UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

IMPLEMENTACIÓN DE SERVICIOS DE ADMINISTRACIÓN Y GESTIÓN BASADOS EN EL CLOUD COMPUTING SAAS QUE PERMITAN MEJORAR EL TIEMPO DE RESPUESTA ANTE INCIDENTES EN LA RED GPON DE LA EMPRESA CAYAMBEVISION S.A.

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN TELECOMUNICACIONES

AUTOR: DEYLAN JAVIER LEMA VILLAVICENCIO

DIRECTOR: ING. HERNÁN MAURICIO DOMÍNGUEZ LIMAICO, MSC

ASESOR: ING. EDGAR ALBERTO MAYA OLALLA, MSC

IBARRA-ECUADOR

2023

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1727256834		
APELLIDOS Y NOMBRES:	Lema Villavicencio Deylan Javier		
DIRECCIÓN:	Cayambe – 24 de Mayo y Rocafuerte		
EMAIL:	djlemav@utn.edu.ec		
TELÉFONO FIJO:	02 2361329	**TELÉFONO MÓVIL:**	0958906182

DATOS DE LA OBRA	
TÍTULO:	"IMPLEMENTACIÓN DE SERVICIOS DE ADMINISTRACIÓN Y GESTIÓN BASADOS EN EL CLOUD COMPUTING SAAS QUE PERMITAN MEJORAR EL TIEMPO DE RESPUESTA ANTE INCIDENTES EN LA RED GPON DE LA EMPRESA CAYAMBEVISION S.A."
AUTOR:	Lema Villavicencio Deylan Javier
FECHA:	07/06/2023
PROGRAMA:	x **PREGRADO** ☐ **POSGRADO**
TITULO:	Ingeniero en Telecomunicaciones
DIRECTOR:	MSc. Hernán Mauricio Domínguez Limaico

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 7 días del mes de junio de 2023.

EL AUTOR:

Deylan Javier Lema Villavicencio

CI: 1727256834

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN:

MAGÍSTER HERNÁN MAURICIO DOMÍNGUEZ LIMAICO, CON CÉDULA DE IDENTIDAD Nro. 1002379301, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de Titulación "IMPLEMENTACIÓN DE SERVICIOS DE ADMINISTRACIÓN Y GESTIÓN BASADOS EN EL CLOUD COMPUTING SAAS QUE PERMITAN MEJORAR EL TIEMPO DE RESPUESTA ANTE INCIDENTES EN LA RED GPON DE LA EMPRESA CAYAMBEVISION S.A.", Ha sido desarrollado por el señor Lema Villavicencio Deylan Javier bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad.

.....

Ing. Hernán Mauricio Domínguez, MSc.

DIRECTOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

Este logro no habría sido posible sin su amor, apoyo y dedicación a lo largo de mi vida. Gracias por ser mi fuerza y mi inspiración en los momentos difíciles, y por celebrar conmigo en los momentos felices. El presente trabajo de titulación es el resultado de años de esfuerzo, y estoy agradecido por tenerlos a mi lado en cada paso del camino. Espero que este trabajo sea una fuente de orgullo y felicidad para todos nosotros.

Con todo mi amor y gratitud,

Deylan Lema

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco a Dios, quien me ha dado la sabiduría y la fortaleza para superar los obstáculos y alcanzar mis metas. A mis padres Oscar y Marisol, gracias por su amor incondicional, su apoyo y su motivación constante. Ustedes son mi ejemplo para seguir y siempre estaré agradecido por todo lo que han hecho por mí. A mi novia Milagros, gracias por estar a mi lado en los buenos y malos momentos, y por ser mi compañera en este camino. También quiero agradecer a mi familia por su amor y por creer en mí. Este logro es un tributo a su amor y dedicación, y espero que este trabajo de titulación inspire a otros a alcanzar sus metas y perseguir sus sueños con pasión y determinación.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo describe la implementación de servicios de administración y gestión basados en el Cloud Computing SaaS que permitan mejorar el tiempo de respuesta ante incidentes

en la red GPON de la empresa CayambeVision S.A. Para lo cual, se a iniciado con el estudio del fundamento teórico que sustente el presente trabajo de investigación, en donde se puede identificar la estructura de una red GPON, sus componentes y funcionamiento.

Posterior a esto se realiza el desarrollo del proyecto enfocado en el cumplimiento de las mejores prácticas basadas en el modelo metodológico de la ISO/IEEE 29148 la cual se basa en establecer los requisitos para la ingenia de software y sistemas. Una vez definido el modelo metodológico para el desarrollo del presente proyecto se procede a investigar en el mercado aquellos servicios en la nube los cuales se puedan adaptar a la red acorde a un benchmarking competitivo y que cumplan con las necesidades de la empresa.

Seleccionadas las herramientas de gestión y administración se realiza la implementación de cada una de estas, levantando los procesos anteriores identificados en la red y proponiendo mejoras en la gestión de estos basados en el modelo FCAPS, logrando así la adaptación correcta de las herramientas a la red de backbone de la empresa e identificando escenarios que se puedan desarrollar a lo largo de la adaptación de los servicios.

Para finalizar se realiza la ejecución de los servicios integrados en la red y se verifica su impacto correspondiente a los tiempos obtenidos en la ejecución de los nuevos procesos integrados en la red de CayambeVision S.A. de esta manera se puede constatar el correcto funcionamiento y cumplimiento de los objetivos planteados en la presente investigación.

ABSTRACT

The present work describes the implementation of administration and management services

based on Cloud Computing SaaS that allow for improving the response time to incidents in the GPON network of CayambeVision S.A. To do so, we began with a study of the theoretical foundation that supports this research work, where the structure of a GPON network, its components, and functioning can be identified.

Following this, the project development is carried out, focused on compliance with the best practices based on the methodological model of ISO/IEEE 29148, which establishes requirements for software and system engineering. Once the methodological model for the development of the present project is defined, market research is carried out to identify cloud services that can be adapted to the network according to competitive benchmarking and meet the company's needs.

After selecting the management and administration tools, the implementation of each of them is carried out, by identifying the previous processes in the network and proposing improvements in their management based on the FCAPS model. This allows for the correct adaptation of the tools to the company's backbone network and identifying scenarios that can be developed throughout the adaptation of the services.

Finally, the integrated services are executed in the network, and their impact is verified corresponding to the times obtained in the execution of the new processes integrated into CayambeVision S.A.'s network. In this way, the proper functioning and achievement of the objectives proposed in this research work can be verified.

1. CAPITULO I - ANTECEDENTES

En este capítulo se describen los requisitos necesarios para llevar a cabo el trabajo de titulación actual, que incluyen el tema seleccionado, la problemática a abordar, los objetivos a alcanzar, el alcance del proyecto y la justificación para garantizar su éxito.

1.1. Tema

IMPLEMENTACIÓN DE SERVICIOS DE ADMINISTRACIÓN Y GESTIÓN BASADOS EN EL CLOUD COMPUTING SAAS QUE PERMITAN MEJORAR EL TIEMPO DE RESPUESTA ANTE INCIDENTES EN LA RED GPON DE LA EMPRESA CAYAMBEVISION S.A.

1.2. Problema

Un informe realizado por el FTTH Council ha identificado que en la actualidad 14 países superan el 1% de hogares con conexiones de fibra óptica. El top 3 de países con la mayor penetración de fibra óptica en hogares son Corea del Sur, Hong Kong y Japón, con tasas de 31.4%, 23.4% y 21.3%, respectivamente. Suecia es el cuarto país de la lista, con una tasa del 7.1%. Además, otros 10 países también han adoptado esta tecnología, incluyendo Taiwán, Noruega, Dinamarca, Estados Unidos, Eslovenia, Islandia, China, Holanda, Italia y Singapur. En América Latina, ciudades como Bogotá, São Paulo, Buenos Aires y Santiago ya ofrecen servicios de redes GPON.

Según datos recolectados de Arcotel menciona que “En el Ecuador el servicio de internet a través de conexiones físicas ha crecido de manera exponencial entre los años 2001 a 2020. El crecimiento se da hasta un promedio de un 8% por año el cual está influenciado por la innovación y desarrollo

tecnológico.” El planteamiento de políticas y estrategias gubernamentales han beneficiado en el crecimiento de interconectividad en los últimos años.

El desarrollo actual de la sociedad ha generado una necesidad en el establecimiento de una conexión con el internet, es por esto que han surgido pequeñas y medianas empresas que brindan este servicio de internet a sus localidades. En Pichincha en la localidad de Cayambe existe un ISP mediano el cual alberga a clientes de la zona, ofreciendo el servicio tanto en lugares rurales como urbanos, por lo que su crecimiento con el paso de los años se ha visto significativamente en el número de clientes registrados a su servicio.

Actualmente en la empresa CayambeVision SA debido a su crecimiento presenta falencias en la administración y gestión de la red FTTH, generando malestar en los clientes y gasto de recursos en la empresa. Es por lo cual que se busca implementar servicios que permitan gestionar y administrar la red de manera rápida. Permitiendo el acceso a la información de clientes y estado de la red al instante desde cualquier dispositivo y en cualquier lugar, provisionando un servicio al cliente con parámetros adecuados.

1.3. Objetivos

1.3.1. Objetivo General

Implementar servicios de administración y gestión basados en el Cloud Computing SaaS que permitan mejorar el tiempo de respuesta ante incidentes en la red GPON de la empresa CayambeVision SA.

1.3.2. Objetivos Específicos

- Estudiar el fundamento teórico que conlleva a las redes GPON FTTH para conocer la estructura funcionamiento operación y mantenimiento que permita tener una base conceptual en la que se sustente la investigación.
- Determinar herramientas de Administración y Gestión en la nube basadas en las necesidades del ISP CayambeVision mediante un benchmarking competitivo.
- Implementar las herramientas de Administración y Gestión seleccionadas en base al estudio de benchmarking previamente realizado en la empresa CayambeVision S.A.
- Realizar pruebas del funcionamiento de las herramientas implementadas para evidenciar el impacto en el tiempo de respuesta en la resolución de problemas y la mejora a la capacidad Administrativa de la Red GPON FTTH de la empresa CayambeVision.

1.4. Alcance

El propósito de este proyecto tiene como finalidad mejorar el tiempo de respuesta ante incidentes reportados por los clientes del Proveedor de Servicio de Internet (ISP) CayambeVision S.A., estableciendo un servicio adecuado hacia el mismo y a la vez lograr una adecuada gestión y

administración de la red a través de la implementación de servicios alojados en la nube que permitan visualizar estados de enlace de los clientes en la red en tiempo real, para el desarrollo de este proyecto se propone:

Iniciar con un estudio teórico sobre la arquitectura de red GPON, exponiendo características generales y los componentes principales de una red FTTH GPON, así como también cada uno de los equipos de certificación de una red de fibra óptica basado en el estándar establecido por la ITU G.984.x.

En la siguiente etapa se generará un proceso de Benchmarking Competitivo en el cual se analicen las buenas prácticas relacionadas con la administración y gestión de la red que se maneja a nivel de ISP, buscando herramientas que se alojen en el Cloud que permitan facilitar la capacidad Administrativa y Gestión en el ISP CayambeVision S.A., los cuales brinden acceso a la información y control, para la toma de decisiones de manera remota.

Después de identificados los servicios alojados en la Nube, se propone un escenario para su aplicación, verificando las herramientas necesarias tanto en hardware como en software y el modelo que se procederá a utilizar para generar una topología con la cual se logrará añadir estos servicios integrados al ISP CayambeVision S.A. El proceso de implementación se establecerá usando distintos métodos orientados a conexión como Destination NAT el cual se empleará para hacer que las conexiones entrantes puedan acceder a un dispositivo local (OLT) y VPN para mejorar la seguridad de la conexión desde la red externa a la interna sin necesidad de una IP pública.

Finalmente se propondrá pruebas de funcionamiento que permitan comprobar así la efectividad de los servicios implementados, tales como conexión remota desde cualquier punto, capacidad de

generar cambios de manera externa, realizar lecturas del estado de la red en tiempo real, notificar problemas de usuarios y establecer soluciones de manera eficaz y rápida.

1.5. Justificación

En la actualidad el desarrollo de la sociedad ha generado una necesidad en el establecimiento de una conexión con el internet, es por esto por lo que han surgido pequeñas y medianas empresas que brindan este servicio de internet a sus localidades.

CayambeVision SA es una Empresa de Telecomunicaciones que brinda el servicio de internet en la Zona 2, ubicado en el cantón Cayambe. Debido a su favorable crecimiento en el número de clientes se han logrado desarrollar varias problemáticas vinculadas a la baja capacidad administrativa y de gestión que cuenta esta empresa privada. Generando malestar en los clientes y gasto de recursos en la empresa. Es por lo cual que se busca implementar servicios que permitan gestionar y administrar la red de manera rápida. Permitiendo el acceso a la información de clientes y estado de la red al instante desde cualquier dispositivo y en cualquier lugar, provisionando un servicio al cliente con parámetros adecuados.

Por otra parte, dentro de las bondades que brinda el Cloud Computing se tiene Software como servicio (SaaS). Este software, está alojado en el servidor del proveedor y el cliente accede a él a través de una conexión vía internet. Todo lo relacionado con el mantenimiento, soporte y disponibilidad es manejado por el proveedor SaaS. Por lo cual es una herramienta útil para cumplir con lo requerido para la empresa CayambeVision S.A.

2. CAPITULO II - MARCO TEÓRICO

2.1. INTERNET SERVICES PROVIDER (ISP)

El Internet es una red mundial que ofrece acceso a información mediante conexiones inalámbricas y terrestres. En Ecuador, la Corporación Interinstitucional de Comunicación Electrónica (Intercom) estableció el primer nodo de acceso a Internet en 1991, a través de Ecuanex. Desde entonces, se han establecido varios puntos de acceso a Internet a nivel local, como resultado de esta iniciativa temprana de conectividad.

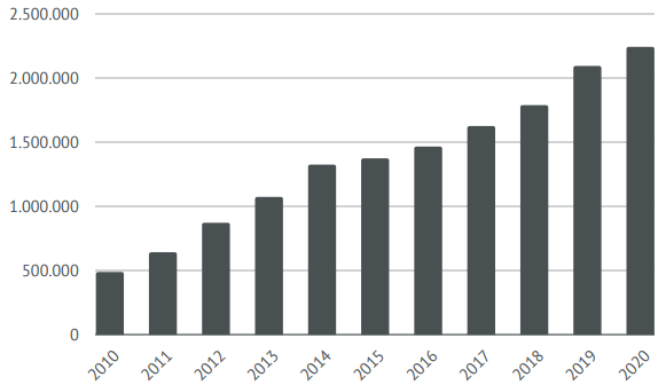
En la actualidad el acceso al internet es una herramienta esencial para lograr el desarrollo económico y social de una población. Esto gracias a la capacidad de acceso a información que nos brinda esta red de redes, pues a través de su acceso se puede realizar búsquedas de herramientas que nos ayuden a enriquecer el conocimiento.

El desarrollo tecnológico ha permitido la aparición de sistemas que aumentan la velocidad de conexión y modifican los planes de acceso a Internet. Actualmente, los proveedores de servicios de Internet (ISP) ofrecen conectividad de banda ancha. Los ISP son compañías que brindan acceso a Internet a hogares y empresas.

Un boletín estadístico establecido por la Agencia de Regulación y Control de las Telecomunicaciones en Ecuador hace referencia al crecimiento que ha tenido el servicio de internet a través de las conexiones físicas entre el año 2001 hasta el 2020 (Ver ***Figura 1***). En el territorio ecuatoriano se puede observar una tasa promedio anual de crecimiento del 8%, la misma que incrementa conforme a los avances tecnológicos, políticos y estratégicos gubernamentales de conectividad establecidas en los últimos años. (ARCOTEL, 2020, pág. 4).

Figura 1

Cifras de conexiones físicas a nivel nacional hasta septiembre de 2020



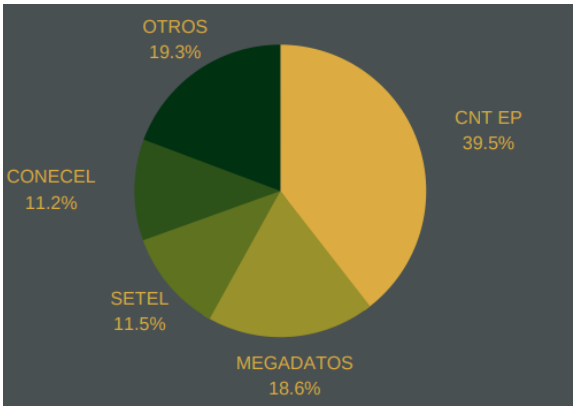
Nota: adaptado de "Servicio de Acceso a Internet", por ARCOTEL, 2020, p. 4.

Con al avance de las tecnologías de conexión a internet iniciadas desde DSL (Digital Suscriber Line) con la implementación de par trenzado, HFC (Hybrid Fiber-Coaxial) con su estructura basada en cable coaxial y actualmente redes FTTx establecidas en redes de fibra híbridas. Los ISP de primer nivel han logrado obtener gran impacto en el mercado de internet fijo, siendo las empresas: SETEL, CONECEL, CNT EP, MEGADATOS, entre otras las que se encargan de distribuir y brindar acceso a empresas mucho más pequeñas y a los clientes finales.

En la **Figura 2** se puede observar un gráfico que hace referencia a la participación de mercado en el internet fijo que ocupan las empresas en el Ecuador hasta septiembre de 2020 según el boletín estadístico establecido por el SAI en noviembre 2020 (ARCOTEL, 2020).

Figura 2

Participación de mercado en el internet fijo de Ecuador



Nota: adaptado de "Servicio de Acceso a Internet", por ARCOTEL, 2020, p. 4.

2.1.1. Arquitectura Básica de un ISP

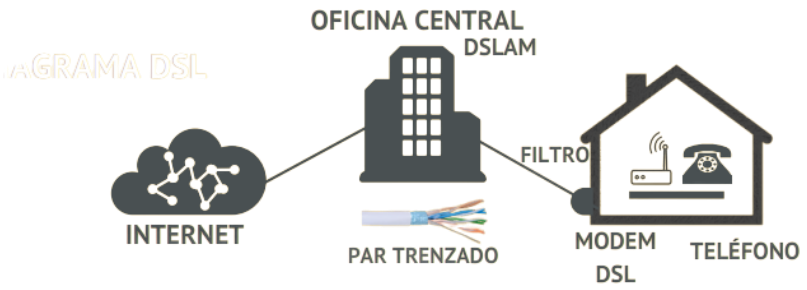
Existen varios tipos de arquitecturas alámbricas de un ISP en las que se puede clasificar acorde al tipo de tecnología que se utiliza para lograr obtener el acceso hacia el internet.

2.1.1.1. Diagrama DSL

La tecnología DSL (Digital Suscriptor Line) es aquella que su capacidad de transmisión de información puede llegar hasta los 7.1 Mbps a través del uso del par trenzado en líneas telefónicas. El servicio DSL puede variar en SDSL para velocidades simétricas en ancho de banda y ADSL para velocidades asimétricas. SDSL puede ser usado para aplicaciones que se necesitan las mismas velocidades en Downlink y Uplink como podrían ser servicio de video conferencias en empresas. Por otro lado, ADSL es usado por usuarios finales que no requieren mayor tráfico de datos en niveles de envió (Uplink) pero se requiere un mayor ancho de banda de descarga (Downlink). En la **Figura 3** se puede observar el diagrama DSL para conexión a internet (ARCOTEL, 2020).

Figura 3

Diagrama de conexión DSL



Nota: *adaptado de "Servicio de Acceso a Internet",* por ARCOTEL, 2020, p. 10.

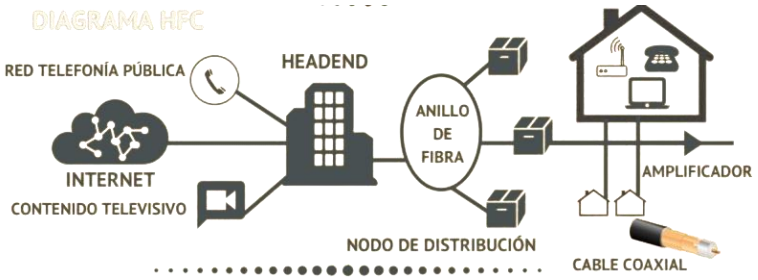
2.1.1.2. Diagrama HFC

Las HFC (Hybrid Fiber Coaxial) en un inicio es utilizado el cable coaxial para la emisión de información de descarga hacia un televisor para la televisión análoga. Las redes HFC fueron mejoradas para lograr establecer el tráfico de datos mediante el mismo cable coaxial con la ayuda del estándar DOCSIS 3.0 y 3.1.

Una ventaja frente a la tecnología DSL es su capacidad de transmisión de datos superior, pero con muchos inconvenientes para hacer que sea un tipo de tecnología con la cual se pueda acceder a los hogares debido a su costo y perdida de velocidad acorde a la distancia de despliegue hacia el usuario cliente. En la **Figura 4** se muestra el diagrama que ocupa HFC para establecer su transmisión de datos.

Figura 4

Diagrama HFC



Nota: *adaptado de "Servicio de Acceso a Internet",* por ARCOTEL, 2020, p. 10.

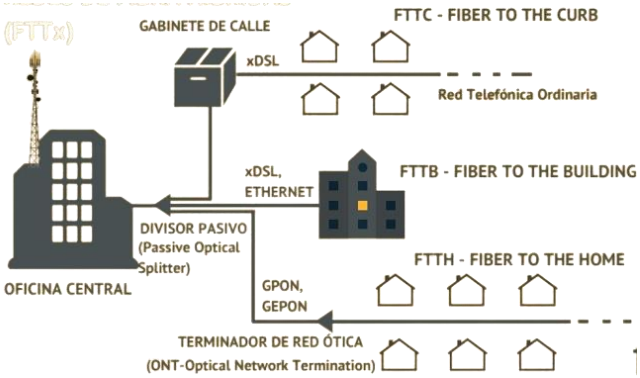
2.1.1.3. Diagrama FTTx

Las redes FTTx (Fiber To The X) son mucho más dedicadas para el uso en usuarios finales, las cuales llegan hasta el domicilio sin ningún tipo de inconveniente, ofrecen un costo mediano y accesible para el beneficiario. La tecnología FTTx ofrece un mayor rendimiento en comparación al resto de tecnologías gracias a su gran distancia de cobertura de hasta 80 km y altas velocidades acorde al tipo de versión con la que se esté trabajando.

En la **Figura 5** se muestra un modelo de diagrama de distribución híbrida de la fibra óptica.

Figura 5

Diagrama FTTx



Nota: *adaptado de "Servicio de Acceso a Internet",* por ARCOTEL, 2020, p. 10.

El desarrollo de la tecnología PON (Passive Optical Networks) ha permitido la utilización de elementos mucho más económicos los cuales no dependen de la electricidad e hizo que esta tecnología sea mucho más aceptada en comparación con las anteriores.

2.1.2. Tipos de ISP

Los diferentes tipos de ISPs se los clasifica dependiendo de las características que los definen de manera particular, tales como:

2.1.2.1. Por el rango de cobertura geográfica.

- *ISPs Locales*

Son proveedores pequeños los cuales poseen un área de cobertura limitada referentes a una ciudad o a una parte de esta.

- *ISPs Regionales*

Estos son proveedores de internet que cubren una determinada región. Estos ISPs manejan una infraestructura mucho más robusta y requieren de muchos nodos para lograr una administración completa.

- *ISPs Nacionales e Internacionales.*

El rango de cobertura de estos ISPs cuenta con infraestructura propia de telecomunicaciones y por lo general están conectados directamente con la salida al internet.

2.1.2.2. Por el número de usuarios.

Los usuarios influyen en otra manera de clasificación, en el cual de acuerdo con las regiones del país se puede apreciar mayor volumen de beneficiarios del servicio.

- *ISPs de nivel 1*

Poseen cobertura de manera global, el modo de ruteo no es por defecto debido a que poseen entradas para todas las conexiones de internet. Debido a que les pertenecen routers, enlaces de datos de alta velocidad y otros equipos que se interconectan con otro tipo de redes, buscan establecer una capacidad de envío de paquetes extremadamente elevada.

Algunas características que poseen los ISP nivel 1 son:

- ✓ Tener Cobertura Internacional
- ✓ Estar conectados a una red de ISP nivel 1

- ✓ Estar conectados a un gran número de ISP nivel 2

En el Ecuador algunas empresas que representan un ISP Tier 1 son: SETEL, CONECEL, CNT EP, MEGADATOS.

- *ISPs de nivel 2*

La infraestructura que poseen los ISPs nivel 2 es muy amplia al igual que los de nivel 1, lo que los diferencia es que los de tipo 2 se interconectan con los tipos 1 para que así su capacidad de transporte de datos se incremente y poder enviar mayor número de paquetes hacia el internet. La cobertura que brinda un ISP Tier 2 está comprendida en el área regional o nacional.

Están representados en el Ecuador por empresas que poseen gran cobertura a nivel servicio en el territorio, algunos ejemplos son: Netlife, Puntonet, Fibramax, Nedetel, entre otras.

- *ISPs de nivel 3*

Las empresas que conforman los ISPs de nivel 3 son aquellas que poseen pocos clientes finales. Sus tablas de enrutamiento se las realiza por defecto y estos están conectados a ISPs nivel 2 para poder tener acceso hacia el internet. La cobertura que brindan es de manera local dedicada a una provincia en específico o parroquia.

En el Ecuador existen muchas empresas de tipo 3 de las cuales se puede mencionar: Cinecable, Inno Fiber, CayambeVision, entre otras.

2.1.3. Parte regulatoria de los ISPs

En el marco legal para los proveedores del servicio de internet existen reglamentos, leyes y normas que rigen y que deben ser cumplidas y respetadas para el correcto funcionamiento de los ISPs dentro del país. Como la ley más importante del Ecuador es la Constitución la cual realiza la regulación de las acciones de las personas en su entorno.

En el Ecuador el organismo vigente para la regulación y control de las telecomunicaciones es el ARCOTEL, el cual nace de la ley Orgánica de Telecomunicaciones, con fecha de aprobación el 18 de febrero del 2015. Su principal objetivo es establecer el correcto servicio por parte de los agentes de Telecomunicaciones a los usuarios.

La eficiencia de un ISP radica en el desempeño que cumple en los objetivos planteados, tales como su funcionamiento, desde el punto de vista externo e interno de sus clientes. La alta disponibilidad de un ISP es lo que lo caracteriza debido a que en todo momento debe estar disponible para sus clientes, del mismo modo se garantizan factores técnicos como redundancia en la red, seguridad, solución rápida frente a fallas, reducir al mínimo el impacto en el servicio al cliente.

2.1.3.1. Requisitos para obtener el título habilitante

En la página web https://www.arcotel.gob.ec, las personas naturales pueden participar en el proceso de solicitud del Título Habilitante para el Servicio de Acceso a Internet ante la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), presentando los requisitos establecidos en la regulación actual. Los requisitos necesarios para realizar este trámite se encuentran en la página web oficial de ARCOTEL.

- ✓ Solicitud General (FO-CTHB-12).
- ✓ Datos de identidad de la persona y su cédula
- ✓ Documento notariado de la persona que busca realizar el procedimiento. (ver detalles en el numeral 3 del art. 38 de la Resolución 15-16-ARCOTEL-2019).
- ✓ Elaborar un plan que respalde la parte financiera de la persona.
- ✓ Plan de expansión de la red.

- ✓ Plan técnico en caso de ser inalámbricos
- ✓ Proyecto del AVIS
- Enlaces que van a ser usados de manera radioeléctrica
- Enlaces sujetos a uso de satélites

✓ Es necesario presentar un Certificado emitido por la Dirección General de Aeronáutica Civil (DGAC) que indique que la estructura no afectará a los sistemas de radionavegación aeronáutica. En caso de que la estructura se encuentre dentro de un radio de 500 metros de los sistemas de navegación aérea, se debe presentar un Certificado adicional. Se recomienda verificar la ubicación geográfica actualizada de los sistemas de navegación antes de realizar el trámite.

✓ La Declaración de Responsabilidad, que debe ser firmada por la persona natural, es un documento en el que se manifiesta bajo su responsabilidad que cumple con los requisitos establecidos por la normativa vigente para obtener y ejecutar el título habilitante, y que la información y los documentos presentados son verdaderos. Además, se informa que en caso de que la ARCOTEL verifique lo contrario, el trámite y el resultado final podrían ser negados. Este documento se encuentra identificado con el código FO-CTHB-12.

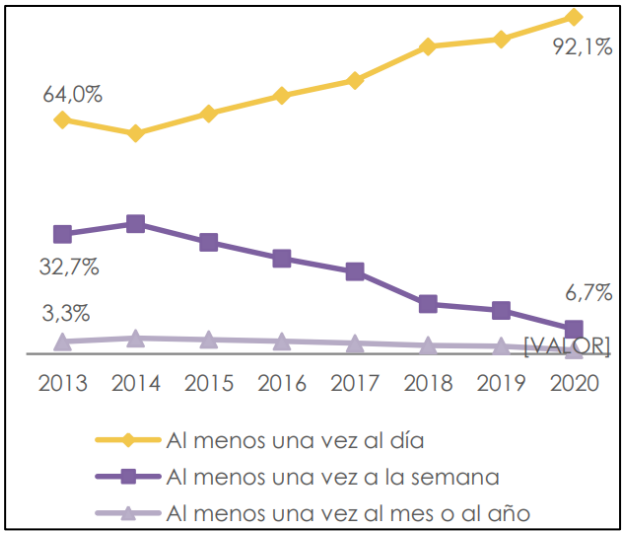
✓ En los procesos de otorgamiento de títulos habilitantes del régimen general de telecomunicaciones, el solicitante debe incluir una autorización que permita a la ARCOTEL solicitar información a las entidades y autoridades competentes para validar sus datos y determinar si está incurso en prohibiciones o inhabilidades. Esta autorización abarca información financiera y bancaria, sin que pueda alegarse el secreto bancario, y puede ser requerida durante la ejecución del título habilitante para fines de administración y control.

2.2. RED GPON

El requerimiento de conexiones hacia internet en el Ecuador ha aumentado considerablemente, según el boletín técnico emitido por el INEC en abril 2021 menciona que la frecuencia de conexión de internet a nivel nacional se ha incrementado drásticamente. Con el pasar de los años, la búsqueda del desvanecimiento de la brecha digital en el Ecuador se ha desarrollado de manera efectiva, arrojando como resultado un alto porcentaje de conectividad en el pueblo ecuatoriano. La **Figura 6** muestra un avance significativo basado en la frecuencia de uso de internet en un rango del año 2013 hasta el 2020.

Figura 6

ENEMDU Diciembre (2013-2017).



Nota: Encuesta Multipropósito (2018-2020).

El avance en las tecnologías orientadas a la transmisión de datos basada en la capacidad de envío y recepción de datos con mayor fiabilidad y velocidad ha permitido que se desarrollen nuevas ideas de transmisión que garanticen este paso de datos requeridos. Las redes de fibra óptica

son ideales para soportar un gran ancho de banda y altas velocidades de transmisión las cuales realizan el paso datos a través de hilos de fibra.

Una red basada en fibra permite enviar y recibir varios tipos de datos, tales como: servicio de televisión, telefonía e Internet. Todos estos tipos de servicios se pueden enviar a la vez usando un solo hilo de fibra haciendo uso de diferentes tipos de onda para cada uno de los servicios.

La tecnología GPON (Red Óptica Pasiva con Capacidad de Gigabit) a comparación de las tecnologías DSL y HFC ofrece mayor seguridad de la información, resistencia a interferencias electromagnéticas, menor atenuación de la señal, dando como resultado un tipo de red que satisface cada una de las necesidades de transmisión actuales a nivel de ISPs.

2.2.1. Análisis de la Tecnología GPON

La mayoría de las redes actuales utilizan GPON, este tipo de tecnología está establecida por la norma ITU-T G.984.x., en donde "x" hace referencia a toda la serie de recomendaciones (1, 2, 3, 4, 5, 6, 7), basadas en el estándar que buscan ayudar a tomar bases en el diseño y la certificación de las redes GPON proporcionando un criterio clave para mejorar el rendimiento. (Quisnancela & Espinosa, 2016)

Las primeras series de recomendaciones desde la ITU-T G.984.1 hasta la ITU-T G.984.4 hacen referencia a especificaciones básicas del sistema GPON:

- ITU-T G.984.1 → Especificaciones Generales.
- ITU-T G.984.2 → Especificaciones de Capa Física.
- ITU-T G.984.3 → Especificaciones de Capa Transporte.

- ITU-T G.984.4 → Especificaciones de Interfaz de Gestión y Control.

Las últimas series de recomendaciones dadas desde ITU-T G.984.5 hasta la ITU-T G.984.7 hacen referencia a:

- ITU-T G.984.5 → Banda de mejora.
- ITU-T G.984.6 → Extensión de alcance.
- ITU-T G.984.7 → Largo alcance.

La Tabla 1 muestra cómo se establecen cada una de las recomendaciones de la Norma ITU-T G.984.x, sus distintas versiones y las características que analiza en cada una de estas.

Tabla 1

Norma ITU-T G.984.x

Norma ITU-T G.984.x				
ITU-T G.984.1 (ITU-T. 2011)	Características Generales	Arquitectura del Sistema OAM. Tipos de Interfaz: servicio, usuario. cobertura	Tipos de Servicio Tasa física de transmisión y recepción Eficiencia del sistema	
ITU-T G.984.2 (ITU-T. 2012)	Medios Físicos dependientes.	**Parámetros Class B+** Potencia de salida máxima Potencia de salida mínima Sensibilidad mínima Potencia de salida mínima de sobrecarga	**ONT** + 5 dBm + 0.5 dBm - 27 dBm - 8 dBm	**OLT** + 5 dBm + 1.5 dBm - 28 dBm - 8 dBm
ITU-T G.984.3 (ITU-T. 2014)	Sincronización de Transmisión	Subcapas GPON	Estructura de Trama Protección de red Asignación dinámica de ancho de banda Gestión de red	
ITU-T G.984.4 (ITU-T. 2011)	Administración de ONT, descripción de la interfaz de control	Compatibilidad de OLTs y ONTs de ensambladores distintos		
ITU-T G.984.5 (ITU-T. 2014)	Optimización de transmisión	Asignación de longitudes de onda para señales de servicio. Especifica requisitos técnicos para aplicación de filtro en la ONT		
ITU-T G.984.6 (ITU-T. 2012)	Mayores Distancias	Explica la estructura y la conexión de los sistemas GPON de mayor cobertura.		

Nota: Cada una de las versiones que pertenecen al grupo ITU-T G.984.x trabajan de manera simultánea con especializaciones dentro la tecnología GPON. Fuente: Quisnancela, E., & Espinosa, N. (2016). *Certificación de redes GPON, normativa ITU G.984.x.*

- *Características de GPON*

Las especificaciones presentes en la tecnología GPON están ligadas a características como velocidad y la capacidad de acceso a servicios que ofrece este tipo de tecnología. Entre características de mayor importancia se tiene:

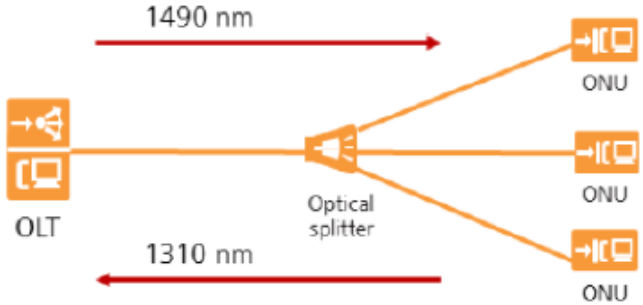
- Velocidad 2,4 Gbps (downstream).
- Velocidad 1,2 Gbps (upstream).
- Distancia máxima lógica: 60km.
- Distancia máxima física: 20km.
- Seguridad a nivel de protocolo: Cifrado.

- *Funcionamiento de transferencia de paquetes en GPON*

Una red GPON realiza el proceso de multiplexación en el tiempo la cual se conoce con el nombre de TDM (Time Division Multiplexing), este consiste en realizar el envío de información a través de diferentes espacios de tiempo. La **Figura 7** muestra el transporte de datos de acuerdo con la longitud de onda, en donde se utiliza la longitud de onda de 1490 nm para Downlink y 1310 nm para Uplink (Quisnancela & Espinosa, 2016).

Figura 7

Tráfico Bidireccional GPON

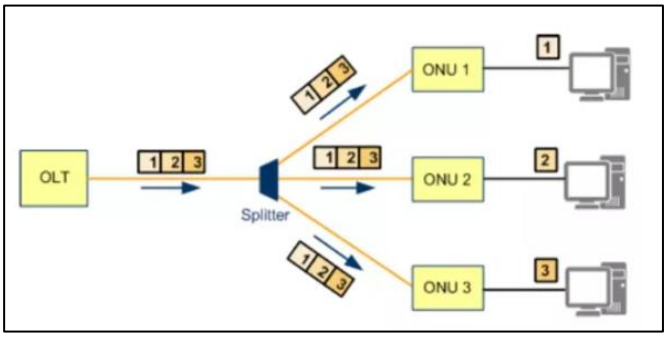


Nota. Extraído de: https://forum.huawei.com/enterprise/es/red-de-acceso-huawei-principios-de-gpon/thread/586574-100275

La **Figura 8** muestra cómo todo el tráfico generado en la OLT se divide en múltiples paquetes a través del Splitter Óptico hasta llegar a la ONU/ONT (Unidad de Red Óptica/ Unidad Terminal Óptica) del cliente.

Figura 8

Transferencia de Paquetes GPON.



Nota: Extraído de: https://www.redeszone.net/tutoriales/redes-cable/tecnologia-ftth-gpon-que-es-funcionamiento/

- *Modos de Multiplexación de datos GPON*

Según el foro oficial de Huawei menciona que: "Una red GPON implementa el modo de transmisión bidireccional sobre un mismo conductor de fibra el cual se realiza usando la tecnología WDM (Wavelength Division Multiplexing / División por Multiplexación de Longitud de Onda)" (Huawei, 2019). Para identificar las distintas señales que emiten los usuarios dentro de un mismo conductor de fibra se usan las siguientes tecnologías:

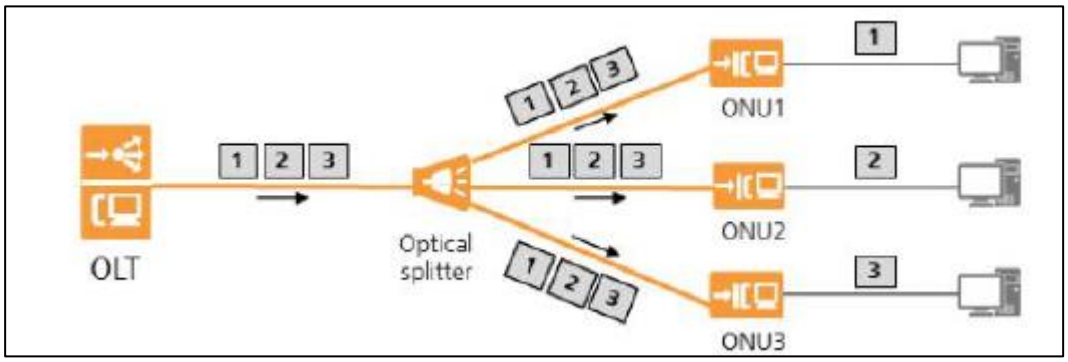
- Broadcast - Para el tráfico Downlink.
- TDMA – Para el tráfico de Uplink.

Tráfico Downlink: Como se muestra en la **Figura 9** la transmisión de datos de manera descendente se realiza mediante el uso de longitud de trama en 125 microsegundos, en donde todas

las ONU's receptan los datos y mediante el GEM PORT ID se logra distinguir los datos que tienen una ONU en específico para establecer comunicación (Huawei, 2019).

Figura 9

Tráfico Downlink GPON.

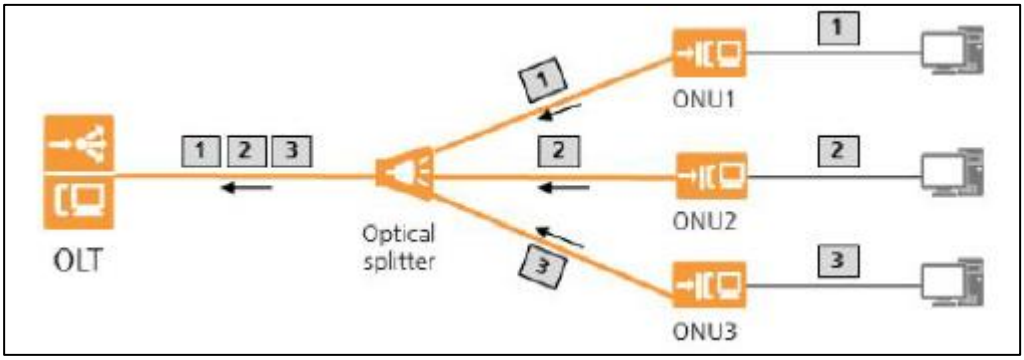


Nota: Extraído de: https://forum.huawei.com/enterprise/es/red-de-acceso-huawei-principios-de-gpon/thread/586574-100275

Tráfico Uplink: En GPON, la transmisión ascendente de datos sigue el esquema representado en la Figura 10. El tráfico fluye desde la ONU/ONT hasta la OLT, mediante el modo TDMA (Acceso Múltiple por División en el Tiempo). El enlace de subida se divide en distintos intervalos de tiempo que se asignan a cada ONU en función del ancho de banda que requiere. (Huawei, 2019).

Figura 10

Tráfico Uplink GPON



Nota: Extraído de: https://forum.huawei.com/enterprise/es/red-de-acceso-huawei-principios-de-gpon/thread/586574-100275

2.2.2. Arquitectura de la Tecnología GPON

La arquitectura de una red GPON consta de tres bloques los cuales se basan en la interconexión entre el bloque central y el bloque de los usuarios finales. A continuación, se determina los siguientes bloques:

- *OLT (Optical Line Termination)*

Terminal de línea óptica ubicado en la oficina central se representa en la **Figura 11**. Este es un elemento de tipo activo el cual se encarga de ser la fuente de potencia distribuida a lo largo de toda la red.

Figura 11

Optical LineTerminal - OLT

Nota: Extraído de: https://image.made-in-china.com/2f0j00sImYTJzErZkA/Gpon-Olt-Optical-Line-Terminal-Ma5680t-for-FTTH-FTTB-Telecom.jpg

- *ODN (Optical Distribution Network)*

La red de distribución óptica (Optical Distribution Network) incluye la red troncal o fuente, la red de distribución y la red distribuida. En el tramo perteneciente al ODN no se incluyen elementos ópticos activos. Estos elementos de carácter pasivo trabajan de manera bidireccional, en un rango de longitud de onda para el downstream de 1530 a 1570 nm, y para upstream entre 1280 hasta 1340 nm.

De con (Pérez Ruiz, 2019) los elementos que se utilizan para establecer la distribución óptica en una red GPON son:

- ✓ Patchcord UPC/AP.
- ✓ ODF (Distribuidor de Fibra Óptica).
- ✓ Splitters de primer nivel.
- ✓ Fibra de Distribución.
- ✓ Splitters de segundo nivel.
- ✓ Cables de acometida al hogar o DROP.
- ✓ Cajas de distribución (NAP - Nivel).
- ✓ Cajas terminales (NAP - Clientes).
- ✓ Roseta óptica.

- *ONT (Optical Network Terminal)*

Terminal de red óptica representado en la **Figura 12**, también conocida como ONU (Unidad de Red Óptica), está ubicada en las instalaciones del usuario final y proporciona una interfaz para el usuario. ONU y ONT son dispositivos que se colocan del lado del usuario, la diferencia que existe entre estas dos denominaciones al equipo final que se coloca al suscriptor de la línea de internet es su nombre. Esta diferencia surge debido al término que se utiliza para referirse a cada una de estos, en el caso de ONT es un término utilizado por la UIT-T mientras que ONU es el término utilizado en IEEE. (Pérez Ruiz, 2019)

Figura 12

Equipo ONT / ONU

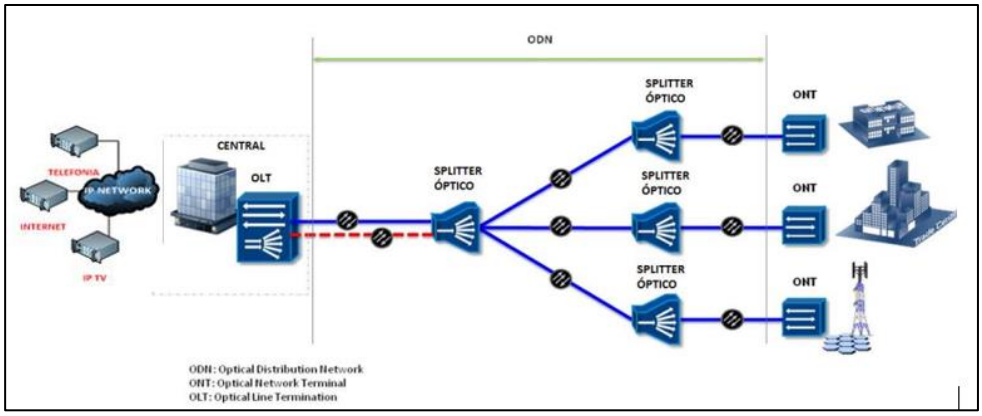
Nota: Extraído de: https://pluscompu.com/?product=ont-huawei-hg8546m

La Figura 13 muestra la arquitectura de una Red GPON. Para establecer la comunicación entre la OLT y la ONU/ONT se realiza el paso por el ODN, en donde se busca dividir la señal emitida por la OLT y desplegarla a través de la fibra óptica, para lo cual se hace uso de los splitters ópticos de primer y segundo nivel respectivamente, estos splitters permiten desplegar la red a varios puntos estratégicos cercanos a los usuarios finales, logrando así finalmente mediante el uso de una ONU/ONT se pueda receptar las señales emitidas por la OLT y se logre la comunicación entre estas.

La forma de distribución de la red se da de manera ordenada mediante el uso de las NAP(Network Access Point) las cuales permiten desplegar la red y son parte fundamental del ODN. Existen Splitters de primer y segundo nivel, los cuales deben cumplir con el máximo nivel de splitteo establecido de hasta 128 para módulos C++. (Quisnancela & Espinosa, 2016)

Figura 13

Arquitectura GPON



Nota: *adaptado de "Certificación de redes GPON, normativa ITU G.984.x", por Quisnancela, E., & Espinosa, N., 2016.*

2.2.3. Normativa de la Ley Vigente

La implementación de la tecnología GPON se rige en base a normas creadas para establecer un control sobre empresas y su despliegue a través de zonas urbanas y residenciales. Existen técnicas propias de cada uno de los ISP para el análisis de varios factores como: construcción de redes, representación de fibra óptica, diseño de despliegue de la red, entre otros, pero todos se basan en las normativas establecidas por el ARCOTEL.

La regulación para la implementación de la tecnología GPON en Ecuador se basa en la normativa establecida por la Resolución ARCOTEL-2017. De acuerdo con el artículo 313 de la Constitución del país, el Estado tiene el deber de gestionar, regular y controlar el sector de las Telecomunicaciones debido a su importancia para la economía nacional. Asimismo, el artículo 314 establece la obligación del Estado de garantizar el acceso a las telecomunicaciones a través de la regulación y el control.

El Artículo 466 del Código Orgánico de Organización Territorial-COOTAD establece la regulación del uso de la vía pública para la construcción, instalación y ordenamiento de redes destinadas a servicios de telecomunicaciones. Según este artículo, se debe priorizar el uso de

soterramiento para la construcción de redes, y solo en casos excepcionales se permitirá el uso de despliegue aéreo con la correspondiente autorización del Gobierno Autónomo Descentralizado.

La Ley Orgánica de Telecomunicaciones (LOT), publicada en el Registro Oficial No. 439, establece en su artículo 3 el Objetivo 5, el cual promueve el despliegue de redes e infraestructura de telecomunicaciones, incluyendo audio y video por suscripción. Además, se establece que este despliegue debe cumplir con las normas técnicas y políticas nacionales relacionadas con el soterramiento y ordenamiento de redes.

2.2.4. Ventajas y Desventajas de la Tecnología GPON

Una vez establecida la búsqueda relacionada a la Tecnología GPON se pueden identificar varios factores positivos y negativos al momento de tratar con este tipo de Tecnología, entre los cuales se tiene:

- *Ventajas*

- **Ancho de Banda:** Al ser una tecnología actual, GPON al momento de hablar de capacidad de transmisión es capaz de alcanzar una velocidad de hasta 2,5 Gbps en tráfico de bajada y 1,25 Gbps en tráfico de subida.

- **Distancia:** La fibra óptica permite alcanzar grandes distancias a comparación de las demás tecnologías llegando a un límite de 20km en GPON.

- **Calidad de Servicio**: Al ser una red capaz de transportar un gran ancho de banda, el usuario final puede ejecutar varios servicios simultáneos sin tener pérdida de paquetes o aumento de latencia en su conexión.

- **Operabilidad**: GPON puede administrar sus equipos de manera fácil mediante comandos desde la OLT.

- **Escalabilidad**: Las redes de fibra óptica se pueden escalar fácilmente, debido a su capacidad de splitteo que actualmente ofrece de hasta 128.

- *Desventajas*

- **Delicadeza:** GPON es una red ampliamente débil en lo que trata a fragilidad del material, esto debido a que la fibra como su nombre lo dice está construida en vidrio lo cual lo hace sensible a rupturas, además todo el conjunto de equipos para la red posee módulos con lectores ópticos sensibles a daños por suciedad y humedad.
- **Precio:** El precio de implementación de fibra óptica es elevadamente caro, por lo cual en lugares rurales se ha visto mayormente la presencia de esta, mientras que en sectores urbanos todavía no se a desplegado este tipo de tecnología debido al costo de tendido de fibra.
- **Detección de daños:** La capacidad de solución ante daños y como poder detectarlos únicamente se los puede realizar con equipos especializados para FO, por lo tanto, son equipos costosos en el mercado.

2.3. CLOUD COMPUTING

El concepto de *Cloud Computing* se estableció en el 2006 por George Gilder el cual menciona en su artículo denominado "Las fábricas de la información". En este documento se presenta el modelo de una nube virtual similar a una estructura de computación. El (National Institute of Standars and Technology) también conocido como NIST define al Cloud Computing como un modelo para habilitar el acceso a la red, de manera rápida, eficaz y segura, los cuales la integran redes, servidores, aplicaciones y servicios (NIST, 2012).

El modelo en la nube se compone de características esenciales como las que se muestran a continuación:

- **Autoservicio:** Un usuario cliente del Cloud Computing puede administrar los servicios ofrecidos, como tiempo del servidor y almacenamiento en red, sin necesidad de interacción humana con cada proveedor de servicios.
- **Acceso a la red:** Todos los servicios alojados en el Cloud Computing están disponibles a través de la red los cuales pueden ser accedidos por medios de dispositivos conectados a la red a través de plataformas en computadores, tablets, teléfonos inteligentes, entre otros.
- **Servicio Múltiple:** Los servicios en la nube están diseñados para permitir múltiples conexiones de usuarios clientes a través del modelo multiusuario, en el cual los recursos físicos y virtuales son asignados acordes a la demanda establecida por el consumidor.
- **Elasticidad:** Las capacidades ofrecidas por los servicios en la Nube con capaces de expandirse con gran facilidad lo cual permite obtener una escalabilidad en el servicio.
- **Servicio Controlado:** Los sistemas en el Cloud controlan y optimizan de manera automática el uso de recursos lo que permite aprovechar la capacidad de almacenamiento, procesamiento, ancho de banda y las cuentas activas de los usuarios. El servicio controlado permite monitorear, controlar e informar.

La nube sin embargo no es un espacio ilimitado, ya que depende de una infraestructura física. En la Figura 14 se muestra un servidor físico el cual permite establecer el desarrollo del *Cloud Computing.*

Figura 14

Servidor Físico.

Nota: Extraído de: https://gr9iacav.files.wordpress.com/2020/03/cloud-computing-indesign-completo.pdf

2.3.1. Modelos de despliegue en el Cloud

Existen diferentes tipos de modelos de despliegue en la nube que se caracterizan por su propiedad, tamaño y acceso. Actualmente, se pueden identificar cuatro modelos de despliegue en la nube, los cuales se detallan a continuación:

2.3.1.1. Nube Privada

La nube privada es la más seleccionada por las compañías que buscan una mayor protección de datos, en donde el entorno del Cloud es gestionado por un solo cliente el cual controla las aplicaciones que se van a ejecutar. Las empresas compran su propio servidor local y administran a los usuarios que quieren que tengan acceso hacia esta. Una ventaja del uso de las nubes privadas es que las empresas poseen privacidad en la información, por lo cual no pone en riesgo sus datos privados.

2.3.1.2. Nube en Comunidad

La nube en comunidad proporciona servicios para que se haga uso privilegiado únicamente en empresas que comparten objetivos similares. El método de administración de este modelo de Cloud puede ser ejecutado por las propias empresas, por terceros o por alguna alianza entre ellos. La ventaja principal del uso de una nube en comunidad es la reducción de costes.

2.3.1.3. Nube Pública

Según (Ortiz, 2014) menciona que "La nube pública estará disponible para el público en general o a un grupo grande de compañías que tengan acceso a internet y es de propiedad de una empresa que vende servicios en la nube". La ventaja del uso de las Nubes Públicas es que no es necesario la inversión en infraestructura, pero siempre teniendo en cuenta la seguridad de la información, la cual es netamente responsabilidad del proveedor del servicio.

2.3.1.4. Nube Híbrida

Una nube híbrida es en la que se combinan modelos de nube pública y privada; en donde el usuario que adquiere el servicio tiene unas partes y comparte varias, de manera limitada. Algunas empresas de servicios se ocupan de este tipo nube según las necesidades del usuario, porque la aplicación no es la misma del hogar al negocio.

2.3.2. Servicios en el Cloud

Los servicios en el Cloud se pueden desplegar mediante plataformas informáticas, en los cuales se accede a varios servicios en a nube de internet. Existen distintas formas de desplegar los servicios en el Cloud de las que se puede mencionar:

2.3.2.1. Software as a Service – SaaS

El Software como Servicio es aquel en el cual el proveedor de servicio pone a disposición tanto la infraestructura física como la plataforma de funcionamiento del servicio, la administración de SaaS es realizada por el proveedor (Merchán Campos, 2018).

Este tipo de servicio es una solución de software otorgada a través de servicios en la nube. Según (Merchan, 2018) menciona que "El cliente arrienda el uso de un servicio para su organización y los usuarios acceden al servicio desde Internet con un navegador web. El software y los datos que

se procesan en las aplicaciones están ubicados en el Datacenter del proveedor. La empresa pone en marcha y ejecuta aplicaciones a un mínimo costo."

- *Ventajas de usar SaaS*

- El servicio SaaS tiene escalabilidad en la cual el usuario que adquiere el servicio únicamente paga por lo que usa.
- Gran parte de sus aplicaciones se montan mediante un navegador por lo que es más sencilla de ejecutar.
- Fácil alcance hacia los datos sin importar la ubicación debido a que todos estos están almacenados en el cloud. Lo que permite acceso mediante dispositivos móviles.

2.3.2.2. Plataform as a Service – PaaS

Una plataforma como servicio es aquella en la que la infraestructura al igual que el resto cuenta con: servidores, redes, almacenamiento. Sin embargo, también se hace la implementación de programas informáticos, sistemas, software.

(Microsoft Azure, 2017) menciona que "PaaS incluye infraestructura (servidores, almacenamiento y redes), pero también middleware, herramientas de desarrollo, servicios de inteligencia comercial (BI), sistemas de administración de bases de datos y más."

- *Ventajas*

- El uso de PaaS permite evitar gastos y la complejidad de comprar licencias de software, administración de middleware
- El usuario se encarga de administrar las aplicaciones y las aplicaciones que desarrolla. El proveedor del servicio se encarga de administrar lo demás.

- Variedad de funcionalidades de la implementación sin necesidad de aumentar personal para su funcionamiento.
- Facilidad de desarrollo de aplicaciones en diversas plataformas.

2.3.2.3. Infraestructure as a Service – IaaS

Es un tipo de servicio en el cloud el cual ofrece recursos primordiales de cómputo, capacidad de almacenamiento y estructura física. En donde el usuario posee el manejo administrativo de aquellos SO(sistemas operativos), aplicaciones y centros de datos, los cuales son entregados por el proveedor del servicio (Microsoft Azure, 2017).

- *Ventajas*

- Permite el control dedicado del usuario a los sistemas internos y físicos del servicio Cloud.
- El usuario tiene el poder de controlar los sistemas operativos, aplicaciones y bases de datos que son entregados en la infraestructura, y un control restringido sobre los componentes de red.

2.3.3. Ventajas y Riesgos del Cloud Computing

- Ventajas

- Posibilidad de acceder a programas y archivos desde cualquier ubicación y dispositivo con conexión a Internet, lo que permite la gestión remota de los mismos.
- Reducir el gasto en equipamiento, software y mantenimiento es posible gracias a la gestión y configuración de los programas empresariales a través de un equipo con menos recursos, lo que disminuye la necesidad de contratar personal especializado y, en consecuencia, la inversión necesaria.

- Mayor estabilidad y flexibilidad, ya que los proveedores de computación en la nube ofrecen a los usuarios soluciones robustas y altamente adaptables, además de garantizar una mayor seguridad en los servicios que se ofrecen.

- *Riegos*

- La información se guarda en lugares de almacenamiento compartidos. En situaciones de este tipo, los datos delicados de la organización podrían estar almacenados en el mismo servidor que los de otras empresas.
- Si el proveedor de servicios no cumple con los estándares adecuados en cuanto a seguridad, puede haber una mayor vulnerabilidad de los datos de la empresa, lo que pone en riesgo su integridad, disponibilidad y confidencialidad.
- Una alternativa de despliegue que proporciona mayor control a las empresas es la del Cloud Privado. Esta opción es utilizada por grandes empresas o instituciones que necesitan tener completo control sobre la seguridad.

2.4. ADMINISTRACIÓN Y GESTIÓN DE LA RED

El proceso de administración de una red se basa en optimizar la red tanto a nivel de infraestructura como a nivel lógico. Un sistema de administración de redes trabaja en áreas principales como: monitoreo de rendimiento, administración de configuración, registro de diagnósticos (Ceballos Mendoza & Badillo Angulo, 2004). La administración ha tenido un progreso tecnológico en los últimos años, logrando técnicas de gestión de redes y datos, que permiten controlar y gestionar arquitecturas lógicas, configuración de equipos y detección de errores. La necesidad de administrar una red de datos surge con la búsqueda de mejorar el

desempeño en cuatro áreas específicas: planeación, organización dirección y control, todas estas basados en el ámbito administrativo (Jaramillo & Torres, 2015).

La gestión de la red se refiere al conjunto de actividades establecidas para controlar, supervisar y organizar de mejor manera los recursos de telecomunicaciones, buscando así un servicio controlado y adecuado. El principal objetivo es garantizar: la disponibilidad de servicio, mejorar el rendimiento e incrementar la efectivad de la red (Jaramillo & Torres, 2015).

La Figura 15 muestra el sistema de gestión y administración de una red y las características que posee.

Figura 15

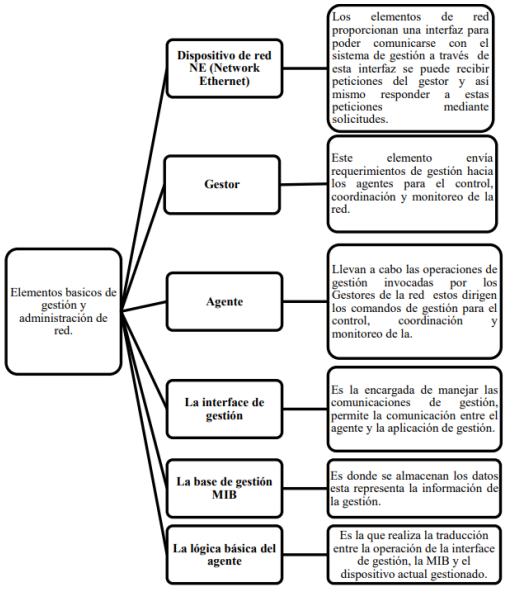
Sistema de Gestión de Red

Nota: Obtenido de http://www4.ujaen.es/~mdmolina/grr/Tema%201.pdf

El modelo de gestión y administración de red se basa en un enfoque tradicional de cliente-servidor, que consta de diversos componentes que permiten su correcta administración. En la Figura 16 se pueden observar cada una de las partes que conforman la administración y gestión de la red, como son: dispositivos de red, gestores, agentes, interfaces de gestión, bases de gestión y la lógica fundamental del agente.

Figura 16

Elementos de la Gestión y Administración.



Nota: Extraído de: http://www.ramonmillan.com/tutoriales/snmpv3.php

2.4.1. Principales Modelos de Administración de red

La necesidad de normalizar mediante parámetros a la administración de la red hace que sean establecidos 3 modelos de gestión fundamentales: Administración OSI, Administración Internet – SNMP y la Arquitectura TMN.

2.4.1.1. Administración OSI – FCAPS

Se establece en la norma ITU-M.3400 un conjunto de funciones denominadas Áreas Funcionales de los Sistemas de Gestión (SMFA8) o FCAPS (Fllas, Configuración, Contabilidad, Rendmiento, Seguridad), las cuales dividen las tareas de administración en cinco categorías para una mejor organización.

La Figura 17 ilustra el modelo FCAPS, que se compone de 5 áreas principales de gestión de redes: gestión de fallas, gestión de configuración, gestión de contabilidad, gestión de desempeño y gestión de seguridad. FCAPS es un modelo que clasifica los objetivos de la gestión de redes en diferentes categorías (Arroyave Arredondo, 2013).

Figura 17

Modelo FCAPS.

Nota: Extraído de: https://www.zpesystems.com/wp-content/uploads/2020/10/FCAPS-525x300-1.jpg

- *F - Fault Management (Gestión de Fallas)*

En este nivel se detectan y solucionan los problemas de la red, además se toman medidas preventivas para evitar futuros problemas. De esta manera, se garantiza que la red esté en constante operación y se minimice el tiempo de inactividad.

- *C - Configuration Management*

En este nivel, se realiza la supervisión y control del funcionamiento de la red. Se lleva a cabo la gestión del hardware y software, incluyendo la adición de nuevos dispositivos y programas, la modificación de los sistemas y la eliminación de equipos fuera de servicio. También se encarga de mantener actualizado el inventario de equipos y programas de forma periódica.

- *A - Accounting Management*

Tiene como función la asignación equitativa y eficiente de los recursos entre los usuarios de la red, lo que permite el uso óptimo de los sistemas disponibles y minimiza los costos de operación. Además, es responsabilidad de este nivel asegurarse de que los usuarios sean facturados de manera adecuada.

- *P - Performance Management:*

Este nivel se enfoca en la administración del rendimiento global de la red, con el objetivo de maximizar su eficiencia, evitar cuellos de botella y detectar posibles problemas. Es fundamental identificar mejoras para aumentar la integridad de la red.

- *S - Security Management:*

En este nivel, se lleva a cabo la protección de la red contra la actividad de hackers, el acceso no autorizado de los usuarios y cualquier daño físico o electrónico. Es de vital importancia garantizar la confidencialidad de la información de los usuarios, salvo en casos justificados o necesarios.

2.4.1.2. Administración Internet – SNMP

El protocolo de gestión de red Simple Network Management Protocol (SNMP) es un protocolo de capa de aplicación que posibilita el tránsito de datos de gestión entre dos ususarios en una red. SNMP es un componente del conjunto de protocolos TCP/IP. La parte administrativa de red pueden utilizar SNMP para monitorizar el rendimiento de la red, identificar y solucionar problemas, y planificar el crecimiento de la red. A continuación, se presenta un resumen de todo lo descrito en la Tabla 2.

Tabla 2

Versiones comparativas de SNMP

Protocolo	Características	Comandos	RFC
SNMPv1	• Generación de Traps. • Envió de notificaciones.	• GET • GET-NEXT • SET	• 1155 • 1157 • 1212
SNMPv2	• Mejora en la Seguridad	• GET-BULK • REQUEST • INFORM-REQUEST	• 1441-1452
SNMPv3	• Autenticación robusta. • Mejora en la seguridad.	• Capacidad adicional de administración	• 1902-1908 • 2271-2275

Nota: Cada una de las versiones de SNMP trabajan actualmente acorde a la aplicación que se le brinde. Fuente: (Jaramillo & Torres) (Administración y Gestión de la red inalámbrica del Gobierno Autónomo Descentralizado (GADIP) del Cantón Cayambe basada en el modelo funcional FCAPS De La ISO, 2015)

2.4.1.3. Arquitectura TMN

TMN (Telecommunications Management Network) es una arquitectura que está orientada a la gestión de los recursos de la red a través de interfaces predefinidas. TMN – LLA (Logical Layered Architecture) utiliza un enfoque jerárquico para el modelado del despliegue de recursos y entidades de gestión dentro del sistema (Songhurst, 1999). Según la recomendación de la (UIT-T, 2000) menciona que TMN se divide en cuatro niveles de administración y gestión, como lo son:

- *Capa de gestión de elementos*

Se ocupa de los recursos de red de nivel inferior (por ejemplo, los sistemas de conmutación) y depende de las características técnicas del equipo gestionado. El seguimiento del rendimiento, el control y la recopilación de métricas contables se encuentran entre las responsabilidades que corresponden a esta capa de gestión.

- *Capa de administración de red*

Proporciona una visión más amplia de la red dentro de la cual se implementan y administran las conexiones. La agrupación jerárquica de los sistemas de conmutación se puede utilizar para la definición de redes de capas, donde los grupos de nodos en una capa aparecen como un solo nodo para la capa superior.

- *Capa de gestión de servicios*

Es el entorno donde se implementa la lógica del servicio y se utilizan los recursos de la red para proporcionar servicios. Los mecanismos de gestión y control de servicios se implementan a través de interfaces que facilitan la comunicación con dominios administrativos y sistemas de gestión adyacentes.

- *Capa de gestión empresarial*

Se ocupa de las relaciones comerciales entre las partes interesadas y los propietarios de diferentes partes de la infraestructura. Esta capa no está estrictamente definida ya que se supone que acomoda funciones que corresponden a los aspectos comerciales del despliegue del servicio.

3. CAPITULO III – DESARROLLO DEL PROYECTO

El presente capítulo inicia con el análisis de la empresa CayambeVisión S.A., con el fin de conocer el tipo de servicio que ofrece, infraestructura, modelo actual de trabajo, ubicación, así como otras características técnicas que describen de mejor manera la empresa.

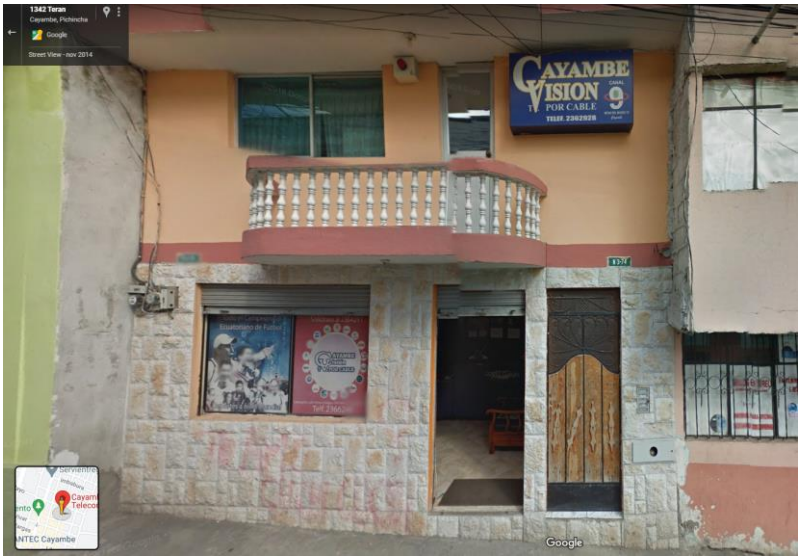
De esta manera se obtiene información actual de la empresa y así posteriormente establecer una comparativa mediante el uso de un benchmarking competitivo el cual permita la selección de las herramientas de gestión y administración que sean capaces de adaptarse a las necesidades de la empresa y de sus clientes.

3.1. SITUACIÓN ACTUAL DE LA EMPRESA

La empresa CayambeVisión S.A., inicia sus operaciones en el año de 2013 en la Zona 2 del Ecuador, ubicada al norte de la provincia de Pichincha en el Cantón Cayambe tal y como se muestra en la **Figura 18**.

Figura 18

Ubicación CayambeVisión S.A.



Nota: Extraído de: Google Maps

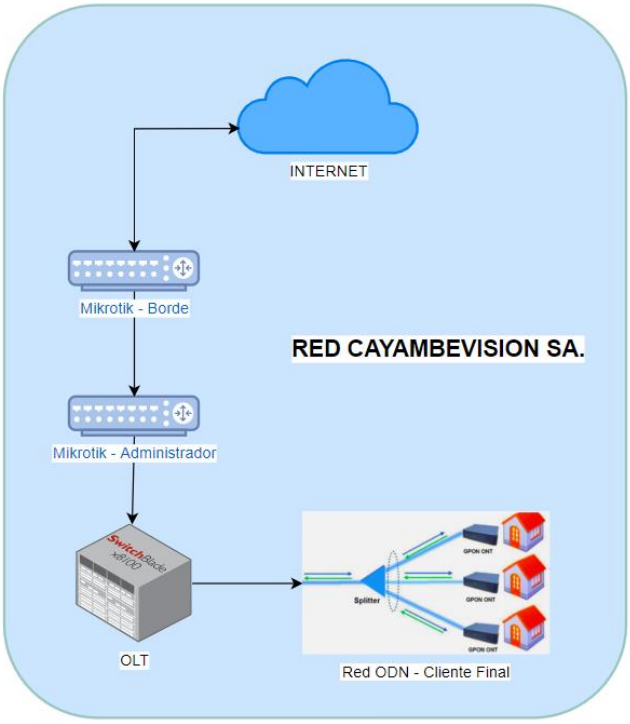
Sus inicios en las Telecomunicaciones surgen con la prestación de servicios de Televisión por Cable, con el paso de los años y el desarrollo de las tecnologías, el internet se constituye como una herramienta demandada por sus clientes, por lo cual la empresa realiza una inversión en infraestructura buscando brindar a la comunidad de Cayambe el servicio de Internet.

De acuerdo con la información recibida a mano de los funcionarios y cuerpo administrativo de CayambeVisión S.A., en la actualidad la topología de red se basa en una red de fibra óptica FTTH con tecnología GPON.

En este sentido, la Red de datos CayambeVisión S.A. se despliega a través de equipos de networking conectados por medio de interfaces físicas tanto para la salida hacia el exterior de la red (Internet) como para la prestación de servicio a los usuarios de manera local (Red GPON). La **Figura 19** muestra la topología actual de la red de Backbone de la empresa.

Figura 19

Backbone CayambeVisión S.A.



Nota: Fuente: Diagrama de datos - CayambeVisión S.A

Para el levantamiento de información sobre la interconexión de la topología de red, se genera un recorrido por el nodo central de la empresa, en la cual se evidencian los equipos mostrados anteriormente en la

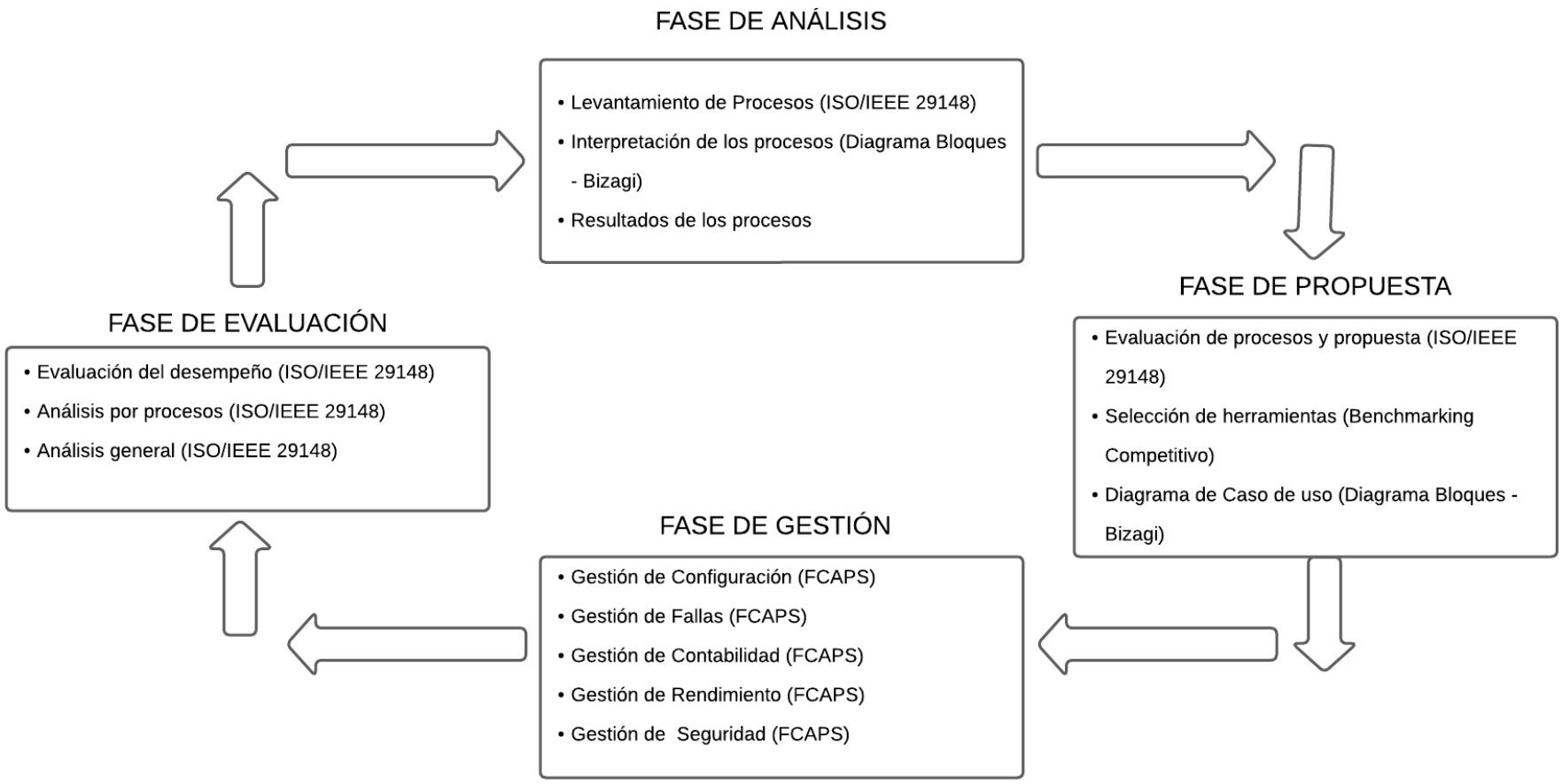
Figura 19 y su función correspondiente dentro de la red.

3.2. MODELO METODOLÓGICO

El presente proyecto se desarrolla siguiendo un modelo metodológico que consta de cuatro fases interconectadas, cuya finalidad es garantizar la calidad y eficiencia del proceso de implementación de un software en la empresa CayambeVision S.A... Modelo mostrado en la Figura 20.

Figura 20

Propuesta Metodológico



- ✓ Fase de Análisis

Se lleva a cabo el levantamiento de los procesos a través de la implementación de la norma ISO/IEEE 29148. Esta fase permitirá identificar los procesos críticos de la empresa y establecer los requisitos necesarios para su optimización. También se realiza una interpretación de los procesos a través del diagrama de bloques en Bizagi, lo que permitirá una mejor visualización y comprensión de los procesos.

- ✓ Fase de Propuesta

Se evalúan los procesos identificados en la fase anterior y se proponen soluciones y mejoras para optimizarlos. Para esto se utilizará la norma ISO/IEEE 29148 y se realizará un benchmarking competitivo para seleccionar las herramientas más adecuadas. Además, se elaborará un caso de uso mediante el diagrama de bloques en Bizagi, que permitirá visualizar de manera clara y precisa la propuesta de mejora de los procesos.

- ✓ Fase de Gestión

En este proceso se lleva a cabo la gestión del desarrollo de cada uno de los servicios basados en el modelo FCAPS, donde se realiza un análisis preventivo de los procesos para mejorar el rendimiento de la gestión en la empresa CayambeVision S.A. De esta manera, se asegura la implementación de buenas prácticas empresariales a nivel de procesos.

- ✓ Fase de Evaluación

Se evalúa el desempeño del software implementado a través de la norma ISO/IEEE 29148. Se realiza un análisis por cada proceso y un análisis general para evaluar el impacto de los cambios en la empresa. De esta manera, se garantizará la mejora continua de los procesos y la satisfacción del cliente.

3.3. LEVANTAMIENTO DE PROCESOS

La obtención de la información y el correcto levantamiento de procesos dentro de la empresa CayambeVision S.A., se realiza mediante el planteamiento referencial del modelo de gestión basado en la norma ISO/IEEE 29148, la cual hace referencia a la documentación de aquellos procesos existentes dentro de la empresa, a partir de la aplicación de criterios y métodos necesarios para el planteamiento y la representación de los escenarios.

Para llevar a cabo el levantamiento de información sobre los casos de estudio existentes, se establece un análisis de los escenarios con un enfoque metodológico mixto; es decir, se lo ejecuta a través de un análisis cuantitativo con el objetivo de calificar con valores numéricos el tiempo de ejecución para cada uno de los procesos, mientras que el análisis cualitativo se lo destina para entender de mejor manera los procesos y ayudar a representarlos, las técnicas destinadas para este análisis son: observación y entrevistas. Esta metodología aplicada para el levantamiento y representación de los procesos se los puede observar en la **Tabla *3***.

Tabla 3

Metodología de levantamiento y representación de procesos

LEVANTAMIENTO DE PROCESOS	Recolección de la información	Entrevista
	Visualización del entorno de trabajo	Observación
	Toma de tiempos	Tiempos mediante cronómetro

REPRESENTACIÓN DE PROCESOS	Procesos de Información	ISO/IEEE 29148
	Diagramación de los procesos	Bizagi Modeler

3.3.1. La Entrevista

Inicialmente se realiza una entrevista con el gerente de la empresa en donde se busca la socialización de la situación actual de la empresa, el conocimiento de su formación y las áreas que se encuentran (Ver ANEXO 1). Una vez obtenida la información, se aplica la entrevista a todo el personal perteneciente a cada una de las áreas (Oficina, Cobradores, Departamento Técnico, Administración de Red) de la empresa CayambeVision S.A. con el objetivo de conocer las actividades y procedimiento que se desarrollan en cada una de las áreas logrando así conocer la situación actual y así poder plantear los escenarios que se ejecutan en cada uno de los departamentos de la empresa.

3.3.2. Observación

Mediante el uso de la observación se logra entender de mejor manera el trabajo de cada una de las áreas, de igual manera se puede identificar la carga de actividades que puede o no poseer cada una de las áreas. Logrando así obtener una visión mucho más clara con respecto a los procesos y subprocesos que se desarrollan.

3.3.3. Interpretación de los procesos

Para realizar la representación de los procesos se realiza un modelado en la herramienta *Bizagi* en donde se establece mediante diagramas de flujos las actividades que se realizan en cada

una de las áreas responsables a eventos mencionados dentro de la empresa. De esta manera se obtiene una lista de procesos mostrados a continuación los cuales serán detallados posteriormente:

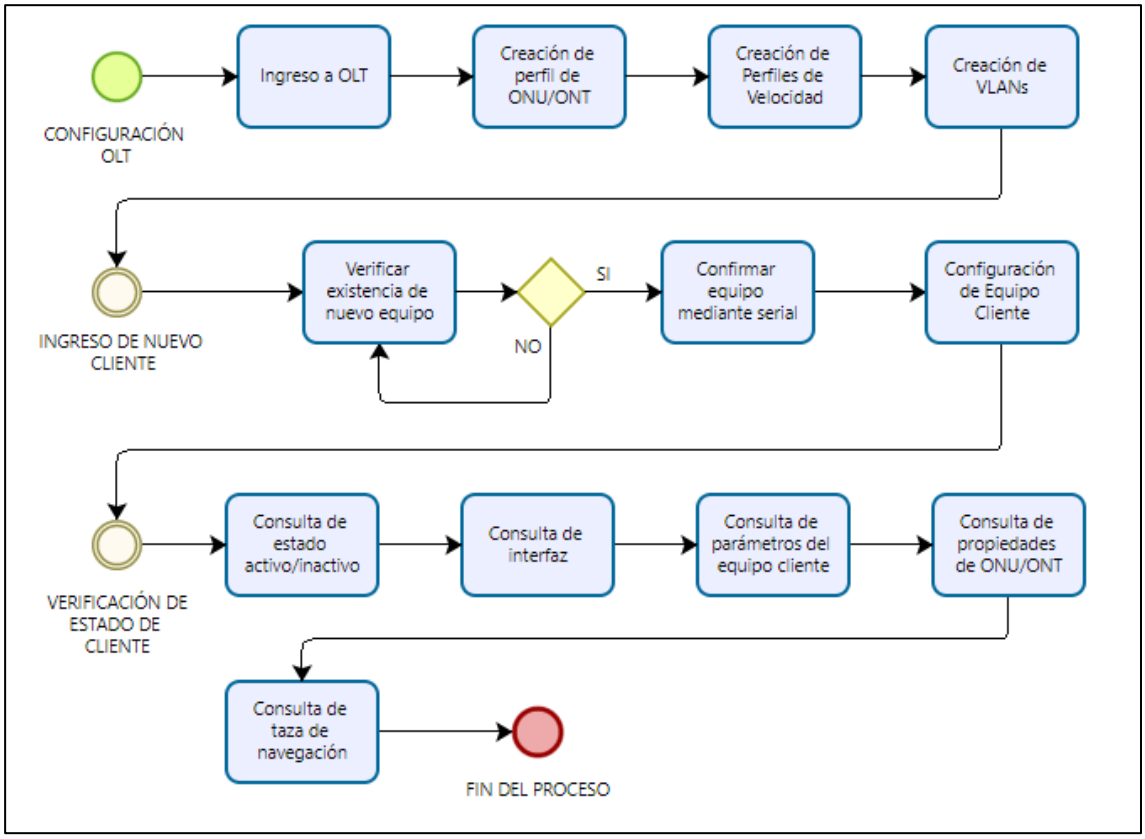
- *Procesos en la Gestión actual de red*
    - *Configuración de OLT*
    - *Ingreso de Clientes (ONU/ONT)*
    - *Comandos de Verificación de Estado*
- *Procesos en la Administración actual de la red*
    - *Ingreso de Clientes*
    - *Suspensión de servicio*
    - *Pago de Servicios*
    - *Generación de Tickets de Soporte*

✓ *Procesos en la Gestión de red*

El proceso de Gestión se basa en el manejo de los dispositivos de red conocidos como OLT y ONT/ONUs. En la empresa CayambeVisión S.A., estos procesos indicados en la **Figura 21** representan un tiempo de respuesta relativamente alto de ejecución para el Administrador de la red, debido a que cada uno de los procesos se lo realiza de forma directa en la OLT.

Figura 21

Procesos Administrativos en la actualidad.



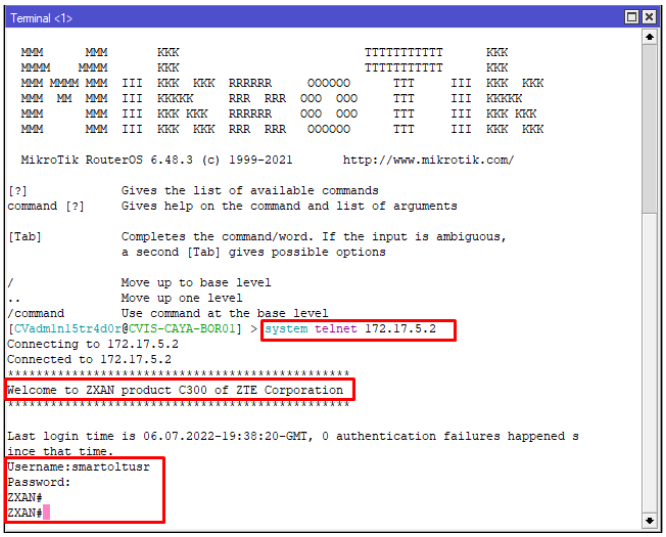
3.3.3.1. PROCESO 1: Configuración de OLT

- *Ingreso a la OLT*

El método de ingreso se lo realiza mediante sentencias de comandos desde el equipo de administración. La **Figura 22** muestra la conexión vía Telnet hacia la dirección IP establecida en la interfaz de administración de la OLT.

Figura 22

Ingreso a OLT.



- *Configuración perfil de la ONU/ONT GPON*

Para la configuración de nuevos perfiles en la OLT, inicialmente se define el tipo de ONU/ONTa ingresar, una descripción en base a los puertos que posee y otro tipo de características que representan al equipo que se busca ingresar; Entre las características a configurar se tiene:

maxgemport: Representa el número máximo de puerto virtual para realizar encapsulación y transmitir paquetes entre OLT y ONU.

max-tcont: Corresponde al valor máximo relacionado con el libre fluido de paquetes.

max-switch-perslot: Es el número máximo de unidades de conmutación por ranura.

max-flow-perswitch: Representa el máximo valor de división por puerto físico de la ONU.

En este sentido, a manera de ejemplo se presenta el ingreso de un nuevo modelo de ONU tipo ZTEG-F660, con un fluido de paquetes igual a 7, un puerto virtual de 32 y algo más importante, la sintaxis del comando empleado se detalla a continuación:

```
1.    ZXAN(config)#pon
2.    ZXAN(config-pon)#onu-type ZTEG-F660 gpon description 4FE,2POTS
max-tcont 7 maxgemport 32 max-switch-perslot 1 max-flow-perswitch 32
service-mgmt-via-non-omci WiFi enable omci-send-mode sync
```

De igual forma se define el *max-flow-perswitch* con valor de 32 el cual permite el fluido de paquetes privilegiado. Otro parámetro importante es la activación del servicio de administración, wifi y la sincronización de la ONU

- *Configuración de perfiles de velocidad*

Estos se definen mediante el ingreso del perfil tcont con el cual se hace referencia al nombre que llevaría el perfil de velocidad que en este caso se definen como *20M* y *50M.* La configuración se lleva a cabo mediante los siguientes comandos:

```
1.    ZXAN(config)#gpon
2.    ZXAN(config-gpon)#profile tcont 20M type 5 fixed 64 assured 64
maximum 20000
3.    ZXAN(config-gpon)#profile tcont 50M type 5 fixed 64 assured 64
maximum 50000
```

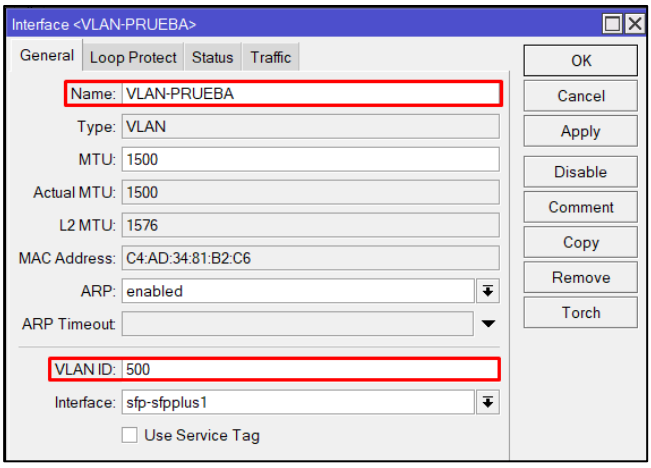
El tipo 5 en el valor de *tcont* abarca todas las configuraciones, y permite el libre fluido de paquetes, los demás limitan en direcciones y privilegios. Mientras que los valores de *fixed* y *assured* se relacionan con el ancho de banda asegurado en la ONU.

- *Configuración de VLAN*

A continuación, se procede con la creación de VLANs, el cual es un factor fundamental para la intercomunicación entre el equipo de Administración y la red interna de la OLT. En este caso de configuración se asigna el ID de VLAN (*500*) y un nombre descriptivo para la VLAN (*VLAN-PRUEBA).* Se debe tomar en cuenta que se coloca el mismo VLAN-ID creado en el equipo de administración, tal como se muestra en la **Figura 23**.

Figura 23

Creación de VLAN – Mikrotik Administrador.



En este sentido, considerando las indicaciones previas, se establece la creación de VLANs en la OLT mediante el ingreso de los siguientes comandos:

```
1.    ZXAN#configure terminal
2.    ZXAN(config)#vlan database
3.    ZXAN(vlan)#vlan 500 name VLAN-PRUEBA
```

Una vez creadas las VLANs en la OLT, se busca generar un paso troncal desde el equipo Mikrotik-CCR1036 que tiene la función de Administrador hacia la red interna de los clientes, por lo tanto, se realiza las configuraciones mostradas a continuación en la interfaz SFP de la OLT que interconecta con el equipo de administración:

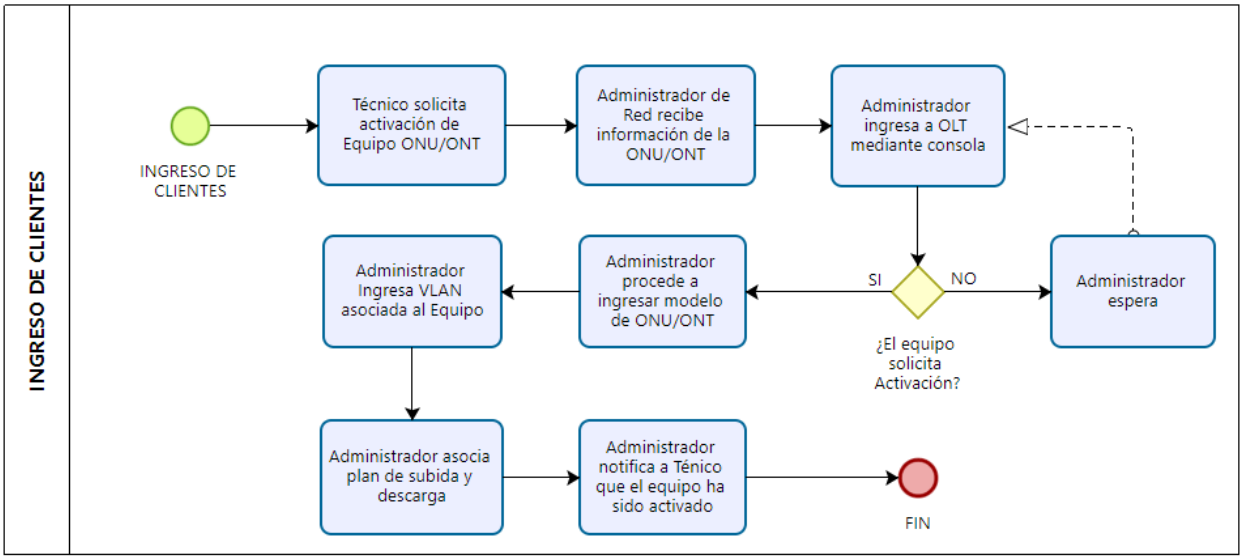
```
1.    ZXAN#configure terminal
2.    ZXAN(config)#interface xgei_1/19/2
3.    ZXAN(config-if)#switchport mode trunk
4.    ZXAN(config-if)#switchport vlan 500 tag
```

3.3.3.2. PROCESO 2: Ingreso de Clientes (ONU/ONT)

El ingreso de nuevos clientes en la empresa CayambeVision S.A. se la realiza siguiendo el orden mostrado en la **Figura *24***, como resultado del proceso se obtiene la validación de una ONU/ONT cliente, proceso el cual posteriormente se representará a través de una situación real usando directamente el puerto de la consola de la OLT. Este proceso se lo toma a través de la perspectiva del Administrador actual de la Red.

Figura 24

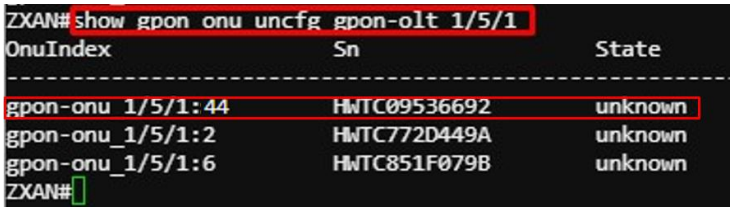
Ingreso de Cliente Actual



Para el ingreso de nuevos usuarios se procede a verificar la existencia de ONUs que necesiten activación y sean reconocidas por la OLT, esto se lo hace mediante el comando `show gpon onu uncfg` con el cual se puede observar una lista de los equipos que están en estado desconocido (unknown), lo cual representa que todavía no están registrados en la OLT. La **Figura 25** muestra lo mencionado anteriormente.

Figura 25

Estado ONU.



Una vez identificado el equipo respectivo de la lista y reconocida la ONU confirmando el número de serie alojado en la parte posterior del equipo como se muestra en la **Figura 26**, se procede a ingresar a la interfaz asignada a la ONU de manera automática por medio de la OLT. Para este caso se usa el comando *interface gpon-onu_1/5/1:3*.

Los parámetros de la interfaz que se asigna a la ONU corresponden a los siguientes parametros:

gpon-onu_{chasis}/{slotid}/{port}:{onu-index}

Chasis: Espacio físico de salida de interfaces GPON.

Slotid: Número de tarjeta asignado en el chasis.

Port: Puerto de salida físico de la OLT.

Onu-index: ID de interfaz virtual asignado a la ONT.

Figura 26

Numero Serial ONT

Posterior a esto se realiza el ingreso a la interfaz del equipo y se agregan las siguientes sentencias para la configuración de la ONU en la cual se definen: nombre, habilitación de servicio, asignación de perfil de velocidad, habilitación del puerto e ID, y asignación de VLAN.

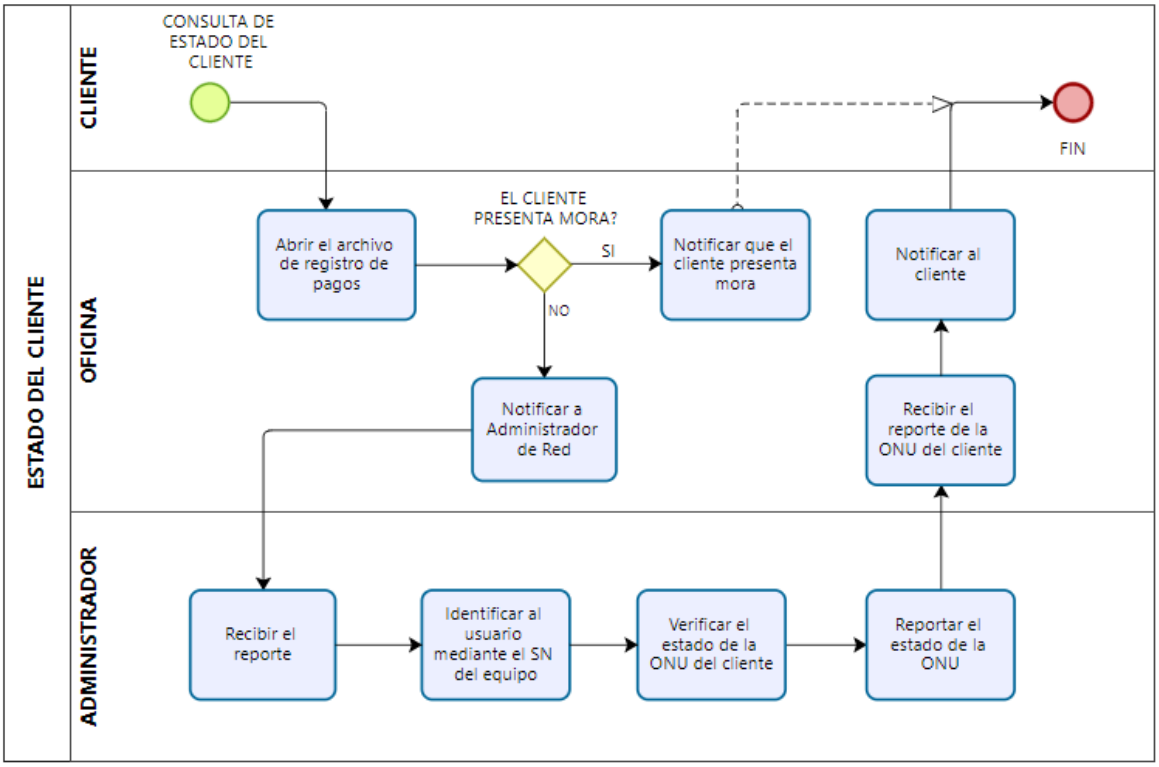
```
1.    ZXAN#configure terminal
2.    ZXAN(config)#interface gpon-onu_1/5/1:44
3.    ZXAN(config-if)#name Prueba_ONU
4.    ZXAN(config-if)#sn-bind enable sn
5.    ZXAN(config-if)#tcont 1 profile SMARTOLT-Estudiantil_20M-UP
6.    ZXAN(config-if)#gemport 1 tcont 1
7.    ZXAN(config-if)#gemport 1 traffic-limit downstream SMARTOLT-
Estudiantil_20M-DOWN
8.    ZXAN(config-if)#service-port 1 vport 1 user-vlan 500 vlan 15
```

3.3.3.3. PROCESO 3: Comandos de Verificación de Estado

Los comandos de verificación de estado se basan en consultas generadas por parte del administrador de la red para así obtener reportes de información tales como: perfiles de la ONU, ancho de banda, estado de la ONU e información detallada sobre los estados del equipo final del cliente. De esta manera se plantean los comandos más utilizados para realizar este tipo de filtrado de datos en la OLT. Este proceso es representado en la **Figura 27**.

Figura 27

Comandos de Verificación de Estado

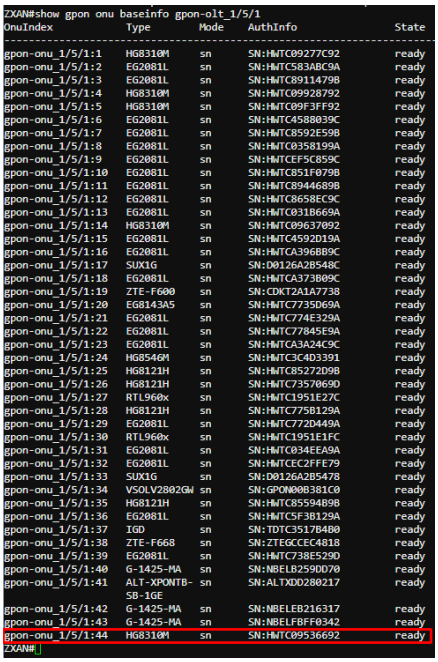


- *show gpon onu baseinfo*

Como resultado de este comando se muestra en la **Figura 28** un resumen de un conjunto de datos que hace referencia a la interfaz (OnuIndex), modelo (Type), número serial (AuthInfo) y el estado (State) de las ONUs.

Figura 28

Consulta OLT



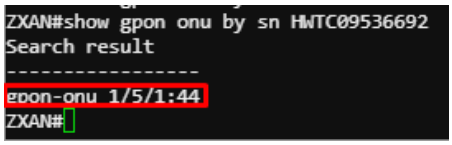
```
ZXAN#show gpon onu baseinfo gpon-olt_1/5/1
OnuIndex            Type        Mode    AuthInfo                State
-------------------------------------------------------------------------
gpon-onu_1/5/1:1    HG8310M     sn      SN:HWTC09277C92         ready
gpon-onu_1/5/1:2    EG2081L     sn      SN:HWTC583ABC9A         ready
gpon-onu_1/5/1:3    EG2081L     sn      SN:HWTC8911479B         ready
gpon-onu_1/5/1:4    HG8310M     sn      SN:HWTC09928792         ready
gpon-onu_1/5/1:5    HG8310M     sn      SN:HWTC09F3FF92         ready
gpon-onu_1/5/1:6    EG2081L     sn      SN:HWTC4588039C         ready
gpon-onu_1/5/1:7    EG2081L     sn      SN:HWTC8592E59B         ready
gpon-onu_1/5/1:8    EG2081L     sn      SN:HWTC0358199A         ready
gpon-onu_1/5/1:9    EG2081L     sn      SN:HWTCEF5C859C         ready
gpon-onu_1/5/1:10   EG2081L     sn      SN:HWTC851F079B         ready
gpon-onu_1/5/1:11   EG2081L     sn      SN:HWTC8944689B         ready
gpon-onu_1/5/1:12   EG2081L     sn      SN:HWTC8658EC9C         ready
gpon-onu_1/5/1:13   EG2081L     sn      SN:HWTC031B669A         ready
gpon-onu_1/5/1:14   HG8310M     sn      SN:HWTC09637092         ready
gpon-onu_1/5/1:15   EG2081L     sn      SN:HWTC4592D19A         ready
gpon-onu_1/5/1:16   EG2081L     sn      SN:HWTCA396BB9C         ready
gpon-onu_1/5/1:17   SUX1G       sn      SN:D0126A2B548C         ready
gpon-onu_1/5/1:18   EG2081L     sn      SN:HWTCA373B09C         ready
gpon-onu_1/5/1:19   ZTE-F600    sn      SN:CDKT2A1A7738         ready
gpon-onu_1/5/1:20   EG8143A5    sn      SN:HWTC7735D69A         ready
gpon-onu_1/5/1:21   EG2081L     sn      SN:HWTC774E329A         ready
gpon-onu_1/5/1:22   EG2081L     sn      SN:HWTC77845E9A         ready
gpon-onu_1/5/1:23   EG2081L     sn      SN:HWTCA3A24C9C         ready
gpon-onu_1/5/1:24   HG8546M     sn      SN:HWTC3C4D3391         ready
gpon-onu_1/5/1:25   HG8121H     sn      SN:HWTC85272D9B         ready
gpon-onu_1/5/1:26   HG8121H     sn      SN:HWTC7357069D         ready
gpon-onu_1/5/1:27   RTL960x     sn      SN:HWTC1951E27C         ready
gpon-onu_1/5/1:28   HG8121H     sn      SN:HWTC775B129A         ready
gpon-onu_1/5/1:29   EG2081L     sn      SN:HWTC772D449A         ready
gpon-onu_1/5/1:30   RTL960x     sn      SN:HWTC1951E1FC         ready
gpon-onu_1/5/1:31   EG2081L     sn      SN:HWTC034EEA9A         ready
gpon-onu_1/5/1:32   EG2081L     sn      SN:HWTCEC2FFE79         ready
gpon-onu_1/5/1:33   SUX1G       sn      SN:D0126A2B5478         ready
gpon-onu_1/5/1:34   VSOLV2802GW sn      SN:GPON00B381C0         ready
gpon-onu_1/5/1:35   HG8121H     sn      SN:HWTC85594B9B         ready
gpon-onu_1/5/1:36   EG2081L     sn      SN:HWTC5F3B129A         ready
gpon-onu_1/5/1:37   IGD         sn      SN:TDTC3517B4B0         ready
gpon-onu_1/5/1:38   ZTE-F668    sn      SN:ZTEGCCEC4818         ready
gpon-onu_1/5/1:39   EG2081L     sn      SN:HWTC738E529D         ready
gpon-onu_1/5/1:40   G-1425-MA   sn      SN:NBELB259DD70         ready
gpon-onu_1/5/1:41   ALT-XPONTB- sn      SN:ALTXDD280217         ready
                    SB-1GE
gpon-onu_1/5/1:42   G-1425-MA   sn      SN:NBELEB216317         ready
gpon-onu_1/5/1:43   G-1425-MA   sn      SN:NBELFBFF0342         ready
gpon-onu_1/5/1:44   HG8310M     sn      SN:HWTC09536692         ready
ZXAN#
```

- *show gpon onu by sn HWTC09536692*

Con este comando se puede buscar la interfaz de conexión de una ONU mediante el ingreso de su número serial tal como se muestra en la **Figura 29**.

Figura 29

Consulta OLT



```
ZXAN#show gpon onu by sn HWTC09536692
Search result
-----------------
gpon-onu_1/5/1:44
ZXAN#
```

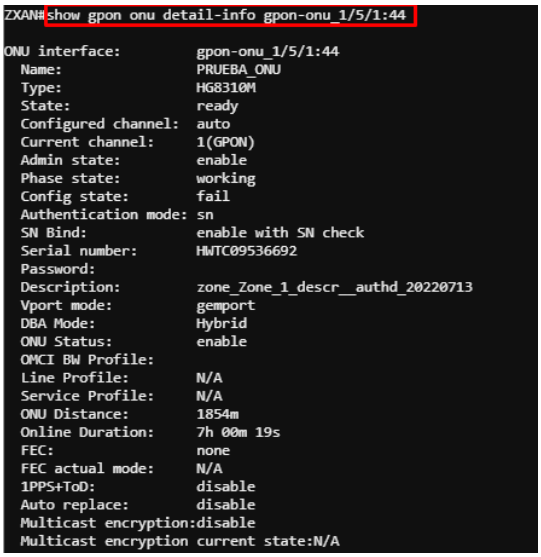
- *show gpon onu detail-info gpon-onu_1/5/1:44*

El comando obtiene información de propiedades de la ONU de manera actualizada, tales como: nombre, tipo, estado, modo de autenticación, numero serial, distancia desde la OLT a la

ONU, estado de conexión y tipos de logs que se almacenan y las posibles causas que las generan, de esta manera se observa los resultados en la **Figura 30**.

Figura 30

Consulta de estado OLT.

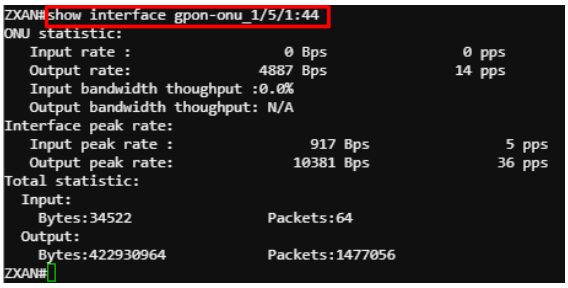


- *show interface gpon-onu_1/5/1:44*

Con el comando presente se puede verificar estadísticas referentes a la taza de navegación de la ONU de manera actualizada como refleja la **Figura 31**.

Figura 31

Consulta de interface en OLT



✓ *Procesos en la Administración de red*

Actualmente la administración de la red se complementa con áreas asociadas, tales como: área de soporte, área de finanzas, área técnica y notificación de suspensión de servicios. El

administrador de red menciona que se ha tenido problemas relacionados con actividades asociadas al trabajo conjunto de todas estas, como: cortes de servicio, reportes de daños en el cliente, reportes duplicados, pagos ingresados con retraso, entre otros.

El paso de información con destino al área administrativa por parte de técnicos, área de finanzas, área de soporte y notificación de suspensión de servicios, ingresa inicialmente a manos de secretarias para posteriormente entregarse a su destino. Esto ha ocasionado problemas debido al proceso largo que se tiene en el paso de la información hasta el área de administración.

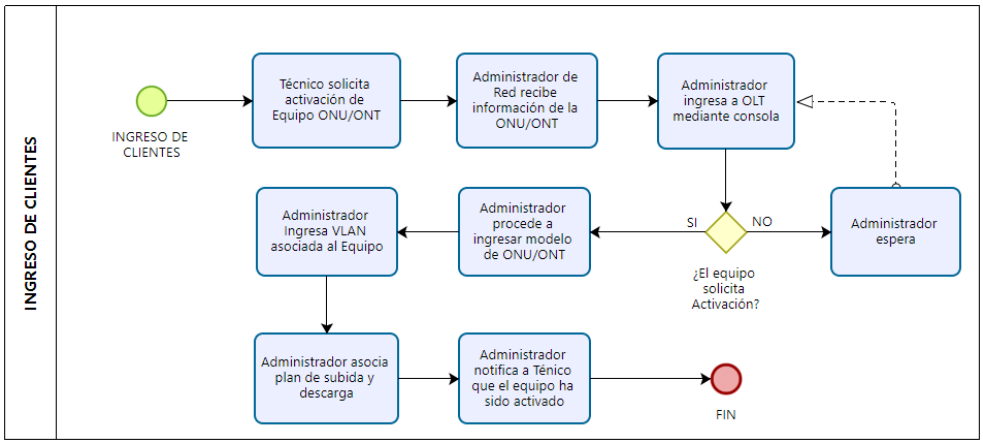
A continuación, se detallan escenarios de procesos actuales que se relacionan con la administración de la red.

3.3.3.4. PROCESO 4: Ingreso de Clientes

El ingreso de clientes se realiza en conjunto con el área de soporte técnico, los cuales una vez realizada la acometida interna en el domicilio del cliente proceden a solicitar la activación del equipo final (ONU/ONT), con el fin de permitir la navegación hacia el internet por parte del usuario cliente. De esta manera se define el proceso que se ejecuta para realizar esta acción en la **Figura *32***.

Figura 32

Ingreso de Clientes

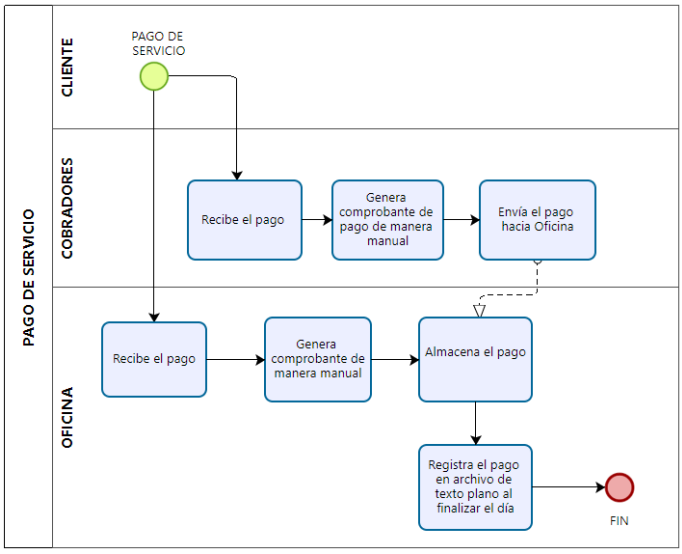


3.3.3.5. PROCESO 5: Pago de Servicios

El pago de servicios se lleva a cabo de dos maneras, el cliente realiza el pago a los cobradores de la empresa y la otra en la que el cliente de manera directa genera el pago a la empresa. La **Figura 33** muestra el proceso que se lleva a cabo para el registro y validación de un cobro de servicio. El registro de pagos a la base Excel se acumula en la parte de secretaría lo que significa una carga laboral extra.

Figura 33

Proceso pago de servicio

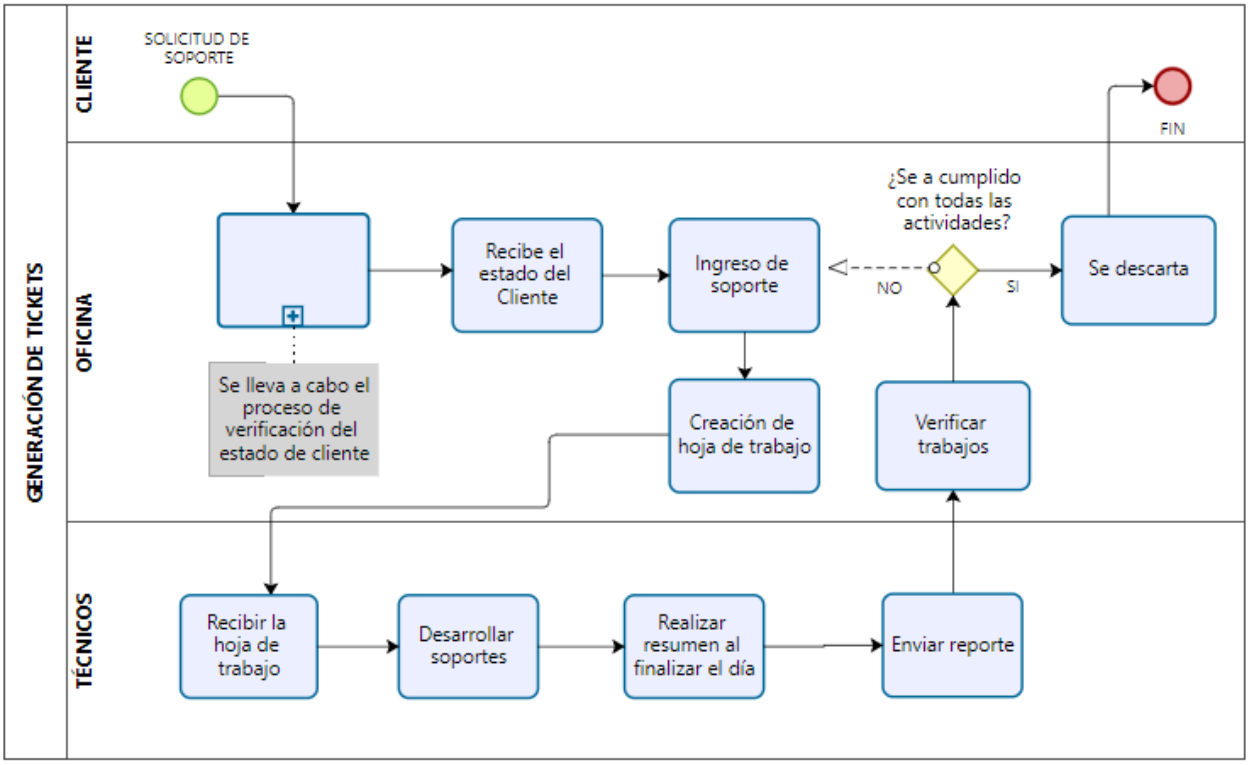


3.3.3.6. PROCESO 6: Generación de Tickets de Soporte

Como muestra la **Figura 34** este es un proceso tedioso ya que se realiza el paso de información por tres áreas distintas iniciando en la parte técnica en el primer escenario y en el segundo de parte de secretaría. Esto ocasiona que la información diagnóstica del estado del cliente llegue tardía.

Figura 34

Proceso actual de generación de tickets



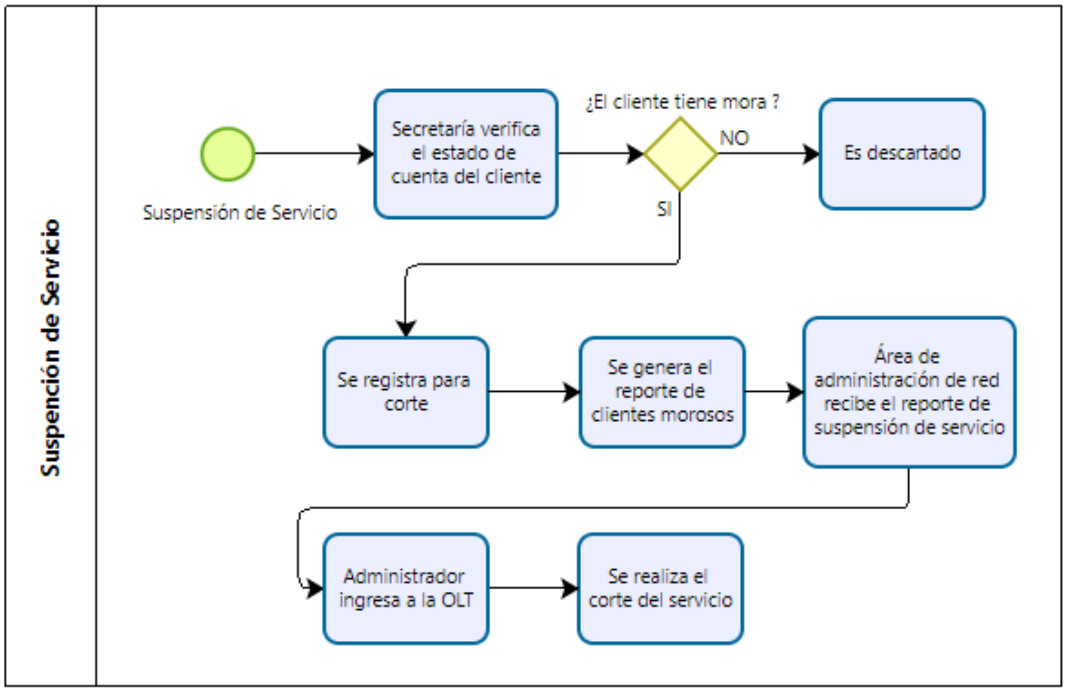
3.3.3.7. PROCESO 7: Suspensión de servicio

La empresa maneja como fecha límite de pago el 10 de cada mes, posterior a esto el cliente es ingresado para realizar un corte de servicio. Los usuarios identificados como morosos por parte de secretaría una vez llevado todo el proceso de validación si existe algún tipo de mora o no, genera

un reporte con los nombres de aquellas personas morosas para ser puestas a corte como se muestra **Figura 35**.

Figura 35

Proceso de suspensión de servicio



3.3.4. Toma de tiempos

Para realizar la toma de tiempos de aquellos procesos identificados, se establece un método de medición vía cronómetro, el cual consiste en la toma de muestras correspondientes al tiempo de respuestas ante de los distintos escenarios identificados a lo largo del desarrollo de este apartado. Esto se lo realiza con el fin de obtener un valor de tiempo aproximado para cada proceso e identificar posteriormente al número de encargados para cada una de las actividades y el desempeño de estas actividades dentro de la empresa De esta manera se establece la siguiente **Tabla *4***.

Tabla 4

Ficha de toma de Tiempos

PROCESO	Subproceso	Tiempo 1 (Minutos)	Tiempo 2 (Minutos)	Tiempo 3 (Minutos)	Promedio (Minutos)
Procesos en la Gestión de red	Configuración de OLT	60 min	50 min	55 min	55 min
	Ingreso Cliente (ONU)	10 min	12 min	9 min	10 min
	Comandos Verificación de estado	15 min	13 min	10 min	13 min
Procesos en la Administración de red	Ingreso de Clientes	15 min	12 min	14 min	14 min
	Pago de Servicio	15 min	13 min	11 min	13 min
	Generación de Tickets de Soporte	12 min	18 min	13 min	14 min
	Suspensión del servicio	9 min	12 min	11 min	11 min

3.3.5. Resultados de los procesos

Una vez establecida la representación y el análisis de cada uno de los procesos, subprocesos y actividades que se desarrollan en la empresa CayambeVision S.A. se puede determinar que existen tiempos de respuesta altos para la ejecución de cada uno de los distintos escenarios planteados a lo largo de este apartado. De la misma manera se analiza la interacción entre las áreas al momento de llevar a cabo un proceso en específico. De esta manera se obtiene como resultado la **Tabla *5***, en donde se muestra el resumen de referencia basado de la norma ISO/IEEE 29148 para el levantamiento de información.

Tabla 5
Resultado de Análisis de Procesos

PROCESO	Subproceso	Tiempo 1 (Minutos)	Tiempo 2 (Minutos)	Tiempo3 (Minutos)	Promedio (Minutos)	Áreas Encargadas	Intervención de áreas
Procesos en la Gestión de red	Configuración de OLT	60 min	50 min	55 min	55 min	Administrador	1
	Ingreso Cliente (ONU)	10 min	12 min	9 min	10 min	Administrador Técnicos	2
	Comandos Verificación de estado	15 min	13 min	10 min	13 min	Oficina Administrador	2
Procesos en la Administración de red	Ingreso de Clientes	15 min	12 min	14 min	14 min	Oficina	1
	Pago de Servicio	15 min	13 min	11 min	13 min	Oficina Cobradores	2
	Generación de Tickets de Soporte	12 min	18 min	13 min	14 min	Oficina Técnicos	2
	Suspensión del servicio	9 min	12 min	11 min	11 min	Oficina Cobradores Administrador	3

3.4. EVALUACIÓN DE PROCESOS Y PROPUESTA DE CAMBIO

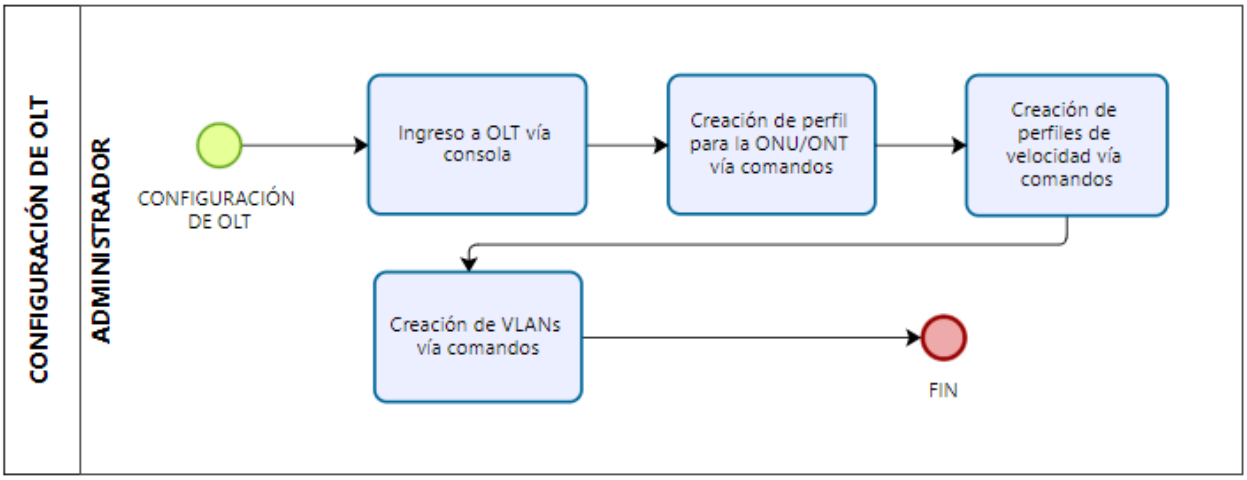
3.4.1. PROCESO 1 - Configuración de OLT

El administrador actual de la red menciona al proceso 1 como uno de los que más dificultad se presenta al momento de su ejecución, esto debido al método usado para desarrollar esta actividad. La manera en la cual se realiza la configuración actual de la OLT es mediante comandos ingresados directamente a través de consola, por lo cual es necesario el uso de grandes tiempos de demora para su ejecución tal como refleja el resultado obtenido en el apartado 3.2.4 encargado de analizar un tiempo promedio para cada actividad.

La solución que se presenta par mejora el tiempo de ejecución para el presente proceso es la implementación del enlace el SISTEMA 1 hacia la OLT alojada en la red interna de CayambeVision S.A., el cual sea capaz de enviar sentencias de comandos a través de un entorno gráfico lo cual simboliza mayor rapidez al momento de llevar a cabo la configuración de cada uno de los subprocesos mostrados en la .

Figura 36.

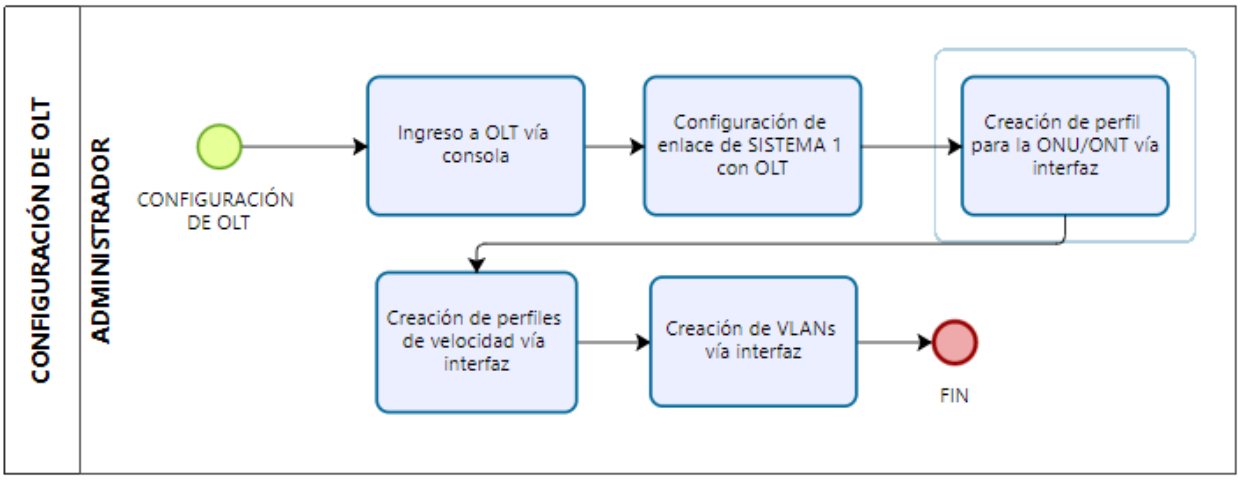
Figura 36 Configuración Actual de OLT



El número total de acciones realizadas no representa un cambio ya que son necesarias para posteriormente ingresar ONU/ONTs clientes, lo que se busca a través de la implementación del

SISTEMA 1 es la forma sencilla de configuración de la OLT gracias a la interfaz gráfica que presenta y a la facilidad de enlace que existe entre el SISTEMA 1 y la OLT. Obteniéndose así el nuevo modelo presentado en la **Figura *37*** como una solución en cuanto al tiempo ocupado para llevar a cabo este proceso.

Figura 37 Configuración de OLT - Solución



3.4.2. PROCESO 2 y PROCESO 4 – Ingreso de Clientes

En la empresa CayambeVision S.A. se desarrolla el proceso anteriormente mostrado en la **Figura *24***, en el cual se busca el ingreso de un nuevo cliente a la red. Para ingresar un nuevo cliente se realiza alrededor de ocho acciones previas a la culminación del evento. Según el administrador actual de la red, esto toma alrededor de 10 minutos en promedio por cada activación solicitada por parte de los técnicos, debido a que las configuraciones son ingresadas en base a comandos manuales hacia la consola de la OLT.

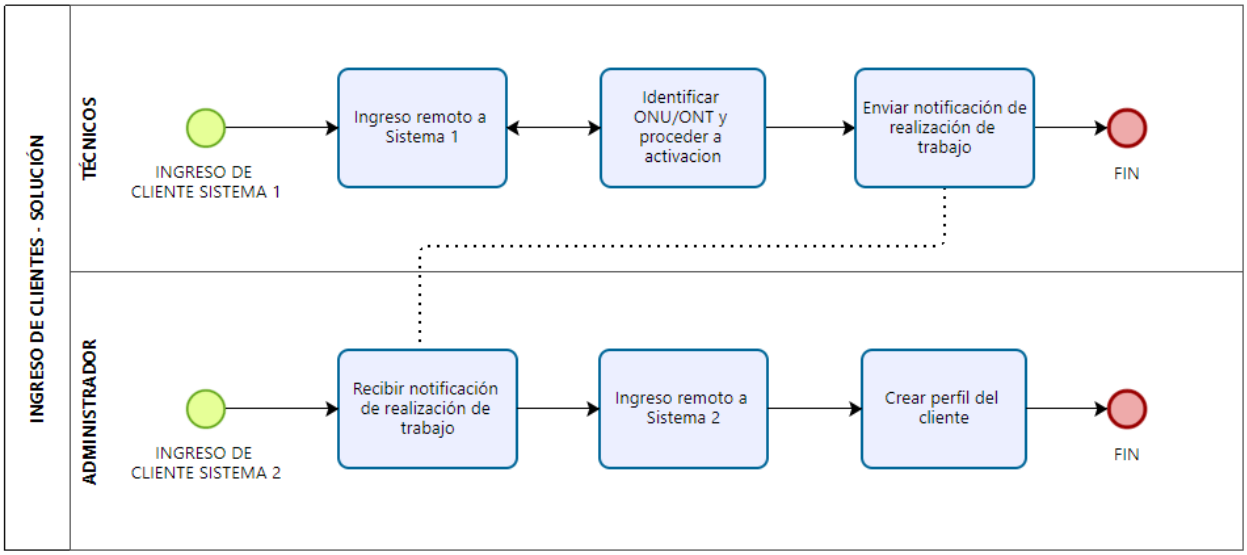
El incremento en la demora de tiempos depende de la disponibilidad y la coordinación del administrador con los técnicos para llevar a cabo las actividades. Sin embargo, una vez culminado el proceso, no se lleva un registro adecuado de la información que posee el cliente, debido a la

inexistencia de un sistema que registre las configuraciones respecto a la dirección IP y el perfil del cliente, esto provoca una pérdida de información valiosa que podría ser utilizada posteriormente al momento de ejecutar un soporte a los clientes.

La propuesta que se presenta para mejorar el rendimiento y reducir el tiempo de respuesta a esta problemática es: vincular dos sistemas que sean capaces de otorgar credenciales de nivel de usuario a los técnicos. Permitiendo llevar a cabo el ingreso de clientes desde un dispositivo que se encuentre conectado a internet. De esta manera se podría mejorar el tiempo de respuesta ya que el técnico se encargaría de ingresar a los clientes sin la necesidad de realizar comunicación con el administrador de la red, logrando así disminuir el número de acciones a un total de tres por cada activación y utilizando un tiempo aproximado de dos minutos por cada proceso, tal como se muestra en la **Figura 38**. ANEXO C2 evidencia el proceso en el SISTEMA 1

La razón por la cual se propone la implementación de dos sistemas es debido a que, el SISTEMA 1 será capaz de realizar la autorización de las ONU/ONT de manera remota, y el SISTEMA 2 permite ingresar información y enlazarla al perfil que posee el cliente, pudiendo así llevar más control sobre su estado y configuraciones establecidas, este proceso se detalla en el ANEXO C4, correspondiente al SISTEMA 2.

Figura 38 Ingreso de Clientes - Solución



Para prevenir escenarios futuros de ingresos no admitidos por parte de la hoja de trabajo de los técnicos se realiza una ficha de responsiva en la cual consta la información de los clientes ingresados de manera diaria, la cual deberá ser revisada y aprobada por el administrador en donde se deberá verificar cada uno de los ingresos realizados en el SISTEMA 1 y compararlos con la ficha del técnico, de esta manera se llevará un correcto control en el proceso.

Para lograr ejecutar este proceso se entrega guías técnicas con las cuales, mediante capacitaciones, el personal del área técnica y de administración de red serán capaces de ejecutar el procedimiento de manera rápida y eficaz. El documento de guía técnica se lo encuentra disponible en el ANEXO 2.

3.4.3. PROCESO 3

Al momento de buscar realizar una consulta del estado del cliente, en la red de CayambeVisión S.A., se encuentra un proceso mostrado con anterioridad en la **Figura 27** el cual posee muchas actividades a realizarse e intervienen dos áreas de trabajo para obtener como resultado final el estado del cliente. Esto hace que el tiempo de respuesta a consultas aumente

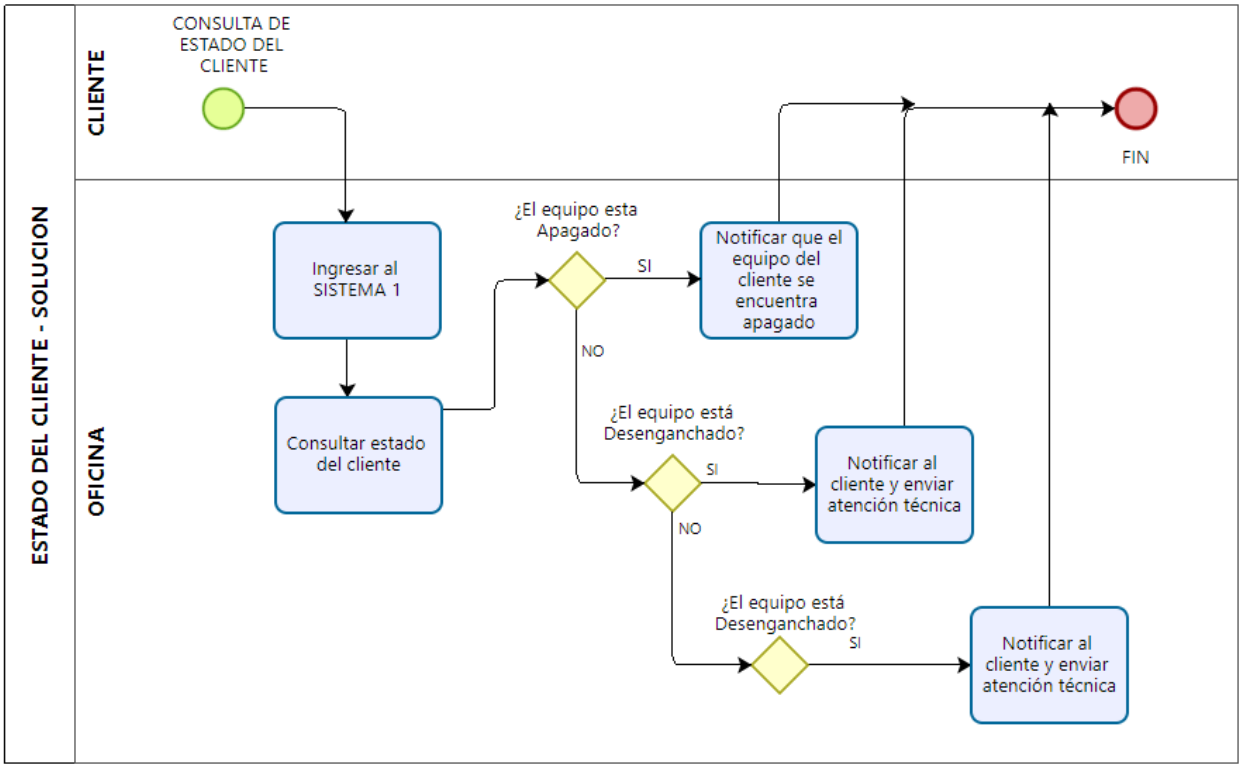
debido a que, si no existe una información actualizada de las dos áreas, pueden presentarse problemas a la hora de enviar un resultado final. El cual sirva como guía para obtener una solución rápida a problemas presentados en equipos de los clientes.

Para verificar el estado de una manera mucho más rápida y eficiente se plantea el uso del SISTEMA 1 el cual permitirá gestionar equipos y realizar consultas de estados de clientes de manera instantánea debido a que deja de existir la intervención del área administrativa, lo cual reduce el tiempo de espera por parte del cliente, establece un reporte más acertado y mejora el servicio de soporte otorgado por parte de la empresa.

Para implementar este proceso se realiza una capacitación al área de Oficina, las cuales verificaran el estado del cliente acorde a tres tipos de casos presentados en la red: Equipo Apagado, Equipo Desenganchado y Desconocimiento del estado del equipo. Para esto se entrega credenciales de acceso al SISTEMA 1 que permita la verificación del estado del cliente. El proceso propuesto se lo muestra en la **Figura 39**.

Figura 39

Estado del Cliente - Solución



El administrador de la red deberá establecer capacitaciones periódicas respecto al uso del SISTEMA 1 referente a consultas de estado de clientes por parte del área de Oficina, de igual manera, se deberá realizar una guía de manejo y definición sobre cada uno de los tipos de escenarios que pueden presentarse al realizar este tipo de proceso, logrando así facilitar el manejo apropiado del SISTEMA 1 y mejorando el rendimiento de soporte en la empresa.

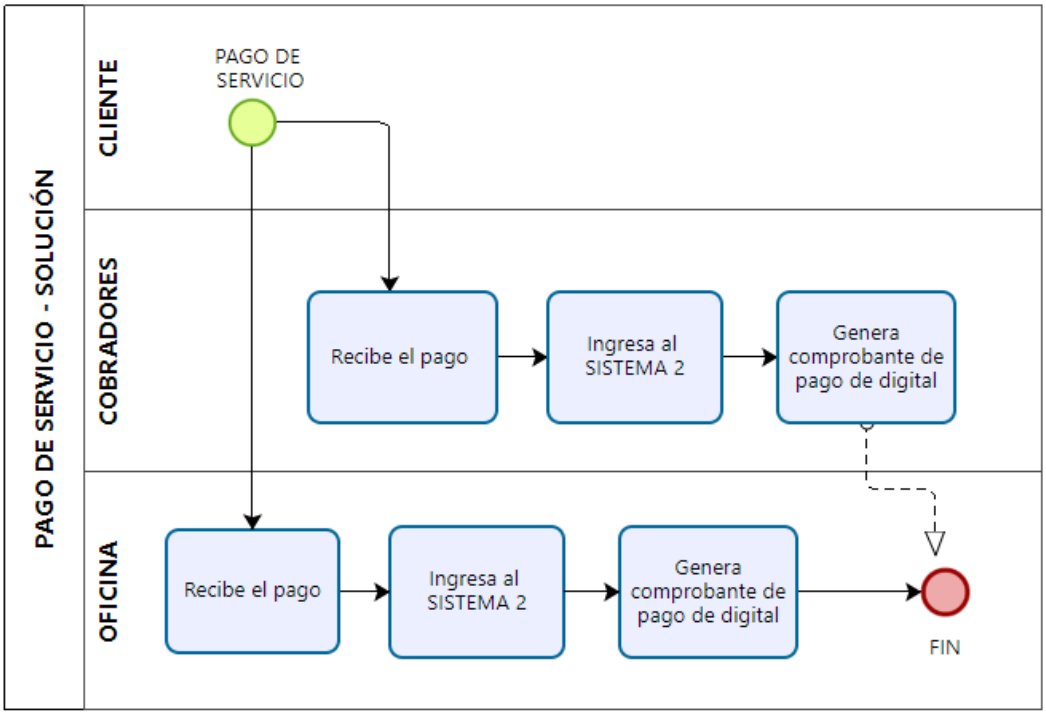
3.4.4. PROCESO 5

El pago de servicios en la empresa CayambeVisión se lo puede realizar a través de dos canales, los cuales son: oficina y cobradores. El proceso para realizar y validar pagos dentro de la empresa es deficiente, debido a que todos los pagos realizados por los clientes se registran en un archivo de texto plano. En donde, para ingresar datos en el archivo de texto se puede observar en la **Figura 33** la participación conjunta entre personal de oficina con la parte de los cobradores hasta llegar a validar correctamente un pago de una línea de cliente. El inconveniente se extiende cuando, un pago no fue validado a tiempo debido a la sobre carga de actividades de Oficina y el plazo de cancelación del servicio del cliente caduca, por lo cual, al momento de realizar cortes de servicio el cliente es identificado con mora, a pesar de haber cancelado su mensualidad a tiempo se realiza una errónea suspensión del servicio.

Para mejorar el proceso se plantea la migración del modelo de ingreso de pagos al SISTEMA 2 el cual es capaz de registrarlos de manera inmediata y generar comprobantes de pago digitales, reduciendo el tiempo en la validación de estos, quitando carga de trabajo al área de Oficina y evitando generar molestias por cortes erróneos en los clientes de la red de CayambeVision S.A. De esta manera se podrá tener un mayor control sobre el estado de cuenta de cada uno de los clientes, al igual que los montos diarios recibidos por parte de cobradores y oficina. En la **Figura 40** se puede evidenciar la reducción de procesos y tiempo al momento de registrar un nuevo pago y posteriormente validarlo.

Figura 40

Pago de Servicios - Solución



Para realizar el control de las acciones del área de oficina y cobranza se le entregará una cuenta con acceso al SISTEMA 2 a cada uno de los usuarios con un perfil destinado para el cobro y registro de pagos, esto con el fin de establecer un control diario, el cual se representa mediante la presentación del ANEXO 3 y adjuntando el resumen diario de pagos otorgado por SISTEMA 2 al finalizar el día.

3.4.5. PROCESO 6

CayambeVision S.A. no cuenta con un registro adecuado de tickets de soporte, el modelo de manejo se lo realiza mediante el ingreso directo a las hojas de trabajo diarias de los técnicos. El problema se manifiesta cuando, al área de oficina llegan nuevos reportes de daños por parte de los

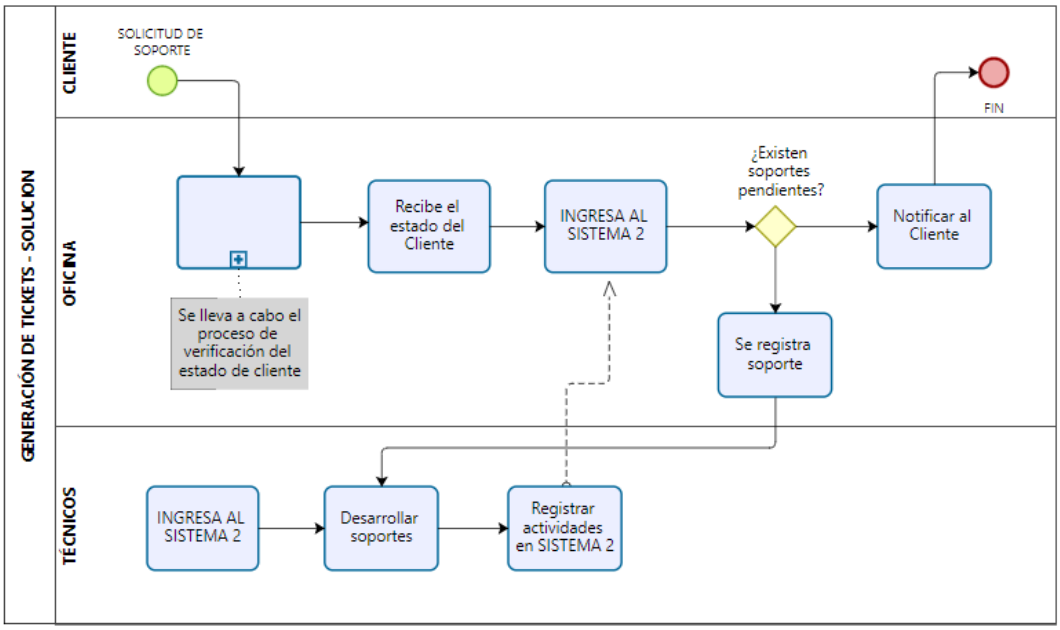
clientes, lo cual ocasiona que al momento de finalizar el día y revisar el cumplimiento de los soportes diarios de los técnicos, estos no hayan alcanzado a cumplir con toda su hoja de trabajo, lo que ocasiona la postergación de las actividades nuevas ingresadas en oficina, generando un sobre cargo de trabajo a realizarse al siguiente día y extendiendo el tiempo de solución a los nuevos reportes ingresados. Este proceso se lo visualiza en el apartado anterior en la **Figura 34**.

La solución que se plantea para mejorar el rendimiento y llevar una correcta información sobre el estado del cliente, es la implementación del SISTEMA 2, el cual se encargará de llevar un correcto orden y permitirá registrar el avance de actividades realizadas por parte de los técnicos en relación a los soportes diarios, de esta manera no solo se contará con información actualizada sobre el estado de soportes, sino que también se podrá almacenar información sobre tickets generados por parte de los clientes.

Para ello necesario otorgar credenciales en la sección de Tickets al área de Oficina la cual permitirá generar Tickets de soporte y al área Técnica ya que estas actividades se verán reflejadas en el perfil del responsable asignado a cada actividad. Con ello se propone el trabajo conjunto de manera mucho más rápida y evitando generar tiempos de espera extendidos hacia los clientes al momento de generar el ingreso de un nuevo soporte. En la **Figura 41** se puede observar a solución.

Figura 41

Generación de Tickets – Solución



Para realizar el control y el buen manejo del SISTEMA 2, se propone realizar una capacitación conjunta entre el área de oficina y técnica en el cual se realice pruebas de funcionamiento del sistema, además la realización de guías que faciliten el proceso de consultas de los procesos relacionados con la generación y registro de actividades.

3.4.6. PROCESO 7

El problema existente en el proceso de corte de servicio en la empresa CayambeVision S.A. se debe, al excesivo tiempo toma realizar los cortes la falencia de información actualizada de la lista de clientes destinados a corte de servicio por falta de pago. El proceso se da cada día 10 de cada mes, en donde, oficina realiza el proceso de *Pagos de Servicio* detallado anteriormente y una vez validado cada pago, se envía dicha información al administrador de la red, la cual es la persona encargada de realizar la suspensión del servicio al cliente de manera manual, este subproceso se

lo realiza ingresando por consola a la OLT y ejecutándolo para cada cliente, esta actividad conlleva gran tiempo de ejecución por lo cual, la empresa recompensa esta extensión de tiempo a pagos de horas extras, tanto a oficina como al administrador de la red. Este proceso se ve reflejado anteriormente en la **Figura 35**.

Ingresar el a la red de CayambeVision S.A. el SISTEMA 2, el cual se encarga de realizar cortes automáticos de internet y reactivación del servicio una vez sea ingresado el pago y generado el comprobante digital, de esta manera ya no se solicita la información del listado de clientes destinados a corte de servicio por falta de pago y no se extiende periodo de trabajo para las áreas de oficina y administrador de la red, realizando la reducción de tiempo en la ejecución del proceso, evitando cortes de servicio a clientes por error y evitando el pago de horas extras al personal de las áreas destinadas a esta actividad.

3.5. BENCHMARKING – SELECCIÓN DE HERRAMIENTAS

Para establecer la presente investigación se procede a seleccionar el benchmarking competitivo como herramienta comparativa entre aquellos servicios de administración y gestión de red que cumplan con las necesidades planteadas por la empresa CayambeVisión tales como: Creación de planes de servicio, Activación/Corte de servicios de clientes, Tickets de Soporte, Ingreso de nuevos clientes, acceso remoto, información del estado del cliente.

Para presentar las distintas herramientas se procede a identificarlas en el mercado como una opción y evaluar sus características frente a otras, observando ventajas, desventajas y así poder seleccionar aquellas que cumplan de mejor manera las necesidades previamente planteadas.

3.5.1. Métricas de benchmarking

Las herramientas mencionadas a continuación: SmartISP, SmartOLT, AdminOLT y Wisp HUB, se han agrupado en base a su uso y función que tendrían dentro de la red de CayambeVision S.A., siendo así SmartOLT y AdminOLT se definen como herramientas para el uso en la Gestión de la OLT y ONT/ONU, mientras que SmartISP y Wisphub son herramientas destinadas a la Administración de la red. Las métricas para su medición están basadas en la escala de Likert para su calificación. Esta se valora en ítems ponderados acorde a las **Tabla 6**, **Tabla 7** y **Tabla 8**.

Tabla 6

Tabla de Valoración 1

Respuesta	Valoración
Si	1
No	0

Fuente: (Cañadas & Sanchez, 2012).

Tabla 7

Tabla de Valoración 2 - Valor

Respuesta	Valoración
Muy Bueno	5
Bueno	4
Regular	3
Malo	2
Muy Malo	1

Fuente: (Cañadas & Sanchez, 2012).

Tabla 8

Tabla de Valoración 3 - Dificultad

Respuesta	**Valoración**
Muy Fácil	5
Fácil	4
Regular	3
Difícil	2
Muy Difícil	1

Fuente: (Cañadas & Sanchez, 2012).

3.5.2. Benchmarking de las herramientas de administración y gestión

El benchmarking establecido para el análisis de las herramientas de administración y gestión se centra en la evaluación de características como: Capacidad de Clientes, Tipo de Soporte, Facilidad de Implementación, Aplicaciones de herramienta, Costo. De esta manera se realiza la selección y aprobación de aquellas herramientas destinadas para la implementación posterior en la empresa CayambeVisión S.A.

3.5.2.1. Capacidad de Clientes

La capacidad de clientes que pueden ser almacenados en el Cloud de las distintas herramientas presentadas se basan en la necesidad fundamental que posee la empresa CayambeVisión S.A. para poder administrar y gestionar un número de clientes determinados de manera simultánea. Por consecuente en la **Tabla 9** se procede a valorar los distintos planes que se ofertan en las páginas presentes en de cada una de las herramientas planteadas.

Tabla 9

Tabla de capacidad de clientes activos por herramienta

N° Clientes	SmartOLT	AdminOLT	Wispro	SmartISP
1 – 100	1	1	1	1
101 – 300	1	1	1	1
301 – 1000	1	1	1	1
1001 – 3000	1	1	1	1
Mas de 3000	1	1	1	1
ValoraciónLikert	5	5	5	5

Fuente: Datos obtenidos de Internet

3.5.2.2. Tipo de Soporte

El tipo de soporte que se evalúa en este apartado está relacionado con el medio de uso para realizar el proceso de ayuda técnica hacia el solicitante del servicio de soporte, para lo cual se establece la **Tabla 10** para realizar la ponderación correspondiente.

Tabla 10

Tabla de tipo de soporte generado

Tipo Soporte	SmartOLT	AdminOLT	Wishub	SmartISP
En línea	1	1	1	1
Atención Personal	1	0	0	1
Valoración Likert sobre 5pts	5	3	3	5

Fuente: Datos obtenidos de Internet

Para establecer el proceso de ponderación sobre 5 puntos se aplica la *Ec. (1)* de la siguiente manera:

$$Valoración\ Likert/5 = \frac{N°\ items\ marcados * Puntaje\ MAX\ Likert}{items\ TOTALES} \qquad Ec.\ (1)$$

- *SmartOLT*

$$Valoración\ Likert = \frac{2 * 5}{2} = 5\ pts$$

- *AdminOLT*

$$Valoración\ Likert = \frac{1 * 5}{2} = 2{,}5\ \approx 3\ pts$$

- *Wishub*

$$Valoración\ Likert = \frac{1 * 5}{2} = 2{,}5\ \approx 3\ pts$$

- *SmartISP*

$$Valoración\ Likert = \frac{2 * 5}{2} = 5\ pts$$

3.5.2.3. Implementación

Este apartado hace referencia al proceso necesario para la vinculación del servicio con los equipos de trabajo alojados en la red de la empresa CayambeVisión S.A., esto se realiza con el fin de seleccionar la herramienta más conveniente respecto al proceso de implementación.

Por lo cual se genera la **Tabla 11** con el fin de conocer el nivel de dificultad relacionado con el proceso de adaptación de las herramientas almacenadas en el Cloud con la red.

Tabla 11

Promedio de dificultad de implementación de herramientas

Valoración 1 – 5	SmartOLT	AdminOLT	Wishub	SmartISP
	4	4	5	3

Fuente: Datos obtenidos de Internet

3.5.2.4. Expectativas de la herramienta

Las expectativas de las herramientas a implementar se han dividido en base al uso de cada una de estas, en este caso se tiene para Gestión: SmartOLT y AdminOLT, mientras que para Administración: Wisphub y SmartISP. Aquí se analizará el cumplimiento de las necesidades de la empresa en la parte de gestión y administración de la red y sus aplicaciones, de esta manera se plantean los siguientes ítems mostrados en la Tabla 12 y **Tabla 13**, los cuales hacen referencia a cada uno de estos.

Tabla 12

Aplicaciones de herramientas de Gestión

Aplicaciones	SmartOLT	AdminOLT
✓ Actualización de información de ONU	1	0
✓ Configuración OLT	1	1
✓ Activación de ONUs	1	1
✓ Creación de Perfiles de Velocidad	1	1

✓ Ingreso de nuevos clientes	1	1
✓ Acceso Remoto	1	1
✓ Información del estado del cliente	1	1
✓ Gráficas	1	1
✓ Generación de reportes	1	0
✓ Generar nuevos perfiles de ONUs	1	0
✓ Monitoreo de la red	1	1
✓ Nivel de Usuarios		
Valoración Likert sobre 5pts	5	4

Fuente: Datos obtenidos de Internet

Para establecer el proceso de ponderación sobre 5 puntos se aplica la Ec. (1) de la siguiente manera:

- *SmartOLT*

$$Valoración\ Likert = \frac{11 * 5}{11} = 5\ pts$$

- *AdminOLT*

$$Valoración\ Likert = \frac{8 * 5}{11} = 3{,}6 \approx 4\ pts$$

Tabla 13

Aplicaciones de herramientas de Administración

Aplicaciones	**Wishub**	**SmartISP**
✓ Control de Ancho de Banda	1	1
✓ Acceso Remoto	1	1
✓ Notifico General	1	0
✓ Servicio Prepago y Pospago	0	1
✓ Duplicación de ancho de banda nocturno	0	1
✓ Envió de Notificaciones	1	1
✓ Suspensión automática a clientes morosos	1	1
✓ Promesas de Pago	1	1
✓ Días de Tolerancia de corte del servicio	0	1
✓ Generación de reportes	1	1
✓ Estadísticas de Consumo	1	1
✓ Perfiles de Usuarios	1	1
✓ Monitoreo de la red	1	1
✓ Generación de Tickets	1	1
✓ Portal Cliente	1	1
Valoración Likert sobre 5pts	4	5

Fuente: Datos obtenidos de Internet

- *Wisphub*

$$Valoración\ Likert = \frac{12 * 5}{15} = 4\ pts$$

- *SmartISP*

$$Valoración\ Likert = \frac{14 * 5}{15} = 4{,}6\ \approx 5\ pts$$

3.5.2.5. Costo

Las herramientas de Gestión y Administración que se buscan implementar en la red de CayambeVision S.A. tienen una variación en el mercado referente al costo de cada una de estas, por lo tanto, es necesario analizar la inversión destinada por parte de la empresa para adquisición de dichos servicios. Para este caso se procede a utilizar la **Tabla 7** para ponderar el costo que tienen las distintas suscripciones a cada una de las herramientas a implementar, de esta manera se procede a consultar el valor de suscripción por un tiempo de tres meses y con un límite de 1500 clientes. Por lo tanto, en la Tabla 14 se expresa las cantidades en dólares de cada una de estas.

Tabla 14

Costo por suscripción trimestral

Herramienta	Costo	Valoración Likert
SmartOLT	$79.50 inc. IVA	5
Admin OLT	$84.00 inc. IVA	4
Wisphub	$235.00 inc. IVA	3
SmartISP	$141.00 inc. IVA	5

Fuente: Datos obtenidos de Internet

3.5.3. Resultados del benchmarking

En las siguientes secciones **Tabla 15** y **Tabla 16** se muestran todos los datos promedio recopilados en base a la ponderación en escala de Likert con valores de 5 puntos como máximo y 1 punto como mínimo. A estas herramientas se las ha agrupado acorde a su función, las cuales permitirán mejorar el rendimiento de tiempos de respuesta a incidentes relacionados con la Gestión y Administración de la red de CayambeVision S.A.

Tabla 15

Resultado Benchmarking para la Gestión

Ítems Evaluados	**SmartOLT**	**Admin OLT**
Capacidad de Clientes	5	5
Tipo de Soporte	5	3
Implementación	4	4
Expectativas de la herramienta	4	5
Costo	5	4
TOTAL	23	21

Tabla 16

Resultado Benchmarking para la Administración

Ítems Evaluados	Wisphub	SmartISP
Capacidad de Clientes	5	5
Tipo de Soporte	3	5
Implementación	5	3
Expectativas de la herramienta	4	5
Costo	3	5
TOTAL	20	23

3.5.4. Conclusión del benchmarking

Una vez analizados los datos resultantes del estudio de benchmarking, se procede a seleccionar aquellas herramientas que brinden una mejoría en la Gestión y Administración de la red de CayambeVision S.A., se consideran aspectos fundamentales en la empresa como: el costo de membresía y funcionalidades que ofrecen.

De esta manera resaltan SmartOLT como un sistema que permite la gestión de los equipos de red (ONT/ONUs, OLT) mientras que para la parte de Administración de red se destina a SmartISP el cual se encarga de realizar procesos automatizados en el equipo CCR-1036(Administrador). Estos sistemas de Gestión y Administración cumplen con las funcionalidades buscadas por la empresa con un costo relativamente bajo a comparación de las otras herramientas sometidas al benchmarking.

Por otro lado, se considera la dificultad de implementación que se tiene en Wisphub y SmartISP, a pesar de que Wisphub, tiene un proceso mucho más simple de implementación, SmartISP resalta en el tipo de soporte personalizado y presencial que se brinda a las empresas al momento de buscar integrar el sistema a sus equipos de red. Por lo que se ubica de mejor manera frente a Wisphub.

Por consecuente, una vez realizado el benchmarking competitivo y obtenido el puntaje final de cada uno de los ítems analizados, se puede concluir que las herramientas que mejor se adaptan al contexto de estudio en la red de CayambeVision S.A. son: SmartOLT y SmartISP.

3.6. DIAGRAMA DE CASO DE USO

El caso de uso como su nombre lo dice, hace referencia a los distintos servicios que pueden ser utilizados por parte de los usuarios finales, en el caso de la empresa CayambeVision S.A. estos usuarios son representados por el Área de Oficina (Secretarias), Área de Finanzas (Cobradores), Área Técnica (Técnicos de Soporte) y el Administrador de la red. De esta manera se puede analizar los procesos que se generarían en cada una de las herramientas seleccionadas a partir del Benchmarking realizado en el apartado anterior las cuales se busca implementar.

3.6.1. Diagrama SmartOLT

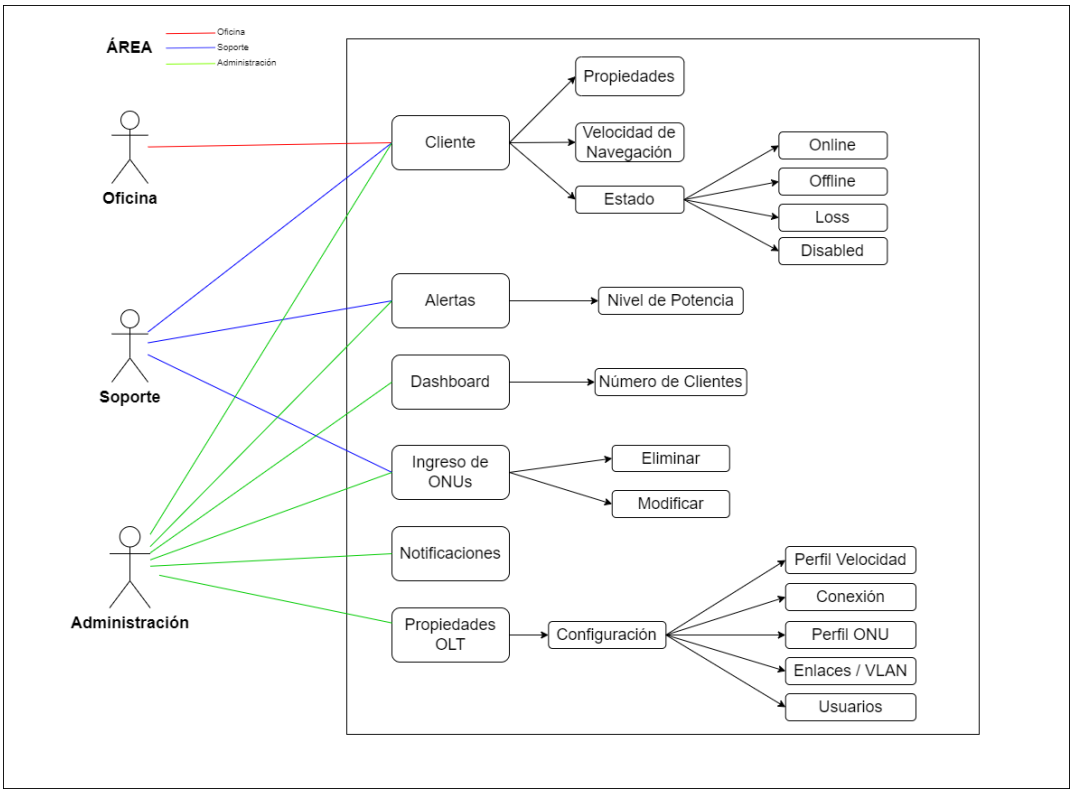
SmartOLT es una herramienta almacenada en el Cloud que permite generar un nuevo enfoque sobre la interacción con los dispositivos de red. Se considera como una herramienta de Gestión amigable de equipos tales como ONUs y OLT; de tal manera que para los usuarios finales no es necesario un conocimiento técnico avanzado para que sean capaces de utilizarlo.

Las herramientas que posee representan varias funciones las cuales interactúan con el usuario final, para el caso de la empresa CayambeVisión S.A. los usuarios destinados a utilizar

poseen cierto nivel de privilegio acorde al cargo que representa el usuario en la empresa. De esta manera se define el uso de cada uno de estos en la **Figura 42**.

Figura 42

Diagrama de Uso - SmartOLT



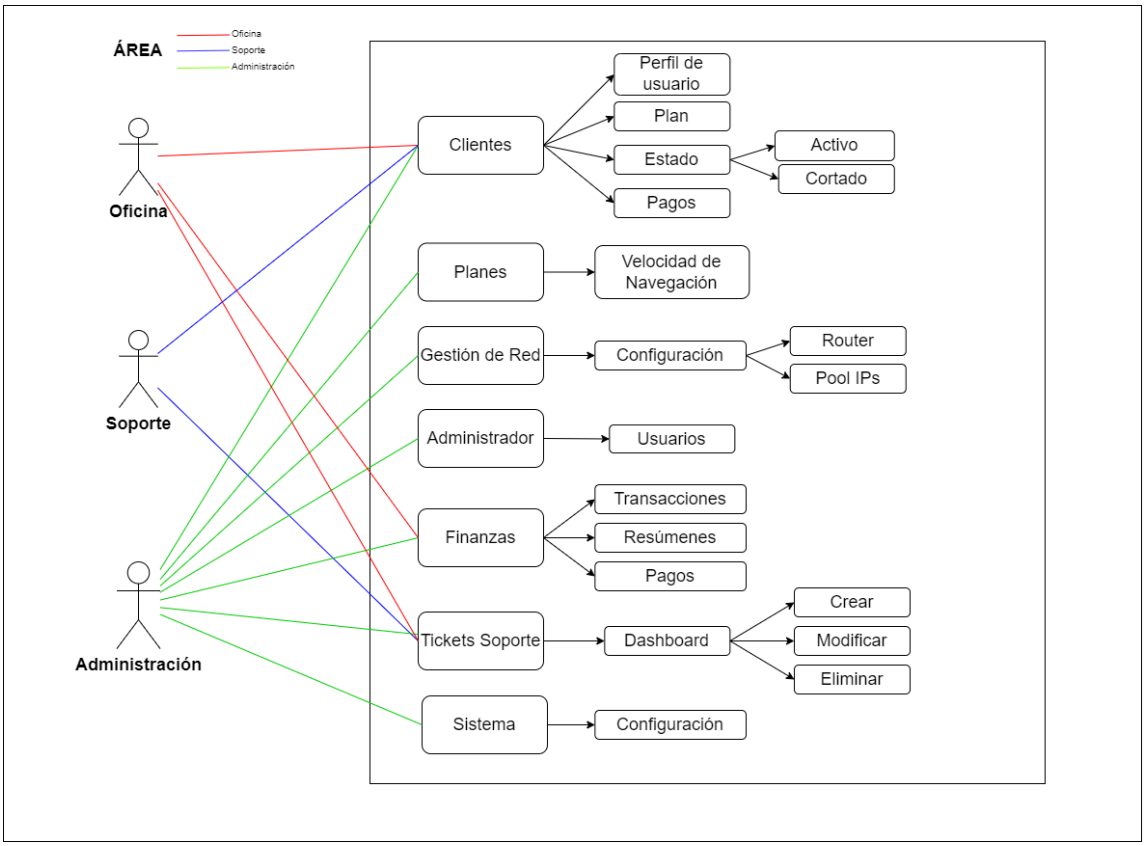
3.6.2. Diagrama SmartISP

SmartISP es un software desarrollado en el Cloud, el principal objetivo de esta herramienta es la mejora del rendimiento del ISP, esto debido a su capacidad administrativa de la red de los clientes, permitiendo realizar acciones automáticas las cuales reducen los tiempos de respuesta a los distintos escenarios que se presentan en una empresa con gran cantidad de usuarios clientes. Estos distintos escenarios dentro de una red se reflejan en acciones que pueden ser realizadas por los usuarios destinados a utilizar el sistema, es por esto que se plantean mediante la **Figura *43*** el

diagrama de uso correspondiente para cada uno de los usuarios acorde a su nivel de privilegio dentro de la empresa.

Figura 43

Diagrama de Uso – SmartISP



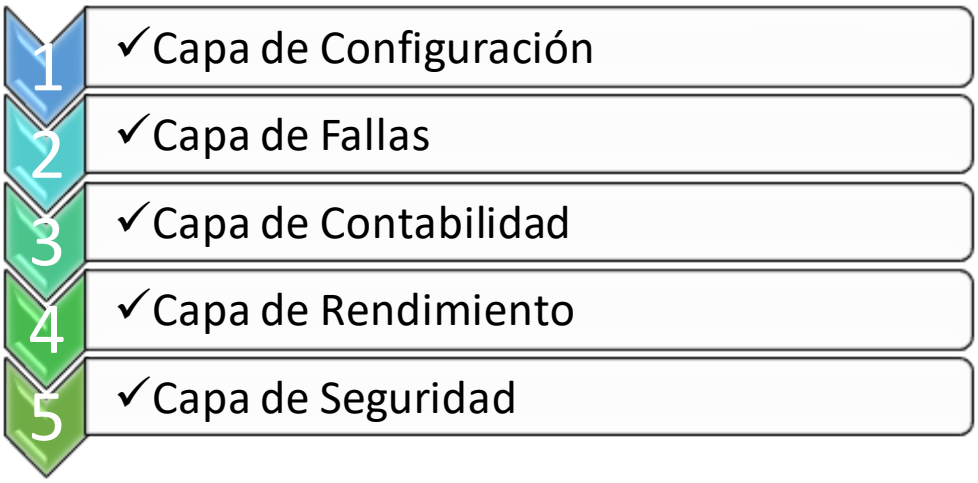
4. CAPITULO IV – GESTIÓN DE LOS SERVICIOS

La implementación de servicios de gestión de red es un proceso crítico para asegurar el correcto funcionamiento de la infraestructura de red en una organización. Uno de los marcos más utilizados en este proceso es el modelo FCAPS, el cual define cinco categorías de gestión de red: fault (fallas), configuration (configuración), accounting (contabilidad), performance (rendimiento) y security (seguridad).

La implementación de servicios basados en FCAPS es importante porque permite a las organizaciones mantener una red confiable y segura al asegurar que los dispositivos de red estén configurados correctamente, detectar y corregir fallas de manera oportuna, monitorear el rendimiento de la red y mantener la seguridad de la información y los datos que circulan en la red. Es por eso que se realiza la adaptación de FCAPS para la integración de los servicios seleccionados para mejorar el tiempo de respuesta ante incidentes en la red de CayambeVision S.A.. Se ha modificado el esquema iniciando desde la segunda capa del modelo (configuración), ya que actualmente en la red no se presenta ningún servicio integrado. De esta manera se tiene en la Figura 44:

Figura 44

Modelo FCAPS - Adaptado CayambeVision S.A.



Para mejorar el rendimiento en la gestión de los procesos de CayambeVision S.A. se propone la designación de actividades mediante la incorporación de departamentos los cuales serán los encargados de ejecutar las acciones que se presentan a lo largo de este apartado, de esta manera una vez establecidos se los procede listar y describir en la **Tabla 17** que se encuentra a continuación.

Tabla 17

Departamentos y Roles asignados en la empresa

DEPARTAMENTO	FUNCIÓN
Redes	Mantenimiento de la infraestructura de red, asegurar la seguridad de la red y garantizar el acceso a los recursos y servicios necesarios.
Monitoreo	Supervisión del rendimiento y disponibilidad de sistemas, aplicaciones y servicios, detección y resolución de problemas.
Sistemas	Gestión y mantenimiento de los sistemas de información, configuración y actualización de sistemas operativos, aplicaciones y bases de datos, asegurar la seguridad y la integridad de la información almacenada y garantizar el acceso eficiente y seguro de los usuarios.
Técnico	Proporcionar servicios técnicos especializados a los usuarios o clientes, incluyendo instalación, configuración, mantenimiento y reparación de equipos o sistemas, brindar soporte técnico para resolver problemas y dudas relacionados con el uso de los sistemas o equipos.

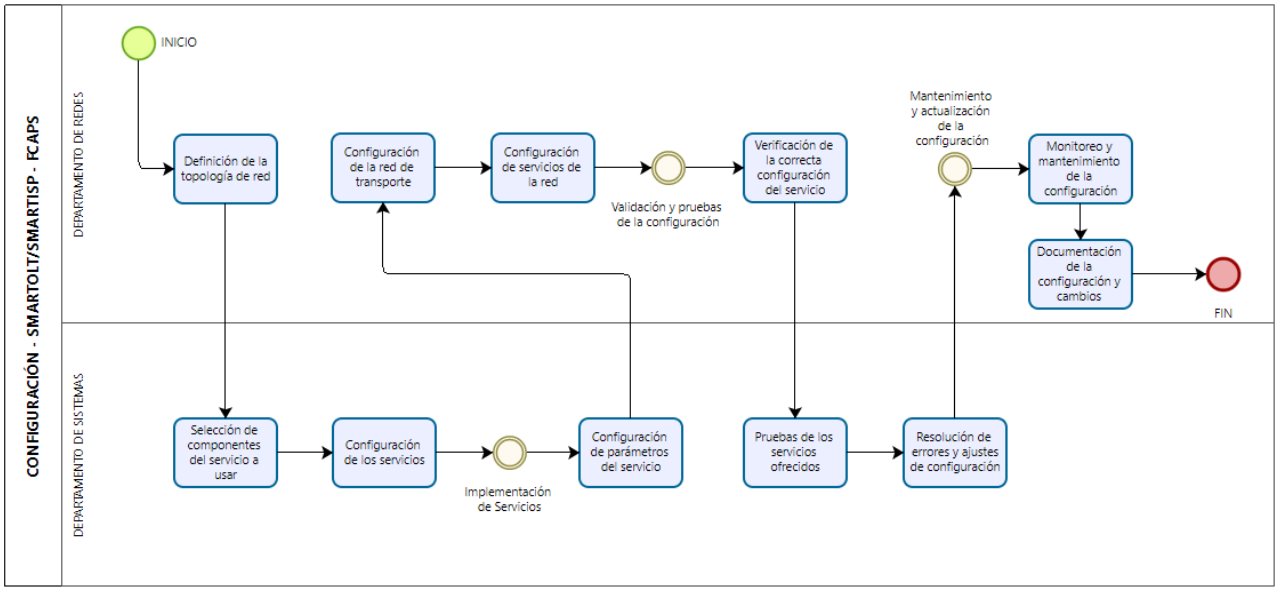
4.1. GESTIÓN DE CONFIGURACIÓN

Esta capa del modelo FCAPS se encarga de la gestión de la configuración de la red, incluyendo la definición y documentación de la configuración de los elementos de la red, así como la gestión de los cambios en la configuración. Se asegura de que todos los componentes de la red

estén configurados correctamente y de acuerdo con los estándares internacionales. El modelo en Bizagi mostrado a continuación representa un proceso lineal que permite la correcta integración de las configuraciones de SmartOLT y SmartISP en la red de CayambeVision S.A.

Figura 45

Proceso de Configuración de los Servicios



4.1.1. Definición de la topología de red

La topología de red se refiere a la forma en que los dispositivos de una red están conectados entre sí y cómo se transmiten los datos a través de esa conexión. En otras palabras, es la estructura física o lógica de una red. La elección de una topología de red depende de los requisitos y las necesidades específicas de la red, como la cantidad de dispositivos que se deben conectar, la distancia física entre ellos, el nivel de seguridad requerido y la cantidad de tráfico de red que se espera manejar. De esta manera proceder a definir la red de CayambeVision S.A. y los equipos que lo conforman.

4.1.1.1.Equipamiento

La empresa CayambeVisión S.A., posee una infraestructura de red robusta para brindar el servicio de Internet y Televisión por suscripción a sus clientes. Los equipos que conforman dicha infraestructura de red GPON se describen en la **Tabla 18**

Tabla 18

Equipos CayambeVisión S.A.

Cant	Equipo/Marca	Modelo	Estado
1	Mikrotik	CCR1036-8G-2S+	Funcional
1	Mikrotik	CCR1072-1G-8S+	Funcional
1	OLT - ZTE	ZTE – c300	Funcional

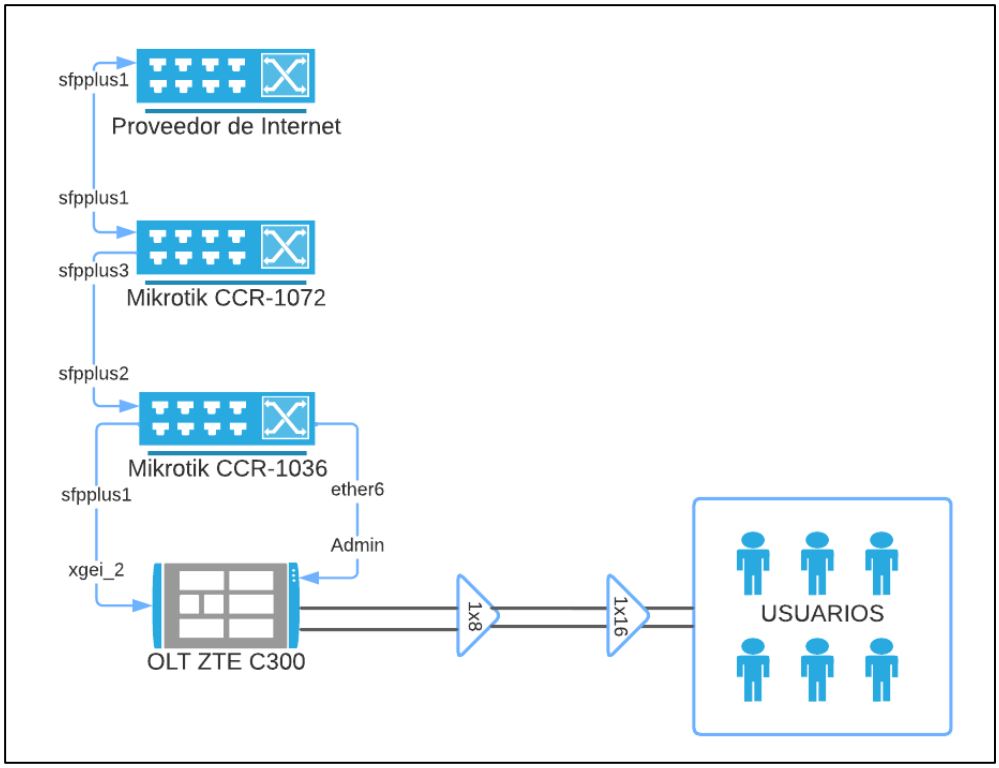
Fuente: Administrador de red CayambeVisión SA.

4.1.1.2.Conexión Física

La empresa cuenta con dos equipos Mikrotik interconectados entre sí con funcionalidades diferentes, el quipo CCR1036-8G-2S+ tiene el fin de administrar la red interna y el equipo CCR1072-1G-8S+ o llamado también router de borde que se encarga de dar salida hacia el internet a los clientes de la red. La **Figura 46** muestra la conexión entre equipos de la red CayambeVisión S.A. a través de sus interfaces físicas.

Figura 46

Conexión de equipos física

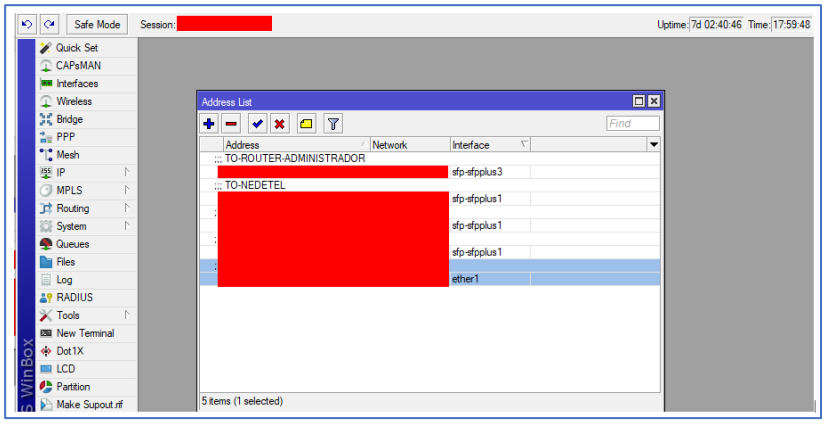


- *Mikrotik CCR1072-1G-8S+*

Este equipo también denominado router de borde es aquel que se encarga de enrutar las peticiones de conexión desde la red interna de los clientes de CayambeVisión S.A., hacia el internet. En la **Figura 47** se puede ver las interfaces que están conectadas y su respectiva función como son: spfplus3 el cual está conectado con el router Mikrotik CCR1036-12G-4S o también llamado router de Administración y sfpplus1 el cual se conecta con los proveedores que brindan salida al internet.

Figura 47

Interconexión router de borde.

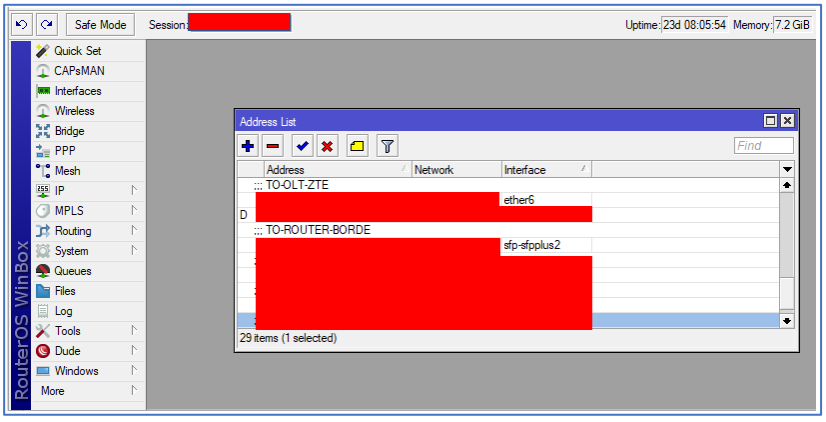


- *Mikrotik CCR1036-8G-2S+*

El equipo también denominado router de Administración cumple varias funciones dentro de la red tales como: generar redes internas para la red de clientes, interconexión con la OLT mediante un enlace troncal y enviar solicitudes de conexión hacia el router de borde. La **Figura 48** muestra la asignación de IPs a las interfaces.

Figura 48

Interconexión router de borde.



En la **Figura 49** se muestra la manera en la cual se genera la interconexión entre el equipo de administración y la red interna, esta se basa en el uso de VLANs con el fin de generar redes

privadas para los clientes, las cuales son asignadas a la interfaz sfp-sfpplus1 generando así un enlace troncalizado con la interfaz de la OLT.

Figura 49

Establecimiento de VLANs

;;; TO-OLT-ZTE				
R	sfp-sfpplus1	Ethernet	1500	1580
R	VLAN 13	VLAN	1500	1576
R	VLAN 14	VLAN	1500	1576
R	VLAN 15	VLAN	1500	1576
R	VLAN 20	VLAN	1500	1576
R	VLAN 30	VLAN	1500	1576
R	VLAN 125	VLAN	1500	1576
R	VLAN 200	VLAN	1500	1576
R	VLAN 300	VLAN	1500	1576

- *OLT ZTE c300*

El método de conexión establecido para la OLT y su administración está alojado en un puerto específico, el cual cumple esta función a través de la interconexión con el Mikrotik de Administración. El paso de las redes internas de los clientes se lo genera mediante el puerto spfplus1 y se las despliega a través del ODN gracias las funcionalidades que ofrece la OLT. Mediante el comando *show interface mng1* se puede obtener la información de la interfaz de administración de la OLT, tal como se ve en la **Figura 50**.

Figura 50

Direccionamiento OLT. Fuente: Autor.

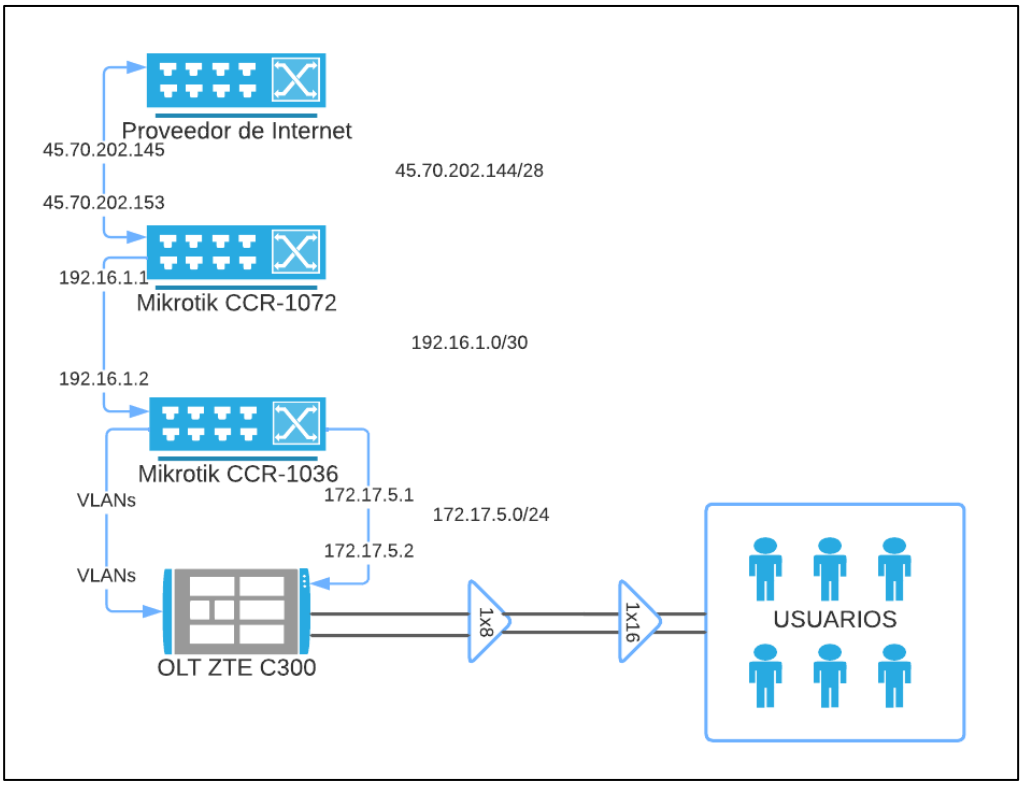
```
ZXAN#show interface mng1
mng running information
 ip address      : 172.17.5.2
 config-filename : startrun.dat
 imgfile-location: local
 inband-mac      : ccla.fad0.926b
 outband-mac     : ccla.fad0.926c
 admin-status    : no shutdown
 negotiation auto: enable
 speed           : auto
 duplex          : auto
 tag-mode        : untag

mng configuration information
 ip address      : 172.17.5.2
 config-filename : startrun.dat
 imgfile-location: local
 inband-mac      : ccla.fad0.926b
 outband-mac     : ccla.fad0.926c
 admin-status    : no shutdown
 negotiation auto: enable
 speed           : auto
 duplex          : auto
 tag-mode        : untag
```

4.1.1.3. Conexión Lógica

A continuación, se presenta el diagrama de conexión con la información sobre el direccionamiento alojado en la red de CayambeVision S.A. La **Figura 51** muestra los enlaces existentes y sus conexiones lógicas entre los equipos tanto para la conexión externa (WAN) como para la conexión interna (LAN). Esta información fue suministrada por el administrador actual de la red.

Figura 51

Conexión de equipos lógica



En la **Tabla 19** se muestran las direcciones IP asignadas a cada una de las interfaces de los equipos de la red de backbone de CayambeVision S.A. Tanto su direccionamiento interno (LAN) como externo (WAN) serán de utilidad en el desarrollo de los próximos capítulos presentados a lo largo de este trabajo de investigación, con el fin de tener una visión clara de su entorno actual.

Tabla 19

Tabla de direccionamiento lógico

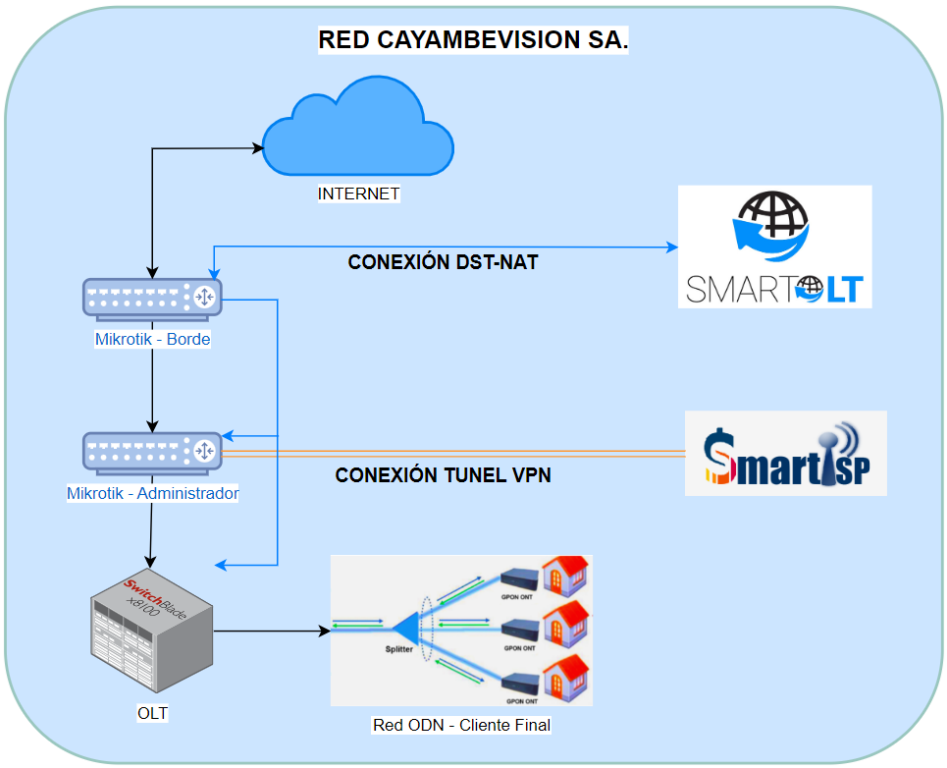
Dispositivo	**Interfaz**	**Dirección IP**	**Máscara de red**
Mikrotik CCR 1072	sfpplus 1	45.70.202.153	/28
	sfpplus 3	192.16.1.1	/30
Mikrotik CCR 1036	sfpplus 2	192.16.1.2	/30
	sfpplus 1	VLANs	--------
	ether6	172.17.5.1	/24
OLT ZTE C300	Ether	172.15.5.2	/24

4.1.2. Diseño de red

Para la aplicación de aquellos servicios seleccionados a partir del proceso de Benchmarking realizado en el capítulo anterior. La red de backbone de la empresa CayambeVision S.A. consta de equipos interconectados los cuales han sido mencionados con anterioridad en la **Figura 50** y **Figura 51**. El diseño de red que se busca plantear para la implementación de aquellos servicios destinados a la Gestión y Administración de la red se representa en la **Figura 52**.

Figura 52

Diagrama de topología propuesta



El diagrama de topología representa la propuesta de implementación para las herramientas de SmartOLT y SmartISP seleccionadas para la red de backbone de la empresa CayambeVisión S.A. para ello se procede a generar una planificación para la implementación de las herramientas, la cual representa los procesos que se llevarán a cabo en cada una de las herramientas mencionadas con anterioridad.

4.1.2.1. Planificación

Se ordena de manera secuencial los puntos considerados en el proceso de las herramientas. El tiempo de plazo máximo destinado para cumplir con el procedimiento de implementación de SmarOLT y SmartISP es de cuatro meses. A continuación, se detalla en la Tabla 20 y Tabla 21 los pasos que se implican para lograr el objetivo de este apartado.

Tabla 20

Planificación del proceso SmartOLT

Id	Nombre de tarea	Comienzo	Fin
1	**IMPLEMENTACION SMART OLT**	**lun 1/8/22**	**vie 16/9/22**
2	INICIO	lun 1/8/22	lun 1/8/22
3	Configuración de OLT	lun 1/8/22	vie 5/8/22
4	Configuración de Port Forwarding	lun 1/8/22	vie 12/8/22
5	Enlace SmartOLT-OLT	lun 15/8/22	vie 19/8/22
6	Configuración del Sistema	lun 22/8/22	vie 2/9/22
7	Ingreso de ONTs	lun 29/8/22	vie 16/9/22
8	FIN	vie 16/9/22	vie 16/9/22

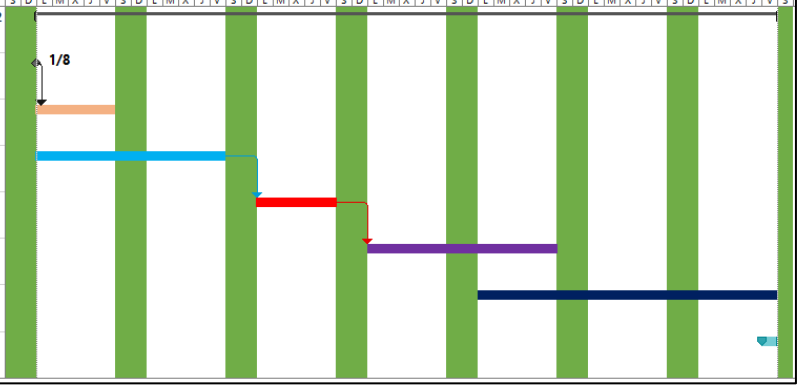
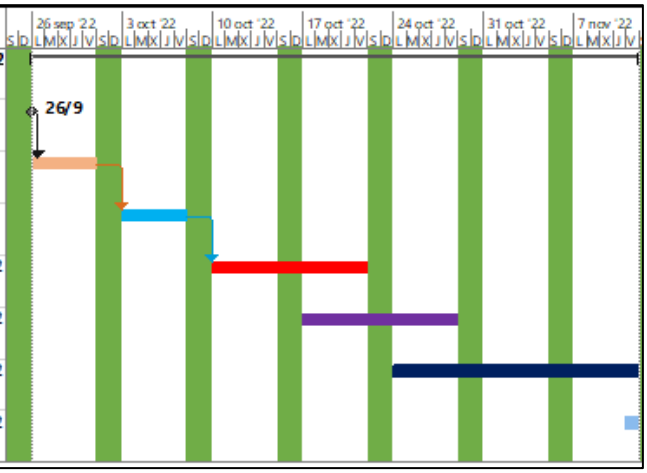


Tabla 21

Planificación del proceso SmartISP

Id	Nombre de tarea	Comienzo	Fin
1	**IMPLEMENTACION SMART ISP**	**lun 26/9/22**	**vie 11/11/22**
2	INICIO	lun 26/9/22	lun 26/9/22
3	Creación de Cloud Server	lun 26/9/22	vie 30/9/22
4	Instalación de SmartISP	lun 3/10/22	vie 7/10/22
5	Configuración de Tunel VPN	lun 10/10/22	vie 21/10/22
6	Configuración del Sistema	lun 17/10/22	vie 28/10/22
7	Ingreso de Información de Clientes	lun 24/10/22	vie 11/11/22
8	FIN	vie 11/11/22	vie 11/11/22



4.1.3. Configuración de servicios

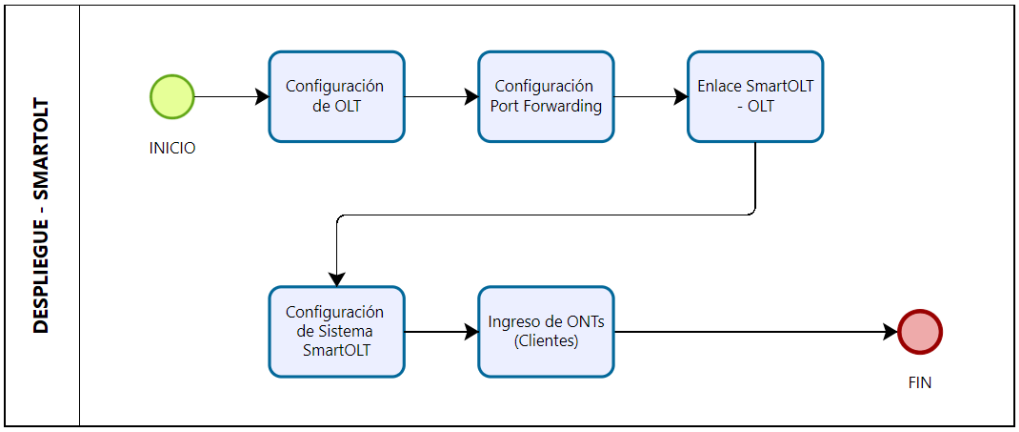
La configuración de servicios en una red se refiere al conjunto de ajustes, ajustes y parámetros que se aplican a los diferentes elementos de la red para garantizar el correcto funcionamiento y la prestación de los servicios requeridos. Es por esto que se procede a generar dos apartados destinados para la configuración de los servicios (SmartOLT y SmartISP) los cuales serán integrados en la red de CayambeVision S.A.

4.1.3.1.Implementación de SmartOLT

La implementación de SmartOLT se realiza mediante el proceso presentado en la **Figura 53** en donde, a partir de este diagrama se detallan cada uno de los pasos que hacen posible la integración de esta herramienta a la red de Backbone de CayambeVision S.A. De esta manera se presenta a continuación el desarrollo de los siguientes ítems.

Figura 53

Diagrama de Despliegue – SmartOLT

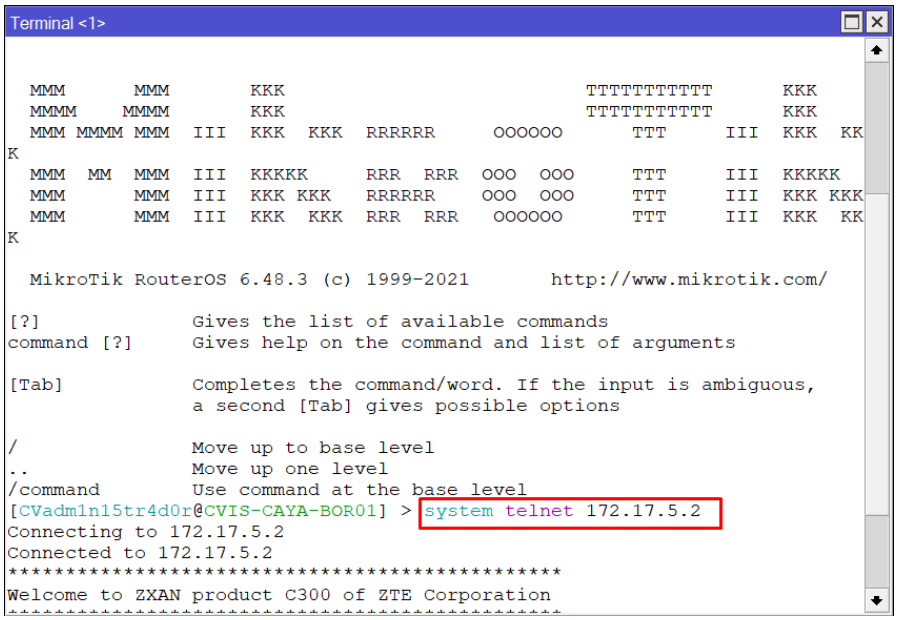


Configuración de OLT

La configuración de la OLT se la realiza a través del equipo CCR-1036(Administrador) el cual se encuentra interconectado mediante la interfaz de administración de la OLT hacia la interfaz sfpplus1 del equipo Administrador. De esta manera se procede a ingresar el comando `system telnet 172.17.5.2` en la consola de Winbox como se muestra en la **Figura 54** el cual permite el ingreso hacia la OLT.

Figura 54

Ingreso vía consola Winbox a OLT



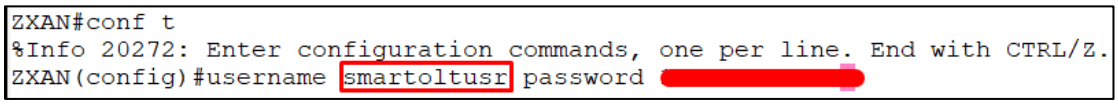
Una vez establecida la conexión remota a la OLT, es imprescindible que la OLT tenga salida hacia Internet, ya que necesita tener comunicación con la herramienta SmartOLT, la cual esta alojada en el Cloud, para ello se establece el enrutamiento de la red mediante el siguiente comando: `ip route 0.0.0.0 0.0.0.0 172.17.5.1`

A continuación, tal como se muestra en la **Figura 55**, se crea el usuario smartoltusr con su respectiva contraseña (`username smartoltusr password [ingresar contraseña]`), al cual se le asigna el perfil de administrador dentro de la OLT (`max-sessions 16 privilege 15`). Los parámetros que se asignan a este nuevo perfil son: el número de sesiones permitidas con el usuario, en este caso viene por defecto con un valor de 16. Con este usuario smartoltusr; y como segundo parámetro, nivel de privilegio de 15, lo cual permite la lectura, escritura, modificación y eliminación de datos dentro de la OLT. , la herramienta SmartOLT, enviará remotamente

sentencias de comandos para la gestión de las ONT_clientes de la red GPON de CayambeVision S.A.

Figura 55

Creación de usuario SmartOLT



Con el fin de guardar todas las configuraciones que se han llevado a cabo hasta las 18:00 de cada día, el siguiente paso es configurar la sobreescritura del archivo de arranque del equipo, para lo cual se ingresa el comando `auto-write 18:00:00 everyday` con ello, en el caso de apagarse la OLT y después encenderla, todas las configuraciones anteriores no se perderán.

Finalmente, un factor primordial para el trabajo conjunto entre SmartOLT y la OLT, es el sincronismo, por lo cual es necesario activar el protocolo NTP (Network Time Protocol) y enlazarlo a través de las direcciones IP (`91.189.89.199 y 80.96.196.58`) las cuales corresponden al servidor primario y secundario que administra el Sistema Operativo Linux en la distribución de Ubuntu (medio en el cual se aloja SmartOLT). Estas prioridades de los servidores se las asigna como se muestra a continuación:

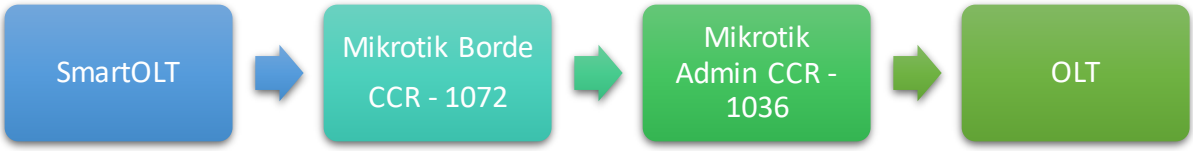
```
ntp server 91.189.89.199 priority 1
ntp server 80.96.196.58 priority 2
ntp enable
```

Configuración Port Forwarding

Con el propósito de establecer la comunicación entre SmartOLT alojado en el Cloud y la OLT alojada en la red interna de CayambeVision S.A., se opta como solución la configuración de un Port Forwarding el cual permite el redireccionamiento de puertos hacia un host específico que se encuentre dentro de la red. De esta manera se representa en la **Figura 56** el proceso que se realiza para la conexión entre SmartOLT y la OLT.

Figura 56

Configuración Port Forwarding



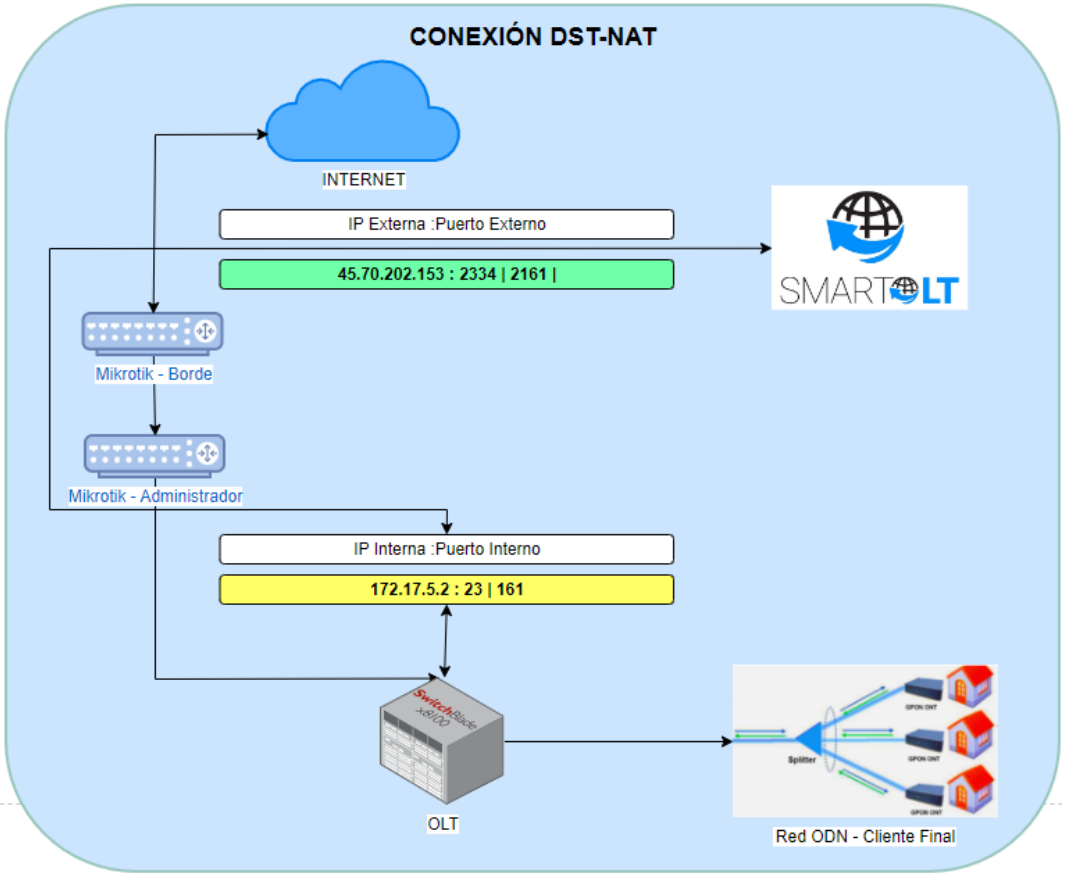
Los parámetros que destina el administrador de la red para realizar el port forwarding son:

- IP Externa: 45.70.202.153 (IP alojada en la interfaz WAN del Equipo CCR-1072)
- Puertos Externos: 2334 y 2161 (Puertos externos del Equipo CCR-1072)
- IP Interna: 172.17.5.2 (IP alojada en la interfaz de administración de la OLT)
- Puertos Internos: 23 y 161 (Puertos internos de la OLT)

En Mikrotik, la regla que permite generar una conexión vía port forwarding desde un host externo a un host interno es el DST-NAT (Destination Network Address Translation). Esta es una cadena de conexión que permite realizar el direccionamiento de puertos externos a puerto internos, tal como es el caso para la conexión entre SmartOLT y la OLT. En donde, se usa el puerto 2334 para una conexión TCP hacia el puerto 23, con el fin de enviar sentencias de comandos de manera remota vía Telnet hacia la OLT y el puerto 2161 para una conexión UDP hacia el puerto 161 usado para consultas de estado del cliente mediante SNMP. De esta manera se representa el modelo de conexión DST-NAT en la Figura 57.

Figura 57

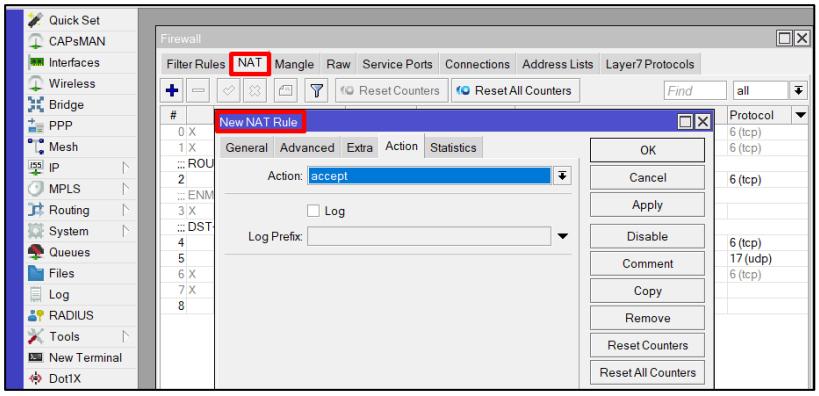
Port Forwarding – DST-NAT



La configuración de la regla DST-NAT se la realiza en el equipo CCR-1072 via Winbox, para lo cual se procede a ingresar al menú IP→Firewall→NAT, como se muestra en la **Figura 58**. Aquí se crea un nuevo tipo de regla NAT en donde se configuran los parámetros destinados a los dos tipos de conexión TCP y UDP los cuales son necesarios para la comunicación de SmartOLT con la OLT.

Figura 58

Creación de Regla DST-NAT

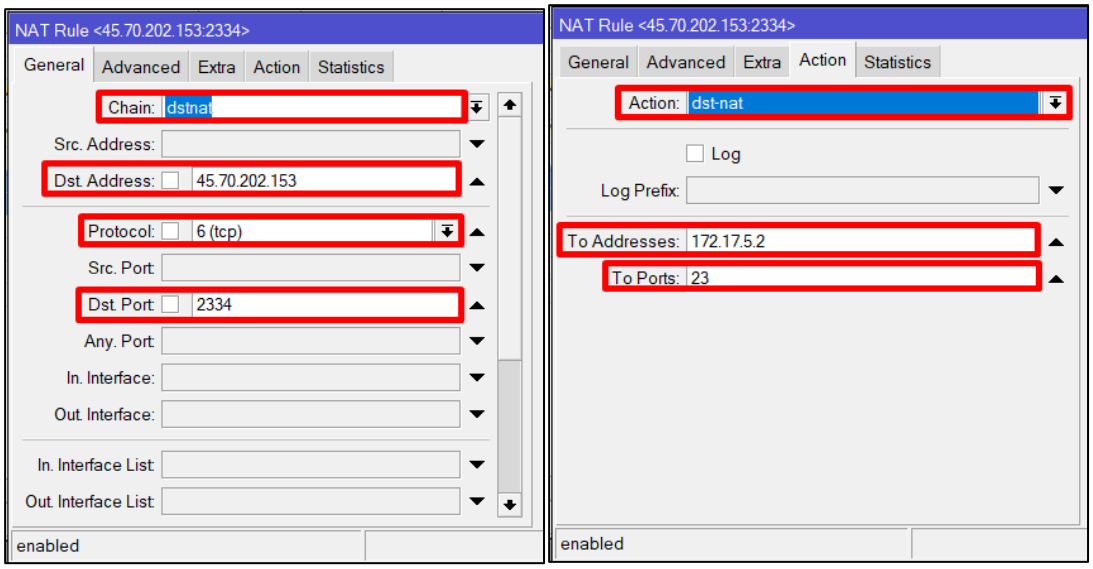


Inicialmente, se crea la regla para la conexión TCP. Este proceso se muestra en la **Figura 59**, en donde se configuran varios parámetros mostrados a continuación, los cuales permiten realizar el redireccionamiento del tráfico a través de la IP externa (*45.70.202.153)* y puerto externo (2334) hacia el host interno (*OLT*) mediante la IP (*172.17.5.2)* y el puerto (23), correspondiente para establecer una comunicación Telnet.

- **Chain:** *dstnat (Cadena de Conexión destinada para port forwarding)*
- **Dst Address:** *45.70.202.153 (IP Externa de Conexión)*
- **Protocol:** *TCP (Protocolo de conexión)*
- **Dst Port:** *2334 (Puerto Externo de Conexión)*
- **Action:** *dst-nat (Acción de redirección de puertos)*
- **To Addresses:** *172.17.5.2 (Dirección IP Interna destinada a la redirección de puertos)*
- **To Ports:** *23 (Puerto destinado a la redirección del tráfico)*

Figura 59

Configuración Regla TCP - DST NAT

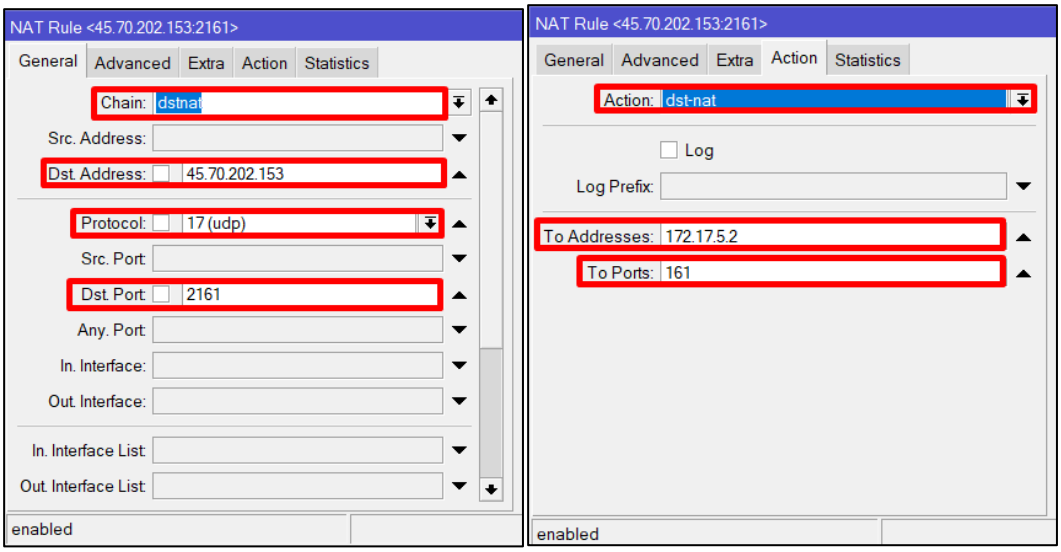


Posterior a esto, en la **Figura 60** se observa la creación de la segunda regla la cual tiene como objetivo permitir una conexión remota UDP a través del puerto externo (*2161*) destinado para la conexión SNMP hacia el puerto interno (*161*) de la OLT, para lo cual se establecen los siguientes parámetros:

- **Chain:** *dstnat (Cadena de Conexión destinada para port forwarding)*
- **Dst Address:** *45.70.202.153 (IP Externa de Conexión)*
- **Protocol:** *UDP (Protocolo de conexión)*
- **Dst Port:** *2161 (Puerto Externo de Conexión)*
- **Action:** *dst-nat (Acción de redirección de puertos)*
- **To Addresses:** *172.17.5.2 (Dirección IP Interna destino de redirección de puertos)*
- **To Ports:** *161 (Puerto destino de redirección del tráfico)*

Figura 60

Configuración Regla UDP – DST NAT

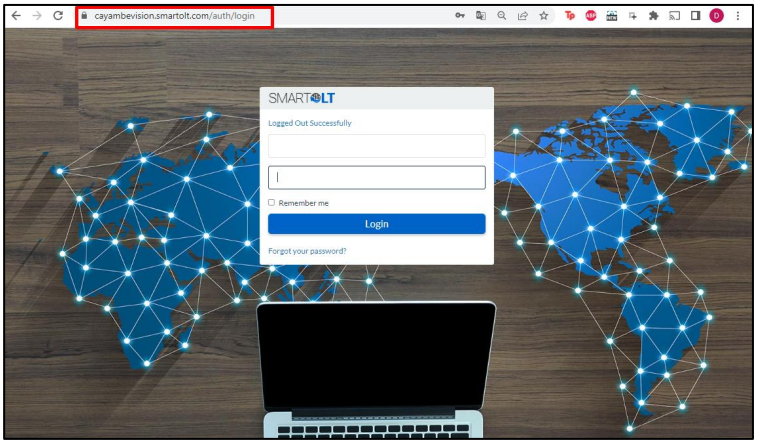


Enlace SmartOLT-OLT

Para realizar el enlace de conexión entre SmartOLT y la OLT se procede a ingresar al sitio web de SmartOLT mostrado en la **Figura 61**. La URL para el ingreso al sistema al igual que las credenciales son otorgadas por parte los propietarios del sistema al momento de realizar la suscripción a la licencia, de esta manera se obtiene el siguiente enlace https://cayambevision.smartolt.com/

Figura 61

Sitio Web – SmartOLT

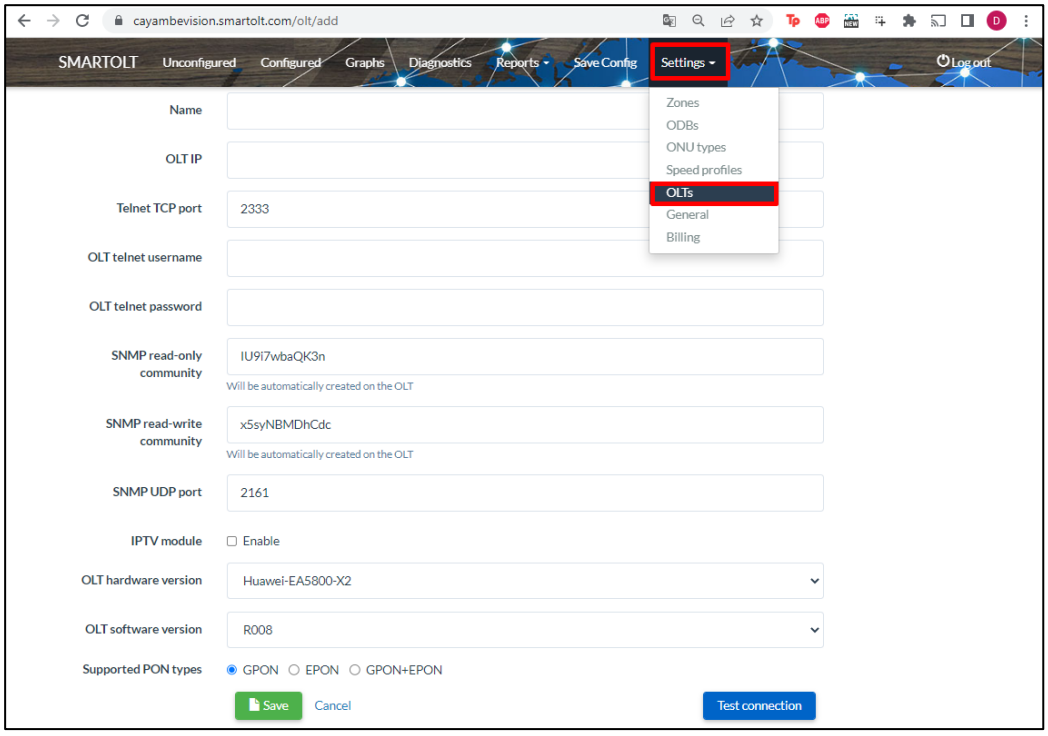


Una vez ingresado al sistema el siguiente paso es realizar la conexión hacia la OLT, para lo cual se dirige al menú *Settings→OLT→Create New*. Esta acción permite crear un nuevo perfil para la OLT tal como se muestra en la **Figura 62**. Todos los parámetros solicitados deben ser llenados y posteriormente validados con el objetivo de interconectar el Sistema SmartOLT con la OLT. A continuación, se describe cada uno de los campos que conforman la creación de un nuevo perfil para OLT:

- **Name:** *OLT-ZTE300 (Nombre Descriptivo)*
- **OLT IP**: *45.70.202.153 (IP Pública – Acceso Externo)*
- **Telnet TCP port**: *2334 (Puerto Externo - TCP)*
- **OLT telnet username**: *smartoltusr (Usuario SmartOLT)*
- **OLT telnet password:** *xxxxxxxxx (Contraseña Usuario - SmartOLT)*
- **SNMP read-only community:** *xxxxxxxxxxx (Comunidad de lectura SNMP)*
- **SNMP read write community**: *xxxxxxxxxxx (Comunidad de escritura SNMP)*
- **SNMP UDP port**: *2161 (Puerto Externo - UDP)*
- **IPTV module**: *no (Servicio de IPTV)*
- **OLT hardware *versión:*** *2.x (Versión de OLT)*
- **Type PON:** *GPON (Tipo de Red)*

Figura 62

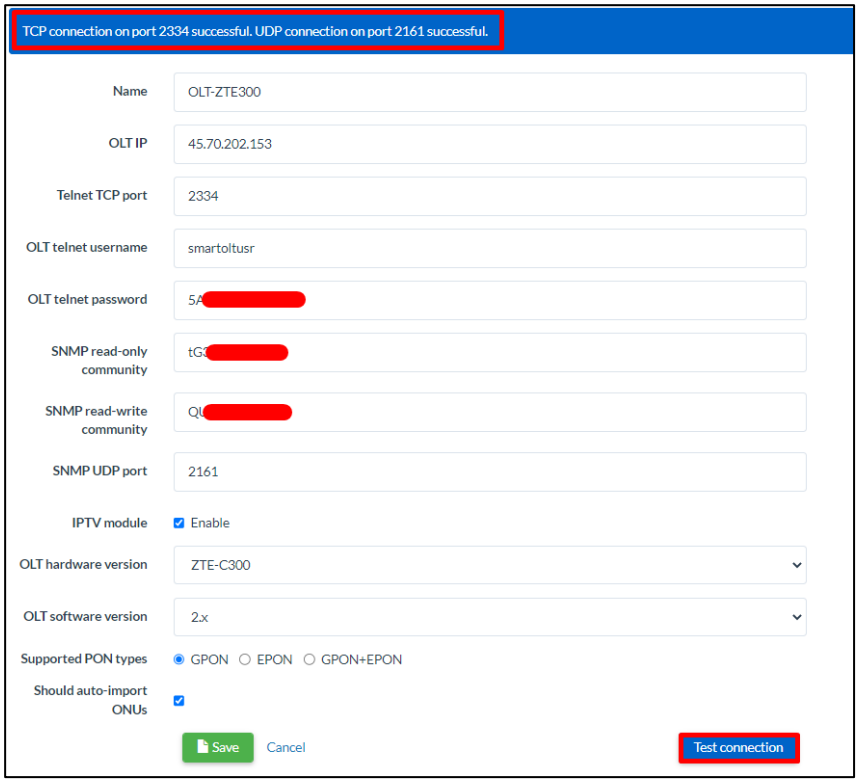
Parámetros de Conexión SmartOLT – OLT



Finalmente, llenados los campos se presiona el boton “Test Conection” y se verifica el mensaje mostrado en la **Figura 63** que menciona “*TCP connection on port 2334 successful. UDP conection on port 2161 successful”*. El cual confirma que se ha realizado correctamente la conexión entre SmartOLT y la OLT.

Figura 63

Mensaje de Conexión SmartOLT-OLT



Configuración de Sistema SmartOLT

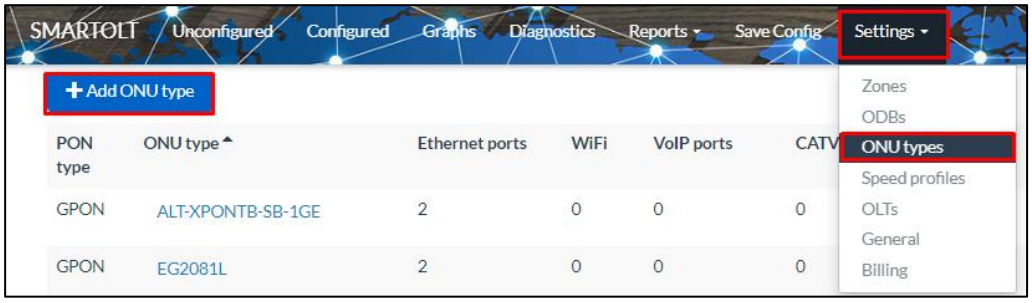
✓ *Configuración de Perfil ONTs/ONUs*

El perfil de las ONT/ONUs hace referencia a los equipos colocados en la última milla hacia el cliente. Estos equipos poseen distintas características específicas, tales como: modelo de ONU, número de puertos físicos, número de SSID (Nombre de red WLAN) y la capacidad de trabajo respecto a su funcionamiento como un puente de conexión o enrutador.

Para realizar la configuración de un nuevo perfil de ONU en SmartOLT se debe dirigir a *Settings → ONU Types → Add ONU Type,* como se muestra en la **Figura 64**. En donde se listan todos los tipos de ONUs creados por defecto por parte del sistema.

Figura 64

Configuración Perfil ONT/ONU

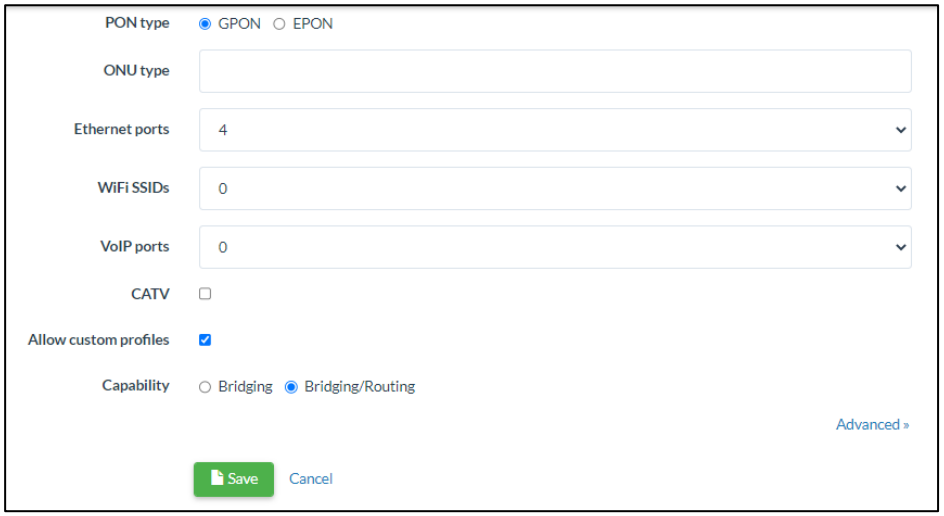


Los parámetros que se muestran para la creación del nuevo perfil de ONU/ONT son aquellos presentados en la **Figura 65**, los cuales solicitan la siguiente información:

- **PON type:** GPON (Tipo de Tecnología FTTH de trabajo)
- **ONU type:** EG2081L (Modelo de ONT)
- **Ethernet ports:** 4 (Numero de puertos físicos ethernet)
- **Wifi SSIDs:** 0 (Numero de nombres para red WLAN)
- **VoIP ports:** 0 (Numero de puertos para telefonía)
- **CATV:** no (Puerto de conexión coaxial)
- **Capability:** Bridging (Capacidad para trabajar modo puente/enrutamiento)

Figura 65

Parámetros de Perfil ONT/ONU

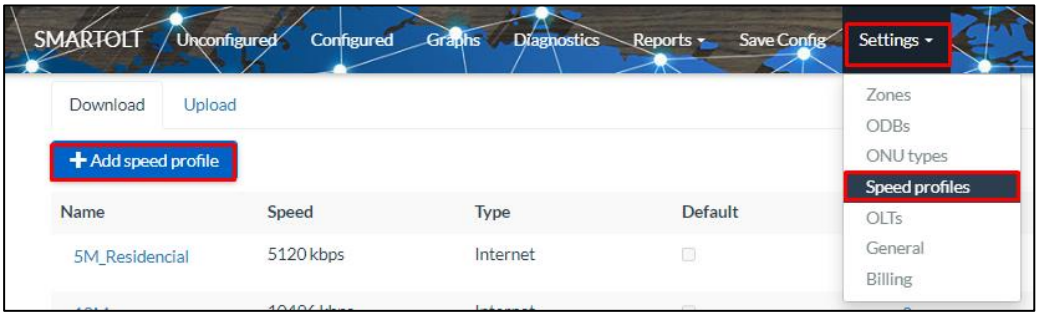


✓ *Configuración de Perfil de Velocidad*

La configuración de los perfiles de velocidad se realiza con el fin de establecer un control del ancho de banda en la navegación de subida (upload) y de bajada (download) de la ONU/ONT cliente, es por ello por lo que se ingresa al menú *Settings* → *Speed profiles* → *Add speed profile* como se muestra en la siguiente **Figura 66**.

Figura 66

Configuración de Perfil de Velocidad



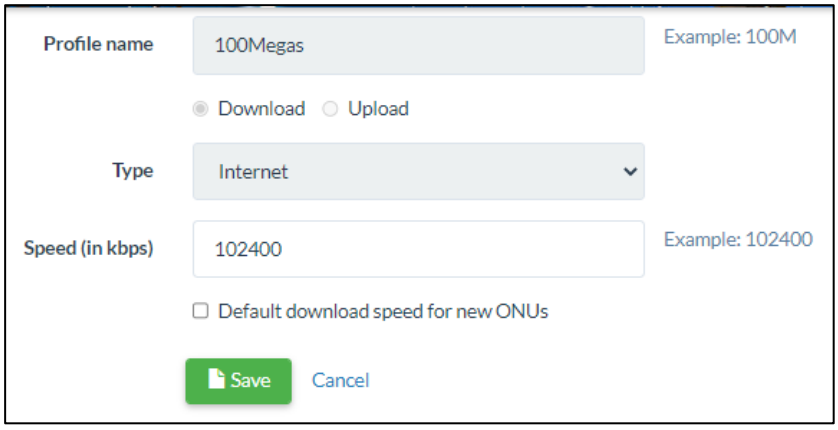
Para la configuración de los perfiles de Velocidad se procede a calcular la velocidad destinada en valor de kbps para lo cual se utiliza la *Ec. (2).* En donde, se procede a crear un nuevo perfil de velocidad como ejemplo con un valor de 100Mbps tanto para upload como download.

$$Velocidad\ en\ kbps = Velocidad\ en\ Mbps * 1024 \qquad Ec.\ (2)$$

En la **Figura 67** se muestran los parámetros para la creación del perfil de Download. Estos son: nombre de perfil, tipo de conexión, velocidad en kbps y finalmente el botón de guardar con el cual se cierra el proceso de creación. Mediante la Ecuación 2 se procede a calcular el valor en unidades de Kbps.

Figura 67

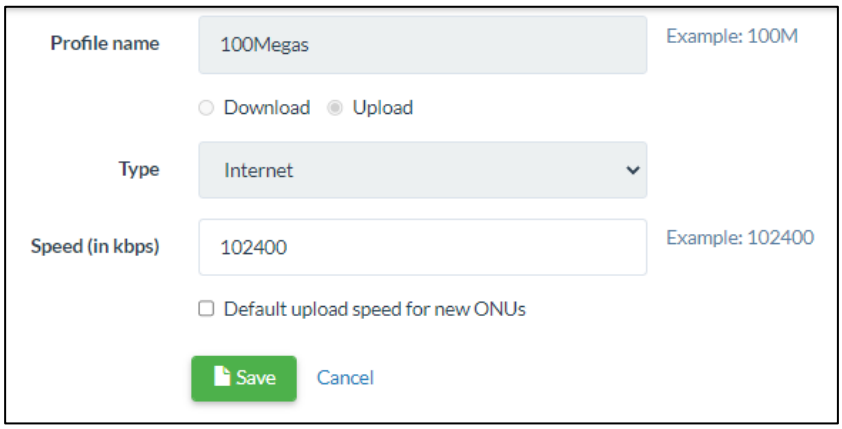
Perfil de Velocidad Download



De igual manera para el perfil de Upload se realiza el mismo cálculo de la Ecuación 2 y se coloca el valor de 102400 kbps obtenidos al momento de buscar una velocidad de 100Mpbs en el cliente, tal como se muestra la **Figura 68**.

Figura 68

Perfil de Velocidad Upload



✓ Configuración de Nivel de Privilegio de Usuarios

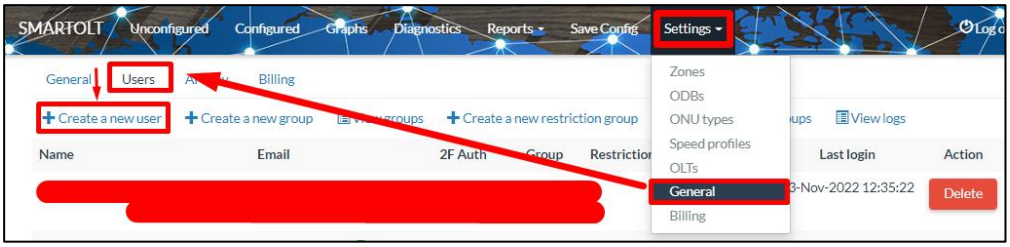
El nivel de privilegio de cada uno de los usuarios destinados para el uso de SmartOLT se los configura con el fin de establecer límites, los cuales se establecen acorde a cada una de las

funciones que cumple el usuario dentro de la empresa CayambeVision S.A. Estos niveles se basan en el Diagrama de Uso presentado anteriormente en la **Figura 42**.

Por consiguiente, para la creación de un nuevo perfil de usuario se procede a ingresar al menú *Settings→General →Users→Create new user.* La **Figura 69** representa los pasos a seguir para realizar este proceso.

Figura 69

Configuración Perfil de Usuario



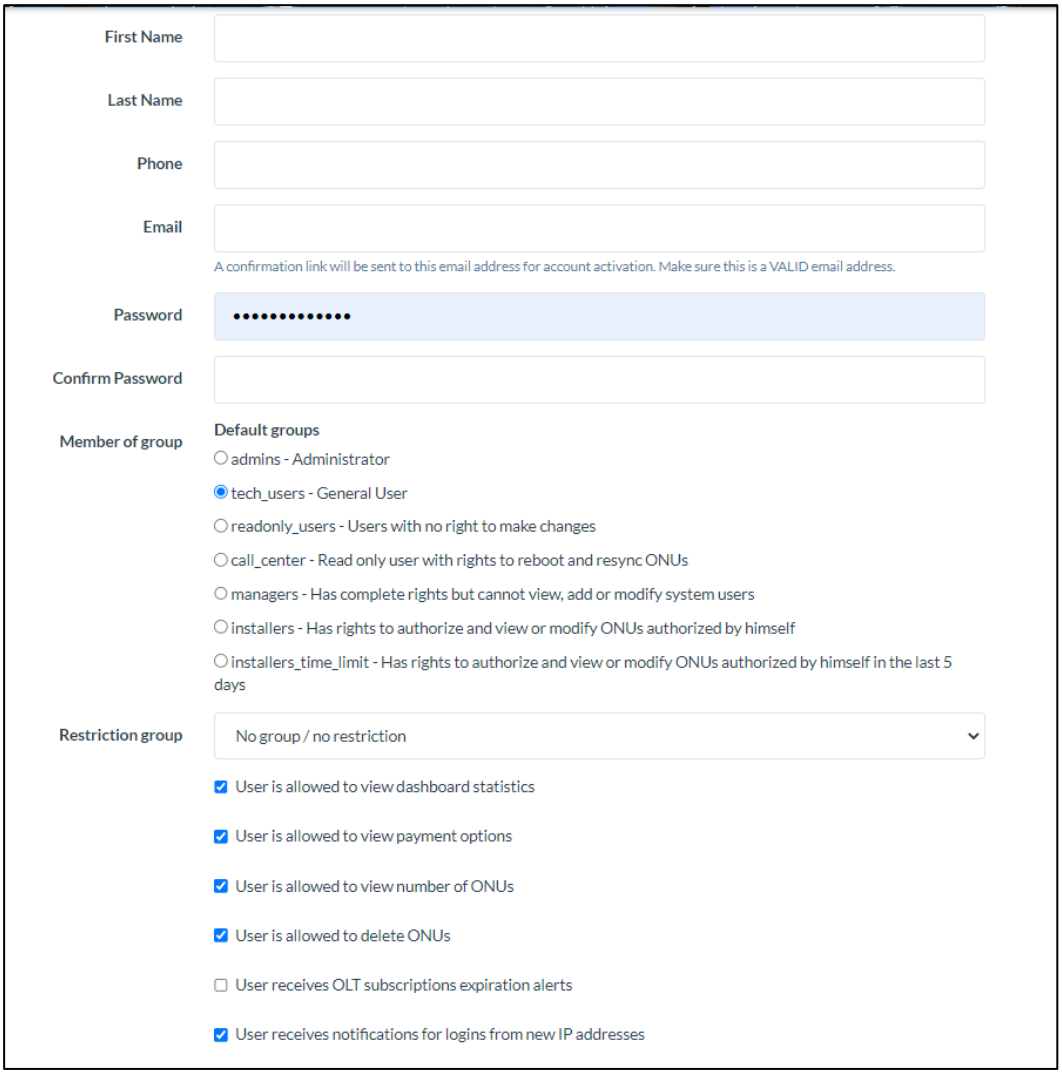
SmartOLT por defecto genera distintos grupos de usuarios, tales como: admin, tech_users, read_only_users, call_center, managers, installers, installers_time-limit. Estos tipos perfiles de usuarios se los asocia a los niveles de usuarios de CayambeVision S.A. de la siguiente manera:

- admin → Administración. (Manejo absoluto del Sistema)
- call_center → Oficina. (Permite la lectura y permite el reinicio de equipos)
- installers → Soporte. (Permite el ingreso y modificación de equipos)

A continuación, en la **Figura 70** se muestra el formulario que permite crear un nuevo usuario. Los datos que se solicitan para esto son: nombre completo, teléfono, email, contraseña, tipo de grupo y en el caso de existir algún tipo de restricción se la marca en el listado mostrado.

Figura 70

Formulario de Usuario SmartOLT



Ingreso de ONTs – Clientes

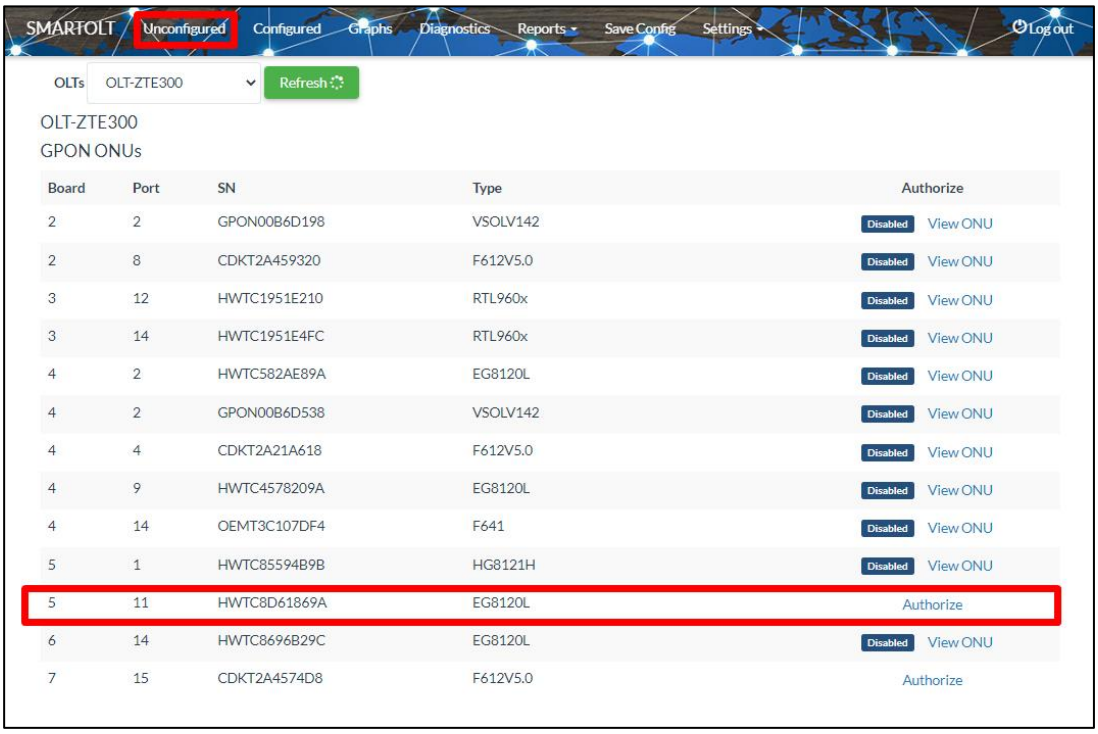
Para el ingreso de ONTs el usuario administrador debe cumplir con todo el proceso de integración mostrado en los ítems anteriores. Siendo así, se procede a ingresar un nuevo cliente y registrarlo en SmartOLT dirigiéndose al menú de Unconfigured mostrado en la **Figura 71**, aquí se listan todos aquellos equipos que no han sido autorizados o se encuentren en estado "deshabilitado".

El siguiente paso consiste en identificar al equipo que se busca ingresar mediante el tipo de ONT/ONU, SN (Serial Number) y el estado de Autorización. Una vez que se haya localizado el

nuevo equipo, como se muestra en la **Figura 71** se procede a presionar en "Autorizar", de esta manera se ingresa a los parámetros de configuración de la ONT.

Figura 71

Ingreso de ONT Cliente SmartOLT



Finalmente, se procede a autorizar la ONT llenando los datos del perfil del cliente con la información solicitada en la

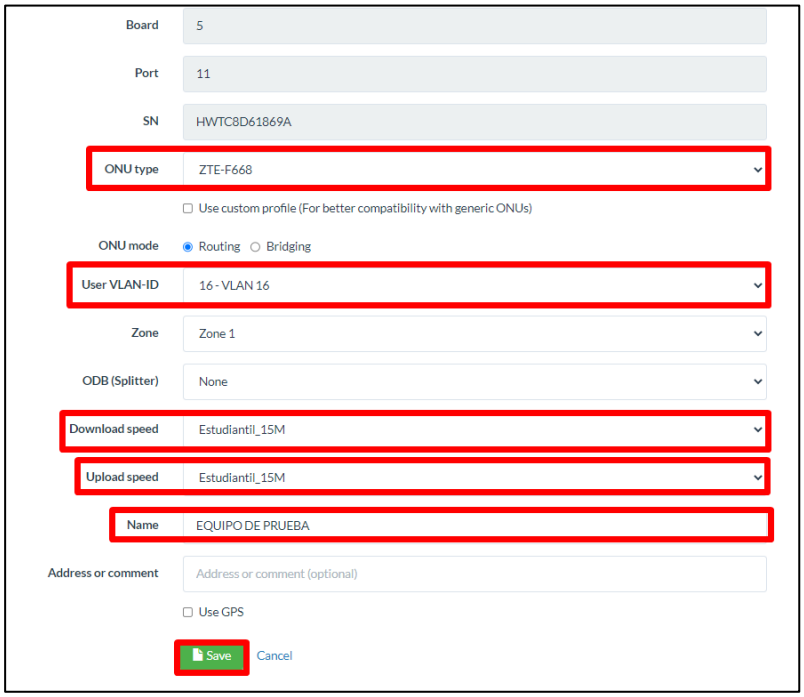
Figura 72, de la siguiente manera:

- **Board:** 5 (Número de tarjeta destinado para el cliente)
- **Port:** 11 (Numero de Puerto destinado para el cliente)
- **SN:** HWTC8061869A (Número Serial del equipo)
- **ONU type:** ZTE-F668 (Perfil de modelo ONT)
- **ONU mode:** Routing (Modo de trabajo del equipo routing/bridging)
- **Use VLAN ID:** 16-VLAN16 (Vlan asignada para el quipo)
- **Zone:** Zona 1 (Zona referencial a la ubicación del equipo)
- **ODB Splitter:** None (Caja de Distribución de Fibra Óptica)

- **Download Speed:** Estudiantil_15M (Perfil destinado al tráfico de descarga)
- **Upload Speed:** Estudiantil_15M (Perfil destinado al tráfico de subida)
- **Name:** EQUIPO DE PRUEBA (Nombre del usuario cliente)
- **Address or comment:** (Dirección referencial a la ubicación del cliente)

Figura 72

Ingreso de usuario cliente – SmartOLT

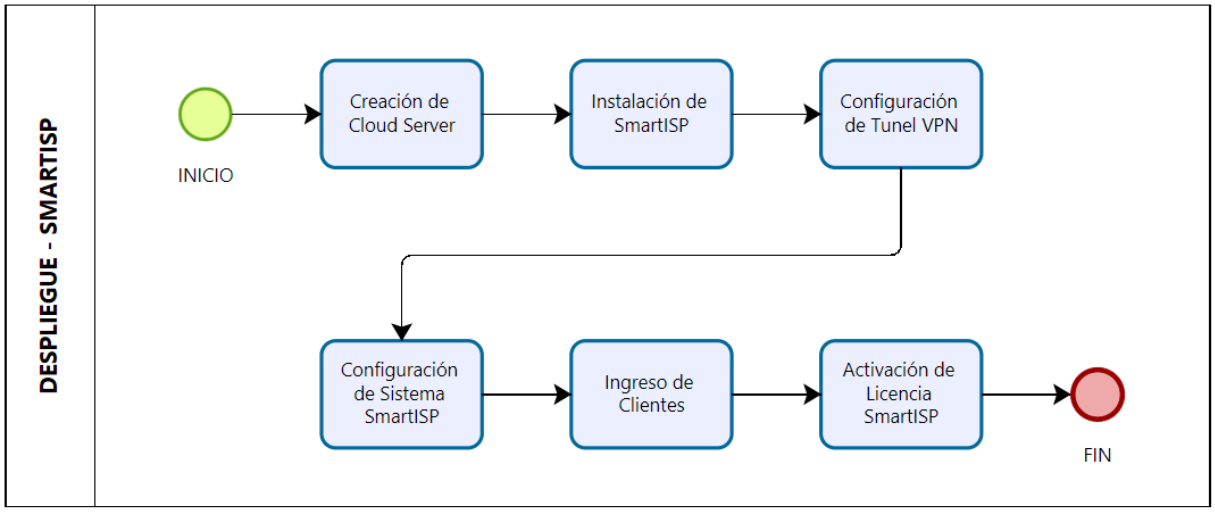


4.1.3.2.Implementación de SmartISP

La implementación de SmartISP en la red de CayambeVision S.A. es un procedimiento secuencial el cual tiene como objetivo realizar el enlace entre el equipo de Administración CCR-1036 y la herramienta de SmartISP alojada en la Nube, para lo cual se ha plateado cada uno de los ítems presentes en la **Figura 73**, los cuales detallan el proceso paso a paso a lo largo de este apartado.

Figura 73

Diagrama de implementación SmartISP

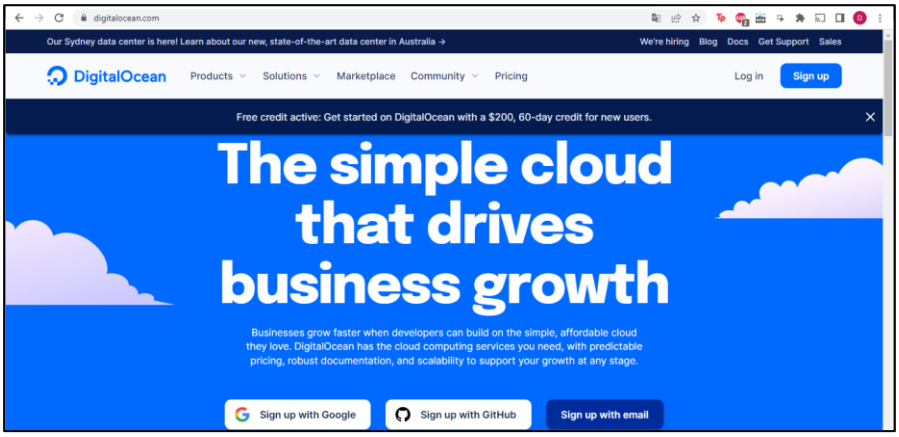


Creación de Cloud Server

La creación del Cloud server se la realiza con el fin de obtener una máquina virtual almacenada en la nube la cual posea una IP de acceso público. Es por ello por lo que se ingresa a la página https://www.digitalocean.com/ la cual se muestra en la **Figura 74**. Digital Ocean es un servicio el cual se encarga de realizar hosting de máquinas virtuales con la facilidad de parametrizarlos acorde a las necesidades del usuario.

Figura 74

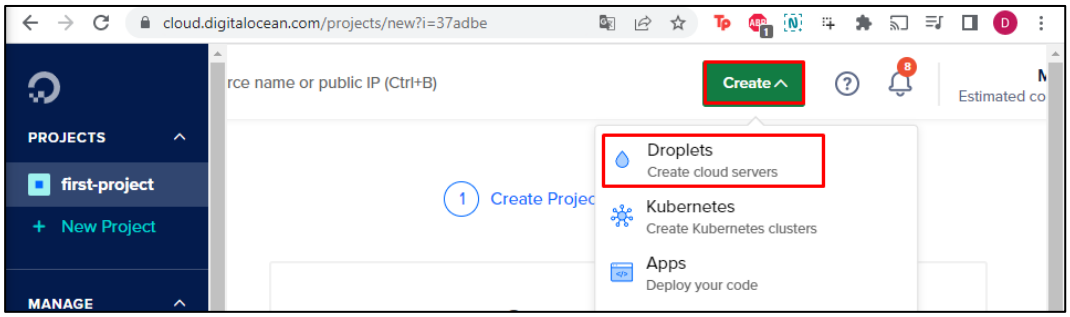
Sitio Web Digital Ocean



Un Cloud Server dentro de Digital Ocean se lo representa como un Droplet debido a su capacidad de expansión del servidor a las necesidades de su creador. En la **Figura 75** se muestra la manera en la cual se procede a crear un nuevo proyecto dirigiéndose a *Create→Droplets.*

Figura 75

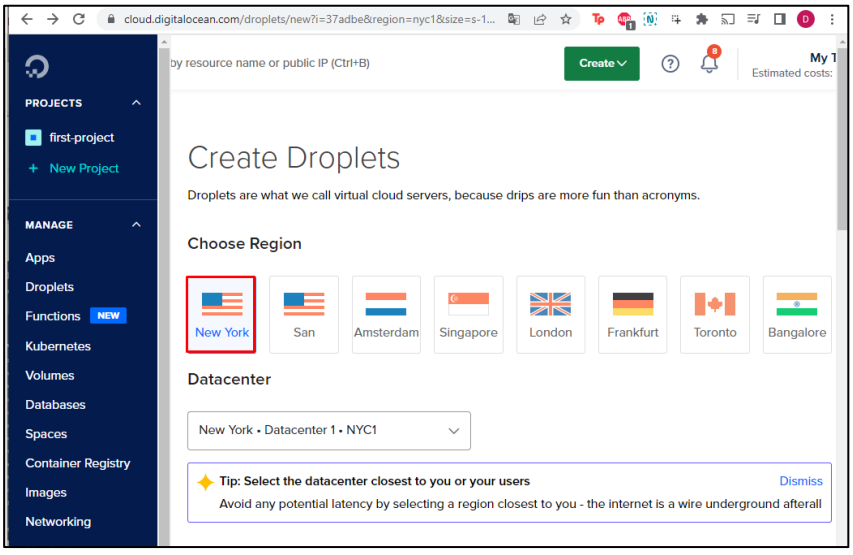
Creación de Cloud Server



Posterior a esto, se solicita el sitio destinado a albergar la máquina virtual, para el caso de SmartISP se selecciona *New York* como la región por defecto para la locación de Ecuador, esta selección se la puede ver en la **Figura 76**.

Figura 76

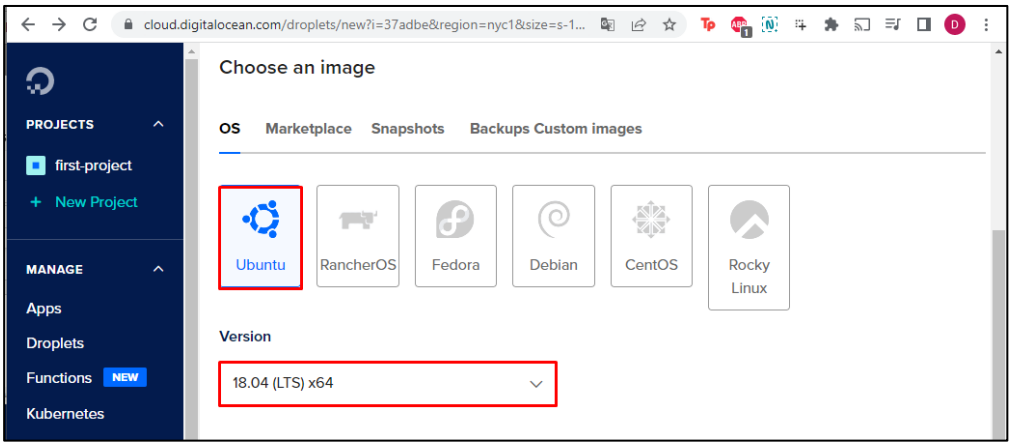
Región de Cloud Server



Como siguiente paso se selecciona la imagen del sistema operativo en la cual se busca correr en el servidor. SmartISP recomienda trabajar con el SO de Linux Ubuntu con la versión 18.04 (LTS) x64, por lo que en la **Figura 77** se seleccionan estas propiedades.

Figura 77

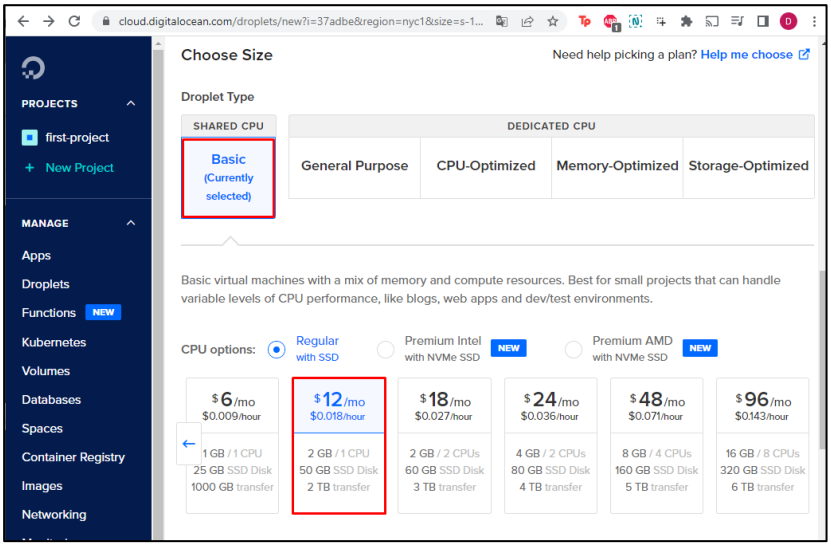
Configuración de SO y Versión



Una vez finalizado el paso anterior, se configura las características físicas del Servidor Virtual acorde a las necesidades para albergar SmartISP. Por lo cual, se selecciona un modelo *Básico* para la máquina virtual debido a que no se necesita un equipo robusto para poder correr SmartISP. Al Droplet de tipo básico le corresponde un precio de $12.00/mes el cual consta de 2GB de CPU, 50GB de Almacenamiento y 2TB para transferencia de datos. La **Figura 78** muestra la selección de las propiedades mencionadas.

Figura 78

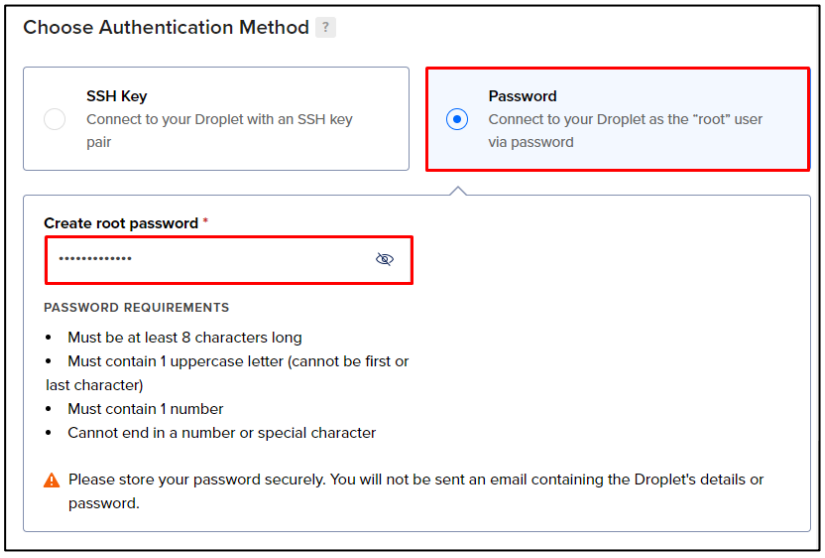
Configuración de Propiedades Fisicas del Servidor Virtual



Para finalizar el proceso de la creación del Cloud Server se solicita una contraseña de autenticación del usuario root para el acceso hacia nuestra máquina virtual. Esta contraseña debe contener mínimo 8 caracteres de longitud con al menos: una letra mayúscula, un carácter especial y un número como se muestra en la **Figura 79**.

Figura 79

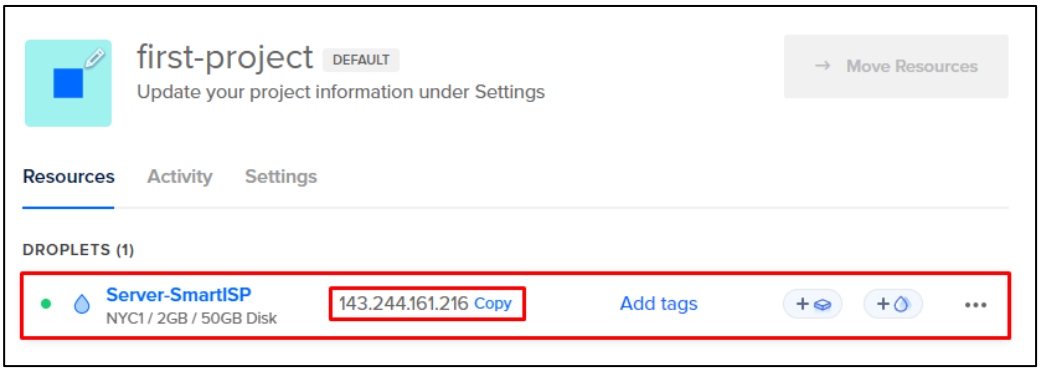
Configuración de Password Cloud Server



Como resultado final en la **Figura 80** se muestra la creación de la Máquina virtual a la cual se la asocia un IP de acceso externo (IP Pública – 143.244.161.216) con la que posteriormente se podrá ingresar mediante consola SSH(Acceso remoto Seguro) hacia el Cloud Server.

Figura 80

Resutado Cloud Server

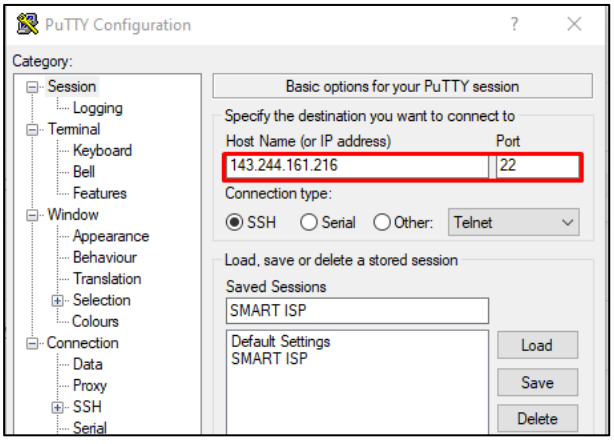


Instalación de SmartISP

Para iniciar con el proceso de Instalación de SmartISP se ingresa mediante Putty a la máquina virtual creada anteriormente. En donde, se ingresa la IP Pública 143.244.161.216 del Servidor Virtual y el puerto 22 que corresponde a una autenticación segura SSH. Este proceso se evidencia en la **Figura 81**.

Figura 81

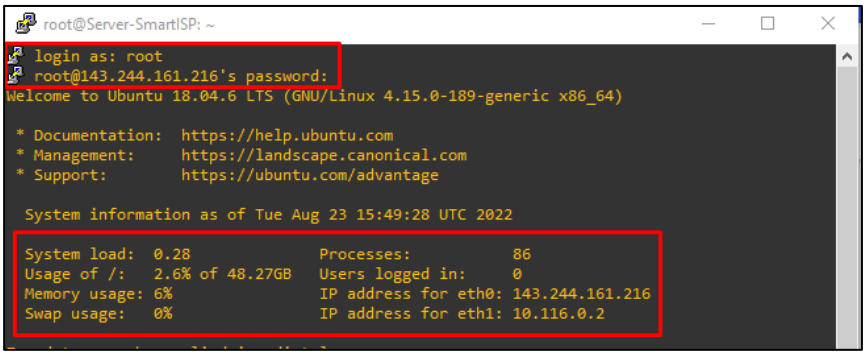
Ingreso Cloud Server via Putty



El siguiente paso es ingresar las credenciales creadas anteriormente del usuario root y así acceder a la máquina virtual. Este proceso mostrará como resultado las propiedades que posee el Servidor Virtual como se observa en la **Figura 82**.

Figura 82

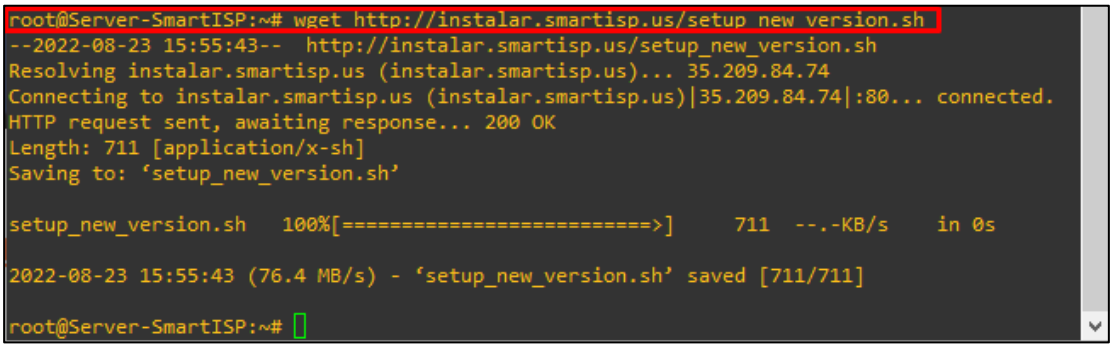
Ingreso Correcto a Servidor Virtual



La descarga del paquete de SmartISP se la realiza mediante el ingreso del comando wget http://instalar.smartisp.us/setup_new_version.sh en la consola, el cual permite descargar los paquetes e iniciar con la instalación como muestra en la **Figura 83**.

Figura 83

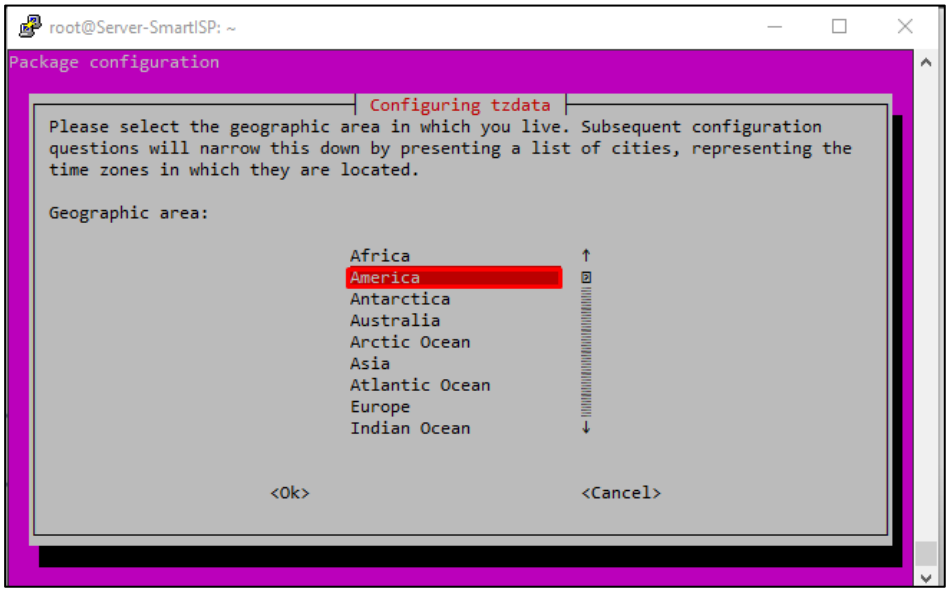
Descarga de SmarISP



Una vez descargados los paquetes se despliega un menú en cual permite la configuración de la zona horaria en la que se establecerá SmartISP, es por esto por lo que se selecciona el área geográfica de “América” como se muestra en la **Figura 84** la cual corresponde a la locación de CayambeVision S.A.

Figura 84

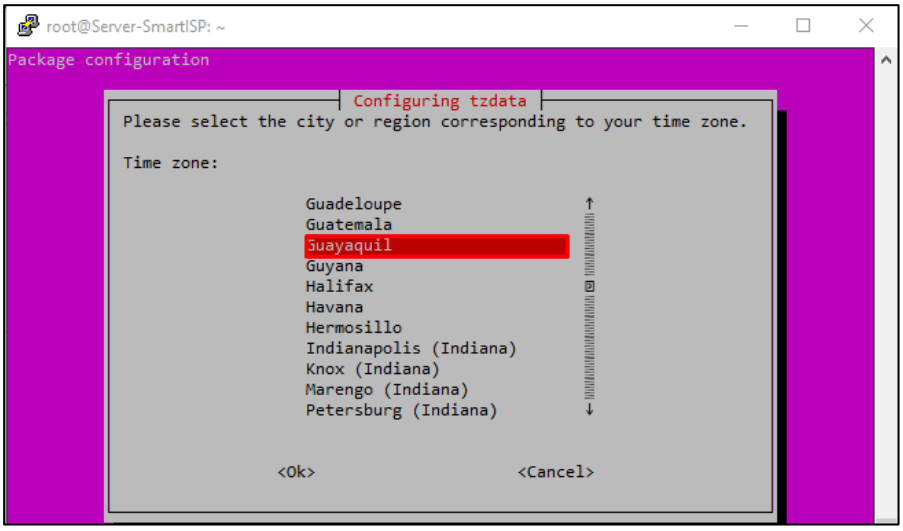
Configuración de Área Geográfica



Siguiendo con el procedimiento se configura la zona horaria correspondiente a nuestra ubicación por lo que se elige “Guayaquil” ya que es la correspondiente a Ecuador. De esta manera se podrá sincronizar la hora de SmartISP con los Equipos de CayambeVision S.A. este proceso se lo configura en la **Figura 85**.

Figura 85

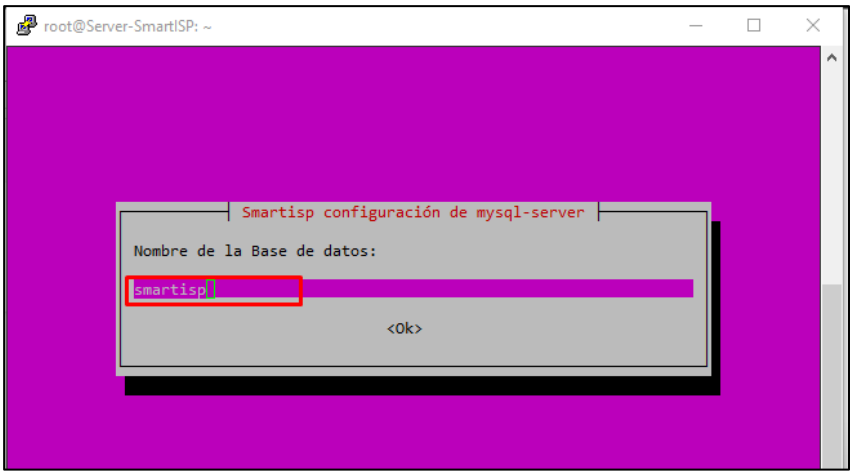
Configuración de Zona Horaria



Como siguiente paso se requiere crear una base de datos la cual guarde toda la información que se cargue en el sistema. En la creación de la base de datos de SmartISP se coloca el nombre "smartisp" tal como muestra la **Figura 86**, este nombre es tomado como recomendación de los autores del sistema.

Figura 86

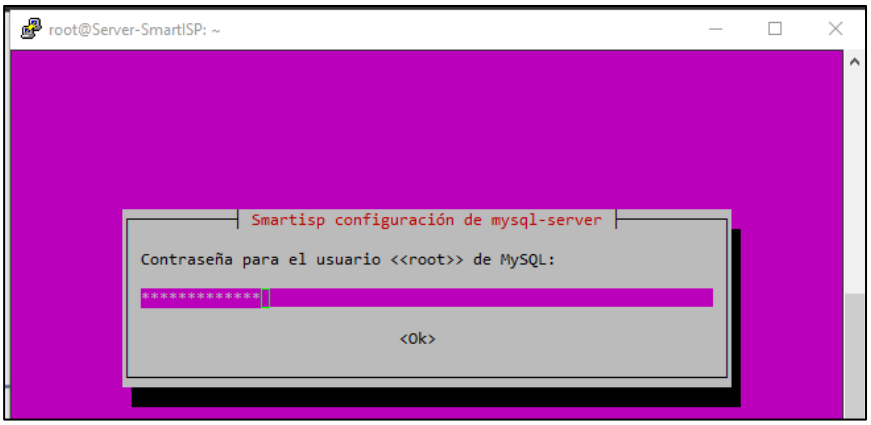
Creacon de base de datos SmartISP



La configuración de la base de datos concluye con la creación de una contraseña, esta sirve para autenticar el acceso a ella, por lo que se recomienda el ingreso de una llave fuerte y con varios tipos de caracteres como se observa en la **Figura 87**.

Figura 87

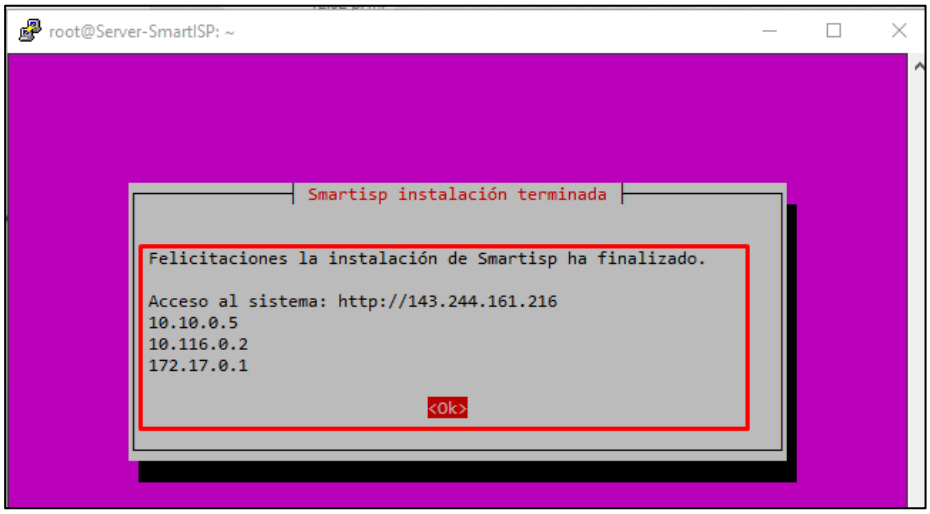
Contraseña Base de Datos SmartISP



Finalmente, en la **Figura 88** se muestra un cuadro de texto el cual refleja la culminación del proceso de instalación de SmartISP. Este cuadro muestra la IP de acceso al sistema mediante el siguiente enlace http://143.244.161.216/admin

Figura 88

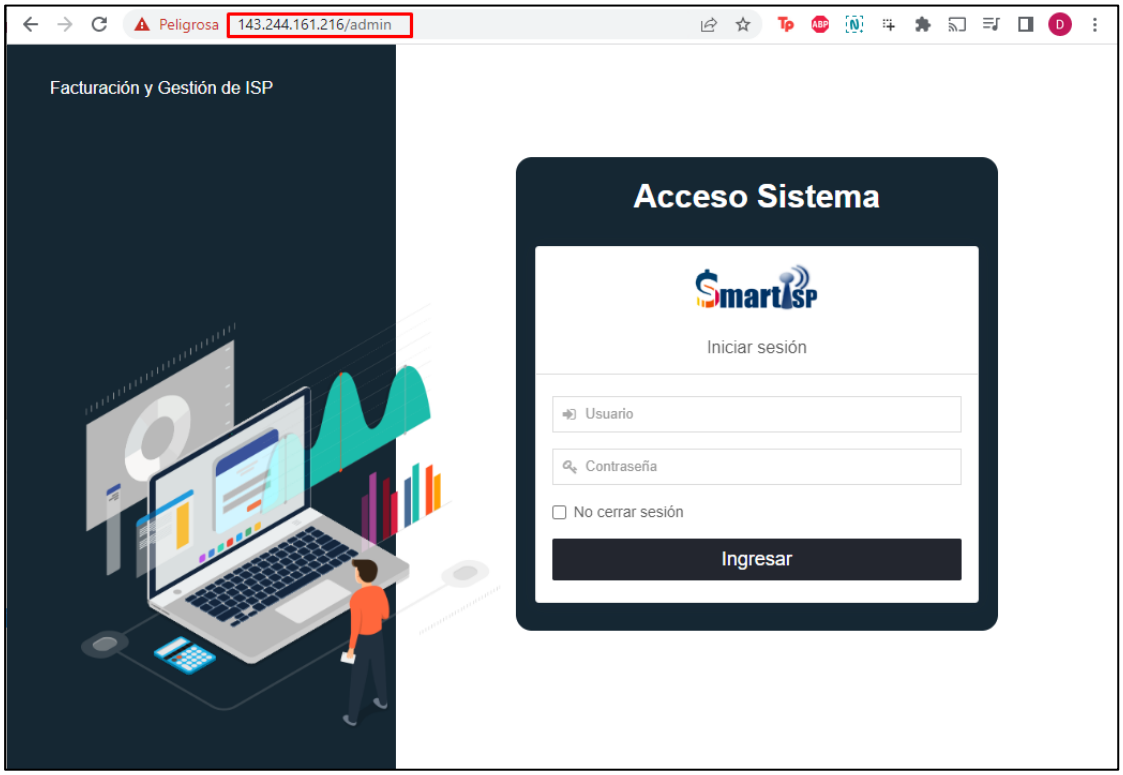
Finalización de Instalación SmatISP



Al momento de ingresar al enlace mostrado en el paso final del proceso de instalación, se obtiene como resultado en la **Figura 89** la página principal de acceso al Sistema SmartISP alojado e instalado en nuestro servidor en la nube. Las credenciales para el acceso a la plataforma son otorgadas por SmartISP vía correo.

Figura 89

Sistema SmartISP



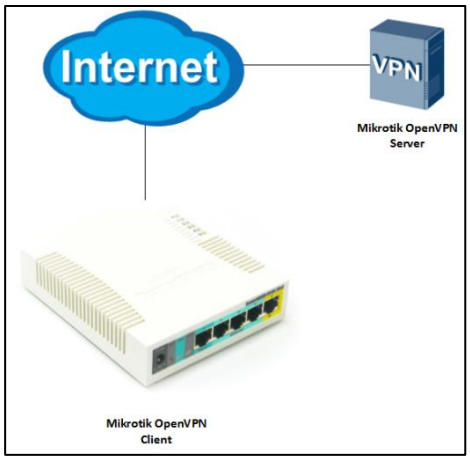
Configuración de Túnel VPN

La configuración del Túnel VPN tiene el fin de establecer una conexión punto a punto entre el equipo Mikrotik de Administración (CCR-1036) y el Sistema de SmartISP (Cloud Server). Haciendo así posible el envío de órdenes hacia el equipo Administrador.

El diagrama mostrado en la **Figura 90** representa la conexión vía VPN entre el usuario cliente (Mikrotik CCR-1036) y el Servidor OpenVPN (Cloud Server). El proceso de creación del Tunel VPN se lo puede observar detalladamente en el ANEXO A.

Figura 90

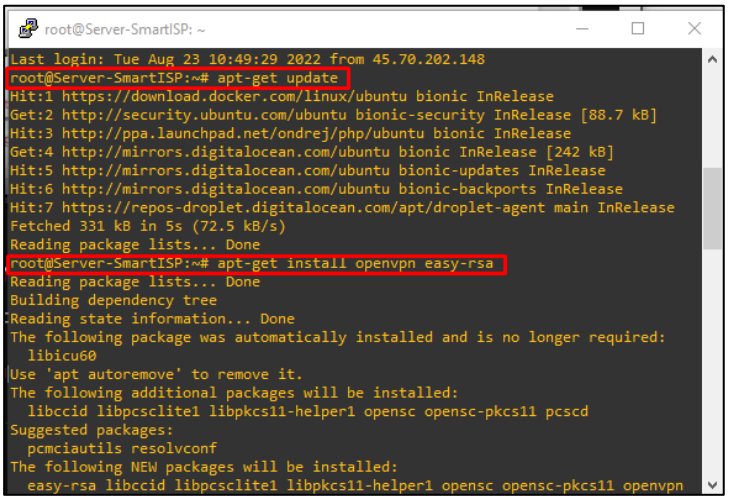
Diagrama de conexión VPN



Para instalar OpenVPN, lo primero que se realiza es la actualización de la máquina virtual y posterior ingresar el comando apt-get install openvpn easy-rsa tal como se muestra en la **Figura 91** con el cual se descargan los paquetes OpenVPN.

Figura 91

Instalación de OpenVPN



- ✓ *Creación de certificados y llaves del Servidor OpenVPN - Cliente*

Una vez instalado OpenVPN se procede a configurar los certificados de autorización los cuales permiten la autorización de conexión entre cliente y servidor VPN, para esto se ingresa el comando make-cadir certificates && cd certificates el cual se encarga de crear las carpetas destinadas para estos certificados.

El siguiente paso es la creación de certificados de autorización del servidor, para lo cual se ingresa el comando ./clean-all && ./build-ca, con el proceso de creación de los certificados también se crean las llaves de conexión para el servidor OpenVPN por lo cual se ingresa ./build-key-sever. Finalmente, ingresando openvpn --genkey --secret keys/ta.key. se crea la llave ta.key la cual servirá para introducir una firma digital HMAC en todas las transacciones entre el cliente y el servidor. De esta forma se puede verificar la integridad de los paquetes intercambiados entre el cliente y el servidor VPN.

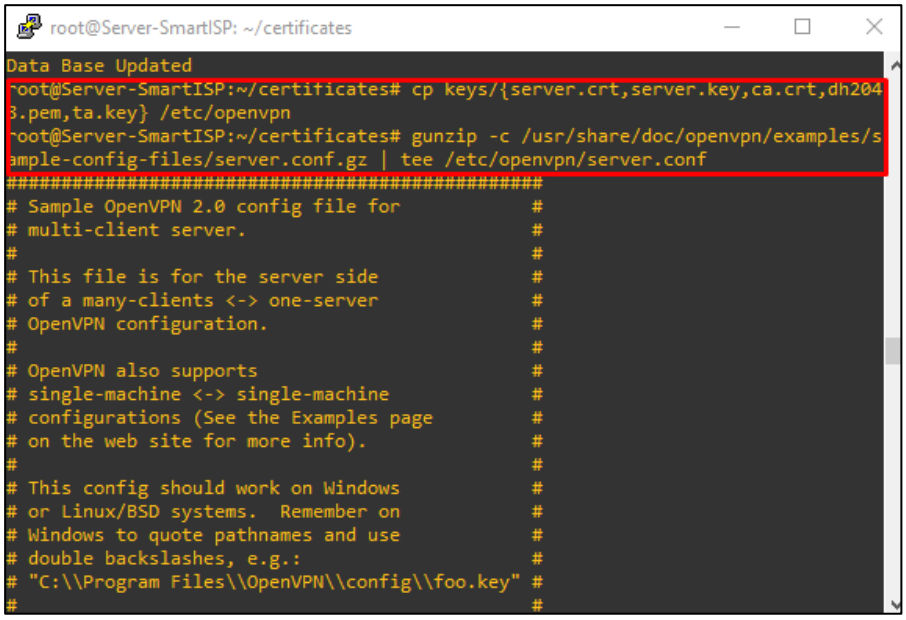
Posteriormente obtenidas las llaves y certificados para el Servidor OpenVPN se crean las destinadas para el usuario cliente, este proceso se realiza mediante source vars && ./build-key client de esta manera se obtiene como resultado las llaves que permiten la autenticación del usuario cliente con el servidor OpenVPN.

- ✓ *Configuración del Servicio OpenVPN*

A continuación, para la configuración del servicio OpenVPN se copia a la dirección /etc/openvpn las llaves, certificados de autenticación y certificación del servidor OpenVPN mediante el comando cp keys/{server.crt,server.key,ca.crt,dh2048.pem,ta.key} /etc/openvpn, como se muestra en la **Figura 92**.

Figura 92

Configuración del Servicio OpenVPN



Una vez ejecutado el comando para copiar se descomprime los archivos correspondientes al servidor de OpenVPN. Como paso siguiente se realizan cambios mostrados en la **Figura 93** al archivo alojado en /etc/openvpn/server.conf por lo que se ingresa y se realizan los siguientes cambios:

- Establecer el cifrado AES-128-CBC

cipher AES-128-CBC

- Cambiar protocolo de UDP a TCP:

protocol tcp

;protocol udp

- La compresión LZO debe estar deshabilitada

;comp-lzo

- Des comentar la configuración de nombre común duplicado (esto permite que varios clientes se conecten al servidor usando el mismo certificado):

duplicado-cn

- Comentar esta configuración (de lo contrario, produce errores de autenticación)

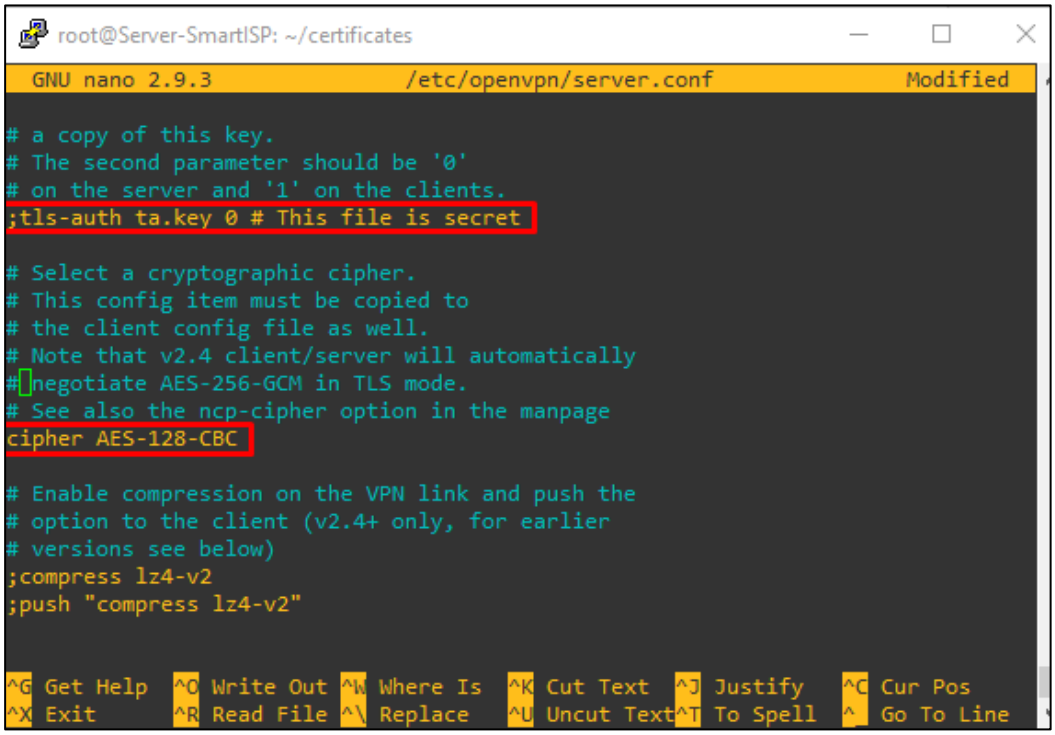
;tls-auth ta.key 0

- Comentar la configuración (no compatible con TCP):

;explicit-exit-notify 1

Figura 93

Configuración de Servcio OpenVPN

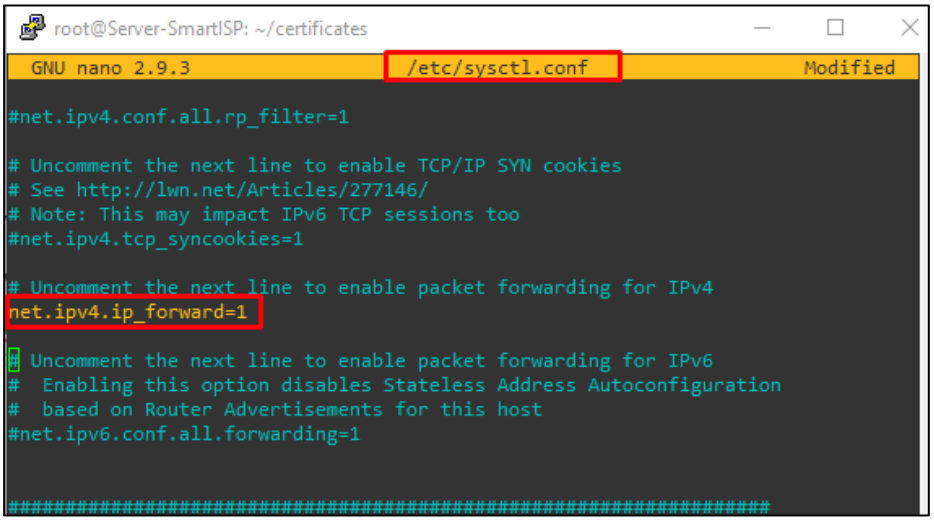


✓ *Configuración de red del Servidor OpenVPN*

El propósito de configurar la red del servidor es permitir la conexión entre el cliente VPN y el servidor VPN por lo que se ingresa a la dirección /etc/sysctl.conf en donde se des comenta la línea de comando net.ipv4.ip_forward=1. La cual permite el paso de datos a través de las interfaces del Servidor OpenVPN. La **Figura 94** muestra lo expuesto anteriormente.

Figura 94

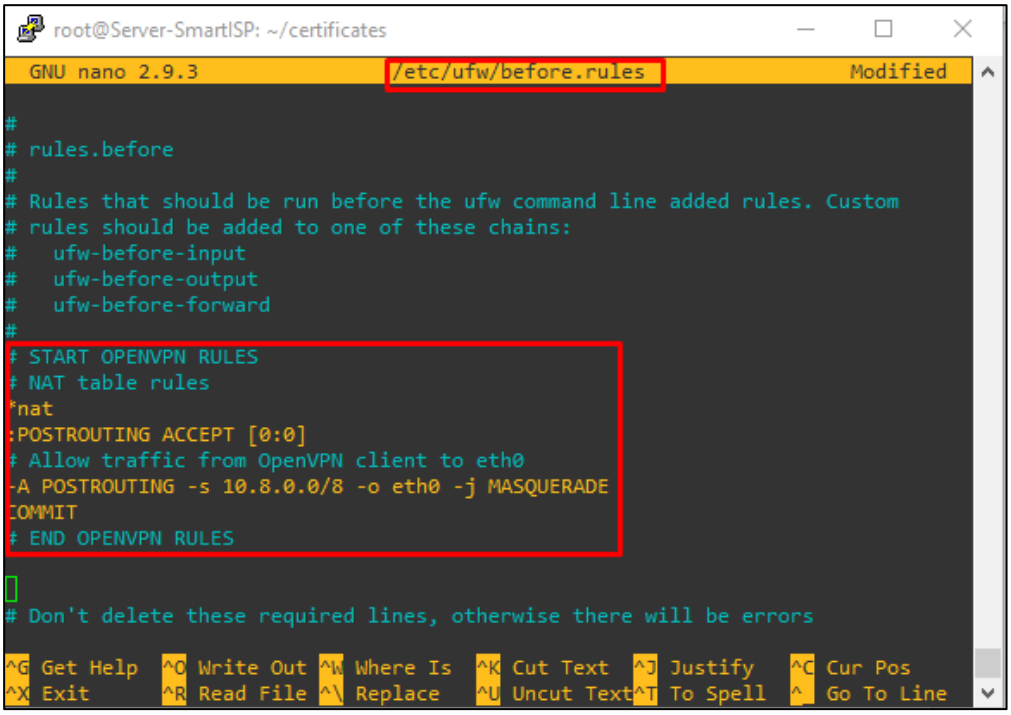
Activación de Forwarding Server VPN



El direccionamiento asignado para el Túnel VPN se lo ingresa en el fichero /etc/ufw/before.rules. Aquí se activa el NAT mediante el segmento de salida 10.8.0.0/8 a través de la interfaz eth0 del Servidor OpenVPN, como se observa en la **Figura 95**, en este caso se busca permitir el ingreso externo mediante el túnel VPN.

Figura 95

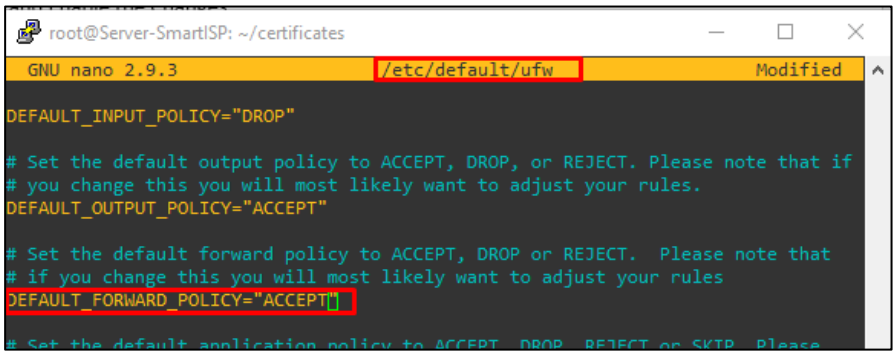
Direccionamiento NAT para Tunel VPN



A continuación, se configura el Firewall del Cloud Server en donde se cambia el estado de "DROP" a "ACCEPT" en la dirección /etc/default/ufw con el fin de permitir la conexión a través de la interfaz del Cloud Server para así tener conexión con SmartISP, esto se observa en la **Figura 96**.

Figura 96

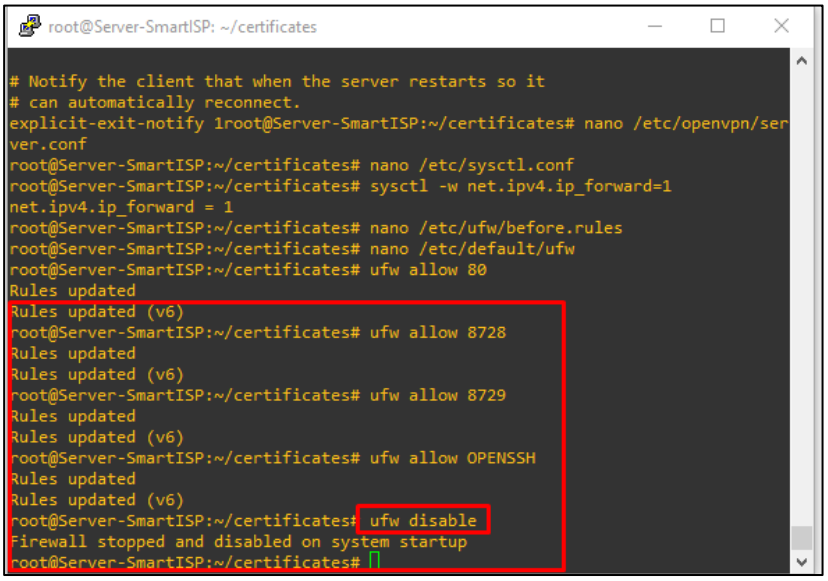
Cambio de Politicas de Conexión - Tunel VPN



La configuración de la red finaliza habilitando los puertos 8728, 8729, OPENSSH correspondientes al puerto API y conexión segura SSH. También se deshabilita el firewall para que no exista bloqueo de hosts al momento de establecer el túnel VPN, en cuadro rojo de la **Figura 97** se hace énfasis a lo mencionado anteriormente.

Figura 97

Configuración de Firewall

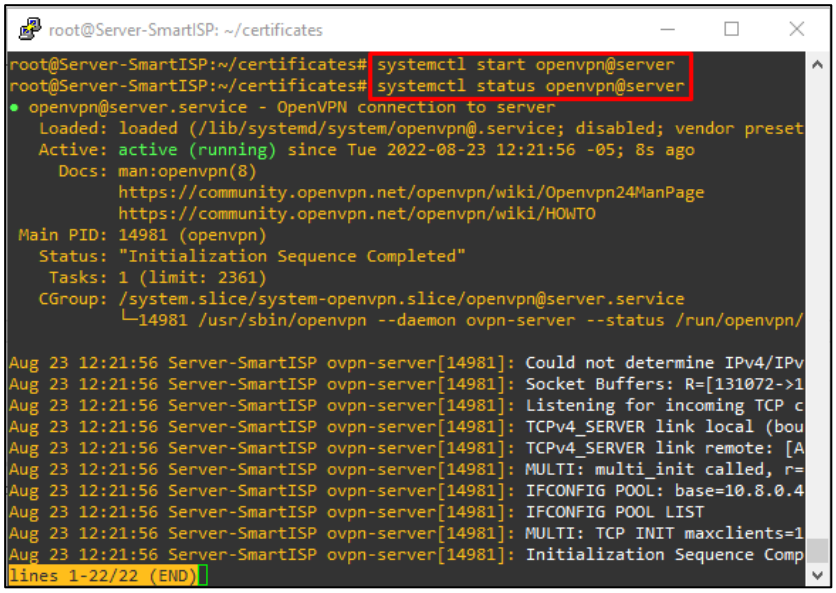


Establecidas las configuraciones anteriores se procede a habilitar el inicio automático y activación del servicio de OpenVPN con el fin de prevenir cualquier tipo de caída y que el Administrador de red deba levantar el servicio de manera manual. Para esto se utilizan los comandos que se indican en la **Figura 98**.

- systemctl start openvpn@server
- systemctl status openvpn@server
- systemctl enable openvpn@server

Figura 98

Activación de OpenVPN Server



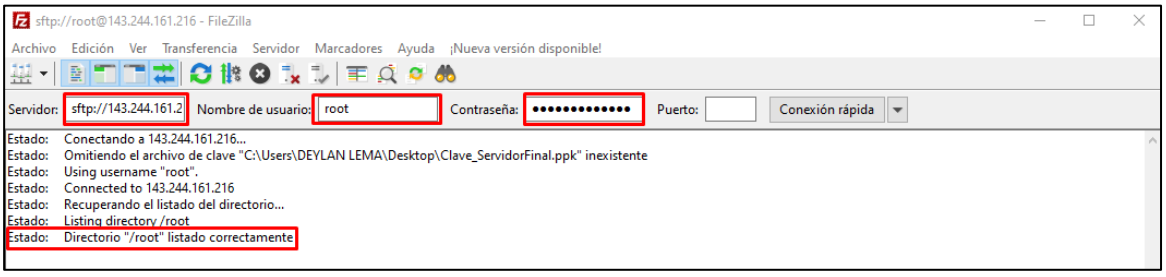
- ✓ *Configuración de enlace Mikrotik a OpenVPN Server*

Para realizar las configuraciones en el Mikrotik se necesita descargar las llaves del cliente que serán asociadas al Tunel VPN. Se utiliza el programa FileZilla mostrado en la **Figura 99** el cual es un servidor FTP que nos ayuda a descargar y subir archivos a un host en específico. De esta manera se procede a ejecutar FileZilla e ingresar las credenciales de acceso a la máquina virtual.

Host: *143.244.161.216* Usuario: *root* Puerto: *22*

Figura 99

Ingreso a Servidor FTP - FilZilla



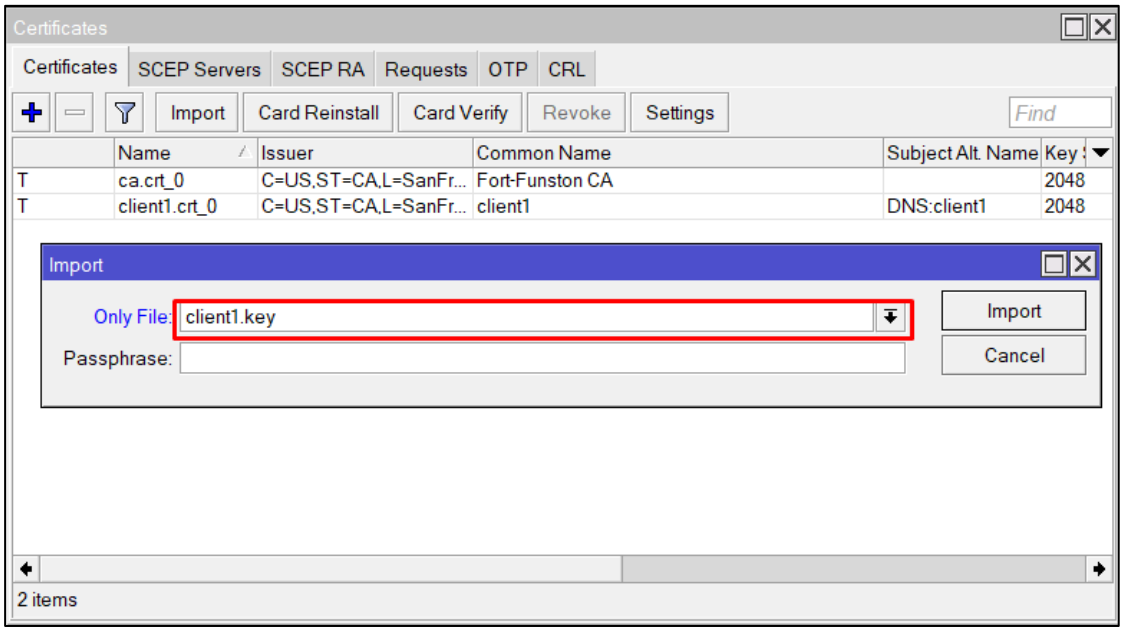
Una vez ingresados se extraen las llaves creadas para el cliente1 por lo cual se ingresa al fichero /root/certificates/keys/ y se descarga los certificados:

- client1.crt
- client1.key
- ca.crt

Estos certificados son introducidos en la carpeta de archivos del equipo CCR-1036 los cuales son agregados uno a uno en la parte de System→Certificates en el siguiente orden: ca.crt client1.crt y finalmente client1.key. Este proceso se evidencia en la **Figura 100**.

Figura 100

Ingreso de Certificados de Cliente 1

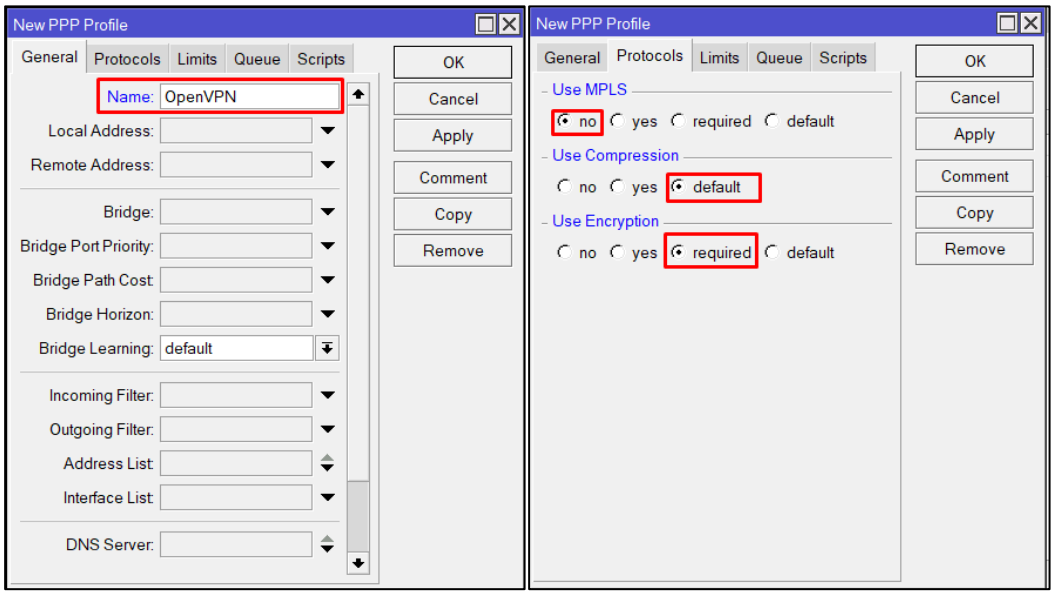


A continuación, en la **Figura 101** y **Figura 102** se procede a crear el perfil PPP (Point to Point - Protocol) ingresando al menú *PPP→Profiles*. Aquí se coloca el nombre del perfil. El

siguiente paso es cambiar a la pestaña de protocolos y deshabilitar MPLS, usar la compresión por defecto y requerir la encriptación.

Figura 101

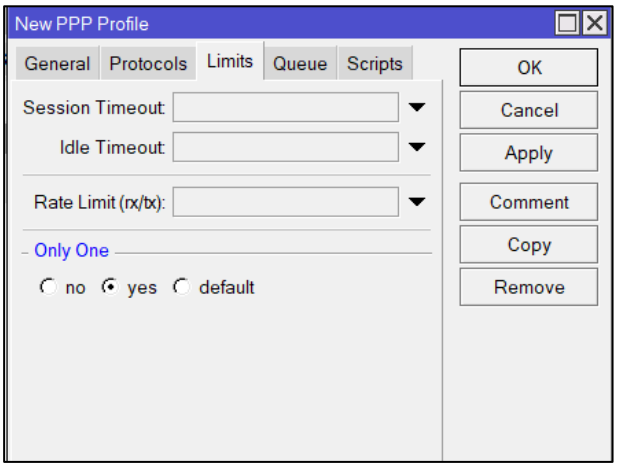
Creación de Perfil PPP



Los límites de la sesión se establecen en uno solo con el objetivo de proteger que más un perfil OpenVPN Server pueda ingresar al equipo.

Figura 102

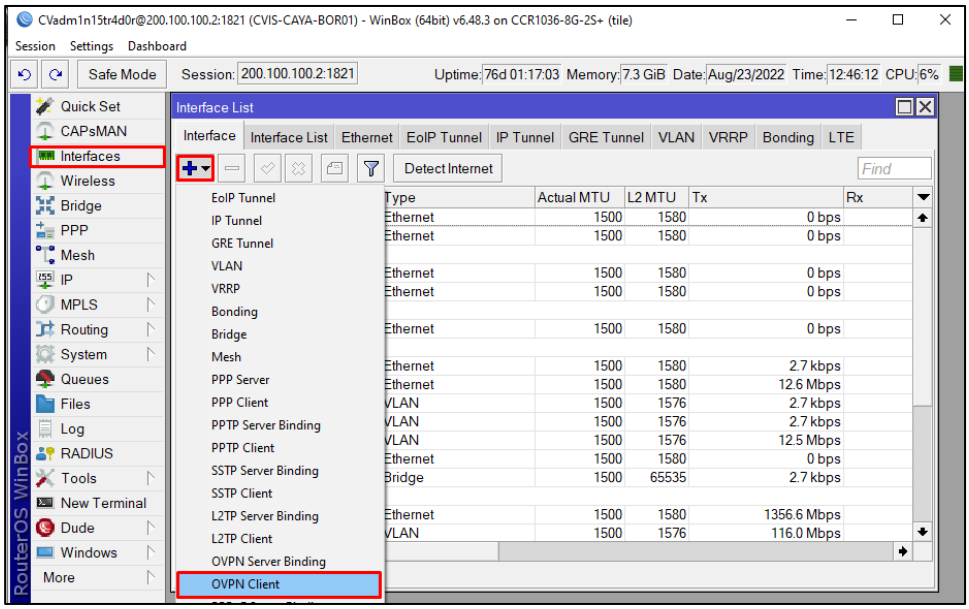
Configuración de Perfil PPP



Finalmente se crea una interfaz virtual destinada para la conexión OpenVPN cliente hacia el servidor configurado previamente. Para esto se ingresa a *PPP→-Interface* y se crea un "*OVPN Client*" como es mostrado en la **Figura 103**.

Figura 103

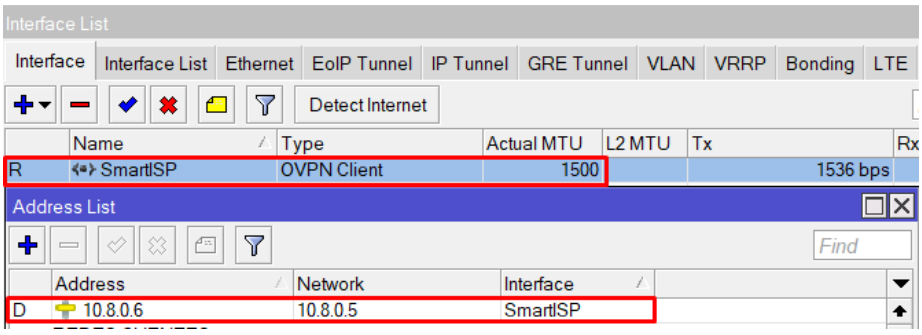
Creación de interfaz OVPN



Como resultado de la creación de la interfaz OVPN Client se obtiene la **Figura 104** en la cual se verifica la correcta creación del cliente VPN ingresando a *Interface* identificando la letra R en la parte izquierda lo cual significa *Running* y también dirigiéndose a *IP→Address List* en donde se puede observar que se otorga por parte del servidor VPN una IP dinámica al Cliente VPN dentro del segmento 10.8.0.0/8 configurado con anterioridad.

Figura 104

Conexión Establecida con OpenVPN Server



Configuración del Sistema SmartISP

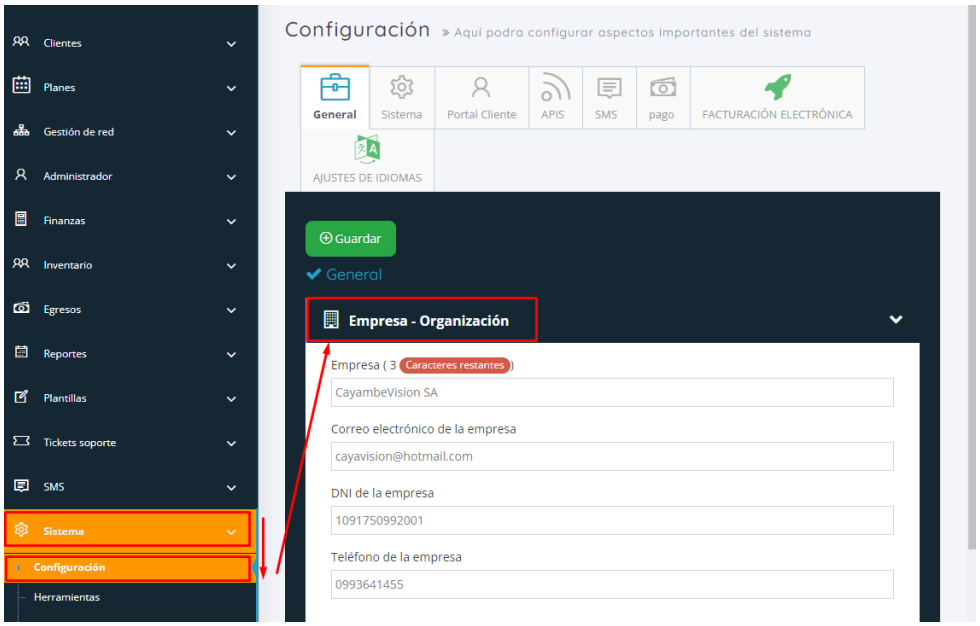
La configuración del Sistema SmartISP consiste en personalizar la plataforma con datos técnicos (conexión con SmartISP, ingreso de direcciones IP, configuración de planes de servicio) y administrativos de la empresa (perfil de empresa, creación de usuarios). Todos estos datos mencionados anteriormente permiten darle una identidad al sistema y enlazarlo con la información que se presenta en la red de CayambeVision S.A. De esta manera se desarrollan los puntos mostrados a continuación y se los detalla en el **ANEXO** B.

- ✓ *Configuración Empresa*

El apartado que permite la configuración del perfil de la empresa se lo encuentra en *Sistema→Configuración→Empresa → Organización,* en donde se procede a completar la información que identifica a la empresa. Esta información solicitada se la puede observar en la **Figura 105**.

Figura 105

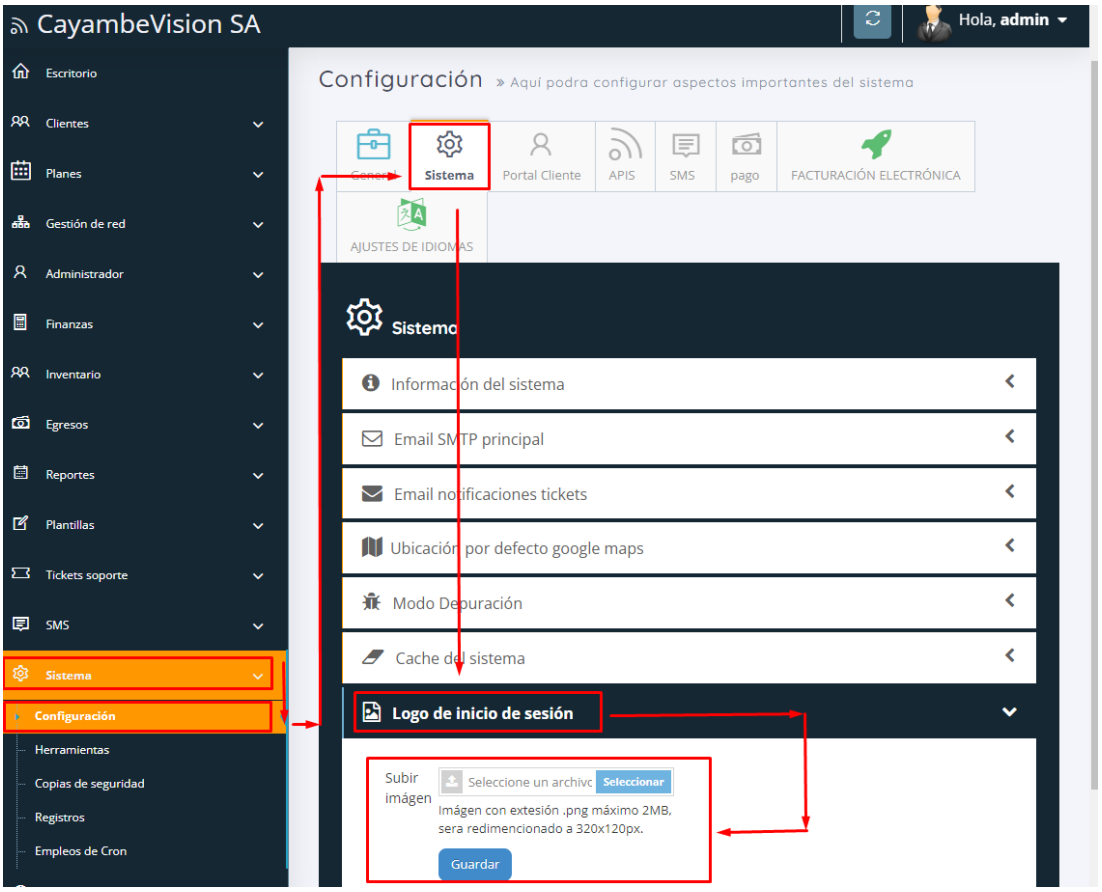
Configuración de Perfil de Empresa



Posterior a esto, también es necesario modificar el logo de inicio de sesión que se muestra al momento de ingresar a SmartISP, para lo cual se debe dirigir a *Sistema→Configuración→Sistema→Logo de inicio de Sesión*. Aquí se ingresa el logo de la empresa en un formato *.png* con una extensión de *320x120px* y un peso máximo del archivo de *2MB*. Esta información mencionada se la muestra en la **Figura 106**.

Figura 106

Configuración Logo de inicio

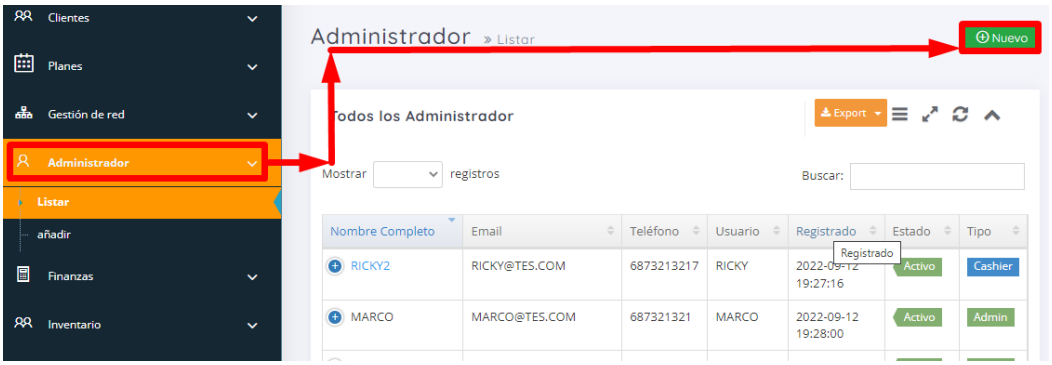


✓ *Creación de Usuarios*

La creación de los usuarios para el manejo de SmartISP se la realiza a partir del nivel que el usuario posea dentro de la empresa. Para ello en la **Figura 107** se ingresa al menú *Administrador→Nuevo* en donde se inicia el proceso de creación de un nuevo perfil de usuario.

Figura 107

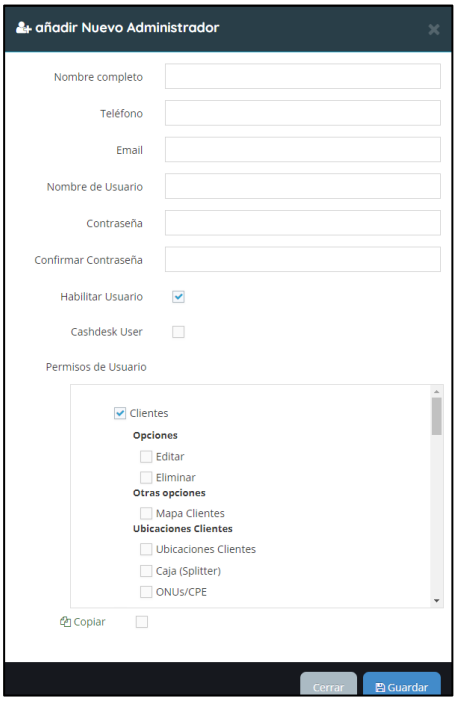
Creación de perfil de usuario



Posterior a esto, se despliega la ventana mostrada en la **Figura 108**, en donde finalmente se llenan los campos del usuario tales como: nombre, teléfono, usuario, contraseña. Aquí también se definen los permisos que poseerá dicho usuario al momento de ingresar a SmartISP, estos campos son llenados por el administrador acorde a sus necesidades.

Figura 108

Características de usuario

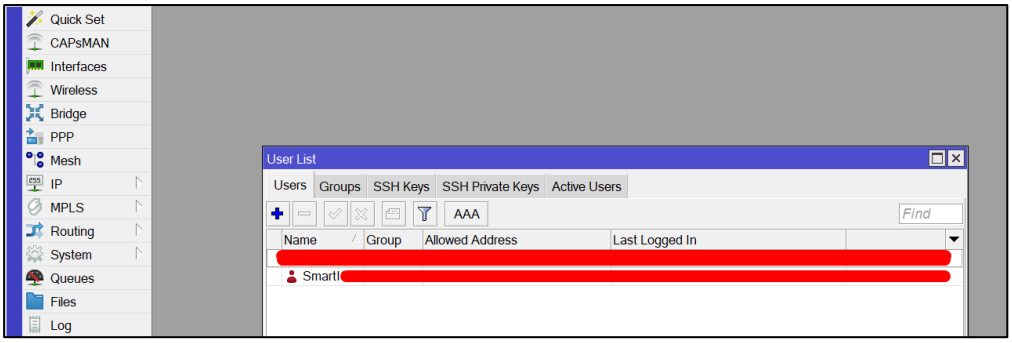


✓ *Conexión SmartISP – Mikrotik Administrador (CCR-1036)*

Para la conexión de SmartISP con el Core Mikrotik CCR-1036 se procede a crear un usuario en el equipo Administrador ingresando al menú *System→Users* como se muestra en la ***Figura 109*** y se crea un nuevo perfil de usuario con las credenciales de administrador, ya que este usuario será capaz posteriormente de enviar sentencias a través de comandos hacia el equipo mediante el túnel VPN creado anteriormente.

Figura 109

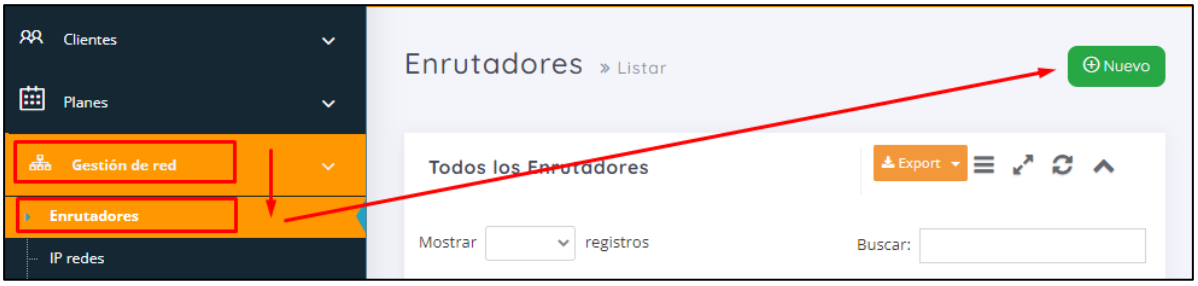
Perfil de administracion CCR-1036



Posteriormente, en SmartISP se ingresa al menú *Gestión de Red→Enrutadores→Nuevo* con el objetivo de crear un nuevo perfil de equipo enrutador, para así poder enlazar el equipo de administración y el servicio de SmartISP. En la **Figura 110** se puede evidenciar el proceso mencionado con anterioridad.

Figura 110

Creación de nuevo enrutador - SmartISP

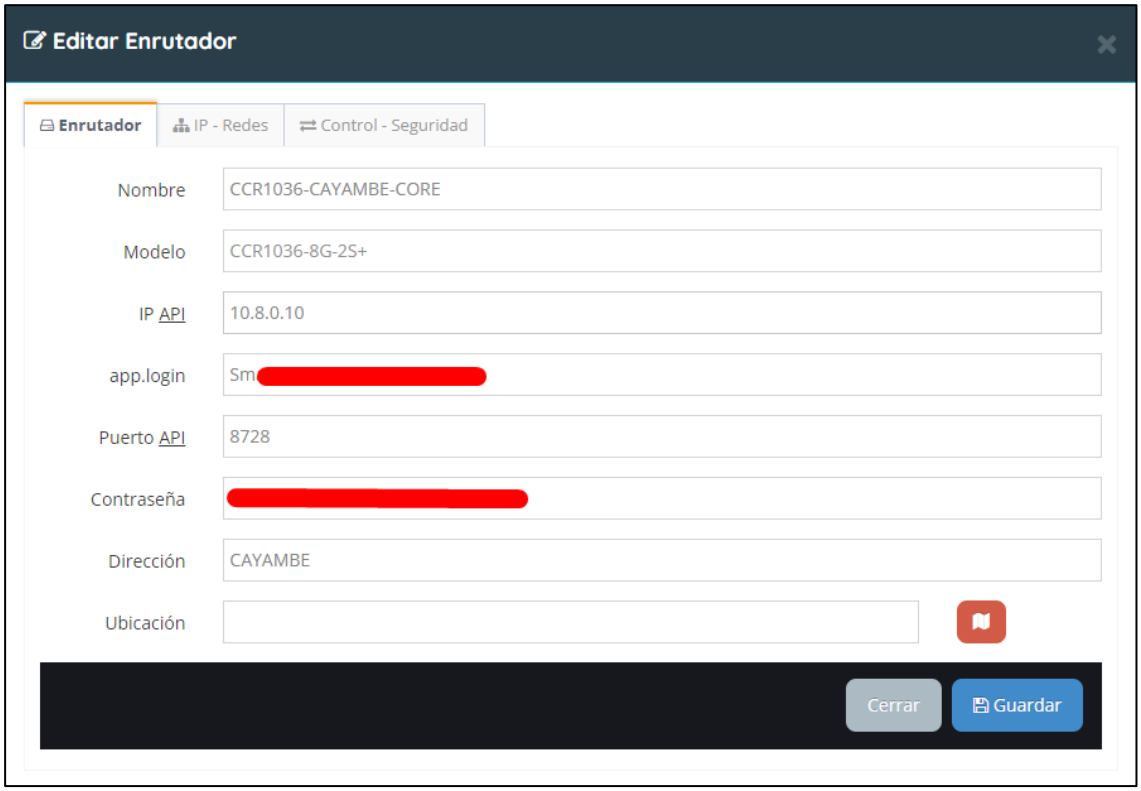


Una vez presionado en *Nuevo* se despliega el cuadro mostrado en la **Figura 111** en el cual se solicitan datos como: nombre, modelo, ip api, app.login, puerto api, contraseña, dirección, ubicación. Todos estos datos han sido obtenidos en los procesos de configuración realizados con anterioridad. A continuación, se detalla de mejor manera los requisitos:

- **Nombre:** *CCR1036-CAYAMBE* (Nombre distintivo para el Enrutador).
- **Modelo:** *CCR1036-8G-2S+* (Modelo del Equipo Mikrotik).
- **IP API:** *10.8.0.10* (IP asignada por el Servidor OpenVPN).
- **App.login:** *XXXXXXX* (Usuario Mikrotik).
- **Puerto API:** *8728* (Puerto API Mikrotik).
- **Contraseña:** *XXXXXXX* (Contraseña de usuario Mikrotik).
- **Dirección:** *CAYAMBE* (Dirección referencial).
- **Ubicación:** Ubicación Maps.

Figura 111

Ficha de creación de Enrutador – SmartISP



Finalmente, en la **Figura 112** se puede evidenciar el estado "En línea" el cual confirma que se ha realizado correctamente la conexión de SmartSIP y el equipo Mikrotik CCR-1036, de esta manera una vez concluido el proceso SmartISP a través de un túnel VPN será capaz de enviar sentencias de comandos hacia el equipo de administración alojado en la red interna de CayambeVision S.A.

Figura 112

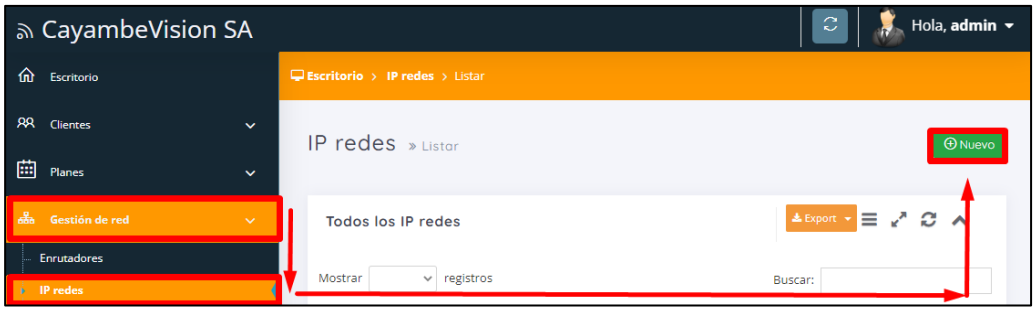
Creación finalizada perfil Enrutador -SmartISP

✓ *Configuración de Red – IPs*

Esta configuración se la realiza con el fin de albergar en el sistema SmartISP todas las redes existentes en el equipo de Administración CCR-1036, de esta manera se logra emparejar posteriormente a cada usuario de la red con su respectiva IP, para lo cual se realiza el proceso indicado en la **Figura 113**, ingresando al menú *Gestión de Red→IP redes→Nuevo.*

Figura 113

Configuración de IPs – SmartISP



✓ *Configuración de Planes*

La configuración de los planes que se ofrece en CayambeVision S.A., se la realiza siguiendo los pasos mostrados en la **Figura 114**, presionando en el menú *Planes* → *Listar*→ *Crear Plan*. De esta manera se procede a crear los planes con la velocidad de uplink, dowlink y el costo respectivo para cada uno de estos. Los cuales posteriormente serán asociados a los usuarios cliente según sea necesario.

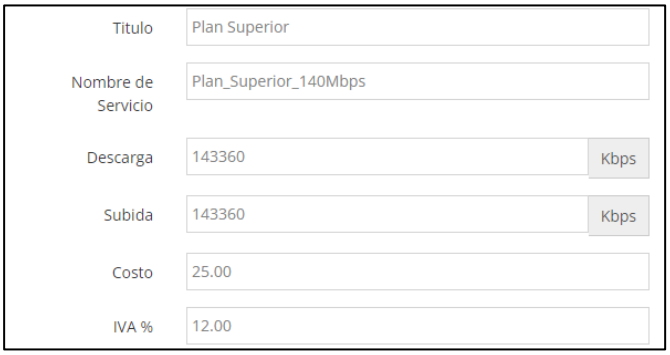
Figura 114

Configuración de Planes

Una vez presionado en *Crear Plan* se despliegan los campos mostrados en la **Figura 115**. correspondientes a: nombre del Plan, Velocidad de Descarga, Velocidad de Subida, Costo, Porcentaje de IVA. Todos estos campos deberán ser llenados con la información que se oferta en la empresa CaymabeVision S.A.

Figura 115

Creación de Plan

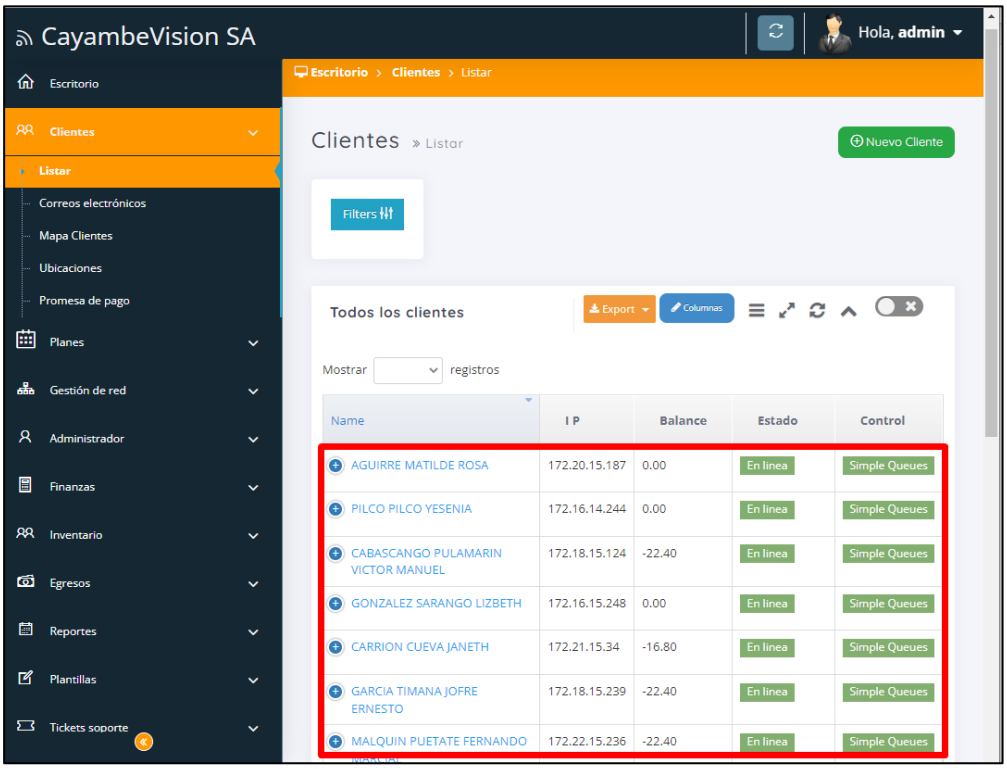


Ingreso de Clientes

El ingreso de clientes se lo realiza a través de los datos del cliente, en donde se debe listar en un archivo de Excel la siguiente información: nombre, dirección, IP del cliente, Plan de suscripción, fecha de pago. Una vez obtenidos los datos se procede a importar el archivo hacia la plataforma de SmartISP en donde una vez realizado el proceso se obtiene como resultado la **Figura 116**, en donde, en el menú Menú *Clientes→Listar* se encuentran los perfiles de clientes importados correctamente.

Figura 116

Ingreso de Clientes



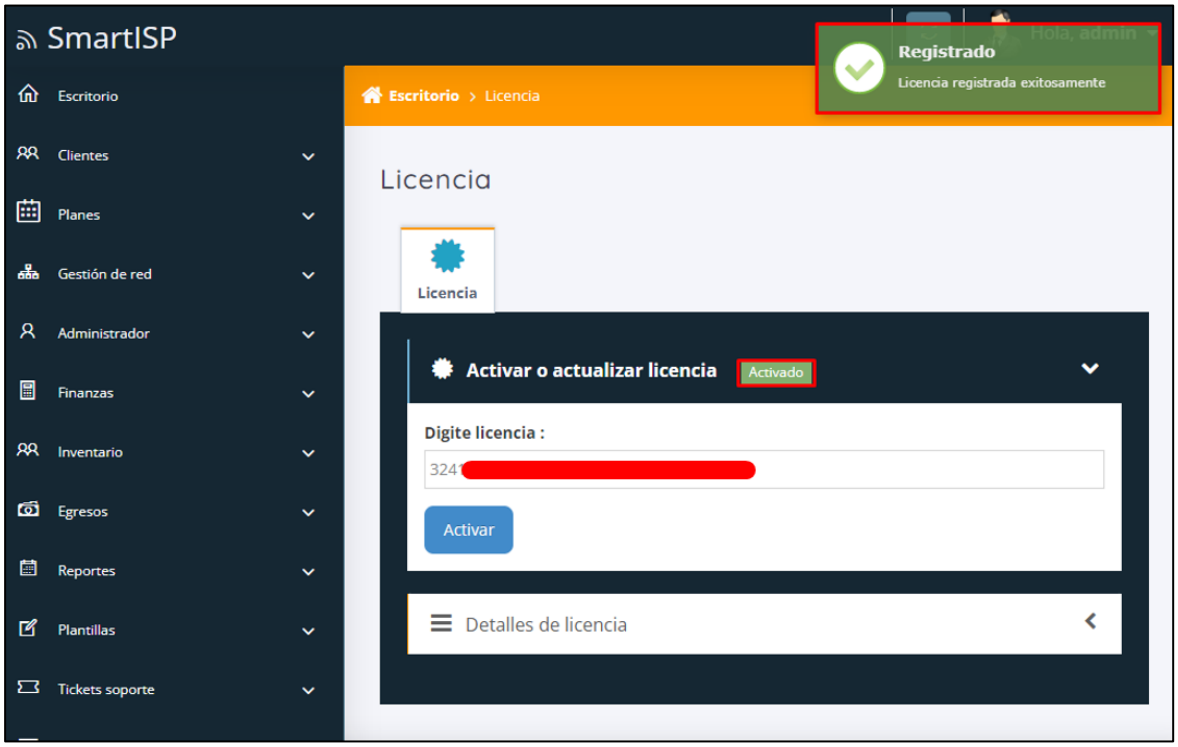
Activación de Licencia SmartISP

Para proceder con la activación de la Licencia SmartISP se ingresa al sitio oficial www.smartisp.us, en donde se realiza la compra y posteriormente se obtiene el código de la

licencia. La licencia permite activar el servicio y así permitir el uso de todas las herramientas para la Administración de la red que ofrece. Una vez ingresada la Licencia se identifica el mensaje de registro mostrado en la **Figura 117** la cual confirma la correcta activación del servicio de SmartISP.

Figura 117

Activación de Licencia SmartISP



4.1.4. Control de Cambios

Para lograr la correcta implementación de los servicios se genera un control de cambios, en el cual se refleja las modificaciones realizadas en la red de CayambeVision S.A., esto se realiza con el fin de documentar todas las actividades ejecutadas por parte de la persona a cargo del proyecto y el administrador (encargado responsable) actual de la red. De esta manera se procede a generar un documento que respalde todo el proceso de la implementación de las herramientas en la red.

En CayambeVision S.A. no se contaba con un formato destinado al control de las configuraciones físicas y lógicas dentro de la red, de esta manera se procede a generar una ficha basada en la ISO/IEEE 29148 en la cual se requiera información concisa y específica para llevar un correcto control de cambios dentro de la empresa. Se procede a plantear la Tabla 22 como referencia al nuevo modelo de control en la red. Este modelo es presentado y se lo aplica con la respectiva aprobación del administrador logrando así obtener el ANEXO 4 en el cual se refleja todo el proceso de implementación de las herramientas en la red.

Tabla 22

Ficha de control de cambios

VERSIÓN	FECHA DE MODIFICACIÓN	MODIFICACIÓN	RESPONSABLE
00	dd/mm/aaaa	Breve descripción del proceso realizado	Responsable del cambio realizado
01	dd/mm/aaaa	Breve descripción del proceso realizado	Responsable del cambio realizado

4.1.5. Liberación de Servicios

Una vez realizadas todas las configuraciones pertinentes para permitir el enlace de las herramientas destinadas a solucionar problemas presentados por el alto tiempo de respuesta a incidentes en la red de CayambeVision S.A. (soluciones representadas por los servicios SmartOLT y SmartISP), se procede a entregar toda la documentación relacionada con la implementación de

las herramientas, así como guías correspondientes a los procesos identificados en el capítulo anterior.

Para la liberación y ejecución de los servicios se realiza un documento en el cual se busca la autorización por parte de los encargados en el seguimiento de la aplicación del proyecto, para lo cual se pone a disposición ANEXO 5 con el fin de respaldar el procedimiento a través del documento. Una vez aceptada la liberación de los servicios se procede a ejecutar las herramientas implementadas haciendo referencia a los procesos presentados anteriormente en el levantamiento de información con los cuales se busca mejorar el rendimiento de la Gestión y Administración de la red.

Los procesos actuales se los presenta en base a la propuesta de cambio establecida en el punto 3.3 del capítulo anterior, los distintos escenarios se los agrupa acorde a su función, de esta manera se tiene a SmartOLT como la encargada de llevar a cabo los procesos relacionados con la gestión de la red, mientras que SmartISP se utiliza para las actividades de administración de la red, de esta manera se establece la siguiente Tabla 23 en donde se clasifica los procesos con su respectiva herramienta encargada para la ejecución de estos.

Para llevar a cabo la ejecución de la propuesta de cambios presentada en el apartado 3.3. se realiza una capacitación a cada una de las áreas de la empresa CayambeVision S.A.. En donde, se presentan los nuevos procesos obtenidos como soluciones a los problemas existentes en la gestión y administración de la red. Posterior a esto, se brinda una capacitación y la entrega de guías técnicas las cuales buscan establecer un buen manejo de las herramientas SmartOLT y SmartISP por parte de cada uno de los usuarios de la empresa. El ANEXO 6 muestra el proceso de capacitación a cada una de las áreas de CayambeVision S.A.

Tabla 23

Agrupación de procesos actuales

PROCESO	SMARTOLT	SMARTISP
Proceso 1: Configuración de OLT	X	
Proceso 2: Ingreso de Clientes ONT/ONU	X	
Proceso 3: Comandos de Verificación de estado	X	
Proceso 4: Ingreso de Clientes		X
Proceso 5: Pago de Servicios		X
Proceso 6: Generación de Tickets de Soporte		X
Proceso 7: Suspensión de servicio		X

4.1.5.1.Resultados de ejecución SmartOLT

PROCESO 1: Configuración de OLT

La configuración de la OLT mediante el uso de SmartOLT se realiza de manera sencilla gracias a la interfaz gráfica que presenta el servicio. Para analizar el resultado de la ejecución de este proceso, se toma al tiempo de demora como una variable de la misma manera como se realiza en el apartado 3.3.4. logrando así obtener la Tabla 24 que refleja el tiempo promedio y las áreas involucradas para su ejecución. Para representar el proceso actual que se lleva a cabo para realizar la configuración de la OLT se genera una guía técnica indicada en el ANEXO C1.

Tabla 24

Tiempo de respuesta actual Proceso 1

PROCESO	Tiempo 1 (Minutos)	Tiempo 2 (Minutos)	Tiempo 3 (Minutos)	Promedio (Minutos)	Área encargada
Configuración de OLT	30 min	35 min	33 min	33 min	Administrador

Como resultado del proceso de la guía, se obtiene el enlace del servicio SmartOLT con la OLT alojada en la red interna de CayambeVision S.A., en la Figura 118 se puede evidenciar el estado de conexión de la OLT con la cual se confirma que se tiene una conexión y es posible el envío de comandos a través de la plataforma de SmartOLT.

Figura 118

Proceso 1: Configuración OLT

PROCESO 2: Ingreso de Clientes (ONU/ONT)

El ingreso de clientes una vez implementado el servicio de SmartOLT, se lo realiza de manera remota mediante un equipo conectado hacia el internet, esto significa la reducción notoria en los tiempos de ejecución tomando como tiempo promedio 5 minutos, gracias a la reducción en

la interacción de las áreas que participan para este proceso. En la Tabla 25 se visualiza la toma de tiempos de ejecución para esta actividad. El área técnica es la encargada de llevar a cabo el procedimiento en base a la guía técnica descrita en el ANEXO C2.

Tabla 25

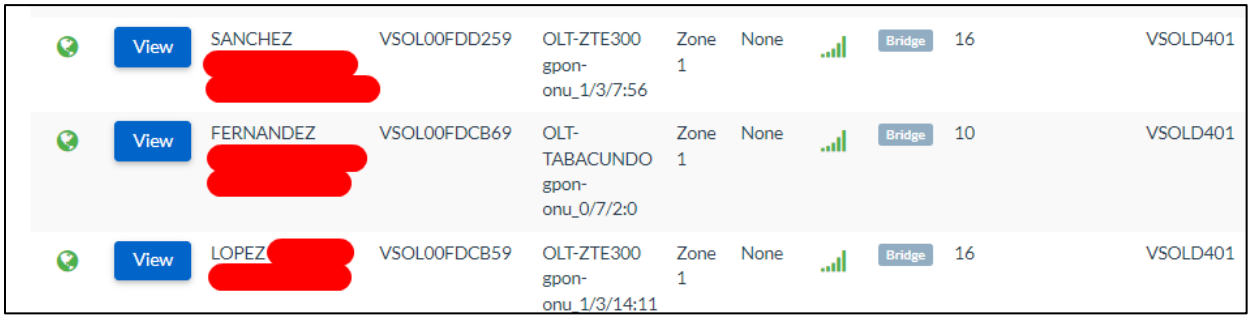
Tiempo de respuesta actual Proceso 2

PROCESO	Tiempo 1 (Minutos)	Tiempo 2 (Minutos)	Tiempo 3 (Minutos)	Promedio (Minutos)	Área encargada
Ingreso de Clientes ONU/ONT	4 min	6 min	5 min	5 min	Técnicos

En el servicio de SmartOLT se puede verificar el ingreso de los clientes mostrados en la Figura 119, los clientes ingresados se los puede visualizar en el menú *Configured* en donde se en listan todas las autorizaciones de ONU/ONT llevadas a cabo. Los equipos cliente se identifican a través de los datos validados como: modelo, vlan, interfaz y plan asignado para cada una.

Figura 119

Proceso 2: Ingreso de Clientes (ONU/ONT)



PROCESO 3: Comandos de Verificación de estado

La verificación de estado de una ONU/ONT cliente se la realiza en el sistema SmartOLT, ingresando al perfil del cliente y obteniendo el estado de conexión, de esta manera se puede observar la información detallada, la cual permite tomar decisiones al área de Oficina al momento de realizar una consulta por parte del cliente, la acción presenta un tiempo de respuesta de 3 a 4 minutos aproximadamente para cada consulta como se muestra en la Tabla 26, logrando así diagnosticar de manera rápida a la ONU/ONT y en el caso de presentar un daño permite informar un tiempo de solución al cliente. Este proceso de verificación de estado del cliente se lo coloca en el ANEXO C3 en donde ordena paso a paso las acciones que se deben ejecutar por parte de Oficina.

Tabla 26

Tiempo de respuesta actual Proceso 3

PROCESO	Tiempo 1 (Minutos)	Tiempo 2 (Minutos)	Tiempo 3 (Minutos)	Promedio (Minutos)	Área encargada
Verificación de estado del cliente	4 min	3 min	4 min	3 min	Oficina

Como resultado de la ejecución del proceso para la verificación del estado del cliente se obtiene la Figura 120, en donde se muestra inicialmente el estado del cliente permitiendo identificar mediante iconos cuál es su situación actual, los distintos estados que pueden presentarse son:  Equipo en línea,  Equipo Apagado,  Equipo desenganchado.

Figura 120

Proceso 3: Comandos de Verificación de estado

4.1.5.2. Resultados de ejecución SmartISP

En el proceso adjunto en el ANEXO C4 se lleva a cabo el ingreso de clientes al sistema SmartISP, en donde, se registra: nombre del cliente, cedula, teléfono, dirección, plan contratado. Esta información ingresada posteriormente nos servirá como base para la aplicación de otros procesos como: pago de servicios, generación de tickets de soporte y la suspensión automática del servicio, es por esto que es esencial el correcto ingreso de los datos de cada uno de estos. Cabe recalcar que anteriormente CayambeVision S.A. no llevaba un documento con información de las IPs, perdiendo así información valiosa de los usuarios clientes.

Una vez obtenida toda la información se procede a crear el perfil para cada uno de los clientes siguiendo la guía adjunta del ANEXO C4. Finalizado el proceso se obtiene como resultado la Figura 121 en donde se muestra el listado de clientes ingresados y su información acorde a cada uno de ellos, de esta manera se puede identificar: nombre, IP asociada al cliente, balance (dinero por cobrar), estado, fecha próxima de corte de servicio, plan contratado.

Figura 121

Proceso 4: Ingreso de Clientes

Name	I P	Balance	Estado	Corte Servicio	Plan
AGUIRRE [redacted]	172.20.15.187	-40.00	En linea	2023-02-11	Plan_INT_TV_Premium1
CABASCANGO [redacted]	172.18.15.124	-22.40	En linea	2023-02-11	Plan_Basico_100Mbps
GONZALEZ [redacted]	172.16.15.248	-22.40	En linea	2023-02-11	Plan_Basico_100Mbps_1

El ingreso de los clientes al sistema SmartISP está a cargo del área de Administración de la red, la cual ingresa los datos correspondientes al perfil del cliente, esta acción de ingreso registra un tiempo promedio de 4 minutos por cada cliente. De esta manera se obtiene la Tabla 27 en la cual se refleja cada uno de los tiempos tomados.

Tabla 27

Tiempo de respuesta actual Proceso 4

PROCESO	Tiempo 1 (Minutos)	Tiempo 2 (Minutos)	Tiempo 3 (Minutos)	Promedio (Minutos)	Área encargada
Ingreso de Clientes	7 min	6 min	7 min	7 min	Oficina

PROCESO 5: Pago de Servicio

El pago de servicio por parte de los usuarios clientes una vez implementado SmartISP se valida de manera inmediata en el sistema, en el ANEXO C5 se evidencia el procedimiento llevado

a cabo por el área de Cobradores y Oficina al momento de ingresar un nuevo pago. Estos procesos son ejecutados de manera remota gracias a la disponibilidad del servicio alojado en la Nube, lo cual facilita al área de cobranza el ingreso de un pago desde el domicilio de un cliente a través de su teléfono móvil. Una ventaja adicional es la obtención del recibo del pago de manera digital, lo cual reduce el tiempo promedio empleado para cada una de estas acciones. En la Tabla 26 se evidencia lo mencionado anteriormente.

Tabla 28

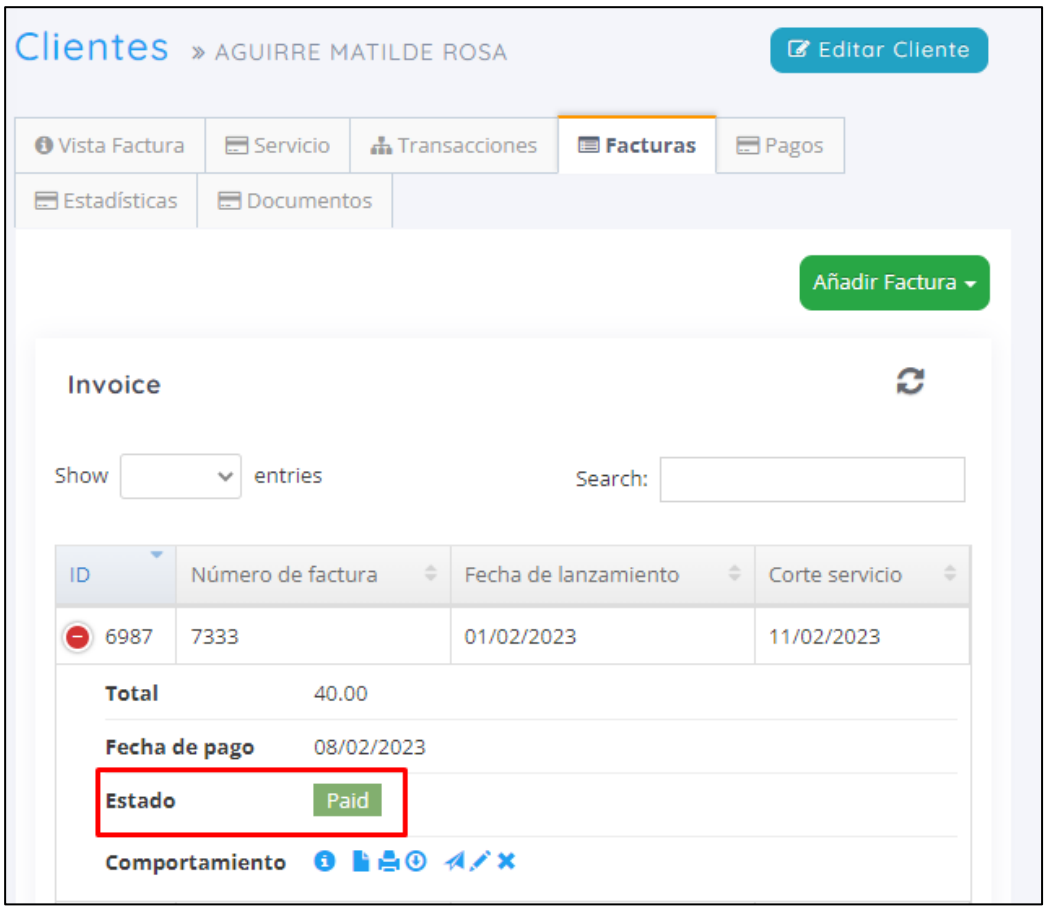
Tiempo de respuesta actual - Proceso 5

PROCESO	**Tiempo 1 (Minutos)**	**Tiempo 2 (Minutos)**	**Tiempo 3 (Minutos)**	**Promedio (Minutos)**	**Área encargada**
Pago de Servicio	4 min	3 min	4 min	3 min	Oficina

Producto de la ejecución del proceso se obtiene como resultado en el servicio SmartISP la Figura 122 en donde se muestra el estado de pago de un cliente basado en las facturas pendientes por cobrar. Una vez ingresado el pago del cliente se lo valida automáticamente en el sistema y se descarta de la función de cortes automática que presenta el servicio SmartISP.

Figura 122

Proceso 5: Pago de Servicio



PROCESO 6: Generación de Tickets de Soporte

El proceso introducido para la generación de Tickets se lo aplica en el servicio de SmartISP, con el cual se puede verificar el estado de cumplimiento de soportes por parte del área técnica de manera remota, mediante esta actividad se puede tener una mejor organización al momento de registrar nuevos soportes por parte del área de Oficina, mejorando así el rendimiento del proceso y evitando el sobre cargo de actividades a los técnicos debido al desconocimiento del desarrollo de su hoja de trabajo. El conjunto de pasos para ejecutar la generación de Tickets se lo desarrolla en el ANEXO C6. En este caso el tiempo de demora para la asignación de tickets de soporte reduce

en un mínimo como se muestra en la Tabla 29, su aporte principal es el de llevar un control del trabajo diario de los Técnicos.

Tabla 29

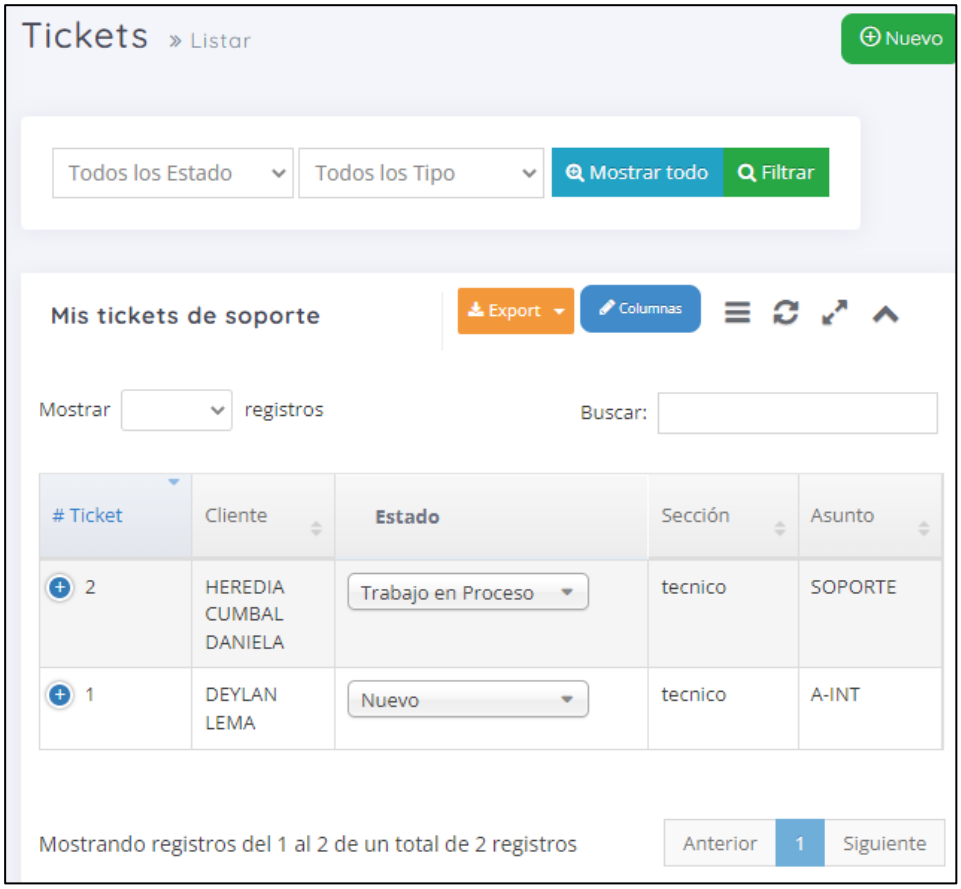
Proceso 6: Generación de Tickets de Soporte

PROCESO	**Tiempo 1 (Minutos)**	**Tiempo 2 (Minutos)**	**Tiempo 3 (Minutos)**	**Promedio (Minutos)**	**Área encargada**
Generación de Tickets de Soporte	14 min	13 min	12 min	13 min	Oficina

El resultado de la ejecución de este proceso se lo evidencia en la Figura 123, en donde se muestra el listado de los Tickets ingresados con la información de: nombre de cliente, estado (nuevo, trabajo resuelto, esperando al cliente, trabajo en proceso), sección (área de destino), asunto (descripción del soporte). Cada uno de los soportes ingresados se refleja en el perfil del técnico al momento de revisar los Tickets en el sistema SmartISP.

Figura 123

Proceso 6: Generación de Tickets de Soporte



PROCESO 7: Suspensión de servicio

El proceso de suspensión de servicio de un cliente por falta de pago es el que mejor rendimiento presenta después de la asociación con SmartISP, esto debido a que los cortes se los realiza de manera programada. En donde, el sistema verifica a aquellos clientes que no han sido registrados sus pagos y procede a cortarlos en una fecha establecida acorde a la configuración que la empresa da como fecha límite de pago. La configuración de fecha límite de pago se la realiza en el apartado 4.4.2.1. al realizar el ingreso del cliente al sistema.

Al mencionar que el proceso es programado, se hace referencia a que ya no es necesaria la intervención humana para llevarlo a cabo el corte de servicio por falta de pago, eliminando así el tiempo destinado para esta actividad y por ende reduce los costos producidos por el sobre cargo de horas de trabajo que anteriormente significaba para cada una de las áreas (Oficina, Cobranza y Administración), lo cual causaba una inversión adicional para la empresa al momento de pagar las horas extras invertidas por el personal de CayambeVision S.A. En la Tabla 30 se puede observar los tiempos obtenidos para este proceso.

Tabla 30

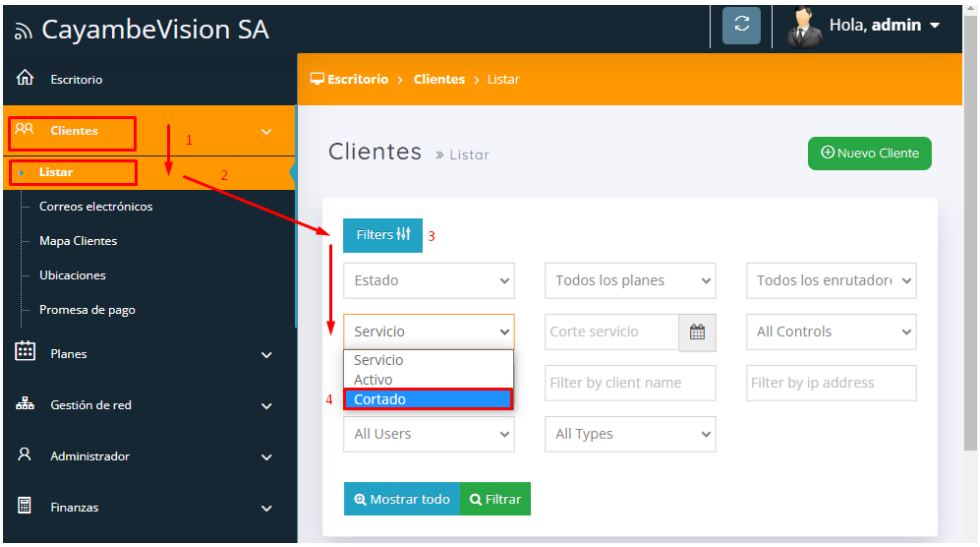
Proceso 7: Suspensión de Servicio

PROCESO	Tiempo 1 (Minutos)	Tiempo 2 (Minutos)	Tiempo 3 (Minutos)	Promedio (Minutos)	Área encargada
Suspensión del servicio	0min	0min	0min	0min	----------

Una vez concluido el corte del servicio por falta de pago se obtiene un listado de clientes, los cuales se los puede filtrar ingresando a SmartISP en el menú *Clientes→Listar→Filtros→Servicio→Cortado,* proceso indicado en la Figura 124. De esta manera se puede conocer el número de clientes que han sido parte del proceso de corte.

Figura 124

Proceso 7: Suspensión de servicio



Como resultado del filtrado de cortes se obtiene la Figura 125 en donde se muestra una lista de clientes los cuales se los puede identificar como “cortados”. La información que se refleja en cada uno de los clientes es: IP, balance (saldo por cobrar), corte de servicio (fecha de ejecución del corte) y servicio (estado cortado). De esta manera al momento de realizar una búsqueda por nombre del cliente se podrá identificar de manera rápida si un cliente posee mora o no.

Figura 125

Proceso 7: Listado de clientes

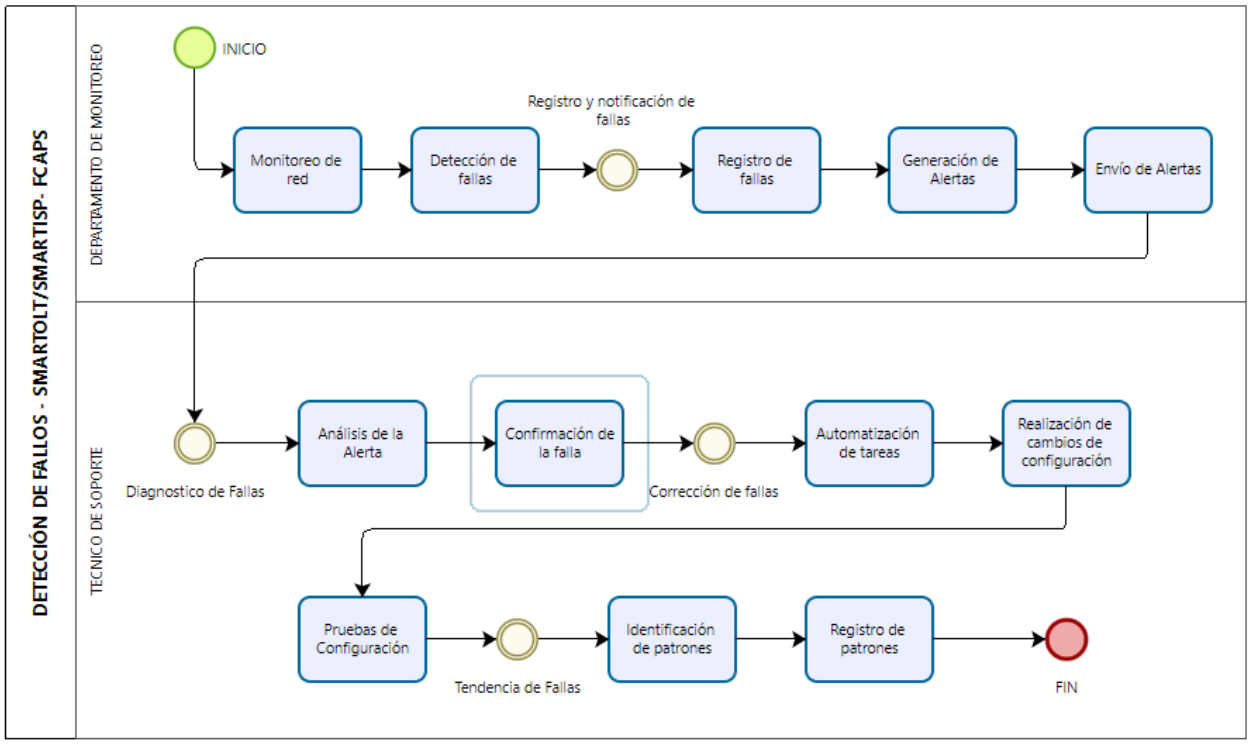
Name	IP	Balance	Corte Servicio	Servicio
PILCO PILCO [redacted]	172.16.14.244	-44.80	2022-12-11	Cortado
ALMEIDA [redacted]	172.22.15.93	-44.80	2022-12-11	Cortado
LECHON [redacted]	20.0.0.165	-44.80	2022-12-11	Cortado

4.2. GESTIÓN DE FALLOS

Los servicios de SmartOLT y SmartISP integra un conjunto de herramientas de gestión de fallos que ayudan a los operadores de red de CayambeVision S.A. a mantener el funcionamiento de la red en niveles óptimos. Los procesos necesarios para llevar a cabo un análisis adecuado de los fallos presentes en la red de backbone de la empresa se detallan en la **Figura *126***. En esta figura se muestran cada una de las actividades que se basan en la búsqueda, detección, corrección, resolución y documentación de fallos.

Figura 126

Proceso para la gestión de fallos



4.2.1. Monitoreo de la red

El monitoreo de red es un proceso el cual consiste en la observación y medición continua de los dispositivos clientes con el objetivo de detectar posibles problemas previniendo problemas futuros y garantizando el rendimiento y la calidad del servicio. El monitoreo dentro de la red de

CayambeVision S.A. se lo puede realizar utilizando las herramientas integradas en SmartOLT y SmartISP, en donde, se puede evidenciar periódicamente el estado de la red.

En la **Figura *127*** se muestra la forma en la cual SmartOLT, permite observar el estado de conexión del equipo del cliente (ONU/ONT). Como resultado del proceso de verificación del estado del cliente, se pueden identificar mediante iconos cuál es su situación actual. Los distintos estados que pueden presentarse son: Equipo en línea, Equipo Apagado, Equipo desenganchado.

Figura 127

SmartOLT Monitoreo – Gestión de Fallos

Mientras que para la herramienta de SmarISP se puede realizar la verificación del estado del cliente realizando la lectura de las dos posibles (En línea o Desconectado). De esta manera se puede tener un breve análisis para la detección de fallos dentro de la red de CayambeVision S.A.

Figura 128

SmartISP Monitoreo – Gestión de Fallos

4.2.2. Registro y notificación de fallas

El registro de fallas es importante para llevar un historial de los problemas que han ocurrido en la red, lo que permite a los administradores de la red identificar patrones y tendencias, y tomar

medidas para prevenir futuras fallas, en la **Tabla *31*** se puede evidenciar el proceso de registro de incidentes para la red de CayambeVision S.A. Posterior a esto una vez identificado se procede a realizar la notificación oportuna al equipo de soporte o a los usuarios finales acerca de una falla en la red o en el equipo final del cliente. Esto se puede hacer mediante alertas en el sistema de monitoreo de red, mensajes de correo electrónico, mensajes de texto, llamadas telefónicas u otras formas de comunicación.

Tabla 31

Registro y notificación - Gesiton de Fallos

Número de incidente	Fecha de reporte	Descripción del incidente	Impacto	Prioridad	Estado actual	Fecha de resolución
INC001	01/05/2023	Cliente sin servicio	Alta	Alta	En curso	-
INC002	02/05/2023	Servicio inestable	Media	Alta	Asignado	03/05/2023

4.2.3. Diagnóstico de fallas

El diagnóstico de fallas es un proceso que incorpora a la red de CayambeVision con el fin de identificar y resolver los problemas en la red. El objetivo principal del diagnóstico de fallas es determinar la causa raíz de un problema y proporcionar soluciones para corregirlo. De este modo se proporciona la **Tabla *32*** en la cual se almacena toda la información para realizar un correcto diagnóstico de las fallas a partir de la identificación de un incidente dentro de la red.

Tabla 32

Diagnóstico de fallas - Gestion de Fallos

Número de Incidente	Fecha de Reporte	Descripción del Problema	Análisis de la Causa Raíz	Solución Propuesta	Fecha de Implementación de la Solución
INC001	01/05/2023	Cliente sin internet	Equipo apagado	Verificar fuente de toma eléctrica	02/05/2023
INC002	02/05/2023	Servicio inestable	Potencia de recepción Alta	Verificar atenuación en fibra cliente	03/05/2023

4.2.4. Corrección de fallas

Una vez que se ha identificado el problema y su posible causa raíz, se propone la ejecución de una solución adecuada para el incidente detectado. De esta manera, la Corrección de fallos se encarga de tomar las medidas necesarias para solucionar los problemas registrados en la red de CayambeVision S.A.

Las actividades necesarias para la Corrección de fallos dependen del tipo de problema que se necesite resolver. En general, para realizar una corrección efectiva en la red de clientes se establecen los siguientes pasos:

- ✓ Análisis de la causa raíz: Una vez identificado el problema, se analiza su posible causa raíz para establecer las medidas correctivas necesarias.
- ✓ Ejecución de la solución: Se propone y ejecuta la solución adecuada para el incidente detectado. Esta solución puede implicar cambios en la configuración de la red, la reparación o reemplazo de dispositivos defectuosos, entre otros.

- ✓ Verificación de la solución: Después de ejecutar la solución, se realiza una verificación para asegurarse de que el problema se ha resuelto correctamente. Esto puede involucrar la realización de pruebas de diagnóstico adicionales y la revisión de los registros de la red.
- ✓ Actualización de la documentación: Finalmente, se actualiza la documentación de la red para incluir detalles sobre la falla, su causa raíz y la solución implementada. Esto ayuda a mantener un historial de las fallas y soluciones en la red para futuras referencias.

4.2.5. Tendencia de fallas

Una vez realizado el monitoreo, registro, diagnóstico y corrección de las fallas, el siguiente paso el almacenamiento de todos los procesos para así permitir identificar patrones de comportamiento en la red, mediante la cual se puedan tomar medidas preventivas para evitar futuras fallas y mejorar así la calidad del servicio. Siendo así se crea la **Tabla *33*** con los distintos reportes que puedan ser ingresados por parte de los clientes de CayambeVision S.A. y se las clasifica acorde a la descripción del problema y la frecuencia que suceden a lo largo del tiempo estimado para el estudio.

Tabla 33

Tendencia de fallas - Gestion de Fallas

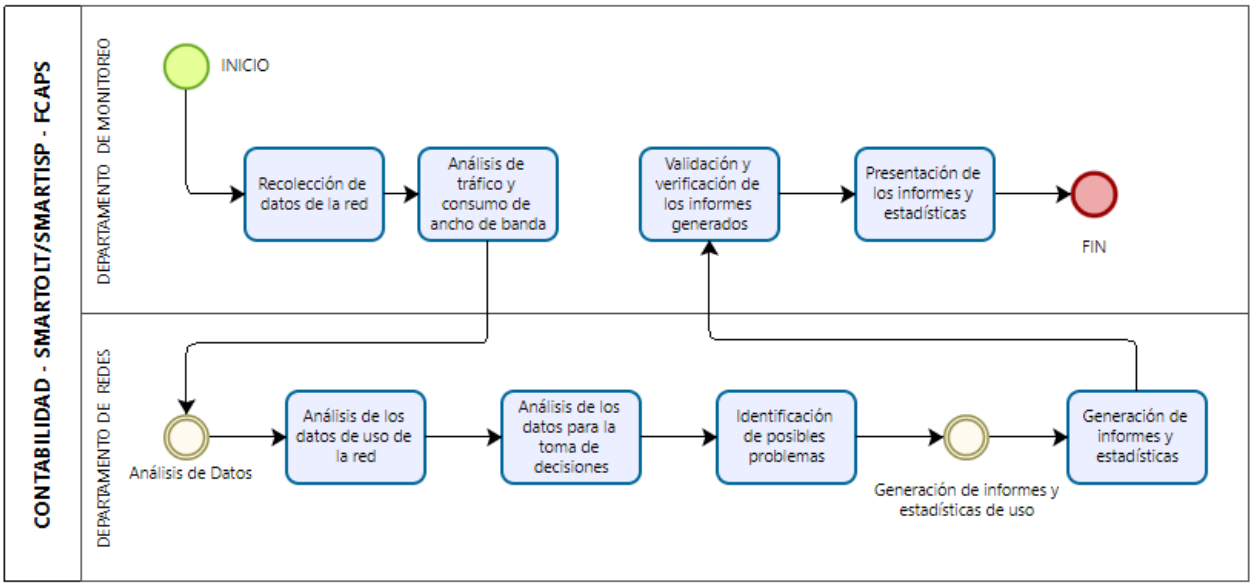
Número de Tendencia	Fecha de Reporte	Descripción del Problema	Frecuencia del Problema	Impacto	Acciones Propuestas
TEN001	01/05/2023	Cliente sin servicio	5 veces en el último mes	Alto	Verificar equipos encendidos, verificar corte de servicio
TEN002	02/05/2023	Servicio inestable	2 veces en la última semana	Medio	Revisar potencia, revisar configuraciones router

4.3. GESTIÓN DE CONTABILIDAD

La contabilidad de la red se fundamenta en el control y registro del ancho de banda utilizado en la red. En este contexto, los sistemas SmartOLT y SmartISP integrados pueden representar los datos de consumo en gráficos para facilitar el análisis y la toma de decisiones acordes a las necesidades de la empresa. En la **Figura 129** se detallan las actividades que conforman la contabilidad de la red en la empresa.

Figura 129

Proceso para la gestión de la Contabilidad

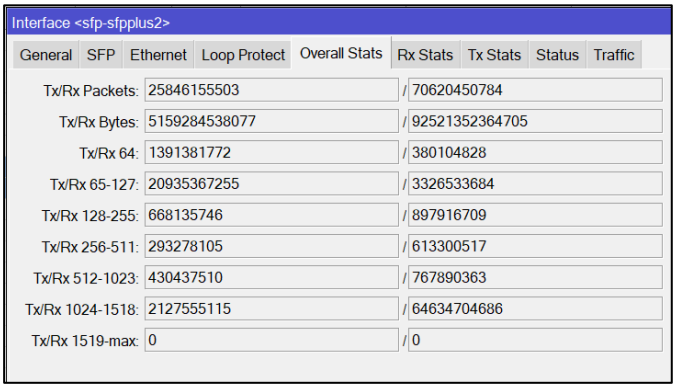


4.3.1. Recopilación de datos

La recopilación de datos en la red de la empresa se la realiza mediante la lectura del tránsito de paquetes que viajan mediante la interfaz del equipo de borde Mikrotik CCR-1072, el cual alberga toda la navegación hacia el internet. De esta manera se tiene un estimado de la cantidad de datos que están cruzando por la red de los clientes, en este caso en la **Figura *130*** se detallan las estadísticas generales del envío y recepción de paquetes.

Figura 130

Recopilación de datos – Gestión de Contabilidad



4.3.2. Análisis de Datos

Después de recopilar los datos, el siguiente paso es representarlos de manera visual. Para esto, se utilizan las herramientas SmartOLT y SmartISP, que permiten verificar el tráfico de paquetes en la red de forma gráfica. Al representar los datos en gráficos, se simplifica el análisis de la información, lo que facilita la toma de decisiones para los responsables de la red. En la **Figura *131*** se muestra la cantidad de ancho de banda que atraviesa la interfaz del equipo CCR-1072 utilizando SmartISP. Además, en la **Figura *132*** mediante SmartOLT se representa de manera gráfica el ancho de banda utilizado en la interfaz de la OLT.

Figura 131

Analisis de datos de red – Gestión de la contabilidad

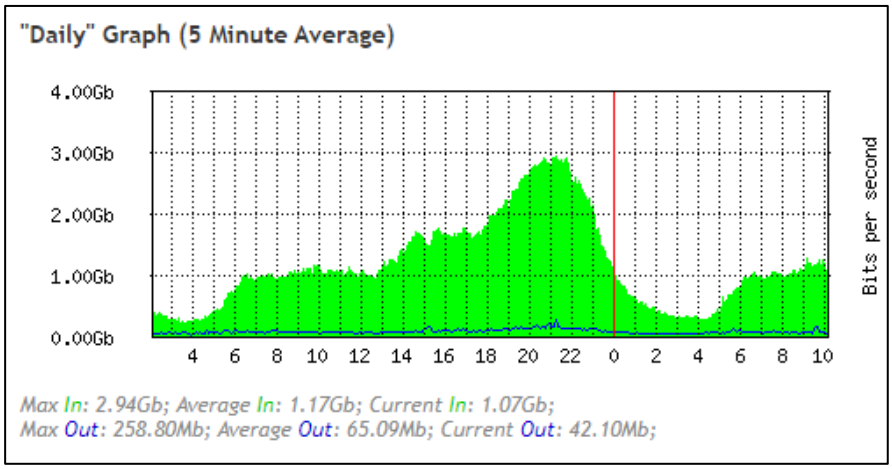
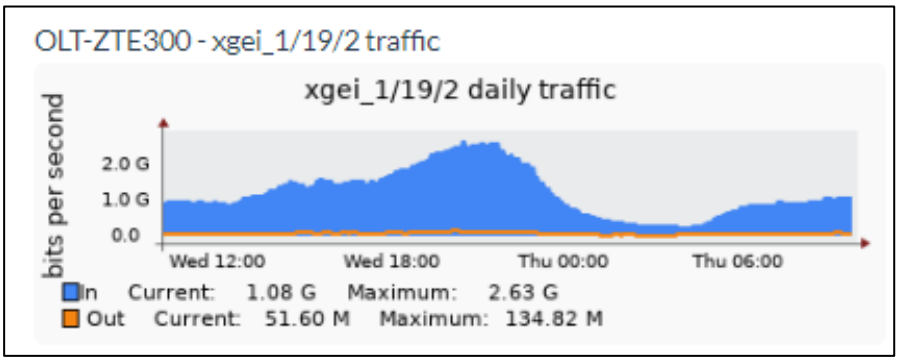


Figura 132

Análisis de datos de red SmartOLT – Gestión de la contabilidad



4.3.3. Generación de informes y estadísticas

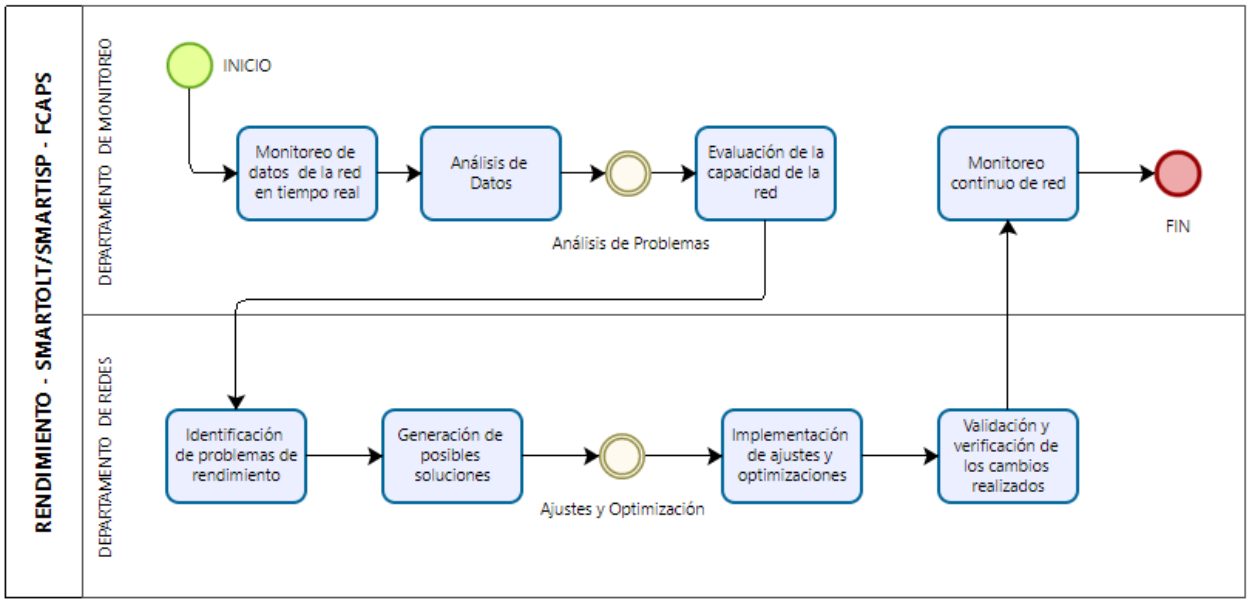
El último paso del proceso consiste en elaborar informes que sinteticen los resultados de la recolección y el análisis de los datos. Estos informes son de gran utilidad para los operadores de la red, ya que les permiten conocer el estado y el rendimiento de los recursos de la red. Entre la información que se puede incluir en los informes se encuentran las alertas generadas, los datos anómalos detectados y las notificaciones enviadas durante el estudio de la contabilidad basada en la red de la empresa.

4.4. GESTIÓN DE RENDIMIENTO

Para realizar el análisis del rendimiento de la red en la empresa CayambeVision S.A., el departamento de redes y monitoreo se encarga de analizar problemas, identificarlos y crear soluciones para optimizar la red. El objetivo es garantizar la disponibilidad y el desempeño de los servicios integrados, así como minimizar el tiempo medio de reparación para evitar caídas del sistema que puedan afectar a los empleados y clientes. En la **Figura *133*** se muestra el proceso iniciando desde el monitoreo de los datos que se obtienen en la red hasta finalizarlo en ajustes que permitan la optimización de los servicios. El rendimiento de la red de una empresa depende del estado en el que se encuentre el core de borde. Por lo tanto, el análisis se enfoca en los datos que representan la salud del equipo.

Figura 133

Proceso para la gestión de rendimiento

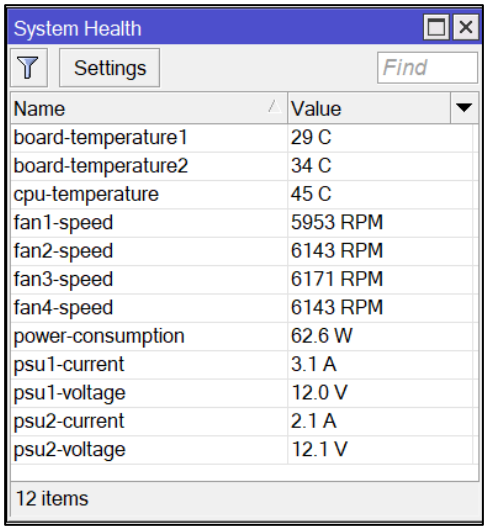


4.4.1. Monitoreo de datos de equipo

Para realizar el análisis del monitoreo de los equipos de la red, se inicia recopilando los datos que presentan los equipos encargados de enrutar todo el tráfico hacia la red interna como hacia el internet, de esta manera se representa en la **Figura *134***, el estado de salud del sistema del equipo CCR-1072 el cual se encarga de procesar todos los paquetes y enrutarlos, de esta manera se puede apreciar datos como temperatura, velocidad de ventiladores, el voltaje de consumo. Lo cual permite verificar que el área de trabajo del equipo este en óptimas condiciones al momento de estar en funcionamiento.

Figura 134

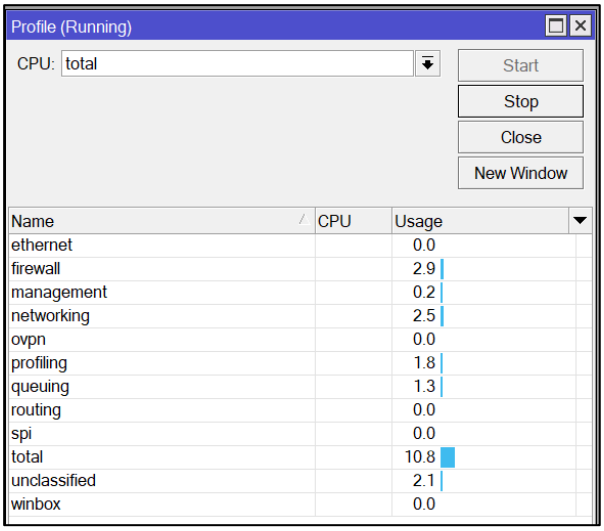
Estado de salud equipo de borde – Gestión de Rendimiento



Además, se analizan los datos del CPU que están siendo utilizados para así verificar las funciones que esta cumpliendo el equipo de borde y si en algun caso, estas funciones estan haciendo un uso elevado del CPU puede representar problemas en la red. Entre estos problemas pueden estar los mas frecuentes los cuales son: perdida de paquetes, baja velocidad de transito de paquetes, reinicio forzado del equipo, entre otros. En la **Figura *135*** se representa la manera de tomar los datos en equipo de Borde.

Figura 135

Monitoreo de datos – Gestión de Rendimiento



4.4.2. Análisis de problemas

Una vez que se han analizado los datos obtenidos por los equipos para identificar los problemas en la red, se procede a registrarlos en una tabla designada (**Tabla *34***), donde se almacenan las descripciones de los posibles problemas asociados con un evento específico en la red. A continuación, se genera un problema para cada uno de estos, asignando una acción que pueda solucionar el inconveniente causado. De esta manera, se puede llevar un registro organizado de los problemas identificados y las soluciones correspondientes para mantener un rendimiento óptimo en la red.

Tabla 34

Análisis de Problemas - Rendimiento

Número de problema	Descripción del problema	Fecha de reporte	Fecha de resolución	Causa raíz	Acciones tomadas
REN001	Pérdida de conexión a internet	05/01/2023	05/02/2023	Problema en el proveedor de servicios de internet	Cambio de proveedor de servicios de internet
REN002	Baja velocidad de internet	05/05/2023	05/06/2023	Sobrecarga en el enrutador de la red	Actualización del enrutador de la red

4.4.3. Ajustes y Optimización

En esta etapa, se llevan a cabo las soluciones desarrolladas para abordar los problemas de rendimiento identificados en el ítem anterior (análisis de problemas). Esto puede implicar cambios en la configuración de la red o la adición de nuevos dispositivos. Para facilitar este proceso, se utiliza una tabla designada (**Tabla *35***) que corresponde a la ejecución de soluciones a partir de un problema identificado en la red y se asigna una causa raíz que lo provocó. De esta manera, se logra optimizar la gestión de manera más eficiente gracias al almacenamiento de información sobre los eventos que pueden afectar el servicio. Esta tabla ayuda a mantener un registro organizado de las soluciones implementadas y su efectividad en la resolución de problemas de rendimiento.

Tabla 35

Ajustes y Optimización de la red - Rendimiento

Número de ajuste	Descripción del ajuste	Fecha de implementación	Resultados	Responsable
AJU001	Actualización del firmware del enrutador de la red	05/03/2023	Mejora en la velocidad de la red	Departamento de Redes
AJU002	Reconfiguración de la red para optimizar el tráfico	05/25/2023	Mejora en la velocidad de la red y reducción en la congestión	Departamento de Redes

4.4.4. Validación y Documentación

Para finalizar, se realiza una verificación y validación con el objetivo de asegurarse que las soluciones implementadas resuelvan los problemas de rendimiento identificados y se alcancen los objetivos establecidos en las etapas anteriores. La documentación de las soluciones obtenidas es fundamental para mejorar la gestión de la red y asegurar que los problemas se lleven de manera efectiva en el futuro.

La documentación debe incluir información detallada sobre los procesos y prácticas utilizados en esta etapa de gestión. Esto puede incluir cambios en la configuración de la red, el ingreso de nuevos dispositivos a la red, la implementación de nuevas políticas o procedimientos, entre otros aspectos. La documentación es esencial para asegurar y garantizar que se mantengan registros precisos y actualizados para futuras referencias y mejoras en la gestión de la red.

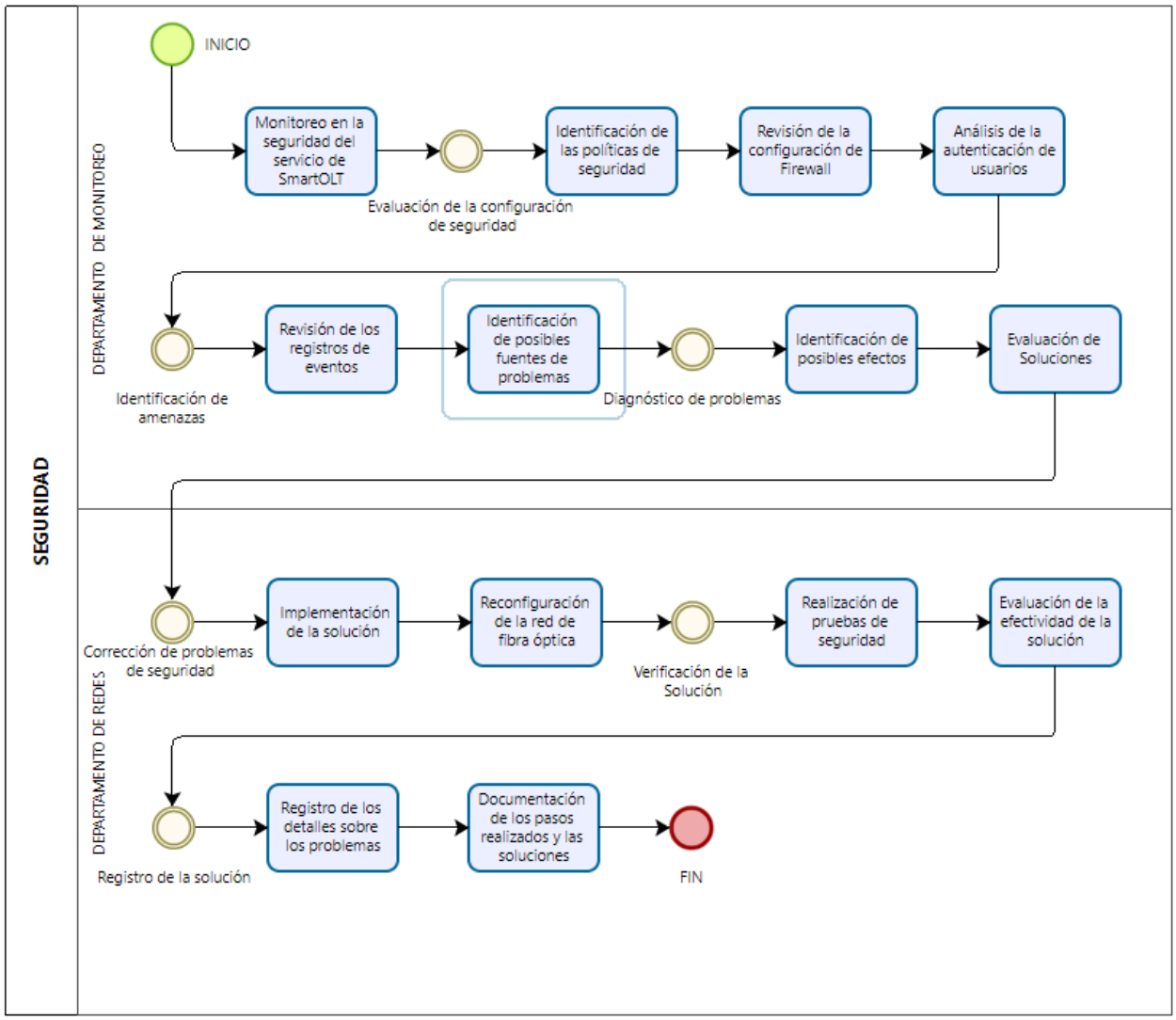
4.5. GESTIÓN DE SEGURIDAD

La gestión de la seguridad en la red de CayambeVision S.A. se basa en los servicios que han sido implementados para garantizar la seguridad de la información y los sistemas. Esta capa se enfoca en prevenir, detectar y responder a posibles amenazas y vulnerabilidades de seguridad. Con este fin, se ha generado un diagrama que representa la correcta gestión de la seguridad, de acuerdo con las herramientas que poseen los servicios de SmartOLT y SmartISP. Este diagrama, mostrado en la **Figura *136***, permite visualizar de manera clara y concisa la estructura y funcionamiento de las medidas de seguridad implementadas en la red.

La gestión de seguridad se centra en el monitoreo, evaluación de los riesgos de seguridad, identificación de amenazas, diagnóstico de problemas, corrección de problemas, la verificación de soluciones y documentación de las soluciones planteadas. La implementación de herramientas como firewalls, sistemas de detección de intrusiones y análisis de registros, permite detectar y mitigar posibles amenazas de seguridad.

Figura 136

Proceso para la gestión de la seguridad



4.5.1. Monitoreo de actividad

El monitoreo de actividad es una práctica fundamental en la gestión de la seguridad de la red de CayambeVision S.A. Consiste en analizar los registros de actividad que dejan los usuarios y dispositivos que acceden a los servicios implementados, los cuales se almacenan en las herramientas de registro (Log) que poseen SmartOLT y SmartISP. De esta manera, se puede realizar una prevención sobre las acciones que han sido realizadas al momento de manejar estos servicios.

En la **Figura *137***, perteneciente al servicio de SmartOLT, se puede observar la detección de actividad, donde se registra cada una de las acciones que han sido realizadas por un usuario en particular que presenta atributos que permiten el ingreso de nueva información en la OLT. Este registro contiene información detallada, como la acción realizada, el nombre de la OLT, el equipo cliente (ONU) involucrado, el usuario responsable, la dirección IP correspondiente y la fecha de ingreso de los cambios. Gracias a esta herramienta de monitoreo, es posible identificar y analizar la actividad realizada por los usuarios en la red, y tomar medidas preventivas ante posibles acciones maliciosas.

Figura 137

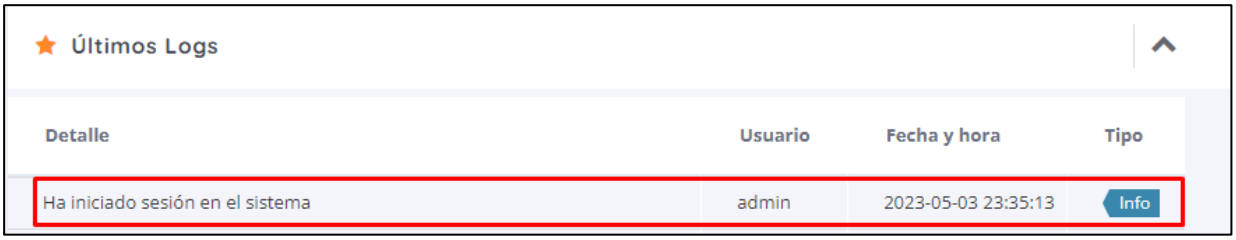
Monitoreo de Actividad SmartOLT – Gestión de la Seguridad

Action	OLT	ONU	User	IP address	Date
ONU D0126AA2D23F gpon-onu_1/5/12:10 authorized	OLT-ZTE300	gpon-onu_1/5/12:10	lem[redacted]	45.2[redacted]	03-May-2023 16:51
ONU D0126AA2D24F gpon-onu_1/8/5:2 authorized	OLT-ZTE300	gpon-onu_1/8/5:2	lem[redacted]	45.2[redacted]	03-May-2023 16:36

Para el servicio de SmartISP en el apartado de Logs mostrado en la **Figura *138*** se puede apreciar el almacenamiento de información de ingreso al sistema, actividad realizada, usuario, fecha, hora y el tipo de actividad que se está llevando a cabo dentro del sistema del servicio. El registro de actividad es una valiosa fuente de información para la gestión de seguridad de los servicios implementados.

Figura 138

Monitoreo de Actividad SmartISP – Gestión de la Seguridad

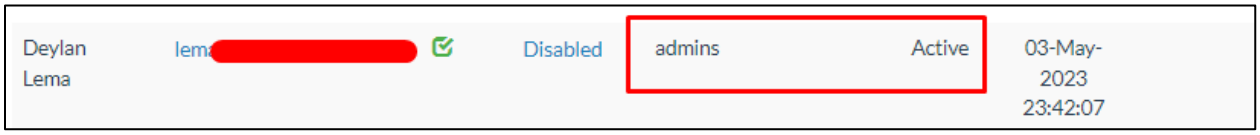


4.5.2. Evaluación de la configuración de seguridad

Para verificar la correcta configuración de seguridad en el acceso y registro de actividades en los servicios SmartOLT y SmartISP, es importante verificar los usuarios creados para el manejo de estas herramientas. En la Figura 139 se pueden validar todos los usuarios dentro de SmartOLT que tienen permisos para realizar cambios en el sistema. Cada usuario tiene características como el nombre, nombre de usuario, nivel de usuario y fecha de activación del perfil. Con esta información, se pueden tomar decisiones para prevenir riesgos y mejorar el rendimiento en la seguridad de la red.

Figura 139

Evaluación de la configuración SmartOLT – Gestión de la Seguridad



Mientras tanto, en lo que respecta a la configuración de los usuarios en el sistema SmartISP y los perfiles permitidos para su manejo, se debe acceder a la pestaña de administración. En esta sección se encuentran almacenados y validados los datos correspondientes a cada usuario, así como los perfiles que les han sido asignados. Esto puede apreciarse en la **Figura *140***.

Figura 140

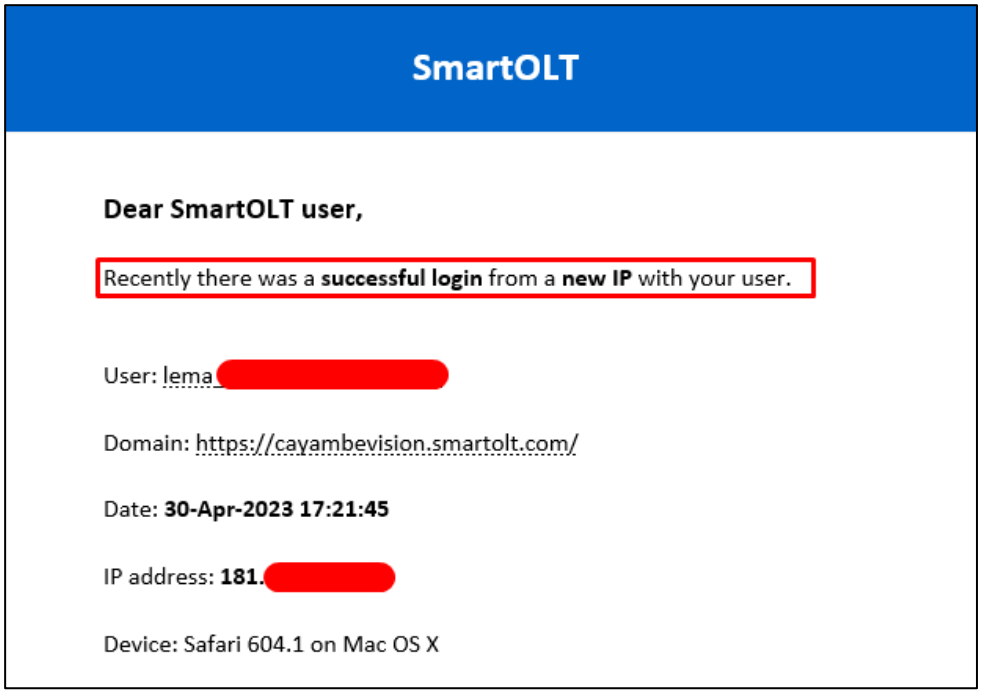
Evaluación de la configuración SmartISP – Gestión de la Seguridad

4.5.3. Identificación de amenazas

La identificación de amenazas en la capa de seguridad del modelo FCAPS es crucial para asegurar la protección de la información y los sistemas de comunicaciones. Esta tarea implica la evaluación de los riesgos asociados con posibles amenazas de seguridad y la implementación de medidas de seguridad para mitigar dichos riesgos. SmartOLT cuenta con la funcionalidad de enviar notificaciones de alerta por correo electrónico, las cuales proporcionan información sobre el acceso al sistema. Estas alertas permiten tomar medidas preventivas en caso de que se detecte un acceso no autorizado, como se muestra en la **Figura *141***. Además, gracias al registro de la dirección IP y del equipo utilizado para el acceso, es posible identificar de manera más eficiente y rápida posibles amenazas de seguridad.

Figura 141

Identificación de amenazas SmartOLT – Gestión de la Seguridad



4.5.4. Diagnóstico y Corrección de problemas

La gestión efectiva de la red requiere la identificación y diagnóstico preciso de los problemas. Esto implica la localización de la amenaza y la causa raíz, permitiendo así asignar una solución y corrección a estas vulnerabilidades relacionadas con la seguridad de la red y los sistemas en ella. Una vez identificado el problema, se establece una tarea de configuración para su resolución y se procede a realizar los cambios necesarios para mitigar los problemas de seguridad en la empresa CayambeVision S.A., específicamente en el uso de los sistemas almacenados en la nube.

4.5.5. Verificación y Registro de la Solución

Tabla 36

Verificación y registro de las soluciones – Gestión de Seguridad

Identificador del problema	Problema de seguridad	Solución implementada	Fecha de implementación	Estado de la solución
SEG001	Acceso no autorizado los servicios	Verificación de usuarios permitidos	21/05/2022	Pendiente
SEG002	Vulnerabilidad en el sistema SmartOLT	Asignación de sitios de trabajo para el uso del servicio	01/05/2022	En proceso

5. CAPITULO V – RESULTADOS

5.1. EVALUACIÓN DEL DESEMPEÑO DE LOS SERVICIOS

Una vez llevado a cabo el proceso de selección, implementación y ejecución de los servicios SmartOLT y SmartISP basados en el proceso lineal de la ISO/IEEE 29148 y el modelo FCAPS, colocando como análisis principal de la presente investigación el tiempo de ejecución de cada proceso. Se logra identificar que los tiempos de respuesta ante incidentes en la red de CayambeVision S.A. son debido a la demora en los procesos de gestión y administración. Para esto, a través de las necesidades de la empresa, conocidas por medio de entrevistas en las diferentes áreas y realizando un benchmarking competitivo de aquellas herramientas ofertadas en el mercado que puedan adaptarse a estas necesidades. Se presenta como soluciones a los servicios SmartOLT y SmartISP las cuales han sido acopladas correctamente a la red, para posteriormente ser liberadas siguiendo un proceso de las mejores prácticas de la ISO/IEEE 29148 y el modelo FCAPS, llevando respaldos y dejando guías técnicas para cada uno de los distintos "nuevos procesos" ingresados a la empresa CayambeVision S.A.

Para la búsqueda de la correcta ejecución de los procesos por parte del personal de las distintas áreas ubicadas en la empresa, se propone realizar capacitaciones en cuanto al uso y responsabilidad al momento de manejar los dos servicios. Las capacitaciones han sido realizadas con éxito, estableciendo un ambiente abierto para cualquier tipo de inquietud por parde del personal. Una vez finalizado este proceso de enseñanza se proceden a la toma de nuevos tiempos de demora para cada uno de los procedimientos. Llegando a obtener la Tabla 37, que refleja la considerable disminución de: tiempos y las áreas encargadas que participan al momento de ejecutar dichas acciones.

Tabla 37: Resumen de evaluación de desempeño

		ANTES DE LA IMPLEMENTACIÓN			DESPUÉS DE LA IMPLEMENTACIÓN		
PROCESO	**Subproceso**	**Promedio (Minutos)**	**Áreas Encargadas**	**Intervención de áreas**	**Promedio (Minutos)**	**Áreas Encargadas**	**Intervención de áreas**
Procesos en la Gestión de red	Configuración de OLT	55 min	Administrador	1	33 min	Administrador	1
	Ingreso Cliente (ONU)	10 min	Administrador Técnicos	2	5 min	Técnicos	1
	Verificación de estado	13 min	Oficina Administrador	2	3 min	Oficina	1
Procesos en la Administración de red	Ingreso de Clientes	14 min	Oficina	1	7 min	Administrador	1
	Pago de Servicio	13 min	Oficina Cobradores	2	3 min	Oficina Cobradores	2
	Generación de Tickets de Soporte	14 min	Oficina Técnicos	2	12 min	Oficina Técnicos	2
	Suspensión del servicio	11 min	Oficina Cobradores Administrador	3	0min	_____	0

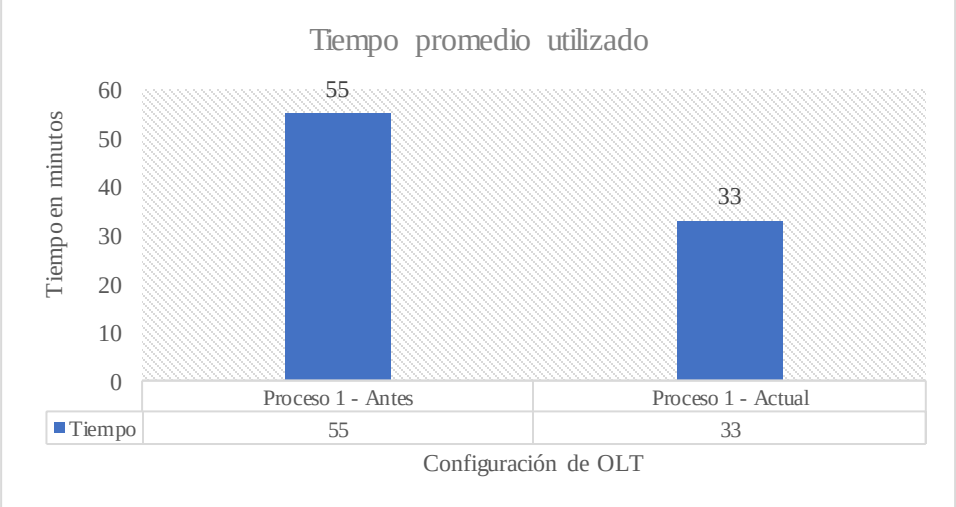
5.1.1. Análisis de desempeño por proceso

✓ Proceso 1: Configuración de OLT.

En la **Figura 142** se puede evidenciar que el tiempo promedio destinado para configuración de la OLT una vez implementado el servicio de SmartOLT reduce en 22 minutos respecto al método anterior, lo cual representa una mejora del 40% en la ejecución para este proceso. Esta reducción de tiempo se da gracias a que las actividades de configuración son desarrolladas de forma remota a través de la interfaz gráfica evitando la configuración vía consola. Las acciones para llevar a cabo esta actividad son ejecutadas por el área de Administración de la red.

Figura 142

Análisis - Proceso 1



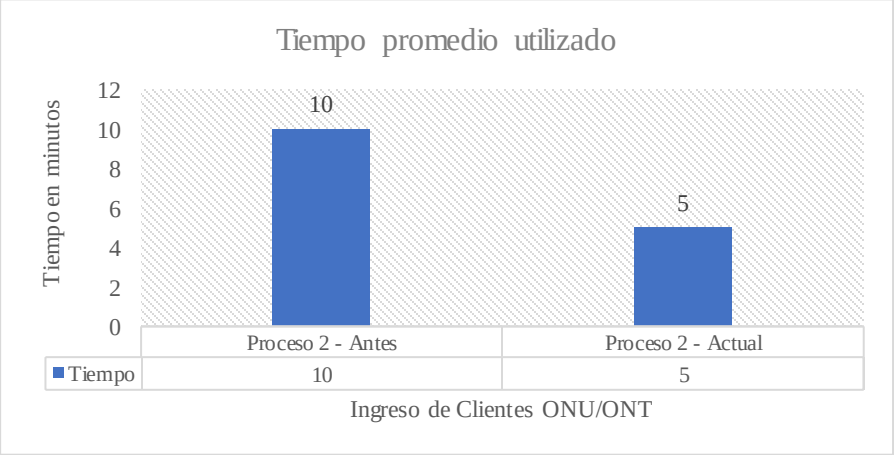
✓ Proceso 2: Ingreso de Clientes (ONU/ONT) – SmartOLT.

En el ingreso de clientes utilizando el servicio de SmartOLT se evidencia la mejora de tiempos en relación con el mecanismo anterior de hasta un 50%, esta reducción significativa se debe a que la ejecución del proceso en la actualidad únicamente depende del área técnica, lo cual

evita la descoordinación entre áreas presentada en el mecanismo anterior. La mejora de tiempos se la puede evidenciar a través del gráfico de barras presentado en la **Figura 143**.

Figura 143

Análisis - Proceso 2

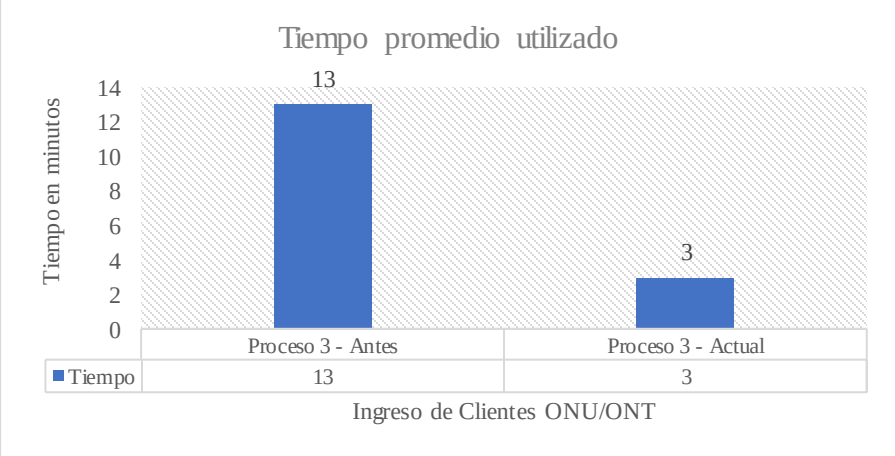


✓ Proceso 3: Verificación de estado.

La verificación de estado de la ONU/ONT del cliente debido a la implementación de SmartOLT ha pasado de ser un proceso de ingreso de comandos manuales, a ser una actividad realizada mediante una interfaz gráfica. Esto facilita la reorganización del proceso, permitiendo la ejecución por parte del área de oficina, evitando así la codependencia entre áreas y dejando libre al área de Administración de red para verificar la correcta ejecución de los distintos procesos en la empresa CayambeVision S.A. En la **Figura 144** se puede evidenciar la comparativa correspondiente a los tiempos de ejecución antes y después de implementar el servicio SmartOLT.

Figura 144

Análisis - Proceso 3

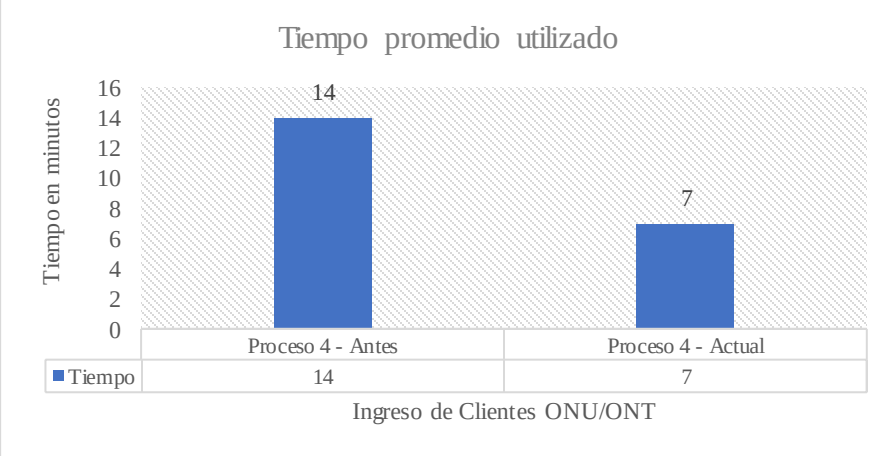


✓ Proceso 4: Ingreso de Cliente – SmartISP.

Los tiempos promedio de la **Figura 145**, muestran una diferencia de 7 minutos entre sí. Esto representa una mejora del rendimiento en un 50% en relación con el proceso anterior. El cambio principal que se ha realizado en esta actividad es la reasignación del proceso anteriormente realizado por Oficina y en la actualidad llevado a cabo por la Administración de red, este cambio se ha ejecutado debido a datos técnicos (IP del cliente) que se maneja para la creación del perfil del cliente. El objetivo de presente proceso es almacenar de mejor manera la información importante para la administración de la red.

Figura 145

Análisis - Proceso 4

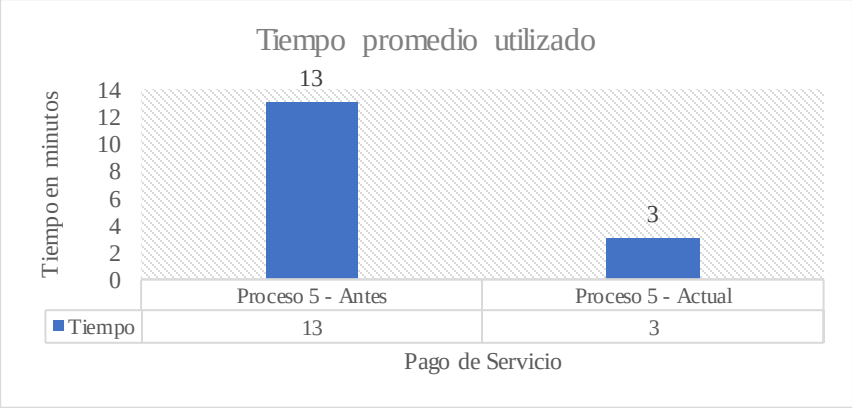


✓ Proceso 5: Pago de Servicio.

La reorganización del proceso 5 mediante el uso de la herramienta SmartISP mejora en los tiempos de respuesta tomados para su ejecución, en la **Figura 146** se puede verificar los tiempos promedios tomados para llevar a cabo el proceso antes y después de la implementación del servicio. Los tiempos actuales se reducen hasta en un 77% para el registro de pagos del servicio de internet. Este proceso al llevar su validación de manera inmediata evita inconvenientes existentes en el proceso anterior, tales como: suspensión no debida del servicio a clientes, sobre carga de trabajo e información no actualizada.

Figura 146

Análisis - Proceso 5

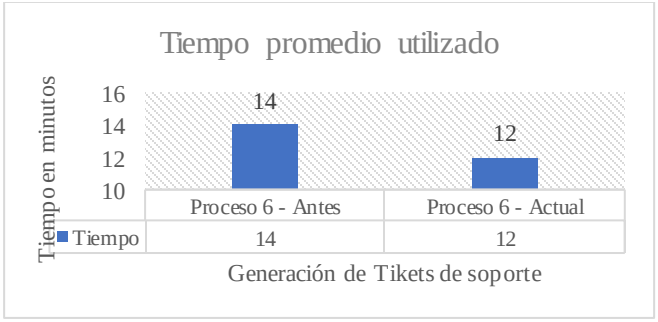


✓ Proceso 6: Generación de Tickets de Soporte.

Con la implementación de SmartISP, el proceso de generación de Tickets ha mejorado la organización y comunicación entre las áreas de oficina y técnica. La plataforma del sistema actual permite realizar un correcto seguimiento de los estados de los soportes ingresados en la hoja de los técnicos, logrando así la correcta toma de decisiones al momento de buscar ingresar un nuevo soporte. A pesar de lo mencionado anteriormente en la **Figura *147***, se observa que el rendimiento en relación con el tiempo ha mejorado únicamente un 14%, esto debido a que es un proceso extenso que inicialmente depende de la ejecución del Proceso 3.

Figura 147

Análisis - Proceso 6

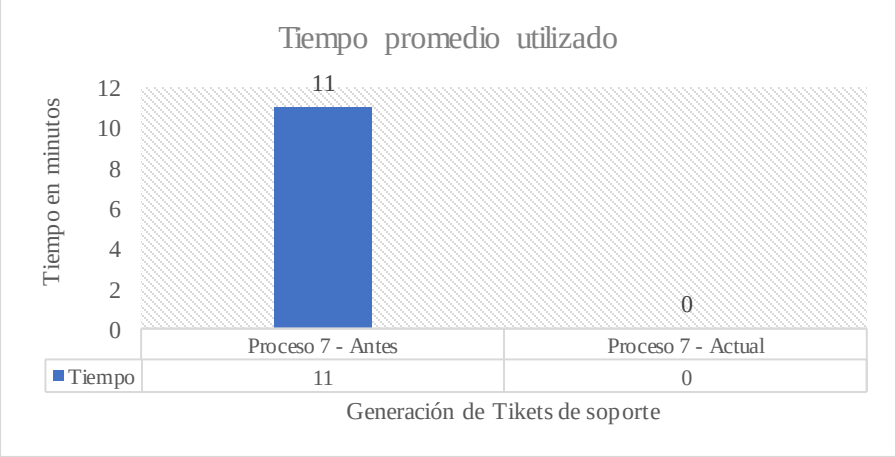


✓ Proceso 7: Suspensión del servicio.

La suspensión del servicio es el proceso que más mejoras refleja al momento de la implementación de los servicios, esto gracias a que el corte de servicio por falta de pago en la empresa CayambeVision S.A. se realiza en la actualidad de manera programada. SmartISP se encarga de identificar en la fecha de corte de servicio a los clientes que no se les ha registrado el pago y proceder a suspender el servicio. Por lo tanto, para su ejecución actual el rendimiento mejora en un 100%, debido a que no se destina tiempo para el proceso, tal como se muestra en la **Figura *148***.

Figura 148

Análisis - Proceso 7



5.1.2. Análisis de rendimiento general

Para llevar a cabo un análisis completo de la efectividad de la implementación de los servicios SmartOLT y SmartISP en CayambeVision S.A., se recopilan los tiempos obtenidos antes y después de la implementación de estos servicios. Estos tiempos se representan en gráficos de barras a continuación para poder visualizar de manera más clara la mejora en el rendimiento de la red.

Con el fin de mejorar la lectura de los datos, se agruparon todos los procesos que utilizan la herramienta SmartOLT para la gestión de la red y aquellos procesos de administración de la red destinados al uso de SmartISP. Esta agrupación permite evidenciar los resultados de la implementación de estos servicios en relación con el objetivo principal de mejorar los tiempos de respuesta ante incidentes localizados en los procesos que se llevan a cabo en CayambeVision S.A.

5.1.2.1. Rendimiento actual - Gestión de Red

En la actualidad, la gestión de la red ha mejorado en un 47,43% como se puede ver en la ***Figura 149*** en comparación con el sistema anterior, gracias a las características de SmartOLT. Esta herramienta se aloja en la nube, lo cual facilita el acceso y la gestión remota de la OLT, reduciendo así el tiempo necesario para la ejecución de los procesos asociados a la gestión de equipos de clientes finales, como ONU/ONT y OLT.

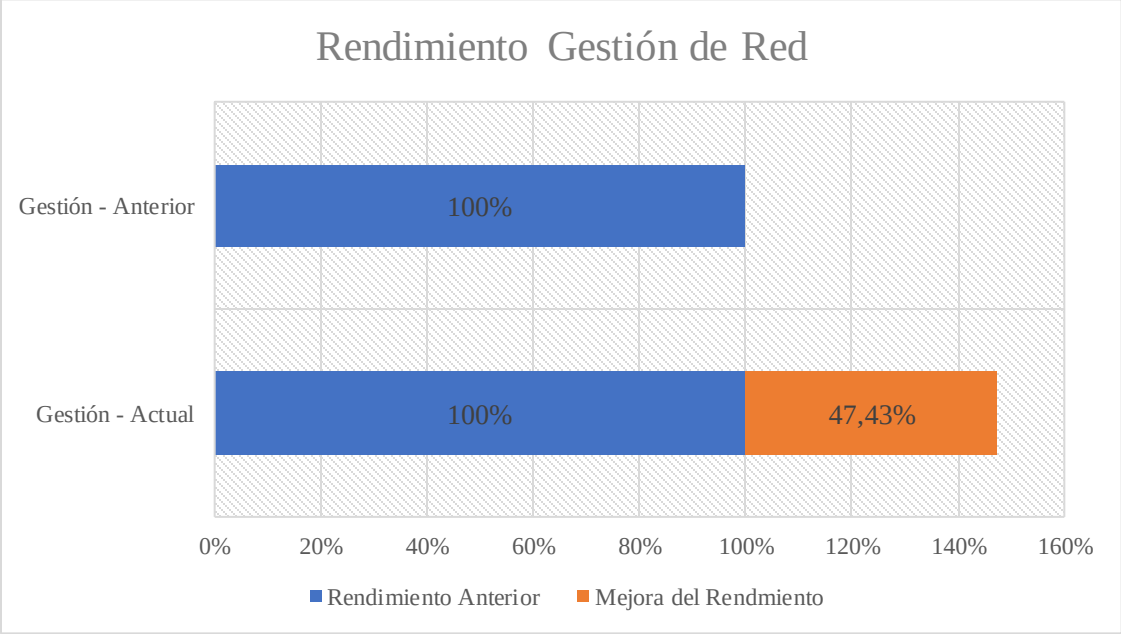
La implementación de SmartOLT ha demostrado una mejora significativa en la ejecución de los procesos, lo que se debe, en gran parte, a la facilidad de interacción que ofrece su entorno gráfico. Esto permite a los usuarios leer y comprender los datos de manera clara y sencilla, lo que hace que la interpretación de la información sea mucho más fácil y efectiva. Además, SmartOLT monitorea equipos clientes lo cual permite a los usuarios que manejan la herramienta detectar y solucionar problemas de manera rápida y funcional. Esto se traduce en una mayor eficiencia en la gestión de la red, ya que los problemas se pueden resolver de manera oportuna, lo que reduce el tiempo de cortes en el servicio y aumenta la satisfacción del cliente.

En resumen, SmartOLT es una herramienta esencial para cualquier empresa que busque mejorar la eficiencia de la gestión de su red. Su facilidad de uso, su capacidad de análisis y su

acceso remoto a través de la nube lo convierten en una solución completa y efectiva para cualquier necesidad de gestión de red.

Figura 149

Rendimiento Gestión de Red



5.1.2.2. Rendimiento actual – Administración de Red

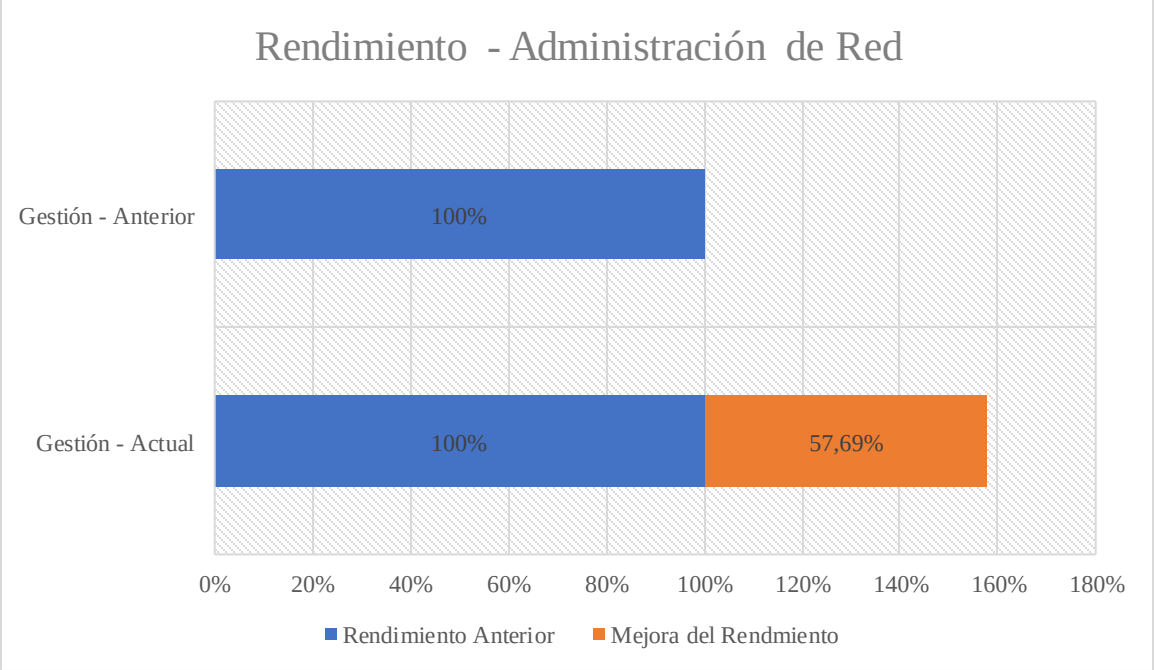
Después de la implementación de SmartISP con el objetivo de mejorar el rendimiento en la administración de la red, los resultados obtenidos son muy positivos, tal como se evidencia en la **Figura 150**. La herramienta SmartISP presenta características muy útiles para la optimización de los procesos relacionados con la administración de la red. En particular, el acceso remoto permite a los usuarios del sistema realizar las tareas necesarias sin necesidad de estar en un lugar específico. Bastando únicamente tener un equipo que tenga conexión a internet, lo cual representa

una ventaja significativa en términos de eficiencia y reducción de tiempos en la ejecución del proceso.

En cuanto al rendimiento, se aprecia un aumento del 57,69% en la mejora de los tiempos de respuesta de los procesos, lo que se traduce en una buena adaptación del servicio de administración. El tiempo empleado para la ejecución del proceso de corte de servicio se reduce significativamente, lo que se traduce en una mayor eficiencia en la administración de la red. Por lo tanto, SmartISP es una herramienta que se ajusta perfectamente a las necesidades presentes en la empresa CayambeVision S.A. en términos de administración de la red.

Figura 150

Rendimiento Administración de Red



5.2. CONCLUSIONES

La documentación bibliográfica obtenida de fuentes oficiales acerca del funcionamiento de la tecnología GPON FTTH resulta fundamental para comprender el entorno en el que se desarrolla la empresa CayambeVision S.A. y las tecnologías que se emplean en la red de Backbone. Este conocimiento resulta imprescindible para el diseño, implementación y mantenimiento de la red, así como para la toma de decisiones estratégicas que permitan mejorar la calidad del servicio ofrecido.

Para garantizar un enfoque metódico y sistemático para el análisis, selección e implementación de servicios destinados a mejorar la gestión y administración de la red de CayambeVisión S.A., se utilizan como referencia las mejores prácticas recomendadas por la ISO/IEEE 29148 y el FCAPS. Estas prácticas ayudan a garantizar que se sigan los procedimientos adecuados y se logren los objetivos de calidad para una mejora continua de la red

Luego de realizar el levantamiento de información de los procesos existentes en la empresa, se sometieron a comparativa distintas herramientas alojadas en la nube ofrecidas en el mercado para solucionar los problemas conocidos en la red de CayambeVision S.A. La evaluación se basó en un benchmarking competitivo utilizando los Likerts como métrica de calificación. Tras el análisis de los resultados obtenidos, se seleccionaron SmartOLT y SmartISP como las herramientas más adecuadas para la gestión y administración de la red.

Una vez obtenido el resultado del benchmarking se realiza una planificación que permita la correcta implementación de los servicios SmartOLT y SmartISP. En donde, SmartOLT es una herramienta fácil de implementar cuyo objetivo es el manejo de la gestión de la red y su principal función es el envío de comandos hacia la OLT de manera remota. Para el manejo de los clientes

de CayambeVision S.A., se integra SmartISP que permite la administración y automatización de procesos a través de los equipos de borde Mikrotik para mejorar el rendimiento de la red.

Tras la implementación de SmartOLT y SmartISP en la red de CayambeVision S.A., las pruebas finales de funcionamiento arrojan porcentajes significativos de mejora en la gestión y administración de la red. La implementación de SmartOLT mejora el modelo de gestión en un 47,43%, mientras que SmartISP mejora el rendimiento en un 57,69%. Estos resultados muestran que estas herramientas cumplen su objetivo de reducir el tiempo de respuesta ante incidentes y de mejorar los procesos de gestión y administración. Con la actual reorganización de los procesos, se logró identificar progresos considerables y así, cumplir con el objetivo de optimizar la red.

5.3. RECOMENDACIONES

Se propone realizar controles continuos en cada área para verificar el correcto uso y funcionamiento de las herramientas SmartOLT y SmartISP. Además, se ofrecerán capacitaciones continuas y se resolverán preguntas que puedan ser planteadas por el personal de oficina, cobranza y técnicos, con el fin de mejorar el rendimiento y la toma de decisiones. Esto permitirá optimizar el servicio al cliente. Es importante asegurar que se brinde una atención óptima y de calidad para lograr la satisfacción del cliente.

Almacenar los manuales técnicos entregados por el responsable a cargo del presente proyecto y distribuirlos en la empresa CayambeVision S.A. de acuerdo con el proceso que se genere en cada una de las áreas. De esta manera, se especializará a cada una de las áreas para el correcto desarrollo de las actividades en los servicios de SmartOLT y SmartISP. Es importante garantizar que los manuales estén disponibles para todo el personal y que sean accesibles para su

consulta en caso de ser necesario. De esta forma, se podrá mejorar la eficiencia y calidad en la prestación de servicios.

Se sugiere que el administrador a cargo de la red verifique constantemente el correcto funcionamiento de SmartOLT y SmartISP. De esta manera, se evitarán posibles problemas al momento de ejecutar los procesos en cada una de estas herramientas. Es importante realizar estas verificaciones de manera periódica para asegurar que las herramientas estén en óptimas condiciones y se pueda brindar un servicio de calidad.

BIBLIOGRAFÍA

ARCOTEL. (2020). *SERVICIO DE ACCESO A INTERNET.*

Arroyave Arredondo, A. F. (2013). *IMPLEMENTACIÓN DEL ÁREA DE SEGURIDAD DEL MODELO FCAPS EN LA INFRAESTRUCTURA DE RED DE LA ALCALDÍA DE ENVIGADO.* Envigado.

Benavidez Vera, E., Colina Morles, E., Segarra Farán, E., Siguenza Guzman, L., & Arcentales Carrion, R. (2019). Process mapping as a basis for the application of activity-based costing systems in assembly industries. *Economía y Política*.

Cañadas, I., & Sanchez, A. (2012). *CATEGORÍAS DE RESPUESTA EN ESCALAS TIPO LIKERT.* Psicothema. Obtenido de https://reunido.uniovi.es/index.php/PST/article/view/7489

Ceballos Mendoza, J. C., & Badillo Angulo, J. R. (2004). *GUÍA PRÁCTICA PARA LA ADMINISTRACIÓN DE REDES DE COMPUTADORAS.* Cartagena.

Huawei. (05 de 12 de 2019). *Foro Huawei*.

Jaramillo, D., & Torres, L. (2015). *Administración y Gestión de la red inalámbrica del Gobierno Autónomo Descentralizado (GADIP) del Cantón Cayambe basada en el modelo funcional FCAPS De La ISO.* Ibarra.

Merchán Campos, L. (2018). *CLOUD COMPUTING COMO ESTRATEGIA TECNOLÓGICA PARA LAS PYMES CASO PRÁCTICO: EMPRESA NOVIATAT S.A. DE LA CIUDAD DE GUAYAQUIL.* Ambato.

Microsoft Azure. (2017). *Cloud computing terms.*

NIST. (2012). *La definición del NIST de computación en la nube.*

Pérez Ruiz, M. A. (2019). *DISEÑO DE UNA RED DE FIBRA ÓPTICA FTTH PARA BRINDAR EL SERVICIO DE INTERNET A LOS USUARIOS DE LA EMPRESA wREDECOM EN EL CENTRO DE LA CIUDAD DE OTAVALO.* Ibarra.

Puentes Gil, P. A., & Cetina sabogal, J. A. (2017). *ESTUDIO DE METODOS Y TIEMPOS PARA LA EMPRESA PAPELES.* Bogotá.

Quisnancela, E., & Espinosa, N. (2016). *Certificación de redes GPON, normativa ITU G.984.x.*

SMARTISP. (2020). *SMARTISP*. Obtenido de https://www.smartisp.us/

Songhurst, D. J. (1999). *Charging Communication Networks.* Cambridge: Elsevier Science.

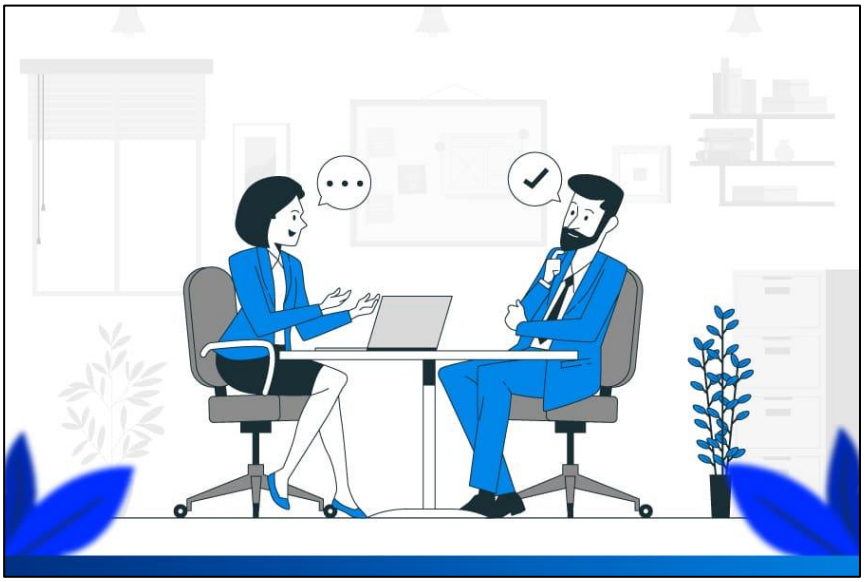
Torres Chicaiza, L. E. (2015). *Administración y gestión de la Red Inalámbrica del Gobierno Autónomo Descentralizado (GADIP) del Cantón Cayambe basada en el modelo funcional FCAPS de la ISO (Bachelor's thesis).*

UIT-T. (2000). *Principios para una red de gestión de las telecomunicaciones, Recomendación UIT-T M.3010 .*

ANEXO 1

ENTREVISTA

GERENCIA CAYAMBEVISION S.A.



ÁREA OFICINA Y ÁREA TÉCNICA

ANEXO 2

PREVENCIÓN PROCESO 2

INGRESO DE CLIENTES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

CAYAMBEVISION
TELECOMUNICACIONES

REPORTE DE INGRESO CLIENTES

NOMBRE DEL ENCARGADO	
FECHA	

NOMBRE CLIENTE	MODELO ONU	SN	CAJA DE DISTRIBUCIÓN

FIRMA DEL ENCARGADO

ANEXO 3

PREVENCIÓN PROCESO 5

PAGO DE SERVICIO

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

CAYAMBEVISION
TELECOMUNICACIONES

REPORTE DE CAJA

NOMBRE DEL ENCARGADO	
FECHA	

INGRESOS

PLAN	COSTO	N°	TOTAL/PLAN
25 MEGAS	$16,80		
100 MEGAS	$22,40		
120 MEGAS	$25,70		
140 MEGAS	$28,90		
160 MEGAS	$33.50		
220 MEGAS	$35.40		
	TOTAL		

EGRESOS

ACTIVIDAD	VALOR
TOTAL	

TOTAL RECAUDADO

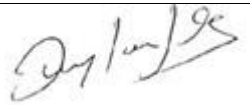
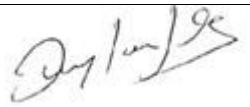
INGRESOS	
EGRESOS	
TOTAL	

FIRMA DEL ENCARGADO

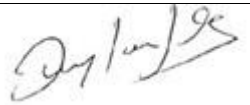
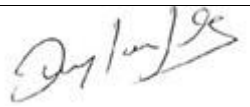
ANEXO 4

CONTROL DE CAMBIOS

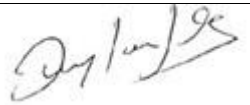
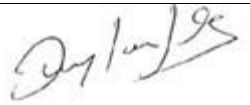
Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

VERSIÓN	FECHA DE MODIFICACIÓN	MODIFICACIÓN	RESPONSABLE	FIRMA DEL RESPONSABLE
00	01/08/2022	Configuración de OLT: • Creación de perfil para administrar OLT	Administrador de red Encargado del proyecto	
01	03/08/2022	Configuración de OLT: • Habilitación de servidores de tiempo	Administrador de red Encargado del proyecto	
02	05/08/2022	Configuración Mikrotik CC-1072: • Levantamiento de información • Asignación de herramientas para el port forwarding	Administrador de red Encargado del proyecto	
03	10/08/2022	Configuración Mikrotik CCR-36: • Configuración de Port Forwarding	Administrador de red Encargado del proyecto	
04	12/08/2022	Configuración Mikrotik CCR-1036: • Finalización de configuración Port Forwarding	Administrador de red Encargado del proyecto	

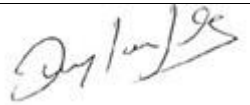
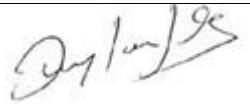
Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

05	15/08/2022	Configuración de SmartOLT: • Primer ingreso hacia el servicio en la nube • Reconocimiento del sitio	Administrador de red Encargado del proyecto	
06	19/08/2022	Configuración de SmartOLT: • Culminación del Enlace SmartOLT y OLT • Pruebas de Conexión	Administrador de red Encargado del proyecto	
07	22/08/2022	Configuración de SmartOLT: • Configuración del Sistema	Administrador de red Encargado del proyecto	
06	02/09/2022	Configuración de SmartOLT: • Configuración del Sistema	Administrador de red Encargado del proyecto	
07	16/09/2022	Configuración de SmartOLT: • Ingreso de Clientes	Administrador de red Encargado del proyecto	
08	26/09/2022	Configuración de SmarISP: • Creación de Cloud Server	Administrador de red Encargado del proyecto	

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

09	30/09/2022	Configuración de SmarISP: • Finalización de Cloud Server	Administrador de red Encargado del proyecto	
10	03/10/2022	Configuración de SmarISP: • Instalación SmartISP	Administrador de red Encargado del proyecto	
11	07/09/2022	Configuración de SmarISP: • Finalización de instalación SmartISP • Prueba de Ingreso	Administrador de red Encargado del proyecto	
12	10/10/2022	Configuración de SmarISP: • Configuración Túnel VPN	Administrador de red Encargado del proyecto	
13	15/09/2022	Configuración de SmarISP: • Creación de Certificados de conexión Túnel VPN • Configuración de Firewall VPN	Administrador de red Encargado del proyecto	
14	21/10/2022	Configuración de SmarISP: • Conexión de OpenVPN Cliente • Pruebas de conexión	Administrador de red Encargado del proyecto	

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

12	25/10/2022	Configuración de SmarISP: • Finalización de configuración de Sistema SmartISP	Administrador de red Encargado del proyecto	
13	11/11/2022	Configuración de SmarISP: • Ingreso de Clientes SmartISP	Administrador de red Encargado del proyecto	

ANEXO 5

LIBERACIÓN DE SERVICIOS

Cayambe 28 de noviembre del 2022.

Autorización de Liberación de Servicios. -

Por medio de este presente me permito a solicitar a la empresa CayambeVision S.A., la autorización para liberar los servicios SmartOLT y SmartISP integrados a la red de la empresa en supervisión del Sr. Lara Maldonado Hugo Roberto encargado del área de Administración actual de la red. Proyecto a cargo del Sr. Lema Villavicencio Deylan Javier, alumno de la carrera de Ingeniería en Telecomunicaciones de la Universidad Técnica del Norte. Dando como fecha programada para el lanzamiento el 01/12/2022.

Particular que me permito dar a conocer para los fines pertinentes.

Atentamente.

Deylan Javier Lema Villavicencio

PERSONA A CARGO

ANEXO 6

CAPACITACIÓN - PERSONAL CAYAMBEVISION S.A.


VISA


SALIDA

ANEXO A

Guía de instalación y configuración de Túnel VPN

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

Guía de Instalación y

Configuración de Túnel VPN

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ÍNDICE DE CONTENIDOS

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

1. Instalar OpenVPN

Para instalar el certificado lo primero que se realiza es la actualización de la máquina virtual y posterior ingresar el comando `apt-get install openvpn easy-rsa` con el cual se descargan los paquetes OpenVPN como se hace énfasis en los recuadros rojos mostrados en la Fig 1.

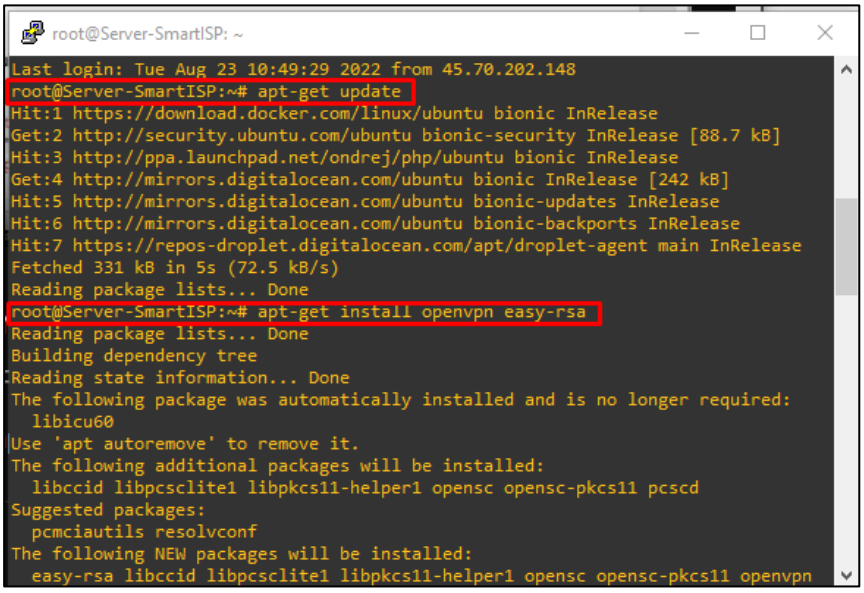


Fig 1: Instalación OpenVPN

2. Creación de Certificado de Autorización CA

El certificado se lo crea ingresando la sentencia `make-cadir certificates && cd certificates` como se muestra en la Fig 2.

Fig 2: Creación de Certificados

3. Construir el Certificado de Autorización

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

Se procede a ingresar `al fichero ./clean-all && ./build-ca` como se muestra en la Fig 3 y se presiona la tecla "enter" hasta que finalice el proceso de creación.

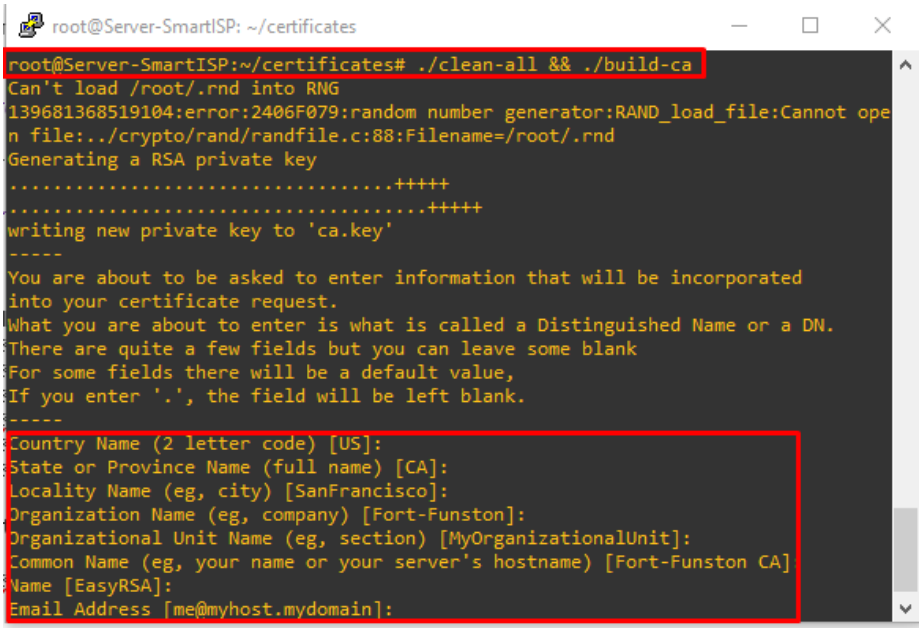


Fig 3: Construcción de CA

4. Creación de Certificados, Llaves y Archivos de Encriptación del Servidor

El siguiente paso es el ingreso del comando `./build-key-server server` con el cual se crean las llaves del servidor OpenVPN, similar al paso anterior se presiona "enter" hasta que se termine de crear.

Posterior a esto se ingresa el comando `openvpn --genkey --secret keys/ta.key` y se acepta todos los parámetros presionando "enter" y al finalizar ingresar "yes" en los parámetros finales cuando termine el proceso como se muestra en la Fig 4.

CAYAMBEVISION TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

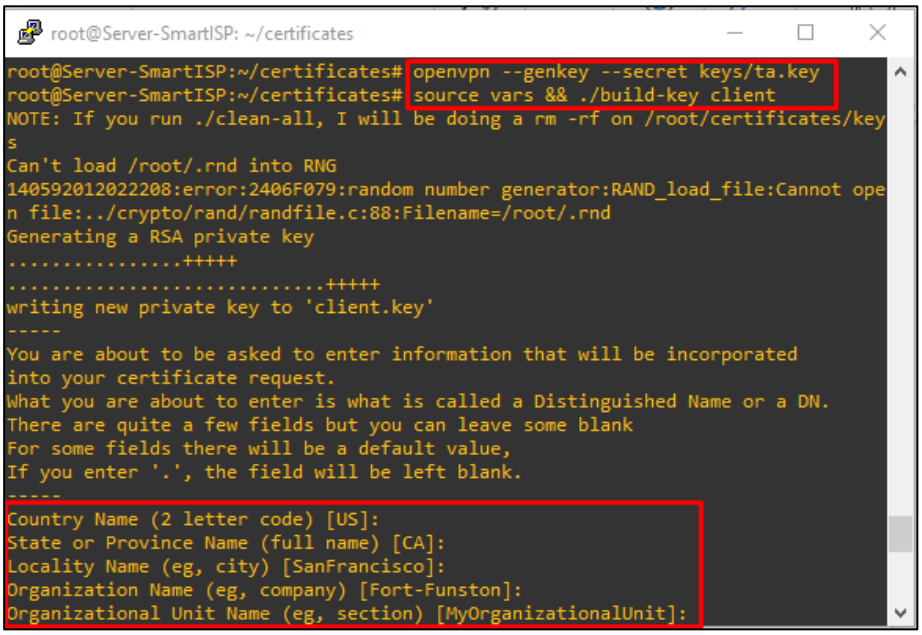


Fig 4: Creación de llaves de autenticación

5. Creación de Cliente

La creación de la llave del cliente se la realiza mediante el comando `source vars && ./build-key client` la cual se realiza como en el paso 4, aceptando y confirmando con "yes".

6. Configuración del Servicio OpenVPN

A continuación se procede a copiar a la dirección `/etc/openvpn` las llaves, certificados de autenticación y certificación del servidor OpenVPN mediante el comando `cp keys/{server.crt,server.key,ca.crt,dh2048.pem,ta.key} /etc/openvpn`. En el cuadro rojo presentado en la Fig 5 se muestra el desarrollo del proceso.

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

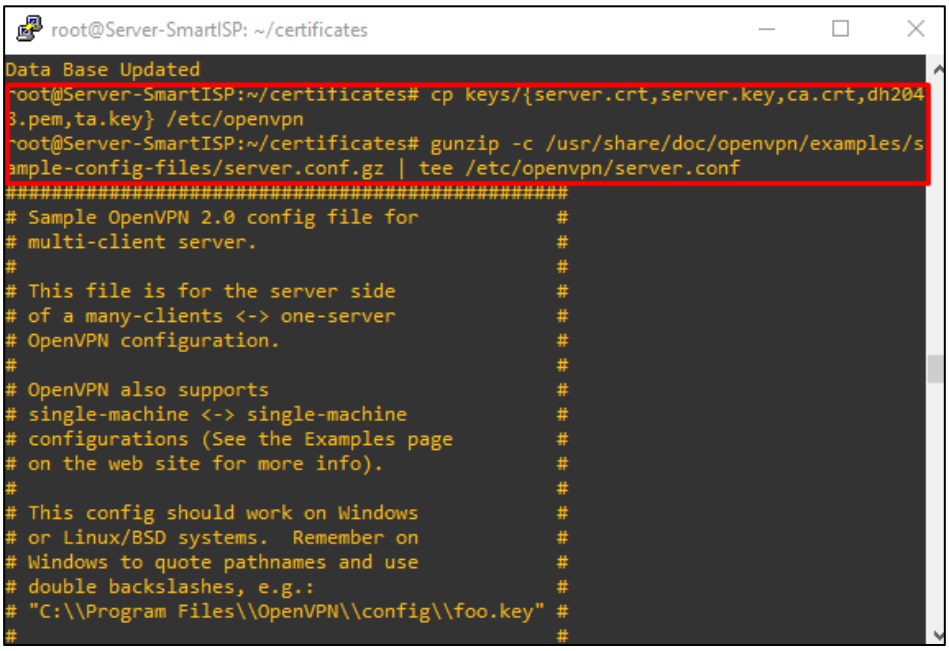


Fig 5: Copia de llaves a Servidor VPN

Una vez ejecutado el comando para copiar se descomprime los archivos correspondientes al servidor de OpenVPN.

Como paso siguiente se realizan cambios al archivo alojado en `/etc/openvpn/server.conf` para lo cual se ingresa y se realizan los siguientes cambios:

- Establecer el cifrado AES-128-CBC

  ```
  cipher AES-128-CBC
  ```

- Cambiar protocolo de UDP a TCP:

  ```
  protocol tcp

  ;protocol udp
  ```

- La compresión LZO debe estar deshabilitada

  ```
  ;comp-lzo
  ```

CAYAMBEVISION TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

- Des comentar la configuración de nombre común duplicado (esto permite que varios clientes se conecten al servidor usando el mismo certificado):

```
duplicado-cn
```

- Comente esta configuración (de lo contrario, produce errores de autenticación)

```
;tls-auth ta.key 0
```

- Comentar la configuración (no compatible con TCP):

```
;explicit-exit-notify 1
```

- Guarde y cierre el archivo modificado como se muestra en la Fig 6.

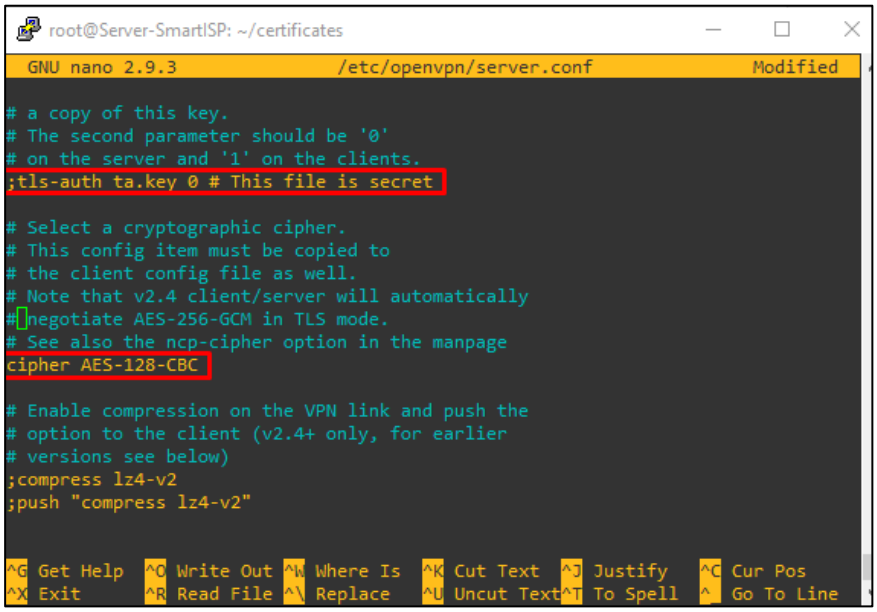


Fig 6: Cambio de Parametros en OpenVPN Server

7. Configurar de red del Servidor OpenVPN

Para configurar la red se ingresa a la dirección `/etc/sysctl.conf` en donde se des comenta la línea de comando `net.ipv4.ip_forward=1`. Como se muestra en la Fig 7.

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

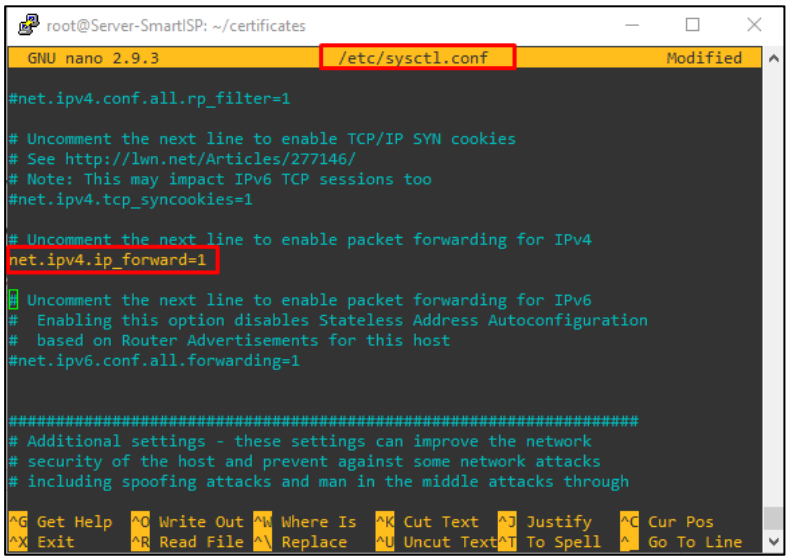


Fig 7: Configuración de Red en OpenVPN Server

Se busca permitir el ingreso externo mediante el túnel VPN para lo cual se ingresa las siguientes líneas de comando que se encuentran subrayadas en el cuadro rojo en la Fig 8 en la dirección `/etc/ufw/before.rules`.

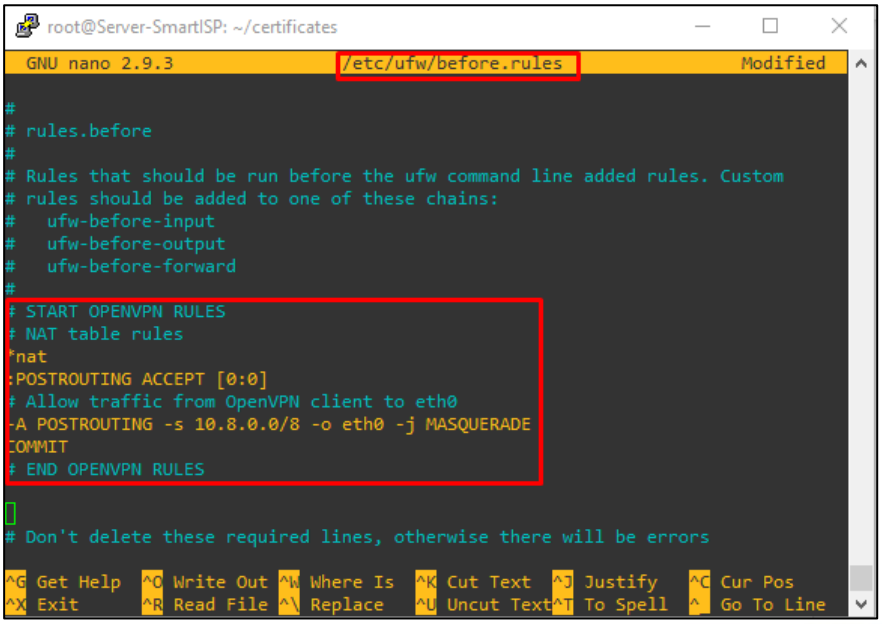


Fig 8: Configuraicón de Interfaces OpenVPN Server

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

A continuación, se realiza el cambio de "DROP" a "ACCEPT" en la dirección `/etc/default/ufw` como se muestra en la Fig 9.

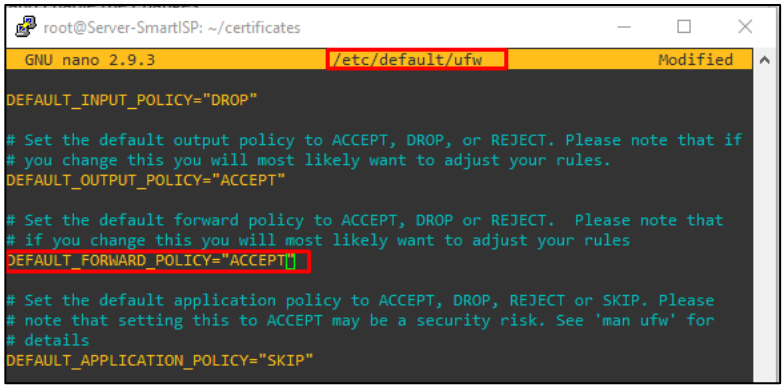


Fig 9: Configuración de Firewall

La configuración de la red finaliza habilitando los puertos 8728, 8729, OPENSSH correspondientes al puerto API y conexión segura SSH. También se deshabilita el firewall para que no exista bloqueo de hosts al momento de establecer el túnel VPN como se muestra en la Fig 10.

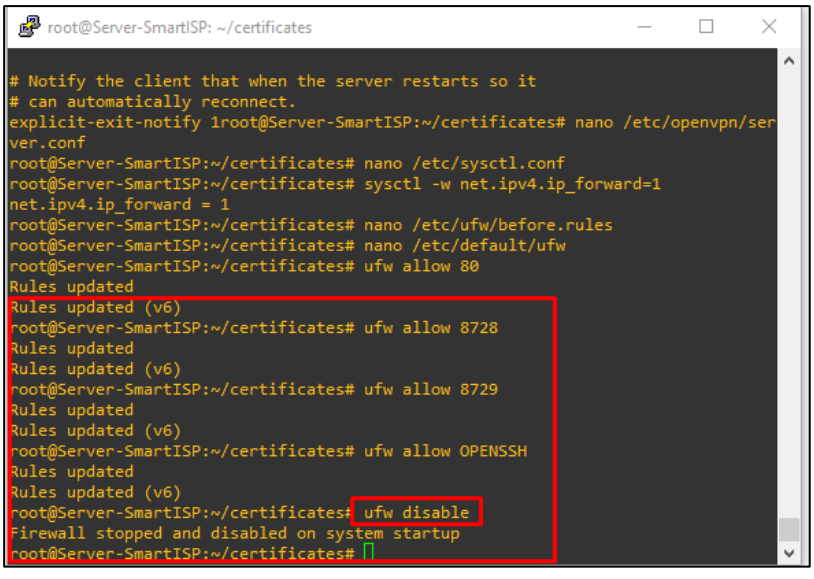


Fig 10: Deshabilitación de Firewall

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

8. Iniciar y habilitar el servicio OpenVPN

Ingresar los comandos de habilitación del servicio como se muestra en la Fig 11:

- `systemctl start openvpn@server`
- `systemctl status openvpn@server`
- `systemctl enable openvpn@server`

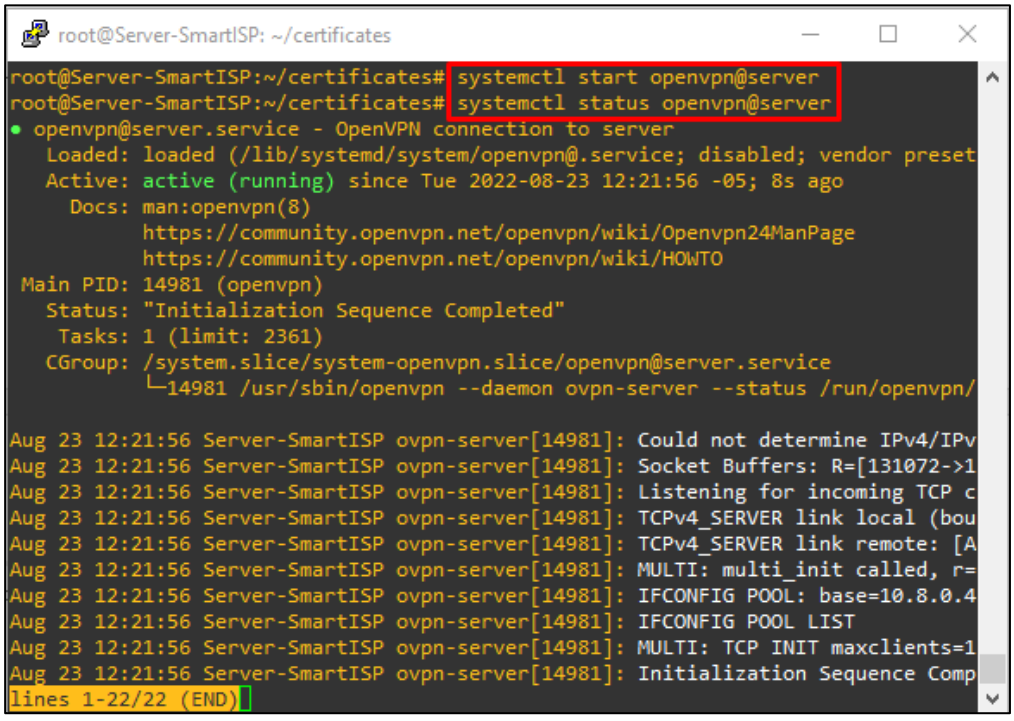


Fig 11: Inicio del Servicio Open VPN

9. Configuraciones Mikrotik

Para realizar las configuraciones en el Mikrotik se necesita descargar las llaves del cliente que será asociado al Tunel VPN. Se utiliza el programa FileZilla el cual es un servidor FTP que nos ayuda a descargar y subir archivos a un host en específico. De esta manera se procede a ejecutar FileZilla e ingresar las credenciales de acceso a la máquina virtual. Procedimiento en la Fig 12.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

Host: *143.244.161.216* Usuario: *root* Puerto: *22*

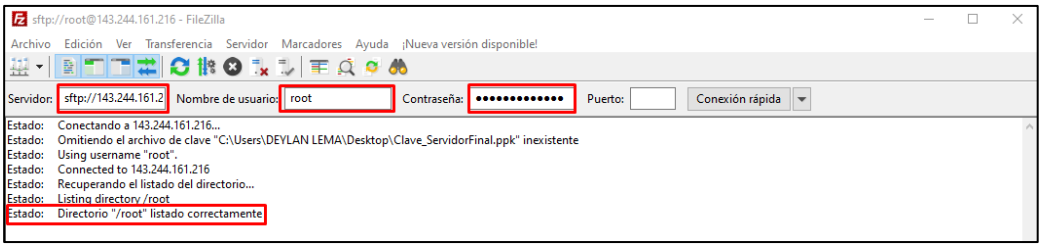


Fig 12: Ingreso FileZila Máquina Virtual

9.1. Copiar las llaves y certificados

Se ingresa al fichero `/root/certificates/keys/` y se descarga los certificados

- `client1.crt`
- `client1.key`
- `ca.crt`

Se procede a abrir el Mikrotik vía Winbox y se realiza el paso de los archivos antes mencionados al *File List*, como se muestra en la Fig 13.

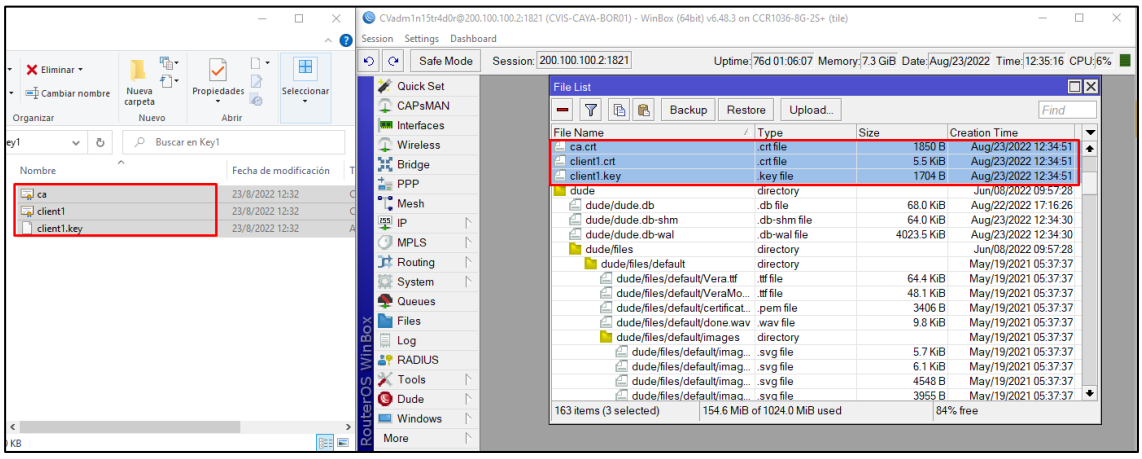


Fig 13: Importación de Certificados

9.2. Instalar certificados

Ingresar a System→Certificates e importar `ca.crt`, este proceso es mostrado a continuación en la Fig 14.

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

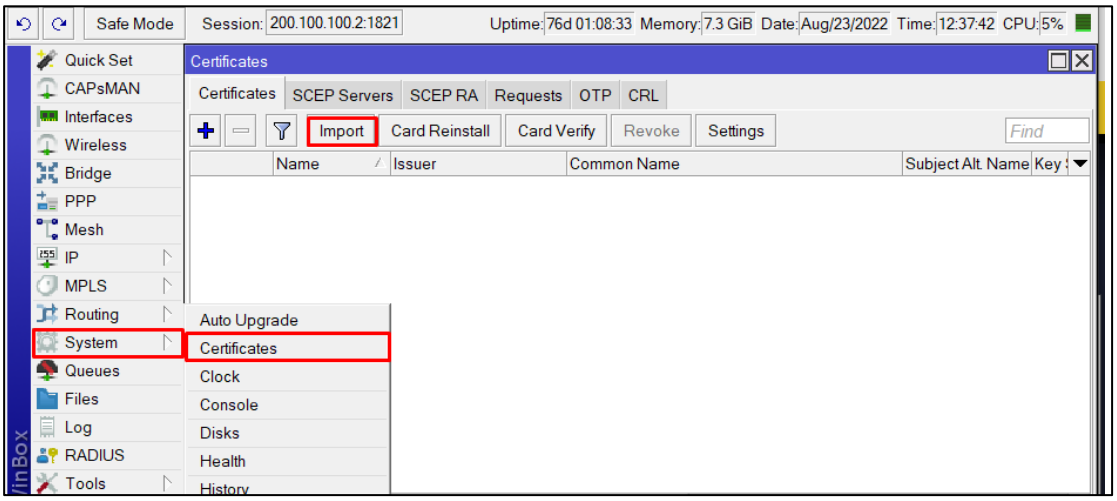


Fig 14: Importación de Certificado de Autorización

De igual manera importar el `client1.crt` y `client1.key`. Fig 15.

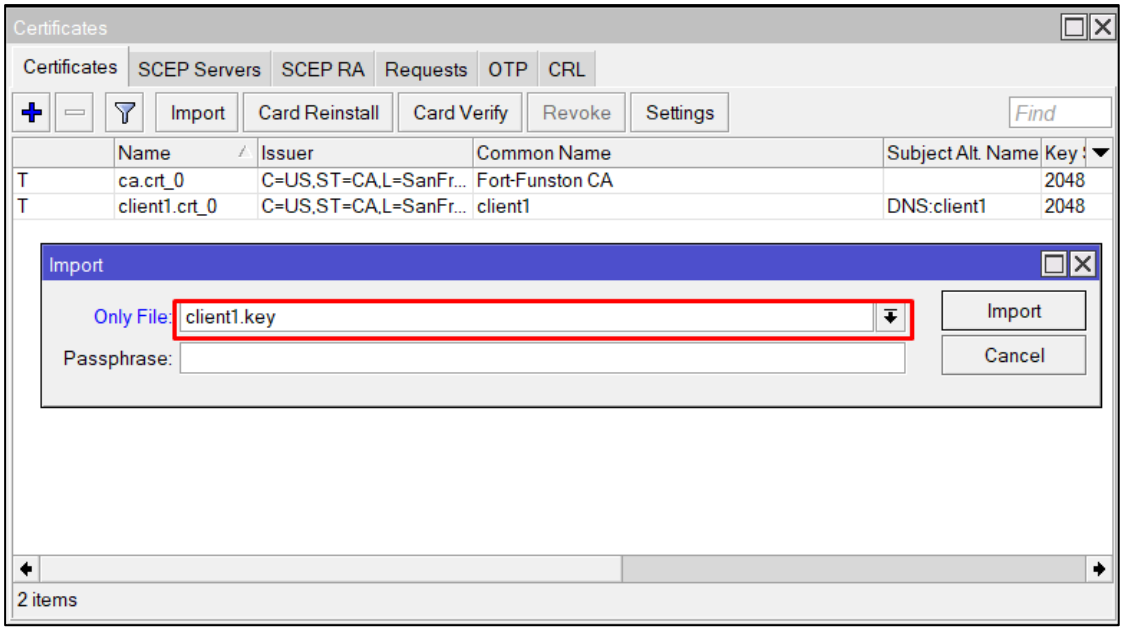


Fig 15: Importación de llave cliente 1

9.3. Crear el perfil PPP (Point to Point - Protocol)

Ingresar a *PPP→Profiles* y crear un nuevo perfil. Aquí se coloca el nombre del perfil.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

El siguiente paso es cambiar a la pestaña de protocolos y deshabilitar MPLS, usar la compresión por defecto y requerir la encriptación. Fig 16.

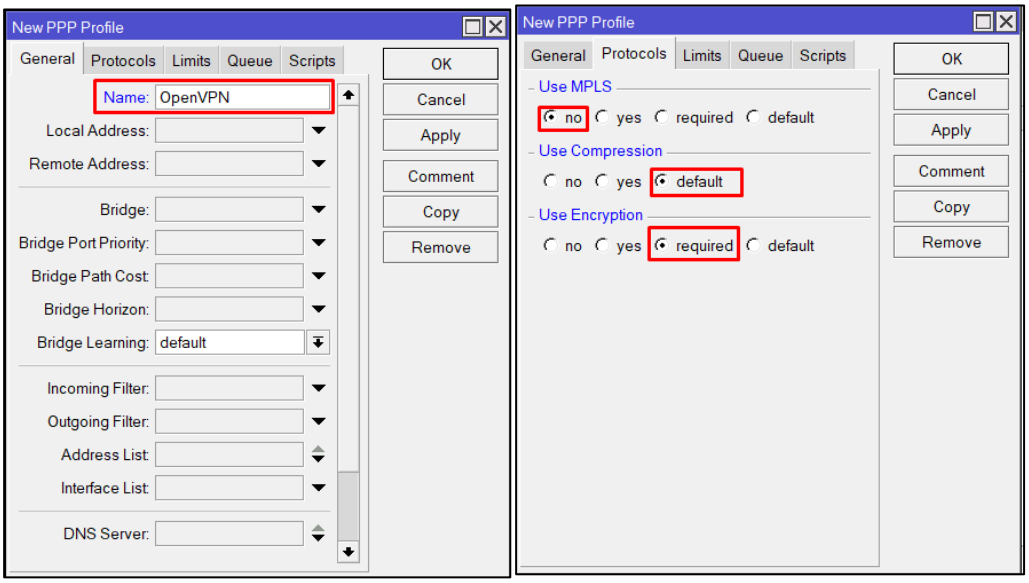


Fig 16: Configuración de perfil PPP

Los límites de la sesión se establecen en uno solo para evitar conexiones simultaneas. Fig 17.

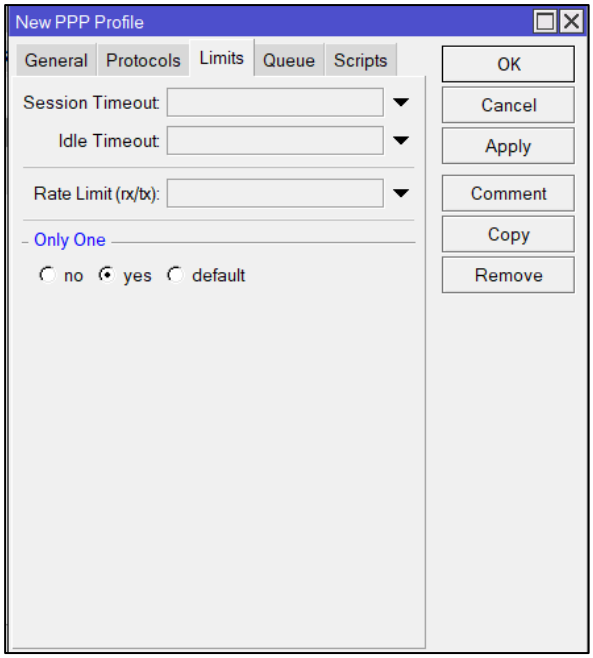


Fig 17: Limites de conexión perfil PPP

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

Una vez creado el perfil *PPP* se ingresa a *PPP→-Interface* y se crea un "*OVPN Client*". Este proceso se lo observa en la Fig 18.

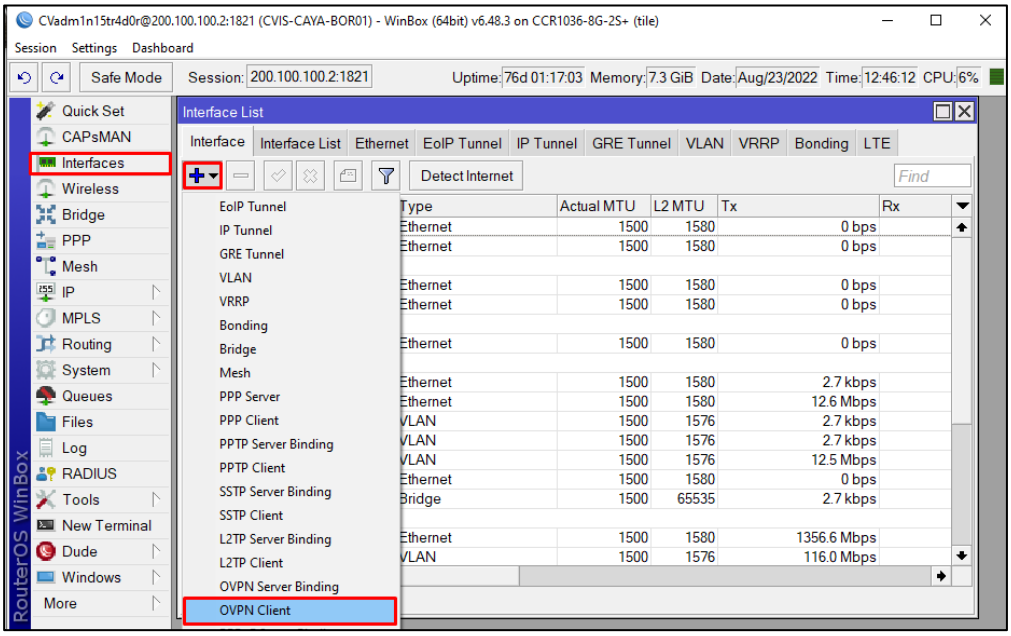


Fig 18: Creaciön de OVPN Client

Para configurar el cliente VPN se ingresan las siguientes propiedades, como se muestra en la Fig 19:

- IP Servidor VPN (Maquina Virtual): *143.244.161.216*
- User: *VPN*
- Certificado: *client1.crt_0*
- Auth: *sha1*
- Cipher: *aes 128*

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

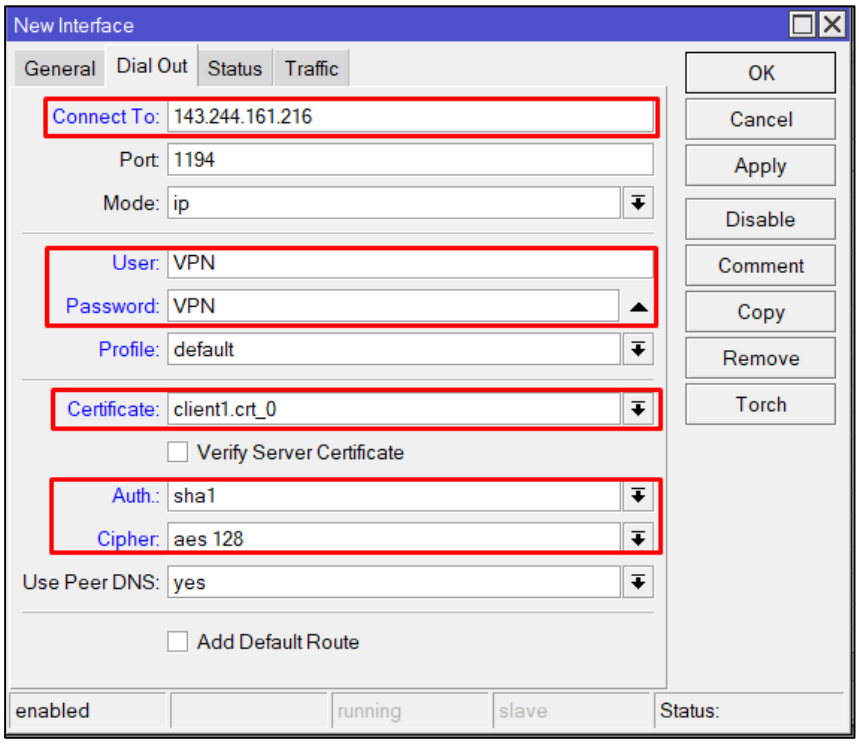


Fig 19: Configuración Cliente VPN

En la Fig 20 se verifica la correcta creación del cliente VPN ingresando a *Interface* identificando la letra R en la parte izquierda lo cual significa *Running* y también dirigiéndose a *IP→Address List* en donde se puede observar que se otorga por parte del servidor VPN una IP dinámica al Cliente VPN.

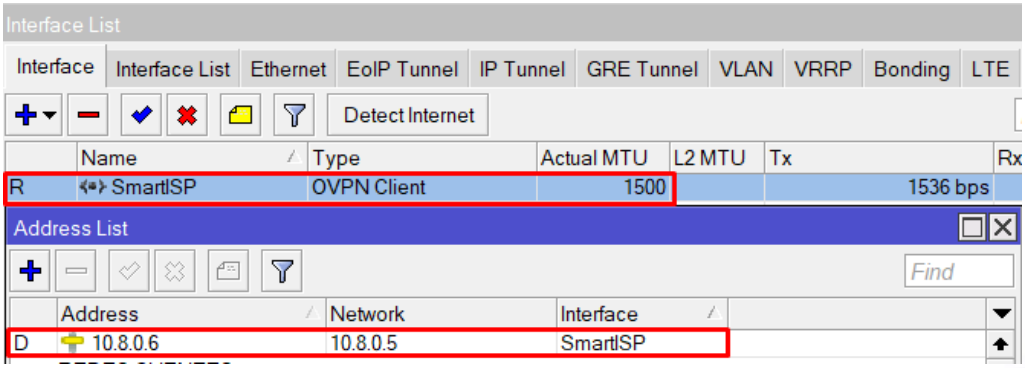


Fig 20: Conexión Open VPN exitosa

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

10. Reservar IPs para clientes OpenVPN

Para reservar IPs fijas a los clientes VPN primero se habilita la opción de configuración de OpenVPN para lo cual se debe ingresar a `nano /etc/openvpn/server.conf`. Ubicar la línea; client`-config-dir ccd` y des comentarla como indica en la Fig 21.

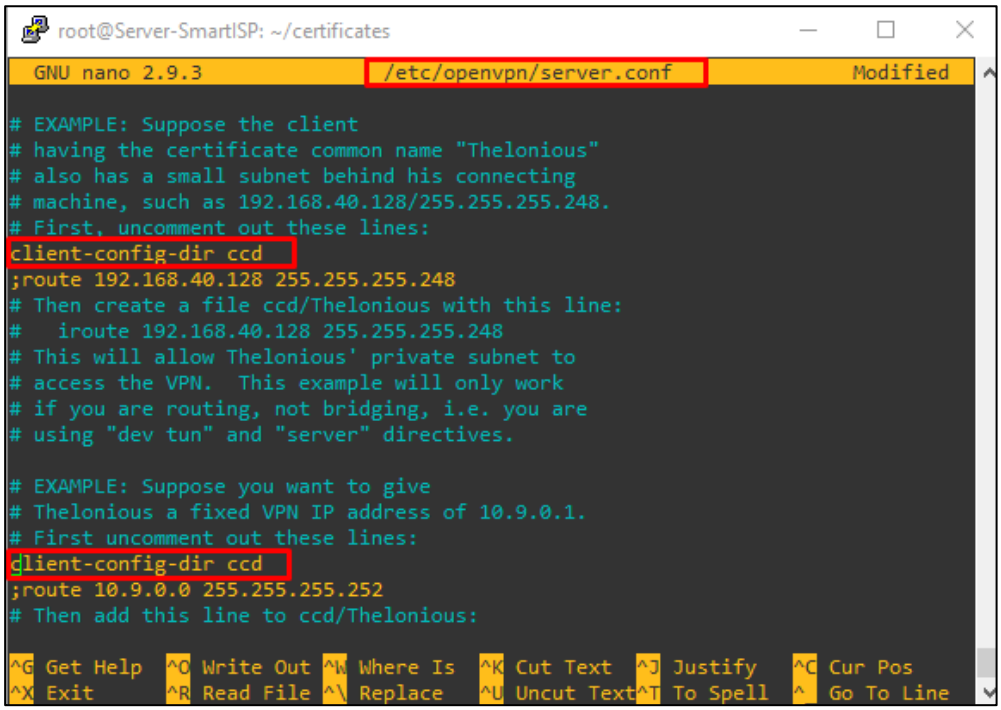


Fig 21: Reservar IP cliente OpenVPN

A continuación, se procede a ingresar al fichero `/etc/openvpn/ccd/client1` y se agrega la sentencia `ifconfig-push 10.8.0.10 10.8.0.1`, mostrado en la Fig 22 la cual permite asignar una IP estática de manera forzada al cliente.

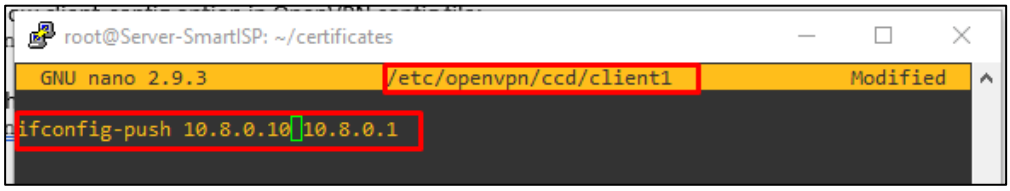


Fig 22: Configuración de IP fija OpenVPN

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

Finalmente, Ingresar al fichero `/etc/openvpn/ipp.txt` y especificar el usuario y la IP a la que se le quiere asignar al momento de establecerse la conexión VPN entre cliente y servidor. Proceso mostrado en la Fig 23.

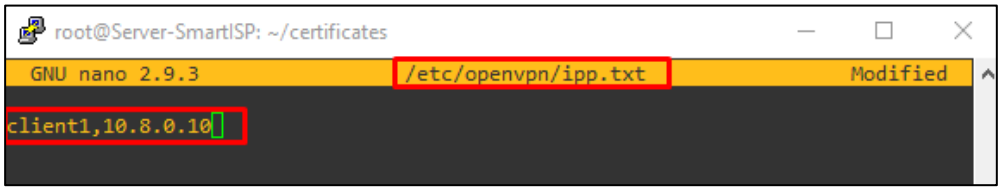


Fig 23: Asignacón de IP Fija

ANEXO B

Configuración de SmartISP

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

Guía de Configuración de Sistema SmartISP

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ÍNDICE

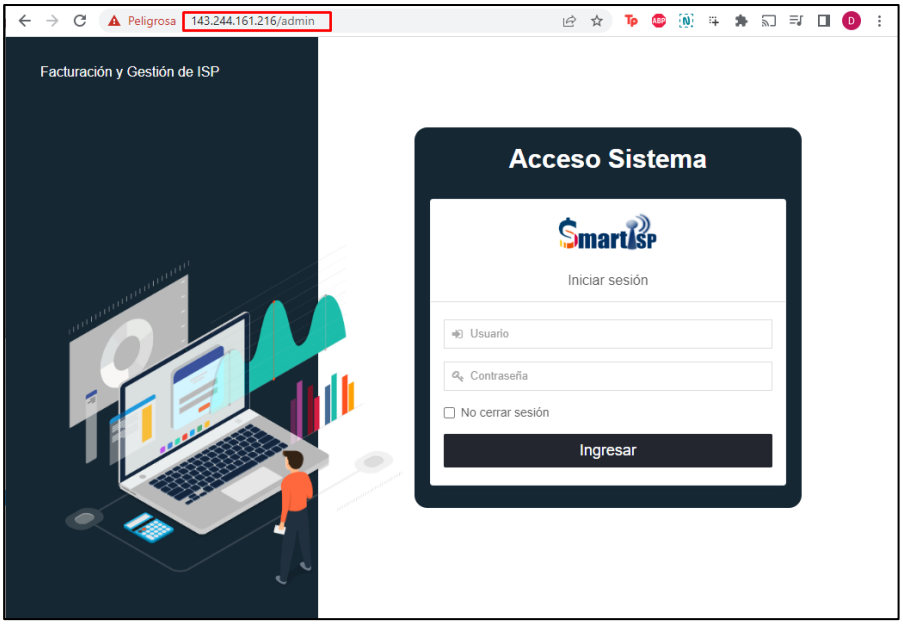
Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

1. Configuración del Sistema – SmartISP

1.1. Configuración Empresa

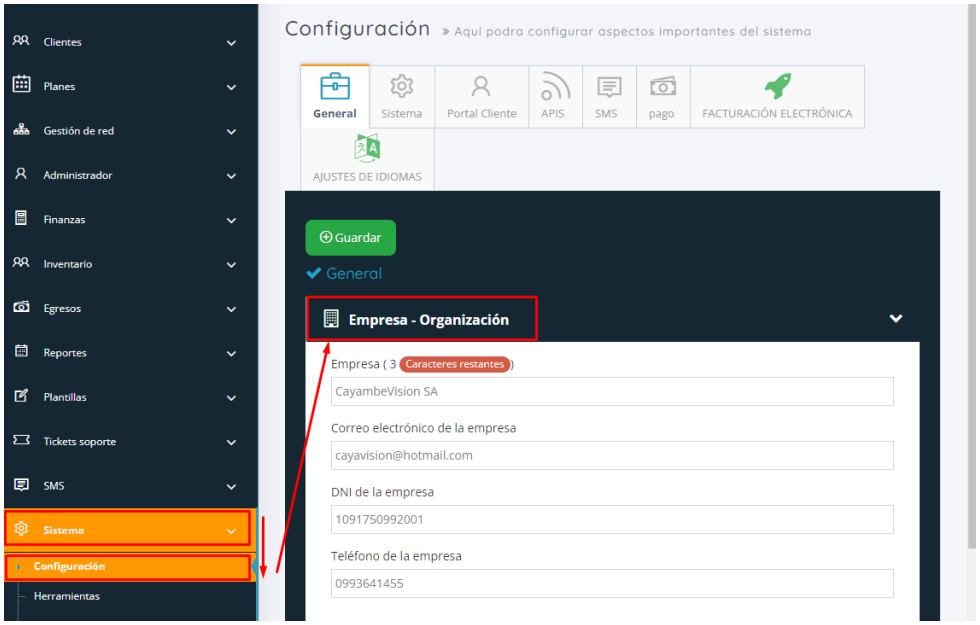
Ingresar a la dirección *http://143.244.161.216/admin.*

Colocar las credenciales asignadas para la administración



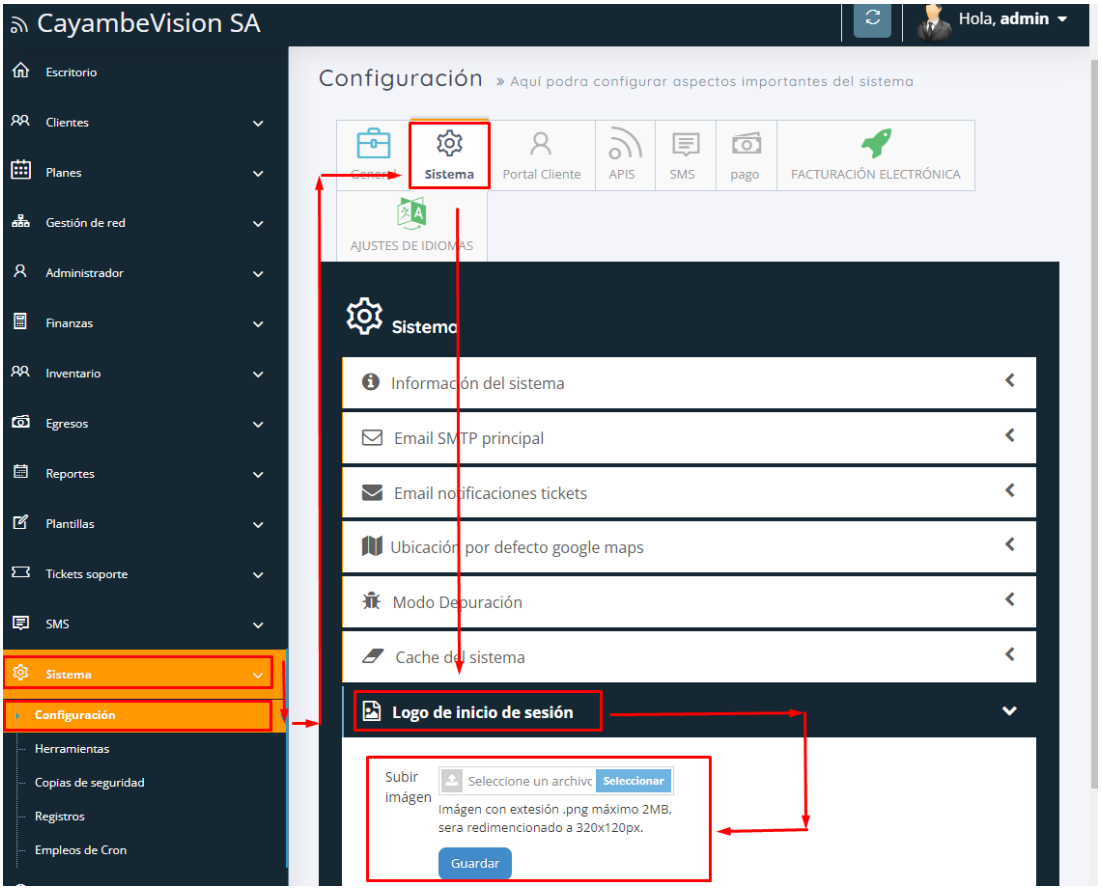
Ingresar a *Sistema→Configuración→Empresa – Organización* y completar la información de la empresa.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



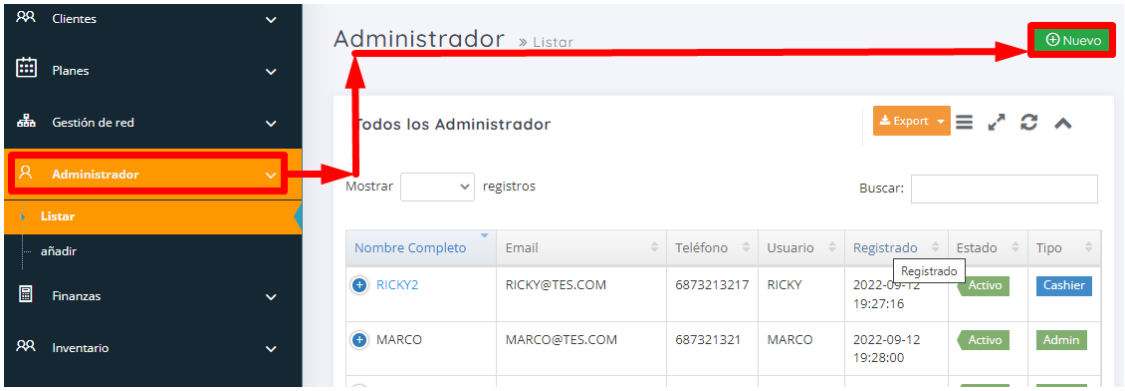
Posterior a esto se modifica el logo de inicio de sesión para SmartISP dirigiéndose a *Sistema→Configuración→Sistema→Logo de inicio de Sesión* y se ingresa el logo de la empresa.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



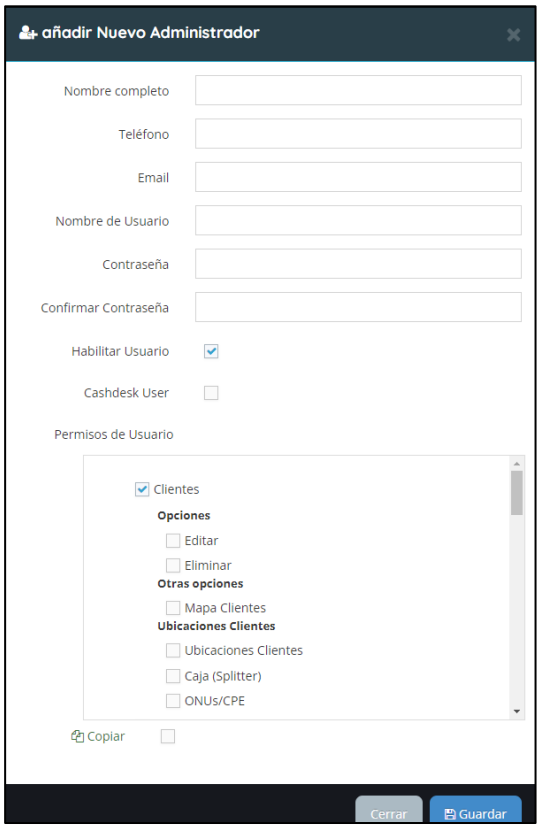
1.2. Creación de Usuarios

Para la creación de usuarios ingresar a *Administrador→Nuevo* de la siguiente manera:



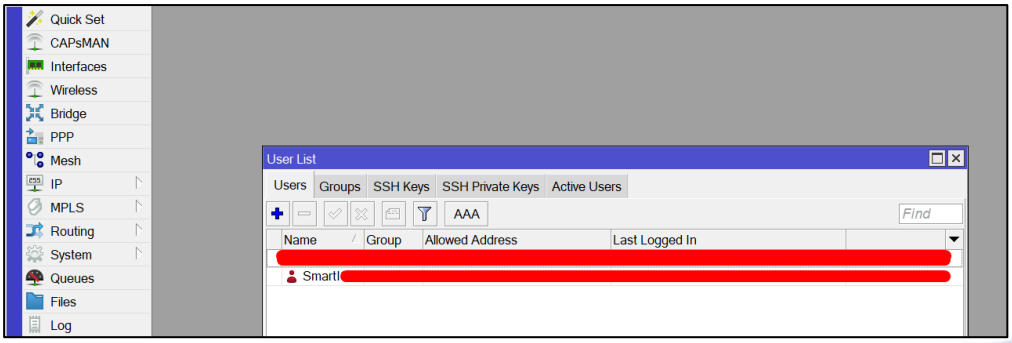
Se procede a crear el perfil de usuario llenando los campos de información y marcando las opciones de permisos acorde a la función dentro de la empresa.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



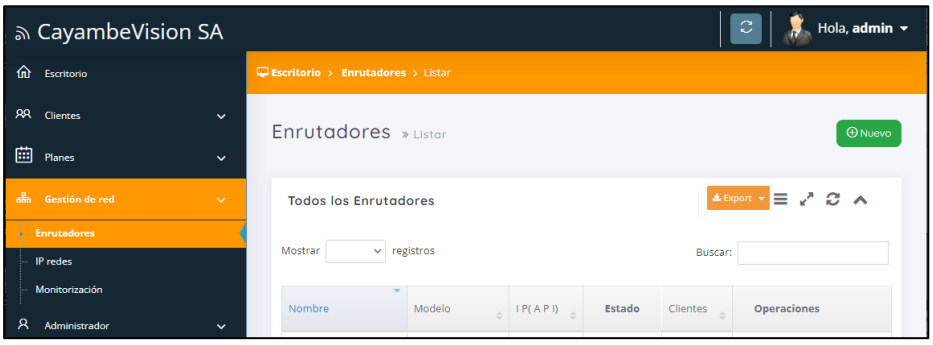
1.3. Conexión SmartISP – Mikrotik Administrador (CCR-1036)

Para la conexión de SmartISP con el Core Mikrotik se procede a crear un usuario en el equipo Administrador ingresando a *System→Users* y creando un nuevo perfil de ingreso al Equipo con permisos full(Administrador).



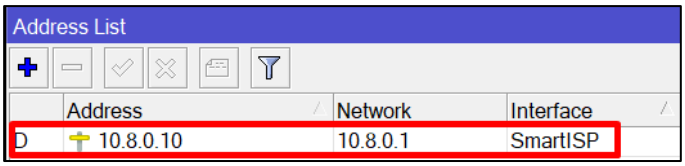
Posteriormente ingresar a SmartISP y se dirige a *Gestión de Red→Enrutadores→Nuevo*

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

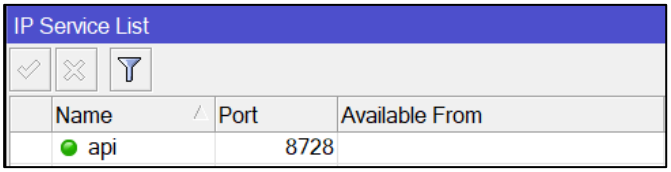


Una vez presionado en *Nuevo* se despliega un cuadro el cual se llena con los siguientes parámetros:

- **Nombre:** Nombre distintivo para el Enrutador.
- **Modelo:** Modelo del Equipo Mikrotik.
- **IP API:** IP asignada por Servidor OpenVPN.

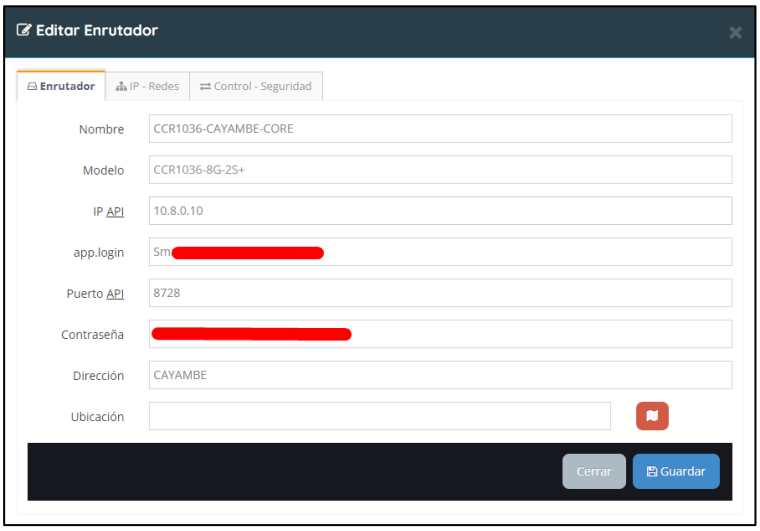


- **App.login:** Usuario Mikrotik.
- **Puerto API:** Puerto API Mikrotik.



- **Contraseña:** Contraseña de usuario Mikrotik.
- **Dirección:** Dirección referencial.
- **Ubicación:** Ubicación Maps.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



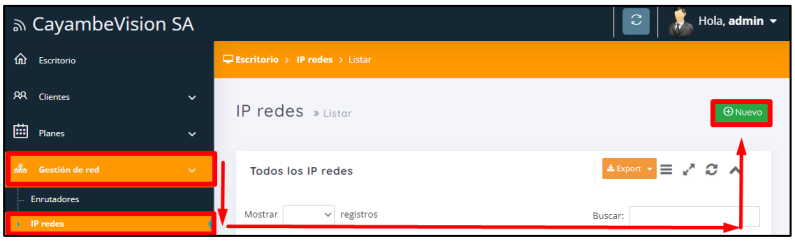
Como paso siguiente se presiona en guardar y se verifica el estado de conexión, en donde se observa el estado "En línea" lo cual corresponde a que se logra la conexión entre SmartISP y Mikrotik Administrador.

Una vez creado el Enrutador se procede a Editar el Equipo con el fin de proporcionar un método de Administración de la red, para lo cual se ingresa a *Control – Seguridad* y se selecciona como tipo de control *Simple Queues* de esta manera se establece el control de ancho de banda para los clientes. También se habilita el portal de clientes para el acceso de usuarios.

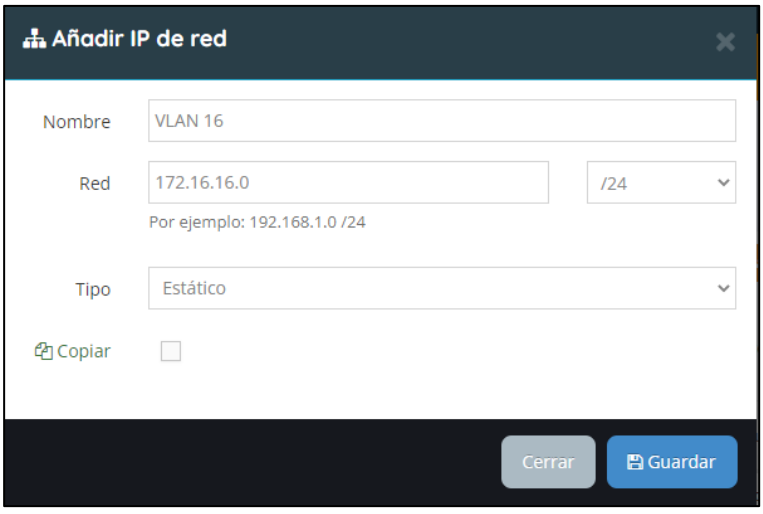
Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

1.4. Configuración de Red – IPs

Ingresar a *Gestión de Red→IP redes→Nuevo*

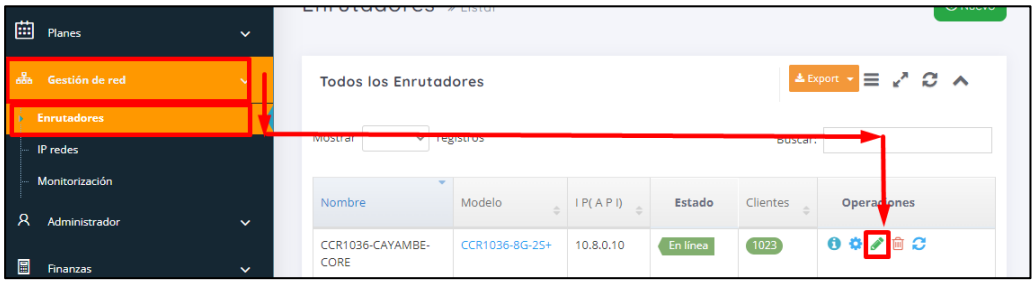


Llenar los campos correspondientes a la red que se desea añadir para los clientes**. Nota:** Todas las redes deben constar en el Equipo Administrador:

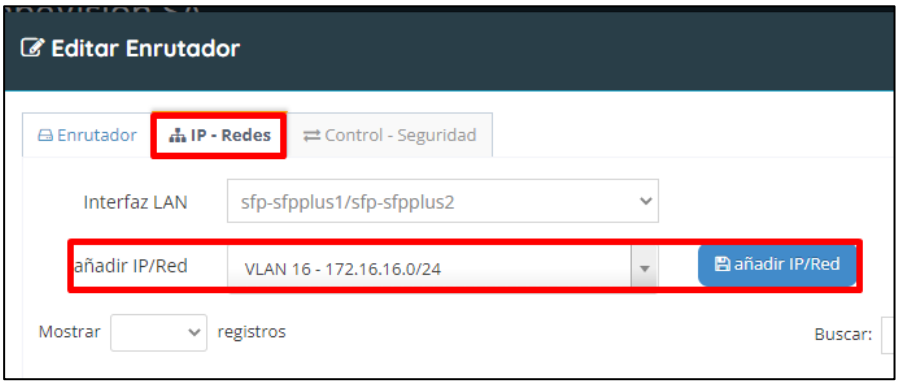


El siguiente paso es asignar al Enrutador el segmento de IPs añadido para lo cual se dirige a *Gestión de Red→Enrutadorres→Editar Enrutador*

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

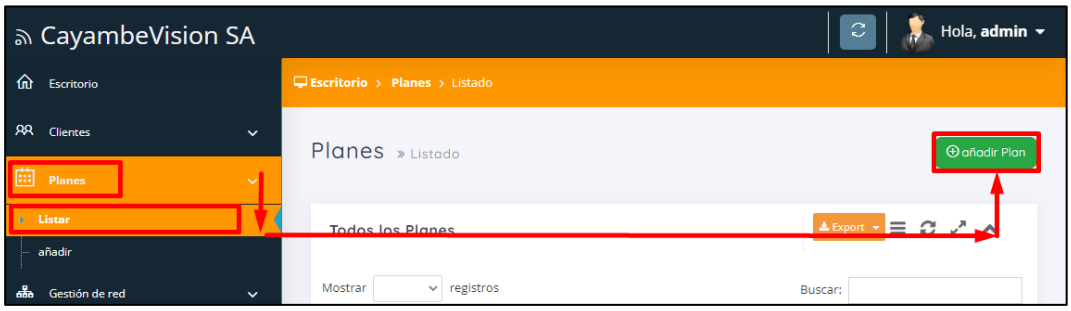


Una vez presionado en *Editar Enrutador* se ingresa a *IP-Redes* y se añade el segmento de IPs con el cual se busca trabajar.



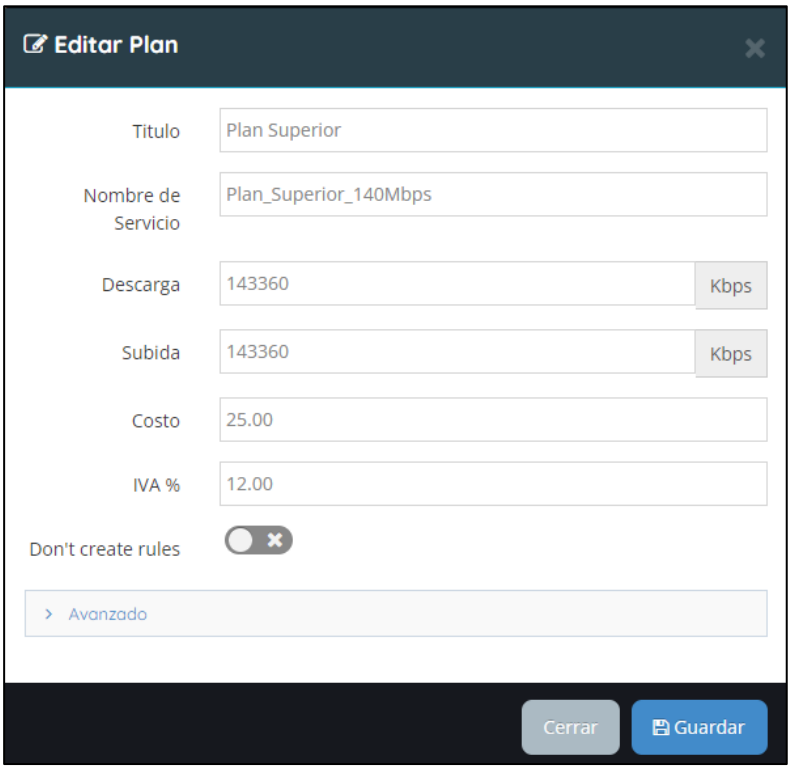
1.5. Configuración de Planes

Los planes corresponden al servicio brindado al cliente, para realizar la configuración de la información se presiona en el menú *Planes → Listar→ Crear Plan*.



Una vez presionado en *Crear Plan* se despliegan los campos correspondientes a: nombre del Plan, Velocidad de Descarga, Velocidad de Subida, Costo, Porcentaje de IVA.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



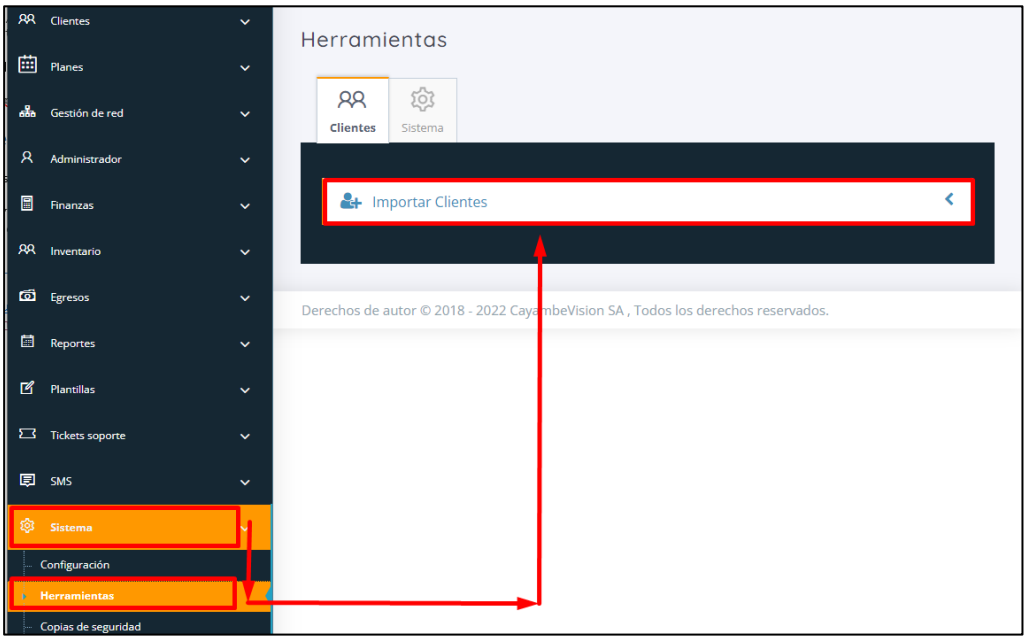
2. Ingreso Clientes

Para el ingreso de Clientes al Sistema de manera rápida se necesita tener actualizada la siguiente información: Nombre, Dirección, IP cliente, Plan, Teléfono, Cédula, Dia de Pago, Correo. Todos estos datos deben estar ingresados en un formato de Excel para posteriormente subirlos al sistema de manera conjunta.

2.1. Importar Clientes

Para importar clientes se debe ingresar a *Sistema→Herramientas→Importar Clientes*

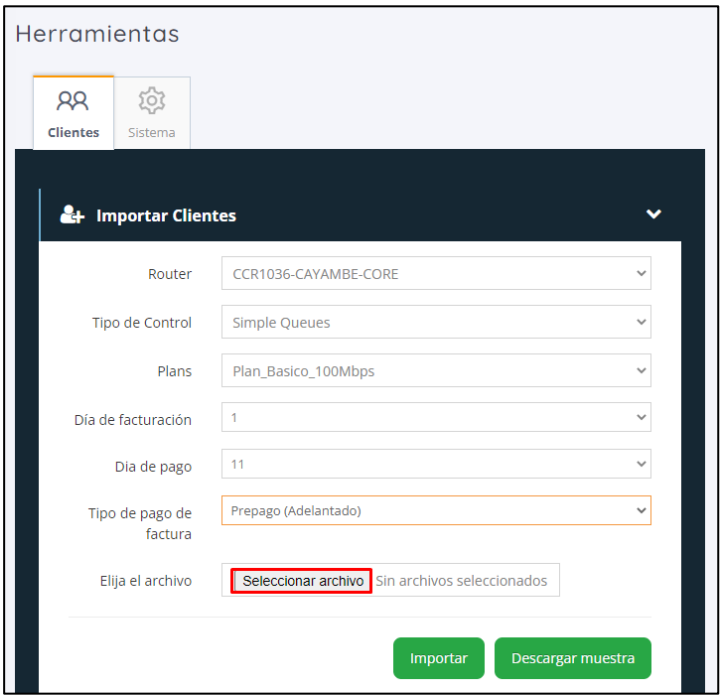
Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



Se ingresa al archivo de Excel en donde se verifica el correcto orden de la información mencionada anteriormente para el perfil del cliente.

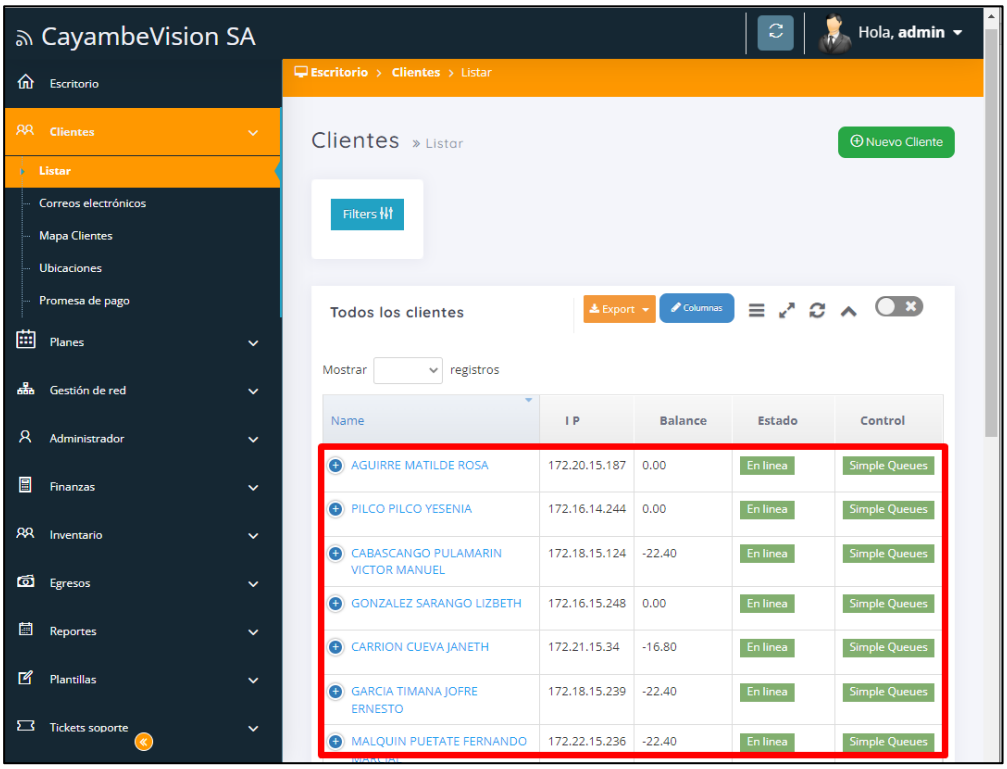
Una vez confirmados los datos se procede a llenar los campos del cuadro siguiente:

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



Se selecciona el Archivo de Excel y se presiona en Importar. Para verificar la importacion de los clientes se ingresa al Menú *Clientes→Listar,* en donde se encuentran los perfiles de clientes importados correctamente.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

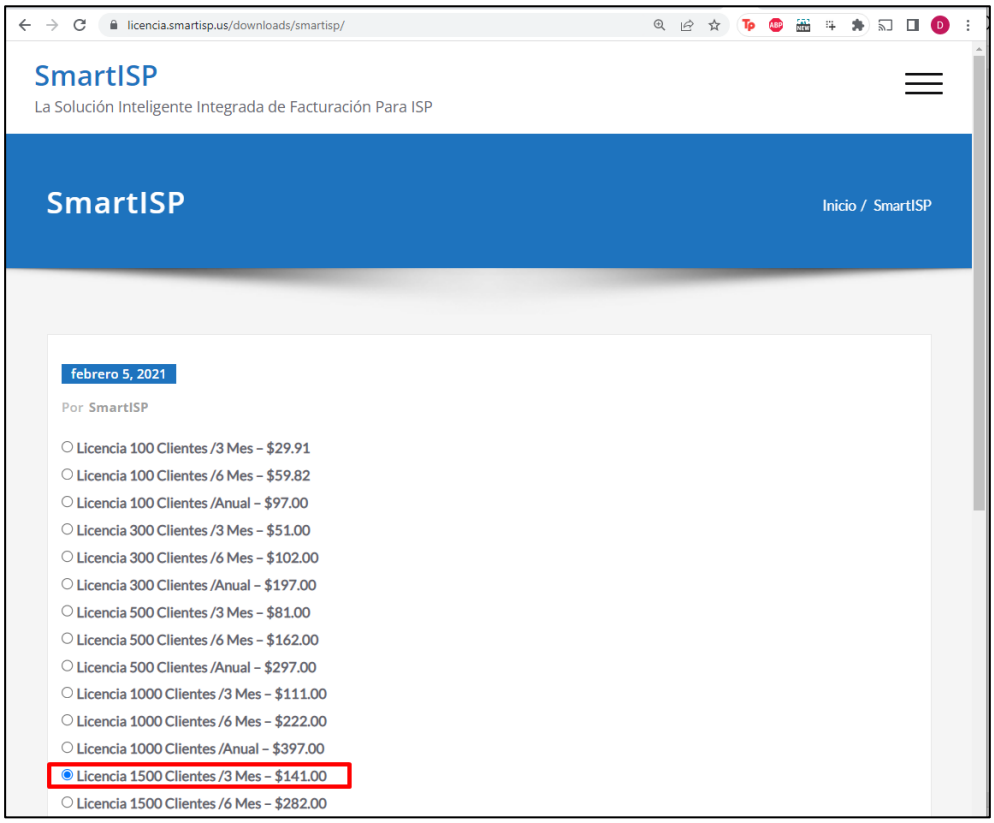


3. Activación de Licencia SmartISP

SmartISP posee una membresía que se renueva cada cierto tiempo, para lo cual la empresa CayambeVision S.A. debido al número de clientes opta por seleccionar el plan de pago cada tres meses con un límite de clientes de 1500 debido a que cubre de manera correcta sus necesidades.

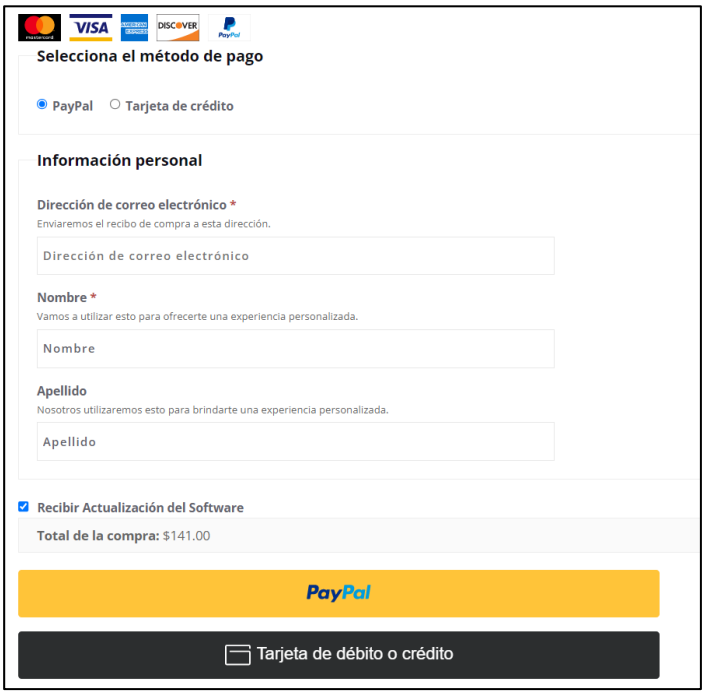
Para la activación de la licencia se debe ingresar a https://licencia.smartisp.us/downloads/smartisp/ en donde se selecciona el plan, una vez seleccionado se despliega hasta la parte inferior de la pantalla y se presiona en “comprar”.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

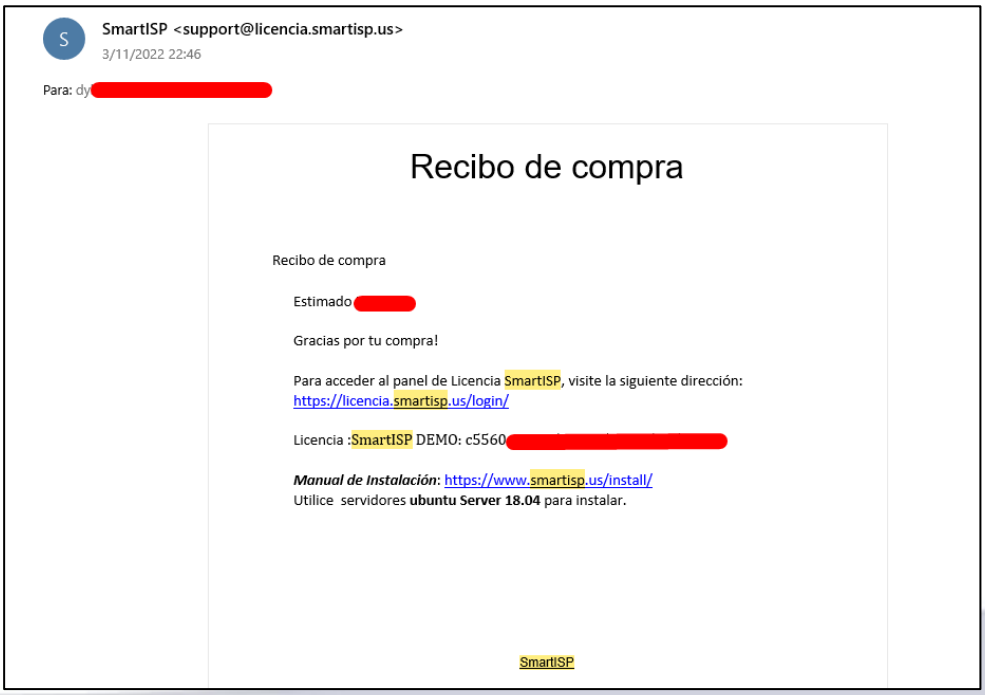


El siguiente paso es ingresar el método de pago, este puede ser ingresando la tarjeta bancaria y pago vía PayPal

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



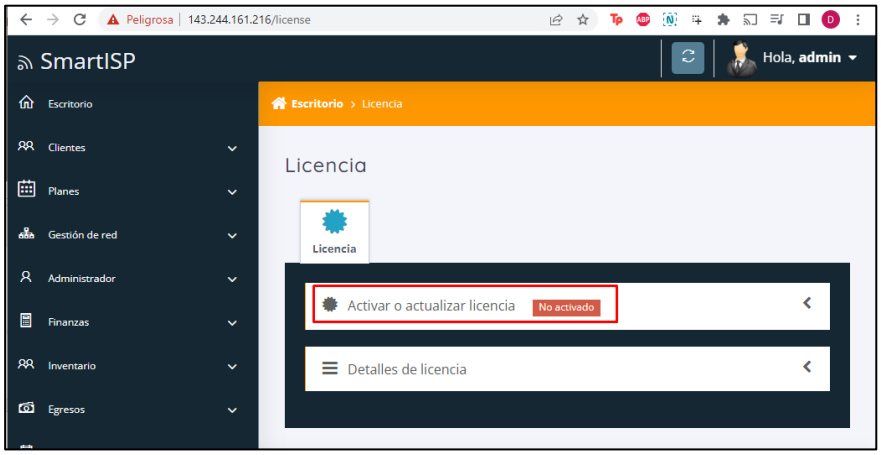
Una vez confirmados los datos de compra, se recibe un correo automático el cual indica la licencia acorde al servicio que se seleccionó con anterioridad.



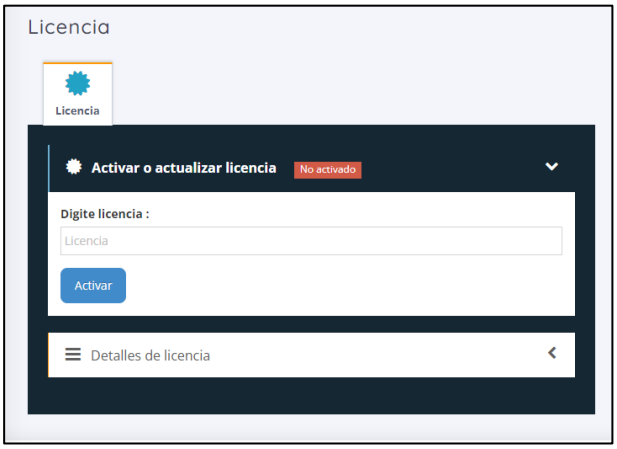
Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

Se procede a copar el código de Licencia para SmartISP y se ingresa al sitio web correspondiente para nuestro servicio de Administración *http://143.244.161.216/admin*.

Establecido el ingreso al Sistema se procede a dirigirse a *Ayuda→Licencia* en donde se presiona en el recuadro rojo mostrado a continuación:

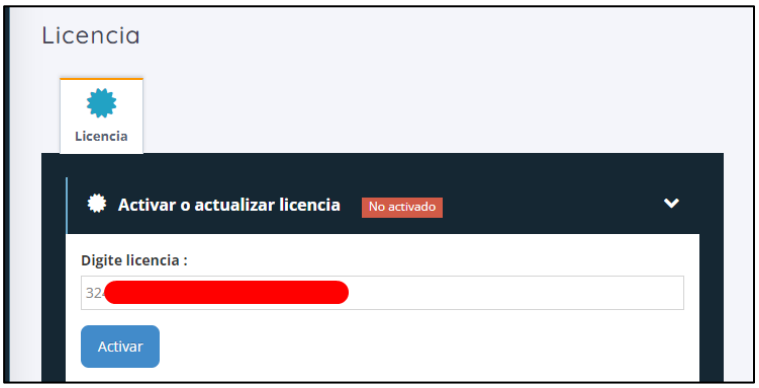


Al momento de presionar se solicita información acerca de la licencia, aquí es donde se ingresa el serial de la Licencia recibido vía correo.

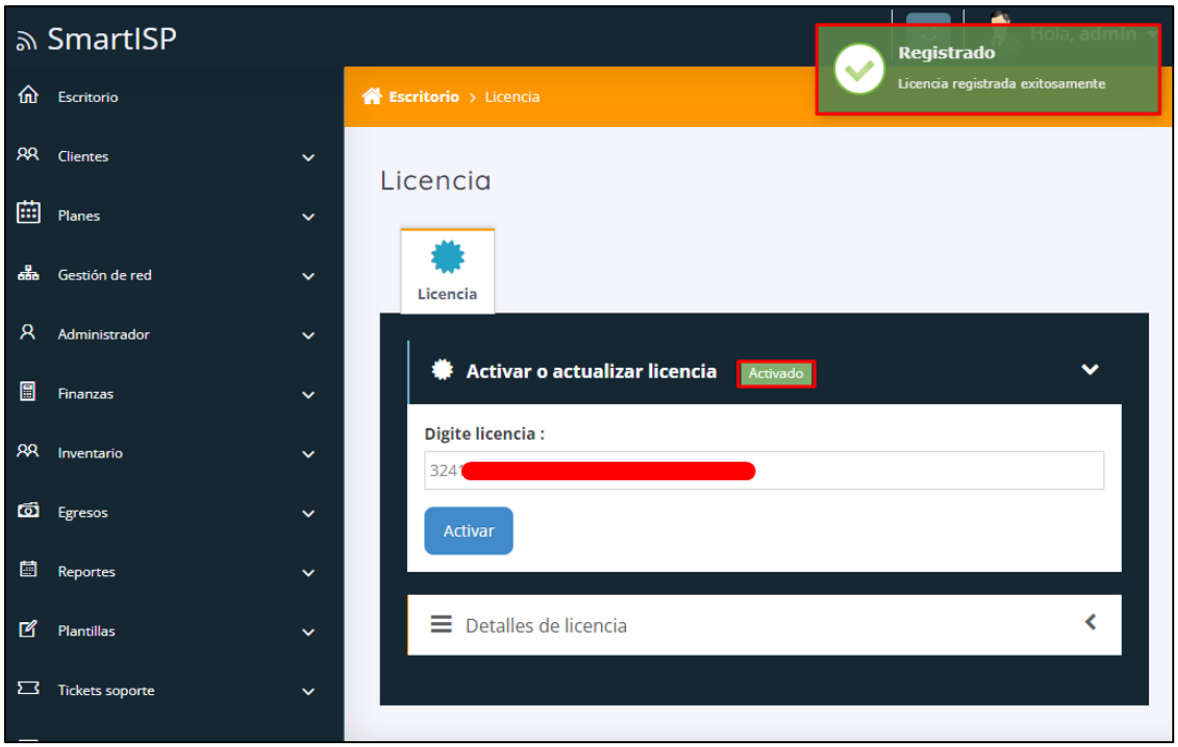


Una vez digitada la licencia de SmarISP se presiona en **Activar**

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251



De esta manera se puede verificar que el estado de la licencia cambia de **No Activado** ha **Activado,** concluyendo así con el despliegue de SmartISP.



ANEXO C

MANUAL DE PROCESOS CAYAMBEVISION S.A.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

MANUAL DE PROCESOS

CAYAMBEVISION S.A.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ÍNDICE DE CONTENIDOS

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ANEXO C1 → CONFIGURACIÓN DE OLT

1. CONFIGURACIÓN DE OLT

1.1. *Ingreso a OLT*

✓ Ingresar el comando `system telnet 172.17.5.2` en la consola de Winbox como se muestra en la Ilustración 1 el cual permite el ingreso hacia la OLT.

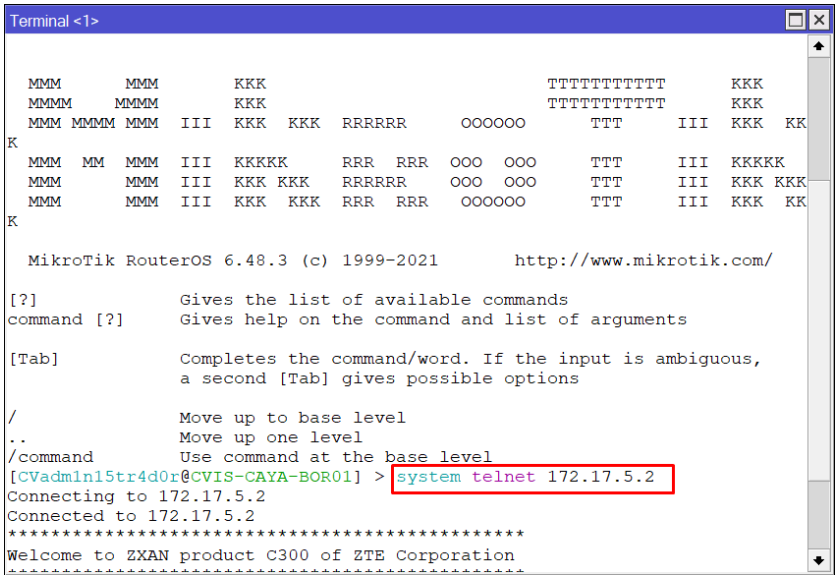


Ilustración 1: Manual - Ingreso a OLT

✓ Establecer el enrutamiento de la red mediante el siguiente comando: `ip route 0.0.0.0 0.0.0.0 172.17.5.1`

✓ Realizar la creación de un nuevo usuario para la administración de la OLT, ingresando el siguiente comando mostrador en la Ilustración 2.

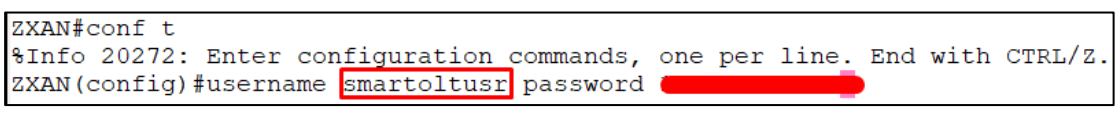


Ilustración 2: Manual: Creación de User OLT

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

✓ Guardar las configuraciones diarias llevadas a cabo hasta las 18:00 ingresando el comando: `auto-write 18:00:00 everyday`

✓ Finalmente, activar el protocolo NTP (Network Time Protocol) y enlazarlo a través de las direcciones IP (`91.189.89.199 y 80.96.196.58`). Estas prioridades de los servidores se las asigna como se muestra a continuación:

```
ntp server 91.189.89.199 priority 1
ntp server 80.96.196.58 priority 2
ntp enable
```

1.2. *Enlace SmartOLT – OLT*

✓ Ingresar al sitio web de SmartOLT mostrado en la Ilustración 3. Mediante el enlace https://cayambevision.smartolt.com/

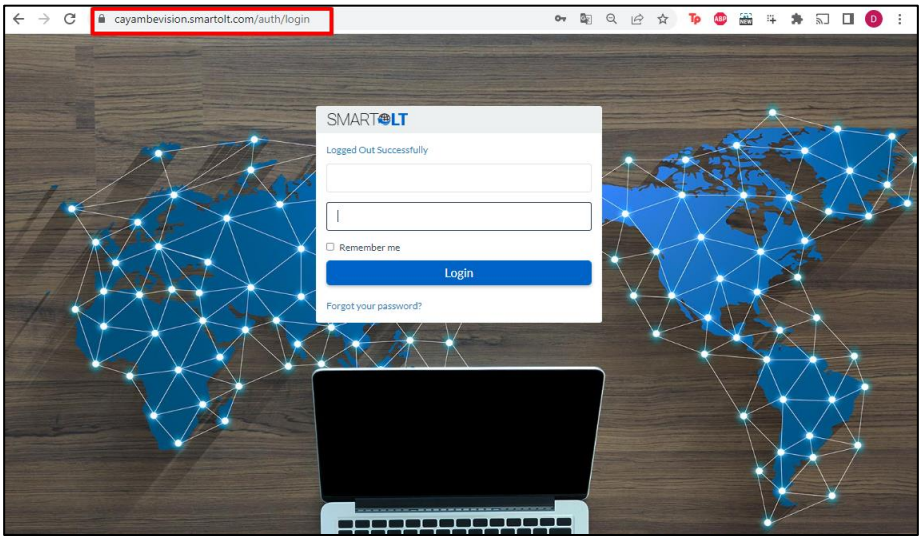


Ilustración 3: Manual - Ingreso a SmartOLT

✓ Realizar la conexión hacia la OLT, para lo cual se dirige al menú Settings→OLT→Create New. Esta acción permite crear un nuevo perfil para la OLT tal como se muestra en la Ilustración 4.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

- **Name: OLT-ZTE300 (Nombre Descriptivo)**
- **OLT IP**: *45.70.202.153 (IP Pública – Acceso Externo)*
- **Telnet TCP port**: *2334 (Puerto Externo - TCP)*
- **OLT telnet username**: *smartoltusr (Usuario SmartOLT)*
- **OLT telnet password:** *xxxxxxxxx (Contraseña Usuario - SmartOLT)*
- **SNMP read-only community:** *xxxxxxxxxx (Comunidad de lectura SNMP)*
- **SNMP read write community**: *xxxxxxxxxx (Comunidad de escritura SNMP)*
- **SNMP UDP port**: *2161 (Puerto Externo - UDP)*
- **IPTV module**: *no (Servicio de IPTV)*
- **OLT hardware *versión:*** *2.x (Versión de OLT)*
- **Type PON:** *GPON (Tipo de Red)*

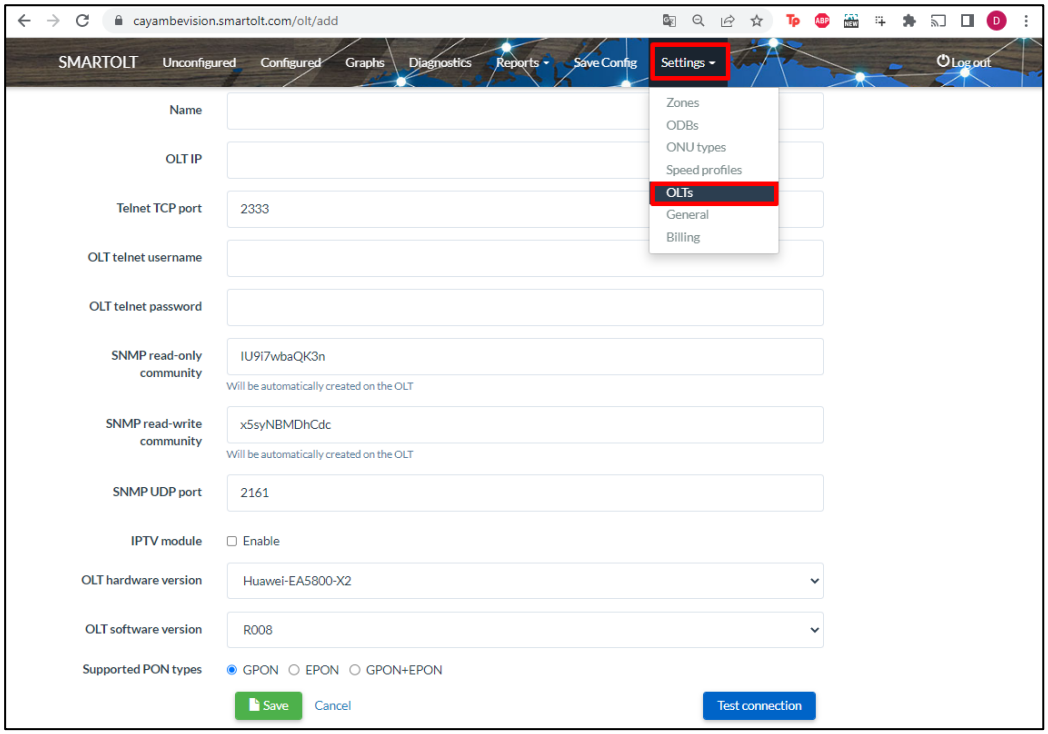


Ilustración 4: Manual: Parametros de Conexión SmartOLT – OLT

✓ Presionar el boton “Test Conection” y se verifica el mensaje mostrado en la Ilustración 5 que menciona “TCP connection on port 2334 successful. UDP conection on

port 2161 successful". El cual confirma que se ha realizado correctamente la conexión entre SmartOLT y la OLT.

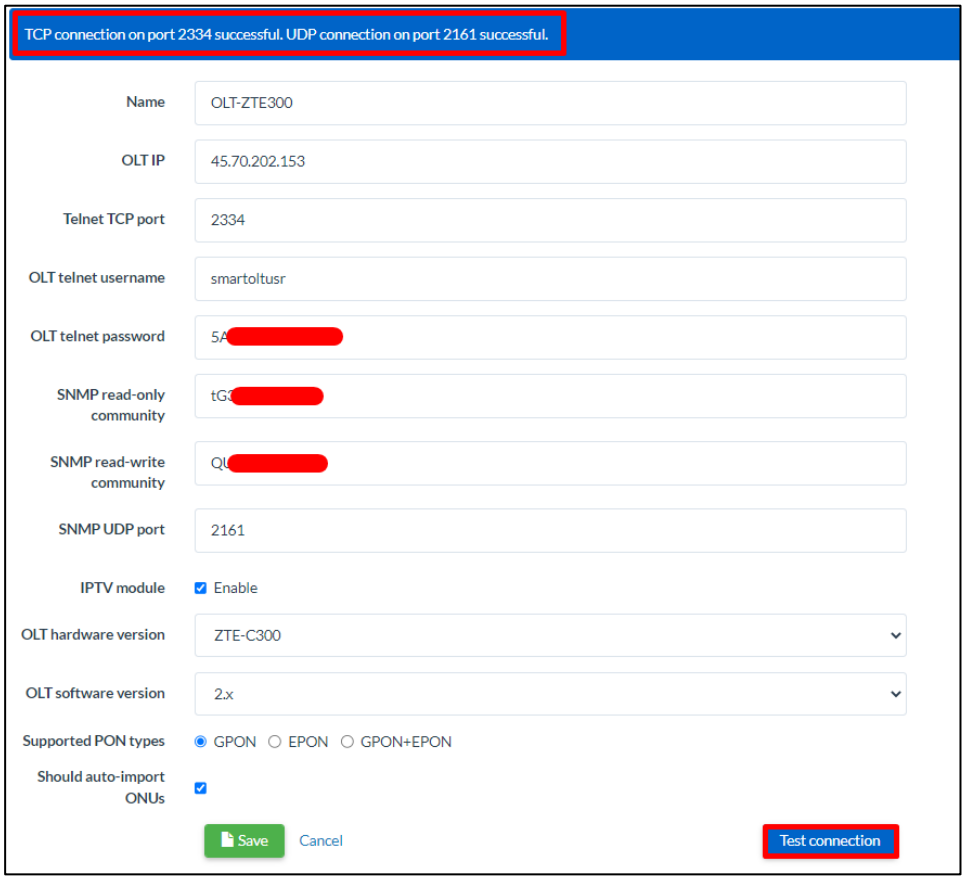


Ilustración 5: Manual: Mensaje de Conexión

1.3. *Creación de Perfil ONU/ONT*

✓ Ingresar a Settings → ONU Types → Add ONU Type, como se muestra en la Ilustración 6. En donde se listan todos los tipos de ONUs creados por defecto por parte del sistema.

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

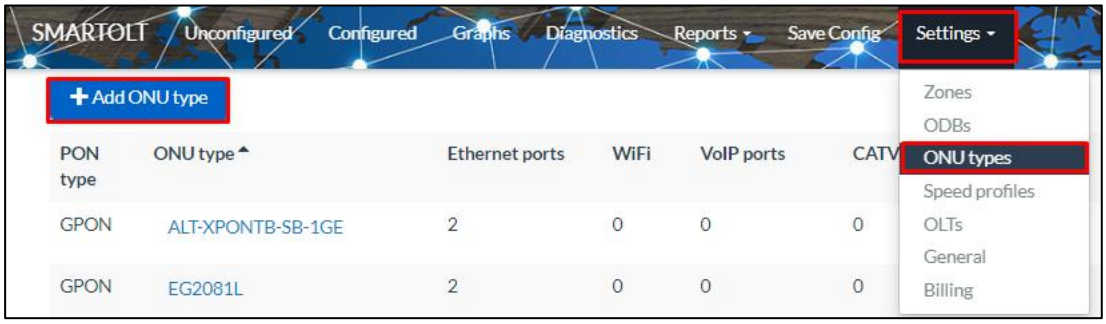


Ilustración 6: Manual: Configuración Perfil ONT/ONU

✓ Llenar los parámetros mostrados en la Ilustración 7 de la siguiente manera:

- **PON type:** GPON (Tipo de Tecnología FTTH de trabajo)
- **ONU type:** EG2081L (Modelo de ONT)
- **Ethernet ports:** 4 (Numero de puertos físicos ethernet)
- **Wifi SSIDs:** 0 (Numero de nombres para red WLAN)
- **VoIP ports:** 0 (Numero de puertos para telefonía)
- **CATV:** no (Puerto de conexión coaxial)
- **Capability:** Bridging (Capacidad para trabajar modo puente/enrutamiento)

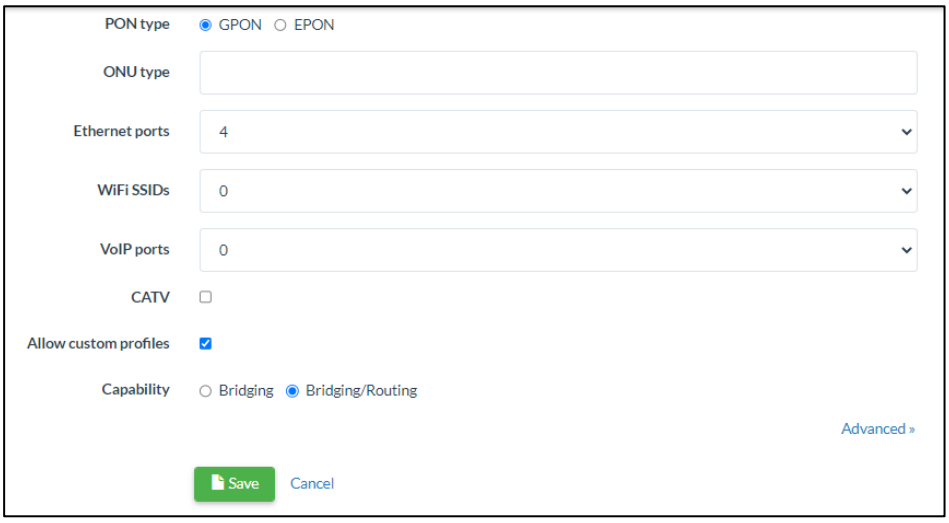


Ilustración 7: Manual: Parámetros de Perfil ONU/ONT

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

1.4. *Creación de Planes de Velocidad*

✓ Ingresar al menú *Settings* → *Speed profiles* → *Add speed profile* como se muestra en la siguiente Ilustración 8.

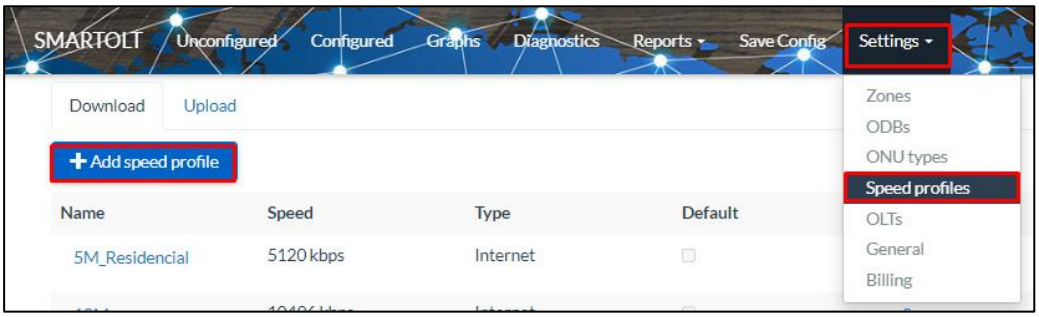


Ilustración 8: Manual: Configuración de Perfil de Velocidad

✓ Colocar los datos correspondientes a la velocidad dowload en kbps como se muestra en la Ilustración 9.

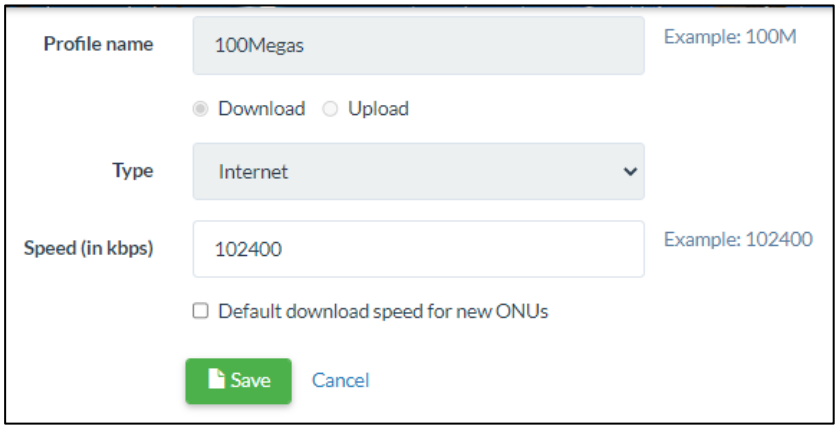


Ilustración 9: Manual: Velocidad Download

✓ De igual manera para el perfil de Upload se realiza el mismo procedimiento. Ilustración 10.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

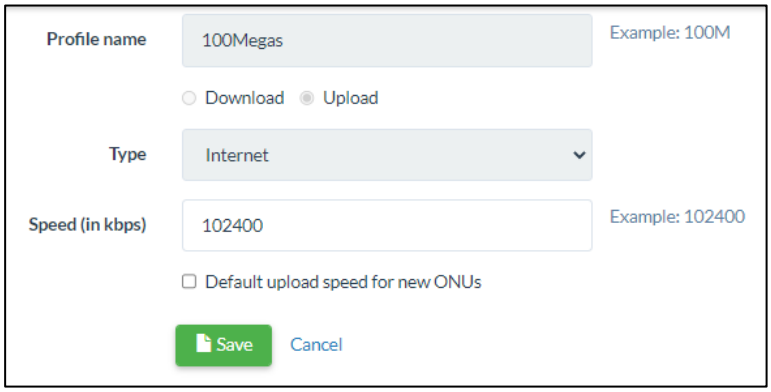


Ilustración 10: Manual: Perfil de Velocidad Upload

1.5. *Creación de VLANS*

✓ Para la creación de una nueva VLAN se ingresa al menú Settings→OLT→VLANs, y se procede a crear un nuevo ID de vlan acorde a lo que se requiera en la red.

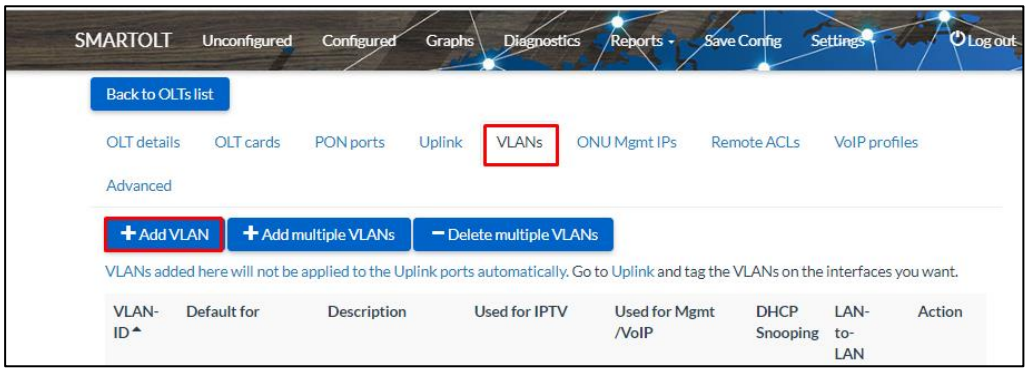


Ilustración 11: Manual: Creación de VLANs

✓ Se procede a ingresar los datos de la VLAN y se procede a aceptar. Ilustración 12.

Ilustración 12: Manual: ID de VLAN

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ANEXO C2 → INGRESO DE CLIENTES (ONU-ONT) – SMARTOLT

2. INGRESO CLIENTES – SMARTOLT

2.1. *Identificar ONU/ONT Cliente*

✓ Identificar al equipo que se busca ingresar mediante el tipo de ONT/ONU, SN (Serial Number) y el estado de Autorización.

✓ Una vez identificado el equipo se presionar en "Autorizar", de esta manera se ingresa a los parámetros de configuración de la ONT. Ilustración 13.

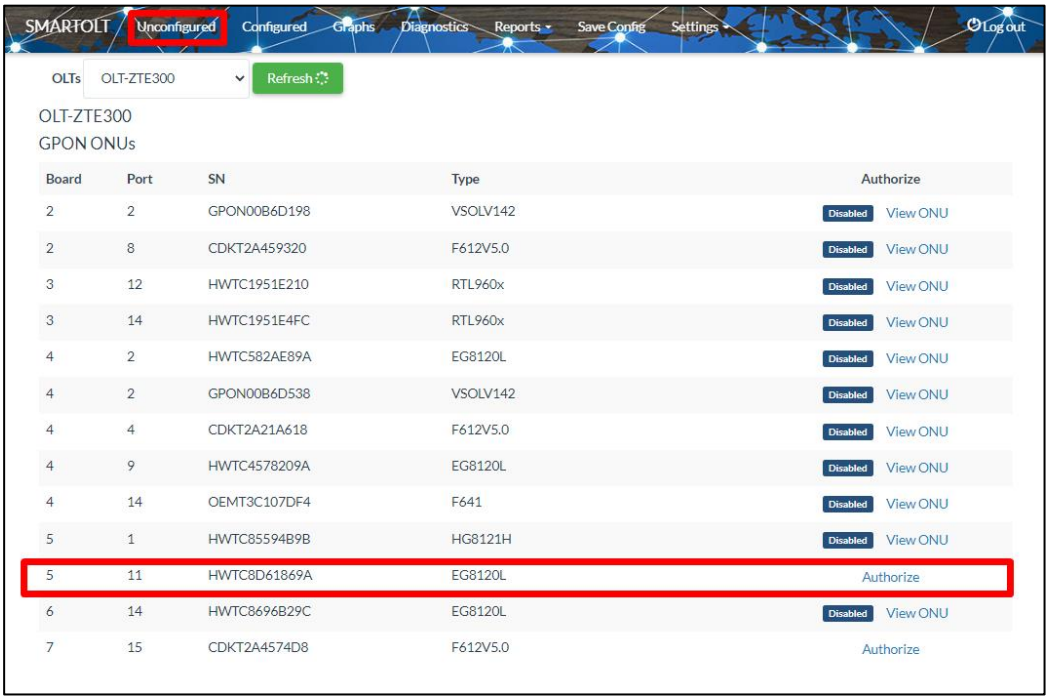


Ilustración 13: Manual: Autorización de ONT/ONU

2.2. *Ingresar datos en perfil de Cliente*

✓ En el perfil del cliente se procede a llenar los datos mostrados en la Ilustración 14, de la siguiente manera:

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

- **Board:** 5 (Número de tarjeta destinado para el cliente)
- **Port:** 11 (Numero de Puerto destinado para el cliente)
- **SN:** HWTC8061869A (Número Serial del equipo)
- **ONU type:** ZTE-F668 (Perfil de modelo ONT)
- **ONU mode:** Routing (Modo de trabajo del equipo routing/bridging)
- **Use VLAN ID:** 16-VLAN16 (Vlan asignada para el quipo)
- **Zone:** Zona 1 (Zona referencial a la ubicación del equipo)
- **ODB Splitter:** None (Caja de Distribución de Fibra Óptica)
- **Download Speed:** Estudiantil_15M (Perfil destinado al tráfico de descarga)
- **Upload Speed:** Estudiantil_15M (Perfil destinado al tráfico de subida)
- **Name:** EQUIPO DE PRUEBA (Nombre del usuario cliente)
- **Address or comment:** (Dirección referencial a la ubicación del cliente)

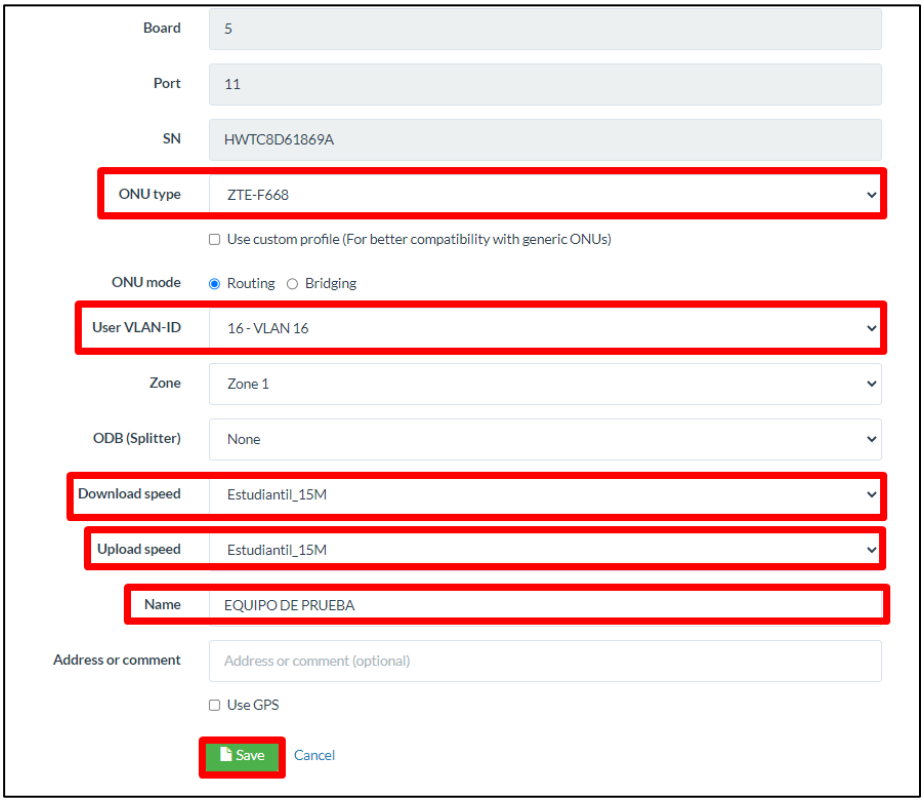


Ilustración 14: Manual: Perfil de Cliente

✓ Una vez finalizado el proceso, se procede a guardar presionando en “Save”.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ANEXO C3 → ESTADO DEL CLIENTE

3. ESTADO DEL CLIENTE

3.1. *Filtrar Cliente*

✓ Para realizar el filtrado de un cliente se procede a ingresar a la pestaña de "Configured" en donde se muestran los equipos previamente activados.

✓ Ingresar el nombre que se desea filtrar en el campo de "Search". Estos pasos anteriores se muestran en la Ilustración 15.

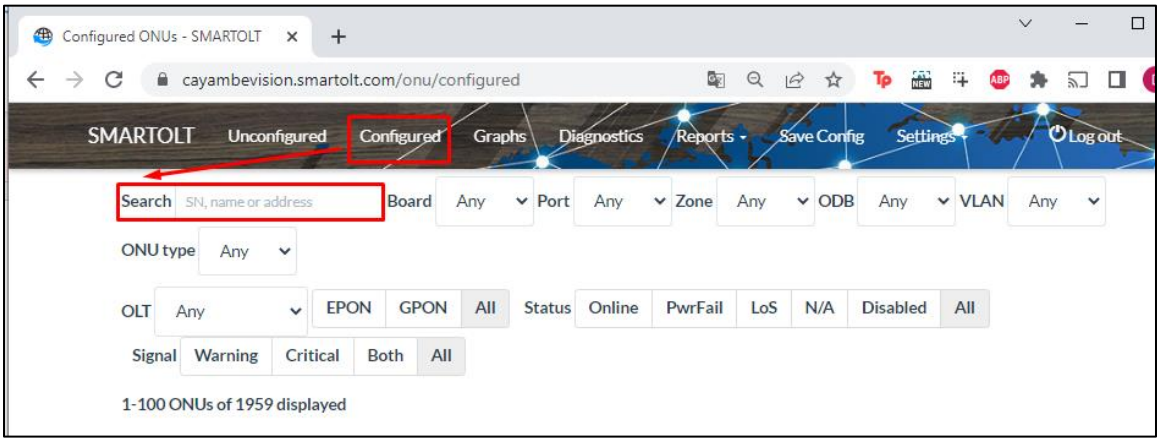


Ilustración 15: Manual: Filtrar Cliente

3.2. *Verificar Estado*

✓ Identificar al equipo que se desea verificar el estado, como se muestra en la Ilustración 16.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

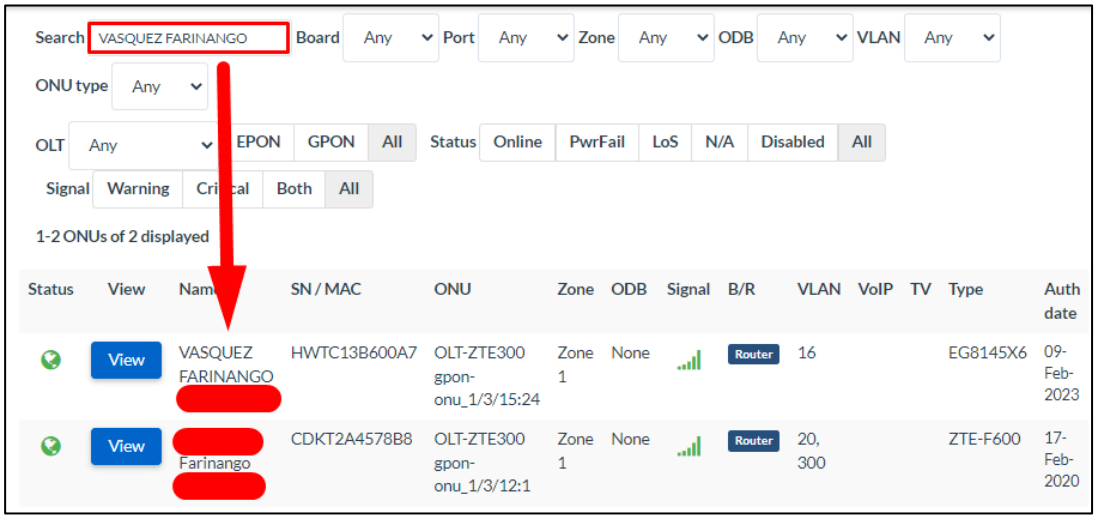


Ilustración 16: Manual: Filtrado de Cliente

✓ Verificar el estado del cliente

NOTA: El estado del cliente puede presentar tres variaciones distintas, entre estas se puede tener: Equipo en línea, Equipo Apagado, Equipo desenganchado.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ANEXO C4 → INGRESO DE CLIENTES – SMARTISP

4. INGRESO DE CLIENTES SMARTISP

4.1. *Crear perfil de Cliente*

✓ Ingresar al Sistema SmartISP mediante la siguiente ULR: 143.244.161.216/admin, mostrada en la Ilustración 17.

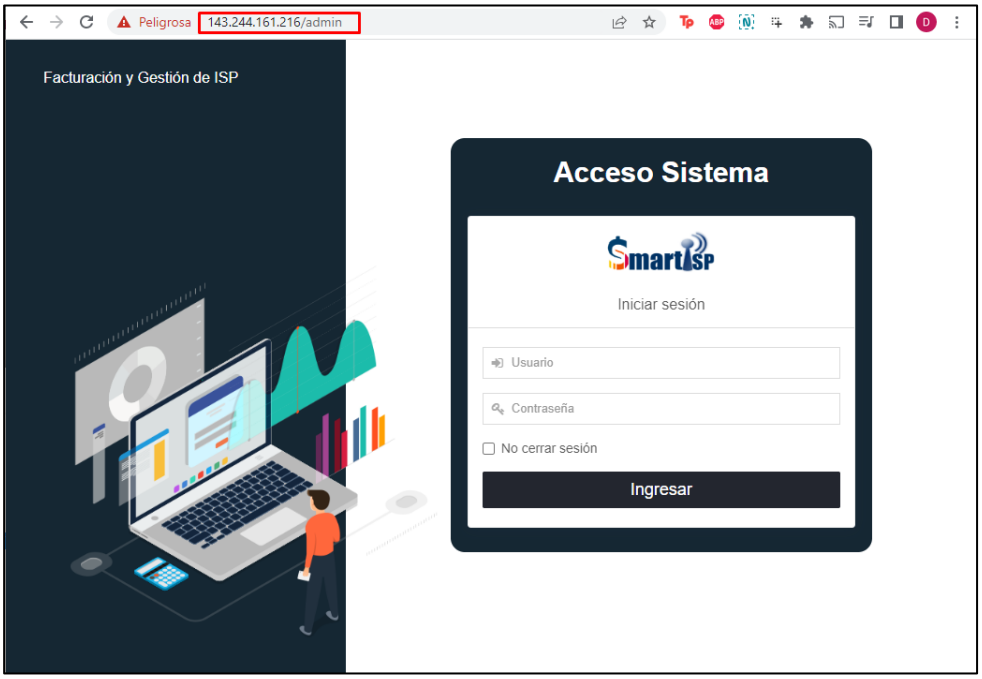


Ilustración 17: Manual: Ingreso SmartISP

✓ Para realizar el ingreso de un nuevo cliente en SmartISP, dirigirse al menú Cliente→Listar→Nuevo Cliente, como se muestra en la Ilustración 18

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

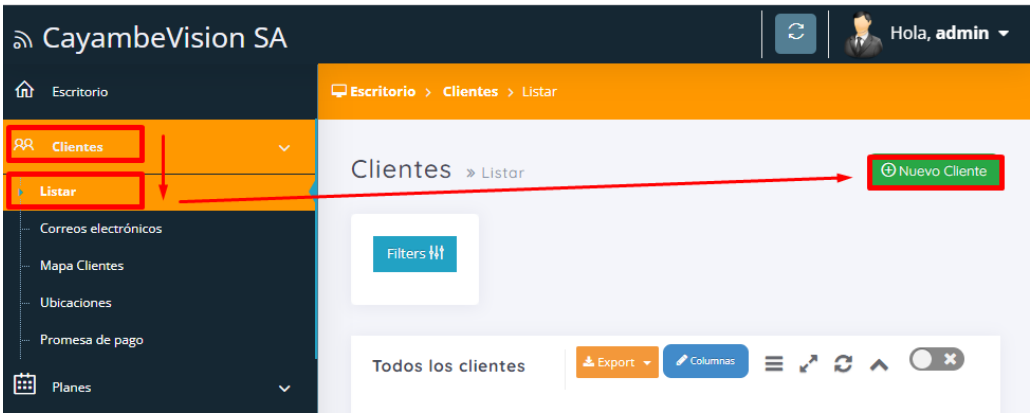


Ilustración 18: Manual: Creación de Perfil Cliente SmartISP

✓ Llenar la información de cliente solicitada mediante la ficha mostrada en la Ilustración 19.

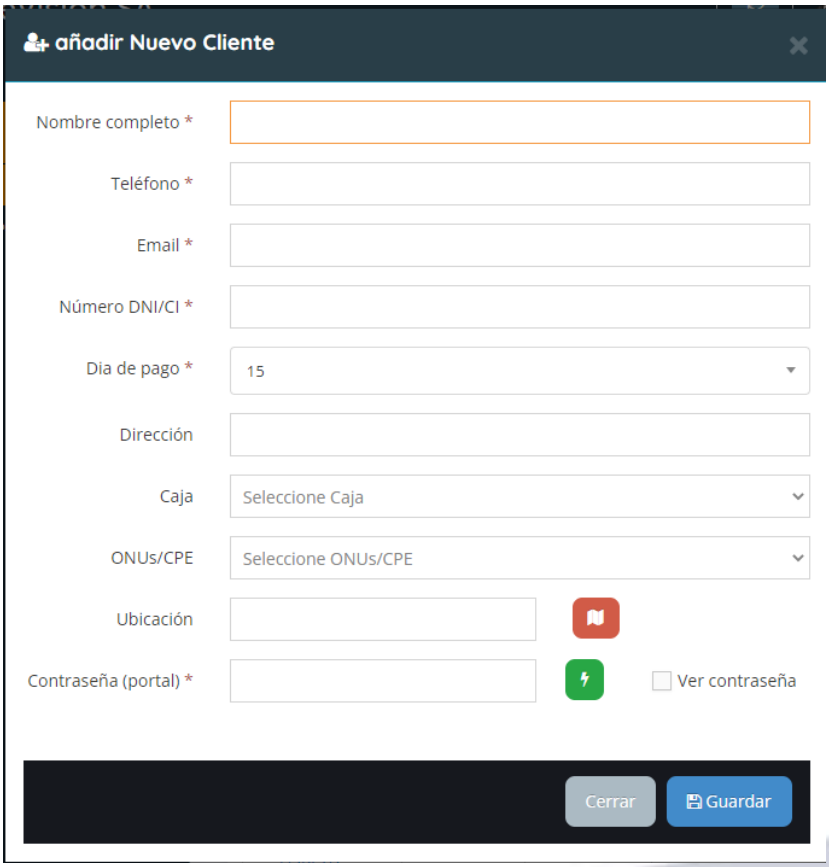


Ilustración 19: Manual: Información Cliente

4.2. *Asignar Servicio*

✓ Asignar el servicio contratado ingresando en el perfil del cliente y dirigiéndose a la pestaña "Servicio". Como se evidencia en la Ilustración 20.

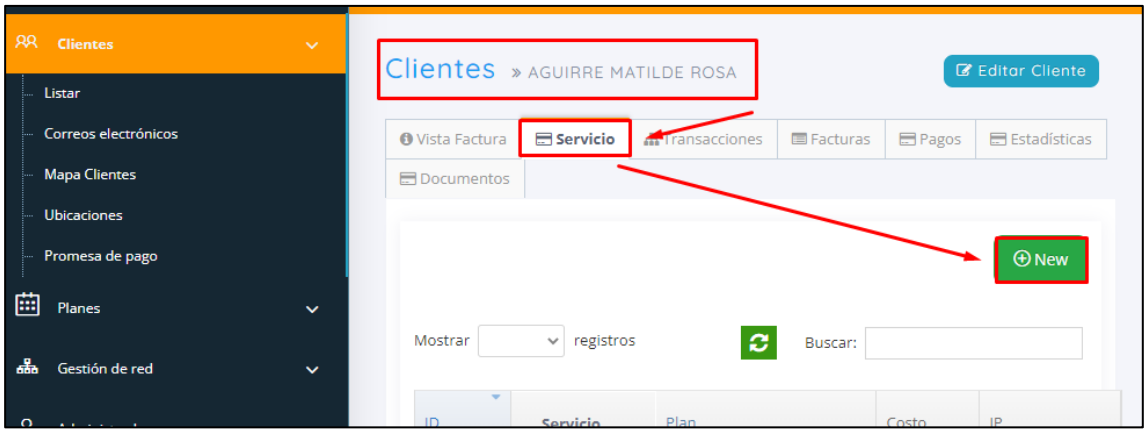


Ilustración 20: Manual: Asignación de Servicio

✓ Añadir un nuevo servicio para el cliente.

✓ Llenar todos los datos solicitados y finalizar presionando en el botón "Guardar". Ilustración 21.

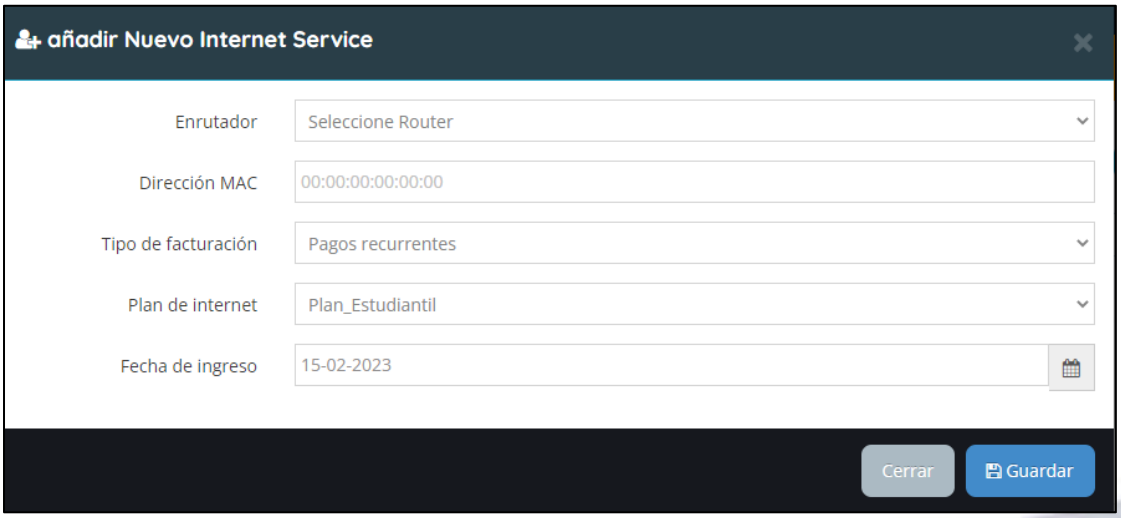


Ilustración 21: Manual: Creación de Servicio

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ANEXO C5 → PAGO DE SERVICIO

5. PAGO DE SERVICIO

5.1. *Filtrar Cliente*

✓ Para registrar el pago de un nuevo cliente, se procede a ingresar al Sistema SmartISP mediante la URL: 143.244.161.216/admin, mostrada anteriormente en la Ilustración 17.

✓ Una vez ingresado al sistema, dirigirse al menú: Cliente→Listar→Filtrar. Este proceso se evidencia en la Ilustración 22.

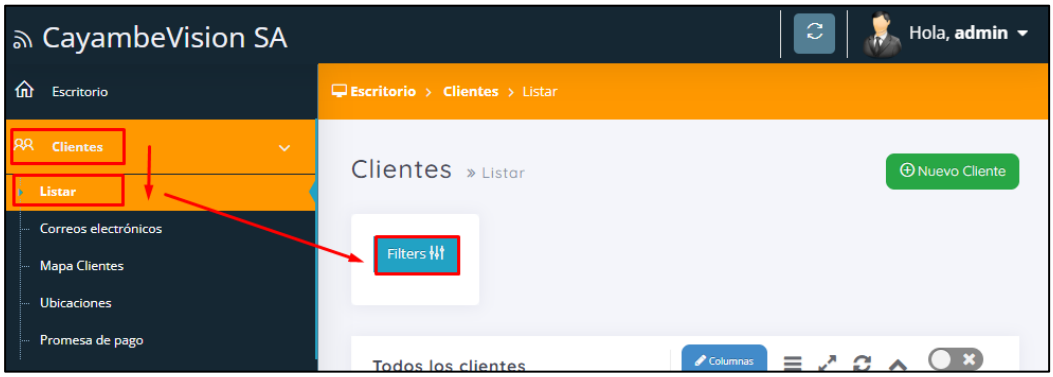


Ilustración 22: Manual: Filtrado de Cliente – SmartISP

✓ Para filtrar al cliente por el nombre se llena el campo mostrado en la Ilustración 23. Una vez llenado el campo se presiona en el Botón "Filtrar".

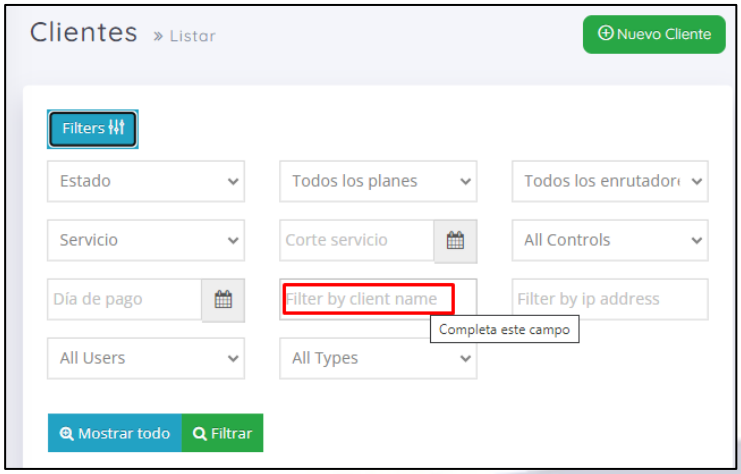


Ilustración 23: Manual: Filtrado de cliente

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

✓ Una vez filtrado el nombre del cliente, se identifica el perfil y se procede a ingresar, como se muestra en la Ilustración 24.

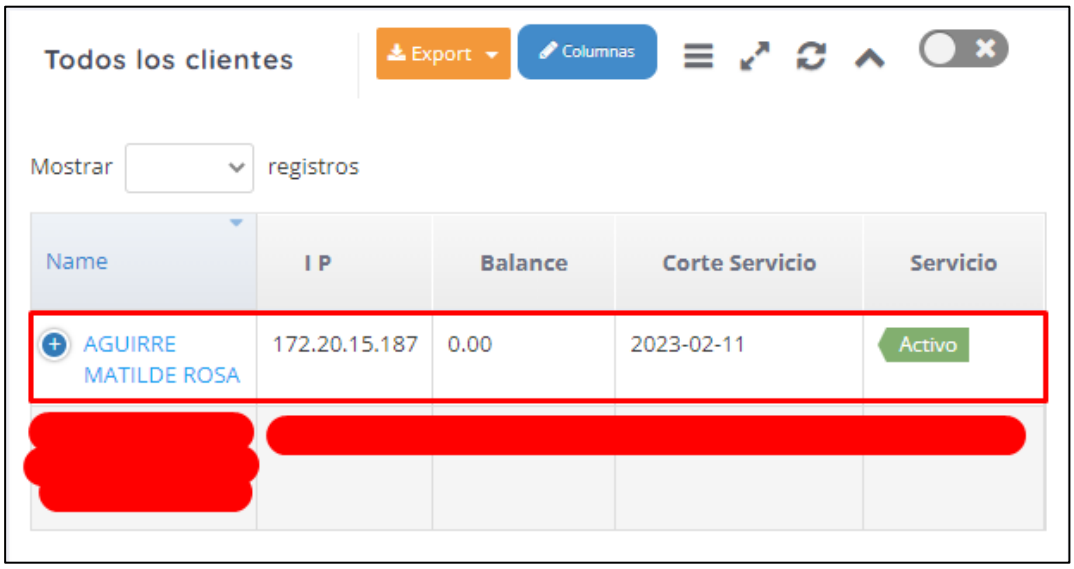


Ilustración 24: Manual: Filtrado e ingreso perfil

5.2. *Ingreso a Facturación*

✓ Ingresar al perfil del cliente

✓ Para revisar las facturas pendientes por cobrar del cliente, se dirige a la pestaña "Facturación", proceso mostrado en la Ilustración 25.

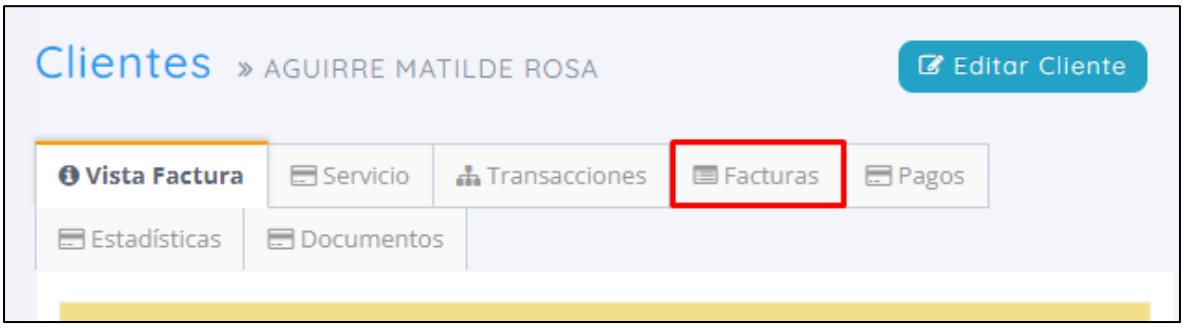


Ilustración 25: Manual: Ingreso a Facturas

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

5.3. *Registrar Pago*

✓ Identificar la factura que se desea registrar el pago. Ilustración 26.

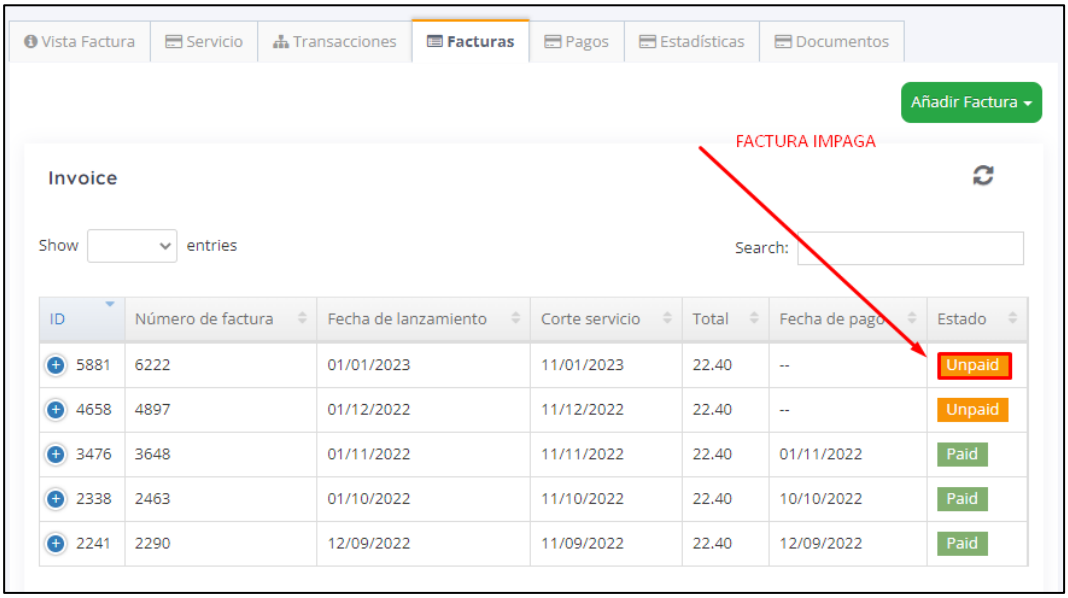


Ilustración 26: Manual: Identificar Factura a Pagar

✓ Para realizar el pago una vez identificada la factura a pagar, se procede a ingresar presionar en la factura y posterior a eso se presiona en el icono de "visto", para pagar el servicio. Proceso mostrado en la Ilustración 27.

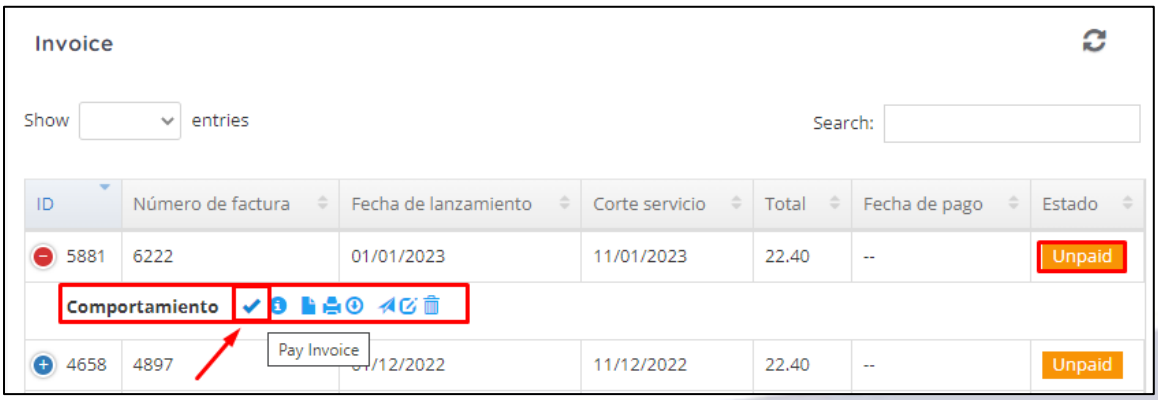


Ilustración 27: Manual: Pago de Factura

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

✓ Completar el pago seleccionando la forma de pago preferente del cliente y presionando finalmente en el botón "Guardar". Ilustración 28.

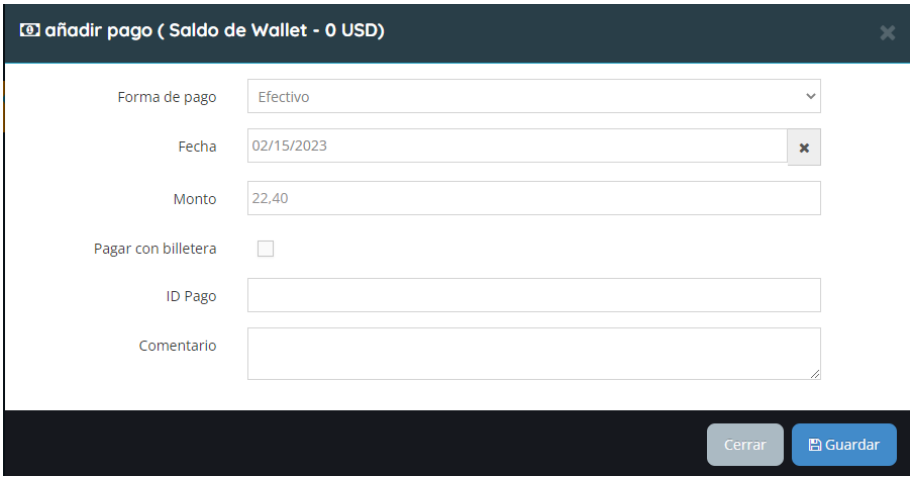


Ilustración 28: Manual: Ingreso de Pago

5.4. *Generar Factura*

✓ Una vez realizado el pago se procede a generar el comprobante de pago, para esto se ingresa nuevamente en la factura y se selecciona la opción mostrada en la Ilustración 29.

Ilustración 29: Manual: Generación de Factura

CAYAMBEVISION
TELECOMUNICACIONES

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

ANEXO C6 → GENERACIÓN DE TICKETS DE SOPORTE

6. GENERACIÓN DE TICKETS DE SOPORTE

6.1. *Verificar Estado del Cliente*

✓ Inicialmente se verifica el estado del cliente siguiendo la guía del proceso anteriormente mostrado en la Página 266 referente a la verificación de estado del cliente en el servicio de SmartOLT.

✓ Una vez identificado el estado del cliente, se procede a ingresar al sistema de SmartISP para posteriormente agendar el ticket de soporte.

6.2. *Generar Ticket de Soporte*

✓ Para generar un nuevo ticket de soporte se ingresa al menú Tickets→Listar→Crear Nuevo. Este proceso se puede identificar en la Ilustración 30.

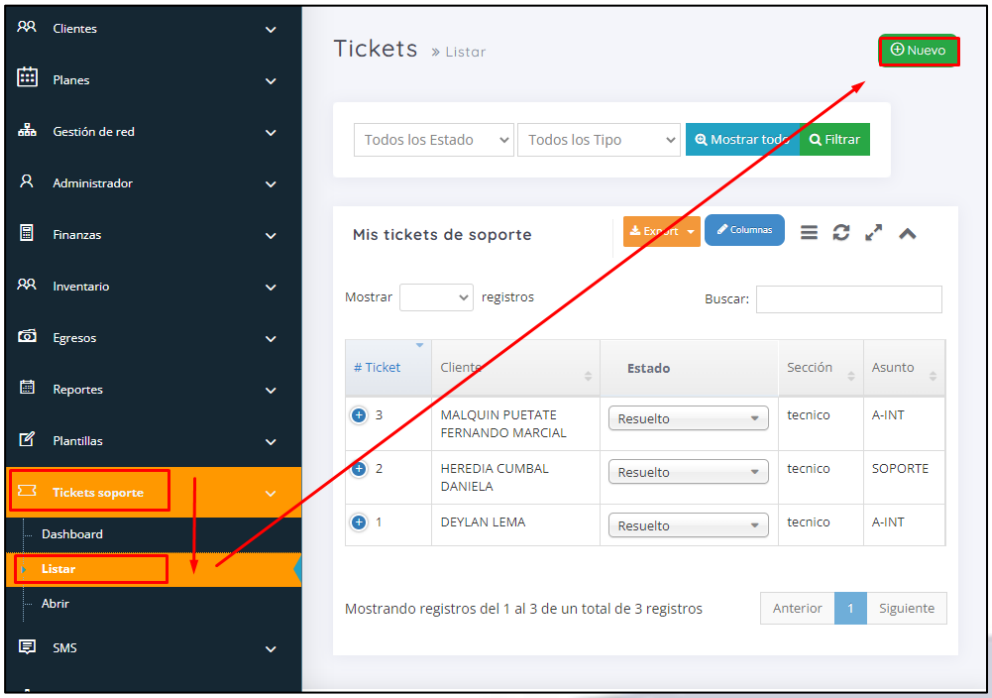


Ilustración 30: Manual: Ingreso a Tickets

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

✓ Para abrir un nuevo Ticket es necesario llenar los campos que se solicitan, como se muestra en la Ilustración 31 como un ejemplo.

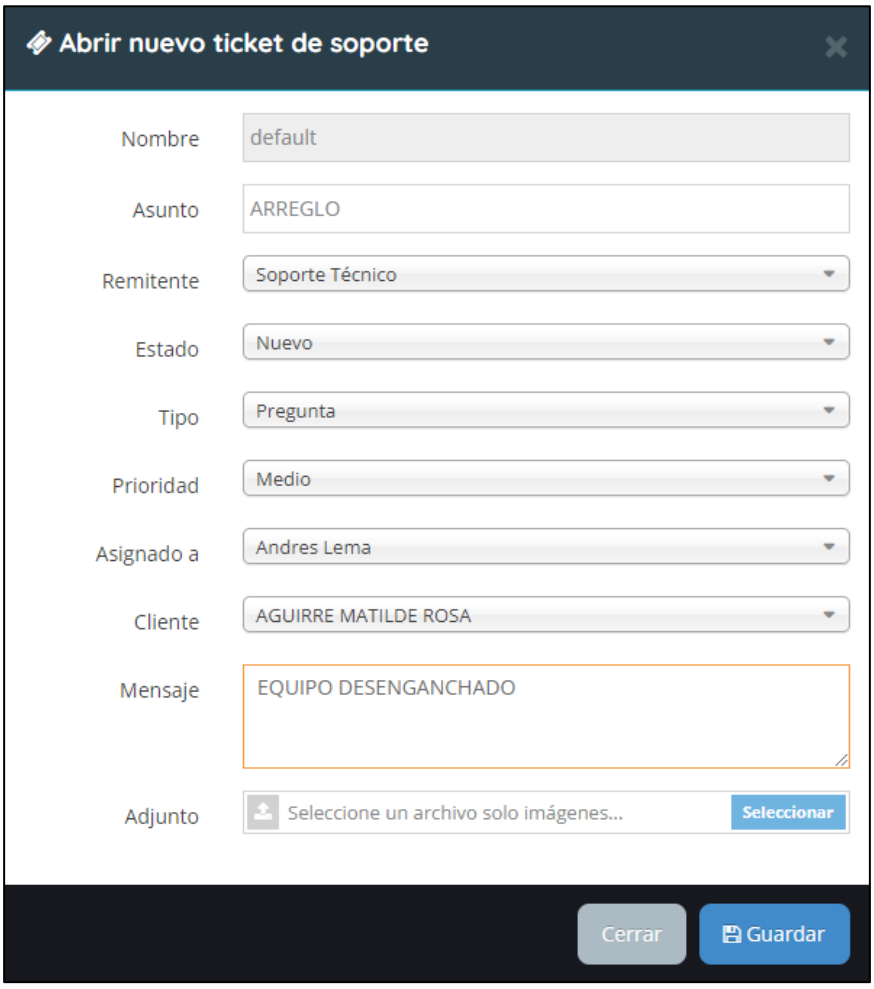


Ilustración 31: Manual: Generación de Ticket

✓ Presionar en "Guardar" para finalizar el proceso.

6.3. *Verificar estado de Ticket de Soporte*

✓ Ingresar al menú Tickets→Listar, en la Ilustración 32 se refleja la lista de actividades creadas y sus respectivos estados.

Cayambe:
Terán N3-76 y 24 de Mayo
022 364 251

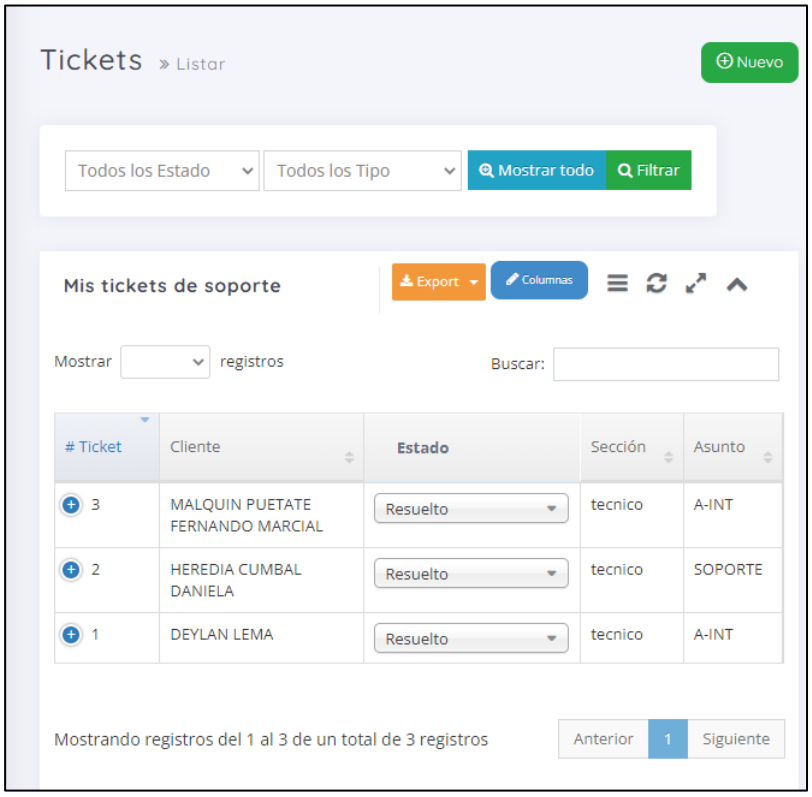


Ilustración 32: Manual: Verificación de estado de Ticket