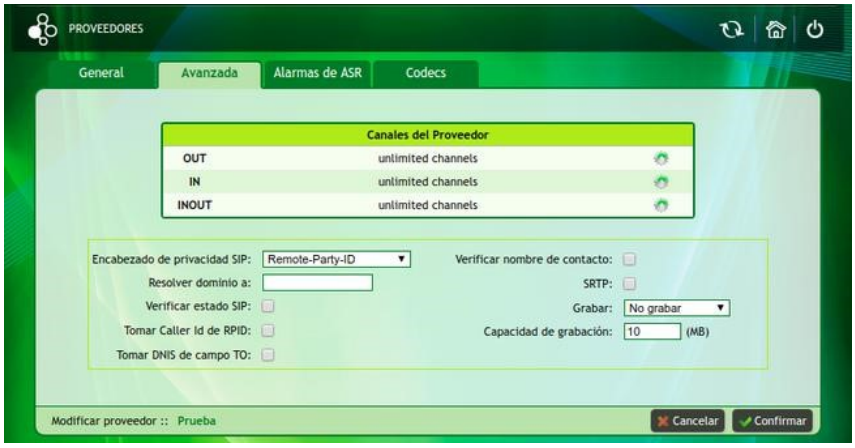

Figura 3.57: Interfaz avanzada: Configuración avanzada del proveedor

- **Canales del proveedor**: con sólo hacer clic en el ícono ⚙ a la derecha del mismo se puede cambiar la cantidad de canales asignada. Se debe tener cuidado con la cantidad de canales que se asignan, por que si se coloca un número menor al existente, se pierden las configuraciones de los canales SMS.
- **Opcionales**:
  - **Encabezado de privacidad SIP**: estas alternativas son para cuando se arma el encabezado SIP, sirven para seleccionar como se envía el Caller ID al destino. Las opciones que brinda el menú desplegable son Remote-Party-ID y P-Asserted-Identity.
  - **Resolver dominio a**: en este recuadro se coloca el IP del proveedor para resolver el Dominio del troncal (este dominio es el que se completa en Proveedor >General).
  - **Verificar estado SIP**: si se tilda el el checkbox correspondiente se verifica el estado de conexión del equipo remoto mediante SIP.
  - **Tomar Caller Id de RPID**: con esta opción, se toma el dato de quien llama (caller id) desde el Remote-Party-ID
  - **Tomar DNIS de campo TO**: con esta opción, se toma el dato de quien llama (DNIS) desde el campo TO en la señalización SIP
  - **Verificar el nombre de contacto**: al tildar en el checkbox cuando se realiza o se recibe una llamada, la central consulta por este ID en bases de datos públicas (Ej: CNAME), de tal manera que visualiza el nombre de quien corresponde el ID
  - **SRTP**: Con esta opción, encripta el audio RTP de las llamadas salientes por este troncal
  - **Grabar**: permite configurar la grabación de llamadas por el troncal
  - **Capacidad de Grabación**: Permite asignar una cuota de grabación (espacio de disco) para las grabaciones de la llamadas realizas por este troncal

3.3.4.2.2.2. Asterisk InterConn Este tipo de troncal brinda las mismas ventajas que TDM InterConn, pero con la particularidad de que utiliza el protocolo IAX2 (Inter-Asterisk eXchange protocol) para la señalización.

Figura 3.58: Interfaz avanzada: Configuración avanzada del proveedor con Asterisk Interconn

- **Canales del proveedor**: con sólo hacer clic en el ícono ⚙ a la derecha del mismo se puede cambiar la cantidad de canales asignada. Se debe tener cuidado con la cantidad de canales que se asignan, por que si se coloca un número menor al existente, se pierden las configuraciones de los canales SMS.
- **Opcionales**:
  - **Capacidad de Grabación**: Permite asignar una cuota de grabación (espacio de disco) para las grabaciones de las llamadas realizadas por este troncal.

- **Grabar**: Permite setear la capacidad de llamar las grabaciones por el troncal.
- **Verificar el nombre de contacto**: al tildar en el checkbox cuando se realiza una llamada, en el extremo receptor, se visualiza el nombre de quien esta realizando dicha llamada.
- **SRTP**: al tildar en la casilla, permite encriptar el audio de las llamadas.

Con el objetivo de que funcione de manera correcta este protocolo, se debe configurar en el otro extremo el cliente Asterisk. Para ello, se recomiendan las siguientes configuraciones dentro del archivo iax.conf:

- Con autenticación

```
[USERNAME]
auth=plaintext
secret=PASSWORD
type=friend
permit=DENWAIP
context=default
host=DENWAIP
port=4569
disallow=all
allow=g729
allow=ulaw
allow=alaw
allow=ilbc
allow=gsm
allow=h264
allow=h263p
allow=h263
```

Archivo iax.conf modificado para uso con autenticación

- Sin autenticación

```
[DENWAIP]
type=friend
permit=DENWAIP
context=default
host=DENWAIP
port=4569
disallow=all
allow=g729
allow=ulaw
allow=alaw
allow=ilbc
allow=gsm
allow=h264
allow=h263p
allow=h263
```

Archivo iax.conf modificado para uso sin autenticación

3.3.4.2.3. Pestaña Alarmas de ASR de Nuevo Proveedor El ASR (*Answer Seizure Ratio*) es uno de los índices que mide la calidad de la red y la tasa de éxito de las llamadas. Se calcula como el porcentaje de llamadas atendidas con respecto al total del volumen de llamadas. Se pueden activar las alarmas ASR con el fin de detectar problemas en cuanto a la cantidad de llamadas cursadas.

Como se muestra en la imagen anterior, los campos a configurar son los siguientes:

- **Alarmas de ASR**: con sólo hacer un clic en la casilla se activan o desactivan. En caso de tildar esta opción, se habilitan los siguientes tres campos de opciones
  - **Umbral de ASR**: es el porcentaje límite con el cual la alarma se activa
  - **Chequear cada**: se coloca el tiempo, en segundos, que se debe esperar para la ejecución del chequeo de ASR

- **Chequear los últimos**: en este ítem se escoge el tiempo, en segundos, en el cual se contabilizan las llamadas atendidas y total de llamadas

- **Enviar alertas por email**: al realizar clic en el checkbox correspondiente se habilita el envío de reportes por email
- **Email**: este campo se dispone sólo si se ha tildado la opción anterior y permite colocar la dirección de email a la cual se envían los reportes de alarmas ASR

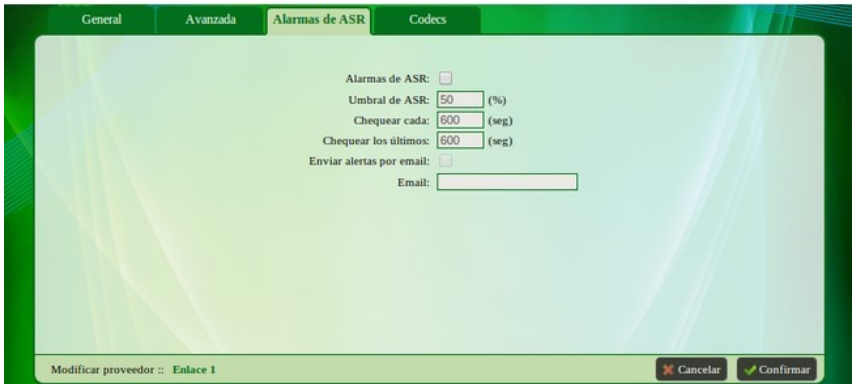

Figura 3.59: Interfaz avanzada: Configuración alarmas de ASR del proveedor

Condición de envío de las alertas

Para el correcto funcionamiento de estas alertas, se debe configurar previamente el servidor de correo electrónico en Configuración >General >Servidor de Correo (ver sección Pestaña Servidor de Correo en la página 92).

Para aplicar los cambios ingresados, solamente se necesita realizar un clic en «✔ Confirmar».

3.3.4.2.4. Pestaña Codecs de Nuevo Proveedor

Como es de esperar, en esta pestaña se deben seleccionar los Codecs, tanto los de audio como los de vídeo, que utiliza el troncal. Además, se requiere la selección del protocolo a usar en modo DTMF y modo FAX.

Figura 3.60: Interfaz avanzada: Configuración codecs del proveedor

Para más información sobre los codecs de audio y video se puede consultar la Pestaña Codecs de Nuevo Usuario (ver Pestaña Codecs de Nuevo Usuario en la página 44).

3.3.4.3. Rutas

En la siguiente imagen se visualiza la ventana de Proveedores >Rutas, la cual proporciona un mecanismo de búsqueda y hace que la misma sea más rápida y eficiente.

Figura 3.61: Interfaz avanzada: Consulta de rutas de los proveedores

En el recuadro de la izquierda de la pantalla: «Buscar Rutas», se brinda la opción de realizar la búsqueda de ruta saliente aplicando alguna clase de filtro, ya sea mediante el uso de textos o por la selección de un proveedor. Puede no aplicarse ningún filtro, de esta manera se muestra el listado completo de rutas de cada uno de los proveedores. Luego, se encuentran las opciones:

- **Confirmar**: sirve para aplicar el filtro de búsqueda y coloca los resultados en el recuadro derecho de la pantalla, como se observa en la siguiente imagen. La primer columna muestra el nombre del proveedor, la segunda la ruta de salida, la tercera indica la prioridad de la misma y la última columna brinda la posibilidad de eliminar la ruta ya creada.
- **Exportar**: permite generar un archivo que contenga las rutas creadas y filtradas. El mismo se crea con la extensión «.csv».

Figura 3.62: Interfaz avanzada: Ejemplo de consulta de rutas de los proveedores

La opción «Agregar Rutas desde Archivo» posibilita agregar rutas de manera sencilla, mediante la carga de un archivo; para ello se debe realizar clic en «Seleccionar archivo». Se precisa que este archivo se encuentre en formato «.csv» y que tenga el orden de la siguiente tabla (este es el ejemplo que se puede descargar pulsando en el ícono al lado de «Sample file:»).

# this line is a comment			
#"Trunk"	IP	Prefix	Priority
GTT PBX	192.168.1.253	54	1
Proveedor A	123.234.123.123	6785432	44
Proveedor A	123.234.123.123	767543	6
Proveedor A	123.234.123.123	8976543	4
Placa TDM	localhost	54	25

Figura 3.63: Interfaz avanzada: Ejemplo de archivo importable con rutas de proveedores

- **Trunk**: en esta columna se coloca el nombre del proveedor.
- **IP**: refiere al número IP al que se quiere alcanzar.

- **Prefix**: se debe colocar en la tercer columna los dígitos que componen al prefijo.
- **Priority**: es necesario establecer el orden de prioridad de las rutas, para ello se utiliza la cuarta columna.

Se recomienda editar los campos de las plantillas y luego corroborar que el formato no haya sufrido modificaciones. Finalmente, se debe hacer clic en el botón «Confirmar».

3.3.5. Preatendedor

El Preatendedor se encarga de atender una llamada, y reproducir un audio que, normalmente, explica al interlocutor que pasos debe seguir para llegar al destino deseado. Es por esto que los audios se denominan IVR (*Interactive Voice Response* o Respuesta de Voz Interactiva). Permiten en cierta manera, interactuar con el usuario. También es posible crear preatendedores con *hung up*, los cuales solo reproducen un audio y luego se corta.

Además, en el menú de Preatendedor, se pueden crear colas para encolar llamadas y que estas estén en espera hasta que los Agentes asociados a ella se liberen y puedan recibirlas. Las colas no reemplazan los IVR sino que se complementan para lograr la funcionalidad de ACD (*Automatic Call Distributor*) para Call Centers.

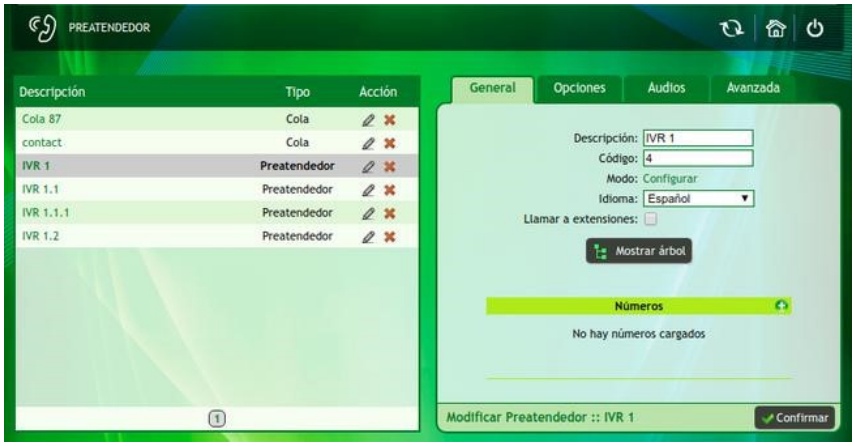

Figura 3.64: Interfaz avanzada: Preatendedores

3.3.5.1. Ver Preatendedor-Colas

Desde esta pestaña se pueden observar los preatendedores creados. Si se hace clic en el ícono ✎ bajo la columna Acción, se puede ver en el recuadro de la derecha todas las configuraciones de este preatendedor. Ahí se despliegan cuatro pestañas, donde se pueden realizar las configuraciones detalladas a continuación.

3.3.5.1.1. Pestaña General de Ver Preatendedor-Colas Desde la pestaña General se pueden modificar los siguientes campos.

- **Descripción**: el nombre o descripción del preatendedor
- **Idioma**: se selecciona el idioma deseado
- **Llamar a extensiones**: permite mientras se escucha el audio del preatendedor llamar a la extensión deseada
- **Código**: número que representa el preatendedor dentro de la base de datos
- **Modo**: es necesario realizar clic en «Configurar» la cual mostrará una ventana en donde se podrá elegir el modo u horario de operación del preatendedor (para mayor información se puede consultar Modos en la página 76). Para salir de esta ventana se deberá pulsar sobre el botón «✔ Confirmar»

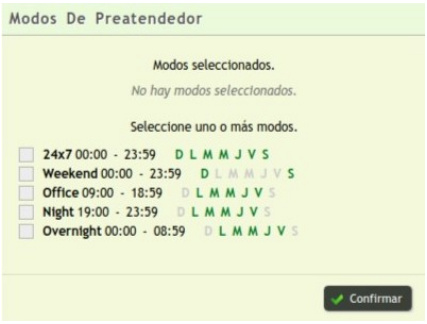

Figura 3.65: Interfaz avanzada: Modos de preatendedor

- **Mostrar árbol**: Presionando sobre el icono se puede observar en forma de diagrama de árbol, todos los preatendedores en cascada a partir del seleccionado. A continuación un ejemplo:

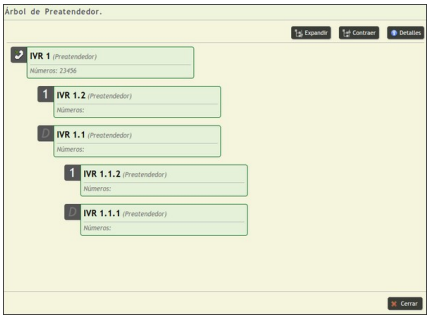

Figura 3.66: Interfaz avanzada: Árbol de preatendedores

La llamadas ingresan al IVR 1 con el número de accesos 23456, el cual presenta dos opciones. Presionando el 1 se ingresa al IVR 1.2 y la opción por defecto es el IVR 1.1. Esta última permite presionar el dígito 1 para ingresar al IVR 1.1.2 o la opción por defecto 1.1.1.

- **Números**:
  - Para agregar números de acceso (para más información sobre los números de acceso se recomienda ver Configuración de proveedor en la página 58) haciendo clic en el ícono ✚. Esto mostrará una ventana emergente en donde es posible seleccionar el número de acceso a asociar, luego de ello, bastará con presionar sobre el botón «✔ Confirmar»; en caso de no desear guardar el cambio, se recomienda pulsar sobre «[Cerrar]»

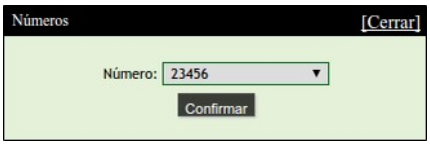

Figura 3.67: Interfaz avanzada: Asignar número de acceso al preatendedor

  - Para eliminar números de acceso solamente será necesario pulsar sobre el ícono ━ ubicado al lado del elemento a borrar

- ✔ **Confirmar**: guarda los cambios que se hayan realizado

3.3.5.1.2. Pestaña Opciones de Ver Preatendedor-Colas La segunda pestaña de configuración es Opciones, desde aquí se realiza la asociación entre el preatendedor y una acción en particular.

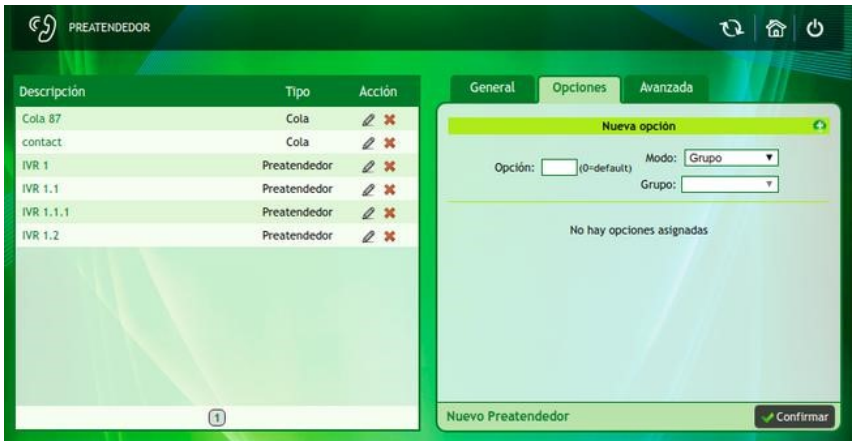

Figura 3.68: Interfaz avanzada: Opciones del pretendedor

Es necesario completar los campos en el recuadro Nueva opción de la siguiente manera:

- **Opción**: número a marcar para ejecutar la acción. Por defecto la opción es cero
- **Modo**: debe ser elegido ente las cuatro posibilidades listadas a continuación:
  - **Grupo**: permite desviar la llamada a un grupo, que se encargará de atender en la forma en que esta configurado el mismo (desde el menú Grupos).
  - **Preatendedor**: se desvían la llamada del preatendedor, a otro preatendedor. Con esto se puede realizar una configuración en cascada (árbol de Preatededores). En esta sección se puede agregar las Colas como opción del Preatendedor.
  - **Aplicación**: si se selecciona esta opción, se ejecuta la aplicación que seleccionada.
  - **Extensión**: permite marcar a la extensión declarada como opción del Preatendedor.

Configuración de las opciones del preatendedor

Es necesario crear una opción por defecto, a esta opción se le asigna el número 0.
Para poder crear las opciones, se deben completar los casilleros, elegir a quien se le asigna y luego, hacer clic sobre el ícono ✚. A medida que se siga este procedimiento para crear las opciones, se forma una lista como la que se observa en la siguiente figura:

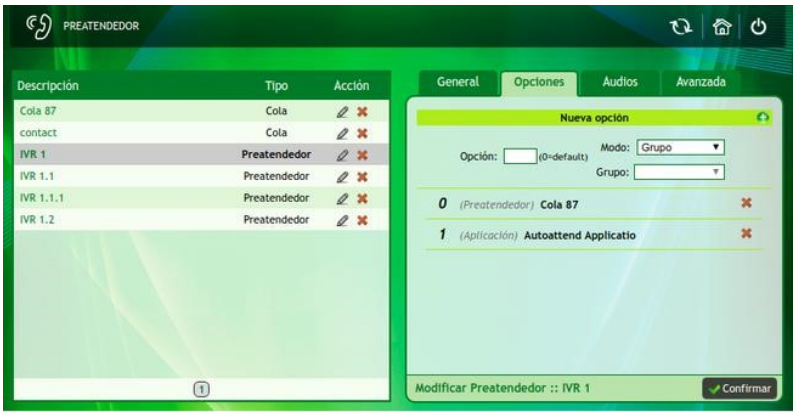

Figura 3.69: Interfaz avanzada: Ejemplo de las opciones del pretendedor

.
Para guardar los cambios se debe hacer clic sobre el icono «✔ Confirmar».

3.3.5.1.3. Pestaña Audios de Ver Preatendedor-Colas

3.3.5.1.3.1. Audios Preatendedor Desde la pestaña Audios se puede seleccionar el audio que se reproducirá en el IVR. Para lograrlo, se debe elegir el preatendedor deseado.

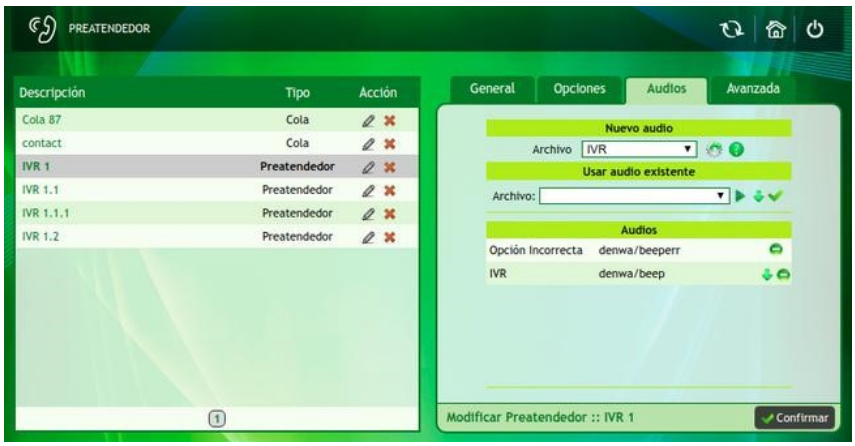

Figura 3.70: Interfaz avanzada: Audios del pretendedor

Luego, en la ventana ubicada a la derecha: «Nuevo audio», en caso de que el archivo de audio se encuentre en el computador, se selecciona el archivo de audio desde el icono ⚙.

También es posible grabar el mensaje de preatendedor mediante un equipo registrado en la red. Para ello se debe marcar *73 y después del tono es posible realizar la grabación. Una vez que se agregan los audios haciendo clic sobre el ícono ✔.

Los audios que hayan sido asignados al preatendedor (ya sea por carga desde el ordenador o por grabación y selección en la lista desplegable) estos se muestran en forma de lista en la parte inferior, bajo el encabezado «Audios»; desde donde es posible descargarlos (🡻) o eliminarlos (━).

Los archivos deben cumplir con las siguientes parámetros para ser compatibles:

- **Tipo de archivo**: WAV
- **Bit Rate**: 128 kbps
- **Audio Sample Size**: 16 bits
- **Canales**: 1 (mono)
- **Audio Sample Rate**: 8 KHz
- **Audio Format**: PCM

Se debe presionar «✔ Confirmar» para guardar los cambios.

3.3.5.1.3.2. Audios Cola Desde la pestaña Audios se puede seleccionar el audio que se reproducirá en el IVR.

Figura 3.71: Interfaz avanzada: Audio de la cola

- **Archivo MOH**: música en espera que se desea configurar
- **Archivo anuncio agente**: anuncio enviado al agente antes de recibir la llamada (normalmente indica el nombre de la opción del preatendedor)
- **Archivo anuncio periódico**: anuncio que se dará cada cierto período de tiempo
- **Nuevo audio de preatendedor**: audio brindado antes de comenzar con la musica en espera
- **Usar audio existente**: archivo proveniente de la grabación generada desde un terminal telefónico

Para seleccionar el archivo de audio tanto para música de espera, anuncio de agente, anuncio periódico y de preatendedor de la cola, en caso de que el archivo de audio se encuentre en el computador, se busca el archivo de audio desde el icono ⚙. En cambio, para eliminar los archivos de música de espera y anuncios de agente se debe presionar ✖.

También es posible grabar el mensaje de la cola mediante un equipo registrado en la red. Para ello se debe marcar *73 y después del tono es posible realizar la grabación. Una vez que se agregan los audios haciendo clic sobre el ícono ✔.

Los audios que hayan sido asignados la cola (ya sea por carga desde el ordenador o por grabación y selección en la lista desplegable) estos se muestran en forma de lista en la parte inferior, bajo el encabezado «Audios»; desde donde es posible descargarlos (🡻) o eliminarlos (━).

Los archivos deben cumplir con las siguientes parámetros para ser compatibles:

- **Tipo de archivo**: WAV
- **Bit Rate**: 128 kbps
- **Audio Sample Size**: 16 bits
- **Canales**: 1 (mono)
- **Audio Sample Rate**: 8 KHz
- **Audio Format**: PCM

Se debe presionar «✔ Confirmar» para guardar los cambios.

3.3.5.1.4. Pestaña Avanzada de Ver Preatendedor

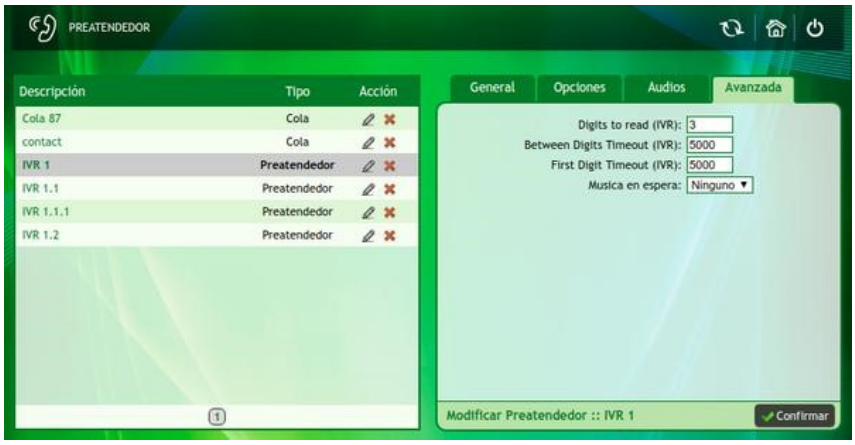

Figura 3.72: Interfaz avanzada: Configuración avanzada del pretendedor

3.3.5.1.4.1. Preatendedor

- **Digits to read (IVR)**: se determinan la cantidad de dígitos que se permiten marcar para realizar la llamada.
- **Between Digits Timeout (IVR)**: se establece el tiempo entre dígitos máximo de espera.
- **First Digit Timeout (IVR)**: tiempo máximo de espera para discar el primer número de la extensión.
- **Música en Espera**: Cuando esta configurado, en la llamada que ingresa a un usuario desde el preatendedor y se deja en espera se reproduce esta música en espera (MOH). Para ello se debe cargar previamente un archivo de audio en la Sección de Configuración >Anuncios >Música en espera (ver Música en Espera en la página 125).

3.3.5.2. Nuevo Preatendedor

Para crear un nuevo preatendedor se deben seguir los siguientes pasos.

- **General**:
  - **Descripción**: el nombre o descripción del preatendedor
  - **Idioma**: se selecciona el idioma deseado
  - **Llamar a extensiones**: permite mientras se escucha el audio del preatendedor llamar a la extensión deseada
  - **Código**: número que representa el preatendedor dentro de la base de datos
  - **Modo**: es necesario realizar clic en «Configurar» la cual mostrará una ventana en donde se podrá elegir el modo u horario de operación del preatendedor (para mayor información se puede consultar Modos en la página 76). Para salir de esta ventana se deberá pulsar sobre el botón «✔ Confirmar»
  - **Llamar a extensiones**: permite mientras se escucha el audio del preatendedor llamar a la extensión deseada.
  - ⁝☰ **Mostrar árbol**: Presionando sobre el icono se puede observar en forma de diagrama de árbol, todos los preatendedores en cascada a partir del seleccionado. Sin embargo, al momento de dar de alta un nuevo preatendedor, se mostrará una ventana emergente que indicará «Debe escoger un preatendedor de la lista»
  - **Números**:
    - Para agregar números de acceso (para más información sobre los números de acceso se recomienda ver Configuración de proveedor en la página 58) haciendo clic en el ícono ✚. Esto mostrará una ventana emergente en donde es posible seleccionar el número de acceso a asociar, luego de ello, bastará con presionar sobre el botón «✔ Confirmar»; en caso de no desear guardar el cambio, se recomienda pulsar sobre «[Cerrar]»

    - Para eliminar números de acceso solamente será necesario pulsar sobre el ícono ━ ubicado al lado del elemento a borrar
  - ✔ **Confirmar**: guarda los cambios que se hayan realizado

- **Opciones**:
  - **Opción**: número a marcar para ejecutar la acción. Por defecto la opción es cero
  - **Modo**: debe ser elegido ente las cuatro posibilidades listadas a continuación:
    - **Grupo**: permite desviar la llamada a un grupo, que se encargará de atender en la forma en que esta configurado el mismo (desde el menú Grupos).
    - **Preatendedor**: se desvían la llamada del preatendedor, a otro preatendedor. Con esto se puede realizar una configuración en cascada (árbol de Preatededores). En esta sección se puede agregar las Colas como opción del Preatendedor.
    - **Aplicación**: si se selecciona esta opción, se ejecuta la aplicación que seleccionada.
    - **Extensión**: permite marcar a la extensión declarada como opción del Preatendedor.

Configuración de las opciones del preatendedor

Es necesario crear una opción por defecto, a esta opción se le asigna el número 0.
Para poder crear las opciones, se deben completar los casilleros, elegir a quien se le asigna y luego, hacer clic sobre el ícono ✚. A medida que se siga este procedimiento para crear las opciones, se forma una lista como la que se observa en la siguiente figura.

- **Avanzada**
  - **Digits to read (IVR)**: se determinan la cantidad de dígitos que se permiten marcar para realizar la llamada.
  - **Between Digits Timeout (IVR)**: se establece el tiempo entre dígitos máximo de espera.
  - **First Digit Timeout (IVR)**: tiempo máximo de espera para discar el primer número de la extensión.
  - **Música en Espera**: Cuando esta configurado, en la llamada que ingresa a un usuario desde el preatendedor y se deja en espera se reproduce esta música en espera (MOH). Para ello se debe cargar previamente un archivo de audio en la Sección de Configuración >Anuncios >Música en espera (ver Música en Espera en la página 125).

Para finalizar se ejecuta un clic sobre el botón «✔ Confirmar».

3.3.5.3. Nueva Cola

Cola es la denominación que se le da a una lista de elementos esperando ser atendidos, hasta que el distribuidor automático de llamadas (ACD), distribuya las llamadas según las reglas definidas a los respectivos agentes (operadores).

Una nueva cola puede crearse desde el menú del preatendedor, el concepto de creación, audio de preatención y números de acceso son iguales a las de un IVR común.

- **General**:
  - **Descripción**: el nombre de la nueva Cola.
  - **Modo**: es necesario realizar clic en «Configurar» la cual mostrará una ventana en donde se podrá elegir el modo u horario de operación del preatendedor (para mayor información se puede consultar Modos en la página 76). Para salir de esta ventana se deberá pulsar sobre el botón «✔ Confirmar»

- **Idioma**: Seleccionar el idioma para esta cola.
- **Grupo**: el nombre del grupo de extensiones al cual se le asigna la tarea de atender las llamadas encoladas.
- **Estrategia**:
  - **Menos reciente**: suena la extensión que más tiempo estuvo ociosa.
  - **Menos llamadas**: se le otorga a la extensión que menos llamadas atendió.
  - **Aleatorio**: sonará cualquier extensión, de forma aleatoria.
  - **Round Robin**: cíclicamente sonarán una vez cada uno.
  - **Lineal**: seguirá un orden lineal. Se establece un orden de atención en los usuarios. Al ingresar una llamada siempre lo hará al agente número uno, en caso de que el mismo se encuentre ocupado o no se encuentre seguirá con el agente dos.
  - **Simultáneo**: suenan todas las extensiones del grupo al entrar una llamada. La estrategia de timbrado simultáneo no es compatible con la utilización del software Denwa Barra CTI. Al seleccionar esta estrategia en una cola, se despliega el siguiente mensaje de confirmación:

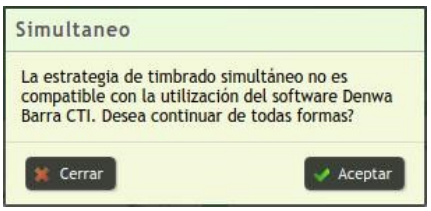

Figura 3.73: Interfaz avanzada: Mensaje de alerta ante la estrategia sumultánea

- **Tiempo de Ring**: el tiempo que durará sonando el interno.
- **Tiempo de espera del Agente**: Es el tiempo que le dará la cola al Agente antes de despachar otra llamada.
- **Extensión por defecto**: Si ningún agente toma la llamada esta se re direccionará a una extensión que puede ser la del supervisor o la extensión asignada a este motivo.
- **Requiere login**: Si la opción está en SI, los agentes requieren hacer login para estar listos para recibir llamadas. De lo contrario no se requiere y siempre pueden recibir llamadas.
- **Números**:
  - Para agregar números de acceso (para más información sobre los números de acceso se recomienda ver Configuración de proveedor en la página 58) haciendo clic en el ícono ✚. Esto mostrará una ventana emergente en donde es posible seleccionar el número de acceso a asociar, luego de ello, bastará con presionar sobre el botón «✔ Confirmar»; en caso de no desear guardar el cambio, se recomienda pulsar sobre «[Cerrar]»
  - Para eliminar números de acceso solamente será necesario pulsar sobre el ícono ━ ubicado al lado del elemento a borrar

- **Avanzada**:
  - **Tiempo de espera máximo**: es el tiempo máximo que esperará el interlocutor antes de que se corte la comunicación. Esperar sin usuarios en cola: permite especificar si la llamada se corta directamente o no, en caso de que no hayan agentes esperando para atender.
  - **Atención automática**: Esta opción permite que si un agente esta logueado en la cola y disponible, la llamada se le deriva atendiendose automáticamente.
  - **Prioridad entre colas**: Configuración de prioridad entre las colas (1 es el valor de mayor prioridad).

- **Anuncio periódico**: Habilitar el anuncio periódico. Este anuncio se carga en la sección de Audios de cola
- **Frecuencia Anuncio Periódico**: Configurar la frecuencia en que se reproduce el anuncio periódico.
- **Posición en la cola**: Configurar la opción de brindar al usuario final la posición en la que se encuentra en la cola.
- **Tiempo promedio de espera**: Habilitar el anuncio de tiempo promedio de espera en la cola.
- **Frecuencia**: Frecuencia, en segundos, en la que el tiempo promedio de espera es reproducido.

- ✔ **Confirmar**: guarda los cambios que se hayan realizado

3.3.5.4. Feriados

En esta sección se explica la función de la central para el desvío de los números de acceso de los preatendedores en fechas especiales. En estas fechas los usuarios no estarán disponibles en las áreas correspondientes.

Requerimiento

Para el uso de la función se debe haber creado los preatendedores con sus respectivos números de acceso y las opciones de cada uno. Además se deben haber creado uno o varios preatendedores con destinos especiales para usarse los días Feriados y asuetos parciales.

La vista principal permite observar el listado de los feriados que han sido configurados, bajo la columna de Acción se encuentran los íconos ✖ que permite eliminar el feriado y ✎ que permite modificar los parámetros del feriado, mostrando una ventana emergente que permitirá cambiar los mismos campos utilizados en el formulario de registro de un nuevo feriado.

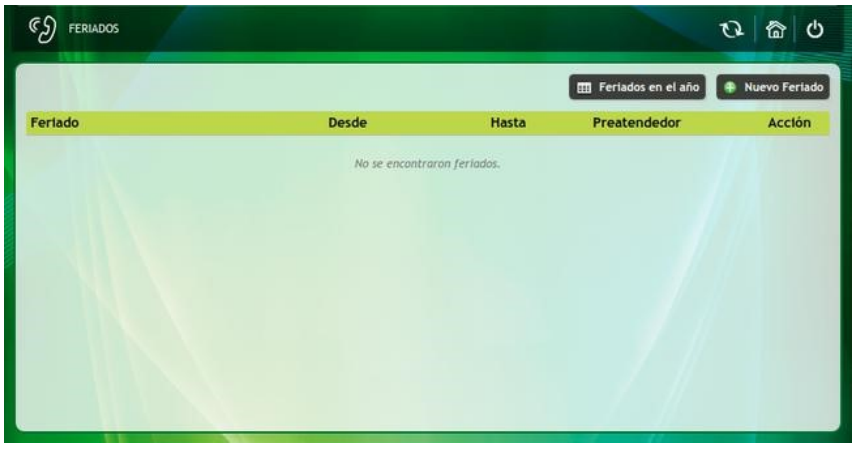

Figura 3.74: Interfaz avanzada: Feriados

3.3.5.4.1. Alta de feriados El alta de feriados puede realizarse desde cualquiera de los dos botones que se encuentran en la pantalla, a saber «⊕ Nuevo Feriado» y «📅 Feriados en el año», solamente que al pulsar sobre el último se mostrará (previo al formulario) un calendario, donde se deberá hacer un doble clic sobre la fecha.

Figura 3.75: Interfaz avanzada: Configuración de feriados

Los datos a completar son:

- **Descripción**: nombre del feriado
- **Desde**: fecha y hora del comienzo de la configuración de este feriado. En caso de haber seleccionado la fecha desde el calendario, este campo se encontrará preconfigurado.
- **Hasta**: fecha y hora del finalización de la configuración de este feriado. En caso de haber seleccionado la fecha desde el calendario, este campo se encontrará preconfigurado.
- **Peatendedor**: nombre del preatendedor donde se desvían los números de acceso, en general este es un preatendedor creado con un audio especial para el tipo de feriado o asueto.
- **Números**: números de acceso que se desvían hacia el preatendedor.

Una vez finalizado este período establecido para el, se vuelve automáticamente la configuración de los números de acceso a sus respectivos preatendedores.

3.3.5.5. Modos

La sección de «Modos» permite realizar configuraciones semanales que luego se asignaran a los preatendedores y colas. Su pantalla principal se encuentra dividida en dos secciones: la izquierda en donde se listan todos los modos ya creados, y la derecha, en donde es posible crear nuevos modos.

Los modos existentes pueden ser borrados (✖) o editados (🖉) pulsando sobre el ícono correspondiente en la columna de «Acciones».

3.3.5.5.1. Creación de Modos Para crear un modo es necesario completar el formulario que se encuentra a la derecha de la pantalla, con la siguiente información:

- **Descripción**: nombre descriptivo del modo. Este campo se verá reflejado en el listado que se mostrará al definir el «Modo» al momento de dar de alta una nueva cola o un nuevo preatendedor (ver Nuevo Preatendedor y Nueva Cola en las páginas 72 y 73, respectivamente) por lo que es necesario que el la descripción sea lo más clara y concisa posible.
- **Desde hora**:horario de inicio del modo
- **Hasta hora**: horario de finalización del modo

- **Día de la semana**: día de la semana en la que se aplicará

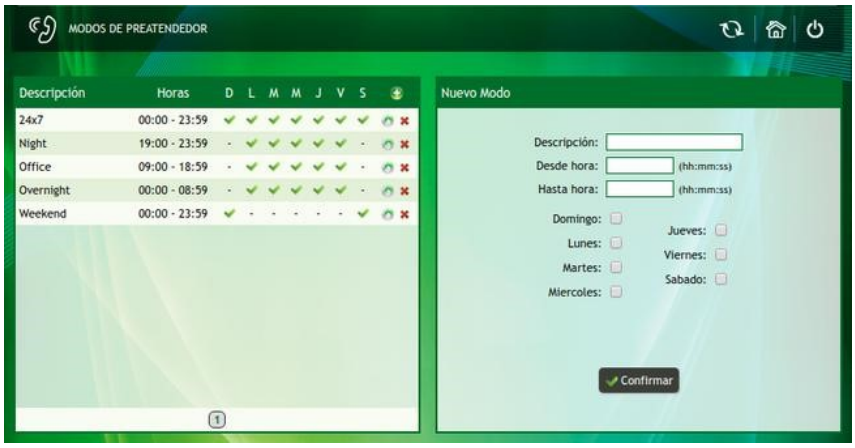

Figura 3.76: Interfaz avanzada: Modos

Día y hora

Para la correcta operación de los Modos es necesario que el equipo cuente con sus parámetros de fecha y hora actuales, esto requiere la adecuada configuración del servidor NTP (ver Servidor NTP en la página 120) y conexión a internet, a menos de que se encuentre localmente.

El proceso finalizará al presionar el botón «✔ Confirmar».

Asociación

En caso de que un modo se encuentre asociado a una cola o un preatendedor, no podrá ser borrado.

3.3.6. Reportes

En esta sección se pueden encontrar todos los registros de llamadas, grabaciones, números de acceso, recursos del sistema y preatendedores.

3.3.6.1. Llamadas

3.3.6.1.1. Todas las llamadas En este reporte es posible visualizar todas las llamadas, ya sean entrantes, salientes o internas; de forma predeterminada muestra los registros del día en curso.

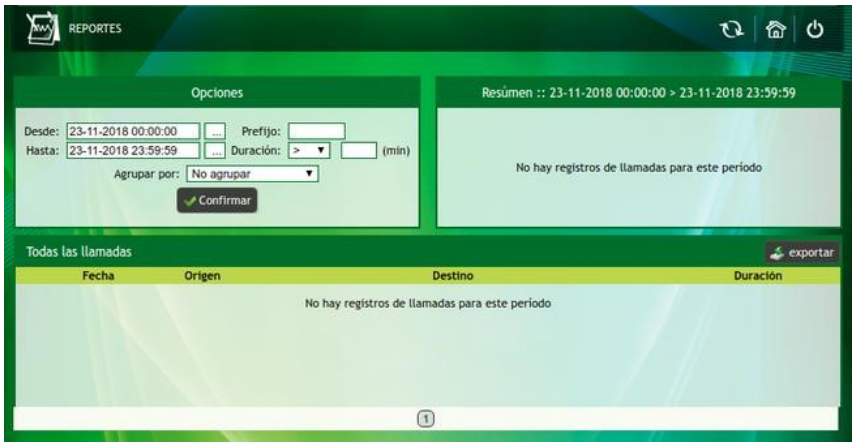

Figura 3.77: Interfaz avanzada: Reporte de todas las llamadas

La pantalla se encuentra dividida en tres recuadros:

- **Opciones**: estas opciones son filtros que permiten realizar una búsqueda más rápida y sencilla para quien deba interpretarla.
  - **Desde**: este campo posibilita realizar la búsqueda entre un período acotado de tiempo (día, mes, año y hora). Para ello, se debe realizar clic en «...» y se observa la ventana de la siguiente imagen; con las alternativas del calendario y la hora.
  - **Hasta**: este campo posibilita realizar la búsqueda entre un período acotado de tiempo (día, mes, año y hora). Para ello, se debe realizar clic en «...» y se observa la ventana de la siguiente imagen; con las alternativas del calendario y la hora.
  - **Prefijo**: este campo es opcional y habilita el filtrado mediante el uso del prefijo. Sólo se deben colocar los dígitos correspondientes en este campo.
  - **Duración**: estos campos son opcionales
    - **>**: Indica que se listará aquellas llamadas que superen el tiempo señalado
    - **<**: Indica que se listará aquellas llamadas que no superen el tiempo señalado
    - **Tiempo**: tiempo a considerar para el filtrado, debe expresarse en minutos
  - **Agrupar por**: este campo es opcional, permite diversas acciones según la selección del menú desplegable. Las opciones son:
    - No agrupar
    - Usuario
    - Grupo

    Si se ejecuta alguna agrupación el detalle del registro se observa en menor cantidad de líneas.
  - ✔ **Confirmar**: este botón dispara la búsqueda de los registros de llamadas correspondientes, aplicando los filtros antes seleccionados.
- **Resumen**: la información mostrada en este cuadro hace referencia a los filtros aplicados. Entre ellos se encuentran:
  - **Total de llamadas**: muestra la cantidad de llamadas; incluyendo de este modo a las que han tenido éxito y aquellas que no.
  - **Llamadas completadas**: esta cantidad refiere al número de llamadas que han sido respondidas.
  - **Llamadas no completadas**: es la diferencia entre el total de las llamadas y las llamadas completadas.
  - **ASR**: muestra el valor porcentual de este ratio, que se calcula tendiendo en cuenta las llamadas atendidas con respecto al total del volumen de llamadas (ver Pestaña Alarmas de ASR de Nuevo Proveedor)

- **Duración total**: refiere a la suma de la duración de cada una de las llamadas.
- **Duración media**: este ítem exhibe la duración promedio de las llamadas.

- **Todas las llamadas**: este cuadro presenta la información ordenada en columnas.
  - **Fecha**: esta columna expone la fecha y hora en la cual se ha realizado la llamada.
  - **Origen**: muestra el número que inicia la llamada.
  - **Destino**: exhibe el número que recibe la llamada.
  - **Duración**: refiere a la duración de la llamada en cuestión.

  En el borde de este cuadro se encuentra el botón «exportar», el cual permite descargar todo el listado en formato .csv.

Fecha	Origen	Destino	Duración	Trunk	Centros de Costos
2018-11-13 10:28:50	101	102	10	102	
2018-11-13 10:28:58	101	102	5	102	
2018-11-13 10:29:18	102	101	53	101	
2018-11-13 10:35:49	101	102	12	102	
2018-11-13 10:37:49	101	102	18	102	
2018-11-13 10:40:27	101	102	11	102	
2018-11-13 10:54:32	102	101	45	101	
2018-11-13 10:55:24	102	101	60	101	

Figura 3.78: Interfaz avanzada: Ejemplo del reporte exportable de todas las llamadas

Duración de los registros de llamadas

De forma predeterminada, los registros de llamadas se guardan hasta tres (3) meses de historial; sin embargo esto puede modificarse en el apartado de las configuraciones de mantenimiento (ver Mantenimiento en la página 133).

3.3.6.1.2. Llamadas entrantes Este reporte cuenta con los mismos recursos que el anterior (ver Todas las llamadas en la página 77), solamente que ya cuenta con el filtro para las llamadas entrantes.

3.3.6.1.3. Llamadas salientes Al igual que con el reporte de llamadas entrantes, cuenta con los mismos recursos que el anterior (ver Todas las llamadas en la página 77), solamente que ya cuenta con el filtro para las llamadas salientes.

3.3.6.1.4. Llamadas internas Del mismo modo que con los dos (2) reportes anteriores, además de contar con las mismas alternativas que en «Todas las llamadas» (ver Todas las llamadas en la página 77), se realiza el filtrado para llamadas internas; es decir dentro de la misma Denwa UC&C 4.0.1 .

3.3.6.1.5. Extendido Este reporte cuenta con los mismos recursos que el reporte de «Todas las llamadas» (ver Todas las llamadas en la página 77); sin embargo posee un agregado de opciones que brindan un detalle más profundo. La ventana Extendido se visualiza en la siguiente figura.

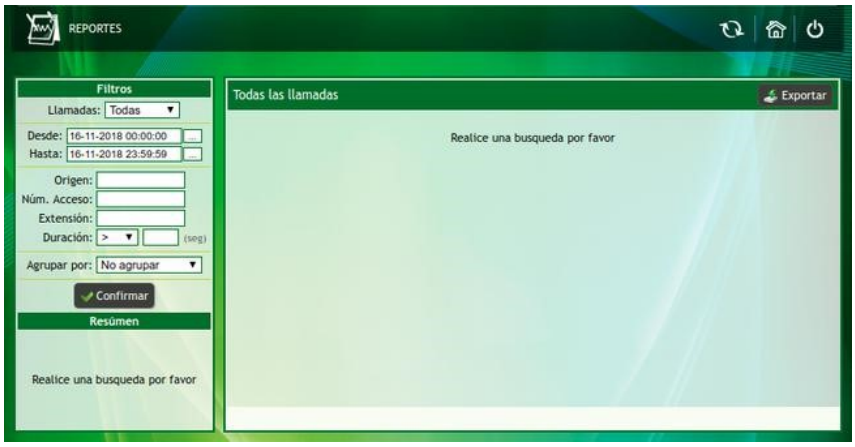

Figura 3.79: Interfaz avanzada: Reporte extendido de todas las llamadas

- **Opciones**: estas opciones son filtros que permiten realizar una búsqueda más rápida y sencilla para quien deba interpretarla.
  - **Desde**: este campo posibilita realizar la búsqueda entre un período acotado de tiempo (día, mes, año y hora). Para ello, se debe realizar clic en «...» y se observa la ventana de la siguiente imagen; con las alternativas del calendario y la hora.
  - **Hasta**: este campo posibilita realizar la búsqueda entre un período acotado de tiempo (día, mes, año y hora). Para ello, se debe realizar clic en «...» y se observa la ventana de la siguiente imagen; con las alternativas del calendario y la hora.
  - **Prefijo**: este campo es opcional y habilita el filtrado mediante el uso del prefijo. Sólo se deben colocar los dígitos correspondientes en este campo.
  - **Duración**: estos campos son opcionales
    - **>**: Indica que se listará aquellas llamadas que superen el tiempo señalado
    - **<**: Indica que se listará aquellas llamadas que no superen el tiempo señalado
    - **Tiempo**: tiempo a considerar para el filtrado, debe expresarse en minutos
  - **Agrupar por**: este campo es opcional, permite diversas acciones según la selección del menú desplegable. Las opciones son:
    - No agrupar
    - Usuario
    - Grupo

    Si se ejecuta alguna agrupación el detalle del registro se observa en menor cantidad de líneas.
  - ✔ **Confirmar**: este botón dispara la búsqueda de los registros de llamadas correspondientes, aplicando los filtros antes seleccionados.
- **Resumen**: la información mostrada en este cuadro hace referencia a los filtros aplicados. Entre ellos se encuentran:
  - **Total de llamadas**: muestra la cantidad de llamadas; incluyendo de este modo a las que han tenido éxito y aquellas que no.
  - **Llamadas completadas**: esta cantidad refiere al número de llamadas que han sido respondidas.
  - **Llamadas no completadas**: es la diferencia entre el total de las llamadas y las llamadas completadas.
  - **ASR**: muestra el valor porcentual de este ratio, que se calcula tendiendo en cuenta las llamadas atendidas con respecto al total del volumen de llamadas (ver Pestaña Alarmas de ASR de Nuevo Proveedor)
  - **Duración total**: refiere a la suma de la duración de cada una de las llamadas.

- **Duración media**: este ítem exhibe la duración promedio de las llamadas.

- **Todas las llamadas**: este cuadro presenta la información ordenada en columnas.

  - **Fecha**: esta columna expone la fecha y hora en la cual se ha realizado la llamada.
  - **Origen**: muestra el número que inicia la llamada.
  - **Destino**: exhibe el número que recibe la llamada.
  - **Duración**: refiere a la duración de la llamada en cuestión.
  - **Causa**: Indica la causa por la cual el llamado fue finalizado.
  - 🔍: Haciendo clic sobre el icono, se muestra una ventana emergente con el detalle de todos los eventos de la llamada, a saber:

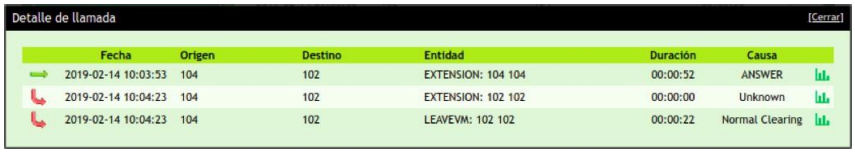

Figura 3.80: Interfaz avanzada: Reporte extendido, detalle de la llamada

  - **Flechas**: Se cuenta con flechas para la representación de los distintos eventos:
    - →: entrante
    - ←: saliente
    - ↳: desglose de la llamada
  - **Fecha**: es la marca temporal del evento, es posible que entre la primera y segunda fila existan unos pocos segundos de diferencia; esto se debe a que cuando el origen, A, realiza una llamada a B, se demora un pequeño lapso temporal en la central que cursará la llamada.
  - **Origen**: quién origina el llamado
  - **Destino**: a quién se dirige el llamado
  - **Entidad**: se indica el tipo de entidad de quien origina o a quién se deriva el llamado; por ejemplo puede ser una extensión, un preatendedor o un troncal
  - **Duración**: duración de la llamada en cada etapa, está en formato de «hh:mm:ss»
  - **Causa**: causa de desconexión o finalización del llamado
  - 📊: permite conocer las estadísticas de M.O.S. (*Mean Opinion Score*)para evaluar la calidad de la llamada:

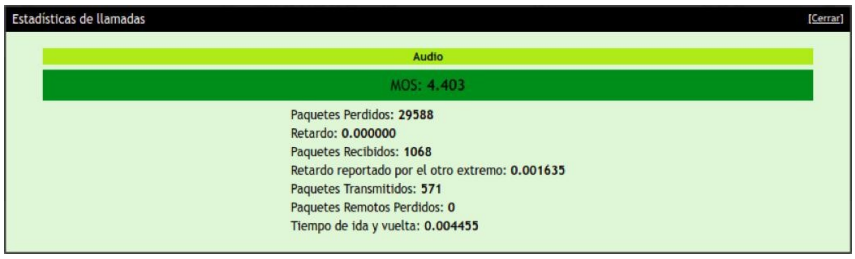

Figura 3.81: Interfaz avanzada: Reporte extendido, estadísticas de la llamada

M.O.S. (*Mean Opinion Score*)

El M.O.S. en VoIP sirve para conocer la calidad del audio de las llamadas. El cálculo se realiza a través de algoritmos/fórmulas y su resultado se distribuye sobre una escala de 1 a 5, siendo:

- 5 Excelente
- 4 Bueno
- 3 Aceptable
- 2 Pobre
- 1 Malo

En el borde de este cuadro se encuentra el botón «exportar», el cual permite descargar todo el listado en formato .csv, dicho archivo contiene la siguiente información:

- **CallId**: esta numeración permite identificar la llamada en los distintos tipos de registros.
- **ConnectTime**: esta columna refiere a la fecha y hora, es decir al tiempo de conexión.
- **LegType**: aquí se indica como ve la llamada la central. Por ejemplo: cuando se llama de un teléfono a otro ocurren dos sucesos, el primero es que la central ve la llamada de origen como entrante (In); luego cursa dicha llamada al destino y la observa como saliente (Out). PeerType: en este campo se constata que tipo entidades son las que participan en la llamada.
- **Peer**: este campo se corresponde con el anterior, ya que muestra el nombre que ha sido designado, por ejemplo, a la extensión o troncal participante.
- **ANI**: (*Automatic Number Identification*) permite identificar el número de quien realiza la llamada.
- **Destination**: se brinda el dato de quien esta ejecutando la llamada.
- **Disconnect/Description**: expone si la llamada se ha respondido, cancelado o quien de los participantes ha finalizado la misma.
- **Duration**: en este campo se verifica la duración, en segundos, de la llamada.
- **Channel/Protocol**: indica el canal que utiliza o protocolo para cursar la llamada, esto depende de si se tienen o no placas de telefonía.
- **ChannelDescription**: en la primer parte de la llamada, es decir desde el origen hasta la central, este campo muestra el IP origen. En cambio, desde la central hasta el destino muestra: el interno si la llamada es entre extensiones, el IP de proveedor si la llamada es externa y el canal si utiliza TDM.
- **PBXPrefix**: se utiliza en el caso de existir centrales virtuales.
- **CallService**: esta columna exhibe el tipo de llamada, entre ellas se encuentran las nacionales, locales, internas, internacionales, especiales, móviles, entre otros.

Duración de los registros extendidos de llamadas

De forma predeterminada, los registros extendidos de llamadas se guardan hasta un (1) mes de historial; sin embargo esto puede modificarse en el apartado de las configuraciones de mantenimiento (ver Mantenimiento en la página 133).

3.3.6.1.6. Reportes programados falta info

3.3.6.1.6.1. Nuevo Reporte Desde aquí se permite generar un Nuevo Reporte programado, para lo cual es necesario completar los siguientes campos:

- **Descripción**: se debe colocar la descripción o nombre del reporte programado.
- **Tipo de llamada**: se selecciona sobre que llamadas se desea el reporte, se debe escoger una de las opciones del menú desplegable: entrantes, salientes o internas. La opción por default es "Salientes".
- **Agrupar por**: en el reporte se pueden realizar agrupación por PBX, usuario, grupo, regla o sin agrupar. La opción por defecto es "No agrupar".
- **Correr cada**: se programa cada cuanto tiempo se genera este reporte, las opciones del menú desplegable son Hora(s), Día(s) y Mes(es). Además de la opción por defecto que es "No agendar", o sea que el reporte no se crea.
- **Incluir los últimos**: incluye el último tiempo sobre el cual se realiza el reporte. Las opciones del menú desplegable son Hora(s), Día(s) y Mes(es).
- **Enviar por e-mail a**: se ingresa la casilla de correo electrónico donde se desea recibir el reporte y se pulsa el botón . Se puede agregar más de una dirección de correo electrónico.
- **Filtros**: También existe la posibilidad de agregar filtros; al realizar clic en el ícono **+** se accede a la siguiente ventana. Donde se permite acomodar las variables siguientes de acuerdo a nuestras necesidades.
  - **Filtrar por**: se puede filtrar por PBX, grupo, duración, origen, destino, redirigida hacia y regla.
  - **Operador**: este campo varía según sea la selección de la opción anterior. El operador también esta asociado con el valor a ingresar del próximo campo. Según el caso el operador puede ser: es (=), empieza con, mayor, menor o igual.
  - **Valor**: de acuerdo a la selección que se haya escogido en Filtrar por será el valor a ingresar. El mismo puede ser una PBX, un grupo, una regla o un valor numérico que que complete la regla en cuestión. Al presionar «**Confirmar**» se genera la regla de filtrado. Se puede observar una lista con las reglas de filtrado asociadas al reporte. Para eliminar una regla se debe presionar el botón **−**.

  Finalmente, con el objetivo de crear el reporte programado se debe realizar clic en el botón Confirmar.

Nota

Se puede agregar varias reglas de filtrado. Para observar las configuraciones de cada reporte programado, se debe hacer clic en la descripción o nombre deseado (sección Reportes) y en el sector derecho de la pantalla se presentan las configuraciones del mismo.

3.3.6.1.6.2. Reportes Aquí se muestra el listado de reportes existentes. Se brindan las opciones para realizar cambios en los mismos, pulsando Modificar o bien haciendo clic sobre el nombre o descripción del reporte. Se permite eliminar los mismos uno a uno (Borrar). Para generar un nuevo reporte programado sólo se debe pulsar el botón Agregar, lo cual habilita el sector derecho de la pantalla con los campos a completar para la respectiva creación.

3.3.6.2. Grabaciones

Esta función permite visualizar, escuchar y descargar las grabaciones de todas las llamadas que estén siendo grabadas, ya sea por usuario (ver Nuevo Usuario, página 32), troncal (Nuevo Proveedor, página 60) o grupo (Nuevo Grupo, página 55).

En la imagen anterior se visualizan dos grandes recuadros, a continuación se explica cada uno de ellos.

- **Filtros**: estas opciones permiten realizar una búsqueda más rápida y sencilla para quien deba interpretarla.
  - **Desde**: este campo posibilita realizar la búsqueda entre un período acotado de tiempo (día, mes, año y hora). Para ello, se debe realizar clic en «...» y se observa la ventana de la siguiente imagen; con las alternativas del calendario y la hora.
  - **Hasta**: este campo posibilita realizar la búsqueda entre un período acotado de tiempo (día, mes, año y hora). Para ello, se debe realizar clic en «...» y se observa la ventana de la siguiente imagen; con las alternativas del calendario y la hora.
  - **Proveedor**: (opcional) este campo ofrece la posibilidad de filtrar las llamadas de los proveedores, en caso que los mismos existan.
  - **Preatendedor**: (opcional) este campo ofrece la posibilidad de filtrar las llamadas que han sido tomadas por alguno de los preatendedores, en caso que los mismos existan.
  - **Duración**: estos campos son opcionales
    - **>**: Indica que se listará aquellas llamadas que superen el tiempo señalado
    - **<**: Indica que se listará aquellas llamadas que no superen el tiempo señalado
    - **Tiempo**: tiempo a considerar para el filtrado, debe expresarse en minutos
  - **Buscar**: al realizar clic aquí se ejecuta la búsqueda contemplando los filtros seleccionados. Los resultados se observan en el recuadro Grabaciones.
  - **Exportar**: cuando se efectúa clic en esta opción se exportan los archivos de las grabaciones; se genera un zip que contiene los audios en formato wav.
  - **Borrar**: al ejecutar clic en este botón se aplican los filtros de búsqueda y se eliminan los resultados obtenidos.
- **Grabaciones**: este campo se presenta el resultado de la búsqueda, ordenada en las siguientes columnas.
  - **Fecha**: esta columna expone la fecha y hora en la cual se ha realizado la llamada.
  - **Origen**: muestra el número que inicia la llamada.
  - **Destino**: exhibe el número que recibe la llamada.
  - **Tamaño**: en esta columna se da a conocer el tamaño de la grabación propiamente dicha.
  - **Acción**: otorga la posibilidad de:
    - ▶: reproducir el audio de la grabación
    - ⃠: eliminar la grabación

3.3.6.3. Números de acceso

En esta sección, se pueden obtener el detalle de los números de acceso (ver Configuración de proveedor en la página 58), y a qué o a quién fue asignado.

Figura 3.82: Interfaz avanzada: Reporte de números de acceso

3.3.6.4. Recursos del sistema

En estas opciones de pueden observar los reportes en tiempo real de las diversas características de la Denwa UC&C 4.0.1 , a saber:

- **Fecha del servidor**: muestra fecha y hora actual.
- **Tiempo de actividad**: indica el lapso temporal que la central esta funcionando.
- **Uso del disco**: esta sección se exhibe un gráfico de torta que muestra de manera rápida y simple de comprender el uso del disco. Además, se presenta un listado con mayor detalle:
  - **Buzón de voz**: permite verificar que espacio ocupan en el disco los mensajes de voz.
  - **Grabaciones**: refiere al espacio que ocupan las grabaciones telefónicas.
  - **Sistema**: es el espacio que ocupa el software de la PBX. También, se contempla el backup.
  - **Espacio libre**: permite comprobar el espacio que aun no ha sido utilizado del disco.
  - **Total**: contempla la capacidad total del disco.
- **Actividad de los últimos 33 minutos**:
  - **Uso de CPU (%)**: muestra tanto el uso de los recursos del CPU expresado en porcentaje, como promedio del mismo.
  - **Uso de Memoria (%)**: al utilizarse por completo la memoria RAM que tiene incorporada la PBX, se emplea el espacio predeterminado en disco. Luego, es necesario pasar los datos del disco a la memoria, este intercambio se denomina swap. Los gráficos contenidos en estos ejes muestran el uso de la memoria y el estado de swap.
  - **Llamadas Activas**: este gráfico expone la cantidad de llamadas que se están cursando. Si se visualiza el tiempo en el eje inferior, se verifica la duración de cada una de ellas.

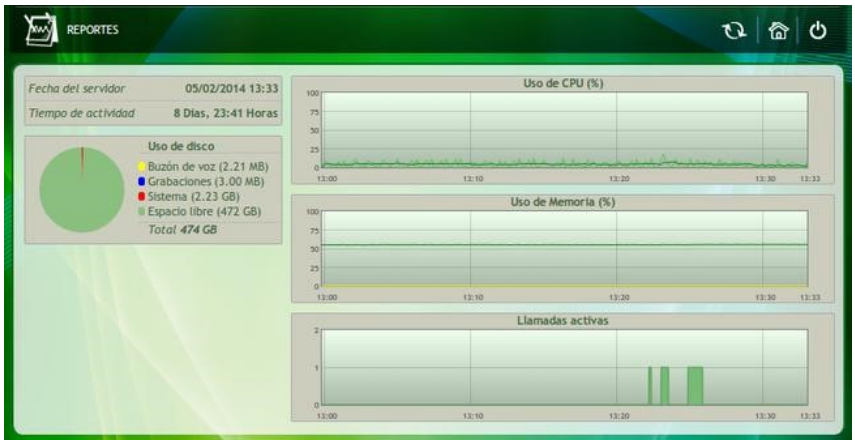

Figura 3.83: Interfaz avanzada: Reporte de recursos del sistema

3.3.6.5. Preatendedores

Inicialmente, en esta sección se debe seleccionar tanto el lapso temporal sobre el cual se desea observar el reporte, como así también preatendedor. Luego, se debe hacer clic en «⊕ Confirmar».

Figura 3.84: Interfaz avanzada: Reporte de preatendedores

Con esto se visualizan dos gráficos. El primero, muestra las opciones que marcó la persona que realizo la llamada al ser atendido por el preatendedor. Además, permite observar cuantas llamadas tuvo cada una de las opciones. En cambio, el segundo gráfico se muestra las extensiones que recibieron llamadas, con la correspondiente cantidad.

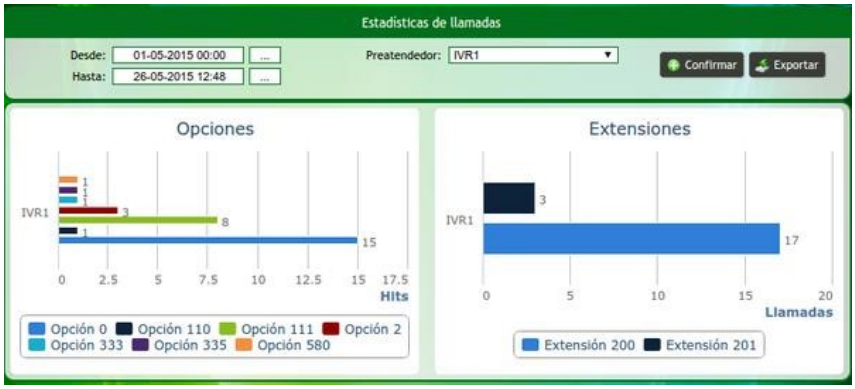

Figura 3.85: Interfaz avanzada: Ejemplo de reporte de preatendedores

Posterior a la obtención del gráfico, se brinda la opción de exportar un documento en .pdf («Exportar PDF») con la misma información de cada uno de los gráficos y una tabla que muestra de manera rápida y sencilla cada uno de los valores; o bien a formato .csv («Exportar CSV») con los siguientes campos:

- **Fecha**: fecha de ingreso de la llamada en formato dd/mm/aaaa
- **Hora**: hora de ingreso de la llamada en formato hh:mm:ss
- **ANI**: número telefónico del llamante
- **Número de acceso**: número de acceso del troncal por donde ingresó
- **Entidad de acceso**: sitio por el cual ingresó el llamado
- **Tiempo de atención**: tiempo al habla con un interno, agente o buzón de voz en formato hh:mm:ss (columna rosa en el diagrama)
- **Tiempo en preatendedores**: tiempo total que se encontró en colas y preatendedores en formato
- **Duración total**: tiempo trasncurrido desde que ingresó el llamado hasta el corte del mismo

- **Tiempo en última opción**: tiempo que aguardó luego de presionar la última opción del preatendedor elegido antes de ser atendido por un buzón de voz, interno o agente en formato hh:mm:ss (columna amarilla en el diagrama)

- **Estado**: estado final del llamado

- **IVR**: nombre del preatendedor reproducido (IVR “A” en el diagrama)

- **Destinos**: se mostrará una columna por cada uno de las posibles ramificaciones del IVR en donde el usuario presionó una opción:

    - **Opción 1**: Primera opción marcada en el preatendedor (1er Opción marcada en el diagrama)
    - **Opción 2**: Segunda opción marcada en el preatendedor (2a Opción marcada en el diagrama)
    - **Opción 3**: Tercera opción marcada en el preatendedor (3ra Opción marcada en el diagrama)
    - **Opción ...**
    - **Opción n-1**
    - **Opción n**

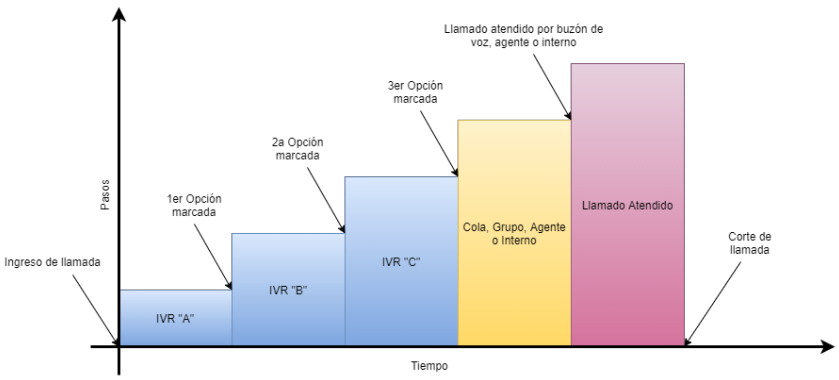

Figura 3.86: Diagrama de los pasos de la llamada

3.3.7. Configuración

3.3.7.1. General

Esta funcionalidad permite configurar las opciones generales de la central.

3.3.7.1.1. Pestaña Básica En la pestaña Básica, se deben ingresar los datos que se observan en la figura siguiente.

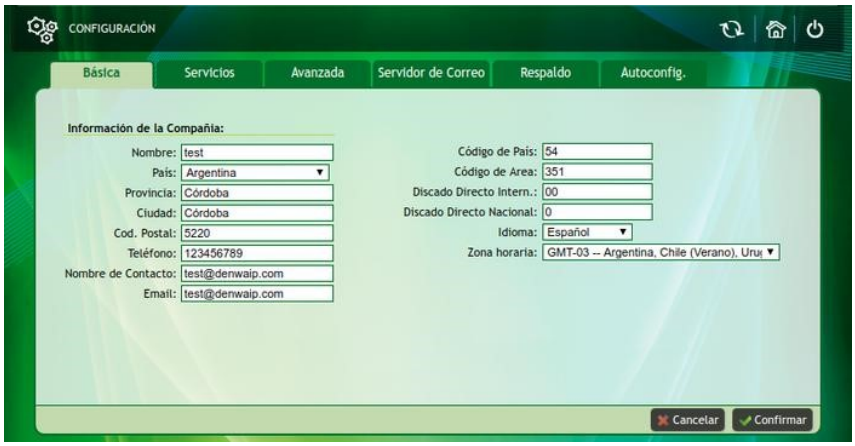

Figura 3.87: Interfaz avanzada: Configuración básica del sistema

- **Nombre**: nombre de la compañía.
- **País**: donde se instala Denwa UC&C 4.0.1
- **Provincia**: provincia, región o estado en donde se encuentra el equipo
- **Ciudad**: ciudad donde está el equipo
- **Código Postal**: código postal de la dirección
- **Teléfono**: número telefónico de contacto
- **Nombre de Contacto**: nombre de la persona de contacto
- **Email**: correo electrónico de contacto
- **Código de país**: código de país utilizado para la marcación internacional (ver `https://es.wikipedia.org/wiki/Anexo:Prefijos_telef%C3%B3nicos_mundiales` para más información)
- **Código de área**: código de área utilizado para la marcación de larga distancia nacional
- **Discado directo internacional**: código utilizado para la salida internacional (habitualmente «00»)
- **Discado directo nacional**: código utilizado para el discado nacional
- **Idioma**:
- **Zona horaria**:

Luego de cargar todos los datos, se debe hacer clic sobre «✔ Confirmar», en caso de no desear guardar los cambios, bastará con pulsar sobre el botón «✖ Cancelar».

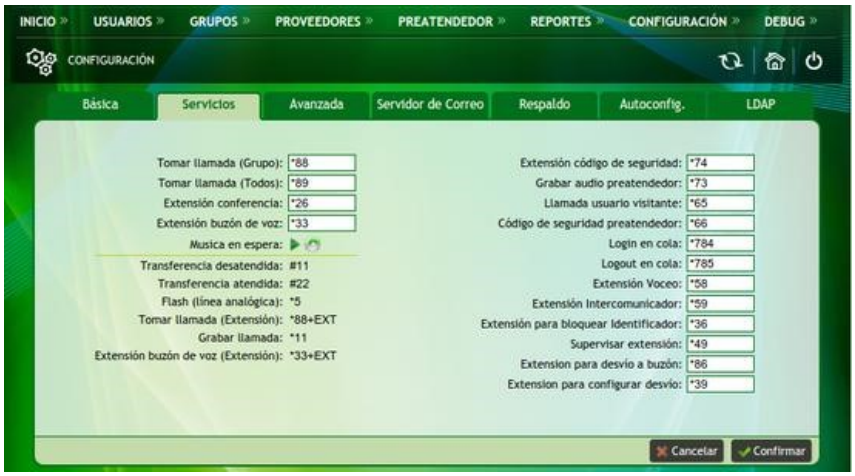

Figura 3.88: Interfaz avanzada: Configuración de servicios del sistema

3.3.7.1.2. Pestaña Servicios En esta pestaña es posible configurar los servicios de la Denwa UC&C 4.0.1 , pueden ser utilizados desde los terminales telefónicos, mediante una combinación de teclas:

- **Tomar llamada (Grupo)**: toma la llamada entrante al grupo donde se encuentra ubicado.
- **Tomar llamada (Todos)**: toma la llamada entrante a todas las extensiones, función utilizada en instalaciones pequeñas.
- **Extensión conferencia**: conferencias OnLine y OnDemand, esta función permite crear una conferencia entre personas por demanda. El usuario que desea crear una sala debe marca *26. Los usuarios que pretenden ingresar en dicha conferencia deben discar *26 + extensión del usuario creador de la sala. Esto también lo debe realizar el usuario creador de la sala.
- **Extensión buzón de voz**: Toma mensajes desde el buzón de voz, donde se requiere el número de extensión y contraseña.
- **Música en espera**: haciendo clic en el icono ⚙ se puede agregar un archivo de audio, como música de espera de la Denwa UC, por otro lado puede ser descargada o reproducida pulsando en el ícono ▶.
- **Extensión Código de Seguridad**: permite cambiar el estado del código de seguridad, activa o desactiva.
- **Grabar audio preatendedor**: permite grabar audios para ser utilizado en los IVRs o preatendedores.
- **Llamada de usuario visitante**: permite realizar llamadas como usuario visitante desde cualquier extensión siempre discando PIN + NÚMERO DE DESTINO.
- **Código de seguridad preatendedor**: permite realizar llamadas a un usuario visitante desde cualquier extensión siempre discando CÓDIGO DE SEGURIDAD + NÚMERO DE DESTINO.
- **Login en cola**: permite hacer login sobre la cola discando el PREFIJO + NUMERO DE LA COLA.
- **Logout en cola**: permite hacer logout de la cola discando el PREFIJO + NUMERO DE LA COLA.
- **Extensión Voceo**: permite realizar funciones de voceo llamando a una extensión tipo grupo. El audio es de una sola vía y se disca PREFIJO + NÚMERO DE EXTENSIÓN.

- **Extensión Intercomunicador**: permite realizar funciones de intercomunicador llamando a una extensión. El audio es de dos vías y se disca PREFIJO + NÚMERO DE EXTENSIÓN.
- **Extensión para bloquear Identificador**: bloquea el ANI.
- **Supervisar extensión**: permite intervenir una comunicación.
- **Extensión para desvío a buzón**: redirecciona las llamadas al buzón de voz.
- **Extensión para configurar desvío**: para que la aplicación funcione es necesario cargar los audios en Mis aplicaciones >Set Forward Application.

Además existen algunas combinaciones de teclas que son fijas y no es posible configurarlas:

- **Transferencia desatendida (#11)**: esta funcionalidad transfiere la llamada al momento de discar la combinación de teclas y corta la comunicación con el primer usuario.
- **Transferencia atendida (#22)**: esta funcionalidad primero permite al receptor de la llamada hablar con la persona a quien se quiere hacer la transferencia. Cuando el que transfiere corta la comunicación, esta se transfiere al usuario que llamó primero. Flash (línea analógica) (*5): permite al momento de tener la línea ocupada habilitar otra línea.
- **Tomar llamada (Extensión) (*88 + EXT)**: esta funcionalidad toma las llamadas de una extensión específica, con la combinación *88 + NÚMERO DE EXTENSIÓN.
- **Grabar llamada (*11)**: permite la grabación de la llamada.

Música de espera

Si la llamada ingresa desde el Preatendedor a un Grupo (no cola) y luego a un interno, al poner una llamada en espera se reproduce el MOH del usuario, si el usuario no tiene configurado se reproduce el MOH del Grupo. Si el usuario y el grupo no tienen configurado el MOH, se reproduce la música de espera del Preatendedor. Si en todos los casos (usuario, Grupo y Preatendedor) no se configura la música en espera, al dejar una llamada en espera se reproduce la MOH de la Denwa UC&C 4.0.1 .

Figura 3.89: Interfaz avanzada: Configuración avanzada del sistema

3.3.7.1.3. Pestaña Avanzada Esta pestaña permite configurar las opciones avanzadas de Denwa UC&C 4.0.1 . Los campos a configurar son los siguientes:

- **Ring de Extensiones**: es el tiempo en segundos que una extensión sonará, luego de este tiempo la llamada se corta, se envía al correo de voz o se transfiere, esto depende de los servicios configurados.

- **Ring de Grupos**: es el tiempo en segundos que un grupo sonará antes de pasar al siguiente grupo.

- **Ring saliente**: es el tiempo en segundos que una llamada saliente sonará, luego de este tiempo, si la llamada no es atendida Denwa UC&C 4.0.1 corta la llamada.

- **Duración máxima de llamada**: es el tiempo máximo permitido para una llamada saliente, luego de superado este tiempo la llamada se corta. Es necesario configurar este parámetro correctamente, debido a que alcanzado el tiempo especificado la llamada se finalizará. Mantener información de Grabación: Permite especificar el periodo máximo por el cual se mantendrá el historial de las grabaciones exportadas para ser incluida en los reportes.

- **Descripción del servidor**: es el nombre elegido para la DenwaUC. Este aparecerá en el sector superior derecho de la pantalla, sobre el modelo de la Denwa.

- **Reiniciar telefonía**: permite definir el periodo en el cual los servicios de telefonía se reiniciarán. Por defecto este parámetro se encuentra configurado todos los días.

- **Soporte ICE**: Opción disponible para centrales en donde se utilice la tecnología WebRTC (habilitado por defecto). En caso de no contar con conexión a Internet, se recomienda deshabilitar esta opción, ya que afecta directamente al tiempo de conexión de una llamada.

- **Nombre de Dominio**: nombre del dominio asignado a la Denwa UC, se utiliza en casos especiales donde la Denwa UC está en una red privada, utiliza IP Pública y DNS dinámico. Con esta configuración se envian todos los mensajes SIP en este dominio para ser contestados.

- **IP Pública**: IP Pública asignada a la PBX, es utilizada en casos especiales donde la PBX está en una red privada con IP Pública fija en un router.

- **Red Local**: es la red privada en la cual estará funcionando la central. Se deben agregar las redes presionando en ⚙. Esto habilitará una nueva ventana, la cual permite agregar las diferentes redes. El formato para agregar las mismas en red/mascara, ambos en formato de cuatro octetos decimales (por ejemplo: 192.168.1.0/255.255.255.0). Luego se debe presionar sobre +.

- **Servidor STUN**: este servidor ayuda a la IP-PBX cuando existen equipos detrás de una NAT, es poco utilizado en nuevas instalaciones VoIP.

- **Tipo de Payload para DTMF**: se puede escoger entre los tipos de carga 97 y 101.

- **Fuente del Directorio Externo**: indica desde donde se puede provisionar la lista de contactos. Puede ser local o externo. Si es externo se debe presionar el botón ⚙, e ingresar la URL donde se encuentra el archivo de aprovisionamiento. Por último «✔ Confirmar».

- **Servicio para CNAM**: es un servicio creado para Estados Unidos que verifica el nombre del contacto, para ello busca este nombre en una base de datos. Se recomienda deshabilitar este servicios en otro país.

En esta pantalla también es posible apagar o reiniciar el sistema, para ello se cuenta con los botones «⏻ Apagar servidor» y «⏻ Reiniciar servidor», respectivamente

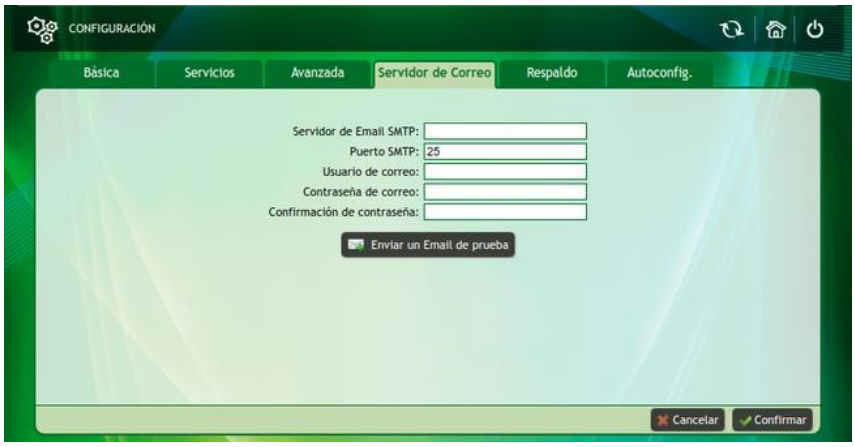

Figura 3.90: Interfaz avanzada: Configuración del servidor de correo del sistema

3.3.7.1.4. Pestaña Servidor de Correo Esta pestaña permite configurar un servidor de correo para Denwa UC&C 4.0.1 . Se solicita: servidor de correo electrónico, puerto, usuario y password.

- **Servidor de Email SMTP**: es un protocolo para la transferencia simple de correo electrónico. Aquí se debe escribir el IP o Dominio del Server SMTP para el envío de Correo de Voz, FAX y alertas de PBX Denwa.
- **Puerto SMTP**: puerto a utilizar para el servidor de email, este depende del proveedor del servidor. Los puertos más usados son 25, 465 y 587.
- **Usuario de correo**: nombre de usuario para la cuenta de email.
- **Contraseña de correo**: contraseña del usuario de email.
- **Confirmación de contraseña**

Pulsando sobre el botón «✉ Enviar un Email de prueba» se realizará una comprobación del servicio, esto mostrará una ventana emergente en donde se mostrará precargada la informacion del listado anterior, siendo necesario indicar una dirección de correo electrónico de destino y, si fuese necesario, modificar el mensaje de prueba. Los botones «✔ Enviar» y «✖ Cancelar», envían el mensaje de prueba o cierran la ventana, respectivamente.

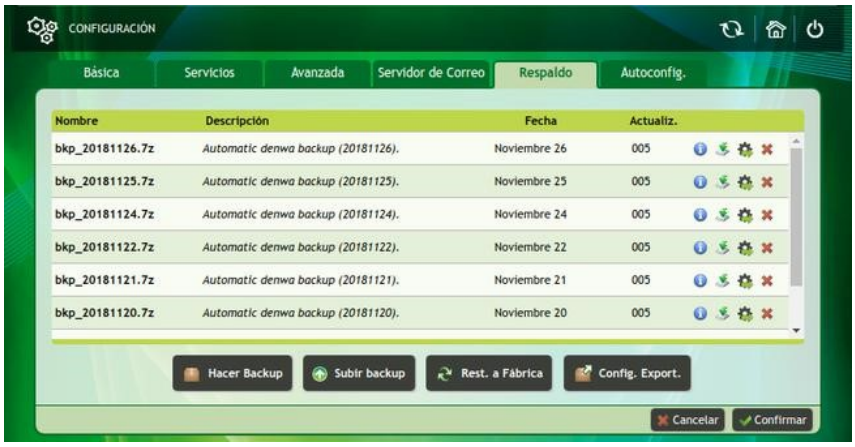

Figura 3.91: Interfaz avanzada: Configuración de respaldos del sistema

3.3.7.1.5. Pestaña Respaldo Esta pestaña se destinada a todas las operaciones de respaldo y restauración de datos de Denwa UC&C 4.0.1 . Lo primero que se observa es una tabla en donde se listan con todos los Backups realizados, donde se muestra:

- **Nombre**:
- **Descripción**:
- **Fecha**:
- **Actualización**:
- **Íconos de Acción**:
  - Muestra información del Backup.
  - Guarda el archivo de Backup en el ordenador.
  - Permite configurar Denwa UC&C 4.0.1 a partir de un archivo de configuración seleccionado, al pulsarlo se mostrará una advertencia indicando los riesgos asociados a la tarea.

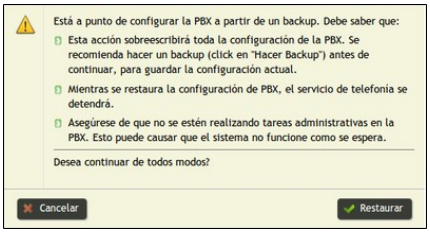

Figura 3.92: Interfaz avanzada: Advertencias para la restauración de los backups

  - ✖ Elimina el Backup.

En la parte inferior hay cuatro (4) botones que ofrecen distintas opciones de backup:

- **Hacer Backup**: permite crear una copia de seguridad. Es recomendable realizar la copia de seguridad cuando Denwa UC&C 4.0.1 este con poco actividad.
- **Subir Backup**: esta opción permite restaurar la configuración desde un archivo guardado en la PC .
- **Rest. a Fábrica**: se restaura la central a los valores de fábrica. Atención! Todos los datos serán perdidos, se recomienda realizar una copia de seguridad con anterioridad.
- **Config. Export.**: esta opción permite exportar la copia de seguridad a un servidor FTP. Se deben completar los datos del servidor FTP en la ventana que aparece a continuación.
  - **Habilitar la exportación de backups**: la exportación de backups unicamente operará si este campo cuenta con un tilde (✔) en su casillero
  - **Protocolo FTP**:
    - **Usuario**: nombre de usuario para iniciar sesión en el servidor FTP
    - **Contraseña**: contraseña del usuario utilizado para iniciar sesión en el servidor FTP
    - **IP / Dominio**: dirección IP o nombre del dominio del servidor FTP
    - **Path**: ruta (dentro del directorio del usuario FTP) en donde se almacenarán los archivos.

Rutas en Windows

Dado que en la mayoría de los sistemas basados en UNIX (como lo es Denwa UC&C 4.0.1) se emplea como caracter de escape, y el mismo es utilizado en los sistemas Windows para la definición de las rutas de los archivos y carpetas; en caso de que el servidor FTP a utilizar sea un equipo Windows, será necesario utilizar el «*backslash*» o «barra invertida» de forma doble, por ejemplo:

```
C:\\users\\pepito\\FTP\\
```

- **Nombre**: nombre distintivo del servidor FTP

- **Botones**:
  - **✖ Cerrar**: cierra la ventana emergente sin guardar los cambios realizados
  - **Verificar conexión**: ejecuta una prueba de conexión al servidor FTP, esta prueba consiste en la creación de un archivo en la ruta antes definida, indicando si la conexión fue exitosa o fallida
  - **Ayuda**: muestra una ventana de ayuda indicando cómo se puede completar cada campo
  - **✔ Configurar**: aplica y guarda la configuración aplicada

Alertas por errores de transferencia

Denwa UC&C 4.0.1 envía correos electrónicos de alerta ante pérdida de conexión con el servidor FTP, o errores de transferencia de los archivos. Esta funcionalidad solamente está disponible si se ha configurado el servidor de correo electrónico (ver sección Pestaña Servidor de Correo en la página 92).

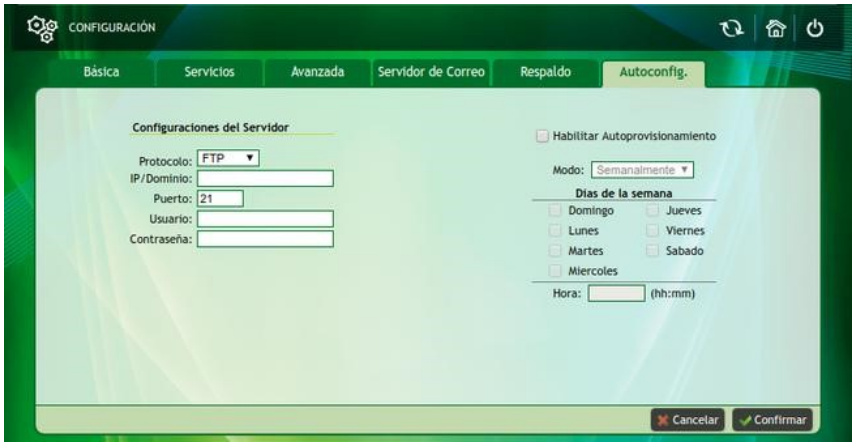

Figura 3.93: Interfaz avanzada: Autoconfiguración del sistema

3.3.7.1.6. Pestaña Autoconfig

Esta pestaña se brinda la posibilidad de obtener las configuraciones de la central desde un servidor FTP, HTTP o HTTPS (HTTP con seguridad).

3.3.7.1.6.1. Configuraciones del Servidor

Aquí se determina el servidor con el que se va a provisionar la central: FTP, HTTP y HTTPS, las opciones que se deben configurar son:

- **Protocolo**: se debe seleccionar entre FTP, HTTP, HTTPS.
- **IP/Dominio**: se configura la IP del servidor.
- **Puerto**: se establece el puerto que utiliza el servidor. Por defecto se usa el FTP (puerto 21), se puede elegir también HTTP (puerto 80) o HTTPS (puerto 443).

- **Usuario**: se determina el usuario del servidor (si se deja este casillero y el de contraseña en blanco se utilizará la metodología sin autenticación).
- **Contraseña**: contraseña del servidor.

Luego de configurar el servidor, se debe configurar la periodicidad con la que se desea realizar el autoaprovisionamiento, para esto se brindan dos opciones: Semanalmente o Repetidamente. Se accede a la configuración de ellas, haciendo clic en el checkbox «■ Habilitar Autoaprovisionamiento».

3.3.7.1.6.2. Modo Semanalmente Esta opción permite configurar que días de la semana y a que hora se realiza el autoaprovisionamiento de la central. Las opciones son muy intuitivas, solo basta con seleccionar los días de la semana y la hora deseada para que la central se autoaprovisione.

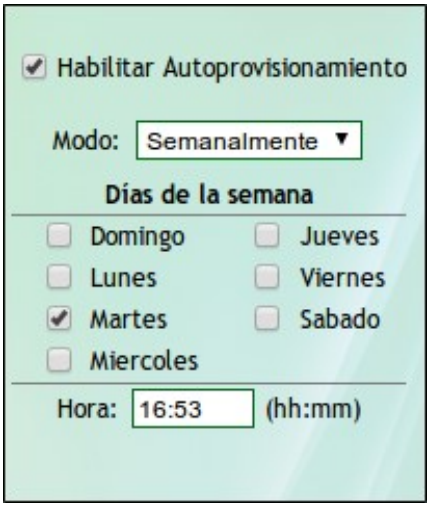

Figura 3.94: Interfaz avanzada: Modo de autoaprovisionamiento semanal

3.3.7.1.6.3. Modo Repetidamente Esta opción permite seleccionar cada cuanto tiempo la central se autoprovisiona.

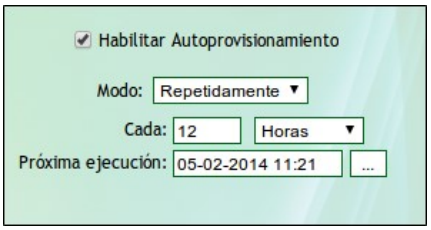

Figura 3.95: Interfaz avanzada: Modo de autoaprovisionamiento repetido

Simplemente se completa el campo cada, y luego se selecciona si este número representa horas, días o semanas. Debajo de estas opciones se debe configurar el día y la hora de la próxima ejecución, clic en se puede configurar el día y la hora para ejecutar el primer autoaprovisionamiento, luego éste se repite de acuerdo al período configurado en el paso anterior.

En todos los casos, luego de completar el modo de autoaprovisionamiento, se deben confirmar los cambios haciendo un clic en Confirmar.

3.3.7.1.7. Pestaña LDAP Esta sección permite la autenticación de operadores con sistema LDAP (Active Directory) permitiendo el acceso con todos los permisos habilitados.

Disponibilidad de pestaña

Esta pestaña únicamente está disponible en equipos que cuentan con el módulo LDAP Auth instalado; adicionalmente, en caso de contar con el módulo de Contact Center, se podrá mostrar una mayor cantidad de campos.

Figura 3.96: Interfaz avanzada: Modo de autoaprovisionamiento semanal

A continuación los parámetros de configuración del servidor:

- **Servidor**: dirección IP o dirección de dominio del Server LDAP. Por ejemplo: ldap.mynetwork.local.
- **Puerto**: refiere al puerto del servidor LDAP donde espera las conexiones IP. Por ejemplo: 389.
- **Usuario**: DN («Nombre Distintivo» por sus siglas en inglés) del usuario para el acceso a las búsquedas dentro de la estructura del Active Directory. Con este usuario se realizará la conexión inicial para la búsqueda del usuario a autenticar, es necesario que posea los permisos necesarios para leer todo el grupo al que pertenecen los usuarios, al cual se le realizarán las consultas. Por ejemplo: «cn=usuario1,ou=people,ou=division1,dc=miorg,dc=es ».
- **Contraseña**: clave utilizada para la autenticación de la conexión inicial. Por ejemplo: «MiClaveLdAp».
- **Buscar**: DN («Nombre Distintivo» por sus siglas en inglés) del grupo u organización a la que pertenecen los usuarios que se autenticarán, utilizando sus credenciales LDAP, como administradores de Denwa UC&C 4.0.1 .

3.3.7.2. Cloud

En esta sección, se puede hacer el Alta, Baja o Modificación (Monitor o Administrador) de los usuarios del Cloud (Integradores).

Para que usuarios del Cloud puedan monitorear o Administrar remotamente la central, se deben asociar las centrales en cloud.denwaip.com (ver documento Cloud para Integradores disponible en el sitio de soporte)

3.3.7.2.1. Configuración En esta sección se puede seleccionar la nube en la cual estará asociada la central:

Figura 3.97: Interfaz avanzada: Selección de la nube desde donde se administrará el equipo

Las centrales pueden ser monitoreadas desde la plataforma Cloud, o desde un sevidor personalizado dentro de la nube o red privada.

3.3.7.2.2. Usuarios En la sección de usuarios, se pueden ver, modificar el rol o eliminar los usuarios que tienen accesos de Administardor o de Monitor de la central

Figura 3.98: Interfaz avanzada: Configuración de usuarios de acceso Cloud

Al ingresar al usuario, se puede ver los datos con lo que el Integrador le ha dado de alta en su cuenta Cloud, y es posible modificar su rol: Monitor o Administrador

3.3.7.3. Administradores

Esta funcionalidad permite configurar a los administradores de Denwa UC&C 4.0.1 .

Figura 3.99: Interfaz avanzada: Administradores de Denwa UC&C 4.0.1

Se verifican dos tipos de usuarios:

- **Web**: usuarios con gestión del equipo vía web.
- **CLI**: usuario con gestión del equipo vía consola o ssh (pbxadmin)

3.3.7.3.1. Nuevo Administrador Si se desea crear un nuevo administrador, se deben hacer clic sobre «⊕ Nuevo Administrador», esto mostrará una ventana emergente en donde se solicita la siguiente información:

- **Nombre**: nombre del usuario
- **Apellido**: apellido del usuario
- **Usuario**: forma en la que se identificará al iniciar sesión en Denwa UC&C 4.0.1
- **Contraseña**: contraseña a utilizar para el inicio de sesión
- **Confirmación de contraseña**: repetición de la contraseña a utilizar
- **Email**: dirección de correo electrónico
- **Habilitado**: casilla para habilitar (✔) o deshabilitar (☐) al usuario
- **Permisos**: pueden ser de lectura y escritura, sólo lectura o ninguno. Deberá seleccionarse a cuales elementos del menú podrá ingresar, a saber:
  - Usuarios (ver página 29)
  - Grupos (ver página 52)
  - Proveedores (ver página 57)
  - Preatendedor (ver página 67)
  - Reportes (ver página 77)
  - Configuración (ver página 87)
  - Debug (ver página 144)

Figura 3.100: Interfaz avanzada: Alta de usuario web

Nuevos administradores

Sólamente es posible generar usuarios de administración web

3.3.7.3.2. Edición de Administrador En caso de desear cambiar algún parámetro de los administradores existentes se debe hacer clic sobre el nombre del administrador, con lo que se mostrará la ventana de edición, la cual cuenta con los mismos campos y características que los mencionados en Nuevo Administrador (ver página 98). Los cambios serán almacenados la pulsar sobre el botón «✔ Confirmar», o si se desea descartar la modificación y cerrar la ventana, se deberá pulsar sobre «✖ Cancelar».

3.3.7.3.2.1. Edición de usuario CLI : Los campos editables son los de contraseña y la posibilidad de deshabilitar el usuario en caso que no sea utilizado este medio de gestión.

Alerta de Seguridad

Es de suma importancia el cambio de contraseña de los usuarios «admin» y «pbxadmin». Para mayor información se recomienda consultar la sección Contraseña de usuarios, en la página 165.

3.3.7.4. Redes

En el apartado «Redes», es posible configurar la forma en la que Denwa UC&C 4.0.1 se relaciona con las redes existentes en su entorno.

3.3.7.4.1. Interfaces de Red

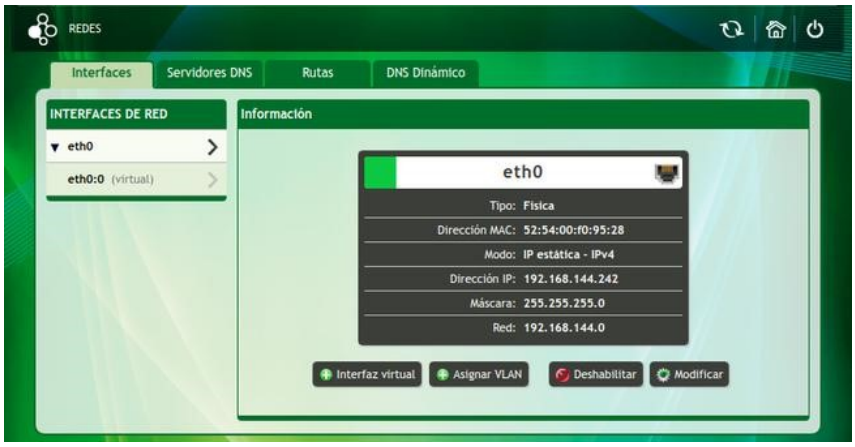

Figura 3.101: Interfaces de Red, pestaña de interfaces

3.3.7.4.1.1. Pestaña Interfaces En la pestaña de interfaces es posible dar de alta a Denwa UC&C 4.0.1 en las distintas redes del cliente, por medio de la asignación de direcciones IP en las distintas interfaces configurables, a saber:

- **Física**: asocia una dirección IP a la interfaz física de red
- **Virtual**: permite asignar varias direcciones IP (una por cada interfaz virtual) a una interfaz física de red
- **VLAN**: permite colocar la etiqueta de VLAN a la dirección IP, ésta se asignará a una interfaz virtual, permitiendo utilizar varias IP de distintas VLAN en una misma interfaz física

Excepción en Alta Disponibilidad

Cuando Denwa UC&C 4.0.1 forma parte de un cluster de Alta Disponibilidad (Activo-Pasivo), la configuración de las Interfaces de Red serán bloqueadas por el sistema, no permitiendo su edición.

La información se muestra en dos secciones principales:

- **Interfaces de red**: enlista todas las interfaces físicas de la plataforma. Al lado del nombre de cada una de las interfaces se encuentra el símbolo ▶ que, al pulsarlo desplegará el listado de las interfaces virtuales (en caso de contar con ellas)
- **Información**: muestra la información de la interfaz seleccionada (ícono › activo), a saber:
  - **Nombre y estado de enlace**: indica el nombre de la interfaz de red, así como el estado de su enlace:
    - **Verde**: enlace establecido
    - **Rojo**: sin conexión
  - **Tipo**: indica si la interfaz es física, o virtual
  - **Dirección MAC**: dirección MAC de la placa de red
  - **Modo**: muestra si la dirección IP fue configurada manualmente (estática) o por medio de un servidor DHCP, además muestra si su configuración es para redes IPv4 o IPv6
  - **Dirección IP**: dirección IP asignada a la placa
  - **Máscara**: máscara de subred
  - **Red**: dirección IP de la red a la que pertenece la IP asignada
  - ⊕ **Interfaz virtual**: permite la creación de una interfaz virtual en la placa seleccionada, al pulsar este botón muestra una ventana emergente para su configuración

- **Dirección IP**: dirección IP a configurar
- **Máscara**: máscara de subred, en caso de ser IPv4 debe indicarse en el formato decimal de cuatro (4) octetos, sin embargo en el caso de IPv6 su formato es el de CIDR
- **Tipo**: indica si se emplea IPv4 o IPv6
- ✖ **Cancelar**: cierra la ventana sin guardar los cambios
- ✔ **Crear**: guarda los cambios y cierra la ventana

◦ ⊕ **Asignar VLAN**: permite la creación de una interfaz virtual con una etiqueta de VLAN, al pulsar este botón muestra una ventana emergente para su configuración

- **Id de VLAN**: número de VLAN a utilizar
- **Dirección IP**: dirección IP a configurar
- **Máscara**: máscara de subred, en caso de ser IPv4 debe indicarse en el formato decimal de cuatro (4) octetos, sin embargo en el caso de IPv6 su formato es el de CIDR
- **Tipo**: indica si se emplea IPv4 o IPv6
- ✖ **Cancelar**: cierra la ventana sin guardar los cambios
- ✔ **Crear**: guarda los cambios y cierra la ventana

Las interfaces de red pueden ser configuradas siguiendo los pasos a continuación:

1. Se debe seleccionar la interfaz deseada, en el caso de la imagen es la eth0. Se puede observar que se muestran todos los datos de la misma.
2. Debajo de la información, se dispone de cuatro opciones para configurar.
   - Interfaz virtual: se asigna una interfaz virtual sobre la eth0. Para configurar este opción se debe ingresar la dirección IP y la máscara de red de la nueva interfaz virtual. Luego se debe presionar en Crear.
   - Asignar VLAN: se genera una VLAN (red de área local virtual). Con este método se crean redes lógicas independientes dentro de una misma red física. Para lograrlo se necesita ingresar el identificador de la VLAN, la dirección IP y la máscara de red.
   - Deshabilitar: se deshabilita la interfaz de red.
   - Modificar: se puede cambiar la dirección IP y máscara de red, eligiendo el modo IP Estático o DHCP y el tipo IPv4 o IPv6.

3.3.7.4.1.2. Pestaña Servidores DNS En la pestaña Servidores DNS, se puede configurar el servidor de nombres de dominio deseado. Para configurar el DNS se debe ingresar una IP o dominio de un servidor en el campo «>Nuevo Servidor DNS», y luego presionar el botón ⊕; con esto se incluirá en listado en la parte inferior. Para eliminar los servidores de la lista se debe hacer clic sobre ✖.

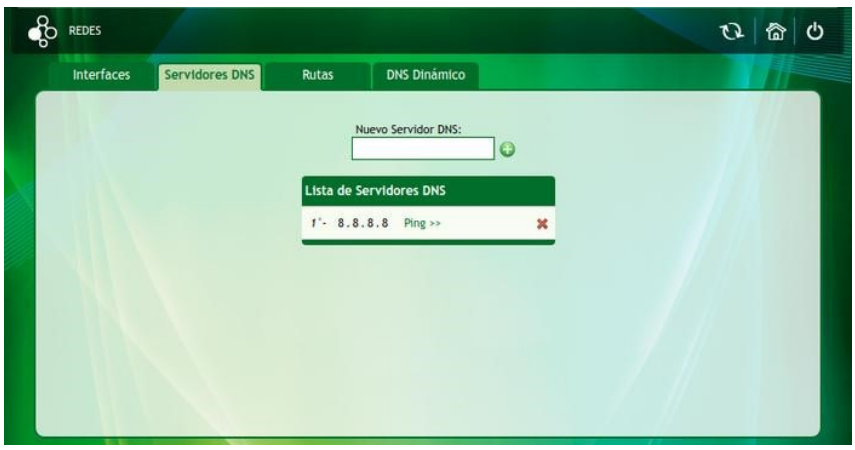

Figura 3.102: Interfaces de Red, pestaña de servidores DNS

Es posible comprobar la disponibilidad del servidor, haciendo clic sobre el texto «Ping» que se encuentra al lado de su dirección IP.

3.3.7.4.1.3. Pestaña Rutas Desde esta pestaña se puede configurar una ruta estática particular para la operación de Denwa UC&C 4.0.1 .

Figura 3.103: Interfaces de Red, pestaña de rutas

La puerta de enlace predeterminada puede ser configurada completando el campo correspondiente al lado de la leyenda «Puerta de Enlace» y pulsando el botón «✔ Aplicar».

En caso de requerir alcanzar destinos por medio de una puerta de enlace diferente a la predeterminada, se deberá pulsar en el botón «⊕ Nueva Ruta» y completar los campos que se mostrarán en el formulario desplegado, estos campos son:

- **Destino**: dirección IP del host o red de destino, se declara en dos campos:
  - **Dirección IP**: dirección IP del host o red de destino
  - **Máscara**: máscara de red declarada en formato de cuatro (4) octetos decimales
- **Interfaz**: permite seleccionar la interfaz por la cual se alcanzará la el host o la red antes declarada, de forma predeterminada se elige automáticamente; en caso de desear declarar una interfaz específica, es necesario remover el ✔de la casilla «Eleccción automática» y seleccionar la interfaz deseada.
- **Puerta de enlace**: dirección IP por la cual se alcanzará el host o la red antes declarada
- **Métrica**: prioridad de la ruta; menor número, mayor prioridad
- **✖ Cancelar**: limpia el formulario y cierra la ventana
- **❓ Ayuda**: muestra un diálogo emergente con texto de ayuda
- **✔ Crear**: guarda los cambios y cierra la ventana

Validación de ruta

La ruta solamente se agregará si el host o la red de destino puede ser alcanzada a través de la puerta de enlace declarada

Una vez agregada la ruta, se mostrará en la tabla que se encuentra en la parte inferior de la pantalla, desde donde se puede visualizar la siguiente información:

- **Destino**: dirección IP del host o red de destino
- **Máscara**: máscara de red declarada en formato de cuatro (4) octetos decimales
- **Puerta de enlace**: dirección IP por la cual se alcanza el host o la red

- **Métrica**: prioridad de la ruta; menor número, mayor prioridad
- **Interfaz**: interfaz por la que se alcanza el host o la red
- **IP Origen**: dirección IP con la que se envían los paquetes al host o red de destino por medio de la puerta de enlace declarada
- **Ícono de estado**: puede mostrarse en dos colores:
  - **Verde**: el host o la red de destino puede ser alcanzado
  - **Rojo**: el host o la red de destino no puede ser alcanzado
- **Acciones**: permite eliminar la ruta haciendo clic sobre el ícono «✖» correspondiente a su fila

Figura 3.104: Interfaces de Red, pestaña de DNS dinámico

3.3.7.4.1.4. Pestaña DNS dinámico No en todas las ocasiones es posible contar con una dirección IP Pública estática, para solventar estos inconvenientes es que existen los servidores de DNS dinámico, éstos monitorean de forma constante los posibles cambios en la dirección IP pública de Denwa UC&C 4.0.1 y actualizan sus registros de modo que siempre haya relación entre el Dominio y la dirección IP pública asignada (por servidor PPPoE, servidor DHCP, o incluso configuración estática). Puede configurarse con la siguiente información:

- **Dominio**: es el dominio registrado en el servidor de DynDNS elegido
- **User de Login**: usuario que se registra en el servidor
- **Contraseña de Login**: contraseña del usuario
- **Servidor**: dominio o dirección IP del servidor
- **Intervalo**: fracción de tiempo en el que la central envía una notificación al servidor de DynDNS para actualizar su dirección IP, debe escribirse en minutos
- **Ayuda**: muestra el diálogo de ayuda, con ejemplos
- ✔ **Confirmar**: guarda los cambios y enciende el cliente de DNS dinámico

Servidores de DNS dinámico

El servicio prestado por los servidores de DNS dinámico es de pago y no se incluye en los costos de licenciamiento y soporte de su licencia Denwa UC&C 4.0.1 . Sin embargo, el cliente (responsable de enviar la información a dichos servidores, se encuentra disponible en la plataforma).

Ante cualquier duda se puede presionar en Ayuda en donde se muestran ejemplos.

El servicio puede ser iniciado o detenido pulsando sobre el ícono ⏻. En caso de requerir el envío anticipado de la dirección IP Pública al servidor de DNS dinámico, puede pulsar sobre el ícono 🔄.

3.3.7.4.2. Clientes VPN Desde esta pestaña se puede configurar una nueva conexión VPN (Virtual Private Network) mediante el protocolo PPTP (Point-To-Point Tunneling Protocol) o el protocolo OpenVPN y editar las conexiones existentes (en caso de disponer de alguna).

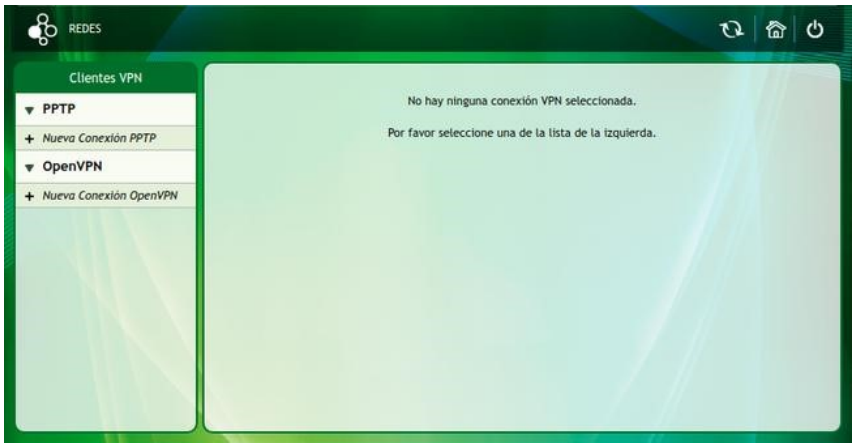

Figura 3.105: Clientes de VPN

Las VPN permiten una extensión segura de la red local sobre una red pública. Para ello, se realiza una conexión virtual punto a punto mediante el uso de conexiones dedicadas y/o cifradas. Presenta la ventaja de reducir el ancho de banda utilizado y aumentar la velocidad. Además proporciona comunicaciones seguras en las redes públicas con derechos de acceso específicos.

3.3.7.4.2.1. Cliente PPTP se conecta directamente al servidor de destino creando una red virtual para cada cliente remoto, que el administrador puede supervisar y administrar como cualquier otro puerto de acceso remoto. Para realizar la configuración de este cliente se debe efectuar un clic en la opción Nueva Conexión PPTP.

Figura 3.106: Clientes de VPN, PPTP

A continuación la descripción de los campos:

- Configuración general

- Nombre de la conexión: nombre que se asigna a la conexión.
- Servidor PPTP: IP o dominio del servidor PPTP.
- Usuario: nombre de usuario para acceder al servidor PPTP.
- Contraseña: contraseña de usuario para acceder al servidor PPTP.
- Conectar automáticamente: habilitar en caso de que la conexión siempre deba encontrarse activa

- Método de Autenticación: se debe seleccionar el o los protocolos de autenticación a usar.
  - PAP (Password Authentication Protocol): es un protocolo simple que autentica un usuario contra un servidor de acceso remoto. Su función es validar a un usuario para que acceda a diferentes recursos. Para esto, PAP transmite contraseñas en ASCII sin cifrar, por lo que se debe usar como último recurso.
  - CHAP (Challenge Handshake Authentication Protocol): es un protocolo de autenticación por desafío mutuo. Este verifica periódicamente la identidad del cliente remoto usando un intercambio de información. Con CHAP, el ID de usuario y la contraseña siempre se envían cifrados, lo que lo convierte en un protocolo más seguro que PAP.
  - MSCHAP (Microsoft Challenge Handshake Authentication Protocol): protocolo de autenticación por desafío mutuo de Microsoft. Este no requiere que ambas partes conozcan la clave en claro, sino un resumen (Hash) de la misma.
  - MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol v2): protocolo de autenticación por desafío mutuo de Microsoft versión 2. Proporciona seguridad de alto nivel para las conexiones de acceso remoto. MS-CHAP v2 resuelve algunos problemas de MS-CHAP.

- Método de Compresión: son métodos de encriptación, únicamente se utilizan con los protocolos MSCHAP y MSCHAPv2.
  - MPPE 40 (Microsoft Point-to-Point Encryption): Encriptación punto a punto de Microsoft de 40 bits.
  - MPPE 128 (Microsoft Point-to-Point Encryption): Encriptación punto a punto de Microsoft de 128 bits.

Luego se efectúa clic en Crear y la VPN se habrá creado. A continuación se puede observar la conexión generada.

Figura 3.107: Clientes de VPN, conexión PPTP configurada

Una vez que se crea la nueva conexión, ésta se puede Conectar, Eliminar o Modificar la conexión desde los botones situados en la sección inferior de la página.

3.3.7.4.2.2. Cliente OpenVPN es un software de red privada virtual de código abierto, que provee seguridad, estabilidad y mecanismos de cifrado sin presentar complejidad. Para configurar el cliente OpenVPN se debe hacer clic en la opción Nueva Conexión OpenVPN.

Figura 3.108: Clientes de VPN, configuración OpenVPN

A continuación la descripción de los campos:

- Configuración General
  - Nombre de la conexión: nombre que se le asignará a la conexión.
  - Servidor OpenVPN: IP o dominio del servidor OpenVPN.
  - Puerto: puerto que se utlizará para la conexión VPN.
  - Conectar automáticamente: habilitar en caso de que la conexión siempre deba encontrarse activa.
- Certificados
  - Autoridad de Certificación (CA): Posibilita importar el archivo.
  - Certificado del Cliente (CRT): Posibilita importar el archivo.
  - Llave del Cliente (KEY): Posibilita importar el archivo.

Estos certificados deben ser otorgados por el administrador del servidor de OpenVPN.

Figura 3.109: Clientes de VPN, configuración OpenVPN

Al igual que con el PPTP, se puede Conectar, Eliminar o Modificar la conexión desde los botones situados en la sección inferior de la página.

3.3.7.4.3. Servidor Web Al ingresar en esta pestaña de configuración, se puede activar o desactivar la opción de navegación segura. Se recomienda activar esta opción, ya que los datos transmitidos se cifran. Por lo cual genera menor probabilidad de que la información

sea interceptada por terceros. Para activar la navegación segura, es necesario hacer clic en el botón Habilitar HTTPS.

Figura 3.110: Servidor Web

HTTP Seguro

Un servidor web seguro consigue que la información viaje, a través de la red, protegida mediante el uso de algún algoritmo de encriptación, asegurando que sea inteligible sólo por el servidor y el usuario que accede a la web

Para habilitar el servidor web seguro, se solicita la generación del certificado para el HTTPs, esto se realiza mediante el botón de Generar Certificado. Con esto se muestra la siguiente página para completar los datos del certificado:

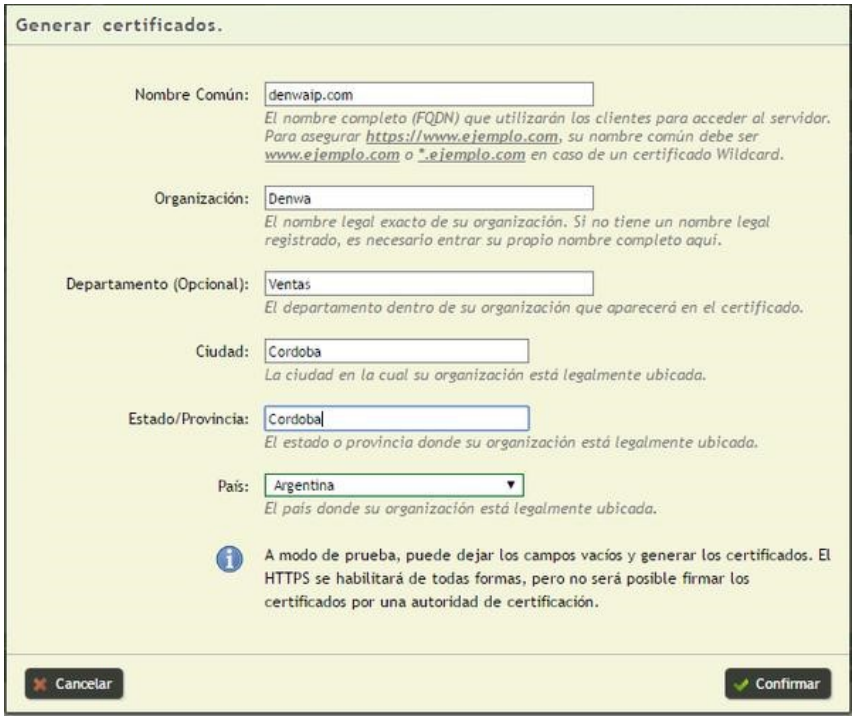

Figura 3.111: Servidor Web, carga de certificado

Con esto se genera y se carga internamente el certificado ssl para que la central funcione con HTTPs, de esta forma se muestra el servicio se encuentra activo. Por supuesto, como

ahora el servidor se encuentra en modo de navegación segura, se debe ingresar nuevamente como administrador para continuar con la configuración de la DenwaUC.

Al ingresar nuevamente a la sección de servidor web, se puede ver el HTTPs activado y la información del Certificado que fue generado.

Figura 3.112: Servidor Web, servicio habilitado

Denwa ofrece la función de descargar el Certificado generado, para ser validado por una entidad Certificadora. Denwa ofrece la posibilidad de validar el certificado ssl y poder cargar nuevamente de manera que al ingresar en modo seguro, no figure el error de certificado en el navegador.

Figura 3.113: Servidor Web, descarga e importación del certificado

Es importante que, en el momento de subir los certificados, se pegue la parte correspondiente a cada uno. En el primer campo el certificado (.crt), y en el segundo la clave privada (.key).

Figura 3.114: Servidor Web, formulario de carga de certificado

Para deshabilitar el servidor web seguro es necesario presionar en el botón de HTTPS, el sistema solicita la confirmación y nuevamente se deber ingresar en la web como administrador para continuar configurando las opciones.

3.3.7.4.4. Servidor DHCP Este servicio nos permite la configuración de un servidor DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. El servidor se encarga de proporcionar al host la configuración de red básica (IP, máscara de red, gateway, DNS, IP de aprovisionamiento).

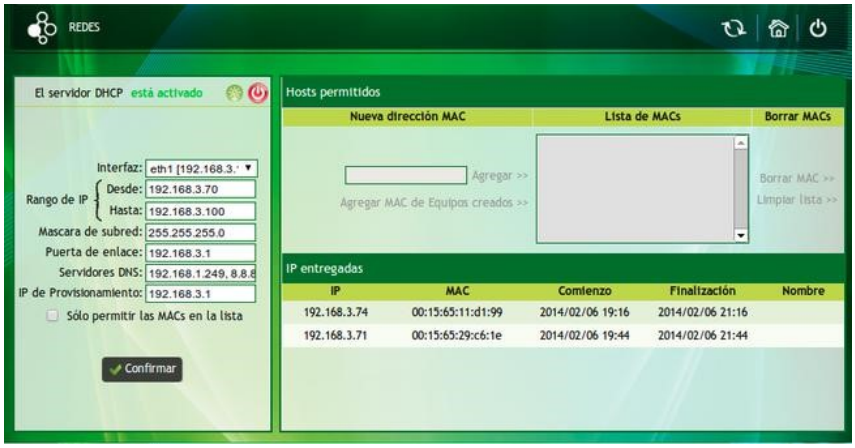

Figura 3.115: Servidor DHCP

Como se ve en la figura anterior, la pantalla esta dividida en tres zonas. En la zona principal, a la izquierda de la pantalla, se encuentra la configuración del servidor DHCP.

Es necesario configurar los siguientes datos para el correcto funcionamiento del servidor.

- **Interfaz**: se debe seleccionar la interfaz de red en la cual va a ser utilizado el servidor DHCP. Recuerde que la interfaz que se configura como servidor DHCP debe estar en el mismo rango de IP que la puerta de enlace e IP de aprovisionamiento.
- **Rango de IP**: es el rango de direcciones IP que el servidor va a entregar a los diferentes clientes (host) que las soliciten.
- **Máscara de subred**: combinación de bits que sirve para delimitar que parte de la dirección IP es el número de red y que parte corresponde a host.
- **Puerta de enlace**: es la puerta de enlace o gateway de la red.
- **Servidor DNS**: es la dirección del servidor DNS que utilizaremos.

- **IP de Provisionamiento**: Es la dirección IP que se utilizará para el aprovisionamiento de equipos. El teléfono al tomar ip por DHCP también tomará la dirección a donde buscar el archivo de configuración.

El campo «☐ Sólo permitir las MACs en la lista» habilita el filtrado de MAC según el listado que se muestra a la derecha de la pantalla. Las MAC pueden ser agregadas de forma manual, escribiendo la dirección en el campo correspondiente y pulsando «Agregar>>»; o agregando a todos los equipos agregados a «Mis Equipos» (ver Pestaña Mis Equipos en la página 126) pulsando sobre «Agregar MAC de Equipos creados >>»

Servidor externo de DHCP

Si utiliza un DHCP alternativo a Denwa, para realizar el aprovisionamiento necesita configurar las opciones 66 y 67 de DHCP apuntándolas hacia `http://ip-denwa/provisioning/general/`

Luego de completar estos parámetros se confirma la configuración pulsando sobre «✔ Confirmar» y se activa el servicio chaciendo clic en el ícono ⏻. En caso de desear reiniciarlo, bastará con pulsar sobre el botón ✱.

En el sector inferior derecho se encuentran los equipos que actualmente están conectados al servidor DHCP, junto con la siguiente información:

- **IP**: dirección IP asignada al dispositivo
- **MAC**: dirección MAC de la placa de red a la que se le otorgó la dirección IP
- **Comienzo**: fecha y hora de la concesión de la dirección IP
- **Finalización**: fecha y hora a la que se renovará la concesión
- **Nombre**: nombre del dispositivo

3.3.7.4.5. Servidor SNMPv1

El Protocolo Simple de Administración de Red o SNMP (por sus siglas en inglés) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas.

SNMP se basa en dos elementos principales, un supervisor y agentes. El supervisor es el terminal que le permite al administrador de red realizar solicitudes de administración y los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados. Estos dispositivos pueden ser información de hardware, parámetros de configuración, estadísticas de rendimiento, etc. Estos elementos se encuentran clasificados en una base de datos denominada MIB («Base de datos de información de administración»).

Para poder realizar el monitoreo como administración es necesario seguir los siguientes pasos

1. Instalar en la PC la aplicación SNMP para realizar el monitoreo desde la consola de linux

```
sudo apt-get install snmp
```

Instalación de SNMP

2. Configurar el servidor SNMP en Denwa UC&C 4.0.1 ingresando a Configuración >Redes >Servidor SNMP

Figura 3.116: Servidor SNMPv1

El primer paso para realizar la configuración es establecer la comunidad autorizada y los permisos para ellas. Existen diferentes métodos para determinar las comunidades la opción public (es posible monitorear de cualquier red), lista (se establecen redes o host determinados) o el casillero vacío (no se configura el permiso para la comunidad).

Luego se debe determinar que host o redes tienen permitido monitorear a la Denwa. Para definir un host se debe ingresar el número de IP con máscara 32 y para una red el número IP de la red y su máscara. Ademas se asigna a cada una los permisos desde el checkbox Modo. Para completar el proceso se debe hacer clic en el signo ⊕. Todas las redes se visualizan en una lista al final de la pantalla.

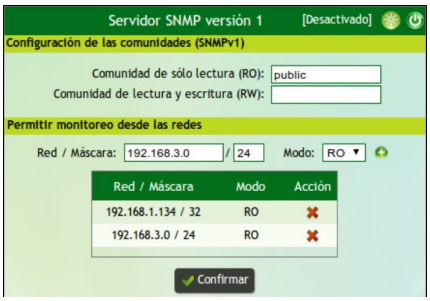

Figura 3.117: Servidor SNMPv1, adición de red

Por último, se debe hacer clic en «✔ Confirmar» y habilitar el servidor SNMP presionando en ✱.

3. Realizar el monitoreo de la Denwa desde la consola de LInux. Para ello se debe escribir el siguiente comando.

```
snmpget -v2c -c public 192.168.1.204 .1.3.6.1.4.1.2021.4.5.0
```

Ejemplo de consulta snmp

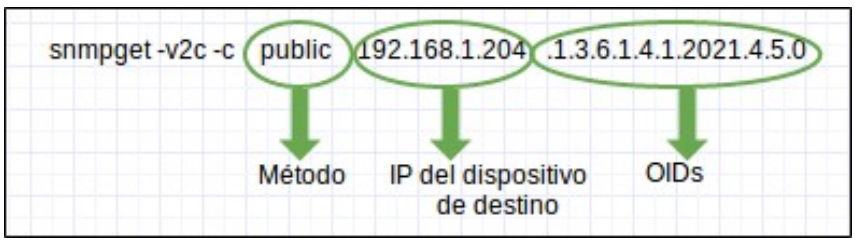

Figura 3.118: Servidor SNMPv1, estructura de la consulta

A continuación se describe algunos de los OIDs con la asociación del tipo de información que presenta cada uno.

- **Estadísticas de CPU**
  - **Carga de último minuto**: .1.3.6.1.4.1.2021.10.1.3.1
  - **Carga de últimos 5 minutos**: .1.3.6.1.4.1.2021.10.1.3.2
  - **Carga de últimos 15 minutos**: .1.3.6.1.4.1.2021.10.1.3.3
- **CPU**
  - **Porcentaje de tiempo de CPU por usuario**: .1.3.6.1.4.1.2021.11.9.0
  - **Tiempo de CPU del sistema**: .1.3.6.1.4.1.2021.11.10.0
  - **Porcentaje de tiempo libre de CPU**: .1.3.6.1.4.1.2021.11.11.0
- **Memory Statistics**
  - **Tamaño total de Swap**: .1.3.6.1.4.1.2021.4.3.0
  - **Espacio de swap disponible**: .1.3.6.1.4.1.2021.4.4.0
  - **RAM total**: .1.3.6.1.4.1.2021.4.5.0
  - **RAM usada**: .1.3.6.1.4.1.2021.4.6.0
  - **RAM libre**: .1.3.6.1.4.1.2021.4.11.0
  - **RAM compartida**: .1.3.6.1.4.1.2021.4.13.0
  - **RAM Buffered**: .1.3.6.1.4.1.2021.4.14.0
  - **Total de memoria cacheada**: .1.3.6.1.4.1.2021.4.15.0
- **Estadísticas de disco**
  - **Ruta donde está montado el disco**: .1.3.6.1.4.1.2021.9.1.2.1
  - **Ruta a la partición del equipo**: .1.3.6.1.4.1.2021.9.1.3.1
  - **Tamaño total de disco/partición(kBytes)**: .1.3.6.1.4.1.2021.9.1.6.1
  - **Espacio de disco disponible**: .1.3.6.1.4.1.2021.9.1.7.1
  - **Espacio de disco utilizado**: .1.3.6.1.4.1.2021.9.1.8.1
  - **Porcentaje de disco utilizado**: .1.3.6.1.4.1.2021.9.1.9.1
  - **Porcentaje de inodes utilizados**: .1.3.6.1.4.1.2021.9.1.10.1

3.3.7.4.5.1. Ejemplo de consulta de RAM Para monitorear la memoria RAM total de la cual dispone Denwa UC&C 4.0.1 , se ingresa en un cliente por consola.

```
snmpget -v2c -c public 192.168.1.139 .1.3.6.1.4.1.2021.4.5.0
```

Ejemplo de consulta de RAM por snmp

La respuesta es:

```
iso.3.6.1.4.1.2021.4.5.0 = INTEGER: 1016600
```

Ejemplo de respuesta a la consulta de RAM por snmp

Donde 1016600 es el tamaño en en megabyte de la memoria RAM.

3.3.7.4.5.2. Ejemplo de consulta de Temperatura Realizando una consulta snmp a los equipos puede obtener la información deseada, sin embargo deberá ser correlacionada. El community se configura desde la interfaz web de la PBX (Configuración Redes Servidor SNMPv1) y la IP corresponde a la IP del equipo que desea consultar.

```
snmpwalk -v 2c -c 1.3.6.1.4.1.2021.13.16
```

Ejemplo de consulta de Temperatura por snmp

El siguiente es un ejemplo de los datos que obtendrá de esta consulta:

```
iso.3.6.1.4.1.2021.13.16.2.1.1.1 = INTEGER: 1
iso.3.6.1.4.1.2021.13.16.2.1.1.2 = INTEGER: 2
iso.3.6.1.4.1.2021.13.16.2.1.1.3 = INTEGER: 3
iso.3.6.1.4.1.2021.13.16.2.1.1.4 = INTEGER: 4
iso.3.6.1.4.1.2021.13.16.2.1.1.5 = INTEGER: 5
iso.3.6.1.4.1.2021.13.16.2.1.1.6 = INTEGER: 6
iso.3.6.1.4.1.2021.13.16.2.1.1.7 = INTEGER: 7
iso.3.6.1.4.1.2021.13.16.2.1.1.8 = INTEGER: 8
iso.3.6.1.4.1.2021.13.16.2.1.1.9 = INTEGER: 9
iso.3.6.1.4.1.2021.13.16.2.1.1.10 = INTEGER: 10
iso.3.6.1.4.1.2021.13.16.2.1.1.11 = INTEGER: 11
iso.3.6.1.4.1.2021.13.16.2.1.2.1 = STRING: "loc1"
iso.3.6.1.4.1.2021.13.16.2.1.2.2 = STRING: "Physical id 0"
iso.3.6.1.4.1.2021.13.16.2.1.2.3 = STRING: "Core 0"
iso.3.6.1.4.1.2021.13.16.2.1.2.4 = STRING: "Core 1"
iso.3.6.1.4.1.2021.13.16.2.1.2.5 = STRING: "Core 2"
iso.3.6.1.4.1.2021.13.16.2.1.2.6 = STRING: "Core 3"
iso.3.6.1.4.1.2021.13.16.2.1.2.7 = STRING: "Core 4"
iso.3.6.1.4.1.2021.13.16.2.1.2.8 = STRING: "Core 5"
iso.3.6.1.4.1.2021.13.16.2.1.2.9 = STRING: "Core 6"
iso.3.6.1.4.1.2021.13.16.2.1.2.10 = STRING: "Core 7"
iso.3.6.1.4.1.2021.13.16.2.1.2.11 = STRING: "Physical id 1"
iso.3.6.1.4.1.2021.13.16.2.1.3.1 = Gauge32: 47000
iso.3.6.1.4.1.2021.13.16.2.1.3.2 = Gauge32: 33000
iso.3.6.1.4.1.2021.13.16.2.1.3.3 = Gauge32: 29000
iso.3.6.1.4.1.2021.13.16.2.1.3.4 = Gauge32: 29000
iso.3.6.1.4.1.2021.13.16.2.1.3.5 = Gauge32: 28000
iso.3.6.1.4.1.2021.13.16.2.1.3.6 = Gauge32: 28000
iso.3.6.1.4.1.2021.13.16.2.1.3.7 = Gauge32: 28000
iso.3.6.1.4.1.2021.13.16.2.1.3.8 = Gauge32: 27000
iso.3.6.1.4.1.2021.13.16.2.1.3.9 = Gauge32: 27000
iso.3.6.1.4.1.2021.13.16.2.1.3.10 = Gauge32: 27000
iso.3.6.1.4.1.2021.13.16.2.1.3.11 = Gauge32: 34000
```

Ejemplo de respuesta a la consulta de Temperatura por snmp

La información debe ser relacionada por número de sensor, siendo este el último número de la cadena de la consulta (en iso.3.6.1.4.1.2021.13.16.2.1.3.11 el número del sensor sería el 11), debiendo leerse los resultados de la siguiente manera:

1	loc1	47000
2	Physical id 0	33000
3	Core 0	29000
4	Core 1	29000
5	Core 2	28000
6	Core 3	28000
7	Core 4	28000
8	Core 5	27000
9	Core 6	27000
10	Core 7	27000
11	Physical id 1	34000

El valor está en miligrados Centígrados, es decir que debe dividirse en mil para ser leída en grados Centígrados; es decir:

1	loc1	47,000 °C
2	Physical id 0	33,000 °C
3	Core 0	29,000 °C
4	Core 1	29,000 °C
5	Core 2	28,000 °C
6	Core 3	28,000 °C
7	Core 4	28,000 °C
8	Core 5	27,000 °C
9	Core 6	27,000 °C
10	Core 7	27,000 °C

11 Physical id 1 34,000 °C

3.3.7.4.6. Servidor OpenVPN En este apartado se configurará el servicio de OpenVPN para disponer de conexiones seguras para usuarios fuera de la red. Al ingresar al servidor se puede observar una pantalla como la siguiente:

Figura 3.119: Servidor OpenVPN

En la columna de la izquierda es posible iniciar o detener el servicio de OpenVPN Server pulsando sobre el ícono ⏻.

3.3.7.4.6.1. Pestaña de Configuración En la imagen anterior se puede notar que el servidor se encuentra deshabilitado y que no existe una configuración pre-cargada. A continuación el detalle de los parámetros a configurar:

- **Puerto**: puerto a utilizar para el servicio de OpenVPN
- **Protocolo**: protocolo que empleado por el servidor
- **Dirección de red/Máscara**: red de la cual se otorgará direcciones IP a los clientes
- **Permitir acceso**: redes a las que se le desea dar acceso a los clientes.

3.3.7.4.6.2. Pestaña de Cuentas En esta pestaña es posible dar de alta cuentas para el acceso remoto a la plataforma de comunicaciones unificadas y/o a las redes seleccionadas en la pestaña de configuración.

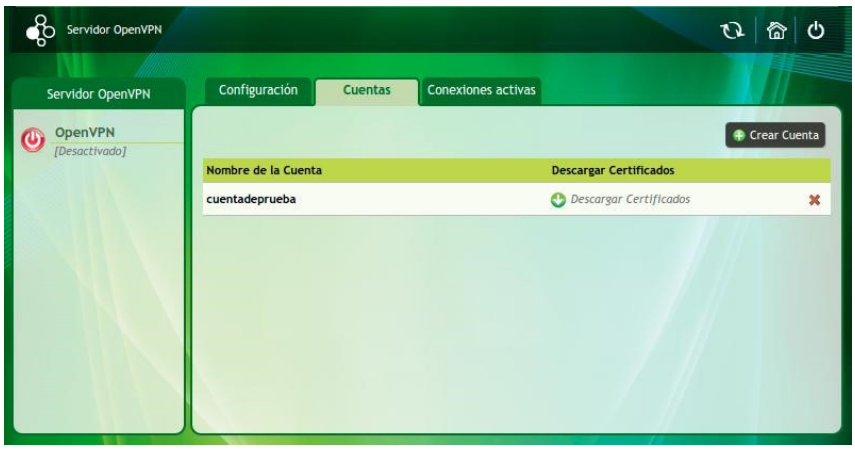

Figura 3.120: Servidor OpenVPN, cuentas de acceso

Para realizar una nueva cuenta simplemente hacemos clic en Crear Cuenta, y complertar el nombre de usuario; con esto la cuenta se ha creado y es posible descargar sus certificados.

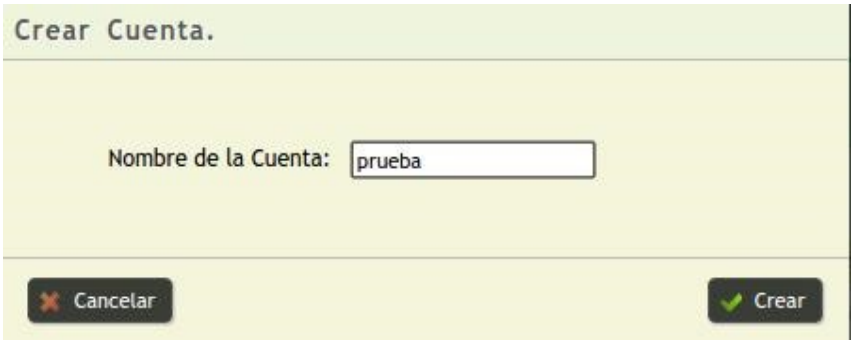

Figura 3.121: Servidor OpenVPN, creación de cuenta de acceso

Para utilizar el servidor de OpenVPN es necesario disponer de los certificados en los equipos que se conectarán a él, por lo que deben ser descargados desde la pestaña cuentas. Una vez en el equipo local es necesario disponer del software «cliente» de OpenVPN y, desde un editor de texto básico, generar un archivo .ovpn como el que se muestra a continuación:

```
##############################################
#   Cliente OpenVPN
##############################################
client
dev tun
proto PROTOCOLO
remote IP_DE_SERVIDOR PUERTO_DE_SERVIDOR
resolv-retry infinite
nobind
comp-lzo
verb 3
# Certificates files
ca "RUTA_DE_CERTIFICADO/ca.crt"
cert "RUTA_DE_CERTIFICADO/NOMBRE_CERTIFICADO.crt"
key "RUTA_DE_CERTIFICADO/NOMBRE_CERTIFICADO.key"
##############################################
```

Debe reemplazar donde dice «PROTOCOLO», «IP_DE_SERVIDOR», «PUERTO_DE_SERVIDOR», «RUTA_DE_CERTIFICADO», «NOMBRE_CERTIFICADO» según las configuraciones realizadas en el servidor, así como los certificados descargados.

3.3.7.4.6.3. Pestaña de Registros En esta pestaña se mostrará el listado de todas las conexiones activas («clientes» conectados) al servicio OpenVPN.

3.3.7.4.7. Firewall Este servicio permite la configuración de un firewall, cuyo objetivo es ayudar a impedir que hackers o software malintencionado obtengan acceso al equipo a través de una red o de Internet. Se encarga de crear una barrera entre Internet y el equipo, igual que la barrera física que constituiría una pared de ladrillos.

El firewall actúa como un filtro controlando todas las comunicaciones que pasan de una red a otra y en función de esto permite o deniega el paso, para ello examina el tipo de servicio al que corresponde. También inspecciona si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

Al ingresar a la configuración de Firewall, se encuentra un panel con tres botones que habilitan y deshabilitan diversas opciones, detalladas a continuación.

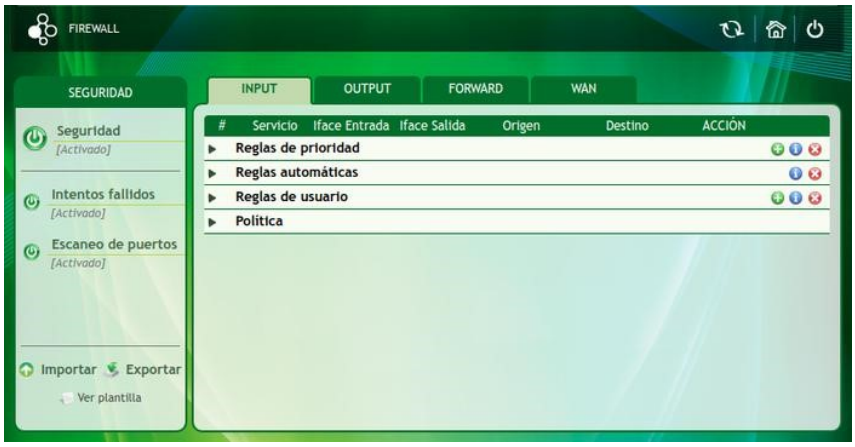

Figura 3.122: Firewall

Desde el botón ⏻ se puede activar o desactivar la seguridad de Denwa UC&C 4.0.1 . Con firewall activado los puertos se abren de manera dinámica, únicamente durante el tiempo que requiera permitir el acceso a los servicios que se desean.

Intentos fallidos : si el sistema detecta más de cinco intentos fallidos de registro de los equipos, automáticamente bloquea el acceso desde la dirección de IP, ya que toma esto como un intento de ataque. La única manera que esta regla sea removida del firewall es que un administrador autorizado la quite de forma manual.

Escaneo de puertos : permite bloquear ataques de este tipo de manera automática, Denwa UC&C 4.0.1 está constantemente chequeando posibles escaneos de puertos sobre el equipo, al detectar esto el sistema automáticamente bloquea la dirección IP que está intentando realizar este posible ataque creando una nueva regla en el Firewall. La única manera que esta regla sea quitada del firewall es que un administrador autorizado la quite de manera manual.

También Denwa permite crear nuevas reglas, estas dependen de lo que se desee. Las nuevas reglas pueden ser de entrada, salida o forward.

Estas reglas permiten ser importadas haciendo clic en el ícono «Importar» o exportadas a partir del ícono «Exportar» mediante un archivo .csv. Para la importación se recomienda descargar una plantilla realizando clic en el ícono «Ver Plantilla» y editar cada fila con la regla que desee agregar. Se sugiere corroborar que el formato no se haya modificado.

Política del Firewall

Denwa UC&C 4.0.1 determina una política general de firewall. Esta puede ser Accept o Drop, si se establece política de **Accept** todas las reglas creadas deben ser de **Drop**, es decir excepciones a la política.

3.3.7.4.7.1. Pestañas INPUT, OUTPUT y FORWARD Desde las pestañas INPUT, OUTPUT y FORWARD se puede gestionar las conexiones entrantes, salientes y redireccionadas, respectivamente.

Figura 3.123: Firewall, configuración de las cadenas

Existen tres (3) tipos de reglas:

- **Reglas de prioridad**: son reglas de alta prioridad creadas por el administrador de la Denwa UC y tienen mayor prioridad que las reglas agregadas por los servicios de bloqueo automático. Cuenta con los botones ⊕ (agregar regla), ℹ (ayuda) y ⊗ (borrar todas las reglas).

  Excepción en Alta Disponibilidad

  Cuando Denwa UC&C 4.0.1 forma parte de un cluster de Alta Disponibilidad (Activo-Pasivo), las reglas de prioridad serán bloqueadas por el sistema, no permitiendo su edición.

- **Reglas automáticas**: estas reglas no son generadas por los administradores, sino que se generan de manera automática por los servicios de escaneo de puertos e intentos fallidos. Cuenta con los botones ℹ (ayuda) y ⊗ (borrar todas las reglas).

- **Reglas de usuario**: son reglas creadas por el administrador. Cuenta con los botones ⊕ (agregar regla), ℹ (ayuda) y ⊗ (borrar todas las reglas).

Tanto en las reglas de prioridad, como en las de usuario, al momento de agregar una regla se muestra la siguiente ventana:

Figura 3.124: Firewall, agregar regla

- **Servicio**: se selecciona el servicio a gestionar desde una lista desplegable. Los servicios pueden ser:
  - SSH

- PING
- RTP
- SIP
- HTTP
- HTTPS
- TFTP
- FTP
- DNS
- XMPP
- VPN
- Todos
- O por protocolo y puerto

En este último caso la ventana cambiará para poder ubicar protocolo (TCP o UDP) y el número de puerto correspondiente.

- **Interface de Entrada**: se elige la interface a la que se le aplica la regla.
- **Origen**: se determina a quien se le fija la regla, puede ser Todo el mundo, Host específico, Red específica o Zona. En el caso e red específica se debe asignar también la IP o Dominio; para el caso de zona se debe seleccionar un país; y para los casos Host específico y Red específica se debe seleccionar el tipo.

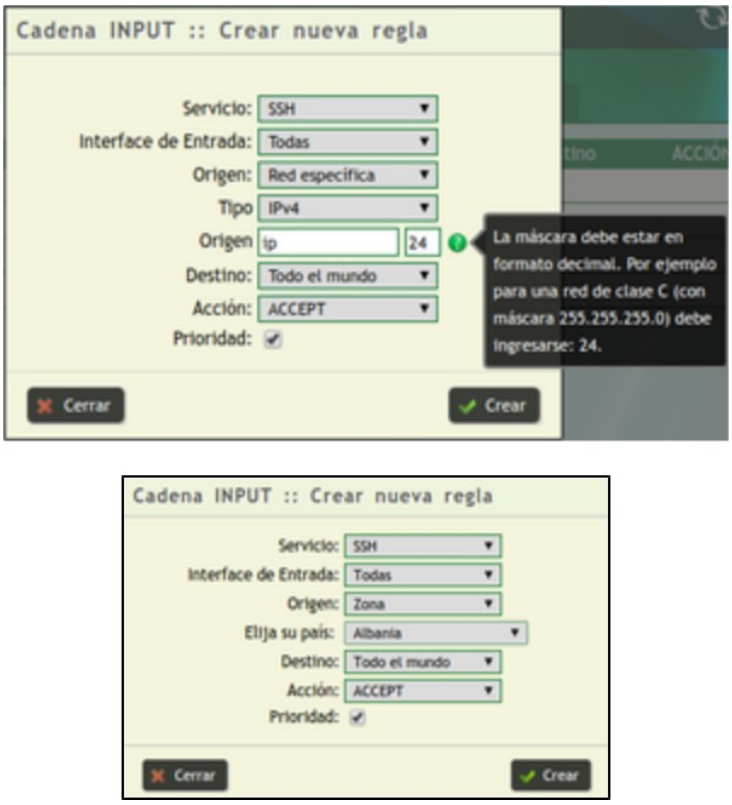

Figura 3.125: Configuración de las cadenas, red específica

- **Destino**: puede ser Todo el mundo, Host específico, o Red específica. En estos últimos casos se debe asignar también la IP o Dominio y el tipo.
- **Acción**: las opciones serán ACCEPT (Aceptar), REJECT (Rechazar) y DROP (Descartar). Estas acciones determinan que tipo de regla se crea.

- **Prioridad:** ☐: este campo indica que la regla creada es de alta prioridad.

Una vez creada la regla se visualiza de la siguiente forma:

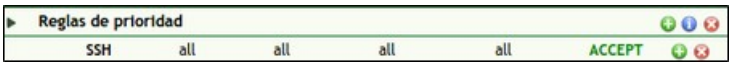

Figura 3.126: Configuración de las cadenas, regla creada

Desde los símbolos ⊕ ⊗ se permite agregar una nueva regla o eliminar la existente, respectivamente. En el primer caso, agregar una nueva regla, proporciona las opciones de:

- Insertar Arriba
- Insertar Abajo

Además de las opciones habituales se permite seleccionar si la nueva regla se va colocar arriba o abajo de la ya existente.

Política Se establece la regla por defecto que todo paquete que no concuerde con alguna de las reglas creadas será aceptado/rechazado, según se selecciona en el menú desplegable; por defecto la política es aceptado.

Orden y prioridad

Se debe tener siempre presente que el firewall es 'secuencial', por lo cual se dará prioridad a aquellas reglas que se encuentren sobre las otras. La secuencia que utiliza dicho firewall es la siguiente: Reglas de prioridad, Reglas automáticas, Reglas de usuario, Servicios (WAN) y Política.

3.3.7.4.7.2. Pestaña WAN En esta sección se permite configurar la seguridad de los servicios WAN, es decir que sólo aplica a tráfico entrante. Se brinda una simple gestión para el administrador mediante una ventana como la que se muestra en la siguiente imagen:

Figura 3.127: Firewall, configuración de WAN

El listado superior muestra las interfaces de red que Denwa UC&C 4.0.1 tiene configuradas, en la última columna se debe seleccionar aquella interfaz que será utilizada como WAN.

Dado que todos los servicios por defecto se encuentran deshabilitados para elevar el nivel de seguridad; se deben habilitar sólo los que se desean permitir desde la WAN.

Orden y prioridad

Se debe tener siempre presente que el firewall es 'secuencial', por lo cual se dará prioridad a aquellas reglas que se encuentren sobre las otras. La secuencia que utiliza dicho firewall es la siguiente: Reglas de prioridad, Reglas automáticas, Reglas de usuario, Servicios (WAN) y Política.

3.3.7.4.8. Servidor NTP NTP (*Network Time Protocol*) es un protocolo para sincronización de los relojes en equipos de red basado en un sistema cliente-servidor. Esta funcionalidad es importante porque permite que los dispositivos de la red tengan en todo momento (incluso cuando se pierda conexión a internet) la configuración de hora correcta.

Con este servidor se provee a los clientes *offset*, *round-trip delay* y referencia de dispersión. El *offset* especifica la diferencia entre la hora del sistema local y la referencia externa de reloj. *Round-trip delay* especifica las latencias de tiempo medidas durante la transferencias de paquetes dentro de la red. La referencia de dispersión de tiempo especifica el máximo número de errores asociados con la información de tiempo recibido de un reloj externo.

Para la configuración del servidor dentro de Denwa UC&C 4.0.1 se deben realizar los siguientes pasos

Figura 3.128: NTP, configuración

Los parámetros de zona horaria y fecha pueden ser modificados. La zona horaria se debe elegir desde el menú desplegable, en tanto que la fecha actual se debe completar en los *textbox* con el formato «dd/mm/yyyy», mientras que el horario en el de «hh:mm». Para aceptar los cambios es necesario hacer un clic en el ícono ✔.

En caso de desear deshabilitar el servicio, este puede ser apagado en el botón ⏻.

Por defecto, Denwa UC&C 4.0.1 , chequea su propia configuración de hora con un servidor externo, este es por defecto el servidor `ntp.ubuntu.com`, es posible agregar o utilizar un servidor distinto al configurado de fábrica completando el dominio del servidor y haciendo clic en ⊕.

Una vez configurado el servidor NTP, Denwa UC&C 4.0.1 procederá a:

- Configurar todos los equipos de la red con la cambios anteriormente realizados.
- Chequear periódicamente que su configuración de hora sea correcta usando los servidores que se configuraron anteriormente (por defecto: ntp.ubuntu.com).
- Si se pierde la conexión a estos servidores, los equipos de la red serán sincronizados contra Denwa UC&C 4.0.1 y no van a perder su configuración.

3.3.7.4.9. Servidor de mensajería El servidor de mensajería permite activar y desactivar la mensajería instantánea de los usuarios creados en la Denwa.

Para activar el servidor se debe hacer clic sobre ✱ y para desactivar en ⏻.

3.3.7.5. Servicio de llamadas

Desde el menú Servicios de llamada se puede crear y gestionar la definición del plan de numeración que se utiliza en el PBX Denwa.

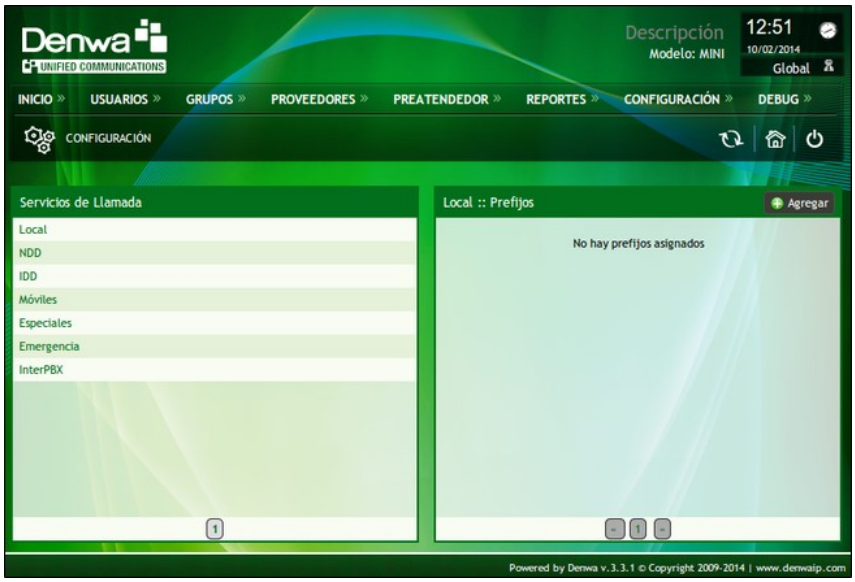

Figura 3.129: Servicio de llamadas

Los diferentes servicios son los siguientes:

- **Local**: son los números discados que el sistema identificará como llamadas locales. Para agregar un prefijo local se debe:

  1. Seleccionar «Local» en el listado de la izquierda
  2. Pulsar el botón «⊕ Agregar» del recuadro llamado «Local :: Prefijos»
  3. Agregar el nuevo prefijo para las llamadas locales
  4. Pulsar sobre el botón «⊕ Confirmar»

  Estos pasos pueden ser repetidos cuantas veces sea necesario, quedando la lista de la siguiente manera:

Figura 3.130: Servicio de llamadas, prefijos de llamadas locales

- **NDD**: son números discados que el sistema identificará como llamadas nacionales. Para agregar un prefijo NDD se debe:

  1. Seleccionar «NDD» en el listado de la izquierda
  2. Pulsar el botón «⊕ Agregar» del recuadro llamado «NDD :: Prefijos»
  3. Agregar el nuevo prefijo para las llamadas nacionales de discado directo
  4. Pulsar sobre el botón «⊕ Confirmar»

Estos pasos pueden ser repetidos cuantas veces sea necesario, quedando la lista de la siguiente manera:

Figura 3.131: Servicio de llamadas, prefijos de llamadas nacionales de discado directo

En este caso para Argentina el discado directo nacional es el 0.

- **IDD**: Son números discados que el sistema identificará como llamadas Internacionales. Para agregar un prefijo IDD se debe:

  1. Seleccionar «IDD» en el listado de la izquierda
  2. Pulsar el botón «⊕ Agregar» del recuadro llamado «IDD :: Prefijos»
  3. Agregar el nuevo prefijo para las llamadas internacionales de discado directo
  4. Pulsar sobre el botón «⊕ Confirmar»

  Estos pasos pueden ser repetidos cuantas veces sea necesario, quedando la lista de la siguiente manera:

Figura 3.132: Servicio de llamadas, prefijos de llamadas internacionales de discado directo

En este caso para Argentina el discado directo internacional es el 00.

- **Móviles**: son números discados que el sistema identificará como llamadas a móviles. Para agregar un prefijo Móvil se debe:

  1. Seleccionar «Móviles» en el listado de la izquierda
  2. Pulsar el botón «⊕ Agregar» del recuadro llamado «Móviles :: Prefijos»
  3. Agregar el nuevo prefijo para las llamadas a móviles
  4. Pulsar sobre el botón «⊕ Confirmar»

  Estos pasos pueden ser repetidos cuantas veces sea necesario. En el caso de Argentina la llamada a móviles comienzan con 15, pero hay que tener en cuanta que móviles que

no son locales se le debe anteceder la código de área. Por ejemplo, para llamadas a móviles fuera del área local se deben cargar de la siguiente manera:

Figura 3.133: Servicio de llamadas, prefijo de llamada a móvil fuera del área local

La lista queda formada de la siguiente manera:

Figura 3.134: Servicio de llamadas, prefijos de llamadas a móviles

- **Especiales**: son números discados que el sistema identificará como llamadas a números especiales como por ejemplo 0800, 0610, 0600, etc. Para agregar un prefijo especiales se debe:

1. Seleccionar «Especiales» en el listado de la izquierda
2. Pulsar el botón «⊕ Agregar» del recuadro llamado «Especiales :: Prefijos»
3. Agregar el nuevo prefijo para las llamadas a números especiales
4. Pulsar sobre el botón «⊕ Confirmar»

Estos pasos pueden ser repetidos cuantas veces sea necesario, quedando la lista de la siguiente manera:

Figura 3.135: Servicio de llamadas, prefijos de llamadas a números especiales

- **Emergencia**: son números discados que el sistema identificará como llamadas a números de emergencia como por ejemplo 911, 101, 100. Para agregar un prefijo emergencias se debe:

  1. Seleccionar «Emergenciaa» en el listado de la izquierda
  2. Pulsar el botón «⊕ Agregar» del recuadro llamado «Emergenciaa :: Prefijos»
  3. Agregar el nuevo prefijo para las llamadas a Emergencias
  4. Pulsar sobre el botón «⊕ Confirmar»

  Estos pasos pueden ser repetidos cuantas veces sea necesario, quedando la lista de la siguiente manera:

Figura 3.136: Servicio de llamadas, prefijos de llamadas a Emergencias

- **InterPBX**: son los números discados para llamadas entre PBX.

Para eliminar los prefijos de la lista se debe presionar en «borrar».

3.3.7.6. Anuncios

Desde la pestaña de Anuncios, se puede personalizar anuncios o mensajes de voz asociados a distintos eventos de Denwa UC&C 4.0.1 . Estos mensajes se encuentran predefinidos por Denwa, pero el administrador puede personalizarlos según su conveniencia. Éstos anuncios se encuentran disponibles en cuatro (4) idiomas, a saber:

- Español
- Inglés
- Portugués
- Hebreo

Figura 3.137: Anuncios

3.3.7.6.1. Anuncios por Idioma Para desplegar el listado de audios correspondiente a cada idoma (o música en espera) se debe hacer clic sobre el nombre del idioma, lo cual cambiará el ícono ▸ en ▾. Se mostrará el ícono › al lado de la opción mostrada.

Todos y cada uno de los audios listados cuenta con las siguientes opciones:

- ℹ: Información sobre las propiedades del archivo de audio.

Figura 3.138: Anuncios, propiedades del archivo de audio

- ▶: Reproducir
- 📥: Descargar
- ✖: Borrar

Para cargar un nuevo anuncio, se debe eliminar primero el archivo de audio a reemplazar para luego ingresar el nuevo. También permite subir y descargar archivos en formato zip, por medio de los botones «⬆ Subir Audios (zip)» y «📥 Descargar Audios (zip)»

3.3.7.6.2. Música en Espera En esta sección se agrega la opción de poder configurar música en espera en troncales, grupos, usuarios, etc. Para la cual el administrador:

- Debe definir nombre y descripción
- Subir un archivo de audio

Además, el administrador puede descargar, escuchar y actualizar cada una de las listas. Una vez cargadas, pueden ser seleccionadas en la sección avanzada de Usuario, en Grupos y Preatendedores.

3.3.7.7. Equipos

Esta funcionalidad de Denwa UC&C 4.0.1 permite buscar e incorporar equipos en la red local para luego asociarlos a cada uno de los usuarios creados.

Requerimientos

Se debe configurar correctamente el servidor DHCP de Denwa UC&C 4.0.1 . Dentro de la configuración del servidor DHCP la IP de aprovisionamiento debe ser la IP de Denwa UC&C 4.0.1 para su óptima operación.
Los equipos a incorporar deben tener la configuración de fábrica, esto se logra desde la página de administración del equipo o desde el menú del mismo. Los pasos a realizar dependen de la marca y modelo.

DHCP externo

Los equipos que no recibieron un IP desde el DHCP de Denwa UC&C 4.0.1 , no se provisionarán automáticamente, por lo cual se debe realizar de forma manual.

3.3.7.7.1. Pestaña Mis Equipos En la pestaña Mis Equipos, se puede conocer el estado de los equipos ya configurados dentro de Denwa UC&C 4.0.1 .

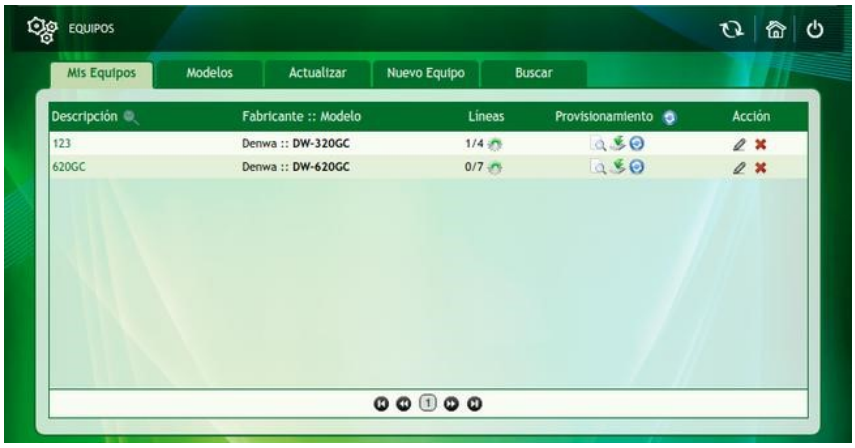

Figura 3.139: Equipos, Mis equipos

En la figura anterior se puede ver una lista de los equipos configurados, es posible filtrar según la Descripción realizando un clic en 🔍.

Para conocer la información sobre los equipos aprovisionados se debe hacer clic sobre el nombre del mismo, que figura bajo la columna «Descripción», con ello se visualizan datos relacionados al dispositivo y a su fabricante, así como también información asociada a la red.

Pulsando sobre el ícono ⚙, es posible administrar las cuentas SIP del equipo, siendo posible desasociar un puerto realizando un clic el ícono con forma de equis (✖) en el puerto deseado.

En la columna «Provisionamiento» se observan tres opciones:

- 📄: Ver archivo de aprovisionamiento.
- 📥: Descargar archivo de aprovisionamiento.
- 🔄: Regenerar el archivo de aprovisionamiento, normalmente se usa cuando se ha generado un cambio.

La columna Acción presenta dos opciones:

- ✎: proporciona información del equipo y permite variar las opciones, como:

- **Descripción**: es un nombre descriptivo del equipo.
- **Número de serie**: número serie del equipo.
- **Registrar en**: interfaz a registrar el equipo
- **Usuario**: nombre del usuario del equipo para el acceso.
- **Contraseña**: clave de acceso al equipo para acceso como usuario

Figura 3.140: Equipos, modifcación de mis equipos

Luego de realizar las modificación es necesario regenerar el archivo de aprovisionamiento para que los cambios tengan efecto.

- ✖: elimina el equipo de la red Denwa.

3.3.7.7.2. Pestaña Modelos En esta pestaña se presenta un desplegable con marcas y modelos de equipos. Con un clic sobre el nombre del fabricante, se mostrará el listado de los equipos que han sido homologados para el aprovisionamiento desde Denwa UC&C 4.0.1 .

Figura 3.141: Equipos, modelos

Los datos que se observan son:

- **Fabricante**: nombre del fabricante
- **Modelo**: muestra el modelo del dispositivo, también es posible ver una foto del mismo pulsando sobre 👁
- **Líneas**: indica la cantidad de líneas SIP que pueden ser configuradas

- **Firmware**: es la versión de firmware utilizada para la homologación del equipo, es necesario utilizar las misma versión o superior.

  Versión de firmware

  Es posible chequear en esta misma pantalla la opción actualizar para verificar que el modelo posea la última versión de firmware homologada.

  A la derecha de esta opción se encuentra el ícono utilizado para poder descargar el firmware homologado ( ).

- **Plantilla**: es posible ver la plantilla al hacer clic sobre o descargarla con un clic en . En ambos casos se observa un archivo de texto que contiene información global de los módulos.

- **Plantilla personalizada**: se permite subir una plantilla personalizada para el equipo al hacer clic sobre .

- **Actualizar**: La opción posee dos secciones:

  - : permite actualizar todas las plantillas de aprovisionamiento de los dispositivos correspondientes a este modelo
  - **Estado de actualización**:
    - : la Denwa UC&C 4.0.1 cuenta con la versión más reciente de firmware y plantillas homologadas
    - : Denwa Technology Corp. ha publicado una versión más reciente de firmware y plantillas homologadas, que pueden ser descargadas haciendo click sobre el ícono.

3.3.7.7.3. Pestaña Actualizar Es similar a la anterior (Pestaña Modelos, página 127), con la salvedad de que únicamente se muestra aquellos dispositivos que cuentan con una actualización pendiente de descarga.

3.3.7.7.4. Pestaña Nuevo Equipo A través de esta pestaña es posible cargar manualmente un equipo a Denwa UC&C 4.0.1 .

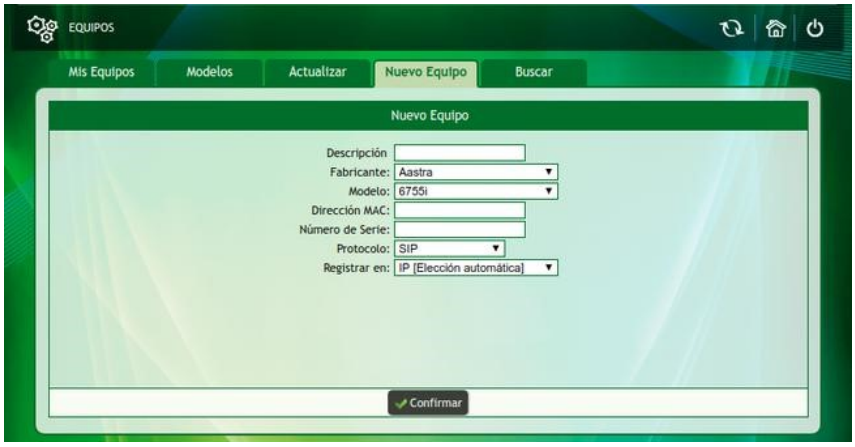

Figura 3.142: Equipos, nuevo equipo

Los campos a completar son los siguientes.

- **Descripción**: es un nombre descriptivo que se le da al equipo.
- **Fabricante**: la lista esta basada en equipos homologados para Denwa UC&C 4.0.1 y su aprovisionamiento.

- **Modelo**: muestra una lista desplegable con los modelos homologados de este fabricante para aprovisionamiento con la Denwa UC&C 4.0.1 .

- **Dirección MAC**: Información de importancia ya que es el identificador único del equipo.

- **Número de Serie**: número serie del equipo.

- **Protocolo**: puede ser SIP o MGCP.

- **Registrar en**: permite seleccionar la interfaz en la que el equipo se va a registrar.

Luego de completar los campos se debe confirmar presionando sobre «✔ Confirmar».

3.3.7.7.5. Pestaña Buscar En esta sección se explican los pasos a seguir para la búsqueda de equipos y el aprovisionamiento de los mismos. Se supone que los requerimientos previos (ver advertencia en Equipos en la página 126) fueron configurados correctamente.

Figura 3.143: Equipos, buscar equipos

La búsqueda de equipos se basa en tablas ARP e identifica los dispositivos descubiertos según su dirección MAC. La pantalla nos muestra dos (2) distintas opciones de búsqueda:

- **Cargar última búsqueda**: permite efectuar nuevamente la última búsqueda realizada con las opciones de búsqueda utilizadas.

- **Realizar una nueva búsqueda**: permite buscar en la red local los equipos existentes, los pasos a seguir son muy simples.

1. Seleccionar la interfaz haciendo clic sobre Interfaz y seleccionar de la lista desplegable la interfaz en la que se quiere buscar equipos.
2. Hacer clic en Realizar una nueva búsqueda.

Una vez realizada la búsqueda se muestra la pantalla:

Figura 3.144: Equipos, resultado de búsqueda de equipos

El listado mostrado contiene los equipos descubiertos en la red a la que pertenece la interfaz seleccionada. Incluye:

- **Fabricante**: permite el filtrado mediante la pulsación sobre 🔍
- **Modelo**
- **Dirección MAC**
- **Dirección IP**
- **Acción**: de acuerdo al estado de aprovisionamiento del equipo, puede mostrar dos (2) íconos diferentes
  - ℹ: se muestra solamente al lado de los equipos aprovisionados, permite visualizar información del dispositivo.
  - ⊕: se muestra solamente al lado de los equipos no aprovisionados, al pulsarlo se muestra una ventana emergente para iniciar el proceso de aprovisionamiento.

Figura 3.145: Búsqueda de equipos, adición de equipo

Sus campos son:

- **Descripción del equipo**: es un nombre descriptivo del equipo.
- **Modelo**:
- **Registrar en**: se selecciona la interfaz donde será registrado el dispositivo.
- **Protocolo**: se selecciona el protocolo, SIP o MGCP.
- **Asignar a usuario:** ☐: permite asignar el equipo a un usuario previamente creado en Denwa UC&C 4.0.1 , al hacer clic en el checkbox se abre una ventana en donde se podrá realizar la búsqueda de usuarios, al seleccionar uno es necesario presionar en «✔ Confirmar»

Figura 3.146: Búsqueda de equipos, adición de equipo

Reinicio para aprovisionamiento

Es necesario luego del aprovisionamiento reiniciar el teléfono provisionado para que tome los datos de aprovisionamiento. Los modelos Denwa soportan la opción de reinicio automático.

3.3.7.8. Mis aplicaciones

Denwa permite que se utilicen aplicaciones con fines particulares, las cuales pueden ser diseñadas por el administrador sobre el modulo DTI (Denwa Telephony Interface). Además permiten asignar las mismas a Preatendedores y/o Usuarios.

3.3.7.8.1. Pestaña Mis aplicaciones Al ingresar a esta pestaña, se observan cinco columnas.

- **Nombre**: el nombre de la aplicación. Al hacer clic sobre el nombre aparece la siguiente ventana.
- **Descripción**: pequeña reseña sobre la aplicación.
- **Tipo**: en donde esta basada la aplicación.
- **Audios**: permite escuchar los audios. Al hacer clic sobre se visualiza la siguiente pantalla.

  Aquí se puede cargar un audio desde y obtener información al hacer clic en . Una vez cargado el archivo se puede reproducir desde, descargar o eliminar .
- **Acción**: modificar o borrar las aplicaciones.

3.3.7.8.2. Pestaña Nueva aplicación Para crear una nueva aplicación,se debe elegir el tipo de aplicación deseada, ingresar un nombre y una descripción. Luego para finalizar se presiona en Confirmar.

3.3.7.8.2.1. Aplicación Jefe-Secretaria En un escenario de Jefe - Secretaria, al levantarse la secretaria de su puesto puede, mediante el uso de su telefono, deshabilitar temporalmente la funcion. A partir de ese momento las llamadas le comienzan a llegar directamente al jefe. Al retomar su puesto, pueda restituir la funcion, y que vuelva a quedar como secretaria.

Esto es similar a tildar y destildar la opcion desde la administracion web, solo que el manejo se realiza desde el telefono de la secretaria mediante una aplicacion.

Para crear la aplicación, en las sección de Configuración >Mis aplicaciones damos de alta la aplicación «Set Boss-Secretary Aplication» y completar Nombre y Descripción.

Luego aparecerá en la lista de Mis aplicaciones. Se deben cargar los audios para que la aplicación pueda funcionar, se pueden personalizar los audios haciendo clic en el ícono y cargar acorde a la función, o hacer clic en para cargar los audios por default de la aplicación.

Al dar de alta los audios, apareceran en la lista y la aplicación estará lista para funcionar.

Para poder llamar a la aplicación, es necesario crear una extensión tipo aplicación y asociar la misma

Solo las extensiones declaradas como secretarias podrán llamar a la extensión tipo aplicación.

Procedimiento

Para el ejemplo de configuración, el interno 300 es la aplicación de Jefe Secretaria. En la siguiente imagen veremos el que interno 107 tiene configurado como Jefe-Secrearia al interno 108

Con lo cual el interno 108 puede llamar a la aplicación (300) para desactivar y activar el Jefe-Secretaria

3.3.7.8.2.2. Aplicación IVR Modo Backup Esta aplicación permite derivar todos los números de acceso de la central hacia un preatendedor creado para el modo Backup

Para crear la aplicación, en las sección de Configuración >Mis aplicaciones damos de alta la aplicación «Set Ivr Backup Applicaction», y completar Nombre y Descripción

Luego aparecerá en la lista de Mis aplicaciones. Se deben cargar los audios para que la aplicación pueda funcionar, se pueden personalizar los audios haciendo clic en el ícono y cargar acorde a la función, o hacer clic en para cargar los audios por default de la aplicación.

Al dar de alta los audios, aparecerán en la lista y la aplicación estará lista para funcionar.

Para poder llamar a la aplicación, es necesario crear una extensión tipo aplicación y asociar la misma

Procedimiento

Para ejecutar la aplicación, en el ejemplo de configuración se asoció la aplicación al interno 301.

Una vez creado el preatendedor, se identifica este preatendedor con el código (para el ejemplo siguiente el código es el 7)

Cuando se llama al interno 301, se solicita el código del preatendedor (en este caso 7) y se brindan las opciones de activar o desactivar el modo backup. La primera vez que se activa, se derivan todos los números de acceso por el término de 24 hs. Si antes de las 24 hs se intenta activar nuevamente, se indica que esta activo pero se respeta el primer plazo de vencimiento de la aplicación.

Una vez terminado el tiempo de ejecución o desactivada la aplicación, los números de accesos siguen operando en los modos horarios de los preatendedores correspondientes.

3.3.7.8.2.3. Aplicación Remote Dialing Code Dentro de las aplicaciones que trae la central por default, encontramos la aplicación Remote Dialing code. Esta aplicación permite tomar línea y realizar llamadas a través del Preatendedor (IVR). Esta operación se conoce en telefonía como la función DISA.

Para utilizar esta aplicación, se programa una opción oculta en el Preatendedor. Para el siguiente ejemplo vemos que la opción 9 es en modo Aplicación y tiene seleccionada Remote Dialing code. Esta opción no se reproduce en el audio del Preatendedor.

En el usuario, se debe configurar el código de discado Remoto

Al llamar al número de acceso del preatendedor y presionar la opción oculta, la central solicita autenticar al usuario con su código de discado remoto. La central identifica al usuario y los permisos del usuario para realizar llamadas acorde a lo que tiene autorizado.

Una vez identificado el usuario, la central brinda tono de discado pudiendo el usuario realizar llamadas como si estuviera desde su interno, es decir, poder llamar al voicemail (*¨33), a otro interno, o realizar llamada salientes utilizando los troncales de la central acorde a los permisos.

3.3.7.8.3. Interfaces de Telefonía La versión 4.0.1 de la Denwa no soporta Placas de Telefonía. Esta pestaña fue heredada de Denwa UC&C 4.0.1 3.3.1, motivo por el cual continúa habilitada.

3.3.7.9. Mantenimiento

En esta página se pueden observar dos sectores: el de Estado y el de Configuración.

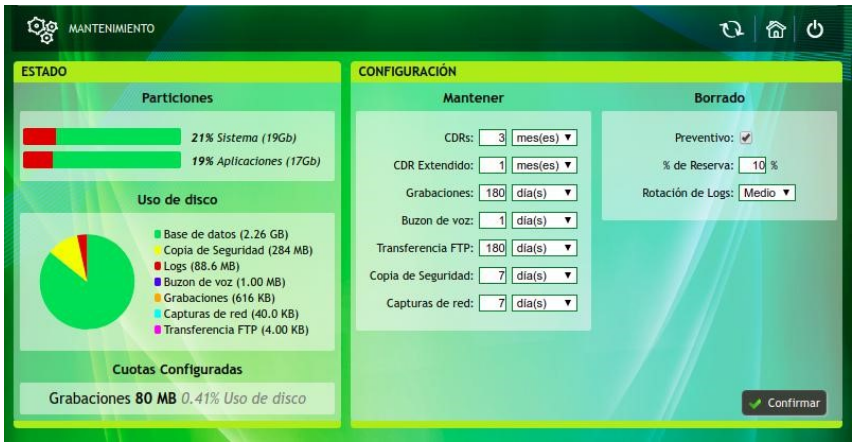

Figura 3.147: Mantenimiento

El izquierdo corresponde al Estado. En él se visualiza información acerca del uso de las particiones del sistema, del disco y de las cuotas configuradas.

- **Particiones:** Porcentaje del uso de las particiones del sistema.
- **Uso de Disco:** esta sección se exhibe un gráfico de torta que muestra de manera rápida y simple de comprender el uso del disco. Además, se presenta un listado con mayor detalle:
  - **Base de Datos**: Refiere al espacio que ocupa en disco la información de la base de datos.
  - **Copia de Seguridad:** Permite comprobar el espacio que ha sido utilizado por el respaldo de los datos.
  - **Logs:** Refiere al espacio que ocupa en disco los logs de la plataforma.
  - **Buzón de voz:** Permite verificar qué espacio ocupan en el disco los mensajes de voz.
  - **Grabaciones:** Refiere al espacio que ocupan las grabaciones telefónicas.
  - **Capturas de red:** Hace referencia al espacio que ocupan las capturas de paquetes de la red.
  - **Transferencia FTP:** Hace referencia al directorio donde se almacenan los archivos pendientes de transferir al servidor FTP externo.

Gráfico de uso de disco

El gráfico sumariza la información a través de todos los dispositivos de almacenamiento disponibles, sin discriminar por partición o disco

- **Cuotas Configuradas:** es la sumatoria de cuotas de grabaciones configurada para Usuarios, Grupos, Trunks, etc. Se contrasta también la información con el espacio disponible.

El sector de la derecha corresponde a las Configuraciones y está dividido por dos secciones: Mantener: En esta sección se configura el tiempo por el cual se almacenarán los datos.

- **CDR's:** Refiere a los registros de llamadas.
- **CDR's Extendido:** Refiere a los registros extendidos de llamadas.
- **Grabaciones:** Hace referencia a las grabaciones de las llamadas.

- **Buzón de voz:** Alude a los mensajes almacenados en el buzón de voz.
- **Transferencia de FTP:** hace referencia al directorio donde se almacenan los archivos pendientes de transferir al FTP externo.
- **Copia de Seguridad:** Corresponde a los archivos de respaldo de configuraciones.
- **Capturas de red:** archivos de capturas (.cap).
- **Borrado:** Esta sección permite habilitar el borrado automático de archivos cuando el porcentaje de uso de disco en alguna de las particiones supere el porcentaje de reserva de disco configurado.
- **Preventivo:** habilitar borrado preventivo.
- **% de Reserva:** porcentaje que debe permanecer libre.
- **Rotación de Logs:** modo de borrado de archivos de logs, se corresponde con la duración de los logs en el sistema, y tamaño aceptado:
  - **Fuerte:** conserva los últimos 2 días de logs al encontrarse en el umbral correspondiente al % de Reserva.
  - **Medio:** conserva los últimos 4 días de logs al encontrarse en el umbral correspondiente al % de Reserva.
  - **Suave:** conserva los últimos 6 días de logs al encontrarse en el umbral correspondiente al % de Reserva.

En caso que la ocupación de Discos llegue al 70 %, Denwa UC envía una (1) alerta por día a los correos electrónicos de los Administradores. En caso que el uso de disco supere el 90 %, envía uno (1) cada hora.

La notificación que llega por mail contiene en porcentaje el uso total del Disco, y de las particiones junto con la licencia de la central de donde se emite la Alerta.

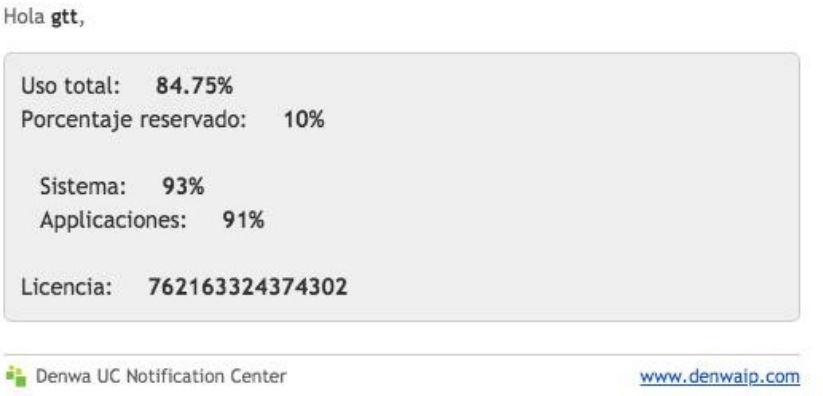

Figura 3.148: Correo de alerta por ocupación de particiones

3.3.7.10. Soporte

Desde este menú, se puede requerir soporte remoto y gestionar las actualizaciones del PBX Denwa.

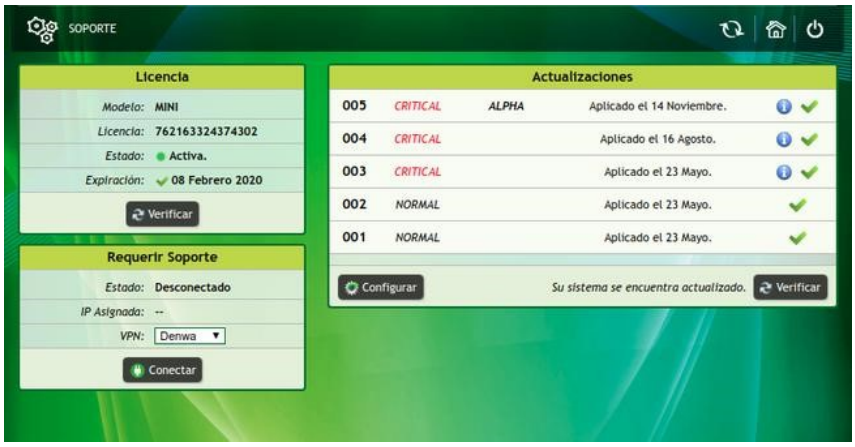

Figura 3.149: Soporte

3.3.7.10.1. Licencia es esta sección se puede visualizar nuestra licencia y el estado del soporte, junto con la fecha de expiración.

3.3.7.10.2. Requerir Soporte esta opción permite conectar la Denwa UC&C 4.0.1 a la red segura del soporte técnico para la solución de problemas, toma de capturas o configuración de la central. El campo Estado nos muestra si se encuentra conectado a soporte o no, y el campo Dirección IP, muestra la IP entregada por la red segura de soporte de Denwa.

En caso de requerir un soporte de primer nivel, se puede optar por conectar la central a soporte del Distribuidor, donde se brinda una pronta respuesta a las consultas más frecuentes, generalmente asociadas con configuraciones de la central o de la red asociada a ella. A continuación un listado de las VPNs disponibles y su relación con los distintos distribuidores:

- **Denwa**: VPN por defecto, entrega direcciones IP en la red 192.168.155.0/24
- **VPN 001**: VPN para Basilvox (Brasil) y Telssa (Nicaragua), entrega direcciones IP en la red 192.168.202.0/24
- **VPN 002**: VPN para Calltech (Colombia), entrega direcciones IP en la red 192.168.206.0/24
- **VPN 003**: VPN para Portenntum (México), entrega direcciones IP en la red 192.168.207.0/24
- **VPN 004**: VPN para Provetel (Argentina), entrega direcciones IP en la red 192.168.204.0/24
- **VPN 005**: VPN para Sistek (Chile) y ProNet (Panamá), entrega direcciones IP en la red 192.168.208.0/24
- **VPN 006**: VPN para Sumtec (Perú), entrega direcciones IP en la red 192.168.205.0/24
- **VPN 007**: VPN para Telered (Ecuador), entrega direcciones IP en la red 192.168.203.0/24
- **VPN 008**: VPN para SignalSoft (Chile) y Ericnet (Argentina), entrega direcciones IP en la red 192.168.197.0/24
- **VPN 009**: VPN para Retracom (Bolivia), entrega direcciones IP en la red 192.168.198.0/24
- **VPN 010**: VPN para Technology Bureau (Argentina), entrega direcciones IP en la red 192.168.199.0/24

Acceso a soporte

El hecho de que el equipo pueda conectarse a cualquiera de las VPNs de Soporte no implica que el mismo cuente con un contrato vigente de atención ya sea por parte de los Integradores, Distribuidores o Fábrica.

3.3.7.10.3. Actualizaciones de la PBX permite habilitar la opción de Aplicar actualizaciones automáticamente, estas se realizan al ser las 07:00 UTC. Al deshabilitar esta opción el administrador puede realizar las actualizaciones de forma manual cuando lo requiera.

También se muestra el código de la última actualización aplicada en Denwa UC&C 4.0.1 .

3.3.7.11. Control de Fraude

En esta sección se analiza uno de los aspectos mas importantes con respecto a la seguridad del Centro de Comunicaciones Unificadas Denwa.

El control de fraude sirve para prevenir el mal uso de la central dado por el abuso de llamadas desde una extensión.

Con el control de fraude se pueden establecer límites de acuerdo al uso de los internos, en los cuales los posibles abusos sean limitados automáticamente; a su vez se evitan ataques de DoS (*«Denial of Service»*, en español «Denegación de Servicio») sobre los troncales digitales, al rechazar automáticamente las llamadas entrantes de ciertos prefijos.

Todo esto se establece a través de reglas.

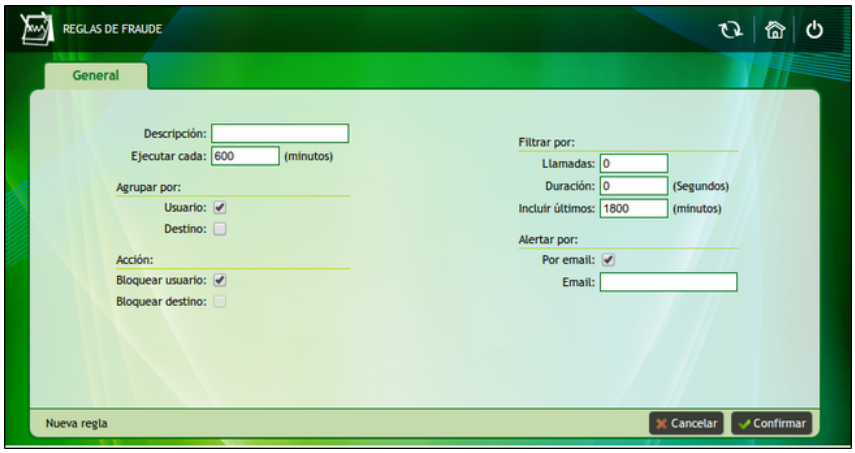

Figura 3.150: Control de Fraude, nueva regla

3.3.7.11.1. Nueva Regla Los parámetros para la creación de las nuevas reglas se detallan a continuación.

- Descripción: nombre que se asigna a la regla. Por ejemplo, «Control 1».
- Ejecutar cada: tiempo en el cual se evalúa si alguna de las reglas estipuladas se cumplen.
- Agrupar por
  - Usuario: al crear las reglas que bloquearán las llamadas, se pueden aplicar a los internos de los usuarios.
  - Destino: al crear las reglas que bloquearán las llamadas, se pueden aplicar sobre los destinos.
- Acción
  - Bloquear usuario: si se cumple la regla, se ejecuta el control de fraude pasando al usuario en modo Suspendido (puede recibir pero no efectuar llamadas).
  - Bloquear destino: si se cumple la regla, se ejecuta el control de fraude bloqueando las llamadas a dichos destinos.
- Filtrar por
  - Llamadas: cantidad de llamadas a realizarse en el intervalo de tiempo monitoreado.

- Duración: duración de las llamadas en el intervalo de tiempo monitoreado.
- Incluir últimos: si bien se determina cada cuanto tiempo se desean evaluar las reglas del control, este parámetro especifica cuanto tiempo atrás se tiene en cuenta.

- Alertar
  - Por email: se activa o desactiva la función de notificación vía email
  - Email: dirección de email al cual llegan las notificaciones cada vez que el control de fraude ejecuta un bloqueo.

Bastará con pulsar sobre el botón «✔ Confirmar» para guardar la nueva regla, o sobre «✖ Cancelar» para desestimar la configuración hecha y volver a la pantalla anterior.

Condiciones de ejecución

Para que se ejecute un bloqueo por control de fraude ambas reglas, por llamadas y por duración, se deben cumplir al mismo tiempo, es decir que se supere la cantidad de llamadas en el tiempo configurado y que la suma del tiempo de duración de estas supere el tiempo máximo de duración.

3.3.7.11.2. Reglas de Fraude En esta sección se observan las reglas creadas, y el momento en que se ejecutarán nuevamente dichas reglas.

Figura 3.151: Control de Fraude, reglas de fraude creadas

Estas reglas se muestran en forma de lista. En la columna Acción de esta pestaña se brinda la posibilidad de editar la regla al realizar un clic en «✎», o eliminarla con un clic en el icono «✖».

Cuando se desea editar la regla y se presiona sobre el icono correspondiente emerge una nueva ventana con dos pestañas. La primera de estas es la configuración general de la regla (ver Nueva Regla en la página 136) y la segunda presenta los prefijos bloqueados (ver Prefijos Entrantes Bloqueados en la página 138).

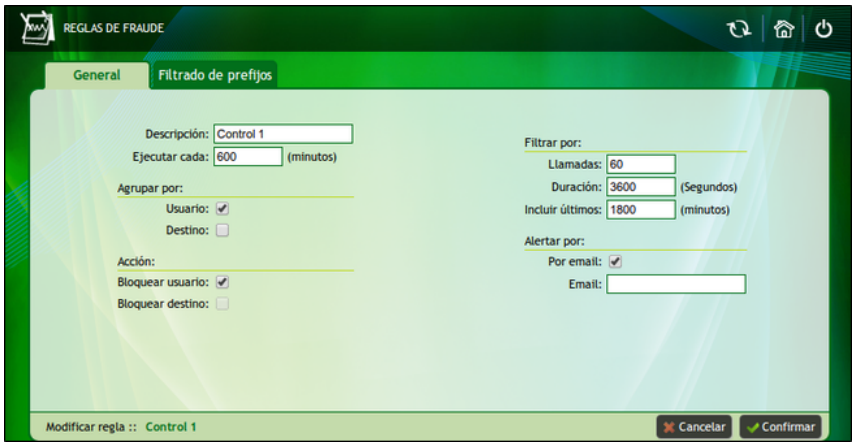

Figura 3.152: Control de Fraude, edición de la regla de fraude previamente creada

Para terminar se debe hacer clic sobre «✔ Confirmar» y los cambios son guardados.

3.3.7.11.3. Prefijos Entrantes Bloqueados Otra característica de la Denwa es el bloqueo de prefijos de las llamadas provenientes de direcciones especificas. Esto es útil para evitar un ataque por DDoS y en caso de troncales hacia el Denwa UC&C 4.0.1 , evitar que se emitan llamadas provenientes de esos troncales.

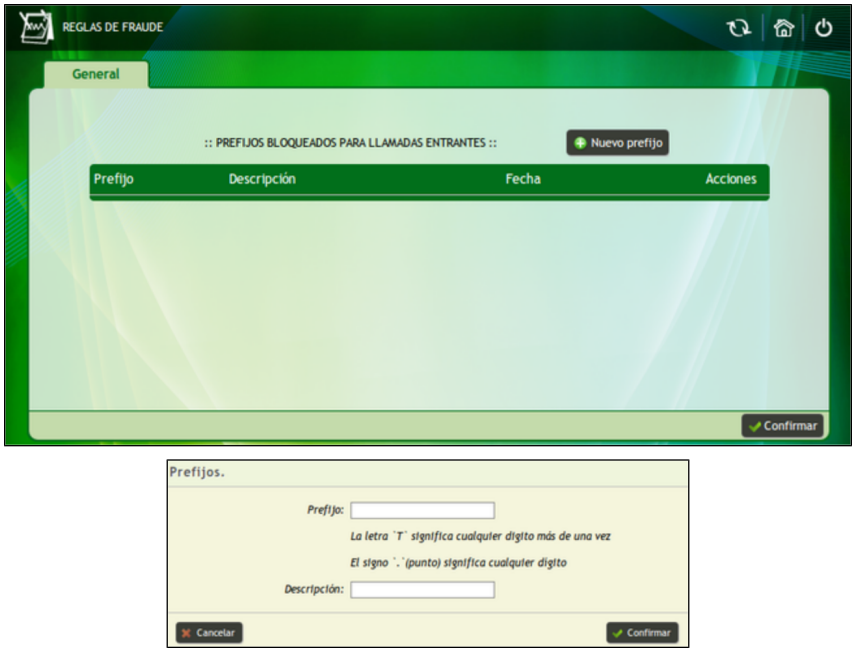

Figura 3.153: Control de Fraude, prefijos bloqueados para llamadas entrantes

En esta sección se observan las reglas de bloqueo de prefijos entrantes, y se permite crear nuevas reglas con un clic en .

- Prefijo: se puede incorporar los primeros dígitos a bloquear, seguido de cualquiera de los siguientes caracteres:
  - «.» indica un (1) único dígito, puede ser repetido la cantidad de veces que sea necesario
  - «T» implica una cantidad indeterminada de dígitos
- Descripción: se agrega una referencia (nomenclatura) para esta regla.

En la imagen siguiente se visualizan dos ejemplos de bloqueo de prefijos entrantes.

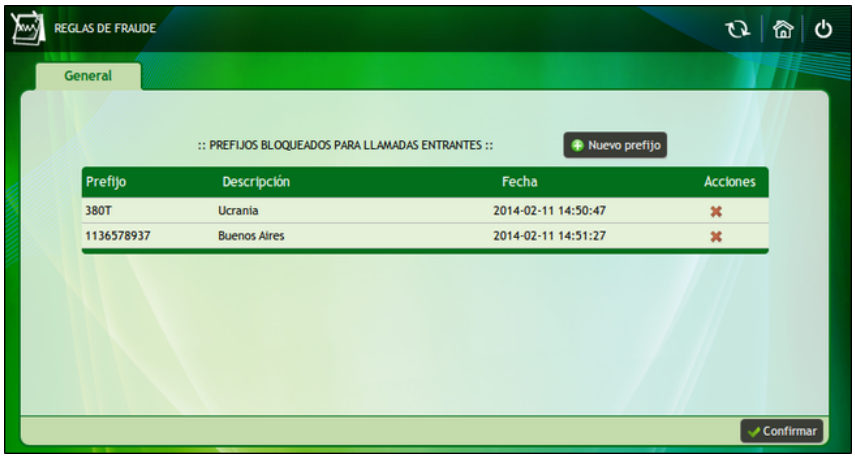

Figura 3.154: Control de Fraude, ejemplo de prefijos entrantes bloqueados

En el primer ítem, se bloquea cualquier número que empieza con 380, en el segundo ítem se bloquean las llamadas provenientes del número 1136578937.

Para eliminar alguna de las reglas creadas se debe presionar en «✖».

3.3.7.11.4. Destinos Bloqueados Para ver y crear bloqueo de llamados salientes se realiza desde Destinos Bloqueados

Los destinos que cumplen con el control de fraude y son bloqueados se pueden observar en esta sección. Además se pueden agregar bloqueos realizando un clic en «⊕ Nuevo prefijo».

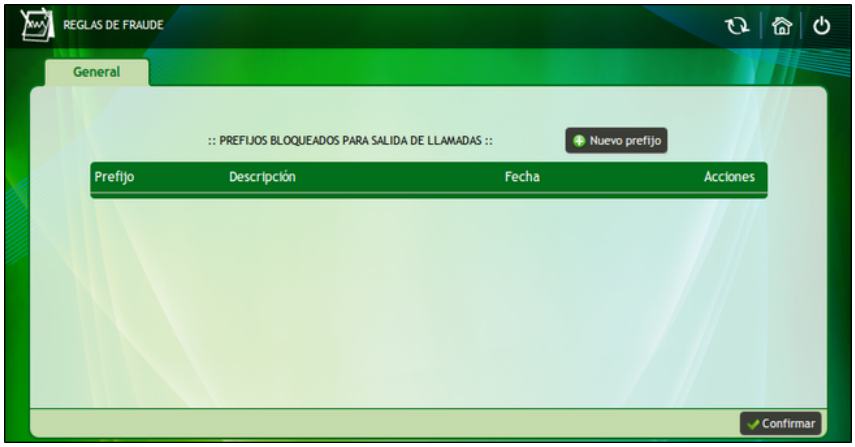

Figura 3.155: Control de Fraude, prefijos bloqueados para llamados salientes

- Prefijo: se puede incorporar los primeros dígitos a bloquear, seguido de T (que significa que cualquier dígito o dígitos).

- Descripción: se agrega una referencia (nomenclatura) para esta regla.

A continuación se muestran dos ejemplos.

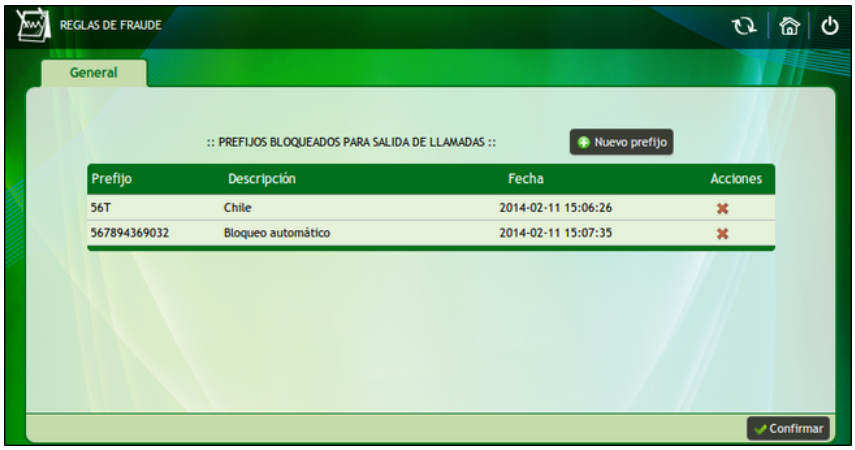

Figura 3.156: Control de Fraude, ejemplo de prefijos bloqueados para llamados salientes

En el primer ítem, se bloquean todas las llamadas salientes hacia Chile, mientras que en el segundo ítem se bloquea las llamadas salientes al número 567896369032.

Para eliminar alguna de las reglas creadas se debe presionar en .

3.3.7.12. Denwa Store

Con la opción Denwa Store se permite la incorporación de nuevas aplicaciones, llamadas módulos para PBX Denwa. Dichos módulos se desarrollan según las necesidades del usuario. Inicialmente se debe disponer de un módulo, para luego instalarlo y gozar de sus ventajas.

Cuenta con dos pestañas: «Instalados» y «Todos»

3.3.7.12.1. Instalados En esta pestaña se observan los módulos instalados para nuestra PBX Denwa. En este caso se ha instalado el módulo Contact Center.

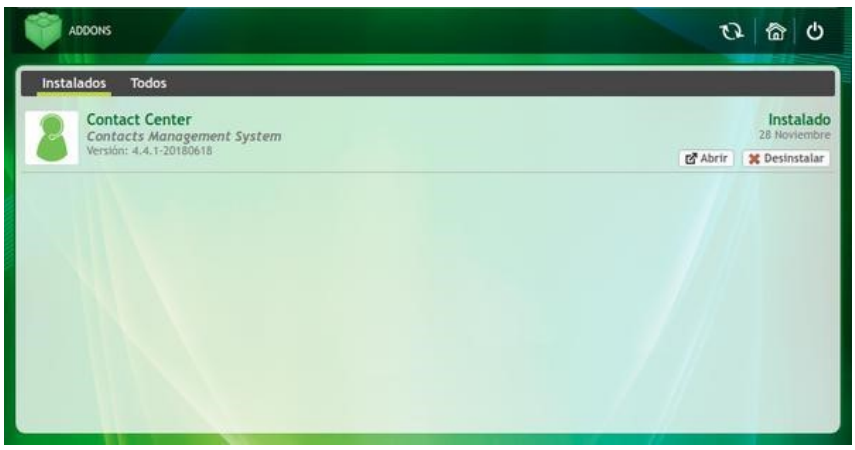

Figura 3.157: Denwa Store, módulos instalados

Figura 3.158: Denwa Store, todos los módulos

3.3.7.12.2. Todos En el listado de la figura anterior se observa la información en dos columnas.

En la primera, se visualizan los módulos disponibles, con una breve descripción y versión correspondiente. Dentro de los módulos existentes se encuentran los siguientes:

- **Control Center**: es una utilidad que permite realizar monitoreo, asignación de costos y facturación a las llamadas en una PBX Denwa o en un grupo de ellas.
- **Contact Center**: este módulo esta orientado como herramienta para los Call Centers. Generalmente, se utiliza para campañas de llamadas entrantes y salientes.
- **H323**: concede la posibilidad de configurar un proveedor utilizando el protocolo H323.
- **Alta Disponibilidad**: esta aplicación permite que una PBX Denwa funcione como respaldo de otra PBX Denwa; es por ello que los datos se actualizan entre ellas. Es necesario que las PBX Denwa participantes sean del mismo modelo. Al instalar este módulo en las centrales, se debe configurar una en modo maestro y la otra en modo esclavo.
- **Hotels**: este módulo facilita los tramites de administración hotelera. Debido a que asigna a cada habitación una extensión, esto permite generar un informe rápido del estado de las habitaciones y un reporte detallado de cada una de ellas. El detalle de las llamadas se entrega a la central mediante Telnet, lo que posibilita que sea en tiempo real. Es decir, que se permite la interacción con el sistema de facturación o PMS (Property Management System) de manera online; lo cual aporta dinamismo.
- **Denwa Audits**: es una funcionalidad que permite el monitoreo de Denwa UC&C 4.0.1 , se puede obtener información correspondiente a ultimas actividades y estadísticas. Las últimas actividades se muestran en tres columnas, en la primera se observa la fecha y hora en la cual tuvo lugar la actividad, en la segunda se verifica el usuario que realizó la misma y en la tercera columna se visualiza en cual de las opciones del menú que brinda Denwa UC&C 4.0.1 se ejecuta alguna acción. Las estadísticas brindan un resumen de las actividades del día, de los últimos diez días y del último mes. Este módulo necesita de una central actualizada a la versión 84.
- **UPS Management**: permite monitorear y administrar UPS. La principal funcionalidad de este módulo radica en la posibilidad de ejecuta diversas acciones según una determinada condición. Se pueden monitorear varias UPS con este módulo y para obtener información sobre el estado de las mismas, cada 30 segundos realiza un chequeo. El cual se realiza mediante SNMP, haciendo ping y las consultas pertinentes para obtener información sobre el estado del voltaje, cortes de luz, capacidad de la batería, tiempo restante estimado de la batería, entre otros.
- **LDAP**: permite la autenticación de operadores con sistema LDAP (Active Directory) permitiendo el acceso con todos los permisos habilitados.

Instalación de módulos

La instalación de módulos únicamente es posible en un equipo cuya licencia se encuentre con un plan de soporte vigente para con Denwa Technology Corp. . Consulte a su implementador por el estado y nivel de soporte de su licencia.

En la segunda columna, se permite corroborar el estado de instalación con sus respectivas características:

- No instalado, tamaño del módulo y opción de instalar el mismo.
- Instalado y no actualizado, fecha de última instalación y las opciones abrir, actualizar y desinstalar.
- Instalado, fecha de instalación y las opciones abrir y desinstalar.

También se puede desde esta pestaña realizar la actualización de los módulos, desde el botón «✔ Actualizar».

Al hacer clic en Actualizar, emerge una nueva ventana, en ella se debe hacer clic en el botón «✔ Actualizar» para continuar con el proceso, o bien «✖ Cancelar» para cancelarlo.

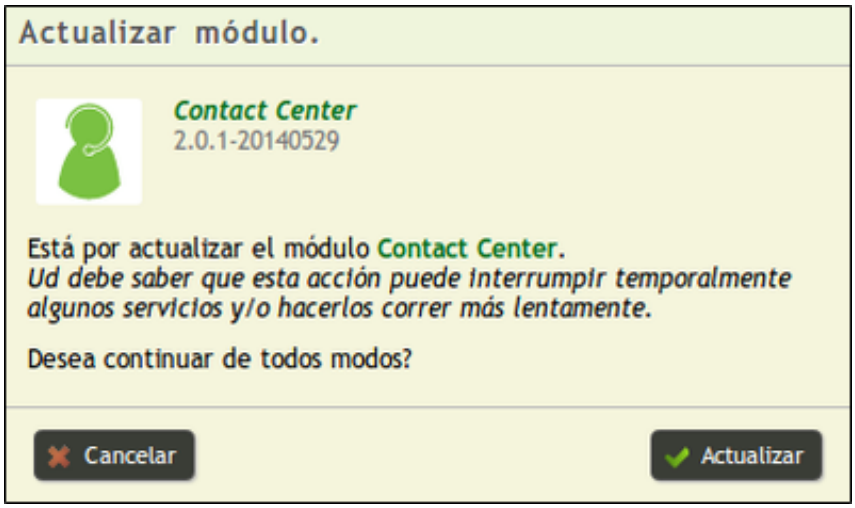

Figura 3.159: Denwa Store, ventana de actualización de un módulo

Figura 3.160: Denwa Store, módulo actualizándose

Actualización de módulos

Dado que la liberación de un módulo puede obedecer tanto al agregar nuevas funcionalidades, así como a la corrección de errores, el proceso automático que se ejecuta internamente durante la actualización consta de cinco pasos:

1. Descarga del paquete de actualización
2. Creación de una copia de respaldo de la información contenida en el módulo a actualizar
3. Desinstalación de la versión actual del módulo
4. Instalación de la versión actualizada del módulo
5. Restauración de la información contenida en la copia de respaldo hecha en el paso 2

3.3.7.13. Licencias

En esta interfaz se puede gestionar la licencia del Web Phone del Desktop que brinda la Denwa UC de manera gratuita y realizar la petición de secciones SBC Premium Simultáneas.

La primera de las licencias se carga sólo una vez y sirve para teléfono del Desktop de todos los usuarios asociados a la Denwa UC en cuestión; en tanto que la segunda indica la cantidad de secciones SBC habilitadas, la Denwa UC Premium incluye 12 secciones incorporadas, pero es posible agregar paquetes de 5 secciones.

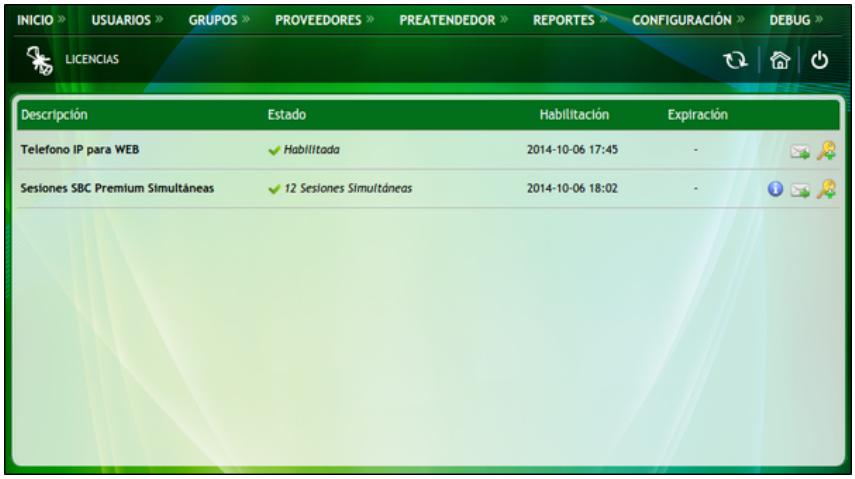

Figura 3.161: Licencias disponibles

En la imagen anterior se muestra la información contenida en columnas. Entre las cuales se encuentran descripción, estado, habilitación y expiración (muestran las fechas respectivas).

- **Descripción**: Breve descripción de la aplicación.
- **Estado**: Permite observar si la licencia esta habilitada y la cantidad de secciones disponibles.
- **Habilitación**: Muestra la fecha en la cuál se habilita la licencia.
- **Expiración**: Actualmente no tiene función válida, ya que las licencias de «Teléfono IP para WEB» la otorga gratuitamente Denwa Technology Corp. , en tanto que las adicionales para las sesiones SBC del equipo Denwa Premium están asociadas al número de serie del equipo.

- **Acción**: se encuentran tres opciones:
  - : este botón sirve para solicitar licencia. Para licencias web el proceso implica el envío de un email al staff de Denwa, luego se recibe la respuesta con el archivo correspondiente. Para secciones de SBC es necesario cargar el código del paquete adquirido en la siguiente ventana.

    Las licencias solicitadas no son transferibles. Eso significa que una vez que Usted requiere Licencias de SBC, éstas se activan sólo para este dispositivo y no será posible utilizarlas en otro. Una vez que las licencias se hayan activado (mediante este requerimiento) no es posible revertir el proceso. El proceso de activación puede llevar alrededor de 3-5 días laborales.
  - : al realizar clic en este icono se debe cargar el archivo que se obtuvo de la solicitud de licencia
  - : se muestran las licencias SBC que actualmente se encuentran cargadas en la Denwa UC Premium.

Consideraciones para la solicitud de la licencia

1. El correo de respuesta con la información de la licencia se recibe en la dirección de correo electrónico declarado en **Configuración >General >Pestaña: Básica**
2. Es necesario contar con conexión a la red de Internet
3. Se debe considerar la configuración de la IP estática

3.3.8. Debug

En esta sección se presenta una herramienta muy poderosa que es capaz de mostrar en detalle los paquetes que participan en cada comunicación. Lo cual permite encontrar corte o fallas importantes que afecten de alguna manera al servicio.

3.3.8.1. Monitor de llamadas

En este apartado se presentan los eventos en tiempo real que ocurren la central. La ventana que se observa es la de la siguiente imagen.

Figura 3.162: Debug, monitor de llamadas

3.3.8.1.1. Total de Llamadas en Línea Se exhibe en esta sección tanto la cantidad de llamadas internas, externas y salientes en tiempo real, como así también la sumatoria de las mismas.

3.3.8.1.2. Filtros Se presenta un variedad de condiciones; al aplicarlas se permiten visualizar sólo aquellas que cumplan con las mismas. Por defecto, muestra todas las llamadas de todos los proveedores.

- **Tipo**: se tiene la posibilidad de observar todas las llamadas, utilizando la opción Todos; también se pueden ver solamente las internas, externas o salientes.
- **Origen**: admite realizar el filtrado según sea el número que inicia la llamada.
- **Destino**: se permite seleccionar el número que recibe la llamada como patrón de filtrado.
- **Proveedor**: en este caso se brinda la posibilidad de escoger un proveedor para ver sus llamadas en línea.

3.3.8.1.3. Llamadas en Línea Se exhibe sólo aquellas llamadas que están ocurriendo en tiempo real, bajo las condiciones de filtrado previamente seleccionadas.

- **Tipo**: se brinda esta información mediante el uso de iconos:
  - ←: llamada entrante.
  - ↻: llamada entre internos.
  - →: llamada saliente.
- **Origen**: muestra el número de quien realiza la llamada.
- **Destino**: permite ver cual es número receptor de la llamada en cuestión.
- **Proveedor**: posibilita la opción de visualizar por que proveedor de la central se cursa la llamada, en caso de ser necesario.
- **Duración**: revela la duración de la llamada, lo cual no implica que la misma haya sido atendida; debido a que se incluye en este lapso el tiempo de ring.

3.3.8.2. Monitor de Señalización

En esta sección se permite visualizar los eventos que ocurren dentro del motor de telefonía de Denwa UC&C 4.0.1 . Cuenta con múltiples botones y filtros.

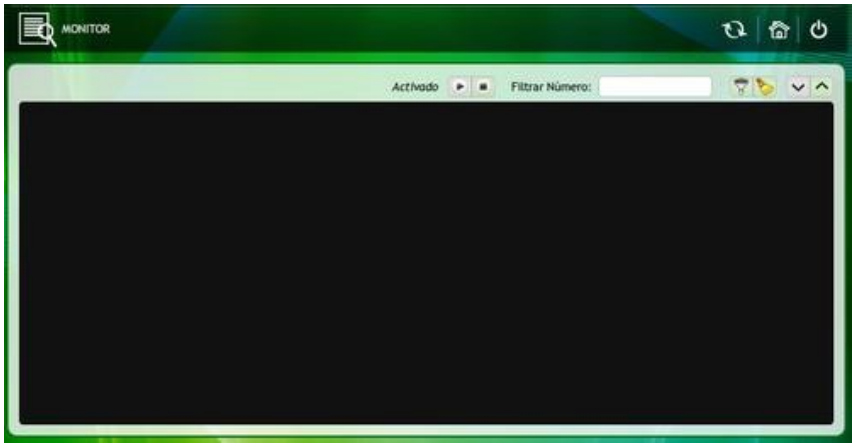

Figura 3.163: Debug, monitor de señalización

- ⏵⏹: para comenzar con el monitoreo se debe hacer clic en el botón cuyo icono es una triángulo («*Play*») y para detenerlo sólo se necesita un clic en el botón que contiene un cudrado («*Stop*»).

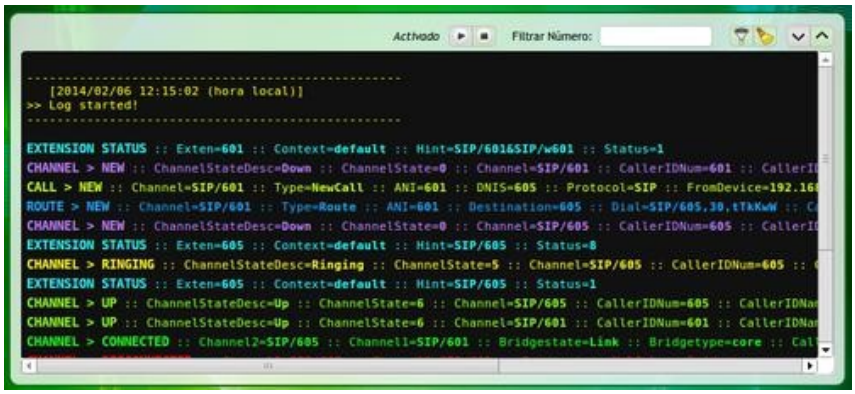

Figura 3.164: Debug, monitor de señalización: resultado de la puesta en marcha del monitor

- **Filtrar número**: sirve para realizar el monitoreo de llamadas de un número en particular.
- ▼: se utiliza para realizar un filtrado puntual. Al realizar clic sobre este icono se despliega una lista, la cual contiene el color con el cual se visualizaran los mensajes y el tipo de mensaje. Finalmente, se encuentran las opciones del tilde y la cruz; que permiten o no captar esos mensajes durante el establecimiento y cierre de la llamada.

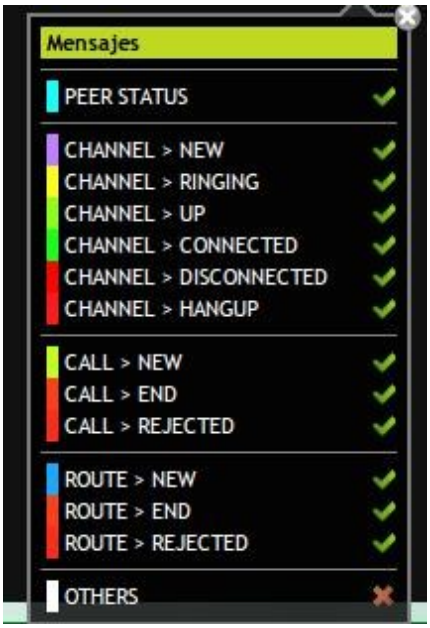

Figura 3.165: Debug, monitor de señalización: filtros disponibles

  - **Peer Status**: brinda información del registro periódico de la s extensiones en Denwa UC&C 4.0.1 .
  - **Channel - New**: se establece un canal para la comunicación a través del protocolo especificado.
  - **Channel - Ringing**: tono de llamado en el destino.
  - **Channel - Up**: se establece el vínculo entre quien origina la llamada y Denwa UC&C 4.0.1 .
  - **Channel - Connected**: en este caso se establece el enlace completo en dos tramos. El primero, abarca desde quien origina la llamada hasta Denwa UC&C 4.0.1 . En cambio, el segundo involucra desde Denwa UC&C 4.0.1 hasta el extremo receptor de la llamada.
  - **Channel - Disconnected**: indica el fin de la conexión.

- **Channel - Hangup**: se termina la llamada y se libera el canal.
- **Call - New**: señala que Denwa UC&C 4.0.1 , internamente, comienza a manipular la llamada.
- **Call - End**: pone en evidencia que la PBX finaliza la llamada, como proceso interno.
- **Call - Rejected**: este mensaje permite observar que la llamada no llega a destino nunca. Por lo que sólo utiliza el vínculo entre el origen y Denwa UC&C 4.0.1 .
- **Route - New**: establece en cada llamada el segundo vínculo.
- **Route - End**: al finalizar la llamada, finaliza el segundo vínculo.
- **Route - Rejected**: en este caso sólo se utiliza uno de los vínculos.
- **Others**: muestra aún más detalles de los procesos internos que maneja la PBX para establecer y cerrar la llamada.

- : al realizar clic sobre este icono se abre la ventana de la siguiente figura. La cual brinda la posibilidad de mostrar sólo los últimos 100, 500, 1000 o 2000 mensajes, ya que estas opciones son las que presenta el menú desplegable. Además, se puede eliminar la totalidad de los mensajes, para lo cual es necesario hacer clic en «Borrar todos los mensajes ahora»

- :estos botones sirven para maximizar y minimizar la pantalla del monitor, respectivamente.

3.3.8.3. Herramientas de Red

En esta sección se encuetran las herramientas para resolución de problemas en redes (troubleshooting), permitiendo así un rápido y mejor análisis de la red.

Las herramientas disponibles son: PING, TRACEROUTE, ARP, ETH-TOOL, NSLOOKUP y My-Traceroute.

3.3.8.3.1. Ping Permite enviar una cierta cantidad de consultas ICMP hacia cierto destino, esto sirve para determinar si la DenwaUC puede alcanzar a este destino.

Los resultados de esta función permiten determinar el porcentaje de paquetes perdidos, cual es el tiempo promedio entre la consulta y la respuesta, y la variación del tiempo entre consulta y respuesta.

3.3.8.3.2. Traceroute Permite enviar consultas ICMP con TTL incremental (comenzado en 1), para determinar la cantidad de saltos o host por cuales una consulta debe atravesar para llegar hasta el destino.

Los resultados de esta función, permite determinar si el tráfico enviado hasta el destino es enviado por la ruta previamente determinada

3.3.8.3.3. ARP La herramienta de escaneo ARP es un escáner de paquetes ARP muy rápido que muestra todos los dispositivos activos en la subred. Dado que ARP no es enrutable, este tipo de escaneo solo funciona en la LAN local (subred local o segmento de red).

La herramienta de escaneo ARP muestra todos los dispositivos activos incluso si tienen firewalls. Los dispositivos no pueden esconderse de los paquetes ARP como pueden esconderse de Ping. Puede ser utilizada con los siguientes parámetros:

- **-a**: muestra la información obtenida a través de todas las interfaces de red
- **-i**: muestra la información obtenida a través de una interfaz en particular
- **-n**: muestra la información en un formato numérico

3.3.8.3.4. NSLOOKUP El uso principal de nslookup es identificar problemas relacionados con DNS.

3.3.8.3.5. ETH-TOOL Muestra la información de la configuración de las interfaces de red. Pudiendo ser utilizado:

- **sin parámetros**: muestra las propiedades de la tarjeta Ethernet, como velocidad, activación, dúplex y el estado de detección del enlace
- **-i**: muestra la versión del controlador, del firmware y los detalles del bus
- **-S**: muestra estadísticas de transmisión y recepción

3.3.8.3.6. My-TraceRoute Esta herramienta es una mezcla de dos (2) antes mencionadas: Ping y TraceRoute. Utiliza:

- chechbox para cada uno de los posibles campos a mostrar en la salida (-o LDRSNBAWVGJMXI), según el siguiente listado:
  - L Loss ratio
  - D Dropped packets
  - R Received packets
  - S Sent Packets
  - N Newest RTT(ms)
  - B Min/Best RTT(ms)
  - A Average RTT(ms)
  - W Max/Worst RTT(ms)
  - V Standard Deviation
  - G Geometric Mean
  - J Current Jitter
  - M Jitter Mean/Avg.
  - X Worst Jitter
  - I Interarrival Jitter
- campo de texto para las IP o nombres de dominio
- checkbox para que se muestre solamente la IP del salto (-n)
- checkbox para que se muestre la IP y el nombre de dominio del salto (-b)
- campo numérico entero para la cantidad paquetes a enviar (-c)
- campo numérico entero para el máximo de saltos (-m)
- campo numérico entero para el intervalo de tiempo entre cada envío de paquetes (-i)
- campo numérico entero para el puerto de destino a consultar (-P)
- campo numérico entero para el puerto de origen (-L)
- campo numérico entero para el tamaño de los paquetes (-s)
- checkbox para seleccionar si se desea que el reporte sea exportable (-r) y habilitación de campo de texto para colocar el nombre del archivo a exportar. En caso de seleccionar esta opción, los reportes generados se listarán en la tabla ubicada en la parte inferior de la pantalla

3.3.8.4. Monitor Líneas Digitales

La versión 4.0.1 de la Denwa no soporta Placas de Telefonía. Esta pestaña fue heredada de Denwa UC&C 4.0.1 3.3.1, es por ese motivo sigue habilitada.

3.3.8.5. Captura de paquetes

Esta opción permite capturar las tramas de la red mediante el uso de un sniffer. Esta herramienta brinda información muy detallada y ordenada. Cuenta contres (3) recuadros que se describen a continuación:

1. **SNIFFER: : Nueva captura**: aquí se deben seleccionar las condiciones sobre las cuales se realiza la captura.
    - **Nombre Cap**: aquí se indica el nombre del archivo a generar.
    - **Interfaz**: refiere a la interfaz sobre la cual se quiere realizar la captura de paquetes.
    - **Mín Tamaño Paq**: asigna el tamaño mínimo de los paquetes que se quieren capturar. Se recomienda utilizar el valor por defecto (1500).
    - **Duración Máxima**: en caso que la captura no se finalice en forma manual, una vez que se cumple este lapso temporal finaliza automáticamente.
    - **Servicios**: se pueden elegir todos (ALL) o seleccionar sólo aquellos protocolos que se desean capturar.
    - ▶■: con estos botones se comienza y finaliza la captura, respectivamente.
2. **Capturas**: en esta sección se pueden visualizar las capturas realizadas.
    - **Nombre Cap**: refiere al nombre con el cual se guardo la captura.
    - **Servicios capturados**: permite observar cuales son los servicios que se capturaron.
    - **Iface**: esta columna muestra las interfaces sobre las cuales se ejecuto la captura.
    - **Fecha Hora**: indica los datos al momento de comienzo de la captura.
    - **Tamaño**: exhibe el tamaño del archivo (KB).
    - **Acción**: en esta columna se presentan tres opciones.
        - ✂: con este icono se permite activar la opción de filtro avanzado, que aparece en la parte inferior.
        - 📥: se posibilita utilizar este icono para exportar el archivo, para luego abrirlo mediante el uso del sniffer.
        - ✖: esta alternativa proporciona la opción de eliminar la captura realizada.
3. **Filtro Avanzado**: permite simplificar el análisis, ya que permite acotar la captura.
    - **Dividir captura**:
        - **Dividir por**: es opción posibilita realizar la división de la captura, mediante un menú desplegable que admite la división por paquetes y por tiempo.
        - **Paquetes**: se admite seccionar el archivo según la cantidad de archivos que contenga.
    - **Filtro Avanzado**: a partir del archivo de captura existente, permite generar nuevos archivos que contengan sólo aquellos datos que se van a filtrar nuevamente. La gran ventaja de esta posibilidad es que los archivos tienen un tamaño considerablemente menor.
        - **Nombre cap**: aquí se debe seleccionar el nombre del nuevo archivo de captura.
        - **Filtro**: al realizar clic en crear se abre una ventana como la siguiente, que permite establecer condiciones puntuales sobre la nueva regla de filtrado. Se puede elegir un protocolo o expresión desde el menú desplegable. También, se brinda la posibilidad de configurar reglas. Se requiere hacer clic en Agregar y luego Confirmar para aplicar el filtro en cuestión.

Apartado III

Guías paso-a-paso

Sección 4

Seguridad sobre Denwa UC&C

Dado que los protocolos VoIP operan sobre redes IP, la integridad de los primeros dependen en gran medida de las segundas; por lo que es necesario el complemento de un sistema de seguridad de alto nivel, para hacer frente a las amenazas potenciales que puedan haber en esta nueva tecnología.

Para llevar a cabo un ataque al sistema, debe existir al menos una vulnerabilidad en el mismo. Puesto que la red IP es susceptible a problemas de seguridad, el sistema deberá estar compuesto por varias aplicaciones en las diferentes partes que conforman la solución, para que la red sea: segura, confiable y brinde protección a todos sus integrantes.

A destacar

Cualquier equipo expuesto a la red sin ninguna protección es vulnerable y candidato a ser atacado.

Nuestra principal recomendación es: **NO** exponer la plataforma Denwa UC&C hacia la internet colocándole una ip publica; a menos de no ser estrictamente necesario y que se cuente (mínimamente) con medios de seguridad tales como lo son: SBC y Firewall.

En este documento se proporciona una guía de configuración del sistema de comunicaciones unificas enfocada a la seguridad de la red. Si bien el tema abordado es muy amplio, se brindan explicaciones y configuraciones (paso-a-paso) necesarias para realizar una configuración óptima.

Importante

La plataforma Denwa UC&C únicamente debe ser accesible desde redes y direcciones IP conocidas y autorizadas, habitualmente redes LAN. Para ello se recomienda configurar un puerto de administración (interfaz de red o VLAN) que solamente sea utilizado por personal autorizado.
En caso de habilitar el acceso a redes y direcciones IP ajenas a la LAN (por ejemplo MAN o WAN), se recomienda permitir el acceso, desde la herramienta de Firewall, únicamente a puertos y protocolos específicos.

4.1. DenwaUC

4.1.1. Esquema general

La siguiente imagen nos muestra todos los bloques que un atacante tiene que atravesar desde el momento que intenta realizar un ataque contra Denwa hasta que logra realizar una llamada no permitida. Asimismo se explicará luego como realizar las configuraciones de todos estos bloques para que de ningún modo el atacante logre su cometido.

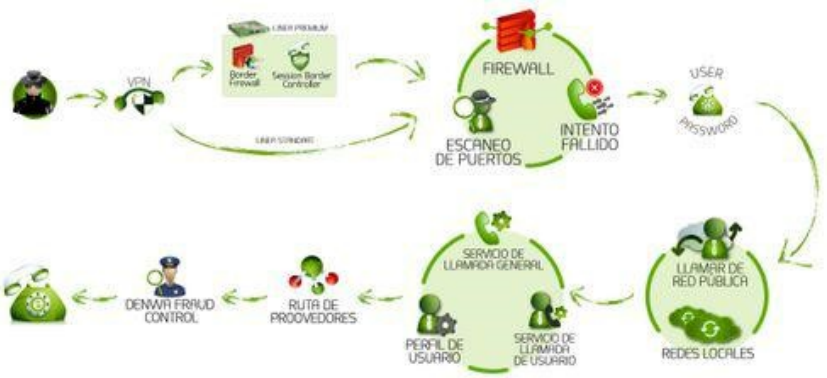

Figura 4.1: Esquema general de bloques

4.2. Pasos previos

Antes de abordar la revisión de cada uno de los ítems descriptos en la imágen anterior, es necesario dejar en claro algunas consideraciones mínimas de seguridad para el acceso a la plataforma Denwa UC&C.

4.2.1. Cambio de contraseñas predeterminadas

Para facilitar el proceso de instalación y primera configuración, la plataforma cuenta con dos (2) accesos predeterminados, uno de ellos permitó el ingreso luego de la instalación del sistema operativo base (desde la ISO); en tanto que el otro, dio el acceso necesario para poder activar la licencia del equipo. Por lo cual, estas contraseñas ”genéricas”deben ser modificadas lo antes posible.

4.2.1.1. Usuario admin

Para realizar el cambio de contraseña del usuario **admin**, deberá ingresar a la interfaz de administración web y dirigirse al menú: Configuración >Administradores. Una vez ahí, podrá visualizar el listado de todos los usuarios tipo administrador de la plataforma. Bastará con realizar un click sobre el usuario admin para que se despliegue una ventana emergente, en donde podrá cambiar su contraseña (deberá reingresarla en el campo Çonfirmación de contraseña”).

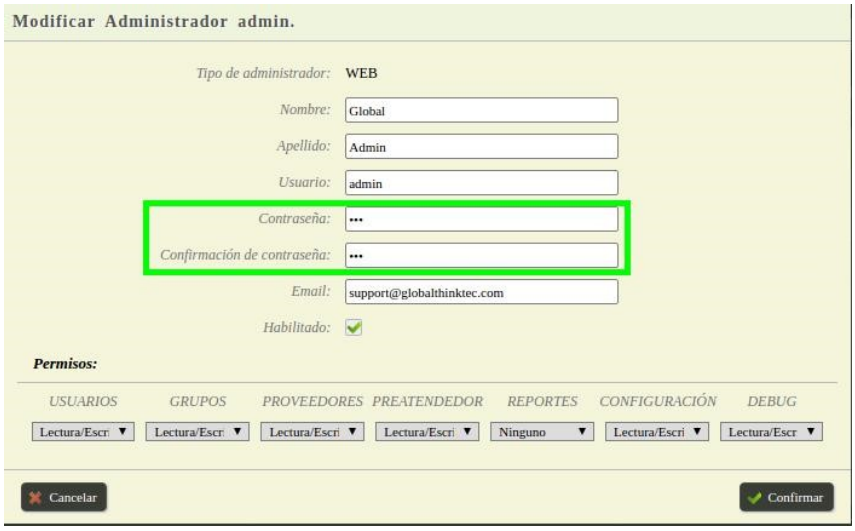

Figura 4.2: Cambio de contraseña del usuario admin

4.2.1.2. Usuario pbxadmin

El caso del usuario **pbxadmin** es igual al anterior, deberá ingresar a la interfaz de administración web y dirigirse al menú: Configuración >Administradores y editar el usuario de la interfaz de la línea de comandos (*CLI* por sus siglas en inglés).

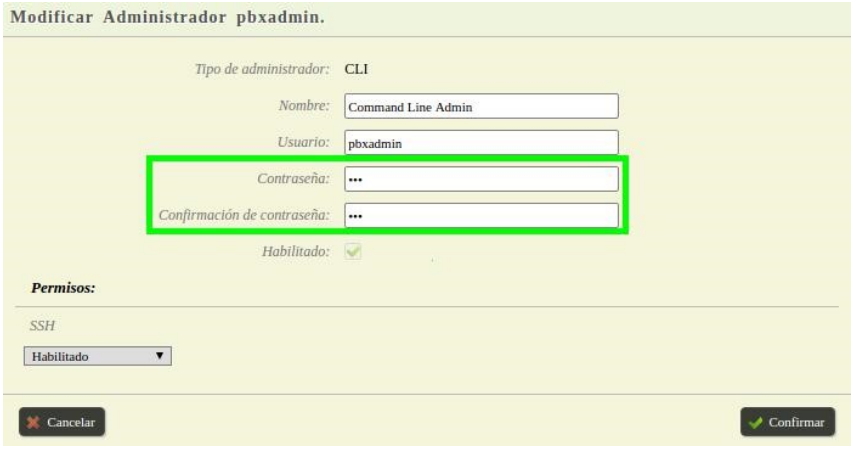

Figura 4.3: Cambio de contraseña del usuario pbxadmin

Sin embargo, en caso de considerar que no es necesario, es recomendable deshabilitarlo desde este mismo apartado.

4.2.2. Uso de HTTPS

El HTTPS es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web. El envío de datos mediante HTTPS está protegido con el protocolo seguridad en la capa de transporte (*TLS* por sus siglas en inglés), que proporciona estas tres capas de seguridad principales:

- **Cifrado**: se cifran los datos intercambiados para mantenerlos a salvo de miradas indiscretas. Eso significa que cuando un usuario está navegando por un sitio web, nadie puede .escuchar"sus conversaciones, hacer un seguimiento de sus actividades por las diferentes páginas ni robarle información.

- **Integridad de los datos**: los datos no pueden modificarse ni dañarse durante las transferencias, ni de forma intencionada ni de otros modos, sin que esto se detecte.

- **Autenticación**: demuestra que tus usuarios se comunican con el sitio web previsto. Proporciona protección frente a los ataques de intermediario y fomenta la confianza de los usuarios, lo que se traduce en otros beneficios empresariales.

Para configurar el uso de HTTPS, es necesario ingresar a la interfaz de administración wev y dirigirse al menú: Configuración >Redes >Servidor web. Es posible generar certificados autofirmados en el propio equipo, o importar los certificados de su dominio.

Figura 4.4: Habilitación del protocolo HTTPS

4.2.3. Firewall

Para resguardar la plataforma ante otros tipos de ataques, además de poder realizar un esquema general de seguridad y reglas para los diferentes equipos y tráficos en nuestra red, se dispone de una herramienta fundamental al momento de realizar una configuración nueva: el Firewall. Esta herramienta puede ser configurada de forma gráfica, intuitiva y simple.

Es posible configurar reglas específicas para el filtrado, aceptación, denegación o descarte del tráfico entrante, saliente o de paso por la plataforma. Esto lo hace especificando: servicios, protocolos, puertos y/o direcciones IP de orígen o de destino. Solamente los administradores pueden hacer este tipo de configuraciones.

Figura 4.5: Configuración del Firewall

Es indispensable la correcta configuración de esta herramienta.

Firewall y Alta Disponibilidad

En el caso de los equipos configurados en un esquema de Alta Disponibilidad, las reglas de prioridad del Firewall no pueden ser configuradas, en su lugar deberán cargarse en la sección de reglas del usuario.

4.2.3.1. Herramientas adicionales Premium

Denwa Premium

Las herramientas mencionadas para Premium únicamente están disponibles en la versión 3.3.1 del sistema Denwa UC&C

El equipo Denwa Premium dispone, además de las herramientas adicionales a las nombradas anteriormente, dos (2) funvionalidades extra: Firewall de borde y SBC (session border controller).

4.2.3.1.1. Firewall de borde El equipo Denwa Premium posee las mismas funcionalidades de router; por tal motivo posee un firewall previo al firewall de Denwa UC. Este firewall permite configurar listas de acceso para permitir y denegar el tráfico que se requiera, tanto entrante como saliente. Puede ser configurado desde la interfaz de administración web, ingresando al menú: Configuración >Denwa Premium >Seguridad (listas de acceso).

Figura 4.6: Configuración del Firewall de borde

Es indispensable la correcta configuración de esta herramienta

4.2.3.1.2. SBC Esta herramienta es quizás el mejor aspecto de seguridad y normalización SIP que un equipo de telefonía puede disponer entre sus características. El SBC como su nombre lo indica nos permite hacer un control exausivo de las sesiones SIP que se realicen en el equipo.

Es de gran ayuda a la hora de mejorar la seguridad ya que el propio SBC descarta el tráfico que no cumple con las reglas básicas del protocolo SIP (tráfico malformado), en el caso de Denwa el SBC, solamente permitirá el tráfico al puerto 5060 de aquellos proveedores (o usuarios) que hayan sido declarados expresamente en el equipo. Además, puede modificar los headers de los paquetes SIP .enmascarando"la IP de la central telefónica y es capaz de controlar todo tipo de registros SIP externos.

Se recomienda utilizar el SBC en los proveedores; para ello es suficiente activar la casilla correspondiente en la pensaña de configuración del proveedor, tal como se muestra en la siguiente imagen:

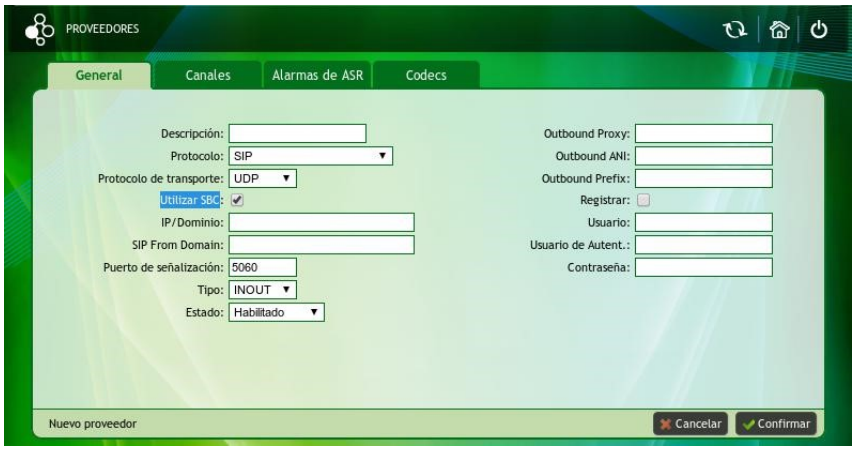

Figura 4.7: Configuración del SBC en los proveedores

4.3. Paso-a-paso de un ataque

Hasta este momento, todo lo indicado que puede ser considerado como: recomendación general; sin embargo es preciso conocer la forma en la que habitualmente se producen los ataques, así como las herramientas que posee la plataforma para repelerlos.

4.3.1. Primer paso: husmear

El atacante en primer lugar intentará capturar la mayor cantidad de tráfico perteneciente a la red para tratar de obtener información que pueda utilizar en su ataque.

Denwa permite utilizar redes privadas virtuales (*VPN* por sus siglas en inglés) para su conexión con el mundo exterior. Se ampliará este tema en la sección VPN en la página 159.

4.3.2. Segundo paso: escanear

Ahora necesita conocer con la mayor exactitud posible los servicios que el equipo atacado posee, para luego poder encontrar vulnerabilidades en los mismos, y así valerse de ellas.

Denwa lo contrarresta con una herramienta de detección de escaneo de puertos, pudiendo bloquear este tipo de ataques. Este tema será abordado en la sección Escaneo de puertos en la página 164.

4.3.3. Tercer paso: accceder

El atacante, luego de haber encontrado el puerto 5060 abierto en el equipo atacado, puede suponer con un alto grado de certeza que el equipo brinda servicios de telefonía. Por lo tanto, para avanzar con su ataque procederá a intentar hacerse con una cuenta dentro del equipo (usuario y contraseña válidos). Habitualmente este tipo de ataques se realizan por fuerza bruta, intentando el registro de usuarios utilizando contraseñas aleatorias, hasta encontrar una efectiva.

Denwa posee una herramienta que detecta intentos fallidos de registro e inicio de sesión, con la cual se agrega a una lista negra la dirección IP de origen de la solicitud luego de errar varias veces su contraseña. Este tema será tratado en las secciones Intentos fallidos (página 164) y Contraseña de usuarios (página 165).

4.3.4. Cuarto paso: generar tráfico

Intentar realizar llamadas sin costo para el atacante, esto es lo que un atacante de un sistema telefónico búsca. Para esto y ya registrado con el usuario y password que pudo captar de su ataque, realiza llamadas a diferentes destinos.

Denwa cuenta con una serie de herramientas para controlar cuál usuario puede, y cuál no, realizar cierto tipo de llamadas; entre ellas:

- Redes locales (ver página 165)
- Llamar desde la red pública (ver página 166)
- Servicios de llamada (ver página 166)
- Servicio de llamada del usuario (ver página 166)
- Ruta de proveedores (ver página 168)
- Control de fraude (ver página 168)

4.4. Recursos de Denwa UC&C

Es de suma importancia conocer las herramientas que se encuentran disponibles en la plataforma de comunicaciones unificadas, ya que de su correcta configuración depende la seguridad de la plataforma.

4.4.1. VPN

Es posible configurar el sistema Denwa UC&C tanto como cliente como servidor de distintos tipos de VPN

4.4.1.1. Como cliente de VPN

Se recomienda la configuración de esta funcionalidad en los escenarios que lo permitan, puede realizarse en la interfaz web de administración, desde el menú: Configuración >Redes >Clientes VPN.

Desde esta pestaña se puede configurar una nueva conexión VPN (Virtual Private Network) mediante el protocolo PPTP (Point-To-Point Tunneling Protocol) o el protocolo OpenVPN y editar las conexiones existentes (en caso de disponer de alguna).

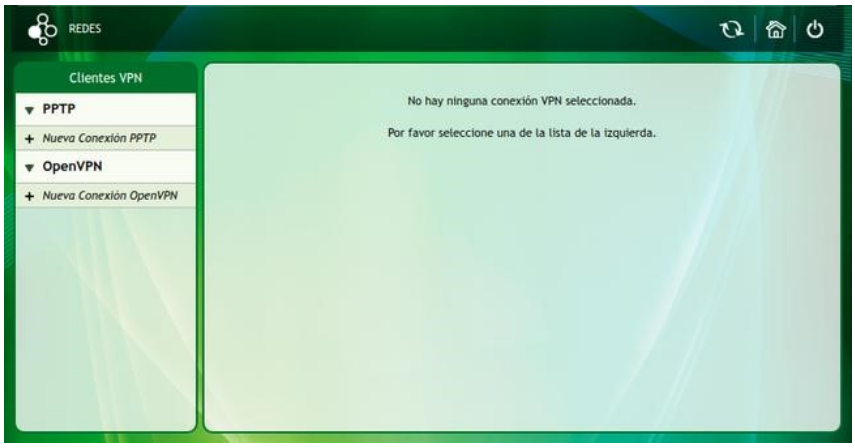

Figura 4.8: Clientes de VPN

Las VPN permiten una extensión segura de la red local sobre una red pública. Para ello, se realiza una conexión virtual punto a punto mediante el uso de conexiones dedicadas y/o cifradas. Presenta la ventaja de reducir el ancho de banda utilizado y aumentar la velocidad. Además proporciona comunicaciones seguras en las redes públicas con derechos de acceso específicos.

4.4.1.1.1. Cliente PPTP se conecta directamente al servidor de destino creando una red virtual para cada cliente remoto, que el administrador puede supervisar y administrar como cualquier otro puerto de acceso remoto. Para realizar la configuración de este cliente se debe efectuar un click en la opción Nueva Conexión PPTP.

Figura 4.9: Clientes de VPN, PPTP

A continuación la descripción de los campos:

- **Configuración general**
  - **Nombre de la conexión**: nombre que se asigna a la conexión.
  - **Servidor PPTP**: IP o dominio del servidor PPTP.
  - **Usuario**: nombre de usuario para acceder al servidor PPTP.
  - **Contraseña**: contraseña de usuario para acceder al servidor PPTP.
  - **Conectar automáticamente**: habilitar en caso de que la conexión siempre deba encontrarse activa
- **Método de Autenticación**: se debe seleccionar el o los protocolos de autenticación a usar.
  - **PAP** (Password Authentication Protocol): es un protocolo simple que autentica un usuario contra un servidor de acceso remoto. Su función es validar a un usuario para que acceda a diferentes recursos. Para esto, PAP transmite contraseñas en ASCII sin cifrar, por lo que se debe usar como último recurso.
  - **CHAP** (Challenge Handshake Authentication Protocol): es un protocolo de autenticación por desafío mutuo. Este verifica periódicamente la identidad del cliente remoto usando un intercambio de información. Con CHAP, el ID de usuario y la contraseña siempre se envían cifrados, lo que lo convierte en un protocolo más seguro que PAP.
  - **MSCHAP** (Microsoft Challenge Handshake Authentication Protocol): protocolo de autenticación por desafío mutuo de Microsoft. Este no requiere que ambas partes conozcan la clave en claro, sino un resumen (Hash) de la misma.
  - **MSCHAPv2** (Microsoft Challenge Handshake Authentication Protocol v2): protocolo de autenticación por desafío mutuo de Microsoft versión 2. Proporciona seguridad de alto nivel para las conexiones de acceso remoto. MS-CHAP v2 resuelve algunos problemas de MS-CHAP.
- **Método de Compresión**: son métodos de encriptación, únicamente se utilizan con los protocolos MSCHAP y MSCHAPv2.
  - **MPPE 40** (Microsoft Point-to-Point Encryption): Encriptación punto a punto de Microsoft de 40 bits.

- **MPPE 128** (Microsoft Point-to-Point Encryption): Encriptación punto a punto de Microsoft de 128 bits.

Luego se efectúa click en «✔Crear» y la VPN se habrá creado. A continuación se puede observar la conexión generada.

Figura 4.10: Clientes de VPN, conexión PPTP configurada

Una vez que se crea la nueva conexión, ésta se puede Conectar, Eliminar o Modificar la conexión desde los botones situados en la sección inferior de la página.

4.4.1.1.2. Cliente OpenVPN es un software de red privada virtual de código abierto, que provee seguridad, estabilidad y mecanismos de cifrado sin presentar complejidad. Para configurar el cliente OpenVPN se debe hacer click en la opción Nueva Conexión OpenVPN.

Figura 4.11: Clientes de VPN, configuración OpenVPN

A continuación la descripción de los campos:

- **Configuración General**
  - **Nombre de la conexión**: nombre que se le asignará a la conexión.
  - **Servidor OpenVPN**: IP o dominio del servidor OpenVPN.
  - **Puerto**: puerto que se utlizará para la conexión VPN.
  - **Conectar automáticamente**: habilitar en caso de que la conexión siempre deba encontrarse activa.
- **Certificados**
  - **Autoridad de Certificación (CA)**: Posibilita importar el archivo.
  - **Certificado del Cliente (CRT)**: Posibilita importar el archivo.

- **Llave del Cliente (KEY)**: Posibilita importar el archivo.

Estos certificados deben ser otorgados por el administrador del servidor de OpenVPN.

Figura 4.12: Clientes de VPN, configuración OpenVPN

Luego, al pulsar sobre el botón «✔Crear» la VPN se habrá dado de alta en el sistema. Al igual que con el PPTP, se puede Conectar, Eliminar o Modificar la conexión desde los botones situados en la sección inferior de la página.

4.4.1.2. Como servidor de VPN

Por otra parte, en caso de no contar con un servidor de VPN, la pataforma de comunicaciones unificadas puede ser configurada para que cumpla dicha función.

4.4.1.2.1. Servidor OpenVPN En este apartado se configurará el servicio de OpenVPN para disponer de conexiones seguras para usuarios fuera de la red. Al ingresar al servidor se puede observar una pantalla como la siguiente:

Figura 4.13: Servidor OpenVPN

En la columna de la izquierda es posible iniciar o detener el servicio de OpenVPN Server pulsando sobre el ícono ⏻.

4.4.1.2.1.1. Pestaña de Configuración En la imagen anterior se puede notar que el servidor se encuentra deshabilitado y que no existe una configuración pre-cargada. A continuación el detalle de los parámetros a configurar:

- **Puerto**: puerto a utilizar para el servicio de OpenVPN
- **Protocolo**: protocolo que empleado por el servidor

- **Dirección de red/Máscara**: red de la cual se otorgará direcciones IP a los clientes
- **Permitir acceso**: redes a las que se le desea dar acceso a los clientes.

4.4.1.2.1.2. Pestaña de Cuentas En esta pestaña es posible dar de alta cuentas para el acceso remoto a la plataforma de comunicaciones unificadas y/o a las redes seleccionadas en la pestaña de configuración.

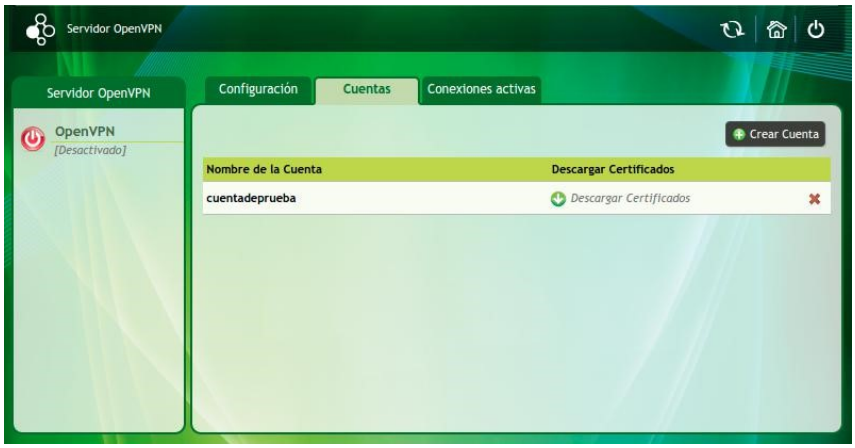

Figura 4.14: Servidor OpenVPN, cuentas de acceso

Para realizar una nueva cuenta simplemente hacemos click en Crear Cuenta, y complertar el nombre de usuario; con esto la cuenta se ha creado y es posible descargar sus certificados.

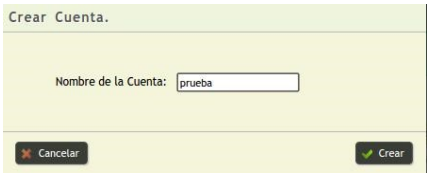

Figura 4.15: Servidor OpenVPN, creación de cuenta de acceso

Para utilizar el servidor de OpenVPN es necesario disponer de los certificados en los equipos que se conectarán a él, por lo que deben ser descargados desde la pestaña cuentas. Una vez en el equipo local es necesario disponer del software «cliente» de OpenVPN y, desde un editor de texto básico, generar un archivo .ovpn como el que se muestra a continuación:

```
##############################################
#   Cliente OpenVPN
##############################################
client
dev tun
proto PROTOCOLO
remote IP_DE_SERVIDOR PUERTO_DE_SERVIDOR
resolv-retry infinite
nobind
comp-lzo
verb 3
# Certificates files
ca "RUTA_DE_CERTIFICADO/ca.crt"
cert "RUTA_DE_CERTIFICADO/NOMBRE_CERTIFICADO.crt"
key "RUTA_DE_CERTIFICADO/NOMBRE_CERTIFICADO.key"
##############################################
```

Ejemplo del contenido de los ficheros .ovpn

Debe reemplazar donde dice «PROTOCOLO», «IP_DE_SERVIDOR», «PUERTO_DE_SERVIDOR», «RUTA_DE_CERTIFICADO», «NOMBRE_CERTIFICADO» según las configuraciones realizadas en el servidor, así como los certificados descargados.

4.4.1.2.1.3. Pestaña de Registros En esta pestaña se mostrará el listado de todas las conexiones activas («clientes» conectados) al servicio OpenVPN.

4.4.2. Escaneo de puertos

La herramienta de «Escaneo de puertos» permite bloquear ataques de este tipo de forma automática, esto porque el sistema chequea constantemente posibles escaneos de puertos sobre el equipo y, al detectar esto, bloquea de forma automática la dirección IP, desde donde se esté realizando el posible ataque, creando una nueva regla en el *Firewall*.

Solamente los usuarios tipo administrador pueden modificar el Firewall para eliminar el bloqueo a una dirección IP, en caso de que se considere que fuera bloqueada por error.

Escaneo de puertos

Es indispensable el uso de esta herramienta

Reglas automáticas

Los bloqueos de direcciones IP creados de forma automática por los procesos de intentos fallidos y escaneo de puertos se crean en la Sección de Reglas automáticas.

Figura 4.16: Escaneo de puertos e Intentos fallidos activados

4.4.3. Intentos fallidos

La herramienta «Intentos fallidos» ofrece la posibilidad de bloquear ataques de «fuerza bruta» de manera automática. El sistema revisa y guarda constantemente el listado de intentos de registro, así como la dirección IP desde donde se intentó realizar; en caso de hallar cinco (5) intentos de registros fallidos desde la misma IP, genera de forma automática una nueva regla en el Firewall para denegar cualquier paquete que posea el mismo origen.

Solamente los usuarios tipo administrador pueden modificar el *Firewall* para eliminar el bloqueo a una dirección IP, en caso de que se considere que fuera bloqueada por error.

Intentos fallidos

Es indispensable el uso de esta herramienta

Reglas automáticas

Los bloqueos de direcciones IP creados de forma automática por los procesos de intentos fallidos y escaneo de puertos se crean en la Sección de Reglas automáticas.

4.4.4. Contraseña de usuarios

La mejor manera de complementar a la herramienta de «Intentos fallidos» es a través del uso de contraseñas robustas, por lo que es importante controlar de manera exhaustiva el nivel de complejidad de las contraseñas de todos los usuarios y asegurarse su complejidad es alta. Esto también aplica para los usuarios tipo administrador.

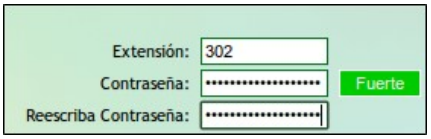

Figura 4.17: Fortaleza de las contraseñas

Ante un ataque de «Fuerza bruta», la complejidad de las contraseñas disminuye la probabilidad de que sean fácilmente descubiertas, aumentando a su vez la probabilidad de que la dirección IP del atacante sea bloqueada por Firewall de manera automática mediante la herramienta de «Intentos fallidos». Esto aplica igualmente para las contraseñas de Denwa Desktop.

Es posible conocer el estado general de la complejidad de las contraseñas de todos los usuarios del sistema desde la pantalla de inicio en la interfaz de administración web.

4.4.5. Redes locales

Denwa necesita conocer de algún modo el esquema de red en donde está instalada, por lo que es necesario indicarle las redes que debe interpretar como «locales»; toda red que no pertenezca a las redes locales será interpretada como una red externa.

Esto es muy importante durante la configuración de los usuarios y sus permisos, ya que es posible configurar que el usuario no pueda realizar llamadas si no se ha registrado desde una red local. Otra herramienta muy útil en el caso de usuarios no deban registrarse desde fuera de la red.

Se debe agregar las redes desde la interfaz web de administración, en el menú: Configuración >General >Avanzada presionando en ícono ⚙ al lado de «Red Local». Esto habilitará una nueva ventana, la cual permite agregar las diferentes redes.

Figura 4.18: Redes locales

Pulsando sobre el ícono ✚, se desplegará una ventana en donde es posible declarar una a una las redes locales. El formato para agregar las mismas en red/mascara (ambas en cuatro octetos decimales).

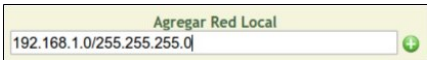

Figura 4.19: Redes locales, agregar una red local

Presionando sobre el ícono ✚retornará a la ventana anterior, pudiendo repetir el proceso

tantas veces como redes locales posea. Luego, bastará con se debe presionar sobre el botón «✔Aceptar» para finalizar la tarea.

4.4.6. Llamar desde la red pública

Esta opción habilita al usuario a poder realizar llamadas cuando está registrado de una red que no pertenece a las redes locales configuradas en el paso anterior.

Se recomienda que solo los usuarios que realmente utilicen esta funcionalidad tengan activa esta opción en la configuración avanzada del usuario.

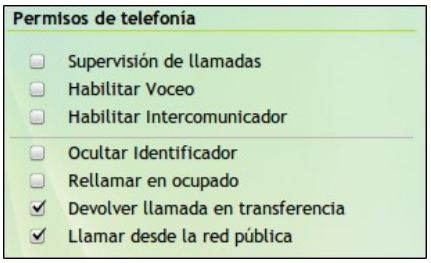

Figura 4.20: Configuración avanzada del usuario, llamar desde la red pública

4.4.7. Servicios de llamada

En este lugar se configuran todos los prefijos de llamadas para cada uno de los tipos de llamadas que podrían ser cursados (Locales, Nacionales, Internacionales, etc.). Por ejemplo, en el caso de las llamadas Internacionales el prefijo sería «00».

Al definir los prefijos esta sección se le permitirá habilitar o denegar los distintos tipos de llamadas a cada usuario de Denwa. Puede ser configurado desde la interfaz de administración web, en el menú: Configuración >Servicios de llamadas.

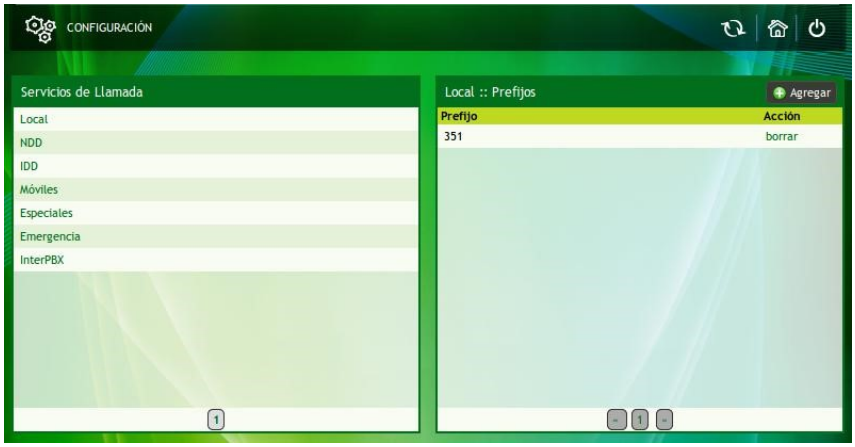

Figura 4.21: Servicios de llamada

Bloqueo de llamadas

Es primordial configurar los servicios de llamadas de manera correcta, ya que de ellos dependen los servicios de llamada de los perfiles de usuario.
En caso de no encontrarse configurado, toda llamada se ra cursada sin importar su destino.

4.4.8. Servicio de llamada del usuario

Solamente si Servicio de llamada del usuario ha sido configurado, el perfil local del usuario tendrá validez. La configuración de los servicios de llamadas de los usuarios, le permite al

usuario administrador habilitar o denegar, a cada usuario de manera individual, el curso de una llamada según su prefijo.

Puede ser configurado desde la interfaz de administración web, en el menú: Usuarios >Ver usuarios >«Nombre_de_Usuario» >Servicios.

Figura 4.22: Servicios de llamada del usuario

Se recomienda configurar los servicios de cada usuario haciendo un estudio previo de que función realiza dentro de la estructura de la empresa.

4.4.9. Perfiles de usuario

Solamente si Servicio de llamada del usuario ha sido configurado, el perfil a configurarse para los usuarios tendrá validez. Los perfiles de usuario en Denwa permite la habilitación o denegación del curso de llamados a distintos destinos según su prefijo, basándose en criterios como: día de la semana, horario y proveedor a utilizar. Esto agrega un mayor control de los llamados, ya que se puede definir: quién (usuario al que se le haya aplicado el perfil), cómo (según el prefijo de la llamada), dónde (según el proveedor definido) y cuándo (según el día y horario) podrá cursar llamados.

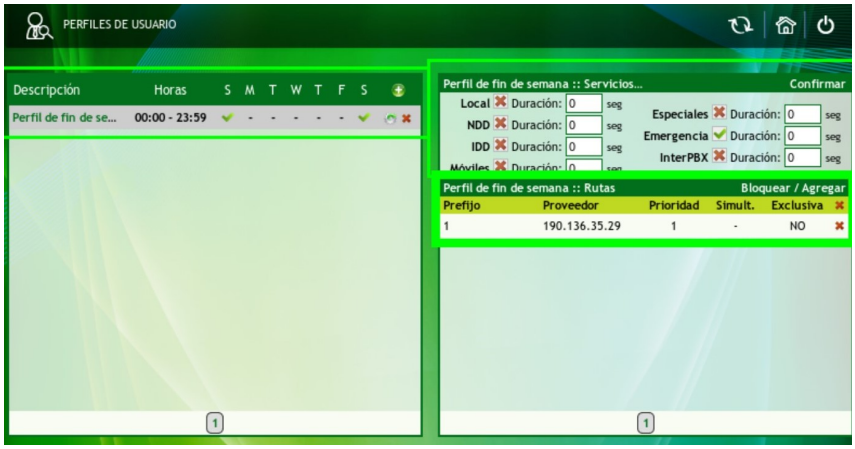

Figura 4.23: Perfiles de usuario

Puede ser configurado desde la interfaz de administración web, en el menú: Usuarios >Perfiles de usuario.

Rutas

En caso de que un perfil no cuente con rutas definidas, el usuario que tenga ese perfil asignado, no podrá cursar llamadas hacia el exterior.

Perfiles de usuario

Es recomendado el uso de esta herramienta.

4.4.10. Ruta de proveedores

Es importante la correcta configuración de las diferentes rutas de cada uno de los proveedores dentro de Denwa. Estas rutas son las que habilitan cursar llamados por uno u otro proveedor, deacuerdo al numero discado. Deben ser configuradas de la manera mas específica posible para que solamente se cursen las llamadas que han sido correctamente discadas. A continuación un ejemplo:

En caso de necesitar que las llamadas que comienzan con el número 0 y tienen una longitud de 7 dígitos (incluyendo el 0)sean cursadas por cierto proveedor, se pueden presentar dos (2) posibles configuraciones:

- **Configuración correcta** (✔): la configuración de la ruta debería ser "0_____"(un cero y seis _)
- **Configuración incorrecta** (✖): la ruta simplemente con 0 y prioridad 1 permite que cualquier llamada que comienza con 0 sea cursada por este proveedor

Ruta de proveedores

Se recomienda una configuración meticulosa de las rutas de los proveedores.

4.4.11. Control de fraude

Por si fuera poco, el sistema Denwa cuenta con una última línea de protección contra ataques, la herramienta de «Control de Fraude». Esta herramienta permite analizar el comportamiento de cada usuario de la plataforma, pudiendo bloquear aquellas llamadas que parezcan sospechosas. Por ejemplo: si una extensión genera 10 llamadas en 5 minutos, posiblemente se trate de un «boot» que está intentando generar llamadas con el objetivo de realizar daño. En tal caso el usuario o el destino pueden ser bloqueados, al mismo tiempo se envía un aviso por correo electrónico para alertar la situación.

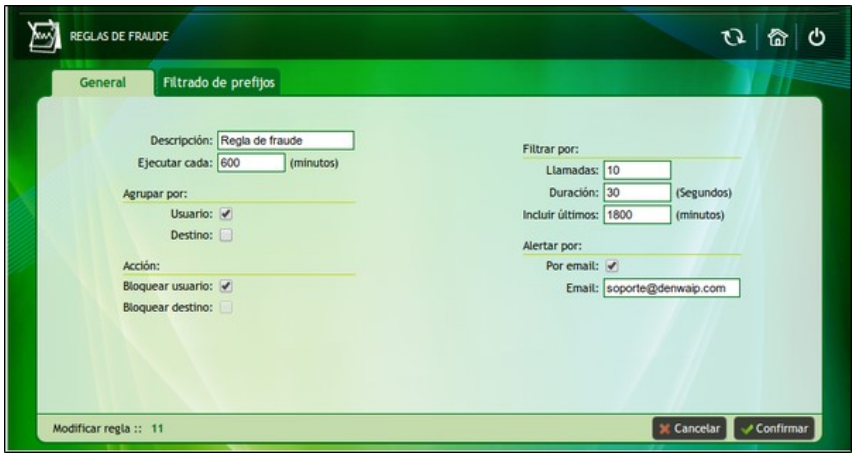

Figura 4.24: Control de fraude

Puede ser configurado desde la interfaz de administración web, en el menú: Configuración >Control de fraude.

Alerta por correo electrónico

Las alertas por correo electrónico únicamente serán enviadas si su servidor de correo se encuentra debidamente configurado (Configuración >General >Servidor de Correo)

4.5. Final de configuraciones sobre Denwa UC&C

Estas son las herramientas que hacen de Denwa una solución extremadamente segura en todos sus equipos. Resumiendo: un atacante requiere que se configure de manera incorrecta todas estas herramientas para realizar llamadas sin autorización a través de nuestra plataforma de comunicaciones unificadas.

En las secciones siguientes se adicionarán recomendaciones generales sobre los dispositivos ajenos a la plataforma de comunicaciones unificadas, pero que hacen a la seguridad del sistema VoIP y a la correcta implementación de la estructura de red.

Figura 4.25: Herramientas de seguridad Denwa

Sección 5

Seguridad sobre terminales de telefonía

A continuación nuestras recomendaciones para la seguridad de los terminales de telefonía:

1. Cambiar la contraseña de administración de los terminales telefónicos.
2. Configurar el firewall interno de los teléfonos Denwa para que solamente puedan ser accesibles desde la dirección IP de la plataforma de comunicaciones unificadas y del rango de direcciones IP de los usuarios tipo administrador de la misma.
3. Habilitar SRTP a fin de contar con cifrado de voz. En caso de realizar el aprovisionamiento de los terminales desde la plataforma Denwa UC&C bastará con habilitarlo en la configuración del usuario (Usuarios >Ver usuarios >«Nombre_de_Usuario» >Avanzada)

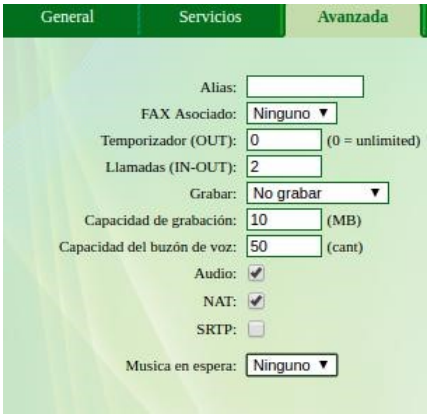

Figura 5.1: Habilitación de SRTP

Sección 6

Seguridad sobre la estructura de red

A continuación nuestras recomendaciones para la seguridad de la estructura de red:

1. Modificación de todas las contraseñas por defecto en los equipos a instalar (Switch, router, etc.). Esto es un paso importante para la seguridad de la red de datos.
2. Uso de VLANs para separar el tráfico
3. Uso de filtrado de MAC en los distintos puntos de acceso a la red, de este modo se permite únicamente que los equipos autorizados puedan tener acceso al puerto específico del Switch, o a la red Wi-Fi.
4. En casos especiales puede solicitar la eliminación de los módulos de grabación y monitoreo de llamadas en los equipos Denwa UC&C.

Sección 7

Follow me

El Follow-me es una aplicación que realiza desvíos de la llamada para contactar al destinatario de la misma en caso de no encontrarse físicamente presente en su extensión. Existen diferentes opciones de funcionamiento, las cuales se detallan a continuación. Cabe aclarar que el tiempo de desvío es el tiempo que timbrará la extensión a la que se desvió la llamada, tener en cuenta que el anuncio consume tiempo de timbrado.

- **Alternado + Anuncio**: Timbrarán alternadamente los números designados, el usuario que originó la llamada deberá anunciar su nombre siguiendo las instrucciones, luego el sistema le informará de la transferencia de la llamada al siguiente interno y reproducirá el anuncio previamente grabado.
- **Simultáneo + Anuncio**: Timbrarán simultáneamente los números designados, el usuario que originó la llamada deberá anunciar su nombre siguiendo las instrucciones, luego el sistema le informará de la transferencia de la llamada al siguiente interno y reproducirá el anuncio previamente grabado.
- **Alternado**: Timbrarán alternadamente los números designados, mientras el sistema informa que debe esperar mientras se intenta la comunicación.
- **Simultáneo**: Timbrarán simultáneamente los números designados, mientras el sistema informa que debe esperar mientras se intenta la comunicación.
- **Alternado + Silencio**: Timbrarán alternadamente los números designados, sin realizar ningún informe a los usuarios.
- **Simultáneo + Silencio**: Timbrarán simultáneamente los números designados, sin realizar ningún informe a los usuarios.

7.1. Problemas frecuentes

En el presente documento se pretende listar los problemas más comunes que suelen presentarse junto con las principales que pueden producir cada uno de ellos y las posibles soluciones a los mismos.

7.1.1. Caso 1: Se puede realizar llamadas pero no se pueden recibir

7.1.1.1. Causas posibles

- DND (Do Not Disturbed - No molestar) activado.
- Pérdida de registro de los equipos.
- Configuración IVR o DID.

7.1.1.2. Solución

- Verificar que no se encuentre activa la funcionalidad DND.
- Reiniciar el teléfono para que se registre. Luego ingresar a la web a la sección Usuarios ->Ver usuarios para verificar el estado en el que se encuentra. Es decir, si la columna Registrado se presenta el estado en color rojo indica que la extensión en cuestión no se ha registrado; por el contrario si el estado esta en color verde indica que la extensión se ha registrado exitosamente.
- Configuración IVR: verificar que los números de acceso se encuentren asignados y sean los deseados. Puede observarse el diagrama de árbol y, en caso de ser necesario, es posible asignar el número directamente a una extensión para verificar que la llamada ingresa correctamente.
- Configuración DID: verificar si el número de acceso se encuentra configurado en el troncal y, luego, si esta debidamente asociado a un usuario.

7.1.2. Caso 2: No se pueden realizar llamadas salientes

7.1.2.1. Causas posibles

- Pérdida de registro.
- La extensión no dispone de los permisos necesarios.
- Rutas erróneas.

7.1.2.2. Solución

- Reiniciar el teléfono para que se registre. Luego ingresar a la web a la sección Usuarios ->Ver usuarios para verificar el estado en el que se encuentra. Es decir, si la columna Registrado se presenta el estado en color rojo indica que la extensión en cuestión no se ha registrado; por el contrario si el estado esta en color verde indica que la extensión se ha registrado exitosamente. (Solución 2 caso anterior).
- Verificar los permisos de servicios de llamada del usuario, desde la web acceder al menú Usuarios ->Ver usuarios ->Pestaña Servicios.
- 3. Verificar que la ruta del proveedor deseado sea correcta.

7.1.3. Caso 3: No se permite el acceso al Denwa Desktop

7.1.3.1. Causas posibles

- Contraseña incorrecta.
- El usuario en cuestión no tiene habilitado el servicio.

7.1.3.2. Solución

- Introducir una nueva contraseña.
- Habilitar al usuario el servicio Desktop.

7.1.4. Caso 4: Firewall, IP de teléfonos DROP en las reglas automáticas

7.1.4.1. Causas posibles

- Reglas automáticas del firewall muestran en su lista IP de equipos pertenecientes a la red.

7.1.4.2. Solución

- Recordar que el firewall es 'secuencial', por lo cual se dará prioridad a aquellas reglas que se encuentren sobre las otras. La secuencia qu utiliza dicho firewall (desde el update 092) es la siguiente: Reglas de prioridad, Reglas automáticas, Reglas de usuario, Servicios (WAN) y Política. Por lo cual, basta con agregar en reglas de prioridad la red en la cual se encuentran dichos equipos.

7.1.5. Caso 5: Desvíos

7.1.5.1. Uso

- NO se permite realizar más de un desvío en una misma llamada. Esto es para evitar que la misma ingrese a un loop.

Sección 8

Conexión al servidor Denwa OpenVPN

De acuerdo al sistema operativo utilizado, se realiza el siguiente instructivo para conectarsevmediante VPN a la central. Una vez descagados los archivos y generado el .ovpn, se disponen de los siguientes archivos:

- ca.crt
- client.ovpn
- client.crt
- client.key

Nombre de los archivos

El nombre «client» es agregado a modo ilustrativo.

8.1. OpenVPN para Windows

Para generar el cliente OpenVPN en Windows, ingresamos al siguiente link `https://openvpn.net/index.php/open-source/downloads.html` y descargamos el instalador para 32 bits o 64 bits. Este proceso fue certificado para Windows XP, Windows 7, Windows 8 y Windows 10

Ejecutamos el instalador con las opciones básicas recomendadas:

En este punto, nos solicitará instalar un adaptador virtual para proveer conexión:

Aceptamos dando click en Instalar, y continuamos la instalación

En el escritorio veremos el siguiente ícono correspondiente al acceso directo a OpenVPN

Pero antes de acceder, debemos configurar el programa cargadole los certificados obtenidos. Para ello vamos al siguiente directorio C:\{}Program Files\{}OpenVPN\{}config y copiamos los certificados en este directorio. Para este ejemplo veremos una conexión de VPN de Denwa

Debemos verificar que el archivo proveedor.client.vpn contenga el siguiente formato:

```
##############################################
# DENWA-PBX VPN CLIENT #
##############################################

client
dev tun
proto udp
remote support.denwaip.com 2288
resolv-retry infinite
nobind
comp-lzo
verb 3
#   Certificates files ca "ca.crt"
cert "denwasupport.crt" key "denwasupport.key"
```

Notar que los parámetros ca, cert y key hace referencia al nombre de los archivos y esta referida en doble comillas (")

Ahora hacer doble click sobre el ícono

nos abre sobre la barra de tareas, en el sector de Íconos de notificación una nueva conexión que inicialmente esta en rojo

Permisos especiales

En Windows 7, Windows 8 y Windows 10 se debe ejecutar este programa como «Administrador».

Haciendo click con el botón derecho nos brinda un sub-menú, con distintas opciones en la que damos a conectar

Entonces nos figura la siguiente ventana donde nos marca el proceso de conexión:

Si la conexión se realiza correctamente veremos el siguiente mensaje de notificación con la Ip asignada por el servidor

Con esto, en la barra de direcciones del navegador colocamos la dirección Ip de la central que nos brinde el Administrador, y tendremos acceso a la web de administrador de la PBX.

8.2. OpenVPN para Linux

Para generar el cliente OpenVPN en Linux, mediante consola con permisos de adminstrador debemos ejecutar el comando:

```
apt-get install openvpn
```

Luego guardamos los certificados provistos en un directorio en el cual luego haremos referencia, en este ejemplo lo guardaremos en el directorio /home/user luego debemos editar el archivo proveedor.client.vpn con el siguiente formato:

```
################################################
# DENWA-PBX VPN CLIENT #
################################################

client
dev tun
proto udp
remote support.denwaip.com 2288resolv-retry infinite
nobind
comp-lzo
verb 3
#   Certificates files ca /home/user/ca.crt
cert /home/user/denwasupport.crt key /home/user/denwasupport.key
```

Notar que los parámetros ca, cert y key hace referencia al nombre de los archivos y están direccionados de acuerdo donde guardamos los archivos.

Luego mediante consola, con permisos de administrador ejecutamos:

```
openvpn /home/user/proveedor.client.vpn
```

y veremos el proceso de conexión. Luego en otra consola

verificamos la conexión mediante el comando ifconfig y se prodrá observar

Donde la interfaz virtual tun0 nos brinda la Ip obtenida de la conexión al servidor de soporte.

Con esto, en la barra de direcciones del navegador colocamos la dirección Ip de la central que nos brinde el

Administrador, y tendremos acceso a la web de administrador de la PBX.

Sección 9

Guía VoIP

9.1. Protocolos VoIP

Hasta hoy en día existe una división clara entre dos tipos de redes:

- Redes de voz: basadas en conmutación de circuitos, por lo que se ocupa un circuito y el enrutamiento durante una comunicación se realiza siempre por el mismo camino. Por ejemplo: Red Telefónica convencional
- Redes de datos: basadas en conmutación de paquetes, la información se envía en paquetes y cada uno de ellos puede viajar por caminos diferentes. Por ejemplo: Internet

Para poder enviar la información por las redes de datos tipo Internet basadas en conmutación de paquetes es necesario adoptar unos protocolos que permitan transmitir y recuperar la información. El problema con la tecnología de conmutación de circuitos es que requiere una significativa cantidad de ancho de banda o bandwidth para cada llamada y el circuito no es empleado eficientemente ya que emplea un canal durante toda la duración de la llamada pero la mayoría de las conversaciones telefónicas están hechas de silencio

Las redes de datos, por el contrario, sólo transmiten información cuando es necesario, aprovechando al máximo el ancho de banda y en la cual el retardo, la alteración del orden de llegada o la pérdida de paquetes no son un inconveniente, ya que en el sistema final se tiene una serie de procedimientos de recuperación de la información original; pero para la voz y el video estos factores son altamente influyentes, por lo tanto se requieren redes y protocolos que ofrezcan un alto grado de QoS (calidad de servicio). Voz sobre IP (VoIP) define los sistemas de enrutamiento y los protocolos necesarios para la transmisión de conversaciones de voz a través de Internet, la cual es una red de conmutación de paquetes basado en el protocolo TCP/IP para el envío de información.

Actualmente existen, principalmente, dos arquitecturas de VoIP para la transmisión de voz por Internet que se utilizan de forma abundante: SIP (*Session Initiation Protocol*, unestándar desarrollado por el IETF, identificado como RFC 3261, 2002).

SIP es un protocolo de señalización para establecer las llamadas y conferencias en redes IP. El inicio de la sesión, cambio o término de la misma, son independientes del tipo de medio o aplicación que se estará usando en la llamada; una sesión puede incluir varios tipos de datos, incluyendo audio, video y muchos otros formatos H.323

H.323 fue el primer estándar internacional de comunicaciones multimedia, que facilitaba la convergencia de voz, video y datos. Fue inicialmente construido para las redes basadas en conmutación de paquetes, en las cuales encontró su fortaleza al integrarse con las redes IP, siendo un protocolo muy utilizado en VoIP.

9.1.1. Arquitectura SIP

El protocolo SIP (Session Initiation Protocol) fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF, definiendo una arquitectura de señalización y control para VoIP. Inicialmente fue publicado en febrero del 1996 en la RFC 2543, ahora obsoleta con la publicación de la nueva versión RFC 3261 que se publicó en junio del 2002.

El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación gracias a dos protocolos que son RTP/RTCP y SDP. El protocolo RTP se usa para transportar los datos de voz en tiempo real (igual que para el protocolo H.323, mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.) SIP fue diseñado de acuerdo al modelo de Internet.

Es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en los dispositivos finales (salvo el rutado de los mensajes SIP). El estado de la conexión es también almacenado en los dispositivos finales . El precio a pagar por esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes producto de tener que mandar toda la información entre los dispositivos finales.

SIP es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes . Se basa en mensajes de petición y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP.

9.1.2. H323

H.323 fue diseñado con un objetivo principal: Proveer a los usuarios con tele-conferencias que tienen capacidades de voz, video y datos sobre redes de conmutación de paquetes. Las continuas investigaciones y desarrollos de H.323 siguen con la misma finalidad y, como resultado, H.323 se convierte en el estándar óptimo para cubrir esta clase de aspectos. Además, H.323 y la convergencia de voz, video y datos permiten a los proveedores de servicios prestar esta clase de facilidades para los usuarios de tal forma que se reducen costos mientras mejora el desempeño para elusuario. El estándar fue diseñado específicamente con los siguientes objetivos: - Basarse en los estándares existentes, incluyendo H.320, RTP y Q.931- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos en tiempo real.- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes. Los diseñadores de H.323 saben que los requisitos de la comunicación difieren de un lugar a otro, entre usuarios y entre compañías y obviamente con el tiempo los requisitos de la comunicación también cambian. Dados estos factores, los diseñadores de H.323 lo definieron de tal manera que las empresas que manufacturan los equipos pueden agregar sus propias especificaciones al protocolo y pueden definir otras estructuras de estándares que permiten a los dispositivos adquirir nuevas clases de características o capacidades.

9.1.3. IAX (*Inter-Asterisk eXchange*)

El protocolo IAX se corresponde con *Inter-Asterisk eXchange protocol*. Como indica su nombre fue diseñado como un protocolo de conexiones VoIP entre servidores Asterisk aunque hoy en día también sirve para conexiones entre clientes y servidores que soporten el protocolo. La versión actual es IAX2 ya que la primera versión de IAX ha quedado obsoleta Es un protocolo diseñado y pensado para su uso en conexiones de VoIP aunque puede soportar otro tipo de conexiones (por ejemplo video) Los objetivos de IAX son: Minimizar el ancho de banda usado en las transmisiones de control y multimedia de VoIPEvitar problemas de NAT (Network Address Translation)-Soporte para transmitir planes de marcación Entre las medidas para reducir el ancho de banda cabe destacar que IAX o IAX2 es un protocolo binario en lugar de ser un protocolo de texto como SIP y que hace que los mensajes usen menos ancho de banda. Para evitar los problemas de NAT el protocolo IAX o IAX2 usa como protocolo de transporte UDP, normalmente sobre el puerto 4569,(el IAX1 usaba el puerto 5036), y tanto la información de señalización como los datos viajan conjuntamente (a diferencia de SIP) y por tanto lo hace menos proclive a problemas de NAT y le permite pasar los routers y firewalls de manera más sencilla.

9.2. QoS QualityOf sevice VoIP

El auge de la telefonía IP es algo evidente y la principal razón es el reaprovechamiento de los recursos y la disminución en el coste de llamadas a través de Internet. Sin embargo, si de algo adolece todavía la VoIP es de la calidad de los sistemas telefónicos tradicionales. Los

problemas de esta calidad son muchos veces inherentes a la utilización de la red (Internet y su velocidad y ancho de banda) y podrán irse solventando en el futuro. Mientras tanto, cuanto mejor conozcamos los problemas que se producen y sus posibles soluciones mayor calidad disfrutaremos.

Los principales problemas en cuanto a la calidad del servicio (QoS) de una una red de VoIP, son la Latencia, el Jitter,la pérdida de paquetes y el Eco. En VoIP estos problemas pueden ser resueltos mediante diversas técnicas que se explican en los siguientes apartados.

Los problemas de la calidad del servicio en VoIP vienen derivados de dos factores principalmente:

1. Internet es un sistema basado en conmutación de paquetes y por tanto la información no viaja siempre por el mismo camino. Esto produce efectos como la pérdida de paquetes o el jitter

2. Las comunicaciones VoIP son en tiempo real lo que produce que efectos como el eco, la pérdida de paquetes y el retardo o latencia sean muy molestos y perjudiciales y deban ser evitados.

9.2.1. Jitter

El jitter se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Las comunicaciones en tiempo real (como VoIP) son especialmente sensibles a este efecto.

9.2.1.1. Causas

El jitter es un efecto de las redes de datos no orientadas a conexión y basadas en conmutación de paquetes. Como la información se discretiza en paquetes cada uno de los paquetes puede seguir una ruta distinta para llegar al destino.

En general, es un problema frecuente en enlaces lentos o congestionados. Se espera que el aumento de mecanismos de QoS (calidad del servicio) como prioridad en las colas, reserva de ancho de banda o enlaces de mayor velocidad (100Mb Ethernet, E3/T3, SDH) puedan reducir los problemas del jitter en el futuro aumque seguirá siendo un problema por bastante tiempo.

9.2.1.2. Valores recomendados

El jitter entre el punto inicial y final de la comunicación debiera ser ser inferior a 100 ms. Si el valor es menor a 100 ms el jitter puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado.

9.2.1.3. Posibles soluciones

La solución más ampliamente adoptada es la utilización del jitter buffer. El jitter buffer consiste básicamente en asignar una pequeña cola o almacen para ir recibiendo los paquetes y sirviendolos con un pequeño retraso. Si alguno paquete no está en el buffer (se perdió o no ha llegado todavía) cuando sea necesario se descarta. Normalmente en los telefonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos perdida de paquetes pero más retraso. Una disminución implica menos retardo pero más perdida de paquetes.

9.2.2. Latencia

A la latencia también se la llama retardo; se define técnicamente en VoIP como el tiempo que tarda un paquete en llegar desde la fuente al destino.

9.2.2.1. Causas

No es un problema específico de las redes no orientadas a conexión y por tanto de la VoIP. Es un problema general de las redes de telecomunicación. Por ejemplo, la latencia en los enlaces via satelite es muy elevada por las distancias que debe recorrer la información. Las comunicaciones en tiempo real (como VoIP) y full-duplex son sensibles a este efecto. Es el problema de ”pisarnos”. Al igual que el jitter, es un problema frecuente en enlaces lentos o congestionados.

9.2.2.2. Valores recomendados

La latencia o retardo entre el punto inicial y final de la comunicación debiera ser ser inferior a 150 ms. El oído humano es capaz de detectar latencias de unos 250 ms, 200 ms en el caso de personas bastante sensibles. Si se supera ese umbral la comunicación se vuelve molesta.

9.2.2.3. Posibles soluciones

No hay una solución que se pueda implementar de manera sencilla. Muchas veces depende de los equipos por los que pasan los paquetes, es decir, de la red misma. Se puede intentar reservar un ancho de banda de origen a destino o señalizar los paquetes con valores de TOS para intentar que los equipos sepan que se trata de tráfico en tiempo real y lo traten con mayor prioridad pero actualmente no suelen ser medidas muy eficaces ya que no disponemos del control de la red. Si el problema de la latencia está en nuestra propia red interna podemos aumentar el ancho de banda o velocidad del enlace o priorizar esos paquetes dentro de nuestra red

9.2.3. Eco

El eco también se suele conocer como reverberación. El eco se define como una reflexión retardada de la señal acustica original. El eco es especialmente molesto cuanto mayor es el retardo y cuanto mayor es su intensidad con lo cual se convierte en un problema en VoIP puesto que los retardos suelen ser mayores que en la red de telefonía tradicional.

9.2.3.1. Causas

El eco se produce por un fenomeno técnico que es la conversión de 2 a 4 hilos de los sistemas telefónicos o por un retorno de la señal que se escucha por los altavoces y se cuela de nuevo por el microfono.

9.2.3.2. Valores recomendados

El oído humano es capaz de detectar el eco cuando su retardo con la señal original es igual o superior a 10 ms. Pero otro factor importante es la intensidad del eco ya que normalmente la señal de vuelta tiene menor potencia que la original. Es tolerable que llegue a 65 ms y una atenuación de 25 a 30 dB.

9.2.3.3. Posibles soluciones

En este caso hay dos posibles soluciones para evitar este efecto tan molesto.

- **Supresores de eco**: Consiste en evitar que la señal emitida sea devuelta convirtiendo por momentos la linea full-duplex en una linea half-duplex de tal manera que si se detecta comunicación en un sentido se impide la comunicación en sentido contrario. El tiempo de conmutación de los supresores de eco es muy pequeño. Impide una comunicación full-duplex plena.
- **Canceladores de eco**: Es el sistema por el cual el dispostivo emisor guarda la información que envía en memoria y es capaz de detectar en la señal de vuelta la misma información (tal vez atenuada y con ruido). El dispostivo filtra esa información y cancela esas componentes de la voz. Requiere mayor tiempo de procesamiento.

9.2.4. Pérdida de paquetes (*Packet Loss*)

9.2.4.1. Causas

Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvian. Además la perdida de paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor. Sin embargo la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante óptima. El problema es mayor cuando se producen pérdidas de paquetes en ráfagas.

9.2.4.2. Valores recomendados

La perdida de paquetes máxima admitida para que no se degrade la comunicación deber ser inferior al 1%. Pero es bastante dependiente del códec que se utiliza. Cuanto mayor sea la compresión del codec más pernicioso es el efecto de la pérdida de paquetes. Una pérdida del 1% degrada más la comunicación si se usa el códec G.729 en vez del G.711.

9.2.4.3. Posibles soluciones

Para evitar la pérdida de paquetes una técnica muy eficaz en redes con congestión o de baja velocidad es no transmitir los silencios. Gran parte de las conversaciones están llenas de momentos de silencio. Si solo transmitimos cuando haya información audible liberamos bastante los enlaces y evitamos fenomenos de congestión. De todos modos este fenomeno puede estar también bastante relacionado con el jitter y el jitter buffer.

Sección 10

Guía de instalación con RAID

Esta guía inicia a partir de la consideración de que se ha seleccionado la opción «*Install Denwa UC Manual Partition*», lo cual permite el particionamiento manual de los dispositivos de almacenamiento.

10.1. Definir el tamaño que tendrán las particiones

Al momento de definir el dimensionamiento se deberá tener las siguientes consideraciones:

- Se debe crear al menos las siguientes particiones:
  - «**boot**» en el disco de estado sólido, para los archivos de arranque del sistema
  - «\» en el disco de estado sólido, para el Sistema Operativo base (20GB mínimo, 30GB recomendado), para:
    - Sistema Operativo
    - Logs del sistema
    - Carpetas de usuarios de Sistema Operativo («pbxadmin», «Soporte Denwa»)
    - Archivos de módulos
  - «**swap**» en el disco de estado sólido, se recomienda de 2GB a 8GB según el equipo.
  - «**denwa**» en el disco de estado sólido, para todos los procesos asociados al motor de telefonía
    - Motor de Telefonía
    - Bases de Datos
    - Interfaz Web
    - Grabaciones por transferirse al FTP Server (si lo hubiese)
  - «**persistent**» en el disco mecánico (si lo hubiese) para el almacenamiento local de la grabación de las llamadas

Consultas

Ante duda consulte al área de soporte de Denwa Technology Corp. .

10.2. Creación de las particiones

Como primer paso es necesario crear todas las particiones en formato «ext4» sin declarar su punto de montaje (esto se realizará más adelante). Es necesario que los dispositivos de almacenamiento que participen en las alineaciones RAID se particionen de forma idéntica, asignando el mismo tamaño a cada partición.

1. Seleccionar el disco

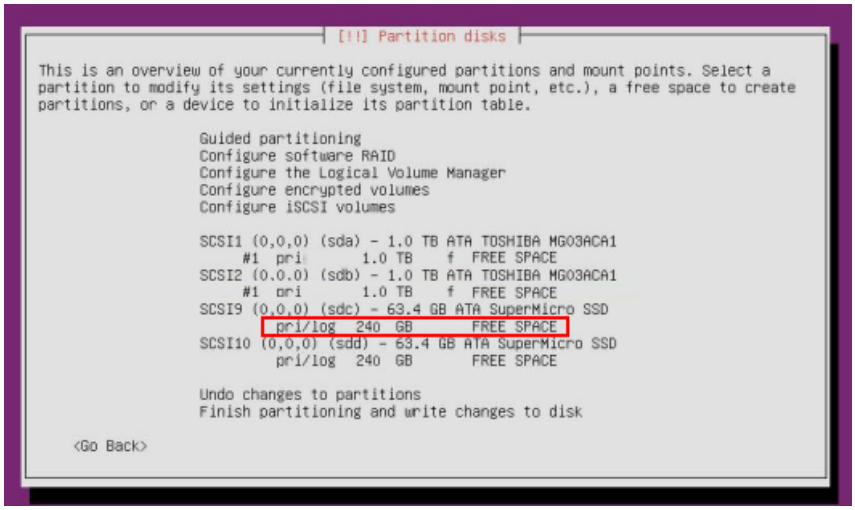

Figura 10.1: Creación de las particiones: selección de disco

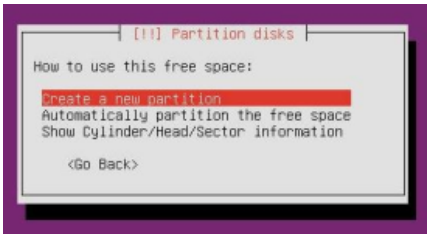

Figura 10.2: Creación de las particiones: crear una nueva partición

2. Asignar tamaño a cada partición

Figura 10.3: Creación de las particiones: dimensionamiento

3. Definir si la partición es primaria o lógica

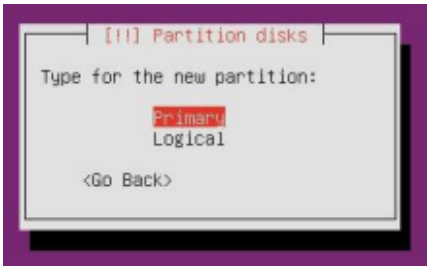

Figura 10.4: Creación de las particiones: tipo de partición

4. Quitar el punto de montaje de todas las particiones y definirlas «ext4», excepto la swap, que deberá definirse como «Swap Area»

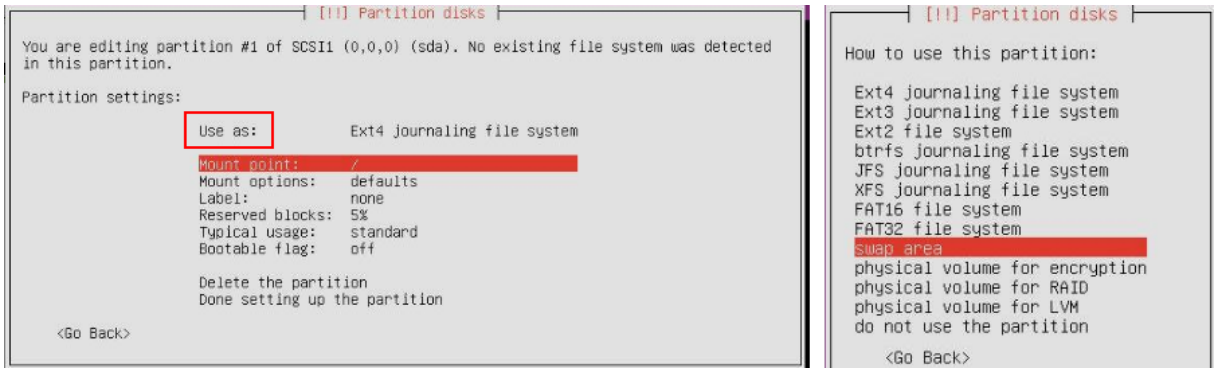

Figura 10.5: Creación de las particiones: formato del sistema de archivos

5. Controlar la igualdad de particiones entre discos

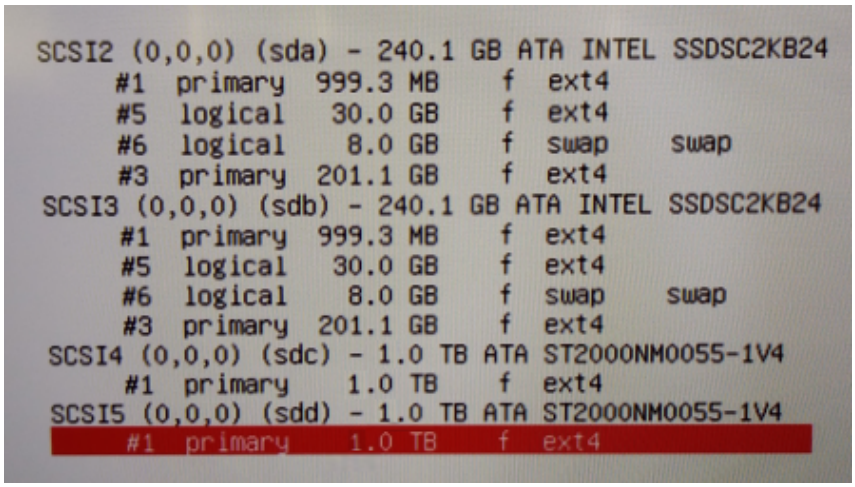

Figura 10.6: Creación de las particiones: comparación de discos

10.3. Configurar el RAID por software

Crear los RAIDs Asigne tipo: RAID1 (espejo) (Unir las particiones idénticas) Confirmar uso de 2 particiones por cada RAID Spare devices: 0

10.4. Configurar los puntos de montaje

10.5. Validación y guardado de configuraciones

Apartado IV

Anexos

Sección 11

Protocolo SIP y Debug

11.1. Componentes y Funcionamiento de una Red VoIP Definición de VoIP

VoIP viene de las palabras en ingles *Voice Over Internet Protocol*. Como dice el término, VoIP intenta permitir que la voz viaje en paquetes IP y obviamente a través de Internet.

La telefonía IP conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y por ende desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, video o cualquier tipo de información.

La VoIP por lo tanto, no es en sí mismo un servicio sino una tecnología que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales conocida como la PSTN, que son redes desarrolladas a lo largo de los años para transmitir las señales vocales.

La PSTN se basaba en el concepto de conmutación de circuitos, es decir, la realización de una comunicación requería el establecimiento de un circuito físico durante el tiempo que dura ésta, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice, incluso durante los silencios que se suceden dentro de una conversación típica.

En cambio, la telefonía IP no utiliza circuitos físicos para la conversación, sino que envía múltiples conversaciones a través del mismo canal (circuito virtual) codificadas en paquetes y en flujos independientes. Cuando se produce un silencio en una conversación, los paquetes de datos de otras conversaciones pueden ser transmitidos por la red, lo que implica un uso más eficiente de la misma.

Según esto, son evidentes las ventajas que proporciona las redes VoIP, ya que con la misma infraestructura podrían prestar mas servicios y además la calidad de servicio y la velocidad serian mayores; pero por otro lado también existe la gran desventaja de la seguridad, ya que no es posible determinar la duración del paquete dentro de la red hasta que este llegue a su destino y además existe la posibilidad de pérdida de paquetes, ya que el protocolo IP no cuenta con esta herramienta.

11.2. Encapsulamiento de una trama VoIP

Una vez que la llamada ha sido establecida, la voz será digitalizada y entonces transmitida a través de la red en tramas IP. Las muestras de voz son primero encapsuladas en RTP (Protocolo de Transporte en tiempo Real) y luego en UDP o TCP antes de ser transmitidas en una trama IP. La siguiente figura muestra un ejemplo de una trama VoIP sobre una red LAN y WAN.

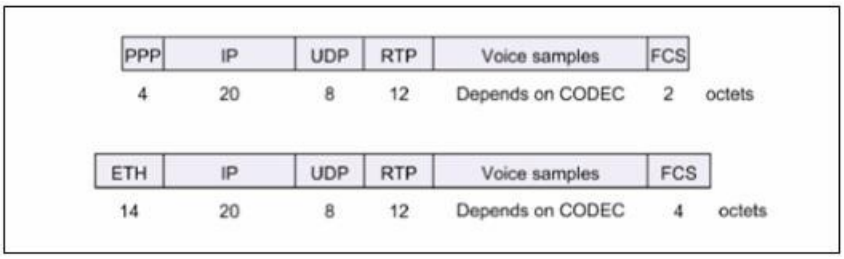

Figura 11.1: Protocolo SIP y Debug: Encapsulamiento

11.3. Session Initiation Protocol

Session Initiation Protocol (SIP o Protocolo de Inicialización de Sesiones) es un protocolo de señalización simple, utilizado para telefonía y videoconferencia por Internet. Basado en el Protocolo de Transporte de correo simple (SMTP) y en el Protocolo de Transferencia Hipertexto (HTTP) fue desarrollado por el IETF MMUSIC Working Group con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual. SIP es uno de los protocolos de señalización para voz sobre IP. SIP es definido completamente en la RFC 2543 y en la RFC 3261.

SIP es un protocolo de la capa de aplicación independiente de los protocolos de paquetes subadyacentes (TCP, UDP, ATM, X.25). SIP esta basado en una arquitectura cliente servidor en la cual los clientes inician las llamadas y los servidores responden las llamadas. Es un protocolo abierto basado en estándares, ampliamente soportado y no es dependiente de un solo fabricante de equipos.

SIP es un protocolo más nuevo que H.323 y no tiene madurez y soporte industrial al mismo tiempo. Sin embargo, por su simplicidad, escalabilidad, modularidad y comodidad con la cual integra con otras aplicaciones, este protocolo es atractivo para uso en arquitecturas de voz paquetizados. SIP puede establecer sesiones de dos partes (llamadas ordinarias), de múltiples partes (en donde todos pueden oír y hablar) y de multidifusión (un emisor, muchos receptores). Las sesiones pueden contener audio, video o datos. SIP solo maneja establecimiento, manejo y terminación de sesiones.

Algunas de las características claves que SIP ofrece son:

- Resolución de direcciones, mapeo de nombres y redirección de llamadas.
- Descubrimiento dinámico de las capacidades media del endpoint, por uso del Protocolo de Descripción de Sesión (SDP).
- Descubrimiento dinámico de la disponibilidad del endpoint.
- Origen y administración de la sesión entre el host y los endpoints.

11.3.1. Beneficios de SIP

Algunos de los beneficios claves de SIP son:

- **Simplicidad**: SIP es un protocolo muy simple. El tiempo de desarrollo del software es muy corto comparado con los productos de telefonía tradicional. Debido a la similitud de SIP a HTTP y SMTP, el rehúso de código es posible.
- **Extensibilidad**: SIP ha aprendido de HTTP y SMTP y ha construido un exquisito grupo de funciones de extensibilidad y compatibilidad.
- **Modularidad**: SIP fue diseñado para ser altamente modular. Una característica clave es su uso independiente de protocolos. Por ejemplo, envía invitaciones a las partes de la llamada, independiente de la sesión misma.
- **Escalabilidad**: SIP ofrece dos servicios de escalabilidad:

- **Procesamiento de servidor**: SIP tiene la habilidad para ser *Stateful* o *Stateless*.
- **Arreglo de la conferencia**: puesto que no hay requerimiento para un controlador central multipunto, la coordinación de la conferencia puede ser completamente distribuida o centralizada.
- **Integración**: SIP tienen la capacidad para integrarse con la Web, E-mail, aplicaciones de flujo multimedia y otros protocolos.
- **Interoperabilidad**: porque es un estándar abierto, SIP puede ofrecer interoperabilidad entre plataformas de diferentes fabricantes.

11.3.2. Diseño del protocolo

SIP es un protocolo de capa de aplicación y puede ejecutarse sobre UDP o TCP.

Los clientes SIP usan el puerto 5060 en TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*) para conectar con los servidores SIP, en caso de utilizar un protocolo seguro como SIPS el puerto a utilizar es el 5061, este punto se analizará más adelante cuando hablemos de TLS (*Transport Security Protocol*).

SIP es usado simplemente para iniciar y terminar llamadas de voz y video. Todas las comunicaciones de voz/video van sobre RTP (*Real-time Transport Protocol*).

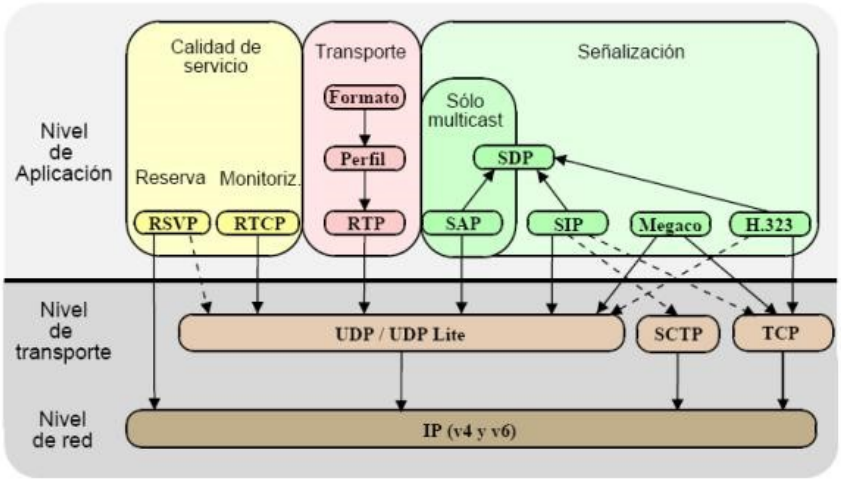

Figura 11.2: Protocolo SIP y Debug: Diseño

La primera versión propuesta para estándar (SIP 2.0) fue definida en el RFC 2543. El protocolo aclarado en el RFC 3261, aunque muchas implementaciones están usando todavía versiones en fase de borrador. Hay que fijarse en que el número de versión sigue siendo 2.0.

11.3.3. Capa de transporte en SIP

SIP puede utilizar en su capa de transporte (Nivel 4 en el modelo OSI) tanto UDP, TCP como TLS *Transport Layer Security* (refiriéndonos a TLS sobre TCP). TLS es utilizado para dar un cierto nivel de seguridad, encriptando la información que usualmente es vulnerable a ataques ya que se envía en texto plano.

La utilización de SIP sobre TCP sin encriptación está tendiendo a desaparecer en usos no pagos o de VoIP en Internet debido a la sencillez de UDP, la creciente confiabilidad de las redes y a la inútil necesidad de retransmisión en una conexión de voz o de media donde esta presente la transmisión en tiempo real.

De todas maneras es importante que un Agente Usuario (UA) de alto rendimiento como un sipphone por ejemplo, soporte tanto TCP como UDP como protocolos de transporte, ya que si un UA trata de establecer una sesión TCP con su par, y esté no soporta TCP en su capa de transporte, la sesión no se podrá establecer desembocando en un mensaje ICMP de "Not Supported.º un reset de la conexión TCP, donde el extremo llamante deberá cambiar el

protocolo de transporte de su mensaje de pedido sobre UDP para crear compatibilidad en la red y establecer la conexión. Siendo el caso más óptimo la compatibilidad al primer intento para aprovechar la capacidad y recursos de la red.

Otro punto crucial en el momento de decidir el protocolo que se utilizará en la capa de transporte es el tamaño máximo de segmento, el cual está involucrado directamente con el codec a utilizar, tomando en cuenta la notable diferencia de compresiones entre, por ejemplo, G.729, G.711, etc. En la RFC 3261 está definido el uso de UDP y TCP obligatoriamente, este último en caso de ser necesario algún tipo de fragmentación del paquete que exceda la MTU.

La negociación de codecs, puertos y serivicios multimedia se realiza en el protocolo SDP (Session Description Protocol) embebido en SIP, donde c omúnmente los puertos utilizados de SIP son el 5060 en texto plano (UDP y TCP) y el puerto 5061 en caso de TLS. Sin embargo, en la práctica se puede presentar el uso de puertos comprendidos entre el 5060 hasta el 5070.

11.3.4. Elementos SIP de red

Los terminales físicos conocidos como agentes usuarios (UA) pueden ser dispositivos en sí o softwares instalados en una PC, con el aspecto y/o funcionalidad de teléfonos tradicionales, pero que usan SIP y RTP para la comunicación. Están disponibles comercialmente gracias a muchos fabricantes. Algunos de ellos usan numeración electrónica (ENUM) o DUNDi para traducir los números existentes de teléfono a direcciones SIP usando DNS (*Domain Name Server*), así llaman a otros usuarios SIP saltándose la red telefónica, con lo que el proveedor de servicio normalmente actúa de pasarela hacia la red pública conmutada de telefonía para los números de teléfono tradicionales (cobrando por ello).

SIP hace uso de elementos llamados servidores proxy para ayudar a enrutar las peticiones hacia la localización actual del usuario, autenticar y autorizar usuarios para darles servicio, posibilitar la implementación de políticas de enrutamiento de llamadas, y aportar capacidades añadidas al usuario. También aporta funciones de registro que permiten al usuario informar de su localización actual a los servidores proxy.

Aunque dos terminales SIP puedan comunicarse sin intervención de infraestructuras SIP (razón por la que el protocolo se define como punto-a-punto), este enfoque es impracticable para un servicio público. Hay varios implementaciones de softswitch (de Nortell, Sonus, Huawei y muchas más) que pueden actuar como proxy y elementos de registro. Otras empresas, como Ubiquity Software y Dynamicsoft tienen productos cuya implementación está basada en estándares, construidos sobre la especificación Java JAIN.

11.3.5. Mensajes del protocolo SIP

11.3.5.1. Direcciones SIP

SIP trabaja en una premisa simple de operación cliente servidor. Los clientes o endpoints son identificados por direcciones únicas definidas como URL's, es decir las direcciones vienen en un formato muy similar a una dirección de correo electrónico, a fin de que las paginas Web puedan contenerlos, lo que permite hacer click en un vinculo para iniciar una llamada telefónica.

- Las direcciones SIP siempre tienen el formato de user@host.
- El user puede ser: nombre, número telefónico.
- El host puede ser: dominio (DNS), dirección de red (IP). b) MENSAJES SIP:

SIP usa mensajes para la conexión y control de llamadas. Hay dos tipos de mensajes SIP: mensajes de peticiones y respuestas. Los mensajes SIP son definidos como sigue:

- **INVITE**: Solicita el inicio de una llamada. Los campos de la cabecera contienen:
    - Dirección origen y dirección destino.
    - El asunto de la llamada.

- Prioridad de la llamada.
- Peticiones de enrutamiento de llamada.
- Preferencias para la ubicación de usuario.

- **TRYING**: Indica que el servidor Proxy esta tratando de establecer la comunicación.
- **RINGING**: Indicación de aviso de llamado.
- **BYE**: Solicita la terminación de una llamada entre dos usuarios.
- **REGISTER**: Informa a un servidor de registro sobre la ubicación actual del usuario.
- **ACK**: Usado para facilitar un intercambio confiable de mensajes entre los pares. Confirmación de diferentes campos del mensaje INVITE.
- **CANCEL**: Cancela una solicitud pendiente.
- **OPTIONS**: Solicita información a una Host acerca de sus propias capacidades. Se utiliza antes de iniciar la llamada a fin de averiguar si ese host tiene la capacidad de transmitir VoIP, etc.
- **200 OK**: Sirve para enviar confirmaciones satisfactorias de diferentes sucesos.
- **INFO**: Usada para señalización de sesiones de media.

11.3.5.2. Llamada de PC a PC sobre TCP

Para establecer una llamada, el llamante crea una conexión TCP con el llamado. La conexión se realiza utilizando un acuerdo de tres vías.

- Envía un mensaje INVITE en un paquete TCP, indicando la dirección de destino, la capacidad, los tipos de medios y los formatos del llamante.
- Si el llamado acepta la llamada, responde con un código de respuesta tipo HTTP (200 para aceptación). Opcionalmente también puede proporcionar información sobre sus capacidades, tipos de medios y formatos.
- El llamante responde con un mensaje ACK para terminar el protocolo y confirmar la recepción del mensaje 200.
- En este punto, pueden comenzar el flujo de datos utilizando el protocolo RTP.
- El flujo de datos se controla mediante el protocolo RTCP.
- Cualquiera puede solicitar la terminación de la llamada enviando un mensaje BYE.
- Cuando el otro lado confirma su recepción, se termina la llamada.

11.3.6. SIP llamadas y transacciones

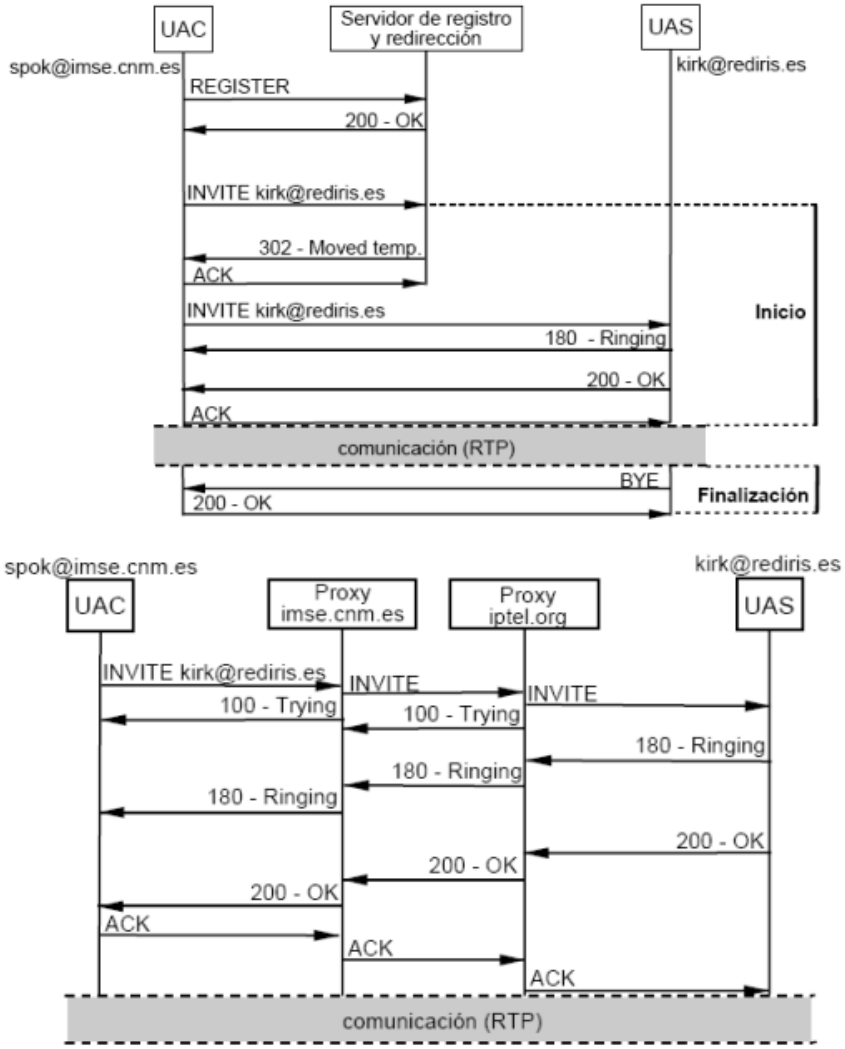

Figura 11.3: Protocolo SIP y Debug: Transacciones

11.3.6.1. Real-time Transport Protocol

RTP son las siglas de ***R****eal-time* ***T****ransport* ***P****rotocol* (Protocolo de Transporte de Tiempo Real), UDP en los puertos del 10000 al 20000. Es un protocolo de nivel de aplicación (no de nivel de transporte, como su nombre podría hacer pensar) utilizado para la transmisión de información en tiempo real, como por ejemplo audio y video.

Está desarrollado por el grupo de trabajo de transporte de Audio y Video del IETF, publicado por primera vez como estándar en 1996 como la RFC 1889, y actualizado posteriormente en 2003 en la RFC 3550, que constituye el estándar de Internet STD 64. Inicialmente se publicó como protocolo multicast, aunque se ha usado en varias aplicaciones unicast. Se usa frecuentemente en sistemas de streaming, junto a RTSP, videoconferencia y sistemas push to talk (en conjunción con H.323 o SIP). Representa también la base de la industria de VoIP.

La RFC 1890, obsoleta por la RFC 3551 (STD 65), define un perfil para conferencias de audio y vídeo con control mínimo. LaRFC 3711, por otro lado, define SRTP (Secure Real-time Transport Protocol), una extensión del perfil de RTP para conferencias de audio y vídeo que puede usarse opcionalmente para proporcionar confidencialidad, autenticación de mensajes y protección de reenvío para flujos de audio y vídeo. Va de la mano de RTCP (RTP Control Protocol) y se sitúa sobre UDP en el modelo OSI.

Bits		0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Byte	0	V			P	X		CC			M			PT								Sequence Number											
	5	Timestamp																															
	9	Synchronization Source (SSRC)																															
	13	Content Source (CSRC)																															
	17																																
	21																																
	n-4																																
	n																																

11.3.6.1.1. Estructura del encabezado RTP

- **V** (Número de versión): 2 bits. La versión definida por la especificación actual es 2.
- **P** (Relleno): 1 bit. Si el bit del relleno está colocado, hay uno o más bytes al final del paquete que no es parte de la carga útil. El byte más último en el paquete indica el número de bytes de relleno. El relleno es usado por algunos algoritmos de encriptación.
- **X** (Extensión): 1 bit. Si el bit de extensión está colocado, entonces el encabezado fijo es seguido por una extensión del encabezado. Este mecanismo de la extensión posibilita implementaciones para añadir información al encabezado RTP.
- **CC** (Conteo CSRC): 4 bits. El número de identificadores CSRC que sigue el encabezado fijo. Si la cuenta CSRC es cero, entonces la fuente de sincronización es la fuente de la carga útil.
- **M** (Marcador): 1 bit. Un bit de marcador definido por el perfil particular de media.
- **PT** (Carga útil): 7 bits. Un índice en una tabla de perfiles de media que describe el formato de carga útil. Los mapeos de carga útil para audio y video están especificados en el RFC 1890.
- **Sequence Number** (Número de secuencia): 16 bits. Un único número de paquete que identifica la posición de este en la secuencia de paquetes. El número del paquete es incrementado en uno para cada paquete enviado.
- **Timestamp** (Marca temporal): 32 bits. Refleja el instante de muestreo del primer byte en la carga útil.Varios paquetes consecutivos pueden tener el mismo timestamp si son lógicamente generados en el mismo tiempo - por ejemplo, si son todo parte del mismo frame de video.
- **Synchronization Source (SSRC)**: 32 bits. Identifica la fuente de sincronización. Si la cuenta CSRC es cero, entonces la fuente de carga útil es la fuente de sincronización. Si la cuenta CSRC es distinta a cero, entonces el SSRC identifica el mixer (mezclador).
- **Content Source (CSRC)**: 32 bits cada uno. Identifica las fuentes contribuyentes para la carga útil. El número de fuentes contribuyentes está indicado por el campo de la cuenta CSRC; Allí puede haber más de 16 fuentes contribuyentes. Si hay fuentes contribuyentes múltiples, entonces la carga útil son los datos mezclados de esas fuentes.

11.4. Detección de problemas

11.4.1. Objetivos

- Alcance del protocolo SIP y su funcionamiento.
- Análisis del paquete IP, capa de red, capa de transporte y capa de aplicación (SIP). Análisis del establecimiento de una llamada. (SDP, etc.)
- Mensajes del protocolo SIP:
  - INVITE
  - Trying
  - Ringing

- 200 ok
- BYE
- REGISTER
- ACK
- CANCEL
- OPTIONS

- Verificar en los ensayos realizados el funcionamiento del protocolo.

11.4.2. Maqueta

En el siguiente gráfico podemos observar el diagrama de la maqueta utilizada para realizar las capturas.

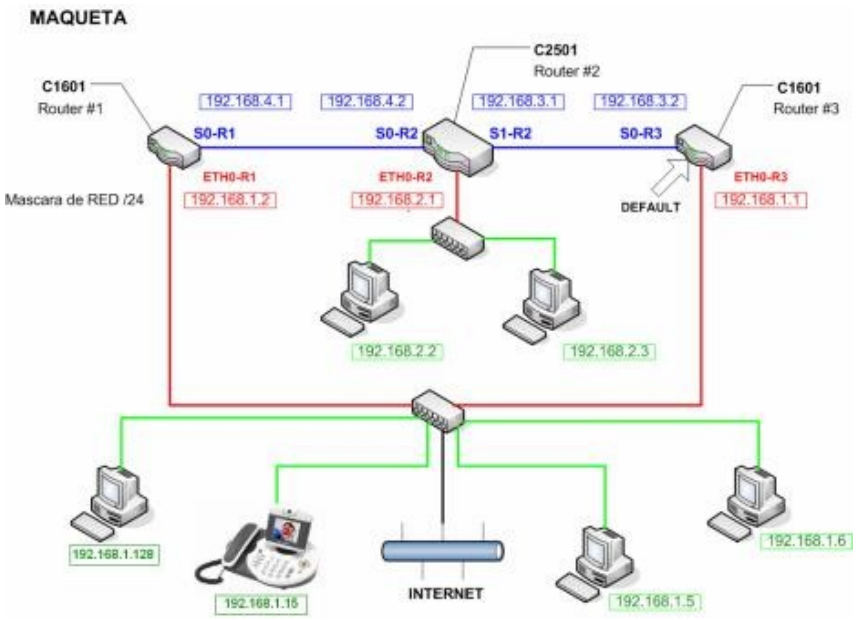

Figura 11.4: Protocolo SIP y Debug: Maqueta

11.4.3. Escenarios

11.4.3.1. Llamada exitosa desde el softphone al videophone

11.4.3.1.1. Objetivo Observar y analizar el establecimiento, transcurso y desconexión de una comunicación con ambos equipos disponibles.

11.4.3.1.2. Desarrollo Para lograr el objetivo planteado se configuró el softphone en modo peer to peer, esto es debido a que las pruebas realizadas fueron dentro de una misma red sin la intervención de un SIP proxy. Esta configuración se debe a que el dispositivo debería estar registrado a un Proxy (en este caso el teléfono SIP) para realizar o recibir llamadas. La dirección IP configurada en la PC en la cual se instaló el Eyebeam era 192.168.1.128, como luego se verá en la captura es quien inicia la comunicación. Los puertos configurados en el software fueron del 5060 al 5062 y los codecs habilitados eran G.711, G.729, etc.

Figura 11.5: Protocolo SIP y Debug: Softphone

La configuración en el videophone fue básicamente la asignación de la dirección IP 192.168.1.15, en forma estática. Los codecs no son configurables en el teléfono utilizado, el único codec que soporta es G.711 A-law. Además, para realizar comunicaciones internas a la red el dispositivo no debe estar registrado en ningún Proxy.

11.4.3.1.3. Ejecución Para realizar la prueba se generó una llamada a la dirección IP del teléfono SIP desde el eyebeam. Cuando se detectó la llamada entrante fue aceptada. Luego de unos segundos desde el softphone se finalizó la llamada. El siguiente gráfico muestra el intercambio de mensajes en la captura realizada desde la PC en que se encontraba el softphone.

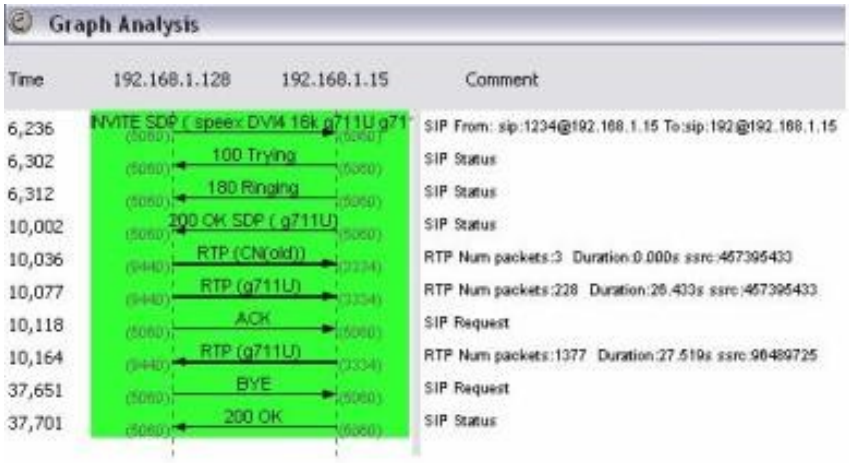

Figura 11.6: Protocolo SIP y Debug: Flujo

Como se puede apreciar, la comunicación sigue el intercambio teórico de mensaje antes mencionados. El establecimiento de la llamada comienza con un mensaje Invite por parte del softphone, donde se envía encapsulado sobre SIP, un mensaje de SDP (session description protocol), con el fin de negociar codec, puertos, etc. En la siguiente captura se analizará

este protocolo más detalladamente. Luego el siguiente mensaje es un Trying enviado por el teléfono sip en respuesta al Invite recibido, luego en el mismo sentido se envía un mensaje de Ringing, para confirmar que se está dando aviso de la llamada entrante. Al aceptar la comunicación (simplemente levantando el tubo en el videoteléfono) éste envía un mensaje de 200 OK con un mensaje de SDP, encapsulado sobre sip, proponiendo codec a utilizarse (G.711 U-Law). A continuación se envían paquetes RTP (real-time transport protocol), con payload Comfort noise, este paquete sirve para ahorrar ancho de banda durante los silencios de voz, emulando un ruido en el otro extremo, para que el usuario no tenga la sensación de interrupción de la comunicación al existir silencios.

El teléfono sip confirma la negociación con un mensaje ACK y luego comienza el intercambio de audio por medio de RTP el protocolo que se utiliza para el intercambio de media, en este sentido es importante aclarar que sip es el protocolo utilizado para la señalización y en esta etapa de la comunicación no aparece. Finalmente se termina la comunicación desde el lado del softphone y envía un mensaje BYE de sip, al cual el otro extremo responde con un 200 ok para confirmar el fin del llamado.

El análisis comienza con el primer mensaje enviado que es el llamado INVITE, a continuación se muestra la captura del paquete correspondiente:

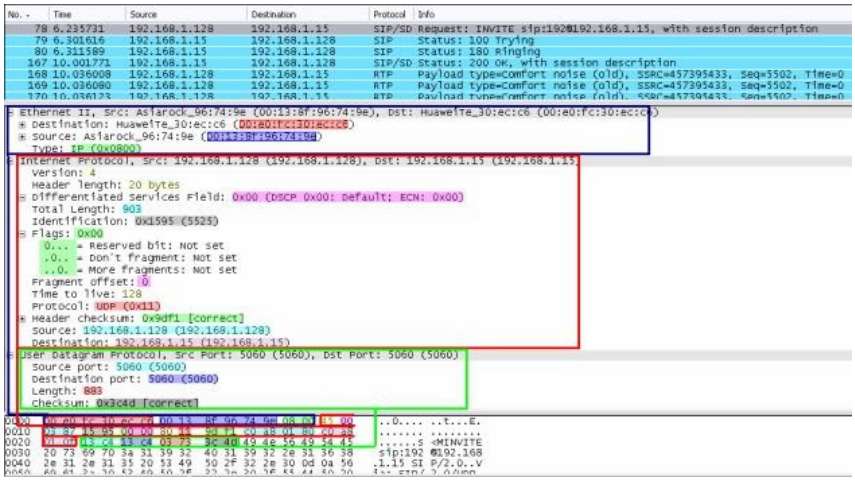

Figura 11.7: Protocolo SIP y Debug: Captura de Paquetes

Aquí se ve en el recuadro superior de color azul el encabezado a nivel de capa de enlace, recordemos su estructura:

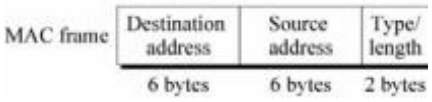

Figura 11.8: Protocolo SIP y Debug: Encabezado en capa de enlace

Como se ver en la captura el protocolo utilizado es Ethernet, por lo tanto el tercer campo indica a que protocolo corresponde el próximo header. En el caso de ser 802.3 este campo refleja la longitud del campo de Data real. Decimos real porque 802.3 se encarga de controlar la longitud mínima de trama, rellenando si hace falta el campo de Data. Por eso es necesario indicar la longitud real del campo de Data, para poder descartar el relleno si lo hubo. Si este campo tiene un valor mayor a 1536 se trata de Ethernet, de otra forma estaríamos hablando de 802.3.

Es posible ver la dirección MAC de destino remarcada en rojo: 00:e0:fc:30:ec:c6, donde los primeros 24 bits indican el fabricante del dispositivo, en este caso sería HuaweiTe_30:ec:c6, por ser Huawei Tecnologies el fabricante.

La dirección MAC de origen remarcada en azul es: 00:13:8f:96:74:9e (Asiarock_96:74:9e), donde Asiarock es el fabricante de la placa de red de la pc en la cual se instaló el software. Luego en el siguiente campo, remarcado en verde, podemos ver que el protocolo de red que encapsula es ip.

A continuación se analiza el header de Ip recuadrado en color rojo en la captura anterior. La estructura del encabezado de ip es la siguiente:

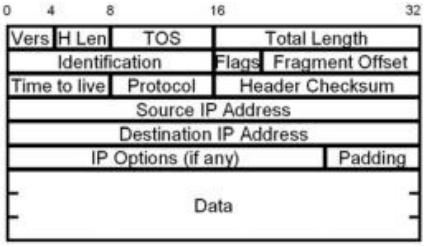

Figura 11.9: Protocolo SIP y Debug: Encabezado IP

- En este caso podemos ver que se trata de un datagrama de Ip versión 4 y de una longitud de 20 bytes (campos remarcados en amarillo), es importante aclarar que el valor de este último campo corresponde a palabras de 32 bits, por lo tanto el valor que aparece es 5. Es decir 5 x 32 bits=160 bits=20 Bytes, a partir de este valor podemos inferir que se trata de un datagrama sin opciones, de otra manera el encabezado tendría un tamaño mayor a 20 Bytes.

- A continuación vemos que el campo de Type of Service (remarcado en lila) tiene un valor nulo, no se hace ninguna distinción para este datagrama en cuanto a confiabilidad, prioridad, retardo o throughput.

- El siguiente campo (resaltado en celeste) es el tamaño total del datagrama que tiene un valor de 903 Bytes.

- Luego el campo de identificación (en gris) del paquete muestra un valor de 5525 que sirve para distinguirlo de otros paquetes, esto es necesario para identificar los fragmentos correspondientes a un datagrama que ha sido fragmentado.

- Vemos que el campo de flags (en verde) tiene un valor nulo, es decir que el datagrama puede ser fragmentado (Don´t fragment=0) y que o bien no ha sido fragmentado o es el último fragmento.

- Luego el siguiente campo de fragment offset (en lila) se encuentra en cero, esto quiere decir que es el primer fragmento o no ha sido fragmentado. Por éstos dos últimos valores inferimos que el datagrama no fue fragmentado.

- El campo de Time to Live (en amarillo) tiene un valor de 128, es decir que este paquete podría atravesar 128 redes como máximo hasta llegar a destino, éste valor se decrementa por cada salto, si éste llegara a 1, se descartaría el paquete.

- El próximo campo indica el protocolo que contiene el payload, aquí se ve que el protocolo utilizado en la capa de transporte es UDP, el valor es de 9 para este protocolo.

- A continuación tenemos el checksum (en verde), que sirve para control de errores del header, en este caso vemos que el encabezado no contiene errores.

- Los siguientes campos son las direcciones ip de fuente y destino respectivamente. En este caso se tiene que 192.168.1.128 es quien generó el datagrama y 192.168.1.15 es el destino de dicho datagrama. (en celeste y gris respectivamente)

El análisis continúa con el próximo encabezado, el de transporte, que en este caso como se dijo anteriormente se utilizará UDP. Recordemos su estructura.

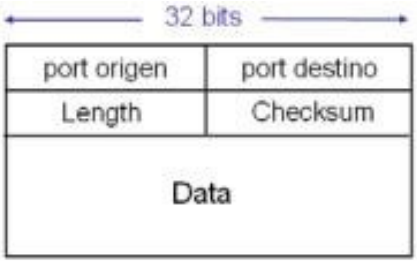

Figura 11.10: Protocolo SIP y Debug: Encabezado de transporte

- El primer campo indica el puerto origen, en este caso por tratarse de sip era esperable que sea 5060 al igual que el puerto de destino (remarcados en celeste y azul respectivamente).
- Luego vemos que el campo siguiente (en rojo) es el que indica el tamaño del segmento UDP incluyendo el header, como era de esperar tiene un valor de 883 Bytes, 20 Bytes menos que del datagrama, el tamaño del header de éste.
- Y por último (en gris) tenemos el checksum del segmento, este es opcional y cuando no se lo calcula, este campo se pone en cero. Aquí vemos que se ha utilizado y no hubo errores.

En la capa de aplicación tenemos el mensaje encapsulado en sip y sus protocolos dependientes, en los próximos escenarios se analizarán estos protocolos más detalladamente.

El próximo mensaje que se envía en respuesta al INVITE anterior es un TRYING, a continuación podemos ver la captura:

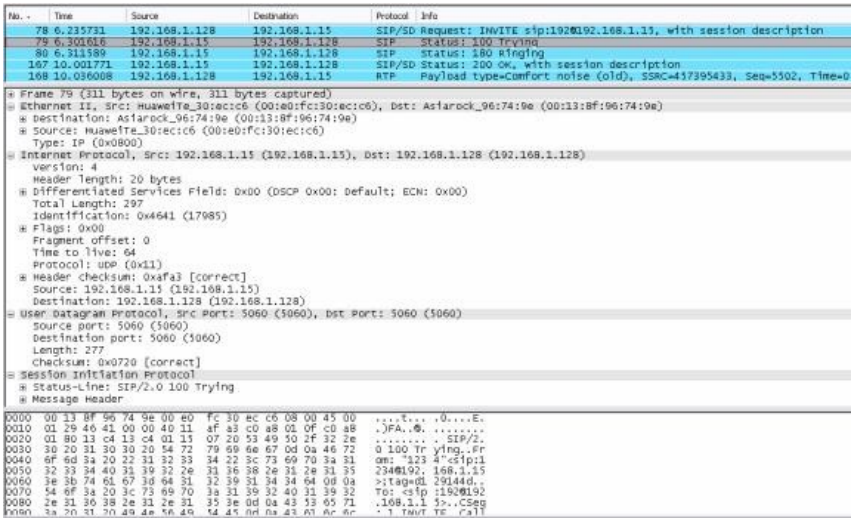

Figura 11.11: Protocolo SIP y Debug: TRYING

El análisis de este mensaje es muy similar al anterior, sólo se indicarán las diferencias más importantes en cada nivel.

A nivel de enlace podemos ver que los campos de direcciones mac se invierten dado que la trama es enviada en sentido inverso, desde el videoteléfono hacia el softphone. Otra vez en el campo de type vemos que se tiene IP como próximo header.

A nivel de red se ve también que las direcciones ip han sido invertidas al igual que las mac. Como diferencia más importante podemos ver que el tamaño del datagrama disminuyó dado que este mensaje no encapsula ningún protocolo auxiliar.

En cuanto al encabezado de UDP, se puede comprobar nuevamente que difiere en 20 bytes respecto al de IP.

Luego se comprueba que el mensaje a nivel de aplicación es el TRYING antes mencionado.

El próximo mensaje es el RINGING, podemos ver su captura, aquí es importante tener en cuenta que el sentido de este datagrama es el mismo que el anterior (trying), coincidiendo con lo que se anticipó en forma teórica.

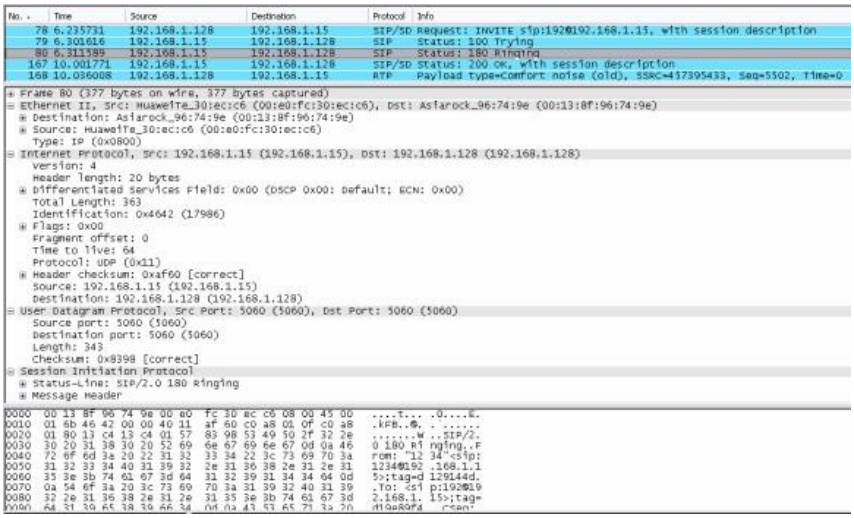

Figura 11.12: Protocolo SIP y Debug: RINGING

Aquí se verifica en los campos de direcciones mac e ip que el sentido del mensaje es otra vez desde el teléfono sip hacia el eyebeam. A nivel de aplicación podemos comprobar que se trata de un mensaje ringing.

El siguiente mensaje es un 200 OK, enviado desde el softphone. La captura se muestra a continuación:

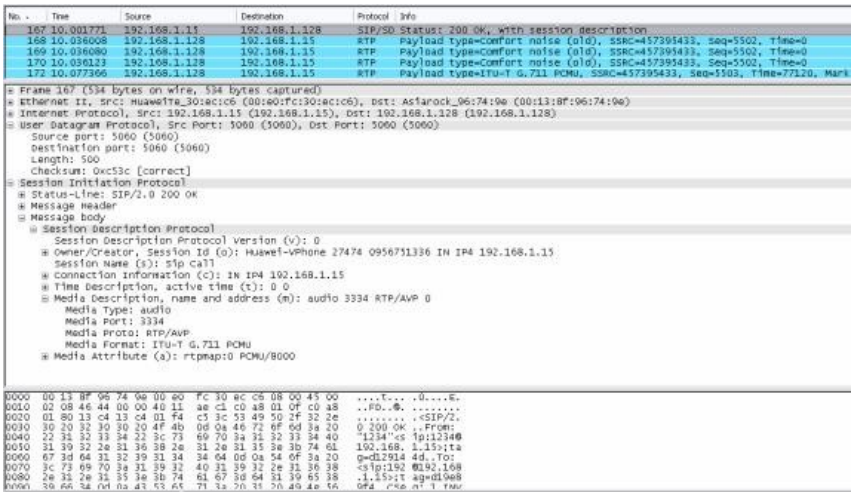

Figura 11.13: Protocolo SIP y Debug: 200 OK

Este mensaje tiene la función de confirmar la aceptación del llamado.

Aquí se ve que se encuentra un mensaje de SDP encapsulado en SIP con el fin de confirmar el codec que será utilizado en la comunicación. En este caso se confirma G.711 U-Law como anticipamos anteriormente. Esto será analizado detalladamente más adelante.

Los siguientes mensajes son de RTP, el primero contiene un mensaje de Comfort Noise, esto sirve para acomodar los parámetros de los filtros FIR que emularán un leve ruido al detectar silencios para confort del usuario. Aquí se ve este tipo de mensaje dado el codec que se está utilizando, G.711 no viene por default con esta opción, por lo tanto se realiza esta facilitie.

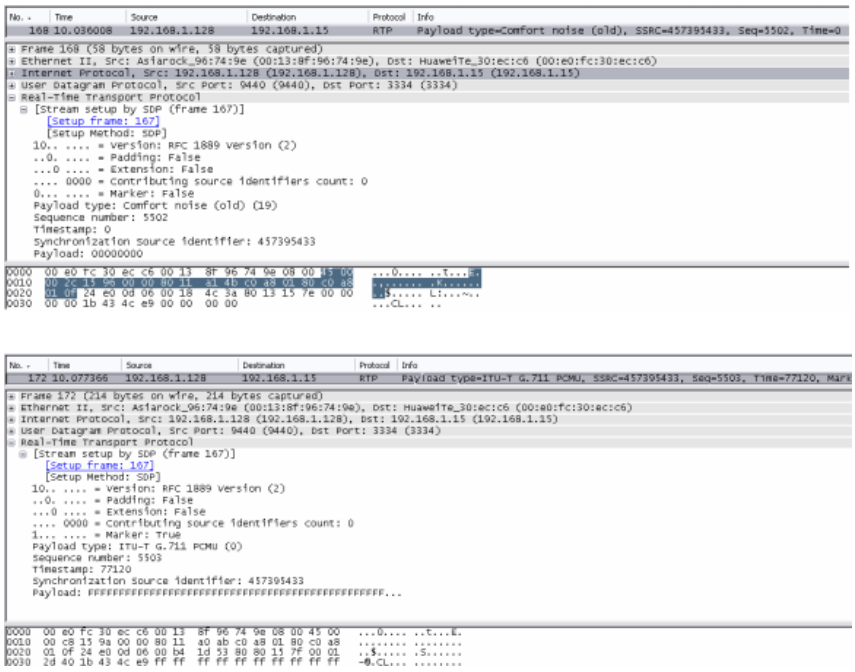

Figura 11.14: Protocolo SIP y Debug: RTP

El siguiente mensaje es enviado desde el soft al videoteléfono y se trata de un ACK, cuya función es confirmar diferentes valores de los campos enviados en el mensaje INVITE. Veamos a continuación como estos campos coinciden en ambos mensajes.

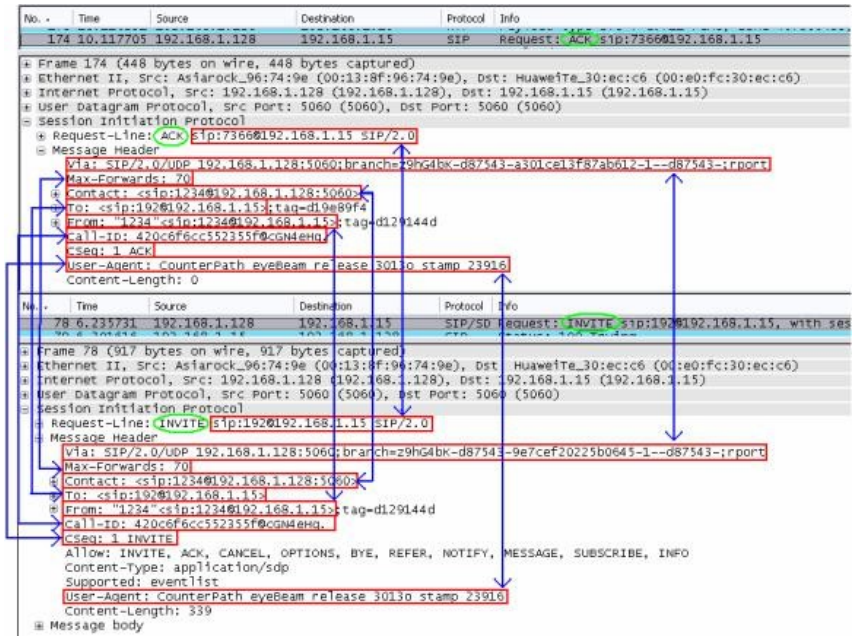

Figura 11.15: Protocolo SIP y Debug: ACK

A partir de ahora comienza el intercambio de audio sobre RTP. Como se ve en el primer gráfico del intercambio de mensajes, sólo hay paquetes desde el videoteléfono hacia el softphone, esto se debe a que en el momento de efectuar las capturas no disponíamos de un micrófono en la pc, por lo tanto no se enviaron paquetes en este sentido. A continuación se muestra sólo un paquete de RTP a modo de ejemplo.

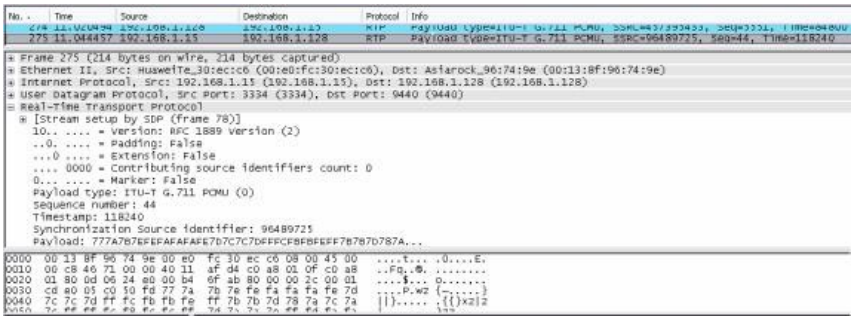

Figura 11.16: Protocolo SIP y Debug: Audio sobre RTP

En este ejemplo se finalizó la comunicación desde el softphone. Aquí se ve, dado que es ese extremo quien envía el mensaje BYE. A continuación podemos apreciar la captura de este paquete.

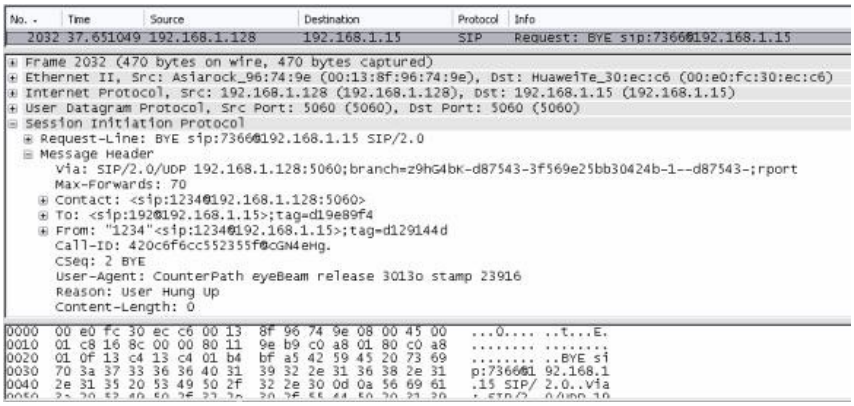

Figura 11.17: Protocolo SIP y Debug: Solicitud de corte

Como se vio anteriormente este mensaje notifica la terminación de una llamada. Del otro extremo este mensaje es contestado con un 200 OK confirmando el término de la llamada.

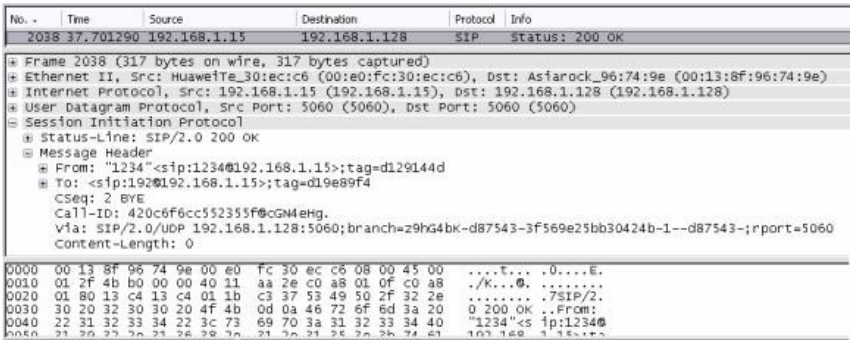

Figura 11.18: Protocolo SIP y Debug: Confirmación de corte

Para finalizar con este escenario podemos concluir que se cumplió con el marco teórico presentado anteriormente. La comunicación se estableció dentro de los parámetros normales, exitosamente. No se encontraron mensajes no esperados. Los campos de nivel de enlace, red y transporte que fueron analizados en cada caso coincidieron con los resultados esperados.

11.4.3.2. Llamada exitosa desde el videophone al softphone

11.4.3.2.1. Objetivo Observar y analizar el establecimiento, transcurso y desconexión de una comunicación con ambos equipos disponibles, así como notar diferencias con el caso

anterior.

11.4.3.2.2. Ejecución El escenario en este caso es el siguiente:

1. El usuario A (teléfono Huawei) llama al usuario B (softphone).
2. Luego de dejar sonar el Softphone, la llamada es atendida.
3. Se espera algunos segundos. El usuario B finaliza la llamada.

La siguiente figura muestra el flujo de dicha llamada:

Figura 11.19: Protocolo SIP y Debug: Flujo de la llamada

11.4.3.2.2.1. Invite La llamada es iniciada por el Usuario A, utilizando el método INVITE. Es interesante ver los bytes del mensaje como son presentados por el ethereal:

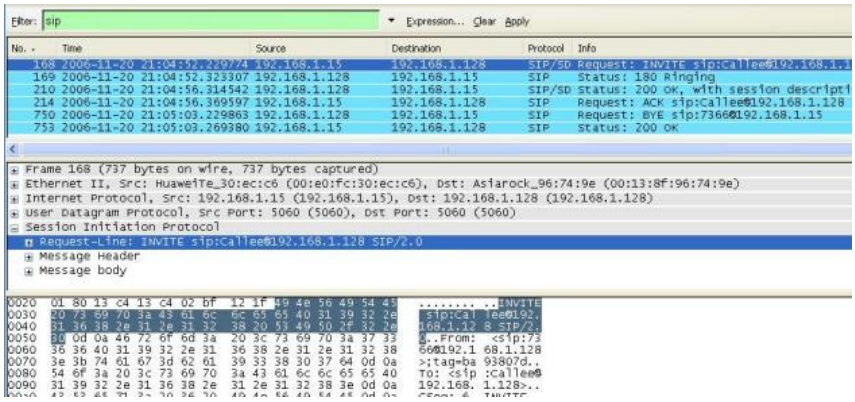

Figura 11.20: Protocolo SIP y Debug: INVITE

Se puede ver que el mensaje se encuentra codificado en ASCII, lo que facilita la decodificación por parte de los usuarios y administradores. El costo de enviar los mensajes en texto plano es un mayor uso de ancho de banda, pero como veremos a continuación, la señalización en condiciones normales, requiere pocos mensajes para establecer la llamada.

Como puede verse en la figura, se identifican 3 segmentos dentro del mensaje INVITE:

- **Request Line**: En esta sección del mensaje se puede ver principalmente el Método de SIP utilizado (INVITE, TRYING, etc.) y la versión de SIP. A diferencia de H.323, SIP no asegura retrocompatibilidad entre las versiones, por lo que podría ser que un método soportado en 1.0 no se siga usando en una versión posterior.

  En el caso del mensaje INVITE, se puede ver el destinatario (TO) del mensaje:[|mailto:Callee@192.168.1.128]Callee@192.168.1.128

```
Request Line: INVITE sip:Callee@192.168.1.128 SIP/2.0
```

- **Message Header**: El header de SIP se puede ver en la siguiente figura:

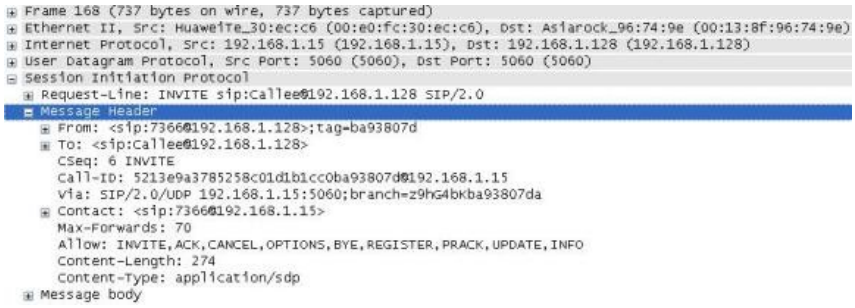

Figura 11.21: Protocolo SIP y Debug: SIP Header

El encabezado de SIP esta conformado por los siguientes campos delimitados por ASCII 13-10 (CR-CF):

- **From**: El campo FROM es el identificador lógico del User Agent que genera el pedido (UA Client). Esta compuesto por el URI (Uniform Resource Identificator) y opcionalmente el parámetro DISPLAY Name, el cual es el nombre que se presentara si el usuario tiene el servicio de caller ID activo. Adicionalmente, dentro del FROM se encuentra el parámetro TAG, el cual es un identificador generado por el user agent client en el momento de hacer el pedido. Este identificador, junto con el parámetro con el identificador de la llamada (Call-ID), sirven para identificar el dialogo entre el User Agent Client y el User Agent Server (UAS).

  En la siguiente figura se puede observar el campo FROM capturado, dentro del INVITE:

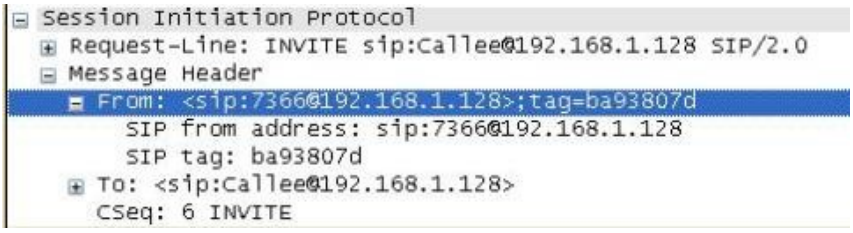

Figura 11.22: Protocolo SIP y Debug: Campo FROM

  Es interesante notar que en este caso el URI: 7366@192.168.1.128 esta utilizando el identificador del Videophone (7366), pero la IP que se utilizó para formar dicho mensaje es la del softphone. Esto es porque los UAC conforman el URI utilizando la IP del SIP- Proxy, y en este escenario, como se configuro el terminal para trabajar en modo peer to peer, se utiliza la ip del destinatario.

  El tag que se generó para establecer este diálogo es: **ba93807d**.

- **To**: En el campo TO se indica el destinatario lógico del pedido. El UAC genera el campo TO a partir de lo ingresado por el usuario del videophone. En este caso, la llamada se generó marcando la IP del destino, por lo que el UAC cliente generó el URI automáticamente:

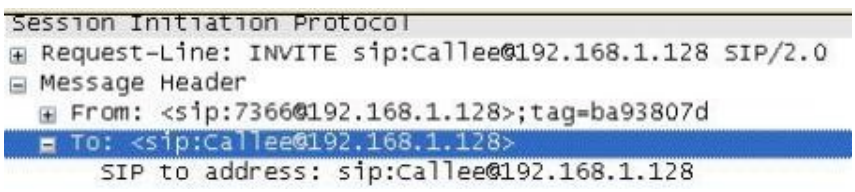

Figura 11.23: Protocolo SIP y Debug: Campo TO

El URI generado automáticamente utiliza el string Çallee@<IP marcada>". Notar que dentro del TO no se está utilizando el TAG.

- **CSeq**: Este parámetro define el orden de las transacciones. Consiste de un número de secuencia y de un método. Este número de secuencia se va incrementando de a 1 por vez. En el caso de esta captura, este parámetro tiene el valor: CSeq: 6 INVITE. El método utilizado para conformar el CSeq debe ser el mismo método utilizado para generar el diálogo.
- **Call-ID**: Este parámetro es un identificador único que agrupara una serie de mensajes. Es obligatorio que sea el mismo durante todos los mensajes que intercambiados entre UAC y UAS. Para asegurar que el identificador sea único se recomienda utilizar RFC 1750. (Uso de cryptographically random identifiers)

  El call-ID capturado es:

```
Call-ID: 5213e9a3785258c01d1b1cc0ba93807d@192.168.1.15
```

  Resulta interesante notar que el UAC del Videophone utiliza su propia IP como parte del new call ID.
- **Via**: El parámetro VIA identifica el protocolo de transporte y la ubicación a donde se debe enviar la respuesta. El UAC debe insertar este parámetro obligatoriamente siempre que se genera el request. Es importante notar que este parámetro está presente en los mensajes enviados por el UAC solamente.

  Dentro del campo VIA se incluye el parámetro Branch, el cual se utiliza para identificar la transacción dentro del UAC. Este parámetro debe ser único.

  La RFC 3261 especifica que el valor que tomará por defecto el Branco ID comienza con z9hG4bK. En la captura se puede ver que el protocolo de transporte es UDP, y la ip y el puerto del mismo es la del Videophone.

```
Via: SIP/2.0/UDP 192.168.1.15:5060;branch=z9hG4bKba93807da
```

- **Contact**: Este parámetro se utiliza para identificar la instancia específica del UA a donde se puede enviar la requests, fuera del dialogo en curso.

  En esta captura, este parámetro tiene el valor:

```
Contact: <sip:7366@192.168.1.15>
```

- **Max Forwards**: Este parámetro sirve para limitar la cantidad de saltos que un request puede transitar. Por defecto este valor se fija en 70 saltos. Si este parámetro llega a 0, la llamada es terminada con código 483 (too many hops).
- **Allow**: Indica todos los métodos soportados por el UA. Si este parámetro no esta presente, no significa que el UA no soporta ningún método, sino que le mismo no los proveyó. Este mensaje busca optimizar la cantidad de mensajes que se necesitan para concluir.

  En el caso del mensaje de invite, este parámetro incluyó:

```
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, PRACK, UPDATE, INFO
```

- **Content-Length**: Indica la cantidad de bytes del message body. Si no hay información en el cuerpo del mensaje, este parámetro debe ser seteado en 0. Este parámetro puede ser abreviado utilizando "l:".

  En este caso el largo del mensaje es de:

```
Content-Length: 274
```

- **Content-Type**: Este parámetro indica el tipo de información contenida en el body. Algunos ejemplos son: Content-Type: application/sdp c: text/html; charset=ISO-8859-4 En este caso, el protocolo que se utilizó:

```
Content-Type: application/sdp
```

- **Message Body**: El cuerpo del mensaje SIP, como se vio en el header, esta usando SDP:

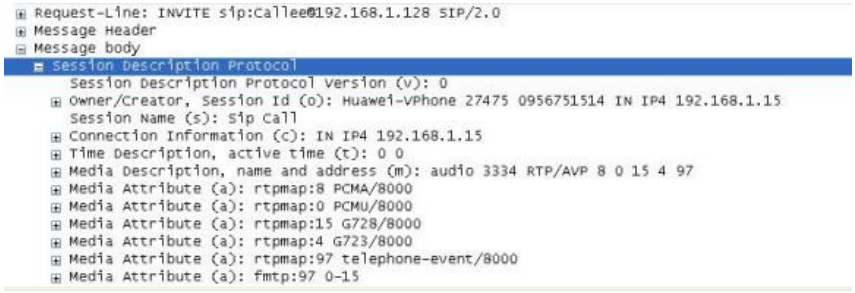

Figura 11.24: Protocolo SIP y Debug: Message Body

El protocolo Session Description Protocol está definido en la RFC 2327. La ventaja de usar un protocolo adicional para establecer los parámetros que definirán el establecimiento de la sesión es que esto permite a SIP adaptarse fácilmente tanto para comunicaciones de voz, como de aplicaciones multimedia.

El protocolo SDP consiste en diferentes tags, cada uno de los cuales describe un parámetro en particular de la sesión. Se puede ver los siguientes parámetros:

- v - SDP Protocol Version
- o – Owner- Creator, Session Id: Dentro de estos parámetros se puede ver el identificador de la session, la IP y el owner:

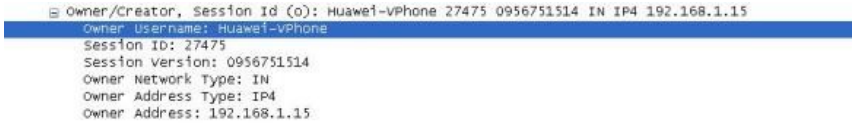

Figura 11.25: Protocolo SIP y Debug: Owner Username

- c – Connection Information: En este parámetro se presenta la IP donde se debe enviar el stream de audio. En este caso es la misma IP del VideoPhone: 192.168.1.15.
- t- Time description : Es el tiempo que lleva activa el stream de audio.
- m- Media Description: Este tag tiene la descripción de todos los codecs soportados por el UAC que inició la conversación. Se especifica el media type, que informa que el contenido de la session es audio, el media port, el cual define el puerto UDP que se asignó para recibir el stream de RTP. Los codecs de audio (video o dtmfs) se identifican utilizando valores preestablecidos estándar: 8 G.711A , 0 G711U, 4 G.723, etc.

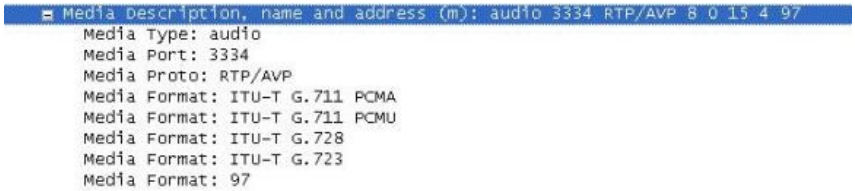

Figura 11.26: Protocolo SIP y Debug: Media Description

Conforme sea necesario, cada codec adapta sus parámetros utilizando media attributes:

- a – Media attributes: En la figura se puede ver como se especifican los diferentes parámetros para cada codec en particular. Los atributos se relacionan con el codec a través del parámetro ”Media Format”.

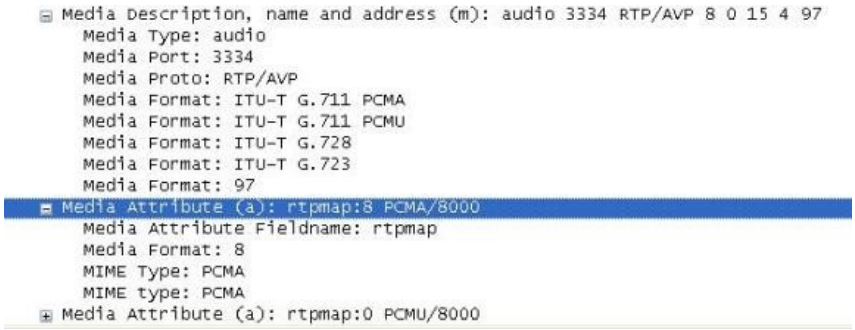

Figura 11.27: Protocolo SIP y Debug: Message Attibutes

11.4.3.2.2.2. Ringing Este mensaje es enviado por el UAS (en este caso, el softhpone) para indicar que el usuario está siendo alertado sobre la invitación. Es importante notar que en comparación al escenario 1, no se está enviando el mensaje TRYING. Esto es propio de la implementación del softphone, ya que no hay una interfase a excitar, como por ejemplo en un teléfono en el que hay una interfase con una línea analógica, la que tarda un tiempo hasta que comienza a sonar.

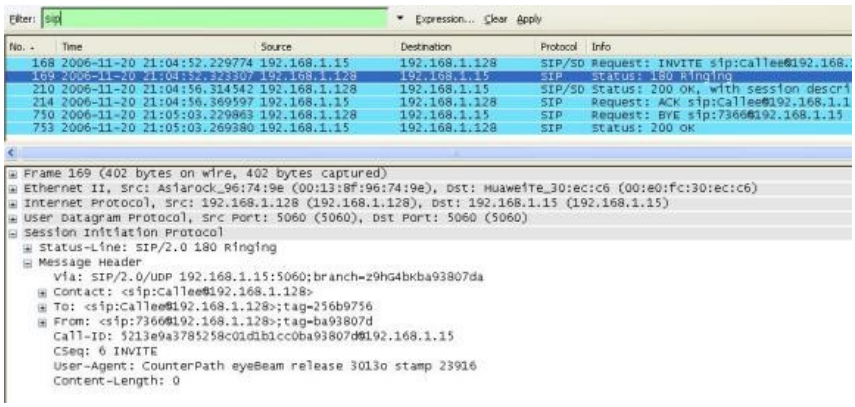

Figura 11.28: Protocolo SIP y Debug: Ringing

Mirando en detalle este mensaje, y comparándolo contra los campos vistos previamente en el INVITE, se puede observar que:

1. EL FROM y el TO enviados en el header del INVITE SE MANTIENEN, es decir, el UAS no cambia los valores provistos por el UAC. La única diferencia es que el UAS agrega el TAG en el TO, con lo que la llamada queda identificada por el Call-ID, tag provisto por el UAC, tag provisto por UAS.

2. El CSeq mantiene el identificador provisto en el INVITE.

3. El parámetro VIA mantiene los mismos valores que en el INVITE, y lo mismo es válido para el Branch.

4. El parámetro CONTACT es actualizado con los valores propios del UAS.

Es interesante ver un detalle de lo que ocurre una vez recibido el mensaje de Ringing:

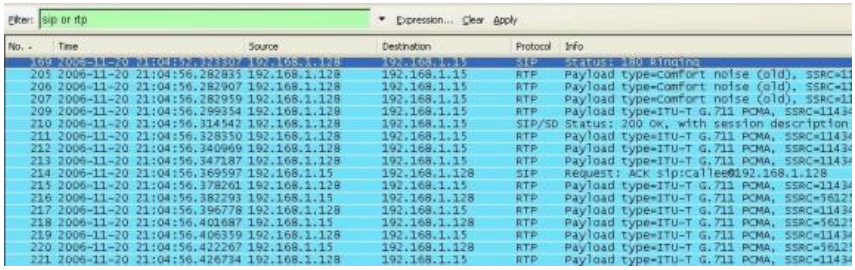

Figura 11.29: Protocolo SIP y Debug: Confort Noise

Se puede ver que el softphone, una vez que envío el mensaje de Ringing, como tiene la información de SDP del Videophone, ya puede comenzar a enviar audio (en un sentido). Antes de enviar el 200 OK con la información necesaria para que el videophone abra el canal en la dirección contraria, envía paquetes de RTP con comfort noise, para que el usuario no quede escuchando un canal mudo, lo que daría la sensación de que la comunicación fallo.

Luego, el sofphone envía el mensaje 200OK con el SDP para que el UAC puede abrir el canal, en el sentido inverso.

11.4.3.2.2.3. 200 OK Este mensaje conserva los mismos valores en los parámetros que el RINGING.

En el Message Body se puede ver que se está enviando como protocolo preferido G.711 Mu (8), y además se utilizará RTP/AVP (101) para los eventos del teléfono (dtmfs). El audio será dirigido al puerto UDP 9440.

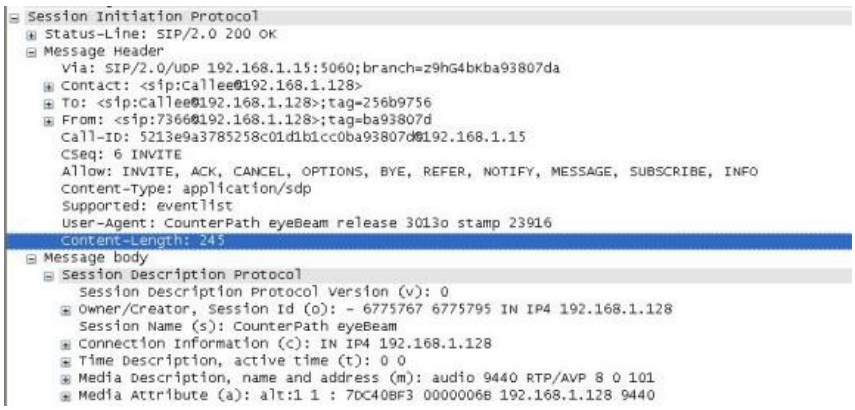

Figura 11.30: Protocolo SIP y Debug: 200 OK

11.4.3.2.2.4. ACK VideoPhone | Softphone Este mensaje confirma que el Videophone recibió la notificación 200 OK del UAS, y que el puerto fue abierto con la información provista en dicho mensaje. Se puede observar que luego de este mensaje, el Videophone comienza a enviar RTP utilizando G.711 al puerto 9440.

Figura 11.31: Protocolo SIP y Debug: ACK

11.4.3.2.2.5. BYE Softphone | VideoPhone Lo primero que resulta interesante es que el mensaje BYE es generado por el Softphone en lugar del videophone, quien era el que había iniciado la conversación.

Como en este caso el UAC es el softphone, se invierte el FROM y el TO, y el VIA se actualiza con los valores correspondientes al Softphone.

Sin embargo, tanto los tags como el call-ID se mantienen como en los otros mensajes.

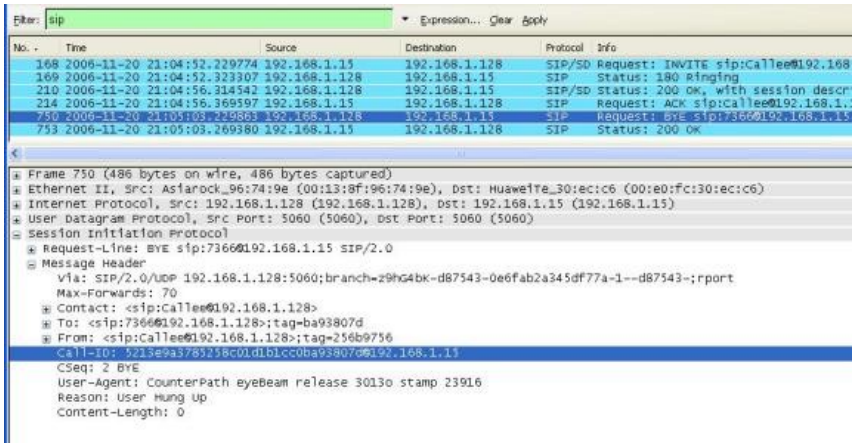

Figura 11.32: Protocolo SIP y Debug: Message Attibutes

11.4.3.2.2.6. 200 OK Videophone | Softphone Este mensaje confirma que la llamada fue desconectada del lado del Videophone. Resulta importante destacar que en este caso el Content-Length está en 0 porque no se incluye información de SDP.

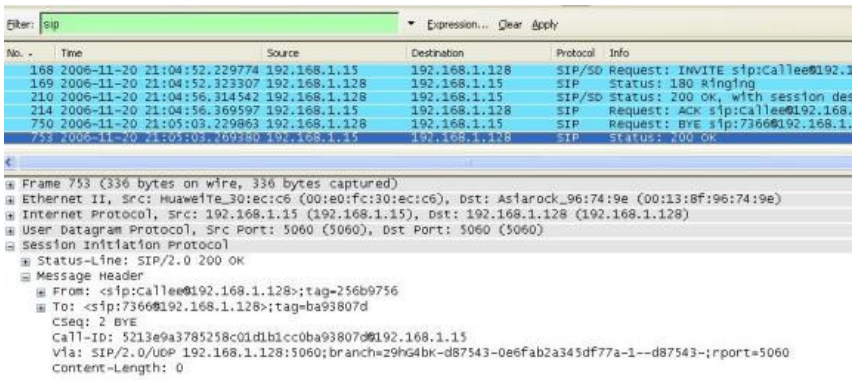

Figura 11.33: Protocolo SIP y Debug: 200 OK - Disconnect

11.4.3.2.3. Conclusiones Del análisis anterior resulta interesante notar que como los parámetros FROM, TO, VIA y CONTACT se adaptan de acuerdo al rol que esta cumpliendo cada Terminal en cada momento (UAC o UAS).

También resulta interesante destacar como se realiza el control de flujo de los mensajes de SIP, lo que justifica porque la mayoría de los fabricantes utiliza UDP como protocolo de transporte en lugar de TCP.

11.4.3.3. Llamada exitosa desde el softphone 1 al softphone 2 y viceversa

11.4.3.3.1. Objetivo Observar y analizar el establecimiento, transcurso y desconexión de una comunicación con ambos equipos disponibles, así como notar diferencias con el caso anterior.

11.4.3.3.2. Desarrollo En el presente escenario se realiza una comunicación exitosa entre dos softphones. El fin de esta captura es verificar que al no existir un sip proxy entre los dispositivos no aparece ningún mensaje del tipo trying. Para efectuar la comunicación nuevamente se tuvo que configurar ambos lados como peer-to-peer. Vemos a continuación el intercambio de mensajes.

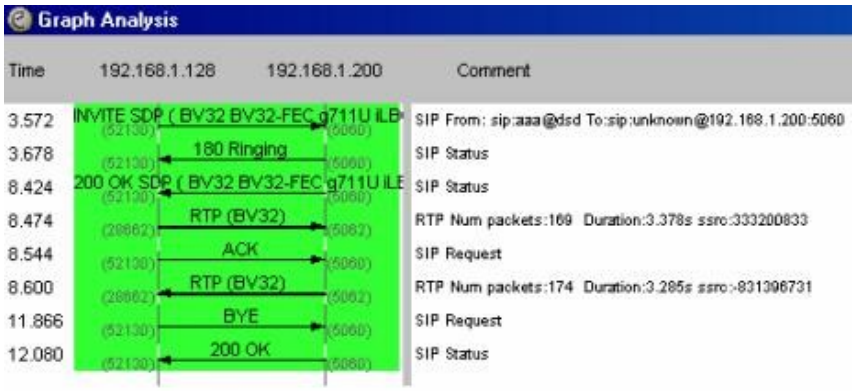

Figura 11.34: Protocolo SIP y Debug: Flujo de la llamada

Aquí constatamos que luego del primer mensaje INVITE el otro extremo responde directamente con un mensaje del tipo RINGING obviando el TRYING. Esto se debe nuevamente a que al no existir un Proxy no tiene sentido en una conexión punto a punto el envío de este mensaje. A continuación vemos la captura.

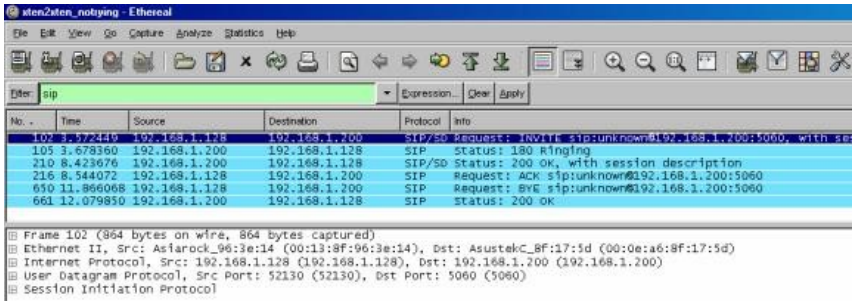

Figura 11.35: Protocolo SIP y Debug: Ringing

Esta comunicación se desarrolla en términos normales igual que los anteriores dos escenarios. En este caso podemos mencionar que aunque no se disponían de micrófonos en ninguno de los dos extremos hay intercambio de audio por RTP. Esto se debe a que al haberse negociado el codec G.711 U-Law no se implementa la supresión de silencios, es decir que hay intercambio de audio pero sin ningún contenido. En conclusión, se verifica la hipótesis respecto del Trying anteriormente planteada.

11.4.3.4. Llamada desde el videophone al softphone en modo DND (Do Not Disturb)

11.4.3.4.1. Objetivo Observar y analizar el establecimiento fallido en una comunicación con el softphone no disponible.

11.4.3.4.2. Desarrollo A continuación se muestra los mensajes intercambiados.

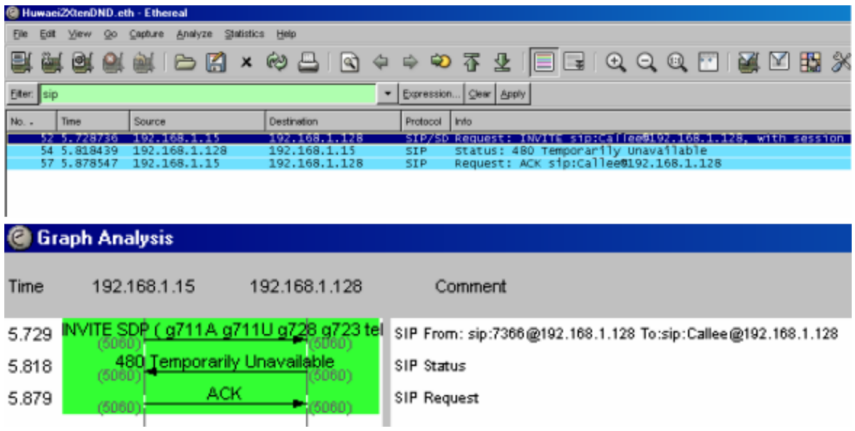

Figura 11.36: Protocolo SIP y Debug: Flujo de la llamada

Esta es la imagen del Soft Phone configurado en modo Do not Disturb.

Figura 11.37: Protocolo SIP y Debug: Soft Phone con DND

Como toda comunicación se inicia con un INVITE desde el VideoPhone, quien inicia la llamada, hacia el Softphone. Este paquete es de características idénticas a los anteriores.

La diferencia fundamental con los escenarios 1, 2 y 3 donde se establecían las llamadas es que al estar el softphone en modo DnD, responde con el mensaje 480 Temporarily

Unavailable solicitando la finalización de la llamada a lo que responde con el mensaje ACK finalizando de esta forma la llamada.

11.4.3.4.2.1. Mensaje 480 Temporarily unavailable Este mensaje es dado cuando el otro equipo está conectado correctamente pero no está en condiciones de responder la llamada. Por ejemplo: cuando no está logueado, cuando está logueado pero en un estado que no permite el ingreso de otra comunicación o se encuentra en modo Do not Disturb (DnD). En el teléfono que realizó la llamada generalmente aparece un mensaje diciendo que el teléfono destino no se encuentra disponible, intente más tarde.

A continuación se muestra la captura del mensaje 480:

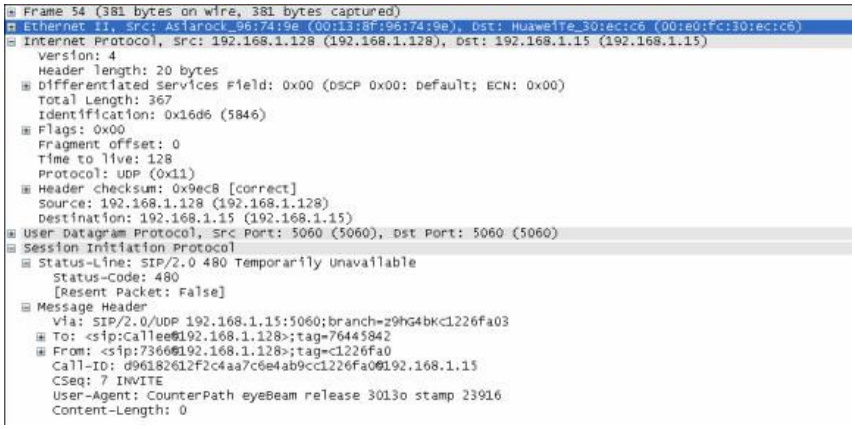

Figura 11.38: Protocolo SIP y Debug: Mensaje 480

En la línea de Status Line se visualiza que el mensaje enviado es el 480, los campos que contiene son los mismos a los del resto de los mensajes SIP.

Cada vez que se termina una llamada o no se concreta por algún motivo especial se envía un mensaje de error en respuesta a los distintos fallos detectados.

Como se ha indicado anteriormente corresponde con las respuestas de la clase:

- **4xx**: Respuestas de fallo de método.
- **5xx**: Respuestas de fallos de servidor.
- **6xx**: Respuestas de fallos globales.

Listado de errores SIP

En el apartado «Lista de errores» que se encuentra en la página 221, se encuentra el listado completo de mensajes de error del protocolo SIP.

11.4.3.4.3. Conclusiones La aparición de varios mensajes no usuales tales como DECLINE, Request Terminated, etc., amplia los escenarios básicos que podrían aparecen en una conexión SIP (analizar tabla de eventos SIP) Æ (RFC 3261).

11.4.3.5. Llamada desde el softphone al videophone ocupado

11.4.3.5.1. Objetivo Observar y analizar el establecimiento fallido en una comunicación con el videophone en uso.

11.4.3.5.2. Desarrollo A continuación se muestra los paquetes intercambiados entre el Soft Phone y el VideoPhone.

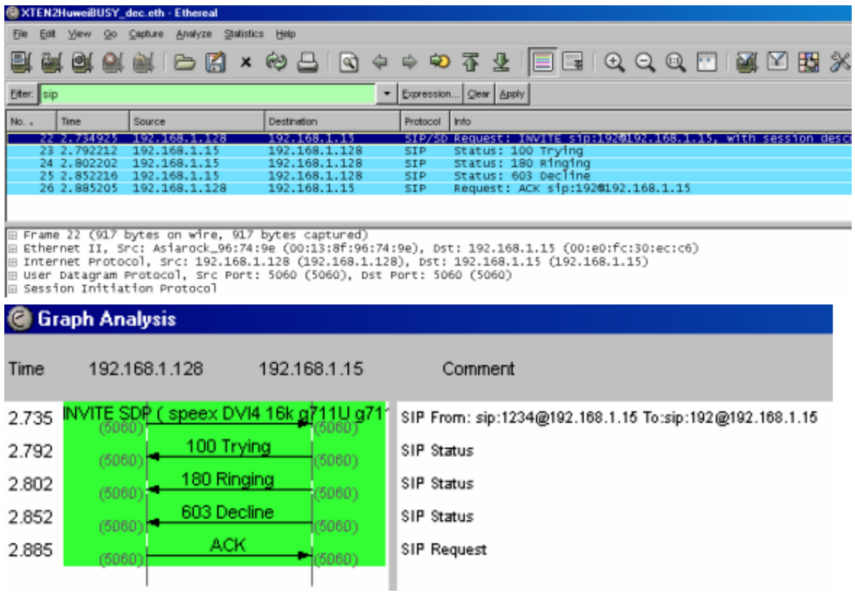

Figura 11.39: Protocolo SIP y Debug: Flujo de la llamada

En este caso, se realizó una llamada desde el Softphone hacia el Videophone, el cual se encontraba ocupado. El videophone responde al mensaje INVITE con un TRYING y RINGING, pero al detectar que no está en condiciones de recibir la llamada, envía el mensaje de error 603 DECLINE o llamada rechazada, a lo que el softphone responde con el ACK terminando la conexión.

11.4.3.5.2.1. Mensaje 603 DECLINE El mensaje 603 DECLINE indica que el teléfono al que se está llamando está correctamente conectado pero el destinatario explícitamente no quiere atender la llamada.

En este caso en el Video Phone se presionó la tecla Cancel mientras ringueaba, terminando así la llamada. En el display del llamante aparece la leyenda Ïntente más tarde".

A continuación se muestra la captura.

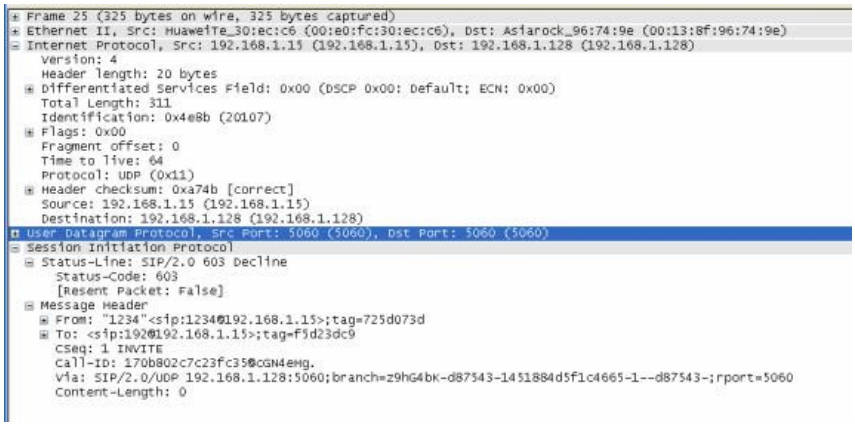

Figura 11.40: Protocolo SIP y Debug: Flujo de la llamada

En el campo Status Line se ve que este paquete es código 603, el cual no posee contenido adicional describiendo el motivo, por lo que tiene características similares a la del resto de los mensajes SIP.

Como se ha indicado anteriormente corresponde con las respuestas de la clase:

- **4xx**: Respuestas de fallo de método.
- **5xx**: Respuestas de fallos de servidor.

- **6xx**: Respuestas de fallos globales.

Listado de errores SIP

En el apartado «Lista de errores» que se encuentra en la página 221, se encuentra el listado completo de mensajes de error del protocolo SIP.

11.4.3.5.3. Conclusiones La aparición de varios mensajes no usuales tales como DECLINE, Request Terminated, etc., amplia los escenarios básicos que podrían aparecen en una conexión SIP (analizar tabla de eventos SIP) Æ (RFC 3261).

11.4.3.6. Llamada fallidas desde el softphone 1 al softphone 2

11.4.3.6.1. Objetivo Observar y analizar las causas por las cuales no fue posible realizar el establecimiento de las comunicaciones.

11.4.3.6.2. Desarrollo A continuación se muestra el esquema de paquetes intercambiados entre los softphones.

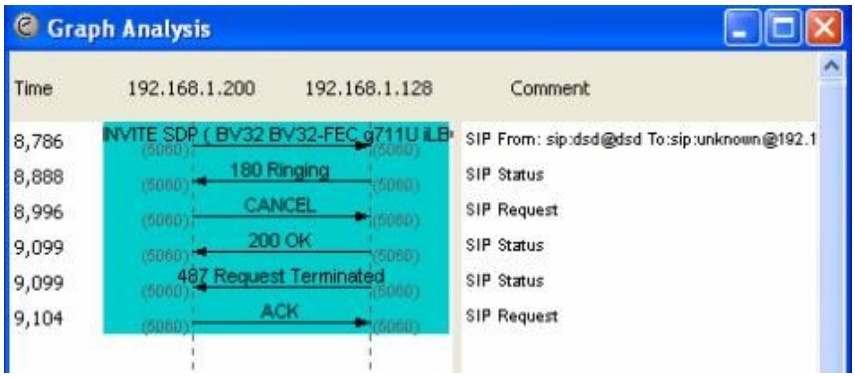

Figura 11.41: Protocolo SIP y Debug: Flujo de la llamada

En esta comunicación el Softphone IP: 192.168.1.200 genera una llamada hacia el Softphone IP: 192.168.1.128, el cual responde con un Ringing indicando que se encuentra conectado y está ringueando.

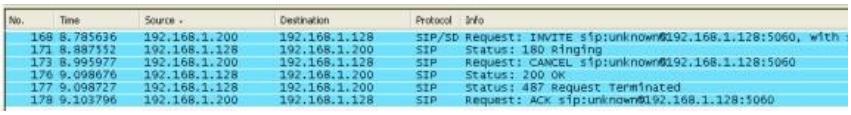

Figura 11.42: Protocolo SIP y Debug: Ringing

Antes de que el receptor atienda la llamada, el softphone que la generó la termina, por lo que este envía un mensaje CANCEL al softphone indicando que se cancela la sesión INVITE y pidiendo al otro softphone que deje de ringuear, a lo que responde con un mensaje de confirmación 200 OK. Luego el Softphone 128 envía el mensaje correspondiente para la finalización de la llamada, en este caso envía el mensaje 487 Request Terminated, el cual indica que recibió un CANCEL. A lo que la otra parte responde con el ACK finalizando la llamada.

Los paquetes INVITE y RINGING ya fueron explicadas por lo que no se muestran.

11.4.3.6.2.1. Mensaje CANCEL El mensaje CANCEL es enviado cuando el que inició la llamada la quiere finalizar antes de que el destinatario la haya atendido o finalizado, o sea, cancelar el pedido de INVITE.

El envío de este mensaje es similar a pedirle a la otra parte que deje de llamar, a lo que la otra parte responde enviando el 200 OK y el mensaje 487, permitiendo así la finalización de la llamada.

En la captura vemos que la línea Req Line describe un paquete CANCEL, el cual no presenta diferencias sobre el resto de los paquetes, debido a que no contiene campo de aclaraciones o contenidos.

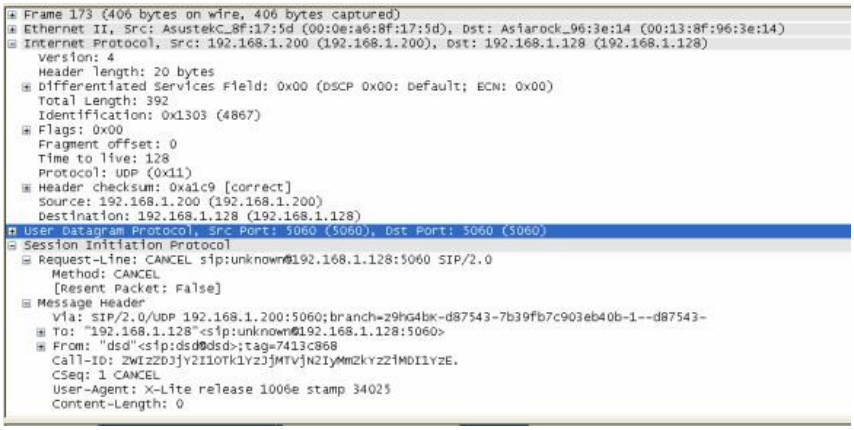

Figura 11.43: Protocolo SIP y Debug: CANCEL

11.4.3.6.2.2. 487 Request Terminated Este mensaje es enviado como respuesta a un CANCEL o BYE permitiendo la finalización de la llamada.

A continuación se muestra la captura.

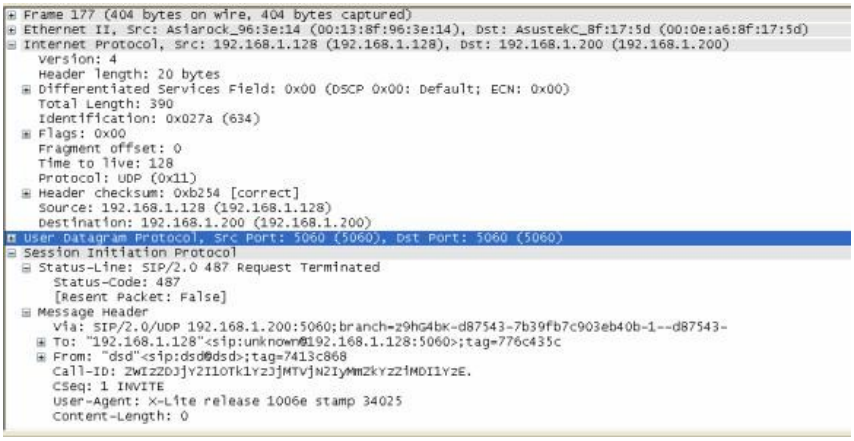

Figura 11.44: Protocolo SIP y Debug: 487 Request Terminated

En la línea Status Line vemos que el mensaje enviado es el 487 Request Terminated. Los campos de este mensaje son similares a los anteriores debido a que tampoco poseen campo de aclaraciones o contenido.

11.4.3.6.3. Conclusiones Podemos observar en este análisis que hay un acuerdo con la descripción teórica detallada anteriormente con respecto al mensaje CANCEL, donde el UA con la dirección IP: 192.168.1.128 envía una petición de cancelación posterior a su petición INVITE, concluyendo de esta manera con la comunicación.

Sección 12

Lista de errores

Estos errores se corresponden con los mensajes de error Q.931 o DSS1 y suponen el mapeo de los eventos SIP con los códigos de error de la RTC (Red telefónica conmutada)

Evento SIP	Valor			Detalle
	Decimal	Hezadecimal	Transmitido en el canal	
400 Bad request	127	7f	ff	Interworking, unspecified
401 Unauthorized	57	39	b9	Bearer capability not authorized
402 Payment required	21	15	95	Call rejected
403 Forbidden	57	39	b9	Bearer capability not authorized
404 Not found	1	1	81	Unallocated (unassigned) number
405 Method not allowed	127	7f	ff	Interworking, unspecified
406 Not acceptable	127	7f	ff	Interworking, unspecified
407 Proxy authentication required	21	15	95	Call rejected
408 Request timeout	102	66	e6	Recover on Expires timeout
409 Conflict	41	29	a9	Temporary failure
410 Gone	1	1	81	Unallocated (unassigned) number
411 Length required	127	7f	ff	Interworking, unspecified
413 Request entity too long	127	7f	ff	Interworking, unspecified
414 Request URI (URL) too long	127	7f	ff	Interworking, unspecified
415 Unsupported media type	79	4f	cf	Service or option not available
420 Bad extension	127	7f	ff	Interworking, unspecified
480 Temporarily unavailable	18	12	92	No user response
481 Call leg does not exist	127	7f	ff	Interworking, unspecified
482 Loop detected	127	7f	ff	Interworking, unspecified
483 Too many hops	127	7f	ff	Interworking, unspecified
484 Address incomplete	28	1c	9c	Address incomplete (invalid number format)
485 Address ambiguous	1	1	81	Unallocated (unassigned) number
486 Busy here	17	11	91	User busy
487 Request cancelled	127	7f	ff	Interworking, unspecified
488 Not acceptable here	127	7f	ff	Interworking, unspecified
500 Internal server error	41	29	a9	Temporary failure
501 Not implemented	79	4f	cf	Service or option not implemented
502 Bad gateway	38	26	a6	Network out of order
503 Service unavailable	63	3f	bf	Service or option unavailable
504 Gateway timeout	102	66	e6	Recover on Expires timeout
505 Version not implemented	127	7f	ff	Interworking, unspecified
580 Precondition Failed	47	2f	af	Resource unavailable, unspecified
600 Busy everywhere	17	11	91	User busy
603 Decline	21	15	95	Call rejected
604 Does not exist anywhere	1	1	81	Unallocated (unassigned) number
606 Not acceptable	58	3a	ba	Bearer capability not presently available

Sección 13

Pruebas de *stress*

Durante las pruebas de *stress* de las plataformas Denwa UC&C 4.0.1 será necesario utilizar distintas herramientas a fin de monitorear el comportamiento tanto de la plataforma, como de los equipos activos de la red local donde se realizará. Para ello Denwa Technology Corp. proporcionará una máquina virtual en formato OVA que contendrá todos los elementos necesarios para el proceso.

13.1. Máquina Virtual

La máquina virtual consta de un Ubuntu 16.04 LTS Desktop en donde se ha disponibilizado herramientas de multiplexación de conexiones ssh, un generador de llamadas y "The Dude" de MikroTik.

13.1.1. Configuración inicial

La máquina virtual cuenta con un entorno gráfico desde donde será necesario que se realice la configuración de red de forma manual. Lo que se describe a continuación, corresponde al contenido de un archivo PDF, que se encuentra en el Escritorio del usuario, en el cual se describe el paso a paso para la configuración de la red.

PDF en Escritorio del usuario de la Máquina Virtual

Instrucciones

Preparativos Previo a realizar cualquier configuración, se deberá validar alguna información de red, para ello será necesario abrir una nueva terminal (Crtl + Alt + T) y escribirá el siguiente comando

```
1 ifconfig -a
```

Con esta información será posible obtener el nombre de la placa de red dentro del sistema, la cual podría ser: eth0, enp3s0, etc.

Configuración de Red La primera vez que ingrese a esta máquina virtual, deberá configurar los parámetros de red para su correcto funcionamiento, esto lo podrá realizar haciendo clic en el ícono que encontrará en la esquina superior derecha de su pantalla. Posteriormente se seleccionará la opción "Edit Connections..." Tras hacerlo, se deberá pulsar el botón "Add", lo cual desplegará una nueva ventana donde seleccionará "Ethernet" como tipo de conexión y deberá hacer clic en "Create". En la siguiente ventana se realizará las siguientes configuraciones: Ethernet

- Device: se seleccionará la placa de red obtenida por el comando ifconfig –a
- IPv4 Settings

- Method: Manual

- Addresses:
  - Address: IP que se le asignará a la VM
  - Netmask: Máscara de red (en cuatro octetos o en formato cidr)
  - Gateway: Puerta de Enlace

DNS Servers: IP de los servidores DNS a utilizar (debe poder resolver el dominio `supportvpn.denwaip.com`). Luego de realizar las configuraciones anteriores, se debe pulsar el botón "Save"

Validación de conectividad Utilizando una terminal (Crtl + Alt + T) es posible realizar pruebas de conectividad mediante las herramientas propias del sistema, tales como:

- ping
- traceroute
- telnet
- mtr

Es necesario comprobar que el dominio supportvpn.denwaip.com pueda ser resuelto y que el puerto 1199 de dicho dominio sea alcanzable por udp.

Conexión a la VPN de Soporte Desde la terminal (Crtl + Alt + T) es posible conectar el equipo a la VPN de Soporte, esto se realizará mediante el uso del comando:

```
sudo openvpn /etc/155.ovpn &
```

Cuando se le consulte por el [sudo] password, deberá ingresar: config y pulsar la tecla Enter. Posteriormente, mediante el comando ifconfig, podrá conocer la IP asignada por la VPN de Soporte, a fin de proporcionarla al personal de Denwa Technology Corp.

De lo anterior es importante recalcar la necesidad de que la IP que se asigne a esta máquina virtual cuente con la posibilidad de conectarse a nuestra VPN de Soporte, a fin de poder gestionarlo remotamente.

13.1.2. Terminator

Esta herramienta es un multiplexor de conexiones ssh, lo cual permitirá organizar la visualización de distintas consultas a los equipos Denwa intervinientes en las pruebas, como por ejemplo:

- Uso de CPU
- Uso de RAM
- Usuarios o Agentes registrados
- Llamadas Concurrentes
- Utilización de disco
- Etc.

Estando cada una de estas consultas en una sesión ssh diferente.

13.1.3. *The Dude*

La herramienta de monitoreo de MikroTik nos proporcionará de forma visual el estado de la red al momento de realizar las distintas pruebas; para ello será necesario contar con la siguiente información:

- Topología COMPLETA la red donde se realizará el monitoreo, señalando:
  - Direcciones IP de cada equipo indicando a qué placa pertenece.
  - Puertos de conexión de los equipos intervinientes en la prueba.
  - Puertos de conexión de TODOS los equipos intermedios, a saber:
  - Routers
  - Switches
  - Etc.
- Descripción del tipo de conexión entre los equipos:
  - Ethernet
  - Giga
  - SPF
  - SPF+
  - Etc.
- Credenciales para consultas vía SNMP en cualquiera de sus versiones (1, 2 ó 3) en:
  - Los dispositivos de los agentes
  - TODOS los dispositivos intermedios, a saber:
    - Routers
    - Switches administrables
    - Etc.

Por ejemplo:

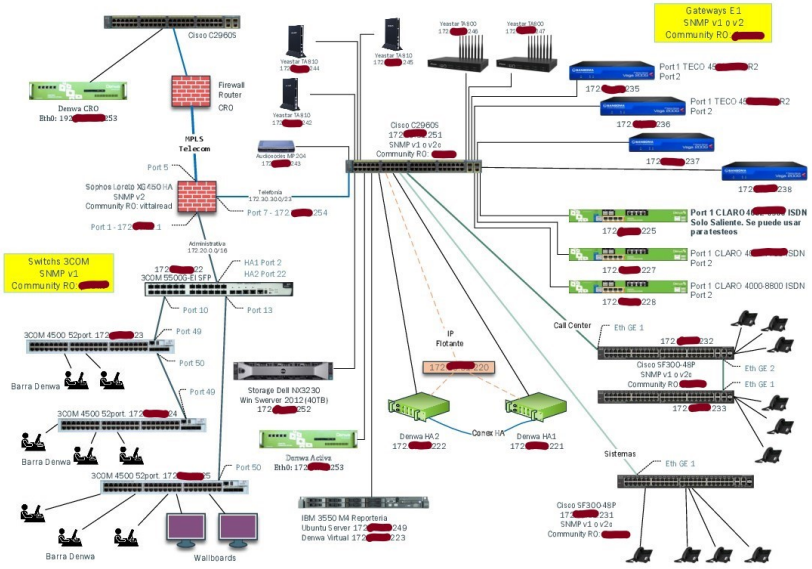

Figura 13.1: Pruebas de *stress*: Topología enviada por el cliente

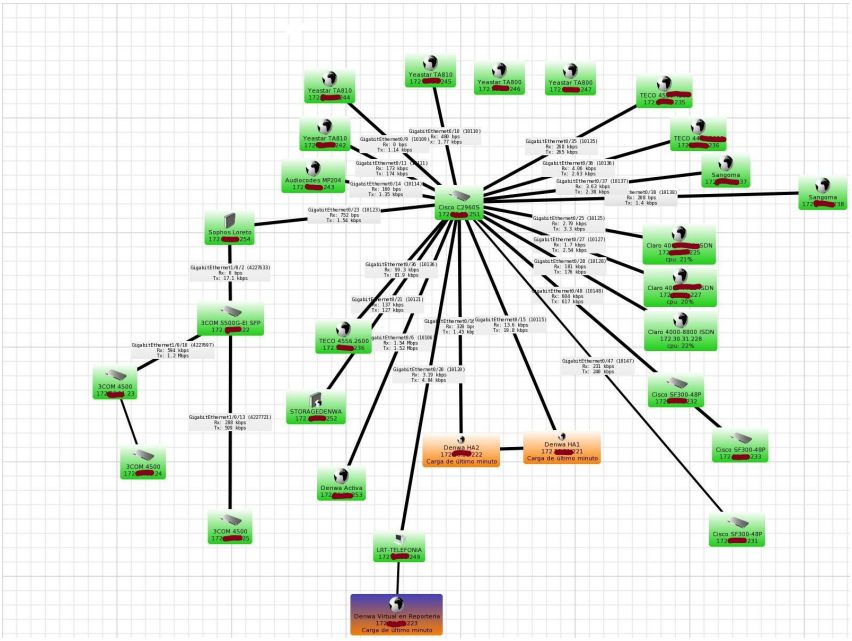

Figura 13.2: Pruebas de *stress*: Monitoreo por «*The Dude*»

13.2. Banco de Pruebas

Una vez que haya sido posible replicar la topología en la herramienta «*The Dude*» de MikroTik y contemos con información relacionada al ancho de banda utilizado en cada una de las conexiones de los distintos equipos por los cuales (consultado por SNMP) se procederá a realizar las pruebas de *stress* mediante el uso del generador de llamadas contenido en la máquina virtual.

A fin de validar los resultados, cada prueba deberá repetirse al menos dos (2) veces, manteniendo el flujo máximo de llamadas por al menos cinco (5) minutos consecutivos. Las pruebas se realizarán de forma escalonada, de la siguiente forma:

- **Prueba 1**: 10 % del total de llamados concurrentes contratados
- **Prueba 2**: 25 % del total de llamados concurrentes contratados
- **Prueba 3**: 50 % del total de llamados concurrentes contratados
- **Prueba 4**: 100 % del total de llamados concurrentes contratados
- **Prueba 5**: 110 % del total de llamados concurrentes contratados

La tasa de crecimiento de los llamados concurrentes, hasta llegar al umbral antes declarado, será constante, y estará definido por la cantidad máxima de llamadas simultáneas ya que para estas pruebas utilizamos un archivo de audio que posee una duración definida de ciento veinte (120) segundos.

$$Tasa = \frac{Llamados\ concurrentes\ maximos}{Duracion\ de\ audio\ de\ prueba}$$

Cabe señalar que, bajo este escenario de pruebas, es posible que la mayor parte de los llamados no lleguen a ser atendidos por el personal del Contact Center destinado para tal fin, por lo que figurarán como “No Atendidos” en la Reportería de la plataforma.

Adicionalmente es necesario considerar que el archivo utilizado en nuestros escenarios de prueba utiliza el códec G.711-A por lo que, en caso de que los internos de los agentes o el troncal utilice otro códec, podría generarse un mayor uso de recursos de la plataforma por causa del transcoding.

Apartado V

Índices

Índice general

Índice de figuras