UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA ELECTRÓNICA

Memoria Laboral

"Implementación y Migración de un Sistema de Nombres de Dominio en el Backbone Internet de Telecel S.A."

Postulante: Hans Paul Zizold Delgado

Asesor: Ing. Julio Cesar Uberhuaga Conde

LA PAZ – BOLIVIA

2023

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERIA

LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

Implementación y Migración de un Sistema de Nombres de Dominio en el Backbone Internet de Telecel S.A.

Postulante: Hans Paul Zizold Delgado
Dirección: Calle México # 1790. Ed. María Reyna. Cel: 77290032.

El propósito principal del proyecto fue implementar y migrar un nuevo Sistema de Nombres de Dominio (DNS) en el Backbone Internet de Telecel S.A., buscando optimizar la confiabilidad y calidad en los servicios de Internet Móvil y Fijo del ISP.

Para lograrlo, se diseñó una estrategia técnica que contempló tanto la implementación en la red del ISP como la migración y puesta en marcha del nuevo sistema. Durante el proyecto, se midieron indicadores clave de rendimiento para evaluar las mejoras en la resolución DNS.

El proyecto se estructuró en tres fases:

Fase de Implementación: preparación de la infraestructura virtual y aseguramiento de la conectividad necesaria.

Fase de Pruebas Preproducción: validación de funcionalidad y rendimiento en ambientes controlados.

Fase de Migración o Puesta en Producción: implementación gradual del nuevo sistema minimizando impactos a los usuarios.

Las tres fases se completaron con éxito, gracias a la meticulosa planificación y el tiempo invertido en el diseño de la estrategia técnica que tuvieron como resultado una transición fluida entre sistemas. Este proceso de modernización incorporó mejoras tecnológicas como la implementación de una infraestructura virtual para el DNS, resultando en una solución más ágil y adaptable. En términos de rendimiento, se observaron tiempos de resolución consistentes y mejorados, beneficiando la experiencia del usuario en el consumo de los servicios de Internet Móvil y Fijo.

En conclusión, se alcanzaron los objetivos propuestos y el proyecto se completó exitosamente. Esta experiencia dejó valiosas lecciones en planificación, coordinación y colaboración entre los equipos involucrados. Con esta nueva implementación, Telecel S.A. ha establecido un pilar sólido para futuras optimizaciones de DNS, posicionándose a la vanguardia en un entorno tecnológico en evolución.

Tabla de contenido

Índice de Ilustraciones

Índice de Tablas

1. INTRODUCCIÓN

1.1 RESUMEN DE LA ACTIVIDAD LABORAL

Mi historia laboral comenzó en mayo de 1997, cuando ingresé a formar parte del equipo técnico de la empresa **Telecel S.A**[1]. Trabajé en esta compañía durante un lapso de 24 años, desempeñando diferentes posiciones, las cuales resumo a continuación.

Mi primer rol fue como ingeniero en el **Centro de Operación y Mantenimiento**, con el objetivo de monitorear la Red de Telefonía Celular a nivel nacional las 24 horas del día, los 7 días de la semana, así como de ejecutar tareas de operación y mantenimiento.

Posteriormente, en abril de 1999, fui asignado al puesto de **Ingeniero de Conmutación**, concentrándome exclusivamente en las tareas de operación y mantenimiento de la Red de Telefonía Celular en la ciudad de La Paz.

En febrero de 2007, fui promovido al puesto de **Supervisor de Conmutación** con alcance a nivel nacional, con el objetivo de operar y mantener los sistemas a cargo, así como de supervisar y dirigir al personal bajo mi responsabilidad.

En noviembre de 2008 fui promovido al puesto de **Responsable de Operación y Mantenimiento de las áreas de CORE[2] y VAP**[3], rol con alcance a nivel nacional. Además del área de **Conmutación**, tuve a cargo las áreas de operación y mantenimiento de los **Sistemas de Valor Agregado** y las **Controladoras de Radio Base**.

En mayo de 2011, después de una profunda restructuración en el área técnica, fui reasignado como **Responsable de Aseguramiento de Servicio de las áreas de CORE e IP**, como parte de la gerencia de **Aseguramiento de Servicio**. Mantuve responsabilidades

[1] TELECEL S.A., comercialmente conocida como TIGO, es una empresa que provee servicios de telecomunicaciones en Bolivia, siendo los principales Telefonía Móvil y el acceso a Internet Domiciliario.
[2] El termino CORE se refiere a los equipos centrales en una red. Para este caso se refiere a las Centrales de Conmutación y a las Controladoras de Radio Base de la red de Telefonía Móvil.
[3] El termino VAP se refiere a las Plataformas de Valor Agregado, como ser sistemas de tarifación en tiempo real, mensajería instantánea o casillas de voz, entre otros.

similares, pero con la diferencia de que se creó un área especializada en **Redes IP**, mientras que el área de **Servicios de Valor Agregado** pasó a otro mando.

1.2 INGENIERO DE CENTRO DE OPERACIÓN Y MANTENIMIENTO

1.2.1 ORGANIZACIÓN

Este puesto fue desempeñado en la empresa Telecel S.A., en el área técnica encargada de la operación y mantenimiento de una red de telefonía celular en el periodo desde mayo de 1997 hasta abril de 1999.

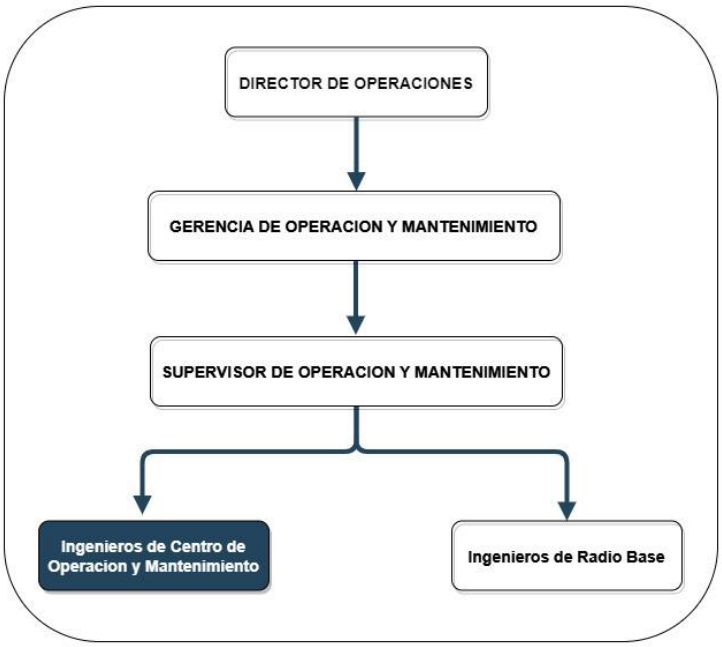
1.2.2 POSICIONES

La posición desempeñada fue la de **Ingeniero del Centro de Operación y Mantenimiento**, posición ejercida en conjunto con otros ingenieros con funciones similares. Esta área estaba liderada por un supervisor.

1.2.3 DEPENDENCIA

La posición desempeñada no poseía dependientes y contaba con un supervisor. En el siguiente diagrama se puede ver resaltada la posición desempeñada.

Figura 1.2.1 Organigrama del Centro de Operación y Mantenimiento



Fuente: Elaboración Propia

1.2.4 ACTIVIDADES PRINCIPALES

Como ingeniero del **Centro de Operación y Mantenimiento (COM)**, el objetivo principal de mi posición consistió en el monitoreo de la red de Telefonía Celular y la ejecución de tareas de mantenimiento. Además, llevé a cabo operaciones solicitadas por el área de planificación, que estaban principalmente relacionadas con actividades de expansión de la red.

1.2.5 RESULTADOS

Dentro de las actividades del **COM**, estuve a cargo de la instalación y puesta en servicio del primer sistema de tarifación en tiempo real en Bolivia, conocido comercialmente como **CELUCASH**, al cual se accedía a través de la compra de tarjetas prepago.

Como parte del COM, fui integrante del equipo responsable de la migración de la red de Telefonía Celular AMPS[4] al sistema TDMA[5], lo que representó un importante avance tecnológico en el ámbito de la Telefonía Móvil.

1.3 INGENIERO DE CONMUTACIÓN

1.3.1 ORGANIZACIÓN

Este puesto fue desempeñado en la empresa Telecel S.A., en el área técnica encargada de la operación y mantenimiento de la red de telefonía celular desde abril de 1999 hasta febrero de 2007.

1.3.2 POSICIONES

La posición desempeñada fue la de **Ingeniero de Conmutación**, posición ejercida en conjunto con otros ingenieros de conmutación. Esta área estaba liderada por un supervisor.

[4] AMPS fue una de las primeras tecnologías móviles. Se puede decir que fue la tecnología de primera generación o 1G de la telefonía celular.

[5] TDMA es una tecnología móvil que junto con la tecnología GSM, fueron versiones diferentes de la segunda generación 2G de la telefonía celular.

1.3.3 DEPENDENCIA

La posición desempeñada no poseía dependientes y era dependiente a su vez de la posición de **Supervisor de Conmutación**. En el siguiente diagrama se puede ver resaltada la posición desempeñada.

Figura 1.3.1. Organigrama del Área de Conmutación

Fuente: Elaboración Propia

1.3.4 ACTIVIDADES PRINCIPALES

El principal objetivo de la posición de **Ingeniero de Conmutación** era asegurar el correcto funcionamiento de los sistemas de conmutación que estaban bajo su responsabilidad a través de la ejecución de procedimientos de mantenimiento rutinarios, mantenimientos correctivos y solución de incidencias.

Después de asegurar el correcto mantenimiento de los sistemas, el Ingeniero de Conmutación debía ejecutar tareas operativas, siendo las principales aquellas provenientes del área de planificación asociadas a los proyectos de expansión y modernización de la red móvil para soportar el creciente tráfico de voz y datos, y para la provisión de nuevos servicios.

1.3.5 RESULTADOS

Desempeñé exitosamente las funciones descritas en el acápite anterior, asignadas al rol de **Ingeniero de Conmutación**.

Debido a que la empresa comenzó a cotizar en las bolsas de valores de Estados Unidos, tuvimos que cumplir la ley **SOX (Sarbanes Oxley)**[6], lo cual demandó la revisión y formalización de los procesos de operación y mantenimiento que teníamos, así como la implementación de nuevos procesos para cumplir la norma SOX.

Como parte del equipo que implementó la norma SOX, aproveché la oportunidad para optimizar y mejorar los procesos de operación y mantenimiento que teníamos, así como para implementar nuevos procesos que robustecieron el funcionamiento del área técnica.

En el ámbito de proyectos, el de mayor relevancia en el que participe fue el cambio de tecnología móvil de TDMA a GSM[7], cambio que también implicó un cambio de proveedor, con lo cual se desplego una red móvil totalmente nueva.

1.4 SUPERVISOR DE CONMUTACIÓN

1.4.1 ORGANIZACIÓN

Este puesto fue desempeñado en la empresa Telecel S.A., en el área técnica encargada de la Operación y Mantenimiento de la red de Telefonía Celular desde febrero de 2007 hasta noviembre de 2008.

1.4.2 POSICIONES

La posición desempeñada fue la de **Supervisor de Conmutación**, posición que tenía alcance a nivel nacional. Esta posición dependía directamente del director del área.

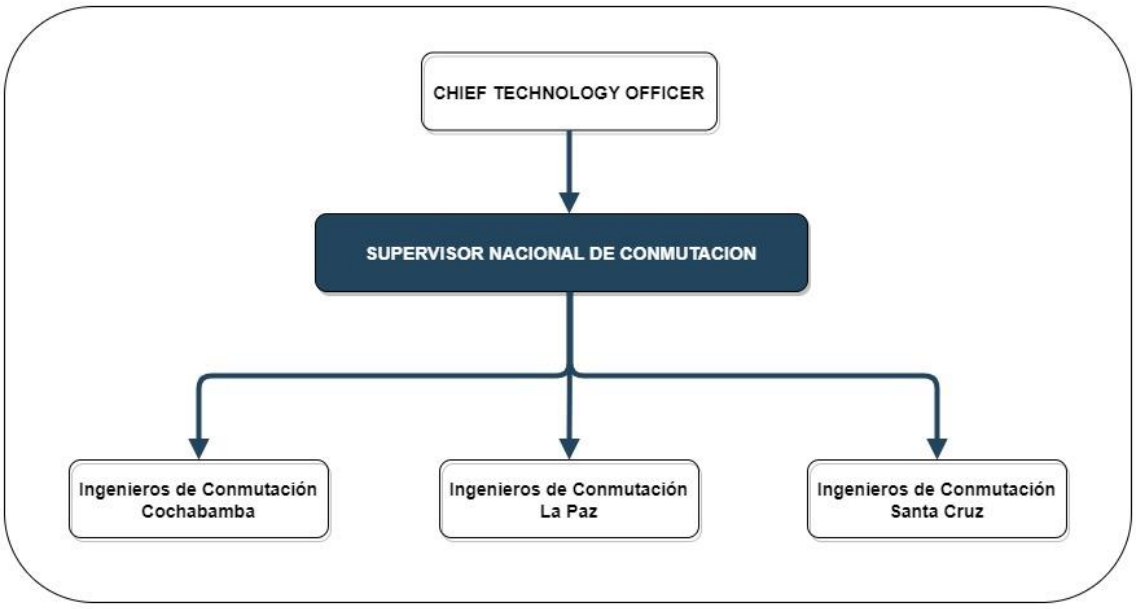
[6] La Ley Sarbanes Oxley se promulgó en Estados Unidos con el propósito de monitorizar a las empresas que cotizan en bolsa de valores, evitando que la valorización de las acciones de las mismas sea alterada de manera dudosa. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversionista.

[7] GSM es la tecnología móvil de segunda generación también conocida como 2G

1.4.3 DEPENDENCIA

La posición desempeñada tenía como dependientes al personal con la posición de **Ingeniero de Conmutación** y era a su vez dependiente de la posición de **Chief Technology Officer**[8]. En el siguiente diagrama se puede ver resaltada la posición desempeñada.

Figura 1.4.1. Organigrama del área de Conmutación



Fuente: Elaboración Propia

1.4.4 ACTIVIDADES PRINCIPALES

El principal objetivo de la posición de **Supervisor de Conmutación** consistió en asegurar el funcionamiento continuo y de calidad de los sistemas de conmutación que eran parte de la red móvil, así como de otros sistemas relacionados bajo la administración del área de Conmutación. Para lograr este objetivo, se llevó a cabo una labor cíclica de diseño, revisión y actualización de procedimientos de mantenimiento rutinarios, correctivos y de tratamiento de incidentes.

[8] Chief Technology Officer o CTO se refiere a uno de los puestos de dirección más altos en el área de tecnología o telecomunicaciones de una empresa

Después de asegurar el buen funcionamiento de los procesos de mantenimiento, el segundo objetivo más importante del Supervisor de Conmutación fue coordinar con las áreas clientes del área de Conmutación la ejecución de tareas operativas requeridas y establecer cronogramas. Una vez realizados los acuerdos, el supervisor debía monitorear el correcto avance para lograr el cumplimiento de tareas operativas y de proyectos de expansión de la red a cargo.

Otras funciones complementarias inherentes a la posición de **Supervisor de Conmutación** fueron la de cumplimiento de la norma SOX en todos los procesos que el área realizaba, principalmente mantenimiento y cambios, y la ejecución de tareas administrativas relacionadas a la posición.

1.4.5 RESULTADOS

Al ser un rol nuevo para mi persona, el desafío principal fue lograr asumir la nueva función mediante la organización, control y coordinación del personal técnico del área, considerando que estaban distribuidos en tres ciudades. En base a la retroalimentación de mis superiores, considero que logré alcanzar el objetivo de supervisar y dirigir correctamente al personal dependiente de mi posición.

A nivel técnico, se lograron alcanzar los objetivos de mantenimiento y ejecución de los proyectos de la compañía, entre los cuales el más importante fue el despliegue de una red móvil nueva con tecnología **UMTS**[9], que se montó sobre la infraestructura 2G existente. Este hecho posibilitó la provisión de servicios orientados a datos, como el consumo de Internet por parte de los usuarios de telefonía móvil. La implementación de estos proyectos se ejecutó cumpliendo los objetivos de mantenimiento y calidad.

[9] UMTS se refiere a la tecnología móvil de tercera generación, más conocida como 3G.

1.5 RESPONSABLE DE OPERACIÓN Y MANTENIMIENTO DE LAS ÁREAS DE CORE Y VAP

1.5.1 ORGANIZACIÓN

Este puesto fue desempeñado en la empresa Telecel S.A., en el área técnica encargada de la operación y mantenimiento de la red de Telefonía Celular desde noviembre de 2008 hasta mayo de 2011.

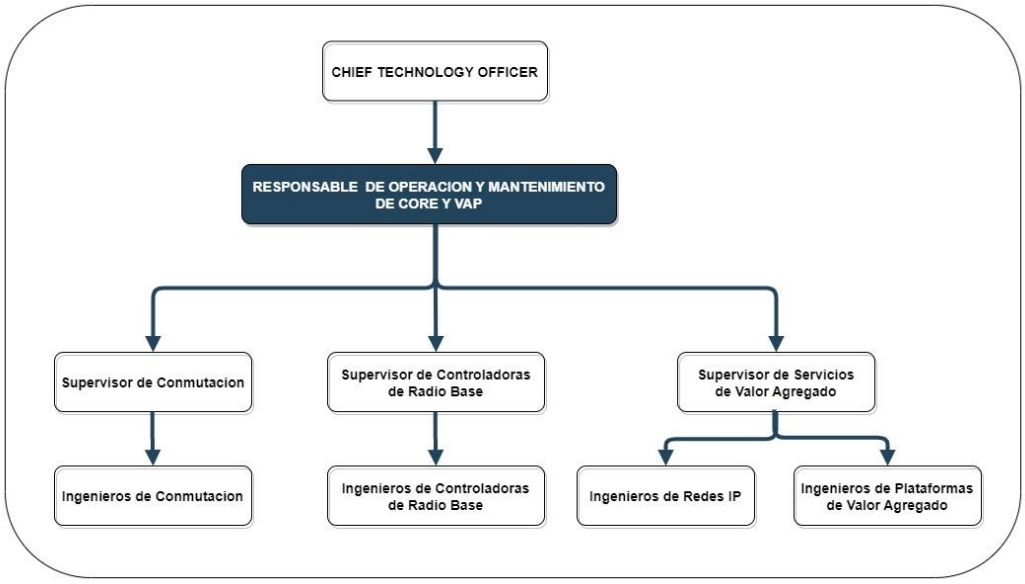
1.5.2 POSICIONES

La posición desempeñada estaba a cargo de tres áreas técnicas con alcance en las tres principales ciudades para la empresa: La Paz, Cochabamba y Santa Cruz. Esta posición tenía dependencia directa del **Director del Área Técnica**.

1.5.3 DEPENDENCIA

La posición desempeñada tenía como dependientes al personal con las siguientes posiciones: **Supervisor de Conmutación**, área a cargo de la administración de las centrales móviles, **Supervisor de Controladoras de Estaciones Base**, área a cargo de la administración de sistemas controladores de estaciones móviles 2G y 3G y el **Supervisor de Plataformas de Valor Agregado**, área a cargo de la administración de sistemas complementarios a la Red Celular, entre los cuales los más importantes eran el Sistema de Tarifación en Tiempo Real y la infraestructura de red IP de la compañía.

Figura 1.5.1. Organigrama del Área de Operación y Mantenimiento



Fuente: Elaboración Propia

1.5.4 ACTIVIDADES PRINCIPALES

El objetivo principal de la posición **Responsable de Operación y Mantenimiento** fue asegurar el funcionamiento continúo de todos los sistemas a cargo, incluyendo sistemas de conmutación, controladores de radio bases, redes IP y sistemas de valor agregado que eran parte del CORE o núcleo de la Red de Telefonía Celular, y también cumplir con parámetros de calidad establecidos para estos sistemas.

Para lograr este objetivo se diseñaron, revisaron y actualizaron los procedimientos de mantenimiento rutinarios, correctivos y de tratamiento de incidentes de todas las áreas a cargo. Complementariamente se incluyeron dentro de los objetivos el cumplimiento de **KPIs**[10] de operación y mantenimiento, para lo cual se implementaron herramientas de medición de eventos, incidentes y problemas.

En conjunto con los supervisores de las áreas a cargo se coordinaron y ejecutaron las tareas operativas que eran requeridas por otras áreas técnicas como **Planificación** y **Calidad**,

[10] KPI o "Key Performance Indicator" en inglés, se refiere a indicadores de calidad a través de los cuales se puede medir el nivel de rendimiento de un sistema o servicio.

principalmente para completar proyectos de expansión en la red y tareas operativas requeridas por las áreas de negocio.

También se cumplió con las normas internas de la compañía y se ejecutaron las tareas administrativas inherentes a la posición.

1.5.5 RESULTADOS

La posición de Responsable de Operación y Mantenimiento surgió como parte de una reestructuración del área técnica, con el objetivo de mejorar y estandarizar los procesos de operación y mantenimiento. Esta reestructuración presentó desafíos importantes, ya que nuevas áreas se me asignaron y tuve que establecer normas que eran nuevas para el personal a cargo. A pesar de estos desafíos, se logró alcanzar los objetivos de manera gradual mediante una sólida coordinación y trabajo en equipo.

En cuanto a los resultados técnicos, logramos cumplir con los objetivos de mantenimiento y llevar a cabo los proyectos clave de la compañía. Entre los más importantes se destacan la expansión de la cobertura móvil a través de la instalación de nuevas estaciones base, el aumento de la capacidad de los sistemas para soportar el tráfico creciente, la implementación de nuevas características de software en la red 3G para mejorar la velocidad del servicio móvil, y la puesta en marcha de una nueva central móvil en el centro de datos de Viru Viru.

1.6 RESPONSABLE DE ASEGURAMIENTO DE SERVICIO DE LAS ÁREAS DE CORE E IP

1.6.1 ORGANIZACIÓN

Este puesto fue desempeñado en la empresa Telecel S.A., desde mayo de 2011 hasta agosto de 2021, en el área técnica encargada del **Aseguramiento de Servicio** para los sistemas agrupados dentro de la denominación **CORE e IP**, los cuales fueron principalmente las

Centrales de Telefonía e Internet Móvil, las **Controladoras de Estaciones Base**, la **Red de datos Corporativa** y el **Backbone de Salida a Internet**[11].

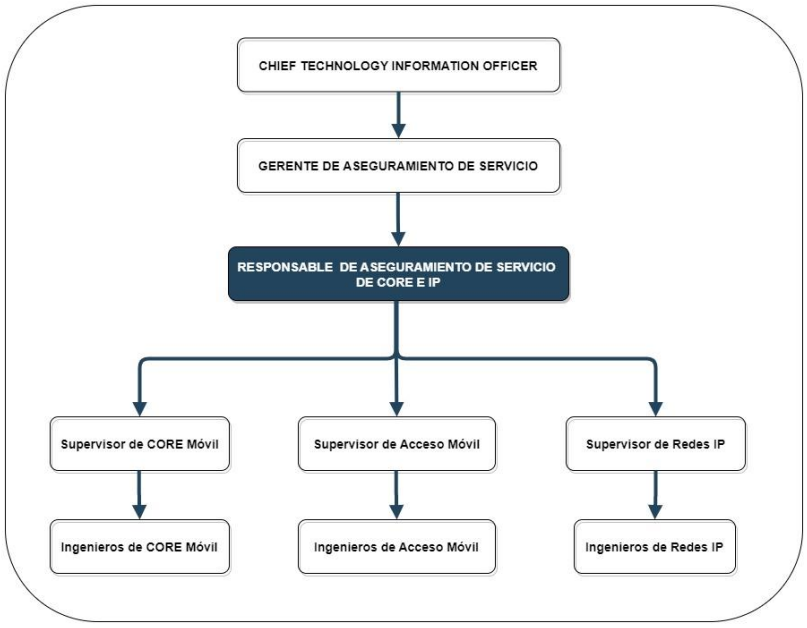
1.6.2 POSICIONES

La posición desempeñada estuvo a cargo de las áreas de **CORE Móvil**, **Acceso Móvil** y **Redes IP** con alcance a nivel nacional. Esta posición reportaba directamente al **Gerente de Aseguramiento de Servicios**.

1.6.3 DEPENDENCIA

La posición desempeñada tuvo como dependientes al personal con las siguientes posiciones: **Supervisor de CORE Móvil** a cargo de las centrales de Telefonía e Internet Móvil, **Supervisor de Acceso Móvil**, a cargo de los sistemas controladores de estaciones móviles y el **Supervisor de Redes IP**, a cargo de la administración de toda la infraestructura de red IP para las redes fijas y móviles y del Backbone de Salida a Internet.

Figura 1.6.3.1. Organigrama del Área de Aseguramiento de Servicio



Fuente: Elaboración Propia

[11] El Backbone de salida a Internet o Backbone Internet se refiere a un conjunto de equipos de red IP que concentran proveen de conectividad a Internet a todos los sistemas de la red de Telecomunicaciones que lo requieren.

1.6.4 ACTIVIDADES PRINCIPALES

El objetivo principal de la posición de **Responsable de Aseguramiento de Servicio** consistió en garantizar la operación ininterrumpida de todos los servicios de la Red de Telecomunicaciones ofrecidos por la compañía, asegurando que se cumplieran los estándares de calidad establecidos. Esto implicó la administración y operación de los sistemas bajo la responsabilidad del área de **CORE e IP**, incluyendo principalmente los sistemas de **CORE Móvil**, **Acceso Móvil**, y toda la infraestructura de **Redes IP** (desde las redes para servicios internos hasta el Backbone de salida a Internet).

Para lograr este objetivo, se diseñaron, revisaron y actualizaron los procedimientos de mantenimiento, tanto rutinarios como correctivos, y se gestionaron los incidentes en todas las áreas a cargo. Además, se establecieron y monitorearon indicadores de calidad e indicadores de niveles de servicio para garantizar el cumplimiento de los parámetros de calidad.

En colaboración con los supervisores de las áreas pertinentes, se coordinaron y ejecutaron las tareas operativas requeridas por otras áreas técnicas, como las áreas de **Planificación** y **Calidad**, para llevar a cabo proyectos de expansión de la Red de Telecomunicaciones y cumplir con otras tareas operativas exigidas por las áreas de negocio.

Finalmente, se aseguró el cumplimiento de las normas internas de la compañía, además de realizar las tareas administrativas asociadas a la posición.

1.6.5 RESULTADOS

La posición de **Responsable de Aseguramiento de Servicio** emergió de una nueva fase en la reestructuración del área técnica, enfocada en consolidar una metodología que garantizara la continuidad del servicio y el cumplimiento de los indicadores de calidad.

Las mejoras en la metodología y las normas de trabajo fueron claves para enfrentar un aumento considerable en los proyectos de expansión e implementación de nuevos sistemas, lo cual presentaba un desafío en términos de mantener la continuidad de servicio. Estas mejoras fueron consensuadas con las jefaturas y gerencias de áreas como Planificación,

Calidad y el área comercial, con las cuales se tenía una fuerte interacción e interdependencia.

Sobre los proyectos más importantes, en 2014 se puso en operación una Red Móvil con la tecnología **LTE**[12]. Este avance, alineado con nuestros objetivos de calidad, permitió un considerable incremento en la velocidad del servicio de datos móviles que ofrecíamos al público.

Además, consolidamos una red IP denominada **Backbone Internet**, centralizando las demandas de acceso a Internet para todos los servicios. Esta red se convirtió en un componente crítico y vital de nuestra infraestructura de telecomunicaciones.

En cuanto al acceso móvil, a partir de 2018, implementamos nuevas redes 3G y LTE en respuesta a una decisión estratégica de la compañía de cambiar a la empresa proveedora de equipamiento móvil.

Por otro lado, desplegamos una red fija basada en la tecnología de **Cable Modem**[13] para el acceso a Internet, lo que permitió masificar la demanda de este servicio. Para satisfacer esta creciente demanda y garantizar la continuidad de servicio, tuvimos que establecer enlaces de salida a Internet por Chile, Perú y Argentina.

[12] LTE o **Long Term Evolution** es el nombre que se le dio a la cuarta generación de tecnología móvil o 4G que trajo principalmente mayores anchos de banda en los servicios de datos móviles.

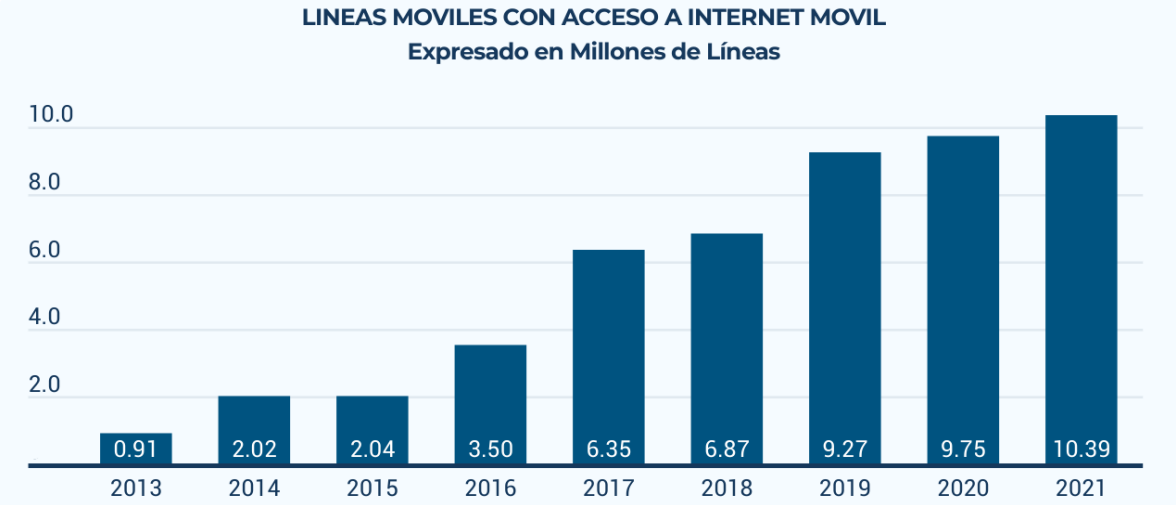
[13] La tecnología de Cable Modem es un sistema de comunicación que utiliza la infraestructura de cable televisivo para ofrecer servicios de Internet de alta velocidad a través de una conexión de cable coaxial.

2. CASO DE ESTUDIO

2.1 ANTECEDENTES

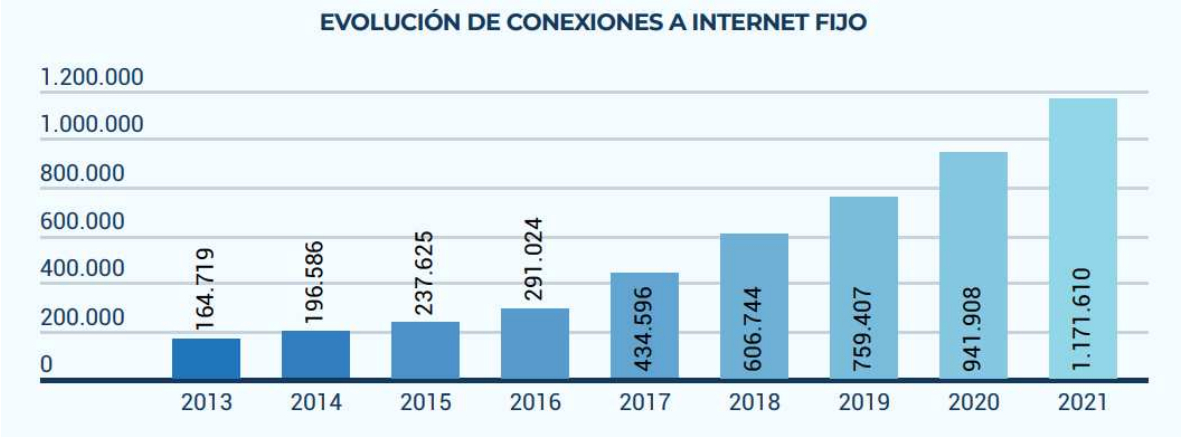
A lo largo de la década de 2010, Bolivia experimentó un crecimiento significativo en el acceso a Internet, impulsado tanto por la evolución de las tecnologías móviles (2G, 3G y LTE), así como por la expansión de los servicios de Internet domiciliario. Las gráficas siguientes ilustran la trayectoria de este crecimiento, desglosando las conexiones a Internet Móvil y Fijo por todos los operadores del país, mostrando un crecimiento evidente. Los datos abarcan el periodo de 2013 a 2021 y se basan en reportes públicos de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

Figura 2.1.1 Evolución del número de líneas móviles con acceso a Internet en Bolivia



Fuente: ATT, Estado de Situación del Internet en Bolivia

Figura 2.1.2 Evolución del número de conexiones a Internet Fijo en Bolivia



Fuente: ATT, Estado de Situación del Internet en Bolivia

Frente a la creciente demanda del mercado, se convirtió en una prioridad para Telecel S.A., el ofrecer servicios altamente competitivos de Telefonía Móvil e Internet Fijo, dado que son pilares de su cartera comercial. Este cambio estratégico elevó las expectativas de rendimiento técnico de los elementos y sistemas relacionados.

Acorde con las crecientes demandas de rendimiento y calidad en los servicios de Internet Móvil e Internet Fijo, la compañía tomó la decisión de modernizar los sistemas críticos para la provisión del servicio de acceso a Internet, entre los cuales, uno de los sistemas fundamentales es el **DNS**[14]. La modernización de este sistema buscaba mejorar sus prestaciones técnicas, niveles de soporte y obtener condiciones económicas más favorables para la compañía.

[14] DNS es el Sistema de Nombres de Dominio, el cual traduce los nombres de dominios como ser Google.com o Youtube.com a sus respectivas direcciones IP.

2.2 OBJETIVOS

2.2.1 OBJETIVO GENERAL

Implementar y migrar un nuevo Sistema de Nombres de Dominio en el **Backbone Internet**[15] de Telecel S.A., que permita mejores prestaciones técnicas, mayor confiabilidad y una mejor calidad en la provisión de los servicios de Internet Móvil y Fijo.

2.2.2 OBJETIVOS ESPECÍFICOS

Los objetivos específicos del presente proyecto fueron los siguientes:

- **Desarrollar una Estrategia Técnica para la Modernización del Sistema DNS.**
  Establecer y describir las fases y consideraciones técnicas requeridas para la renovación del sistema DNS en la red del Backbone Internet. Este plan técnico permitirá la ejecución planificada y ordenada del proyecto minimizando el impacto en los servicios de acceso a Internet Móvil y Fijo.
- **Ejecutar el Nuevo Sistema DNS dentro del Backbone Internet del ISP**.
  Integrar el nuevo sistema DNS en la infraestructura del Backbone Internet del ISP y realizar la transición de los servicios de acceso a Internet hacia este nuevo sistema. El propósito es poner el sistema en operación y documentar las actividades técnicas y mejoras conseguidas en el proceso.
- **Evaluar y Demostrar Mejoras en la Calidad de Resolución DNS**.
  Llevar a cabo mediciones de indicadores clave de rendimiento (KPIs) relacionados con el sistema DNS. Dichas mediciones contemplarán aspectos como tiempos de resolución, volumen de tráfico y nivel de completitud de resoluciones DNS, con la finalidad de cuantificar las mejoras alcanzadas con la nueva implementación en comparación con el sistema anterior.

[15] Backbone Internet: En el contexto de Telecel S.A., es una red troncal IP de alta capacidad que concentra el tráfico de datos de los servicios del operador y los encamina hacia Internet, asegurando una transferencia eficiente y rápida de datos para sus suscriptores.

2.3 JUSTIFICACIÓN

2.3.1 DIAGNÓSTICO DEL PROBLEMA

2.3.1.1 ESTADO ANTES DE LA MIGRACIÓN

Antes de la migración, el sistema DNS existente presentaba limitaciones en términos de escalabilidad, soporte técnico y capacidades funcionales. Estas limitaciones estaban afectando la capacidad del ISP para implementar nuevos servicios y mantener una operación eficiente y rentable.

2.3.1.2 INTERPRETACIÓN DE LA SITUACIÓN

Las limitaciones del sistema existente no eran simplemente inconvenientes técnicos; representaban barreras reales para el crecimiento y la innovación dentro de la organización. Además, los costos asociados con el mantenimiento y la operación del sistema antiguo estaban en desacuerdo con los objetivos financieros a largo plazo de la empresa.

2.3.1.3 JUSTIFICACIONES

La migración del sistema DNS existente fue motivada por razones tanto tecnológicas como económicas. Desde la perspectiva tecnológica, la decisión de migrar a un nuevo proveedor se tomó con el objetivo de contar con un sistema moderno con mejores opciones de escalabilidad, un mejor servicio de soporte ante problemas técnicos, y una mayor variedad de funciones y capacidades técnicas que permitan al ISP tener flexibilidad en la implementación de nuevos servicios.

Desde el punto de vista económico, el realizar esta migración también cumplió con el objetivo de optimizar los costos de operación y mantenimiento, lo cual se logró debido a que la casa matriz **Millicom**[16] realizó una adquisición de sistemas DNS similares para sus operaciones filiales en Latinoamérica.

[16] Millicom es un grupo empresarial multinacional que tiene presencia en varios países a través de distintas empresas. Por ejemplo, Millicom opera en Bolivia a través de la empresa Tigo.

2.4 ALCANCES Y LÍMITES

2.4.1 ALCANCES

El presente documento detalla el proyecto de implementación y migración de un sistema DNS, que fue realizado en el año 2018. Los alcances de esta memoria se organizan de la siguiente manera:

Estrategia de Implementación: En la sección 2.6.3, se va a describir la estrategia de reemplazo adoptada, incluyendo las tareas y responsabilidades involucradas en el proceso.

Descripción del Sistema DNS: La sección 2.6.4.3 va a proporcionar una descripción general del sistema DNS instalado, sus componentes, funciones internas y características de software.

Arquitectura del Backbone Internet del ISP: En la sección 2.6.4.4, se va a explicar brevemente la arquitectura del Backbone Internet del ISP y la posición del sistema DNS dentro de esta estructura, mostrando su inserción y justificación.

Plan de Pruebas y Resultados: La sección 2.6.5 se va a centrar en el plan de pruebas adoptado para aceptar el nuevo sistema, explicando en detalle las pruebas realizadas y los resultados obtenidos.

Puesta en Producción: Finalmente, en la sección 2.6.6 se va a describir el proceso de puesta en producción, incluyendo las medidas tomadas, las pruebas realizadas posteriormente, y otros aspectos relevantes para garantizar una transición exitosa.

2.4.2 LÍMITES

Este documento establece ciertos límites en términos de la información y detalles que se presentan, definidos en los siguientes aspectos:

Restricciones de Confidencialidad: La información presentada en este documento está sujeta a las restricciones de confidencialidad del ISP. En este sentido los datos económicos están restringidos y las descripciones a nivel técnico son de alto nivel, sin entrar en detalles

sobre protocolos de red, comandos de configuración en equipos del ISP, datos técnicos como direcciones IP o números de VLAN y otros relacionados.

Descripción del Sistema DNS: Se realiza una descripción general de los componentes del sistema DNS a nivel macro sin entrar en detalles técnicos específicos como ser pasos de instalación del software, configuración de servidores y otros similares.

Aspectos Físicos: No está dentro del alcance de esta memoria describir los aspectos físicos relacionados con el sistema, como el cableado, las condiciones de energía o las condiciones ambientales de los equipos.

2.5 MARCO REFERENCIAL

Con el fin de dar un contexto técnico adecuado acerca del caso de estudio, primero se dará una explicación resumida acerca del funcionamiento de la red de Internet, para después describir con mayor detalle el funcionamiento del sistema DNS en Internet y también de un sistema DNS a nivel de un ISP.

2.5.1 FUNCIONAMIENTO DE INTERNET

Internet, en resumen, es una vasta red global de computadoras interconectadas. Consiste en nodos o servidores que proporcionan información a los millones de usuarios que se conectan a través de dispositivos terminales, que son principalmente teléfonos móviles y computadoras personales. Los usuarios acceden a Internet a través de los servicios proporcionados por empresas conocidas como Proveedores de Servicios de Internet (ISP).

Los medios de comunicación utilizados para la transmisión de datos varían en diferentes niveles. Por ejemplo, Wi-Fi[17] se utiliza comúnmente a nivel doméstico para distribuir acceso a Internet, mientras que las redes de telefonía celular brindan acceso a Internet a dispositivos móviles. La fibra óptica es utilizada por los ISP para proporcionar servicios a un gran número de clientes domésticos, y también se utiliza para llegar a los Puntos de Acceso a la Red (NAP). Los **NAP**[18] son puntos de intercambio de tráfico de Internet entre diferentes ISP, lo que permite a los usuarios acceder al contenido de Internet global. Estos son solo algunos ejemplos de la infraestructura subyacente que posibilita Internet.

2.5.2 ACCESO A INTERNET

Como se puede observar, existen diferentes medios por los cuales viaja la información. Sin embargo, esto resulta transparente para el usuario final, ya que la comunicación o el

[17] Wi-Fi se refiere a la tecnología de acceso inalámbrica que es comúnmente usada en redes locales o domiciliarias para acceder a Internet.

[18] Los NAP, también conocidos como Puntos de Intercambio de Internet (IXP, por sus siglas en inglés), son infraestructuras físicas a través de las cuales los ISP intercambian tráfico de Internet entre sus respectivas redes. De esta forma un ISP puede proporcionar a sus usuarios un acceso completo a Internet.

intercambio de datos se efectúa mediante un lenguaje común: el protocolo **TCP/IP**[19]. Este protocolo establece las normas de intercambio de paquetes de datos, que todos los dispositivos que participan en el acceso a Internet, respetan.

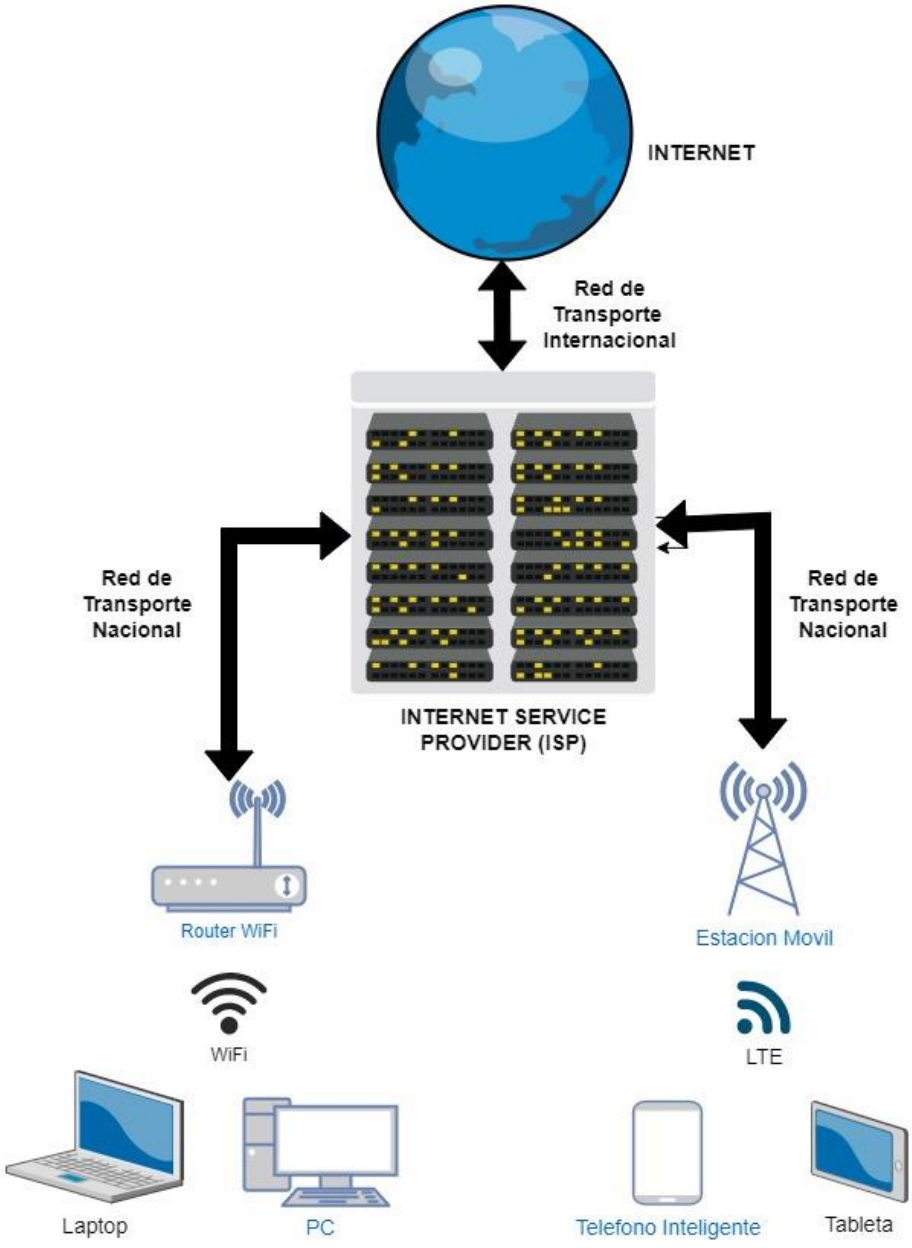
Cuando un usuario quiere conectarse a Internet, lo hace contratando este servicio a un ISP. Un ISP es una compañía que posibilita que sus usuarios accedan a Internet, para ello el ISP cuenta con redes de telecomunicaciones nacionales para poder llegar a los usuarios finales, así como también tiene el acceso a redes de telecomunicaciones internacionales para poder acceder al contenido de Internet a través de los puntos de intercambio mundiales o NAPs. En el medio boliviano, tenemos varios ISP como ser Entel S.A., Nuevatel PCS de Bolivia, Telecel S.A., COTAS, COMTECO, entre otros.

Para proveer el servicio, el ISP debe llegar hasta nuestro domicilio u oficina en el caso de un servicio fijo o tener cobertura para darnos el acceso en caso de un servicio móvil. En cualquier caso, el ISP asigna una dirección IP única a la terminal desde la cual queremos acceder a Internet, lo cual permite que nuestro terminal pueda ser debidamente identificado en Internet y que sea capaz de comunicarse con otros terminales o servidores. Otro dato muy importante que el ISP nos provee es la dirección del DNS que nuestro servicio usará para poder acceder a la información de los diferentes sitios de Internet. El DNS realiza la traducción entre las direcciones IP de los servidores de Internet donde se aloja la información que queremos consumir y los nombres de estos sitios que los usuarios finales estamos acostumbrados a utilizar cuando navegamos por Internet, por ejemplo www.youtube.com o www.facebook.com. Se explicará con mayor detalle la composición y funcionamiento del sistema DNS en secciones posteriores.

[19] TCP/IP, que significa Transmission Control Protocol/Internet Protocol, es un conjunto de protocolos estandarizados que posibilitan la comunicación entre dispositivos en una red, siendo el estándar fundamental de Internet.

En el siguiente diagrama se esquematiza de una forma muy resumida lo explicado en los dos últimos acápites.

Figura 2.5.1 Red de Acceso a Internet



Fuente: Elaboración Propia

2.5.3 EL PROTOCOLO TCP/IP

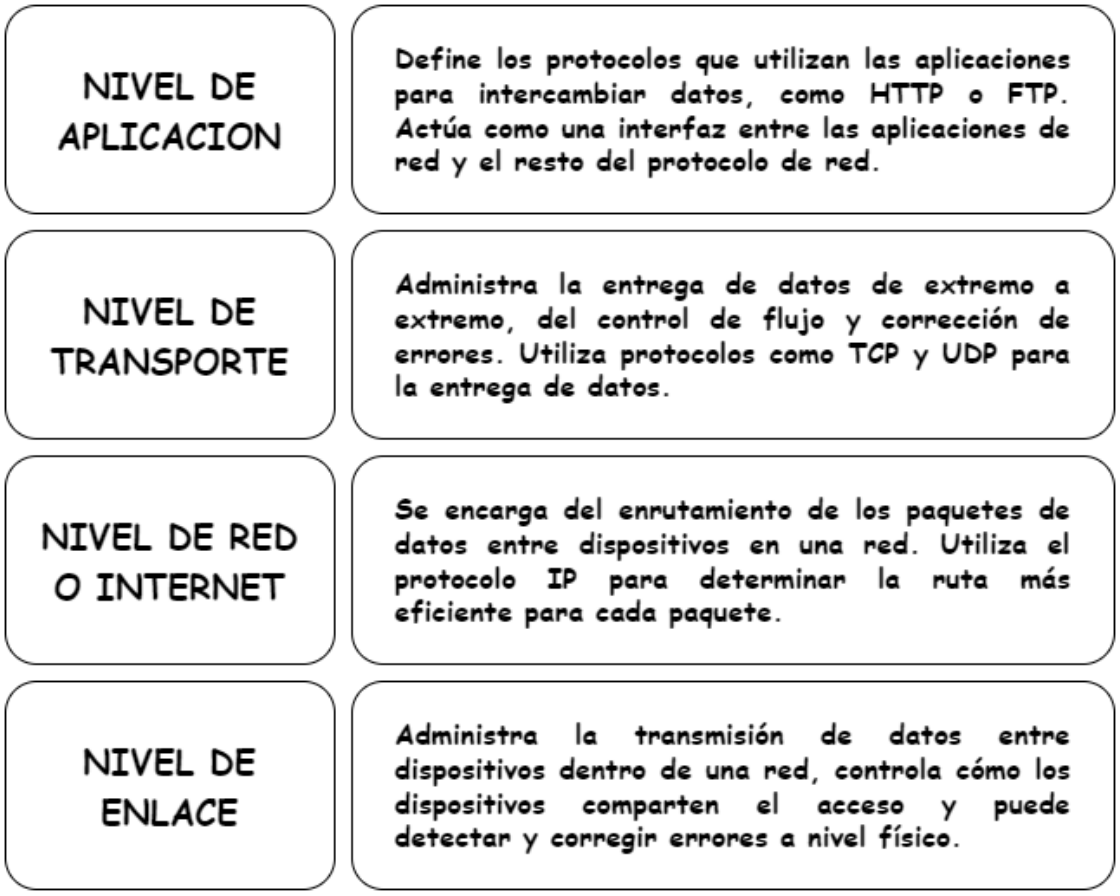
Un computador u ordenador puede realizar muchas operaciones por sí mismo, pero si este equipo está conectado a Internet, sus capacidades se multiplican al poder ejecutar aplicaciones basadas en esta conectividad, como por ejemplo el envío de un correo electrónico, el consumo de servicios de Streaming como Netflix, el poder realizar una transacción bancaria o poder comunicarse con otros usuarios por medio de aplicaciones de mensajería como WhatsApp, son algunos ejemplos de poderosos servicios basados en la conectividad a Internet.

Para que estas aplicaciones o servicios puedan funcionar, se necesita que exista una interacción o comunicación entre los equipos clientes y equipos finales que son los que proporcionan la información o servicio que requerimos. Para que esta comunicación entre equipos sea posible, se necesitan reglas de comunicación que indiquen por ejemplo como iniciar una conversación, a quien le toca responder, como validar los mensajes y como finalizar la conversación. Este conjunto de reglas es lo que se conoce como un protocolo de comunicación que es un conjunto de normas o reglas que permiten a las máquinas y los programas de aplicación intercambiar información.

En este contexto TCP/IP es un protocolo de comunicación que establece las normas para la comunicación en una red que permite que un equipo pueda comunicarse con otros. TCP/IP es el protocolo estándar de Internet y el más utilizado en redes en general. Todos los dispositivos que se conectan a Internet lo usan, y es independiente del medio de transmisión o transporte utilizado.

El protocolo TCP/IP hace posible un intercambio de datos fiable dentro de una red, definiendo cuidadosamente los pasos a seguir desde que los datos son enviados desde un remitente hasta un destinatario. TCP/IP usa un modelo de capas o niveles con jerarquías que se comunican únicamente con su capa o nivel superior (a la que envían los resultados) y su capa o nivel inferior (de la cual se solicitan servicios).

Figura 2.5.2 Modelo TCP/IP



Fuente: Elaboración Propia

Nivel de Aplicación: Es la capa superior en el conjunto de protocolos TCP/IP. Esta capa interactúa directamente con las aplicaciones de software que utilizamos para la comunicación en la red.

Los protocolos que operan en este nivel, como SSH (Secure Shell) para la administración segura de sistemas, FTP (File Transfer Protocol) para la transferencia de archivos, y SMTP (Simple Mail Transfer Protocol) para el correo electrónico, proporcionan servicios específicos que las aplicaciones pueden utilizar para gestionar y coordinar las comunicaciones en red.

Además de gestionar las solicitudes de los usuarios, el Nivel de Aplicación también tiene la responsabilidad de asegurar que la información esté correctamente empaquetada para el viaje a través de la red.

Nivel de Transporte: Se encuentra justo debajo del Nivel de Aplicación en la pila de protocolos TCP/IP. Esta capa tiene la responsabilidad de asegurar la entrega confiable de los datos entre las aplicaciones que se comunican a través de la red.

Los protocolos como TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagramas de Usuario) operan en este nivel. TCP se utiliza para conexiones que necesitan alta fiabilidad y verifica la entrega exitosa de los datos, mientras que UDP se utiliza para conexiones que necesitan menos supervisión, pero más velocidad, como la transmisión de video en vivo o juegos en línea.

Este nivel también utiliza conceptos de **puertos** para identificar diferentes aplicaciones y administrar cómo los datos son enviados y recibidos. Los puertos permiten que diferentes aplicaciones en una misma máquina puedan usar la red simultáneamente, pues cada una se asocia con un puerto distinto.

Nivel de Red o Internet: También conocida como Capa de Internet en la arquitectura TCP/IP, es esencial para el funcionamiento de la red. Su principal tarea es el manejo y enrutamiento de paquetes de datos, denominados datagramas, basándose en las direcciones IP.

En esta capa se sitúa el Protocolo de Internet (IP), que es fundamental para definir cómo se dividen los datos en paquetes para su transmisión y cómo se reensamblan al llegar a su destino. Otros protocolos importantes que operan en esta capa son por ejemplo ARP (Protocolo de Resolución de Direcciones), que mapea direcciones IP a direcciones físicas en la red local e ICMP (Protocolo de Mensajes de Control de Internet), que proporciona mensajes de error y de control.

Cada uno de estos protocolos tiene un papel específico, contribuyendo a la función principal de asegurar que los paquetes de datos lleguen a su destino correcto en la red global de Internet, independientemente de dónde se originen o a dónde se dirijan.

Nivel de Enlace: También conocido como Capa de Acceso a la Red en la arquitectura TCP/IP, es la capa más baja del modelo y su función es proporcionar el medio para transferir datos entre dispositivos en la misma red o entre dos dispositivos adyacentes en una topología de red.

Esta capa es responsable del manejo de la interacción física entre los dispositivos de red, que incluye cómo se formatean los datos en marcos (estructuras de datos que contienen la información que se va a transmitir), cómo se gestionan las colisiones de datos, cómo se controla el flujo de datos para evitar la sobrecarga de los dispositivos receptores, y cómo se maneja el control de errores para garantizar la transmisión precisa y confiable de datos.

La Capa de Enlace incluye protocolos como Ethernet para redes cableadas, Wi-Fi para redes inalámbricas y PPP (Protocolo Punto a Punto) para conexiones de acceso telefónico y DSL. También se encarga de las direcciones MAC (Media Access Control), que son identificadores únicos asignados a cada dispositivo de red y utilizados para la transmisión de datos en esta capa.

2.5.3.1 FUNCIONAMIENTO DEL PROTOCOLO TCP/IP

Los programas de la capa de Aplicación del modelo TCP/IP generan mensajes de datos que serán enviados a través de la red. Estos mensajes son entregados a los protocolos en la capa de Transporte, tales como UDP o TCP.

Estos protocolos de la capa de Transporte se encargan de segmentar los datos de los mensajes de la aplicación en unidades más pequeñas llamadas paquetes. A cada paquete se le añade una cabecera que contiene información relevante para la entrega, incluyendo la dirección de destino. Los paquetes son luego entregados a la capa de Internet.

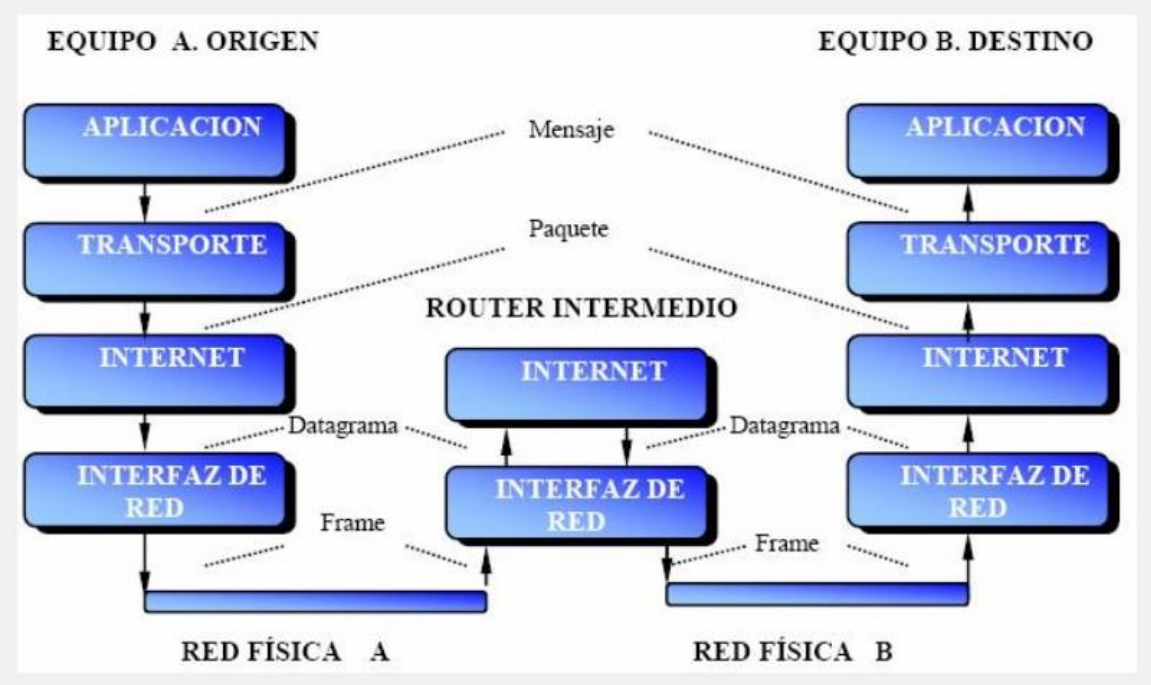
En la capa de Internet, los paquetes son encapsulados dentro de un datagrama IP. Cada datagrama IP tiene su propia cabecera, que incluye la información necesaria para dirigir el datagrama a su destino, ya sea de manera directa o a través de uno o más puntos intermedios. Una vez preparado, el datagrama se entrega a la capa de Acceso a la Red.

La capa de Acceso a la Red, que interactúa con el hardware de red específico, toma los datagramas IP y los transmite a través del medio de red correspondiente, encapsulándolos en unidades de datos llamadas tramas o marcos.

En el dispositivo de destino, los datos pasan a través de las capas del modelo TCP/IP en el sentido inverso. En cada capa se elimina la cabecera correspondiente, procesando y ascendiendo la información hasta que los datos originales llegan a la capa de Aplicación.

Cabe destacar que, durante su viaje a través de la red, los datagramas pueden pasar a través de varios enrutadores. Estos dispositivos funcionan en las capas de Red y Acceso a la Red del modelo TCP/IP, y se encargan de dirigir los datagramas a su destino final basándose en la información contenida en las cabeceras de los datagramas.

Figura 2.5.3 Funcionamiento del Protocolo TCP/IP



Fuente: https://baulderasec.wordpress.com/analisis-software/linux/8-configuracion-basica-de-redes/8-1-las-redes-tcpip/8-1-5-tipos-de-protocolo-de-tcpip

2.5.3.2 DIRECCIONAMIENTO IP

Cada ordenador, servidor, enrutador, conmutador, etc., que se encuentra conectado a una red posee una dirección única que lo identifica inequívocamente. Dentro del protocolo TCP/IP, este identificador se denomina **dirección IP**, la cual, en su versión IPv4, está formada por cuatro cifras de números separadas por puntos, cada una de estas cifras puede tomar valores entre 0 y 255, haciendo un total de 2^{32} direcciones aproximadamente, mientras que en su versión IPv6 la dirección está formada por 8 cifras de cuatro números hexadecimales separados por dos puntos, haciendo un total de 2^{128} direcciones. Por ejemplo:

Dirección IPv4: 190.129.181.238
Dirección IPv6: 1050:0000:0000:0000:0005:0600:300c:326b

Es importante mencionar que la versión IPv6 nace como una necesidad, ya que el espacio de direccionamiento en IPv4 está virtualmente agotado. Es por esto que ya desde hace algunos años la migración de IPv4 a IPv6 ha recibido un fuerte impulso a nivel mundial por los organismos que administran estos espacios de direccionamiento.

2.5.3.2.1 TIPOS DE DIRECCIONES IP

Las direcciones IP se clasifican en dos categorías principales: públicas y privadas. Las direcciones IP públicas son únicas en toda la red de Internet y son asignadas por los proveedores de servicios de Internet (ISP) a los usuarios cuando estos contratan un servicio de Internet. Estas direcciones son visibles y accesibles desde cualquier lugar de la red global.

En contraposición, las direcciones IP privadas son utilizadas dentro de redes locales, como las de una casa, oficina o institución, y no son visibles ni accesibles directamente desde la red de Internet. Estas direcciones se generan y administran internamente en la red local y son utilizadas para identificar los dispositivos dentro de dicha red.

Las direcciones privadas se subdividen en tres bloques de direcciones, cada uno adecuado para redes de diferentes tamaños: Clase A para grandes redes corporativas, Clase B para redes de tamaño medio como las de las universidades, y Clase C para redes más pequeñas,

como las redes domésticas o de pequeñas oficinas. Cada clase de dirección privada tiene un rango de direccionamiento específico asignado.

Con respecto a las direcciones IP públicas, estas pueden ser estáticas o dinámicas. Una dirección IP estática es una dirección que se asigna de forma permanente a un dispositivo y que no cambia. Son útiles cuando se requiere que un dispositivo sea constantemente accesible desde Internet, como un servidor web.

Por otro lado, una dirección IP dinámica es una que puede cambiar cada vez que un dispositivo se conecta a la red. Los ISP suelen utilizar direcciones IP dinámicas debido a su eficiencia en la gestión de direcciones IP limitadas.

2.5.4 SERVICIOS DE INTERNET

Existen muchos servicios basados en Internet y las aplicaciones web, se citan a continuación los más populares.

2.5.4.1 WORLD WIDE WEB

La World Wide Web o simplemente la Web es una red informática mundial conformada por **Páginas WEB** interconectadas que ofrecen diferentes contenidos textual y multimedia. Las páginas web son hipertextos, los cuales se diferencian de textos normales, por contener hipervínculos, más conocidos como **Enlaces** que pueden llevar al usuario a otros puntos dentro de la misma página web o a otra página web diferente. Conocemos el acto de ir de una página web a otra página web como navegar por Internet.

Desde su nacimiento, la web se ha basado en tecnologías libres y está disponible para todo el mundo de forma gratuita, sin patentes ni derechos de autor. Esto propició su rápida difusión y crecimiento.

Hoy por hoy, podemos encontrar en la web cualquier tipo de información que se nos ocurra buscar, por lo cual se ha convertido en una biblioteca digital gigante con información al alcance de nuestra mano. La forma de enseñar y aprender, la forma de trabajar, incluso la forma de entretenernos, han sido impactadas totalmente por el Internet y la World Wide Web.

2.5.4.1.1 LENGUAJE DE LAS PAGINAS WEB

El lenguaje estándar para escribir páginas web es **HTML**[20], el cual es un lenguaje de marcado. Un lenguaje de marcado combina el texto con marcas o etiquetas, las cuales indican al navegador las acciones que debe realizar sobre el texto. Estas acciones van desde dar formato al texto, crear enlaces o insertar otros recursos como imágenes, audio o video.

Complementando a HTML, tenemos otros dos lenguajes que potencian a las páginas web, el primero se denomina **CSS**[21], el cual define el aspecto visual y el segundo **JavaScript**, el cual es un lenguaje de programación que permite agregar interactividad y dinamismo a las páginas web, enriqueciendo la experiencia del usuario. Estos lenguajes se ejecutan en los dispositivos de los clientes, mientras que a nivel de servidores existen otros lenguajes de programación más complejos y completos como por ejemplo **PHP**[22], **Django**[23], **JSP**[24], entre otros, los cuales son capaces de crear páginas web de forma dinámica y administrar las interacciones de las páginas web con bases de datos.

2.5.4.2 CORREO ELECTRÓNICO

Mediante este servicio podemos enviar y recibir correos electrónicos compuestos de texto y contenido multimedia, los cuales se almacenan en espacios de almacenamiento o casillas digitales que son provistos por un proveedor del servicio. Entre los proveedores más populares tenemos a Hotmail, Gmail, Yahoo, entre otros. Las casillas de correo se identifican mediante direcciones del tipo hans@hotmail.com por ejemplo, en donde la primera parte es el nombre de la casilla de correo y la segunda parte después del símbolo de @ o arroba, típicamente es el nombre del proveedor que ofrece el servicio.

2.5.4.3 REDES SOCIALES

Las redes sociales son provistas por aplicaciones web que proveen de espacios donde los usuarios pueden contactar a otros usuarios, así como publicar contenido personal como estados, fotos, videos, los cuales pueden ser vistos por los contactos personales de cada

[20] HTML quiere decir Hyper Text Markup Language o Lenguaje de Marcas de HiperTexto
[21] CSS quiere decir Cascading Style Sheets o Hojas de Estilo en Cascada
[22] PHP quiere decir Hypertext Preprocessor es un lenguaje de código abierto para el desarrollo web
[23] Django es un conjunto de herramientas de alto nivel que permite el desarrollo web
[24] JSP quiere decir Java Server Pages es una tecnología orientada al desarrollo web

usuario, entre las redes más famosas podemos citar a Facebook y Twitter. También existen redes sociales con objetivos específicos donde los usuarios pueden conectar con otros usuarios con intereses similares como por ejemplo LinkedIn que sirve para encontrar oportunidades laborales o Slack que proporciona grupos de tecnología.

2.5.4.4 MENSAJERÍA INSTANTÁNEA

Los servicios de mensajería instantánea permiten enviar mensajes de texto o multimedia de un usuario a otro usuario o a grupos de usuarios, los cuales llegan de forma inmediata. Se requiere que los usuarios estén conectados a Internet y en uso de la aplicación de su preferencia. Entre las aplicaciones más populares están WhatsApp y Telegram.

La popularidad del uso de este servicio ha crecido enormemente entre los usuarios de telefonía móvil, más aún por el hecho de que también se pueden realizar llamadas y videollamadas por este medio, ocasionando un retroceso de la tecnología de telefonía tradicional basada en circuitos frente a la telefonía basada en datos.

2.5.4.5 DIFUSIÓN

Los servicios de difusión o Streaming proveen del acceso a películas y contenido televisivo a través de Internet, por ejemplo, tenemos a Netflix, Amazon Prime, HBO, entre los más conocidos, los cuales proveen este servicio mediante una suscripción. Se espera que para la década de los 2030 estos servicios reemplacen completamente a la televisión tradicional.

2.5.4.6 SERVICIOS FINANCIEROS Y COMERCIO ELECTRÓNICO

Los servicios financieros a través de Internet más conocidos como **Pagos en Línea** nos dan la posibilidad de realizar transacciones bancarias desde cualquier terminal con acceso a Internet, nuestro ordenador o nuestro celular, habiendo implementado todas las entidades financieras portales web y aplicaciones móviles que permiten al usuario realizar el pago de los servicios básicos o transferencias de dinero de una cuenta a otra de forma sencilla y segura.

Con la posibilidad de realizar pagos en línea, aparecen las tiendas en línea de forma masiva haciendo que el comercio electrónico sea una importante alternativa de compra y venta de artículos y servicios.

2.5.5 SISTEMA DE NOMBRES DE DOMINIO

El sistema de nombres de dominio, más conocido como DNS es un sistema de bases de datos que están distribuidas en Internet. Este sistema permite realizar la traducción de un nombre de dominio a una dirección IP y viceversa, estas funcionalidades son fundamentales para el funcionamiento de los servicios descritos en la sección 2.5.5, lo cual convierte al sistema DNS es una parte fundamental de la estructura de Internet.

Para poder entender mejor la importancia del DNS, se debe recordar, por una parte, que todos los equipos conectados a Internet, clientes y servidores, tienen una dirección IP única mediante la cual puedan ser identificados y encontrados, y por otra parte que cuando los usuarios navegan por Internet, en ningún caso acceden a los sitios web escribiendo sus direcciones IP numéricas, sino más bien se usan los nombres de dominio, los cuales son mucho más fáciles de recordar que direcciones IP. Ejemplos de nombres de dominio conocidos son espn.com o google.com.

En este punto es donde el sistema DNS interviene con una función que a grandes rasgos es simple, pero imprescindible para el consumo de los diferentes servicios que se proveen a través de Internet. El DNS realiza la traducción de los nombres de dominio a sus respectivas direcciones IP y viceversa, este proceso se denomina **Resolución DNS**, gracias al cual, nuestro navegador es capaz de obtener la dirección IP de un sitio web al cual se desea visitar y con este dato poder concretar el acceso deseado al contenido del sitio.

En acápites anteriores, se ha descrito la importancia del protocolo TCP como base fundamental del funcionamiento de Internet, pero en el caso de las consultas DNS, no se usa TCP, sino más bien **UDP**[25], debido a que es un protocolo más rápido que TCP al no tener un mecanismo de control de flujo ni de recuperación de errores, lo que significa que los paquetes pueden ser enviados sin esperar una respuesta. Esta característica resulta en una mayor rapidez, lo cual es de suma importancia para el proceso de consultas DNS y el motivo del uso de este protocolo.

[25] UDP (User Datagram Protocol) es un protocolo que permite la transmisión sin conexión de datagramas en redes basadas en IP

En el caso de que exista una pérdida de paquetes y la consulta DNS no llegara, a nivel de capa de transporte no hay nada que hacer, así que la corrección se realiza a nivel de capa de aplicación, en la cual existen mecanismos para manejar este tipo de situaciones. Por ejemplo, si una consulta DNS no recibe respuesta después de un cierto período de tiempo, el cliente DNS enviara la consulta nuevamente.

Otra ventaja de usar el protocolo UDP es que se reduce la carga en los servidores DNS, ya que las respuestas no requieren establecer una conexión como en el caso de TCP.

2.5.5.1 ESTRUCTURA DEL SISTEMA DNS EN INTERNET

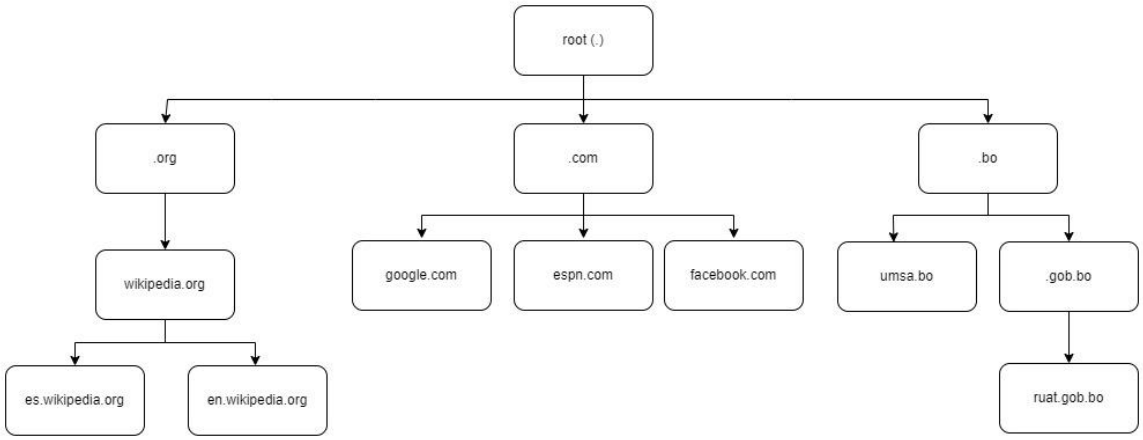
El sistema DNS es un sistema de bases de datos distribuidos en Internet, se dice que es distribuido debido a que la información de nombres y direcciones IP no está concentrada en un grupo único de servidores, sino que está distribuida en múltiples miembros o nodos que forman parte del sistema DNS, los cuales contienen una pequeña parte de la información. Es por esto que las empresas que son dueñas de dominios, son también responsables de proveer sus servidores DNS propios llamados autoritativos, que tienen la función de proveer las direcciones IP de los dominios sobre los que tienen autoridad, de esta forma el mecanismo de traducción entre nombres y direcciones IP es posible.

En el inicio de Internet, en la década de los 70s, se mantenía una lista de nombres de equipos conocidos junto con sus direcciones numéricas en un archivo llamado **hosts.txt**[26], el cual se distribuía periódicamente entre todos los equipos conectados a la red. Pero en la década de los 80s la cantidad de equipos creció de unos centenares a decenas de miles, con lo cual el mantener, distribuir y evitar nombres repetidos llego a ser inmanejable. Por esto en 1983 se creó el sistema DNS, con el objetivo de automatizar el proceso de identificación de las direcciones IP de los dominios existentes en Internet.

[26] El archive hosts.txt aún existe en los sistemas operativos modernos y se puede usar como un mecanismo de resolución alterno.

El sistema creado es un sistema jerárquico que tiene un origen único llamado raíz, del cual se originan múltiples ramas que a su vez se dividen en otras ramas originando un esquema distribuido y cuya administración también es distribuida.

Figura 2.5.4 Estructura Jerárquica del Sistema DNS en Internet



Fuente: Elaboración Propia

En el diagrama se representa la estructura jerárquica mencionada y se puede ver que existen diferentes niveles. También se puede ver ejemplos de algunas ramas y subdivisiones que se van creando a partir de ellas. Cada rama se denomina zona y su administración es independiente de otras zonas. El administrador de una zona puede crear nuevas zonas por debajo y delegar su administración a otra organización.

La raíz no tiene nombre y es representada por un punto '**.**', su administración está a cargo de la **ICANN**[27] y solo se utiliza para para delegar la administración de las zonas de primer nivel que reciben el nombre de **Nombres de Dominio de Nivel Superior** o **TLD** por sus siglas en ingles. Los tipos de TLD más importantes son los siguientes: genéricos (**gTLD**) y de código de país (**ccTLD**). Aproximadamente existen 200 gTLD y 1200 ccTLD. Ejemplos de gTLD más conocidos son '.com', '.net', '.org', '.edu', entre otros. Mientras que los ccTLD corresponden a los países, por ejemplo '.bo' corresponde a Bolivia, '.ar' corresponde a Argentina y '.pe' corresponde a Perú.

[27] La ICANN es la Corporación de Internet para la asignación de Nombres y Números. Es responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.

Cada uno de los nodos del árbol jerárquico está compuesto por un grupo de servidores que se encargan de resolver un conjunto determinado de dominios correspondiente a su zona de autoridad.

2.5.5.2 SISTEMAS DNS DENTRO DE UN ISP

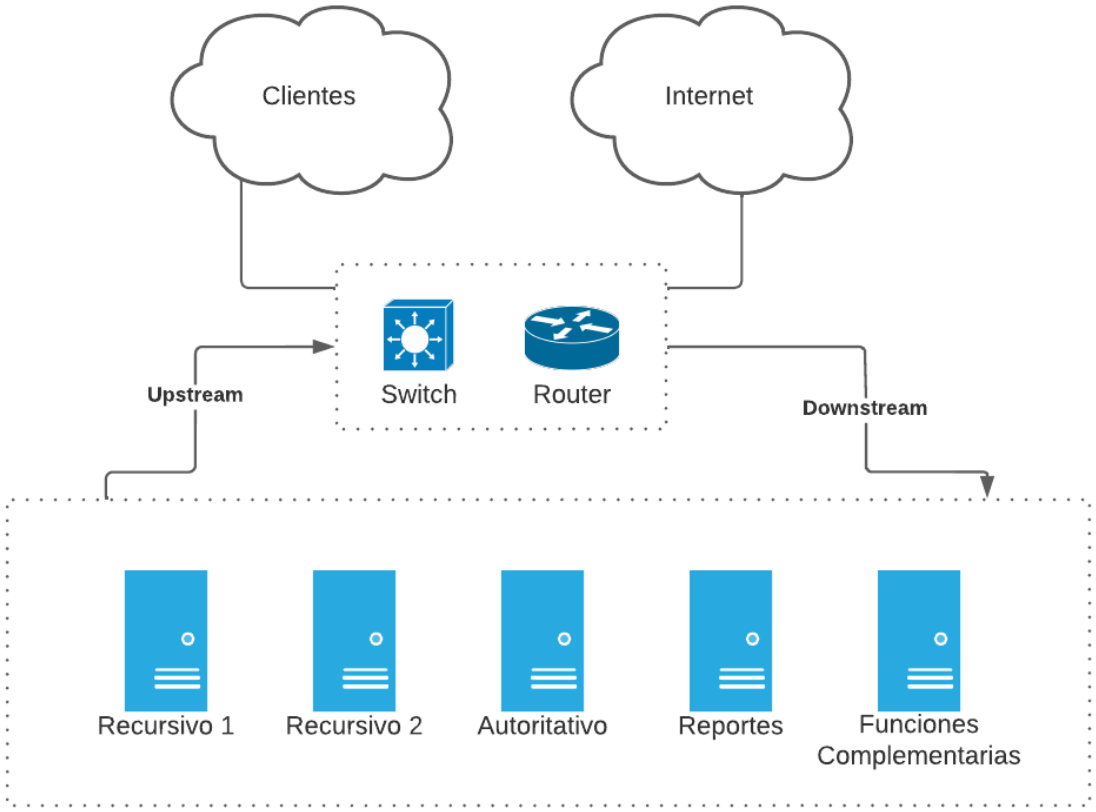
Los proveedores de servicios de acceso a Internet (ISP) integran en su infraestructura de red un sistema DNS, cuyas direcciones IP se configuran en los enrutadores o módems instalados en los domicilios de los usuarios en el caso del servicio de Internet Fijo, o en los equipos de telefonía celular para el caso del servicio de Internet Móvil. De esta manera, los usuarios acceden a Internet utilizando el sistema DNS de su ISP.

Entre los motivos por los cuales un ISP cuenta con un sistema DNS propio están los siguientes:

- **Calidad de Servicio**: al estar la red del ISP más cerca a nivel de IP, puede ofrecer una respuesta más rápida a las consultas DNS, lo cual tiene un impacto positivo en la velocidad del servicio.
- **Ahorro de Ancho de Banda**: al tener un sistema DNS localizado, el ISP puede evitar consultas DNS en sistemas DNS externos a su red, reduciendo así la carga en su ancho de banda y mejorando el rendimiento.
- **Personalización de la Experiencia del Usuario**: el ISP puede personalizar la experiencia de navegación del usuario a través del DNS, proporcionando respuestas DNS diferentes basadas en el tipo de solicitud y la ubicación geográfica del usuario, o priorizar ciertos tipos de tráfico como por ejemplo el de servicios de Streaming o videoconferencia, para mejorar la experiencia del usuario final.
- **Seguridad y Protección**: el ISP puede utilizar su sistema DNS para proteger a sus usuarios de sitios web maliciosos o fraudulentos, mediante políticas aplicadas a nivel del DNS.
- **Monetización**: algunos ISP pueden aprovechar su sistema DNS para obtener ingresos adicionales, como, por ejemplo, mediante la inclusión de publicidad en los resultados de búsqueda de DNS.

El sistema DNS es una pieza crítica en la infraestructura de Internet, ya que permite traducir los nombres de dominio en direcciones IP para que los dispositivos puedan conectarse entre sí. En el caso de los proveedores de servicios de Internet, la importancia del sistema DNS es aún mayor, ya que es esencial para ofrecer el acceso a Internet a sus clientes. Si el sistema DNS del proveedor falla, todos los servicios que dependen de Internet se verán afectados, desde el correo electrónico hasta las redes sociales, pudiendo ocasionar una interrupción de servicio en casos extremos. Incluso un ligero retraso en las consultas DNS puede causar una degradación en la calidad del servicio, lo que puede traducirse en una experiencia de usuario lenta y frustrante. Por lo tanto, es esencial que los proveedores de servicios de Internet mantengan un sistema DNS robusto y confiable para garantizar una experiencia de usuario óptima.

Figura 2.5.5 Diagrama de un sistema DNS genérico para un operador ISP



Fuente: Elaboración Propia

2.5.5.2.1 SERVIDORES RECURSIVOS

La función más importante de los sistemas DNS es realizar la traducción entre los nombres de dominio y sus direcciones IP, esta operación se denomina **Resolución DNS**.

Dentro de la arquitectura de un sistema DNS de un ISP, los elementos que se encargan de ejecutar las operaciones de resolución DNS son los servidores recursivos, lo que los convierte en los elementos más importantes de este tipo de sistema.

Los servidores recursivos responderán directamente las peticiones de resolución DNS de los usuarios, respondiendo desde su cache interno o realizando peticiones DNS a su vez a otros sistemas DNS de mayor jerarquía para poder obtener la dirección IP del recurso que el usuario está consultando.

El proveedor del sistema DNS debe dimensionar la cantidad y capacidad de los servidores recursivos necesarios para un determinado ISP, basado en datos estimados o medidos sobre el número de consultas que se esperan recibir en la **hora pico**[28], además de criterios de disponibilidad y redundancia del ISP. De esta forma, se asegura que el sistema DNS pueda manejar el volumen de tráfico y ofrecer un servicio confiable a los usuarios.

2.5.5.2.2 SERVIDORES AUTORITATIVOS

Los servidores DNS del tipo **Autoritativo**, son servidores que están autorizados para responder consultas DNS para un dominio específico. Estos servidores cuentan con una base de datos local de los registros DNS para ese dominio, y se encargan de actualizar la información de los registros DNS cuando es necesario. En resumen, los servidores autoritativos son uno de los múltiples nodos que conforman la base de datos distribuida en Internet que compone el sistema DNS.

Mediante los servidores autoritativos, el ISP puede alojar los registros de sus propios dominios, permitiendo que la compañía publique su propio sitio web, y ofrezca al público todas las aplicaciones que dispone, tanto web como aplicaciones móviles, de esta forma el

[28] En sistemas de telecomunicaciones se define la hora pico como aquella hora de mayor tráfico durante el día.

usuario podrá realizar subscripciones a los servicios que ofrece el ISP, realizar consultas y reclamos sobre su servicio, realizar pago de facturas, por mencionar algunos.

Los servidores autoritativos de un ISP también pueden alojar dominios de otras empresas. Las empresas que deseen utilizar este servicio pueden contratarlo al ISP por una tarifa. De esta manera, su sitio web y otros servicios web pueden estar disponibles en Internet, y el ISP se encarga de la gestión de los registros DNS asociados a estos dominios.

2.5.5.2.3 SERVIDORES DE MANTENIMIENTO Y REPORTES

Dependiendo del tamaño del sistema y del diseño del fabricante, las funciones de mantenimiento y de reportes o estadísticas, pueden conformar un solo módulo funcional o conformar módulos funcionales separados.

La funcionalidad de mantenimiento se refiere a la capacidad del sistema de controlar que las funciones y procesos principales que conforman el sistema estén operando dentro de los parámetros normales de funcionamiento, pudiendo el propio sistema generar alarmas en un panel de control o **Dashboard**, o en su defecto alertar al sistema de gestión del ISP, mediante protocolos como por ejemplo **SNMP**[29], para que el personal a cargo del monitoreo continuo de la red pueda tomar acciones correctivas. Es importante destacar que esta funcionalidad es esencial para garantizar la disponibilidad y la confiabilidad del sistema, y reducir el tiempo de inactividad en caso de fallos o problemas.

La funcionalidad de reportes y de estadísticas consiste en la recolección y almacenamiento de datos de tráfico de la red, los cuales luego son procesados, analizados y presentados visualmente para que los administradores del sistema puedan revisar los niveles de trafico de la red, el uso del sistema y otros indicadores importantes. Esta funcionalidad permite tomar decisiones informadas y oportunas para optimizar el rendimiento de la red y el sistema, planificar expansiones y también para detectar y solucionar problemas de forma proactiva.

[29] SNMP quiere decir 'Simple Network Protocol Management', es un protocolo de red que permite monitorear el estado y rendimiento de un elemento de la red, así como también realizar tareas de configuración remota.

2.5.5.2.4 OTRAS FUNCIONALIDADES

Un sistema DNS puede ofrecer otras funcionalidades adicionales que complementan las funciones descritas en acápites anteriores. A continuación, se describen algunas.

La funcionalidad RKS (Reputation Knowledge Server) se utiliza en la protección contra correo no deseado. Su función principal es recopilar y almacenar información sobre la reputación de las direcciones IP y los nombres de dominio que envían correo electrónico. Se utiliza esta información para evaluar la confiabilidad de los remitentes de correo electrónico y determinar si los mensajes entrantes deben ser bloqueados o entregados a los destinatarios, por ende, el RKS trabaja junto con otros sistemas de protección contra el spam, como los sistemas de filtrado de correo electrónico, para mejorar la efectividad de la protección contra el correo no deseado.

Funcionalidades de protección contra ataques de denegación de servicio (DDoS). Los sistemas DNS pueden ser objeto de ataques de denegación de servicio distribuidos, por lo que los proveedores de servicios de Internet a menudo implementan medidas de protección contra este tipo de ataques en sus sistemas DNS.

Funcionalidades de distribución de contenido. Los sistemas DNS también pueden utilizarse para distribuir contenido, por ejemplo, al proporcionar a los usuarios direcciones IP diferentes según su ubicación geográfica para acceder al contenido más cercano.

2.5.5.3 PROCESO DE CONSULTAS DNS

Cada vez que un usuario hace uso de un dispositivo para acceder a algún servicio de Internet, por ejemplo, navegar por páginas web, abrir algún aplicativo móvil o acceder a algún servicio de Streaming, se producen múltiples consultas DNS. El dispositivo puede ser un ordenador, un dispositivo móvil, un equipo de televisión inteligente (Smart TV) o una consola de juegos.

2.5.5.3.1 CONSULTA AL CACHE DNS LOCAL

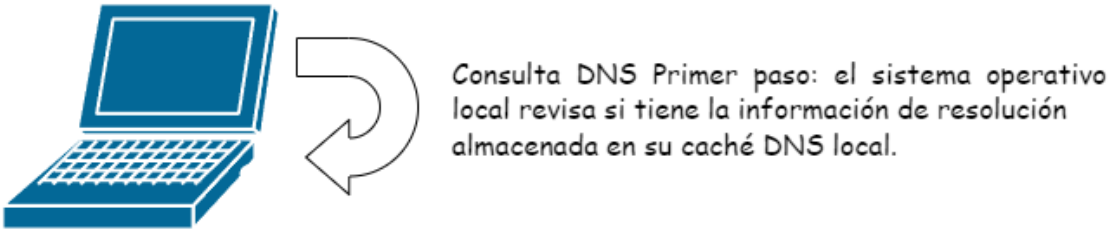
En el entorno local del usuario, se tienen a disposición dos sistemas de cache de DNS locales, uno provisto por el navegador que el usuario está utilizando, por ejemplo, Chrome, Firefox o Edge, y el otro que es provisto por el sistema operativo.

El primer paso en el proceso de consulta DNS consiste en verificar si la información de resolución se encuentra en los caches locales. El cache más relevante es el del sistema operativo, el cual está presente en todos los dispositivos mencionados, como ordenadores, dispositivos móviles, Smart TVs y consolas de juegos. Este cache local se llena con las respuestas a las solicitudes previas realizadas al sistema DNS del ISP y se almacena durante un período de tiempo definido, conocido como Tiempo de Vida (TTL), que generalmente varía entre 12 y 24 horas. En algunos sistemas operativos, los usuarios tienen la capacidad de configurar este tiempo. Por ejemplo, sistemas operativos como Windows, Linux y macOS permiten esta funcionalidad.

El uso de la memoria cache local mejora significativamente el rendimiento del sistema al reducir el tiempo de respuesta de las consultas DNS y disminuir el tráfico de red. Con la memoria cache local, los tiempos de respuesta están por debajo de los 10 milisegundos, mientras que, si es necesario buscar el dato de resolución en Internet, este tiempo puede superar los 100 milisegundos. A primera vista, estos tiempos puede parecer pequeños, pero la mayoría de los sitios web modernos, requieren múltiples consultas DNS para cargar recursos como imágenes, videos u otro contenido, el número de consultas puede en algunos casos llegar al orden de cientos. En esta situación, incluso un tiempo de milisegundos puede convertirse en segundos, lo que en la práctica es perceptible y afecta la experiencia del usuario.

Sin embargo, es importante tener en cuenta que, si el cache DNS local contiene una respuesta incorrecta u obsoleta, esto puede provocar errores de DNS y problemas de acceso a sitios web. Por esta razón, los sistemas operativos tienen herramientas para que el usuario pueda limpiar el cache en caso de tener problemas de acceso. De esta manera, el sistema DNS del dispositivo puede volver a realizar una consulta DNS y obtener la respuesta correcta y actualizada del servidor DNS autoritativo correspondiente.

Figura 2.5.6 Consulta DNS: Primer Paso



Fuente: Elaboración Propia

En caso de que el sistema operativo tenga la información de resolución del sitio web consultado, entonces el proceso de resolución concluye y se accede al sitio web.

2.5.5.3.2 CONSULTA AL DNS DEL ISP

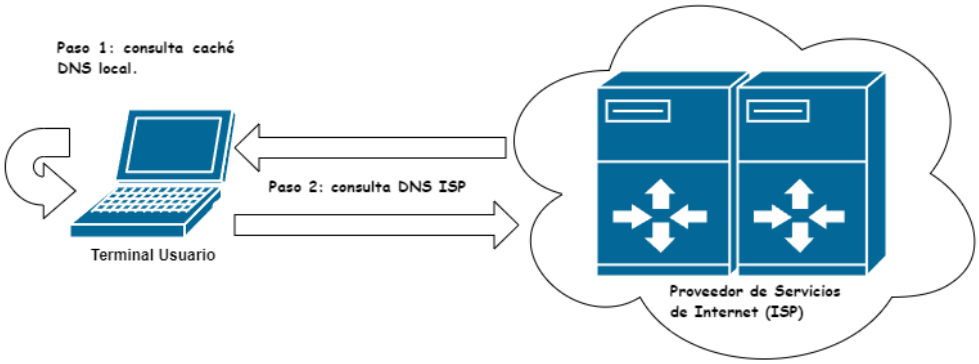
En el segundo paso abordamos la situación en la cual el ordenador del usuario no tenga almacenada la información de resolución necesaria para el sitio o aplicación web que se desea consumir. En este caso, la consulta DNS debe ser dirigida a un servidor DNS externo, específicamente, el servidor DNS de su proveedor de servicios de Internet (ISP). Si es que este servidor cuenta con la información de resolución solicitada, se la devuelve directamente al ordenador que originó la petición concluyendo la consulta DNS, en caso contrario el proceso de consulta debe extenderse a servidores externos.

Cabe hacer notar que los servidores recursivos que responden las consultas DNS a los usuarios cuentan con sistemas de caches internos similares a los que se han descrito para el caso de los ordenadores de los usuarios, y se aplica la misma lógica.

Para que el ordenador del usuario pueda realizar esta consulta, es necesario que se haya configurado la dirección IP del servidor DNS del ISP en el **enrutador de su red local**[30]. Esta configuración generalmente es realizada por el personal del ISP en el momento de la instalación del servicio de acceso a Internet en el domicilio u oficina del usuario.

[30] Se refiere al equipo denominado enrutador o modem que personal del ISP, instala y configura al momento de realizar el servicio de instalación en el domicilio del usuario.

Figura 2.5.7 Consulta DNS: Segundo Paso



Fuente: Elaboración Propia

Normalmente, desde el ordenador del usuario, es posible que no se pueda visualizar los datos de dirección IP local, y tampoco la dirección DNS, estos datos, sin embargo, se pueden consultar en algunos sitios de Internet. Por ejemplo:

https://ipleak.net/

https://www.top10vpn.com/es/herramientas/cual-es-mi-dns/

En donde se puede ver que el DNS primario pertenece al ISP Entel, y como DNS secundario se tiene un DNS de Google:

Figura 2.5.8 Consulta de Servidores DNS

¿Cuál es mi servidor DNS?

Our DNS server checker tool verifies and displays the DNS servers your device is using. It also reveals the country and the owner (ISP) of the DNS server processing your requests.

Pulsa para ver tus servidores DNS.

País	ISP	Servidor DNS
BO	Entel S.A. - EntelNet	168.205.99.141
US	GOOGLE - Google LLC	173.194.91.66
BO	Entel S.A. - EntelNet	2800:cd0:ff:1:81b3:bf88:2753:90be

Fuente: https://www.top10vpn.com/es/herramientas/cual-es-mi-dns/

Es importante mencionar que en este punto el usuario tiene la posibilidad de configurar manualmente una dirección DNS en su ordenador. Los sistemas operativos más comunes como Windows, Linux o macOS brindan esta opción. En Internet existe una infinidad de DNS públicos y gratuitos como se puede ver a continuación:

Figura 2.5.9 Servidores DNS Públicos y Gratuitos

Proveedor de DNS	Dirección principal	Dirección secundaria
1. Google Public DNS	8.8.8.8	8.8.4.4
2. Cloudflare	1.1.1.1	1.0.0.1
3. OpenDNS	208.67.222.222	208.67.220.220
4. CyberGhost	38.132.106.139	194.187.251.67
5. Quad9	9.9.9.9	149.112.112.112
6. OpenNIC DNS	192.71.245.208	94.247.43.254
7. DNS.Watch	84.200.69.80	84.200.70.40
8. Yandex DNS	77.88.8.88	77.88.8.2
9. Neustar DNS	156.154.70.5	156.154.71.5
10. CleanBrowsing	185.228.168.9	185.228.169.9
11. Comodo Secure	8.26.56.26	8.20.247.20
12. UncensoredDNS	91.239.100.100	89.233.43.71
13. FreeDNS	45.33.97.5	37.235.1.177
14. Verisign Public DNS	64.6.64.6	64.6.65.6
15. SafeServe	198.54.117.10	198.54.117.11

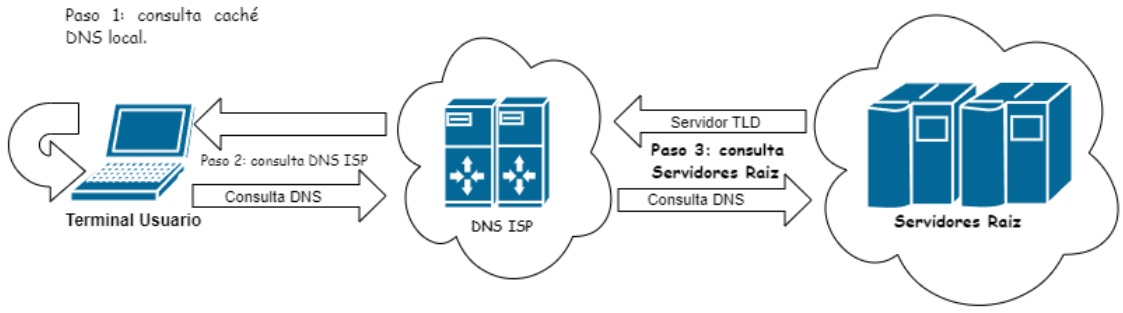
Fuente: https://es.wizcase.com/blog/mejores-servidores-dns-publicos-y-gratuitos/

Un usuario puede optar por esta alternativa, debido a que el ISP este bloqueando el acceso a algún sitio web, o que el sistema DNS del ISP no esté funcionando correctamente. En general, es importante comprender que, si bien es posible cambiar la configuración de DNS en el propio ordenador, el DNS proporcionado por su ISP suele ser el más confiable y seguro. Por lo tanto, si el servicio de DNS del ISP está funcionando correctamente, es recomendable mantenerlo en lugar de cambiar a un DNS público.

2.5.5.3.3 CONSULTAS A LOS SERVIDORES RAÍZ

Como se mencionó en el acápite anterior, en el caso de que los servidores recursivos del sistema DNS del ISP no cuenten con la información de resolución solicitada, estos a su vez realizan una petición de consulta a los servidores raíz, una vez que la búsqueda llega a la zona raíz, la búsqueda bajará en la jerarquía del sistema DNS, alcanzando primero los servidores TLD, luego los servidores para dominios específicos hasta encontrar el servidor que tiene la dirección IP del sitio o aplicación Web que el usuario desea consumir.

Figura 2.5.10 Consulta DNS: Tercer Paso



Fuente: Elaboración Propia

Los servidores raíz son una parte esencial de la infraestructura de Internet. Su principal función es indicar a los servidores recursivos de los sistemas DNS de los ISP a qué servidor TLD deben enviar la solicitud de consulta para poder resolver el nombre de dominio solicitado.

Los servidores raíz administran la zona raíz del DNS, la cual está compuesta de 13 direcciones IP posibles para estos servidores. Esta cantidad obedece a limitaciones de los servidores de la época en la cual se diseñó la arquitectura original de DNS, los cuales eran computadoras muy limitadas en capacidad de procesamiento para las cuales manejar un gran número de direcciones IP hubiera sido difícil en términos de escalabilidad y rendimiento.

En los primeros tiempos de Internet, solo había un servidor para cada una de las 13 direcciones IP, pero en la actualidad, cada una de ellas tiene varios servidores, que utilizan el enrutamiento **Anycast**[31] para distribuir las solicitudes en función de la carga y la proximidad. Por ejemplo, cuando un cliente ubicado en América del Sur envía una solicitud a una dirección IP Anycast de un servidor raíz, la solicitud es dirigida al servidor raíz más cercano geográficamente, que seguramente estará ubicado en América del Sur. Actualmente, hay más de 600 servidores raíz de DNS diferentes distribuidos por todos los continentes.

Es importante mencionar que el protocolo Anycast es el que hace posible que múltiples servidores puedan responder a una misma dirección IP. Cuando un cliente envía una solicitud a una dirección IP Anycast, la solicitud es enviada a uno de los servidores Anycast disponibles, y la respuesta es enviada de vuelta al cliente. Los servidores Anycast pueden estar geográficamente distribuidos y pueden tener diferentes capacidades, pero desde el punto de vista del cliente, todos los servidores Anycast se ven como un solo servidor en la red. De esta manera, se puede distribuir la carga de tráfico de red y mejorar la disponibilidad y redundancia del servicio.

[31] Anycast: técnica de enrutamiento que permite que varias máquinas respondan a una misma dirección IP. Para una mayor explicación: https://es.wikipedia.org/wiki/Difusi%C3%B3n_por_proximidad

Las 13 direcciones IP de los servidores DNS raíz son las siguientes:

Figura 2.5.11 Lista de los 13 Servidores DNS Raíz

List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Fuente: https://www.iana.org/domains/root/servers

Debido a que la zona raíz del DNS está en la parte superior de la jerarquía del DNS, los servidores recursivos no pueden dirigirse a ellos en una búsqueda de DNS. Por ello, todos los servidores recursivos tienen una lista de las 13 direcciones IP de los servidores raíz integrada en su software. Es decir que siempre que se inicia una consulta DNS, la primera comunicación del servidor recursivo es con una de esas 13 direcciones IP.

2.5.5.3.4 CONSULTAS A LOS SERVIDORES TLD

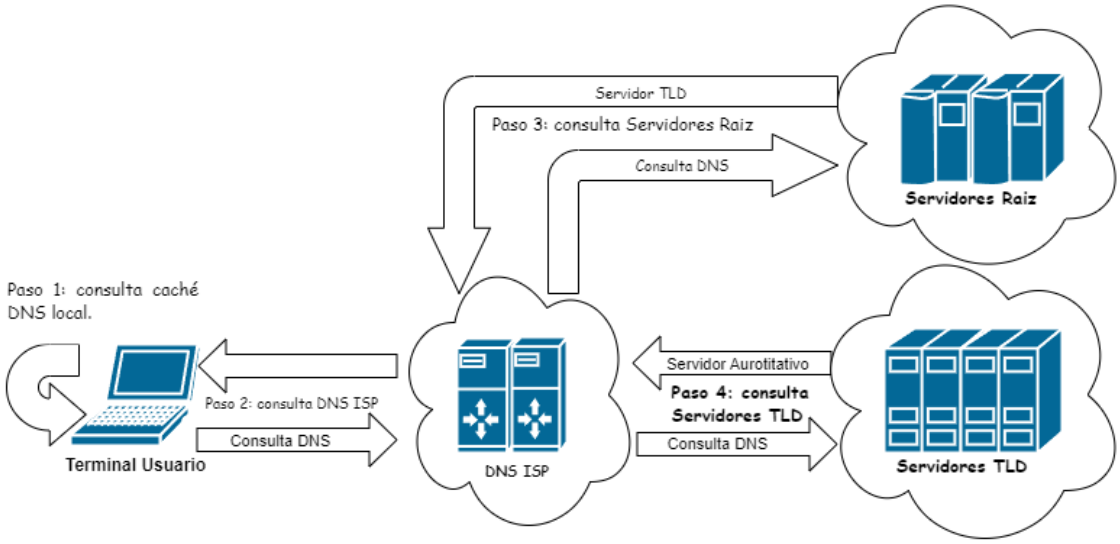
Como se mencionó en el acápite anterior, cuando los servidores recursivos no tienen la información de resolución almacenada en su cache, acuden a los servidores raíz, quienes devuelven la dirección del servidor TLD que corresponda al dominio de la página o aplicación web que se desea consumir.

Dentro de las direcciones web que colocamos en nuestro navegador, un TLD está representado por todo lo que va después del punto final de un nombre de dominio. Por ejemplo, en el nombre de dominio **google.com**, la parte '**.com**' es el TLD, o para el nombre

de dominio **cbasicoing.umsa.edu.bo**, **'.bo'** es el TLD. Otros TLD populares son por ejemplo **'.org'**, **'.uk'**, **'.edu'**.

El servidor TLD devolverá la dirección del servidor autoritativo que tiene la dirección del recurso solicitado, para el ejemplo **cbasicoing.umsa.edu.bo,** es el servidor de la zona **'.edu.bo'**.

Figura 2.5.12 Consulta DNS: Cuarto Paso



Fuente: Elaboración Propia

Desde el punto de vista del DNS, es importante mencionar a las principales entidades que realizan las funciones de control del sistema de nombres de dominio. La más importante es la **ICANN** (Internet Corporation for Assigned Names and Numbers), la cual es una organización sin fines de lucro que se encarga de coordinar y supervisar el sistema de nombres de dominio (DNS) de Internet a nivel global. Su función principal es administrar la asignación de direcciones IP, los nombres de dominio de nivel superior (TLD) y la gestión del sistema de servidores raíz de DNS. La ICANN fue creada en 1998 y se encarga de trabajar con todas las partes interesadas de la comunidad de Internet, incluyendo gobiernos, empresas, organizaciones no gubernamentales y usuarios individuales, siendo

sus funciones fundamentales y cruciales para asegurar la estabilidad, seguridad y resiliencia del DNS y del sistema de nombres de dominio en general.

La **IANA** (Internet Assigned Numbers Authority) es una sección dentro de la ICANN, que tiene la función específica de asignar y mantener los identificadores únicos en Internet, como direcciones IP, nombres de dominio de nivel superior (TLD) y garantiza que los recursos y parámetros necesarios para la comunicación en Internet estén organizados y asignados de manera eficiente.

La IANA reconoce oficialmente tres tipos de TLD:

- **gTLD (Generic Top-Level Domains)**: dominios genéricos de alto nivel.
- **sTLD (Sponsored Top-Level Domains)**: dominios patrocinados de alto nivel.
- **ccTLD (Country Code Top-Level Domains)**: dominios de código de país.

Como se mencionó en secciones anteriores, los TLD más importantes son los gTLD y los ccTLD. Los gTLD más conocidos son por ejemplo **'.com'**, **'.net'**, **'.org'**, entre otros. Mientras que el ccTLD más conocido en nuestro entorno sería el '**.bo**' que corresponde a Bolivia.

Alrededor del 2011, la ICANN abrió la puerta a que las compañías y organizaciones pudieran tener sus propios gTLD, lo cual ha ampliado significativamente la lista de TLD disponibles, pasando de una veintena a tener en la actualidad más de mil TLD. La lista completa se puede consultar en el sitio de la IANA:

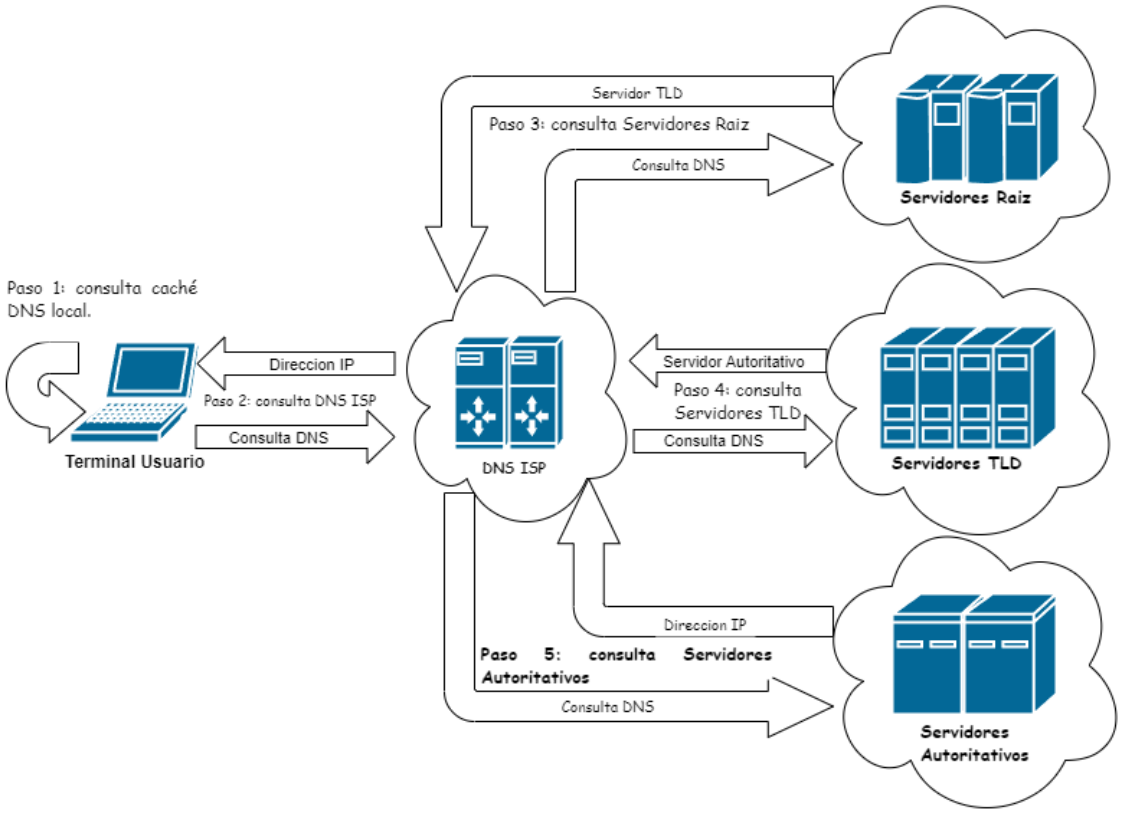
https://www.iana.org/domains/root/db

2.5.5.3.5 CONSULTAS A LOS SERVIDORES AUTORITATIVOS

Una vez que el servidor TLD devuelve la dirección del servidor autoritativo para el dominio solicitado, el servidor recursivo se conecta a ese servidor autoritativo y le realiza la misma consulta DNS. Si el servidor autoritativo tiene la información de resolución en su cache, la proporciona al servidor recursivo inmediatamente. De lo contrario, el servidor autoritativo busca la información de resolución en sus registros DNS.

Es posible que el servidor autoritativo no tenga la información de resolución solicitada, en cuyo caso proporcionará la dirección del servidor autoritativo que posee la información final. Una vez que el servidor autoritativo tiene la información de resolución, la devuelve al servidor recursivo, quien a su vez la devuelve al cliente que realizó la consulta original. La respuesta puede incluir la dirección IP del servidor que aloja la página o aplicación web buscada, o indicar que no se pudo encontrar la información de resolución para ese dominio, lo que finaliza el proceso.

Figura 2.5.13 Consulta DNS: Quinto Paso



Fuente: Elaboración Propia

Un servidor autoritativo alberga los registros de recursos DNS que pertenecen a una zona por la cual es responsable. Este es el servidor al final de la cadena de búsqueda DNS que responde con el registro del recurso consultado al servidor recursivo, el cual transmite este

dato al cliente que originó la consulta, permitiendo que el navegador haga la solicitud para llegar a la dirección IP necesaria para acceder al recurso web solicitado.

Los servidores autoritativos generalmente usan un sistema de almacenamiento propio. Los datos se almacenan en archivos de zona que contienen los registros DNS para el dominio del cual el servidor es responsable. Estos archivos de zona se almacenan en el sistema de archivos del servidor DNS y se actualizan regularmente.

Existen varios formatos de archivo de zona, pero uno de los más comunes es el formato BIND (Berkeley Internet Name Domain), utilizado por el software de servidor DNS más popular. El archivo de zona BIND es un archivo de texto plano que contiene una lista de registros DNS en un formato específico.

Aunque BIND es uno de los servidores DNS más populares y utiliza su propio formato de archivo para almacenar los registros DNS, otros servidores DNS como PowerDNS o MaraDNS pueden utilizar bases de datos como MySQL o PostgreSQL para almacenar sus registros. En general, el formato de almacenamiento de los registros DNS puede variar según el software utilizado, pero el objetivo final es siempre el mismo: proporcionar una respuesta rápida y precisa a las consultas DNS entrantes.

2.5.5.4 REGISTROS DNS

Un registro DNS es una entrada en una base de datos de un servidor DNS autoritativo que almacena información sobre un recurso de red específico, como una dirección IP, un nombre de host, una dirección de correo electrónico o un servidor de correo. Es una pieza de información que se utiliza para resolver consultas de DNS y permitir la conexión a recursos de red. Cada registro DNS tiene un formato específico y su contenido y estructura varían según el tipo de registro y la función que cumple en el sistema de nombres de dominio.

El formato de los registros DNS es muy sencillo, se tiene básicamente una línea para cada registro, la cual tiene el siguiente formato:

<name> <ttl> <class> <type> <rdlength> <radata>

Los campos están separados por un espacio, y se debe considerar también que algunos campos son opcionales.

- **name**: el nombre del dominio.
- **ttl**: el TTL (Time to Live) indica el tiempo en segundos que un registro DNS será almacenado en la memoria cache de los servidores recursivos que han realizado la consulta. Después de este tiempo, el registro puede ser descartado y debe ser consultado de nuevo para obtener información actualizada. El TTL es una medida de cuánto tiempo puede sobrevivir una respuesta DNS antes de que deba ser renovada.
- **class**: normalmente los registros DNS que se utilizan actualmente pertenecen a la clase IN (Internet), por lo que es común que este parámetro sea omitido en las consultas DNS.
- **type**: existen varios tipos de registros DNS, por ejemplo, A, MX, CNAME, entre otros. Se explicará cada caso en siguientes secciones.
- **rdlength**: este campo es opcional en algunos registros, pero si está presente debe contener el tamaño correcto de los datos en el registro de recursos.
- **rdata**: se refiere a la información específica del recurso DNS consultado, que está asociada con el nombre de dominio.

Se describen a continuación los tipos de registros más importantes y comúnmente usados, pero se aclara que existen alrededor de 40 tipos de **registros DNS**[32] diferentes.

2.5.5.4.1 REGISTROS TIPO A Y AAAA

El registro A es probablemente el tipo de registro DNS más importante y también es el más utilizado. Un registro A apunta a una dirección IP para un sitio web o nombre de dominio.

El objetivo del registro A es cumplir la función más importante del DNS, que es asociar una dirección IP con un nombre de dominio.

[32] La lista completa se puede consultar en: https://es.wikipedia.org/wiki/Anexo:Tipos_de_registros_DNS

Ejemplo:

www.example.com. 12879 IN A 93.184.216.34

El registro empieza con el nombre completo del dominio, incluyendo un punto al final, esta notación recibe el nombre de **FQDN**[33]. La información del registro se mantendrá en la memoria cache durante 12879 segundos antes de que deba ser actualizada. La clase es IN que corresponde a Internet. El campo type indica que se trata de un registro tipo A, mientras que el campo de tamaño del registro está vacío, por lo que se toma el valor por defecto igual a 4. El último campo (rdata) contiene la dirección IP.

Los registros del tipo AAAA cumplen la misma función que los registros tipo A, pero se aplican para direcciones IPv6.

2.5.5.4.2 REGISTROS TIPO CNAME

Un registro CNAME (Canonical Name Record) contiene el nombre de otro dominio en lugar de una dirección IP. Este tipo de registro se utiliza para establecer una relación de alias entre dos nombres de dominio. Cuando se consulta un dominio que tiene un registro CNAME, la respuesta apunta al nombre de dominio al que se hace referencia en el registro CNAME, y luego se busca el registro correspondiente (generalmente tipo A o AAAA) para obtener la dirección IP real.

A través de este tipo de registros se consigue que el acceso a un sitio o recurso web se pueda hacer a través de más de un nombre, estos nombres alternativos o alias pueden ser tantos como se desee.

La ventaja de usar registros CNAME es que, si la dirección IP de un dominio cambia, solo se necesita actualizar el registro tipo A correspondiente, y los registros CNAME asociados seguirán apuntando al nuevo nombre de dominio.

[33] FQDN (Fully Qualified Domain Name): Nombre de dominio completo y absoluto que especifica de manera única la ubicación exacta de un host dentro de la jerarquía del Sistema DNS. Un FQDN incluye tanto el nombre de host como el dominio, así como el dominio de nivel superior (TLD), separados por puntos. Por ejemplo, "www.ejemplo.com" es un FQDN, donde "www" es el nombre de host, "ejemplo" es el dominio y "com" es el TLD.

Ejemplo:

```
$TTL 11107
www.example.com.    IN    A        93.184.216.34
www.example.net.    IN    CNAME    www.example.com.
www.example.org.    IN    CNAME    www.example.com.
```

En el ejemplo se ven dos registros CNAME que apuntan al dominio www.example.com, el cual tiene un registro tipo A que resuelve a una dirección IP. El resultado es que si en el navegador se ingresa 'www.example.com', 'www.example.org' o 'www.example.net', se ingresara al mismo recurso web. En este ejemplo y los siguientes se puede ver que el campo TTL se aplica para el grupo de registros.

2.5.5.4.3 REGISTROS TIPO MX

El nombre del registro MX es una abreviación de mail Exchange. Este tipo de registro se utiliza para definir uno o varios servidores de correo electrónico que pertenezcan al dominio en cuestión. Si un dominio dispone de más de un servidor de correo, se pueden establecer niveles de prioridad.

El campo rdata contiene el nombre del servidor de correo electrónico, que también aparece en forma de FQDN.

Ejemplo:

```
$TTL 1200
example.com.    IN    A     93.184.216.34
example.com.    IN    MX    10    mail1.example.com.
example.com.    IN    MX    10    mail2.example.com.
example.com.    IN    MX    50    mail3.example.com.
```

Se observa en primer lugar un registro tipo A, que enlaza el dominio con una dirección IP. A continuación, tenemos tres registros MX que establecen diferentes subdominios que corresponden a tres servidores de correo con los que el dominio cuenta.

La búsqueda de este tipo de registros se realiza en el proceso de envío de correos electrónicos, que en resumen sucede la siguiente forma:

- Un usuario envía un correo electrónico, supongamos a la dirección test@hotmail.com, entonces como primer paso el cliente de correo de origen busca el registro MX del dominio **hotmail.com** mediante una consulta DNS.
- La consulta devuelve el registro MX con la lista de servidores de correo para el dominio **hotmail.com**. El cliente de correo selecciona el servidor con la prioridad más alta.
- El cliente de correo de origen se comunica con el servidor de correo seleccionado y envía el correo electrónico.
- El servidor de correo de destino recibe el correo electrónico y lo guarda en su sistema de correo.

2.5.5.4.4 REGISTROS TIPO PTR

Los registros **PTR**[34] vienen a ser lo opuesto a los registros A, es decir que no asignan un nombre de dominio a una dirección IP, sino justo lo contrario: se conoce la dirección IP y se quiere averiguar el nombre del dominio, es decir, el **URL**[35] mediante el cual se puede acceder al servidor.

Esto quiere decir que para cada dirección IP usada en registros tipo A o AAAA existe, un registro PTR. La dirección IP se forma en este caso en orden opuesto y se le añade, además, el nombre de una zona.

[34] PTR es una abreviación de puntero

[35] URL (Uniform Resource Locator) es una dirección web que se utiliza para identificar y localizar recursos en internet, como páginas web, imágenes o archivos. Está compuesta por elementos como el protocolo (http://, https://), el nombre de dominio (www.ejemplo.com), y la ruta que especifica la ubicación del recurso en el servidor. Las URLs permiten acceder a contenido en la web de manera precisa.

Ejemplo:

Supongamos que tenemos la dirección IP 93.184.216.34 y queremos saber a qué dominio corresponde. Entonces se realiza una consulta DNS a un registro PTR, el cual tendrá la siguiente estructura:

```
$TTL 2100
34.216.184.93.in-addr.arpa. IN PTR example.org.
```

En el campo de nombre podemos ver la dirección IP, pero con los octetos dispuestos en forma inversa y seguidos de **in-addr.arpa**, que es el dominio reservado por la IANA para las búsquedas inversas de DNS (rDNS) en IPv4. En el campo **rdata** viene el nombre de dominio que corresponde a la dirección IP, en este caso es **example.org**.

La aplicación más común de una consulta de DNS inversa es la verificación de la autenticidad del remitente de un correo electrónico. Muchos servidores de correo electrónico utilizan la comprobación de rDNS como una medida de seguridad para evitar correos electrónicos no deseados o fraudulentos, ya que los servidores de correo legítimos suelen estar configurados para responder a una consulta de rDNS con un registro PTR correspondiente al nombre del servidor de correo.

Además, la consulta de rDNS también puede ser útil en la solución de problemas de red, ya que permite a los administradores de sistemas y de red verificar la resolución inversa de direcciones IP y asegurarse de que la configuración de DNS de su red está funcionando correctamente.

2.5.5.5 SEGURIDAD DEL DNS

El sistema de nombres de dominio fue diseñado a mediados de la década los 80, cuando el acceso a Internet estaba restringido a agencias gubernamentales, científicos y militares. A los primeros arquitectos del sistema les preocupaba la fiabilidad y la funcionalidad, no así la seguridad. Como resultado, los servidores DNS siempre han sido vulnerables a una amplia gama de ataques, como ser la denegación de servicio, suplantación de identidad, la amplificación DNS, entre los más importantes.

Se describen a continuación los ataques más conocidos, aunque es importante saber que siempre habrá nuevas técnicas y métodos que se utilizan para realizar ataques a sistemas DNS.

2.5.5.5.1 ATAQUES COMUNES A UN SISTEMA DNS

Ataque de denegación de servicio distribuido (DDoS): son aquellos en los que un atacante intenta sobrecargar el servidor DNS recursivo con un gran número de consultas, para que no tenga capacidad de responder a peticiones legítimas. Estos ataques pueden ser realizados desde múltiples dispositivos, es por esto que se incluye la palabra **distribuido**. Si este tipo de ataque es exitoso, se interrumpirá el consumo de servicios de Internet, o se degradará significativamente.

Envenenamiento de cache DNS: en este tipo de ataque, un atacante envía respuestas DNS falsas al servidor DNS con el objetivo de modificar la información almacenada en su cache. Este tipo de ataque no es sencillo de realizar, pero es posible debido a que las solicitudes y respuestas DNS usan el protocolo UDP, con el cual no existe garantía de que una conexión esté abierta, que el destinatario esté listo para recibir, o que el emisor sea quien dice ser. Por esta razón, UDP es vulnerable a la falsificación; un atacante puede enviar un mensaje mediante UDP y pretender que es una respuesta de un servidor legítimo falsificando los datos del encabezado. En caso de ser exitoso, puede provocar que el servidor redirija a los usuarios a sitios web maliciosos o les impida acceder a sitios legítimos.

Suplantación de identidad (phishing): en este tipo de ataque, los atacantes crean sitios web falsos que se parecen a sitios web legítimos, con el objetivo de engañar a los usuarios para que ingresen sus credenciales de inicio de sesión. Una vez que los atacantes obtienen estas credenciales, pueden utilizarlas para acceder a los servicios reales, uno de los casos más graves es el de la obtención de credenciales bancarias usando este método.

Se puede deducir que el segundo y tercer método son complementarios, es decir primero se engaña al DNS para que dirija al usuario a un sitio web falso, en el cual se le intentara robar datos confidenciales.

Ataques de amplificación DNS: este es un tipo de ataque de denegación de servicio que utiliza servidores DNS mal configurados para inundar a una víctima con tráfico de red compuesto por respuestas DNS **amplificadas**. El ataque aprovecha la capacidad del protocolo DNS para permitir que las consultas sean respondidas por un servidor remoto, lo que significa que los atacantes pueden enviar solicitudes DNS falsificando su dirección IP en las solicitudes para que parezca que provienen de la víctima a la que desea atacar. Adicionalmente el atacante enviara los tipos de consulta DNS que requieran respuestas de gran volumen, como por ejemplo consultas de reflexión y consultas de amplificación de texto sin formato. El atacante puede enviar estas consultas DNS a un gran número de servidores DNS mal configurados o abiertos, que permiten que cualquiera haga consultas a través de ellos sin autenticación o autorización. La combinación de respuestas amplificadas y que provengan de varias fuentes pueden generar una gran cantidad de tráfico de red que puede saturar su capacidad de ancho de banda y/o recursos de red de la víctima, llevando al estado de denegación de servicio.

2.5.5.5.2 SISTEMAS DE PROTECCIÓN

Las medidas de protección que se pueden aplicar deben dotar al propio sistema DNS de mecanismos de protección y buenas prácticas, y de igual forma ser extensivas a los elementos de red que rodean al sistema DNS, por ejemplo, contando con un diseño de red adecuado.

Redundancia: considerando que estamos abordando un sistema crítico en cualquier red de telecomunicaciones, una consideración muy importante es la redundancia. La redundancia proporcionara una protección nativa frente a cualquier ataque que pueda ocasionar que un recurso DNS quede fuera de servicio. Por ejemplo, un nodo DNS debe contar mínimamente con dos servidores recursivos y un autoritativo configurados en un esquema de redundancia, y un segundo nodo debería ser desplegado en otro centro de datos con similares características que el primero.

Un protocolo de pruebas de redundancia periódicas debe ser ejecutado para asegurar que la redundancia sea realmente efectiva.

Mantenimiento: el mantenimiento debe incluir actividades tales como actualizaciones de software, parches de seguridad, respaldo y recuperación de datos, monitoreo constante y recomendaciones del fabricante entre otros. La realización de estas actividades de forma regular y rigurosa garantizará un sistema DNS más seguro y robusto. Esto también debe ser aplicado a los elementos de red, switches, routers, firewalls que interactúan directamente con el sistema DNS y de los cuales el sistema depende para tener conectividad.

Configuraciones de Seguridad: los servidores que componen el sistema DNS, en especial aquellos que puedan estar expuestos directamente a Internet, deberían tener abiertos solo los puertos que necesitan para cumplir su función, por ejemplo, en un servidor recursivo es el puerto 53 del protocolo UDP. En este sentido es una buena práctica realizar pruebas de penetración con herramientas automáticas para detectar huecos de seguridad.

Otras configuraciones importantes en servidores DNS son la limitación de consultas que puedan provenir desde una misma IP en un intervalo de tiempo determinado y un adecuado control de acceso al sistema.

DNS Security Extensions: más conocido como DNSSEC, es una extensión del protocolo DNS que proporciona una capa de seguridad para las consultas DNS. DNSSEC garantiza que los datos que se reciben en respuesta a una consulta DNS no han sido modificados en el camino entre el servidor DNS y el cliente, y que los datos provienen de una fuente de confianza.

DNSSEC utiliza criptografía de **clave pública**[36] para firmar las respuestas de DNS. Los servidores DNS autoritativos firman la información que se envía a los servidores DNS recursivos, y los servidores DNS recursivos, a su vez, pueden firmar la información que envían a los clientes que hacen consultas.

Cuando un cliente realiza una consulta DNS con DNSSEC habilitado, el servidor DNS envía una respuesta que incluye una firma digital que puede ser verificada por el cliente. Si la firma es válida, el cliente puede estar seguro de que la información recibida es auténtica

[36] La criptografía de clave pública es un método de encriptación que utiliza un par de claves para cifrar y descifrar información. Es una técnica ampliamente utilizada para la transmisión segura de información en redes públicas como Internet.

y no ha sido modificada. De esta forma se ofrece protección contra ataques de envenenamiento de cache.

Es importante tener en cuenta que no todos los dominios utilizan DNSSEC. Si un dominio no está configurado para usar DNSSEC, la respuesta DNS que reciba no estará firmada y no se puede verificar su autenticidad con DNSSEC.

DNS Firewall: es una herramienta de seguridad que se utiliza para filtrar y bloquear el tráfico DNS malicioso o no autorizado. Inspecciona las solicitudes de consulta DNS y utiliza reglas predefinidas para determinar si la consulta es legítima o sospechosa. Si la consulta es sospechosa o maliciosa, el DNS firewall puede bloquear la solicitud o redirigirla a un servidor de seguridad para un análisis adicional. Esto ayuda a proteger el sistema DNS de amenazas como ataques de denegación de servicio (DoS), envenenamiento de cache DNS y malware que utiliza el DNS para comunicarse con servidores maliciosos.

Así como existen muchos tipos de ataques, también existen muchas herramientas de seguridad que ayudan a combatirlos. Se han mencionado aquellos que son los más importantes y representativos.

2.6 DESARROLLO DEL PROYECTO

2.6.1 INTRODUCCIÓN

El proceso de selección del proveedor del nuevo sistema DNS se basó en criterios como la viabilidad económica, la funcionalidad técnica y la estrategia corporativa, y contó con la participación de directores, gerentes y especialistas técnicos. Es importante destacar que este sistema fue adquirido para varias operaciones de Millicom en Latinoamérica, obteniendo ventajas económicas significativas debido al volumen de compra. Aunque este proceso no forma parte del alcance de este proyecto, ya que fue llevado a cabo por otras instancias, es fundamental tener en cuenta su relevancia, pues constituye la acción inicial y decisiva para el desarrollo del proyecto. Tras la conclusión del proceso de selección, se notificó a las operaciones locales, incluida la operación en Bolivia, que el proveedor Akamai fue escogido.

Tras ser informada la operación local de la decisión, la gerencia técnica instó a que mi persona, como Responsable de Aseguramiento de Servicio de las áreas de CORE e IP, tomara un papel activo en la dirección y avance del proyecto. En ese sentido, asumí el liderazgo del proyecto, asegurando su progresión y ejecución efectiva. Designé miembros del área de **Redes IP** a mi cargo y coordiné con la jefatura de planificación para asignar miembros de **Planificación IP**. A continuación, establecí contacto con el personal representante del proveedor para una reunión inicial, con el objetivo de acordar una modalidad de trabajo, comunicar expectativas y establecer un cronograma preliminar, entre otros aspectos relevantes.

2.6.2 REQUERIMIENTOS FUNCIONALES

Aunque el sistema fue escogido en una instancia en la cual nuestra operación local no tuvo participación, el sistema DNS escogido cumple con los siguientes requerimientos funcionales:

Funcionalidades de Resolución: El nuevo sistema puede desplegar funcionalidades tanto autoritativas como recursivas, gestionando consultas internas y externas.

Redundancia y Capacidad: El nuevo sistema posee la capacidad de implementar redundancia geográfica, y cada servidor recursivo puede soportar todo el tráfico del ISP sin superar el 50% de carga de CPU.

Monitoreo y Mantenimiento: El nuevo sistema soporta el protocolo de monitoreo SNMP en las modalidades de **polling**[37] y **trapping**,[38] permitiendo un monitoreo activo del estado y comportamiento del sistema DNS.

Análisis y Reportes: El nuevo sistema proporciona funcionalidades para visualizar el tráfico generado a nivel de DNS, la carga de CPU, y otros datos relevantes.

Seguridad y Protección: El nuevo sistema ofrece funciones de seguridad, como DNSSEC, para proteger el sistema contra amenazas como ataques de denegación de servicio, phishing, spam y otros similares.

Gestión de Tráfico: A través de filtros de tráfico, se pueden implementar nuevos planes comerciales y cumplir con solicitudes regulatorias, como el bloqueo de sitios web específicos.

2.6.3 ESTRATEGIA DE IMPLEMENTACIÓN

2.6.3.1 ELECCIÓN DE LA INFRAESTRUCTURA

Dentro del proceso de modernización y búsqueda de eficiencia para el proyecto, se eligió una infraestructura basada en la virtualización. Esta decisión no solo respondió a las tendencias actuales en tecnología de la información, sino también a las ventajas concretas que esta modalidad ofrece, y que contribuyeron al alcance de los objetivos del proyecto. A continuación, se detallan las principales características y beneficios de las infraestructuras virtuales que justificaron esta elección:

[37] Polling: modalidad de trabajo mediante el protocolo SNMP en la cual el gestor de red realiza consultas periódicas al sistema gestionado para obtener información específica, como el estado, utilización, rendimiento, entre otros.

[38] Trapping: modalidad de trabajo mediante el protocolo SNMP en la cual el sistema gestionado envía mensajes, conocidos como 'traps', al gestor de red para alertar sobre alguna situación importante o cambio en su estado.

- **Flexibilidad y Escalabilidad**: Los servidores virtuales pueden ser redimensionados de forma rápida y sencilla, permitiendo adaptarse a las necesidades cambiantes del negocio. En contraste, escalar un servidor físico suele requerir una inversión significativa en hardware y tiempo.
- **Eficiencia de Recursos**: La virtualización permite ejecutar múltiples máquinas en un solo servidor físico, maximizando el uso del hardware y minimizando la necesidad de equipos adicionales.
- **Continuidad del Negocio y Recuperación ante Desastres**: Con servidores virtuales, es más sencillo implementar soluciones de alta disponibilidad. Las máquinas virtuales se pueden trasladar entre servidores físicos sin interrupciones en los servicios, y los **snapshots**[39] permiten una rápida recuperación en caso de fallos.
- **Reducción de costos**: Si bien la virtualización requiere una inversión inicial, puede conducir a ahorros significativos a largo plazo debido a la reducción en hardware físico, costos de energía y mantenimiento.
- **Administración centralizada**: Los sistemas de gestión de virtualización centralizan la administración de los servidores virtuales, simplificando las tareas y reduciendo la posibilidad de errores.

2.6.3.2 PREPARACIÓN DE LA INFRAESTRUCTURA VIRTUAL

Servidores Virtuales: En esta fase, mi labor consistió en seleccionar y validar las especificaciones técnicas de los servidores virtuales proporcionados por el área de **IT**[40] de la compañía. Coordiné con el proveedor y con el personal de IT para asegurarme de que los elementos, tales como CPU, memoria, almacenamiento y conectividad de red, estuvieran en línea con los requerimientos técnicos.

Conectividad de Red Interna: Bajo mi supervisión, el personal del área de Redes IP llevó a cabo la configuración de la red interna, garantizando la comunicación entre los

[39] Un snapshot en el contexto de las máquinas virtuales es una copia del estado de la máquina en un punto específico en el tiempo. Esto incluye la configuración y los datos en ejecución, utilizándose para copias de seguridad y recuperación de datos.
[40] IT se refiere al departamento de Tecnología de la Información o más conocido como el área de sistemas en una compañía.

componentes del sistema DNS y el acceso remoto del proveedor a través de una **VPN**[41] dedicada.

Una vez completadas estas dos acciones, el proveedor pudo proceder con las actividades de instalación y configuración del nuevo sistema.

2.6.3.3 INTEGRACIÓN DEL NUEVO SISTEMA EN EL BACKBONE INTERNET

Diseño de Red: En esta etapa, los ingenieros de planificación y de operación y mantenimiento del ISP, incluyéndome, realizamos un análisis técnico para determinar la posición óptima del nuevo sistema dentro del Backbone Internet.

Conectividad de Red Externa: Bajo mi supervisión, el personal del área de Redes IP configuró la red en el Backbone Internet para permitir la accesibilidad del nuevo sistema desde las redes de servicios móviles y fijos del ISP, así como garantizar su conexión a Internet.

Es importante destacar que, al implementar un nuevo sistema como el descrito, realizar un análisis técnico de posicionamiento como el descrito es muy importante, ya que constituye un cimiento, que en lo posterior será muy difícil de modificar.

Con esta acción completada, el nuevo sistema quedó prácticamente implementado e integrado en la red del ISP en paralelo con el anterior sistema, dando pie a las fases siguientes dedicadas a validación y pruebas.

2.6.3.4 VALIDACIÓN Y PRUEBAS

Validaciones del Proveedor: Tras confirmar al proveedor que la conectividad de red estaba completa, tanto interna como externamente, entramos en un proceso colaborativo de identificación y corrección de observaciones técnicas. Bajo mi coordinación y supervisión, llevamos a cabo sesiones técnicas dedicadas para agilizar y documentar la solución de las

[41] VPN (Red Privada Virtual) es una tecnología que establece una conexión segura y cifrada entre dos dispositivos o redes a través de Internet. Esto permite que los datos viajen de manera segura y privada, como si estuvieran en una red local.

observaciones, garantizando que la conectividad de red quedara finalizada de forma eficiente.

Plan de Pruebas: Con la confirmación del proveedor de que el sistema estaba completamente implementado, dirigí y coordiné la fase de pruebas de validación del ISP. Esto implicó la creación y manejo de ambientes de prueba controlados dentro de las redes de servicios móvil y fijo, lo cual permitió realizar las pruebas preproducción de manera segura y sin afectar los servicios en producción.

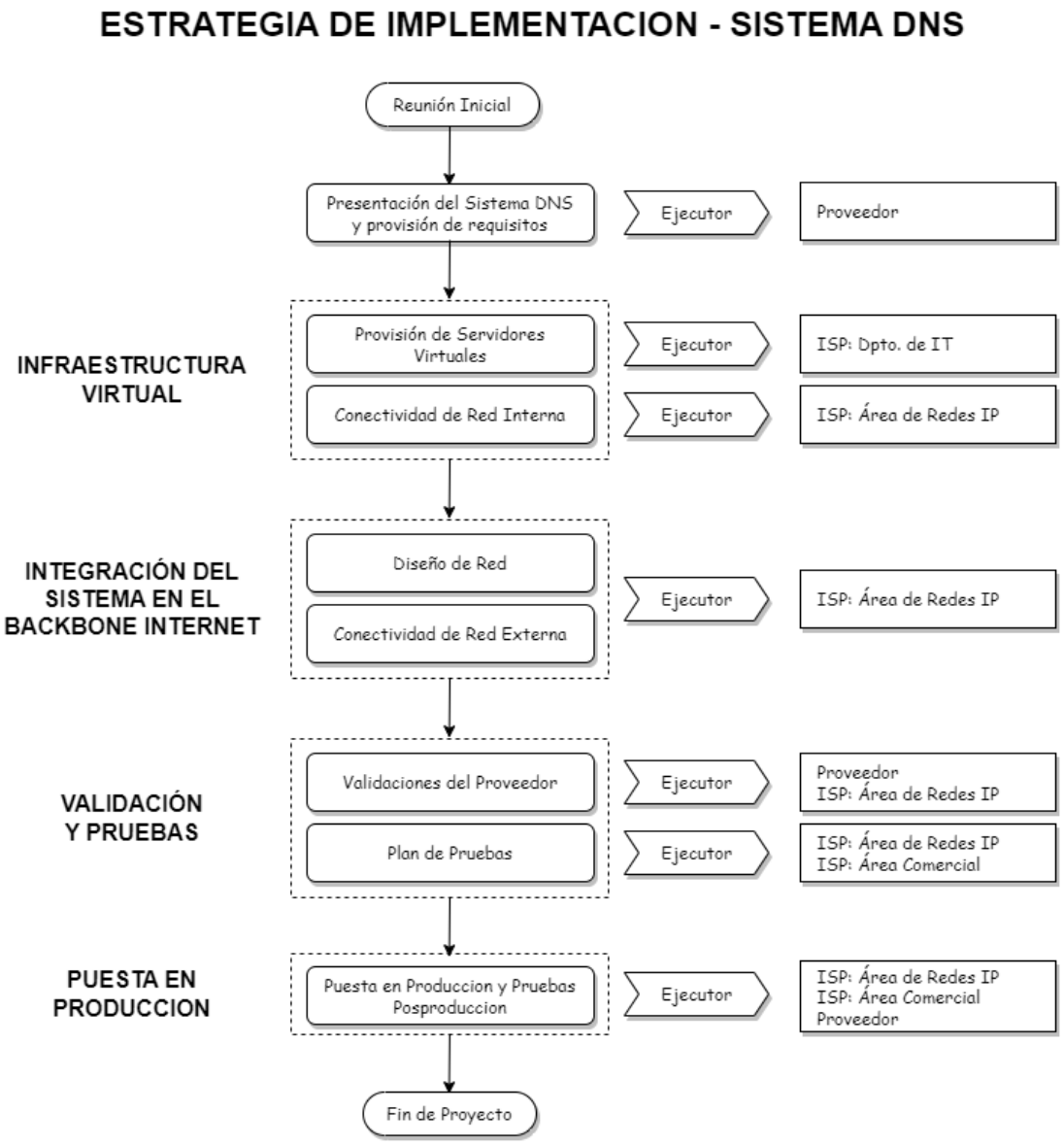
Es importante subrayar la importancia del establecimiento de estos ambientes de prueba controlados, ya que nos permitieron validar el correcto funcionamiento del nuevo sistema y, en base a los resultados obtenidos, tomar la decisión de ponerlo en producción, con plena confianza en su rendimiento y fiabilidad.

2.6.3.5 PUESTA EN PRODUCCIÓN

Una vez realizado y aprobado el plan de pruebas del ISP, establecimos fechas para la puesta en servicio del nuevo sistema, de acuerdo a los procedimientos de cambios del ISP y respetando normas del ente regulador de Bolivia, tal como se explica en la sección 2.6.6, marcando así la conclusión del proyecto.

En el siguiente diagrama podemos ver la estrategia del proyecto esquematizada:

Figura 2.6.1 Estrategia de Implementación



Fuente: Elaboración Propia

2.6.4 ETAPA DE IMPLEMENTACIÓN

2.6.4.1 CRONOGRAMA

Como parte del proyecto se planteó un cronograma con fechas tentativas, cuya versión final se muestra a continuación.

Tabla 2.6.4.1-1 Cronograma del Proyecto

FECHA INICIO	TAREA	DESCRIPCIÓN	RESPONSABLE	ESTADO	PRIORIDAD	FECHA LÍMITE	DEPENDENCIA	AVANCE
21/11/2017	Reunion Inicial	Reunion inicial de coordinacion entre el equipo del proveedor y el equipo del ISP	ISP - Planificacion IP ISP - Redes IP Proveedor	Completo	Alto	21/11/2017	Ninguna	100%
21/11/2017	Entrega de requisitos de Hardware	El proveedor entrega la cantidad de servidores y las caracteristicas de cada uno	Proveedor	Completo	Alto	25/11/2017	Ninguna	100%
21/11/2017	Plan de Direccionamiento	Asignacion de direcciones IP a los compoentes del sistema	ISP - Redes Ip	Completo	Alto	28/11/2017	Entrega de requisitos de Hardware	100%
21/11/2017	Diseno de arquitectura - Low Level Design (LLD)	El proveedor entregar la arquitectura del sistema DNS	Proveedor	Completo	Alto	22/11/2017		100%
25/11/2017	Provisionamiento de los servidores virtuales	El area de Infraestructura del ISP debe configurar los servidores con las caracteristicas solicitadas por el proveedor	ISP - Infraestructura IT	Completo	Alto	15/12/2017	Entrega de requisitos de Hardware	100%
25/11/2017	Cableado interno LPZ	Trabajos de cableado fisico para proveer de conectividad al sistema	ISP - Planificacion IP ISP - Redes IP	Completo	Alto	15/12/2017	Entrega de requisitos de Hardware	100%
25/11/2017	Cableado interno SCZ	Trabajos de cableado fisico para proveer de conectividad al sistema	ISP - Planificacion IP ISP - Redes IP	Completo	Alto	15/12/2017	Plan de Direccionamiento	100%
16/12/2017	Congelamiento de Red	Por politica interna del ISP se suspenden proyectos y tareas operativas				07/01/2018		
08/01/2018	Configuracion Backbone Internet Occidente	Los equipos del Backbone Internet, Routers de Borde, CORE Switches, red de mantenimiento, se deben configurar para permitir el acceso requerido del sistema DNS	ISP - Planificacion IP ISP - Redes IP	Completo	Alto	22/01/2018	Plan de Direccionamiento Provisionamiento de los Servidores Virtuales Cableado interno	100%
08/01/2018	Configuracion Backbone Internet Oriente	Los equipos del Backbone Internet, Routers de Borde, CORE Switches, red de mantenimiento, se deben configurar para permitir el acceso requerido del sistema DNS	ISP - Planificacion IP ISP - Redes IP	Completo	Alto	19/02/2018	Plan de Direccionamiento Provisionamiento de los Servidores Virtuales Cableado interno	100%
19/02/2018	Pruebas Preproduccion La Paz	Pruebas de funcionalidad y rendimiento	ISP - Planificacion IP ISP - Redes IP	Completo	Alto	01/03/2018	Configuracion Backbone Internet Occidente	100%
19/02/2018	Pruebas Preproduccion Santa Cruz	Pruebas de funcionalidad y rendimiento	ISP - Planificacion IP ISP - Redes IP	Completo	Alto	01/03/2018	Configuracion Backbone Internet Oriente	100%
19/02/2018	Solicitud de Permiso de Corte de Servicio a la ATT	Por Precaucion se pide permiso de corte, pero en realidad no se espera afectacion al servicio	ISP - Planificacion IP	Completo	Alto	01/03/2018	Pruebas Preproduccion	100%
06/03/2018	Puesta en produccion Red Movil	Se reconfiguran los APN de la red movil con las direcciones IP de los nuevos DNS recursivos	ISP - Redes IP	Completo	Alto	07/03/2018	Pruebas Preproduccion Permiso de Corte	100%
07/03/2018	Puesta en produccion Red Fija	Se reconfiguran el sistema de aprovisionamiento de la red fija con las direcciones IP de los nuevos DNS recursivos	ISP - Redes IP	Completo	Alto	08/03/2018	Pruebas Preproduccion Permiso de Corte	100%
13/03/2018	Puesta en produccion Funcionalidad Autoritativa	Se reconfiguran el sistema de aprovisionamiento de la red fija con las direcciones IP de los nuevos DNS recursivos	ISP - Redes IP	Completo	Alto	08/03/2018	Pruebas Preproduccion Permiso de Corte	100%

Fuente: Elaboración Propia

2.6.4.2 ESTRATEGIA COMUNICACIONAL

La reunión inicial o **Kick-off Meeting** en inglés, se sostuvo con normalidad entre el personal del proveedor y el personal del equipo de redes IP del ISP. Así como todas las reuniones posteriores y futuras actividades con el proveedor, la reunión se llevó a cabo en remoto, no siendo este un factor de afectación para el desarrollo del proyecto.

Los principales objetivos de la reunión inicial fueron alcanzados y los siguientes pasos establecidos claramente:

- Presentación del personal de ambos equipos. Por parte del proveedor se presentaron los roles de **Global Account Manager**, **Project Manager**, **Technical Point of Contact** y los ingenieros de implementación que iban a estar a cargo del despliegue de la solución. Por parte del ISP se presentaron los roles de **Gerencia de Aseguramiento de Servicio**, **Gerencia de Tecnología y Capacidad**, **Líder de proyecto**, **Responsable de CORE e IP**, **Supervisor de Redes IP** e ingenieros a cargo de la planificación e implementación del proyecto por parte del ISP.
- En base a la estructura presentada de ambos lados se acordó un esquema de escalamiento a aplicarse en casos importantes o urgentes. De otra forma los problemas se discutirían en las reuniones semanales de seguimiento. También se acordó que en base a mutuo acuerdo entre los líderes de proyecto de ambas partes las reuniones podrían suspenderse o postergarse.
- Se intercambiaron contactos telefónicos, WhatsApp y correos. Las comunicaciones formales serian vía correo y en reuniones de seguimiento, más también se permitirían comunicaciones informales por WhatsApp o llamada directa para facilitar la coordinación y comunicación.
- Se pactaron reuniones semanales de seguimiento del proyecto. El **Project Manager** del proveedor pasaría las notas de la reunión a todos los implicados en el proyecto.
- El proveedor explica la composición y funcionamiento del sistema DNS.
- Se establecieron pendientes sobre los siguientes pasos.

Las reuniones posteriores que se sucedieron mantuvieron el mismo formato y fueron de utilidad para dar seguimiento a los pendientes del proyecto, así como analizar y discutir soluciones a problemas que se fueron presentando, los cuales fueron de índole técnico, así como también de coordinación y comunicación.

2.6.4.3 DESCRIPCIÓN DEL SISTEMA DNS

El nuevo sistema DNS se caracteriza como un sistema inteligente centrado principalmente en llevar a cabo la función de recursividad DNS, el sistema reside dentro de la red del ISP y está **cerca del usuario final**[42]. Este sistema proporciona flexibilidad, escalabilidad y rendimiento a los ISP que necesitan proteger su infraestructura DNS contra ataques, anomalías de red, y también mejorar el servicio DNS a través de la implementación de nuevas funcionalidades como el control parental. Basado en un motor de políticas orientado a datos, y gracias a su integración con el **CDN**[43] de Akamai, este sistema optimiza la entrega de contenido durante el proceso de recursividad DNS.

El sistema está compuesto por los servidores cuyas funciones se describen a continuación:

2.6.4.3.1 SERVIDORES RECURSIVOS

De acuerdo con las directrices y recomendaciones proporcionadas por la casa matriz Millicom, los servidores recursivos se dimensionaron de tal manera que un solo servidor pudiera manejar el tráfico total del ISP a un 50% de su carga. La selección de este diseño tenía como objetivo no sólo garantizar una redundancia robusta, sino también ofrecer un amplio margen para el crecimiento futuro del tráfico. Con la instalación de dos nodos DNS, cada uno compuesto por dos servidores recursivos, se esperaba que el sistema en su conjunto operara al 12.5% de su capacidad máxima. Esta configuración ofrecería el beneficio adicional de permitir tomar decisiones de expansión con suficiente anticipación, basándose en la información obtenida de los sistemas de monitoreo y estadísticas del ISP, particularmente analizando los picos de tráfico del último año.

Los servidores recursivos cumplen la función de resolver consultas DNS, como se describió en el marco teórico. Estos servidores responden a las consultas DNS de los usuarios y realizan el proceso de recursividad DNS al consultar a los servidores raíz de Internet.

[42] Cuando se dice que el sistema está "cerca del usuario final", significa que está diseñado para minimizar la latencia y maximizar la velocidad de las consultas DNS.

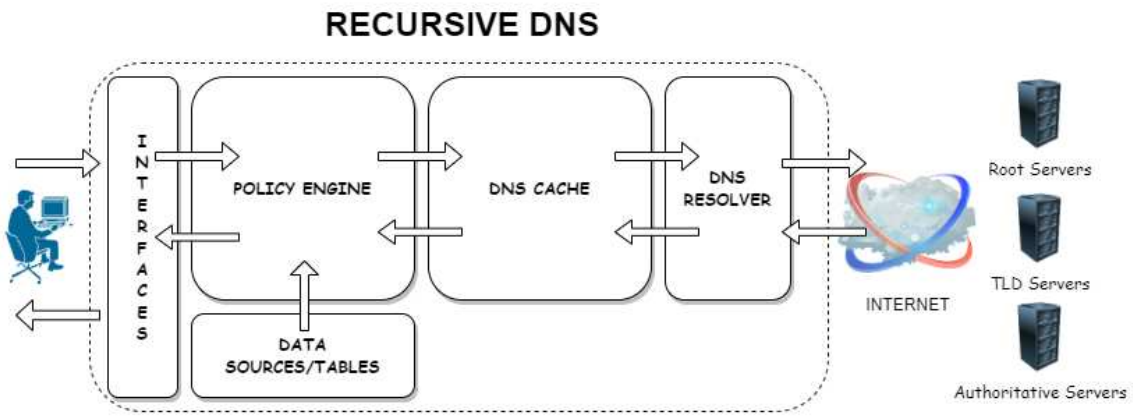
[43] Un CDN (Content Delivery Network) se utiliza para entregar de manera eficiente y rápida contenido web a los usuarios. Cuenta con una infraestructura de servidores distribuidos estratégicamente en diferentes ubicaciones geográficas, con el objetivo de reducir la latencia y mejorar el rendimiento al llevar el contenido más cerca de los usuarios finales.

También mantienen una memoria cache local, lo que permite que el servidor responda directamente si la información requerida está en su cache.

El software que implementa la funcionalidad de recursividad DNS se instala en un servidor y depende del sistema operativo y del hardware subyacente del servidor para su correcta operación.

Desde el punto de vista lógico, el servidor recursivo consta de cuatro componentes principales: el Motor de Políticas (Policy Engine), las Fuentes de Datos y Tablas (Data Sources/Tables), la Cache DNS y el Resolver DNS, tal y como se muestra en el siguiente diagrama:

Figura 2.6.2 Servidor Recursivo del Nuevo Sistema DNS



Fuente: Manual del Proveedor Akamai

El Motor de Políticas y las Tablas de Datos funcionan como el primer punto de control en el servidor recursivo. Si una consulta DNS está destinada a un sitio que se encuentra en una lista negra o sujeta a una política de bloqueo específica, la consulta se detiene en este punto y no pasa a los módulos de Cache o de Resolución.

Desde el punto de vista del mantenimiento, el software DNS incorpora un agente de control que garantiza que los programas necesarios estén funcionando correctamente y permanezcan en ejecución. Este agente también permite que la funcionalidad de resolución recursiva esté disponible automáticamente al encender el servidor.

Además, el software proporciona diferentes tipos de registros que almacenan mensajes de error. Estos mensajes pueden ser útiles para diagnosticar problemas, ya sean problemas de resolución, de conectividad o del propio software o del hardware del servidor. Entre estos mensajes, por ejemplo, los de categoría CRÍTICA indican problemas que requieren atención inmediata, ya que a menudo son signos de que el software está en un estado inoperable o se aproxima a uno.

Por último, el software incluye una interfaz de administración que responde a consultas DNS específicas, proporcionando mensajes que indican la configuración del servidor. Dependiendo de la respuesta, se puede inferir el estado operativo del servidor, lo que ayuda a identificar y resolver problemas rápidamente.

El monitoreo del rendimiento del cache es esencial para el funcionamiento global del sistema DNS. Dada su importancia, se registra regularmente información sobre el rendimiento de la cache que debe ser monitorizada. Los indicadores en los archivos de registro muestran si el tamaño de la cache es adecuado y también indican la tasa de aciertos de la cache, que es crítica para un buen rendimiento. En un servidor saludable, esta tasa de aciertos debería ser del 60-70% o más.

2.6.4.3.2 SERVIDORES DE REPUTACIÓN

Los Servidores de Reputación, conocidos como Reputation Knowledge Server (RKS), juegan un papel esencial en la implementación de listas y la actualización de reglas en el Motor de Políticas de los Servidores Recursivos DNS. Estas listas, de gran importancia, contienen información dinámicamente actualizada acerca de sitios web de reputación dudosa, los cuales pueden incluir phishing, ransomware, malware, entre otros. Dichas listas son proporcionadas por múltiples fuentes confiables en Internet, como Akamai, Symantec y Sophos.

En resumen, los RKS son responsables de establecer y aplicar políticas de seguridad que serán ejecutadas en los Servidores Recursivos DNS, mejorando de manera significativa la protección del usuario final al bloquear el acceso a estos sitios potencialmente peligrosos.

Además, los servidores RKS tienen la capacidad de implementar políticas a nivel de usuario. Esto permite a los proveedores de servicios de Internet personalizar el acceso para usuarios específicos de acuerdo a directivas comerciales o regulatorias. Por ejemplo, en países donde las regulaciones impiden interrumpir completamente el servicio de Internet, se pueden configurar políticas en los RKS para bloquear servicios específicos como Streaming, juegos o sitios con contenido para adultos, que suelen generar grandes volúmenes de tráfico, permitiendo solamente servicios básicos de navegación y mensajería, entre otros.

En conclusión, los servidores RKS funcionan como un escudo de seguridad, proporcionando un conjunto de políticas de seguridad asociadas a nombres de dominio y direcciones IP. Estas políticas se aplican en los Servidores Recursivos DNS para filtrar o bloquear tráfico, protegiendo así al usuario final contra sitios de dudosa reputación y otros riesgos potenciales en Internet.

2.6.4.3.3 SERVIDOR DE REPORTES Y ESTADÍSTICAS

El servidor AnalytX realiza una captura de datos de tráfico DNS en tiempo real, proveyendo un método de agregación de todo el tráfico DNS en un solo servidor para su posterior procesamiento y análisis.

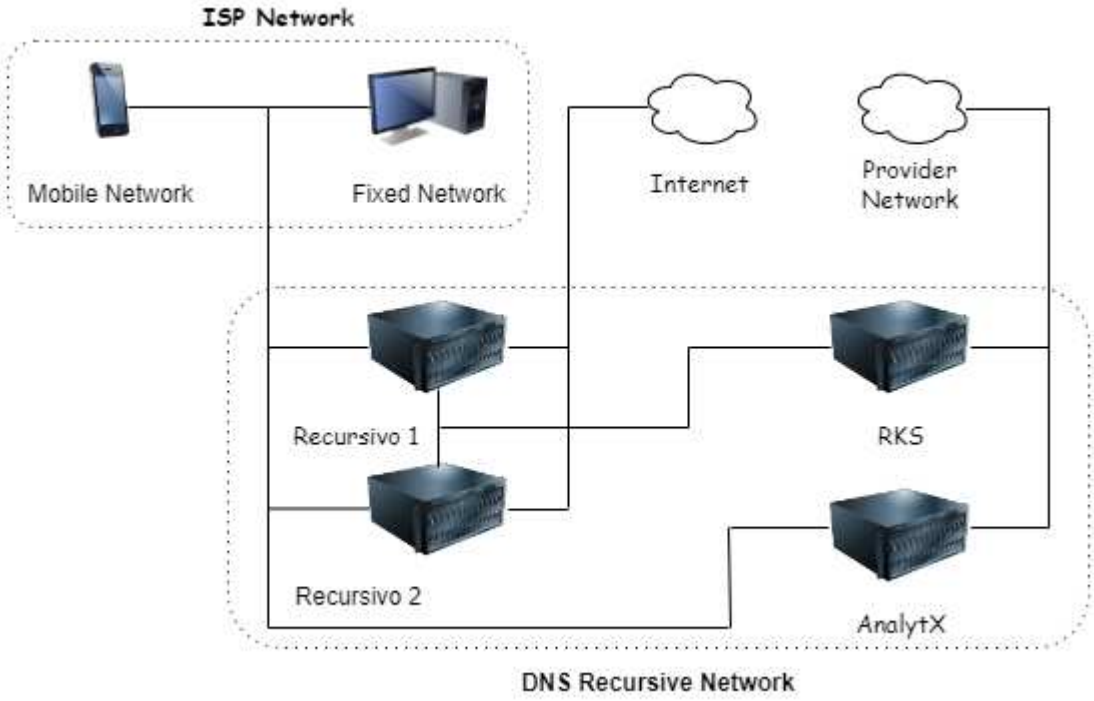
Una vez que todo el tráfico DNS es recolectado y procesado en el motor del servidor AnalytX, el conjunto completo de directivas y fuentes de datos se pueden aprovechar para poder inspeccionar y rastrear el tráfico DNS.

De cara al operador, el servidor AnalytX también provee herramientas de visualización y análisis mediante una interfaz gráfica web, mediante la cual se puede examinar y analizar el tráfico DNS de todo el sistema para determinar tendencias o revisar el impacto de eventos de red.

2.6.4.3.4 DESPLIEGUE DNS – FUNCIONALIDAD RECURSIVA

El siguiente diagrama proporciona una vista de cómo se conectan los elementos del sistema DNS para la funcionalidad recursiva, interna y externamente:

Figura 2.6.3 Funcionalidad Recursiva



Fuente: Manual del Proveedor Akamai

Podemos ver que los servidores recursivos están conectados, tanto a la red del ISP, así como a Internet, para poder recibir, realizar y responder las consultas DNS. También se observa que internamente tienen conexiones con los servidores RKS para recibir las listas de dominios y las políticas a aplicar, y con el servidor AnalytX que es el componente encargado de dar visibilidad de lo que ocurre en el sistema a través de reportes y estadísticas.

2.6.4.3.5 SERVIDORES AUTORITATIVOS

El sistema incorpora servidores autoritativos con la finalidad de almacenar todos los registros de los dominios que son propiedad del ISP, así como también los dominios de los clientes del ISP que han contratado el servicio de alojamiento de dominios.

La función autoritativa del sistema es ejecutada mediante dos servidores: un servidor proxy denominado AuthX y el propio servidor autoritativo, que se encuentra protegido por el AuthX. A través del servidor AuthX, el sistema tiene la capacidad de responder tanto consultas DNS normales como consultas DNS reversas.

El software del DNS autoritativo no se basa en BIND, en su lugar, el proveedor utiliza una implementación propia fundamentada en su experiencia y conocimientos. Esta decisión se toma como una medida de protección contra vulnerabilidades que presentan los sistemas DNS basados en BIND.

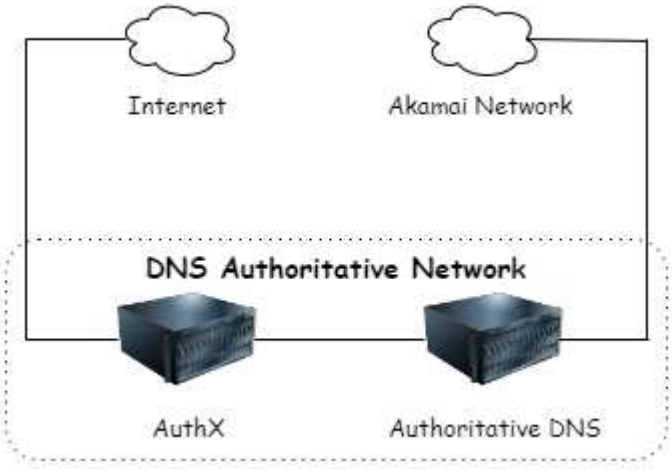
El sistema tiene la capacidad de manejar varias zonas. La información correspondiente a cada zona es almacenada en un archivo distinto, que contiene todos los registros de nombres correspondientes a esa zona. Estos registros albergan la información de correspondencia entre las direcciones IP y los nombres de dominio, lo que permite al sistema responder eficazmente a las consultas DNS.

Los tipos de registros que los servidores autoritativos DNS pueden manejar se encuentran en el Anexo A.

2.6.4.3.6 DESPLIEGUE DNS – FUNCIONALIDAD AUTORITATIVA

El siguiente diagrama proporciona una vista de cómo se conectan los elementos del sistema DNS para la funcionalidad autoritativa, interna y externamente:

Figura 2.6.4 Funcionalidad Autoritativa



Fuente: Manual del Proveedor Akamai

Podemos ver que los servidores autoritativos están conectados solamente a Internet, para poder recibir y responder las consultas DNS externas acerca de los dominios administrados por este sistema DNS. También se observa que para poder llegar al servidor autoritativo se debe pasar primero por el servidor AuthX.

2.6.4.3.7 ESPECIFICACIONES DE LOS SERVIDORES

Como parte del desarrollo del proyecto, el proveedor paso la cantidad necesaria de servidores, así como los requisitos para cada uno de ellos.

Aunque el proveedor no proporcionó una justificación detallada para estas especificaciones, se confió en su experiencia y en su historial de operaciones exitosas en contextos similares para asumir que estas recomendaciones eran las adecuadas.

Cabe mencionar además que para poder contar con redundancia geográfica se instalaron dos sistemas DNS físicamente separados.

Tabla 2.6.4.3-1 Especificaciones de Servidores DNS 1

SERVIDORES RECURSIVOS	
PROCESADOR (CPU)	
Cantidad	4
Núcleos	20
Velocidad	2.5 - 3.5 GHz
MEMORIA (RAM)	
Tamaño	16 Gb
Tipo	DDR4
Velocidad	2400 MHz
ALMACENAMIENTO	
Tamaño	1 Tb
Tecnología	HDD
SISTEMA OPERATIVO	
Sistema Operativo	Linux
Distribución	CentOS 7 o RedHat 7
INTERFACES DE RED	
Cantidad	3
Velocidad	10 Gb

SERVIDORES RKS	
PROCESADOR (CPU)	
Cantidad	2
Núcleos	8
Velocidad	2.5 - 3.5 GHz
MEMORIA (RAM)	
Tamaño	16 Gb
Tipo	DDR4
Velocidad	2400 MHz
ALMACENAMIENTO	
Tamaño	1 Tb
Tecnología	HDD
SISTEMA OPERATIVO	
Sistema Operativo	Linux
Distribución	CentOS 7 o RedHat 7
INTERFACES DE RED	
Cantidad	3
Velocidad	10 Gb

Fuente: Elaboración Propia

Tabla 2.6.4.3-2 Especificaciones de Servidores DNS 2

SERVIDORES ANALYTX	
PROCESADOR (CPU)	
Cantidad	2
Núcleos	8
Velocidad	2.5 - 3.5 GHz
MEMORIA (RAM)	
Tamaño	64 Gb
Tipo	DDR4
Velocidad	2400 MHz
ALMACENAMIENTO	
Tamaño	4 Tb
Tecnología	HDD
SISTEMA OPERATIVO	
Sistema Operativo	Linux
Distribución	CentOS 7 o RedHat 7
INTERFACES DE RED	
Cantidad	3
Velocidad	10 Gb

SERVIDORES AUTHX	
PROCESADOR (CPU)	
Cantidad	2
Núcleos	4
Velocidad	2.5 - 3.5 GHz
MEMORIA (RAM)	
Tamaño	16 Gb
Tipo	DDR4
Velocidad	2400 MHz
ALMACENAMIENTO	
Tamaño	1 Tb
Tecnología	HDD
SISTEMA OPERATIVO	
Sistema Operativo	Linux
Distribución	CentOS 7 o RedHat 7
INTERFACES DE RED	
Cantidad	3
Velocidad	10 Gb

Fuente: Elaboración Propia

Tabla 2.6.4.3-3 Especificaciones de Servidores DNS 3

SERVIDORES AUTORITATIVOS	
PROCESADOR (CPU)	
Cantidad	2
Núcleos	4
Velocidad	2.5 - 3.5 GHz
MEMORIA (RAM)	
Tamaño	16 Gb
Tipo	DDR4
Velocidad	2400 MHz
ALMACENAMIENTO	
Tamaño	1 Tb
Tecnología	HDD
SISTEMA OPERATIVO	
Sistema Operativo	Linux
Distribución	CentOS 7 o RedHat 7
INTERFACES DE RED	
Cantidad	3
Velocidad	10 Gb

Fuente: Elaboración Propia

Todos los procesadores requirieron una configuración multicore y se solicitaron 3 interfaces de red para separar el tráfico entrante, saliente y de gestión.

El requerimiento completo fue solicitado al área de Infraestructura dependiente del departamento de IT, que era el área encargada de la administración de la infraestructura virtual.

2.6.4.4 DESCRIPCIÓN DEL BACKBONE INTERNET DEL ISP

2.6.4.4.1 DEFINICIÓN

Una red **Backbone**[44], también conocida como red troncal, en el contexto de redes IP, se define como un conjunto de enrutadores y conmutadores interconectados que constituyen la columna vertebral de toda la red. Este tipo de red puede tener múltiples usos, como conectar diversas sedes de una organización, edificios gubernamentales, universidades, y más. En términos más amplios, una red Backbone puede conectar diferentes regiones de un país, e incluso diferentes continentes.

En el contexto de un proveedor de servicios de Internet (ISP), una red Backbone de salida a Internet, o simplemente un Backbone Internet, es el conjunto de dispositivos de red, equipos de transporte, sistemas y plataformas relacionadas que, en su conjunto, facilitan una vía para que los usuarios del ISP puedan acceder y consumir servicios de Internet a través de diversas redes de acceso. El acceso a Internet se describió con mayor amplitud en la sección 2.5.2 del marco teórico.

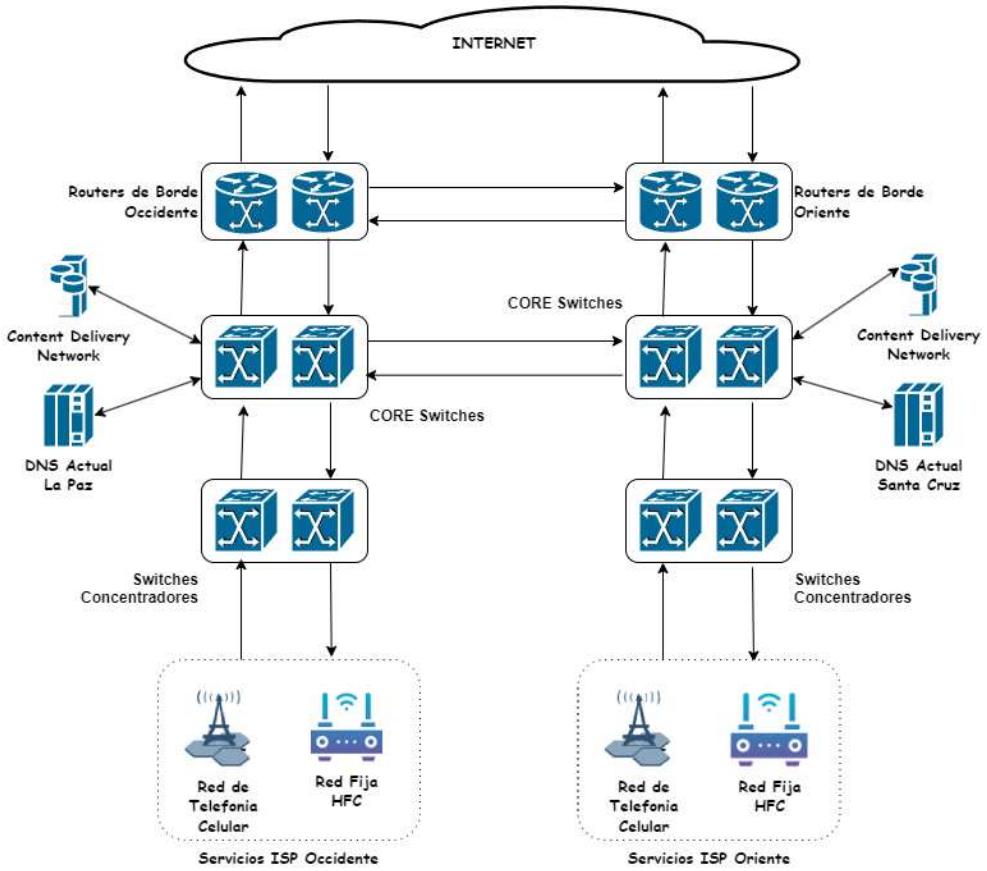
En los acápites subsiguientes, se describirá el Backbone de Internet del ISP. Sin embargo, es importante mencionar que, debido al enfoque específico de esta memoria, ciertos elementos esenciales de la red han sido omitidos en la discusión detallada. Entre ellos se puede citar dispositivos como los CGNAT (Carrier-Grade Network Address Translation), que facilita el reúso eficiente de las direcciones IP, una necesidad crítica dada la limitada disponibilidad de direcciones IPv4 y los equipos que constituyen la red de transmisión del ISP que hacen posible las comunicaciones urbanas y nacionales entre equipos geográficamente distantes. Estos elementos no son el foco principal de este trabajo, pero su presencia es esencial para la operación óptima y eficiente de la red de un ISP.

[44] En ingles la palabra Backbone quiere decir columna vertebral

2.6.4.4.2 BACKBONE INTERNET DEL ISP

En el siguiente diagrama se presenta el Backbone Internet antes de la adición del nuevo sistema DNS.

Figura 2.6.5 Backbone Internet Antes del Cambio



Fuente: Elaboración Propia

El diagrama presentado es un diagrama lógico que muestra los elementos principales del Backbone Internet del ISP.

El ISP maneja dos redes de servicio principales para atender a su base de clientes. La primera es una red de telefonía celular que abarca la totalidad del territorio nacional. Esta red implementa tecnologías 2G, 3G, LTE para proporcionar una amplia gama de servicios de comunicaciones a los usuarios móviles. Los servicios ofrecidos incluyen voz, SMS y

acceso a Internet móvil, satisfaciendo así tanto las necesidades de comunicación básicas como las avanzadas de sus clientes.

La segunda red es una red **HFC**[45], que utiliza la tecnología de cable módems. Esta red proporciona servicios de banda ancha a los hogares, ofreciendo altas velocidades de Internet y la capacidad de manejar múltiples servicios simultáneamente. Además de ofrecer Internet de alta velocidad, la red HFC también soporta servicios de televisión digital, lo que permite al ISP ofrecer paquetes de servicios combinados a sus clientes residenciales. Este tipo de red combina la capacidad de banda ancha de la fibra óptica con la capacidad de distribución de la red de cable coaxial, permitiendo al ISP ofrecer servicios de alta calidad y alto rendimiento.

El tráfico de datos generado por los servicios en las redes de telefonía celular y red fija de banda ancha HFC es inicialmente concentrado y manejado por los Switches Concentradores. Estos switches de alta capacidad funcionan como puntos de conexión central para el tráfico interno de la red del ISP, distribuyendo la información a donde necesita ir dentro de la red interna del ISP.

Este tráfico es entonces derivado a los Switches de Agregación, también conocidos en este contexto como CORE Switches. Estos equipos actúan como un puente entre la red interna del ISP y los Routers de Borde.

Los CORE Switches también proveen acceso y conectividad a dos elementos de red muy importantes. El primero es un conjunto de varias redes de Content Delivery Network (CDN), como ser Google Global Cache (GGC), Facebook Network Acceleration (FNA), y Netflix entre los más prominentes. Estos CDN ayudan a optimizar la entrega de tráfico en la red del ISP, proporcionando respuestas más rápidas a las solicitudes de contenido, y generando un ahorro significativo de ancho de banda internacional para el ISP.

El segundo elemento, crítico en este nivel, es el Sistema de Nombres de Dominio (DNS). En este contexto, estamos refiriéndonos al DNS existente, el cual desempeña todas las

[45] La tecnología HFC, o Hybrid Fiber-Coaxial, es un tipo de red de banda ancha que combina los elementos de las redes de fibra óptica y cable coaxial, que permite a los ISP ofrecer altas velocidades de datos a sus clientes.

funciones de resolución de nombres de dominio que ya se han explicado ampliamente en esta memoria.

Finalmente, el tráfico destinado a Internet, después de pasar por la etapa de los CDN, es encaminado a los Routers de Borde. Estos dispositivos representan el último punto en la red interna del ISP antes de la conexión con Internet. Estos Routers de Borde son responsables de gestionar todo el tráfico que entra y sale de la red del ISP. Utilizan el protocolo **Border Gateway Protocol (BGP)**[46] para establecer y mantener conexiones de red con diversos proveedores internacionales de Internet, proporcionando así múltiples rutas de salida a Internet para el ISP. Gracias al protocolo BGP, los Routers de Borde pueden asegurarse de que los datos enviados a Internet sigan la ruta más eficiente y lleguen correctamente a su destino. Del mismo modo, los datos que llegan de Internet son encaminados de manera eficaz hacia los usuarios internos del ISP.

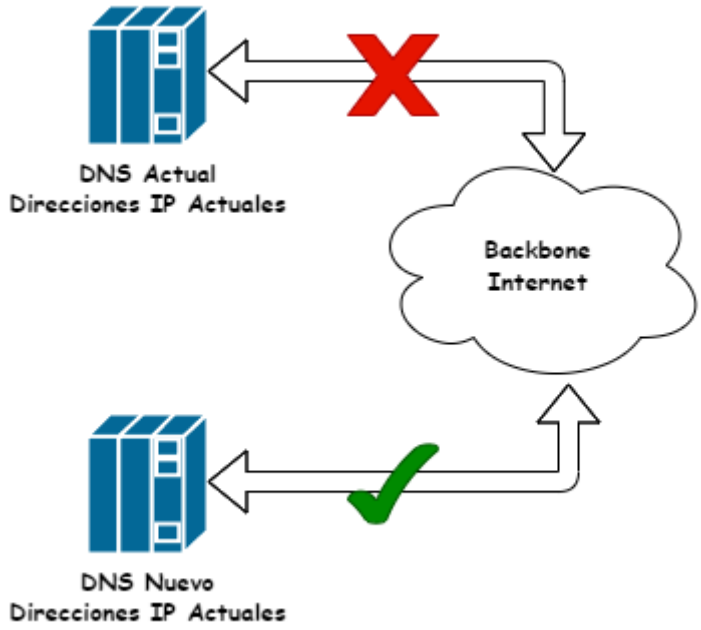
[46] BGP es un protocolo de enrutamiento externo utilizado para intercambiar información de enrutamiento entre routers en Internet. BGP permite que los routers descubran las rutas más eficientes para enviar paquetes de datos a través de las complejas y extensas interconexiones de la red global.

2.6.4.5 DESPLIEGUE DEL NUEVO SISTEMA DNS EN EL BACKBONE INTERNET

Como parte de la estrategia técnica mediante la cual efectuar el reemplazo del nuevo sistema DNS por el actual o existente se consideraron dos alternativas:

A. Provisión del nuevo sistema con direcciones IP temporales, realizar pruebas de funcionamiento en este entorno, y una vez confirmada la adecuada operatividad, reconfigurar las direcciones IP del sistema actual en el nuevo, dejando fuera de servicio al sistema DNS existente.

Figura 2.6.6 Reemplazo del Sistema DNS: Estrategia A

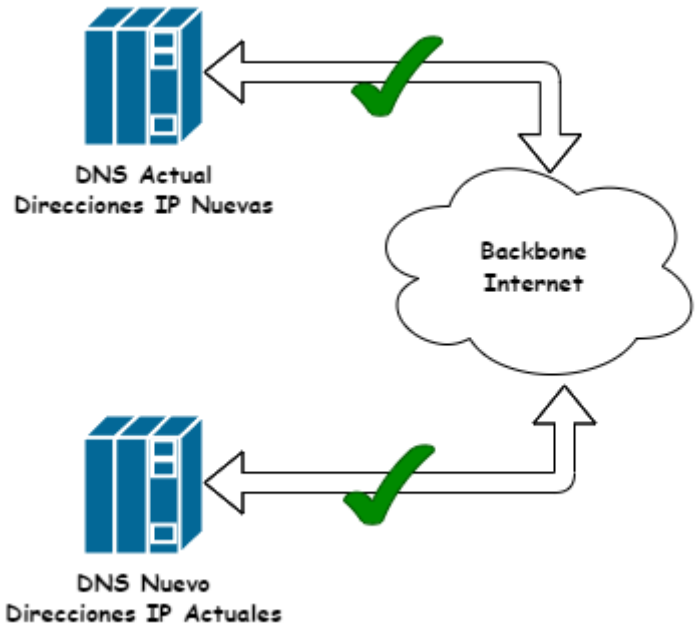


Fuente: Elaboración Propia

B. Provisión del nuevo sistema con direcciones IP definitivas y realización de pruebas de funcionamiento. Tras confirmar un rendimiento correcto, se procederá a reconfigurar los sistemas de la red de telefonía celular y de la red fija HFC con las direcciones IP de los servidores recursivos del nuevo sistema DNS. También se

coordinará con la entidad **NIC Bolivia**[47] para que modifique las direcciones IP autoritativas de los dominios del ISP. En este escenario, ambos sistemas DNS, el antiguo y el nuevo, podrían coexistir durante un período de tiempo determinado. Este enfoque permitiría una transición suave al nuevo sistema DNS, minimizando el riesgo de interrupciones del servicio.

Figura 2.6.7 Reemplazo del Sistema DNS: Estrategia B



Fuente: Elaboración Propia

La estrategia A presenta como ventaja principal que los sistemas externos que dependen del sistema DNS no se verían afectados, logrando un cambio transparente. Sin embargo, posee las siguientes desventajas:

- Se debe modificar las direcciones IP de los servidores recursivos en el nuevo sistema DNS y configurar todas las demás direcciones del sistema con estas nuevas, y también modificar las direcciones IP de los servidores autoritativos en el nuevo

[47] NIC Bolivia (Network Information Center) es una organización que administra los recursos de nombres de dominio y direcciones IP de Internet de Bolivia. Entre sus responsabilidades se incluye el registro y la gestión de dominios de nivel superior de código de país (ccTLD).

sistema DNS. Estas tareas son delicadas y podrían llevar aproximadamente una hora y media según las estimaciones del proveedor.

- Dada la delicadeza de la actividad, habría una dependencia del proveedor para manipular el sistema DNS en este nivel. Es crucial entender que, aunque el personal del ISP podría ser capacitado para operar el sistema, dicha formación no abarca operaciones delicadas como la mencionada.

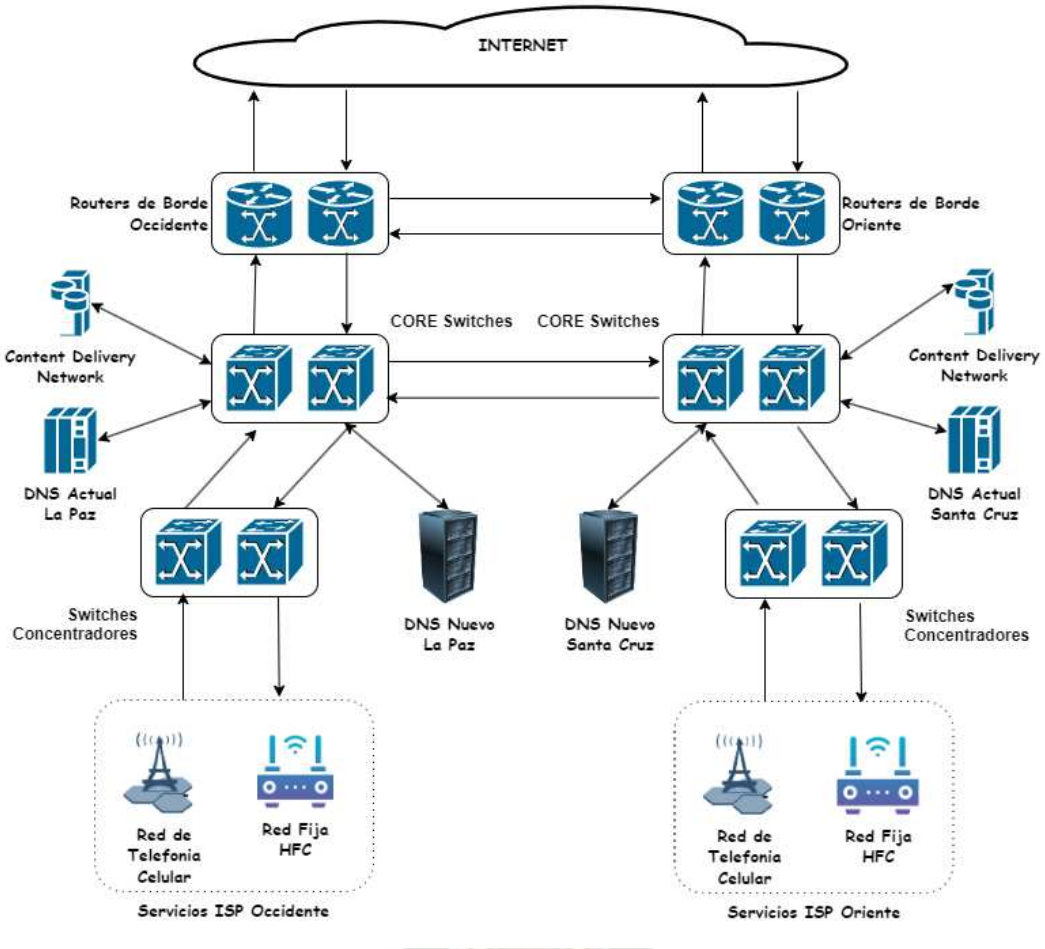
La estrategia B, si bien implica que los sistemas externos tendrían que reconfigurarse con las nuevas direcciones DNS de los servidores recursivos, presenta varias ventajas significativas:

- No sería necesario realizar ningún cambio en el nuevo sistema DNS, lo cual minimizaría la participación del proveedor a solo actividades de supervisión y permitiría eventualmente al personal del ISP manejar este tipo de cambios de forma autónoma.
- Proporciona mayor flexibilidad para realizar pruebas de producción controladas, al tener la capacidad de migrar los sistemas externos uno a la vez.
- De acuerdo con el proveedor de la red móvil, el proceso de modificación de la dirección IP del DNS no tomaría más de 15 minutos.
- Adicionalmente, en la red móvil, fue posible crear un ambiente para que solo un grupo reducido de usuarios de la red móvil consuman el nuevo sistema. De esta forma se pudo realizar pruebas controladas antes de poner el sistema completamente en producción.
- Dentro del nuevo sistema, la función recursiva y la función autoritativa podrían migrarse en momentos distintos, lo que permitiría separar los cambios y, por ende, tener un mejor control de los mismos.

Después de sopesar las ventajas y desventajas de ambas alternativas, se decidió implementar el nuevo sistema DNS usando la estrategia B, ya que proporcionaba mayor robustez en el proceso de pruebas, así como flexibilidad en el proceso de migración de los sistemas dependientes del DNS.

En función a esta decisión el diagrama del Backbone Internet incluyendo el nuevo sistema DNS quedo de la siguiente forma:

Figura 2.6.8 Backbone Internet del ISP incluyendo el nuevo Sistema DNS



Fuente: Elaboración Propia

Como se puede apreciar en el diagrama, el nuevo sistema DNS se interconectó hacia los mismos CORE Switches a los que estaba conectado el sistema DNS actual. Esta decisión estratégica simplificó significativamente la implementación del nuevo sistema. Dado que los CORE Switches ya estaban configurados para gestionar el tráfico DNS, no fue necesario hacer cambios sustanciales en la configuración de la red para incorporar el nuevo sistema DNS. Esta medida permitió no solo una transición más suave, sino que también

redujo el riesgo de interrupciones de servicio durante el proceso de implementación del nuevo sistema.

2.6.4.6 REDUNDANCIA

Para la implementación de la redundancia geográfica en el sistema, se optó por el uso del protocolo Anycast. Este protocolo permite que múltiples servidores compartan una única dirección IP, lo que facilita que el tráfico sea dirigido al nodo más cercano en términos de métricas de enrutamiento. Es decir que los cuatro servidores recursivos instalados respondían a una única dirección IP de Anycast.

2.6.4.7 PLAN DE DIRECCIONAMIENTO DEL SISTEMA DNS

El plan de direccionamiento IP es una parte muy importante en la implementación de cualquier sistema nuevo en la red. Este plan es básicamente un esquema que muestra cómo se asignarán y administrarán las direcciones IP dentro del nuevo sistema, ya que cada componente del sistema necesitará comunicarse en la red mediante una dirección IP única.

Los planes de direccionamiento se diseñan como parte de un proceso de administración de las direcciones IP que están a cargo de los administradores de red y deben garantizar que los recursos IP se utilicen de manera eficiente para que la red pueda crecer sin problemas, que no se comprometa su seguridad y acerca del nuevo sistema, que también este pueda acceder a la conectividad requerida y tener un espacio de crecimiento adecuado, teniendo en cuenta factores como la ubicación de los servidores, sus necesidades de comunicación interna y externa con los usuarios, y con otros sistemas y componentes de red.

Para preservar la confidencialidad, no se mostrarán en esta memoria datos de direccionamiento reales, pero se comparte la tabla utilizada en el presente proyecto para el sistema DNS.

Tabla 2.6.4.7-1 Plan de Direccionamiento IP del nuevo Sistema DNS

PLAN DE DIRECCIONAMIENTO																
	Ciudad	Servidor	Data Center	Funcion	Upstream IP [Public]	Subred	VLAN	Gateway	Puertos	Protocolos	Downstream IP [Private]	Subred	VLAN	Gateway	Puertos	Protocolos
1	Santa Cruz	Recursivo_SC	Paragua	Resolucion Recursividad												
2	Santa Cruz	Recursivo_SC	Paragua	Resolucion Recursividad												
3	Santa Cruz	RKS_SC	Paragua	Reputacion Seguridad												
4	Santa Cruz	AnalytX_SC	Paragua	Reportes Estadisticas												
5	Santa Cruz	Authoritative-SC	Paragua	Funcion Autoritativa												
6	Santa Cruz	AuthX-SC	Paragua	Funcion Autoritativa												
7	La Paz	Recursivo_LP	Alpacoma	Resolucion Recursividad												
8	La Paz	Recursivo_LP	Alpacoma	Resolucion Recursividad												
9	La Paz	RKS_LP	Alpacoma	Reputacion Seguridad												
10	La Paz	AnalytX_LP	Alpacoma	Reportes Estadisticas												
11	La Paz	Authoritative-LP	Alpacoma	Funcion Autoritativa												
12	La Paz	AuthX-LP	Alpacoma	Funcion Autoritativa												

Fuente: Elaboración Propia

2.6.5 PLAN DE PRUEBAS PREPRODUCCIÓN

Una vez concluidos los trabajos necesarios para la operatividad del nuevo sistema y su integración en el Backbone Internet del ISP, se pasó a la etapa de pruebas. El objetivo de estas pruebas era validar tanto el correcto funcionamiento del sistema como su integración apropiada dentro de la red del ISP.

De acuerdo a la estrategia de implementación explicada en la sección 2.6.3, se debe considerar que hasta este punto ya se habían completado las siguientes actividades:

- El equipo de redes IP del ISP elaboró el plan de direccionamiento para el nuevo sistema DNS, que se explicó en el acápite 2.6.4.7.
- El departamento de IT del ISP provisionó los servidores virtuales de acuerdo a las especificaciones requeridas por el proveedor, que se detalló en el acápite 2.6.4.3.7.
- El proveedor implementó y configuró los servidores del nuevo sistema DNS y realizó la integración del sistema usando la infraestructura virtual y los recursos de red provistos por el ISP, de acuerdo a la descripción que se realizó en la sección 2.6.4.3.
- El equipo de redes del ISP ejecutó las actividades necesarias para poder integrar el nuevo sistema DNS en el Backbone Internet del ISP, fue necesario realizar

actividades de cableado físico y posteriormente configurar los equipos de red del Backbone Internet del ISP para dotar al nuevo sistema de conectividad hacia Internet, hacia las redes de servicios del ISP y hacia los sistemas de gestión del ISP, que se explicó con mayor detalle en el acápite 2.6.4.5.

De acuerdo al rol de líder de proyecto que me fue asignado, me encargué de coordinar y realizar seguimiento a cada una de estas actividades, así como realizar reportes de avance para los directores del área técnica.

Habiendo completado todas estas actividades, estábamos listos para comenzar con la fase de pruebas.

2.6.5.1 PRUEBAS EN AMBIENTE CONTROLADO EN LA RED MÓVIL

Una vez que el sistema DNS fue correctamente provisionado y configurado, confirmado por el proveedor, pasamos a la fase de pruebas previas a la puesta en producción del sistema. Estas pruebas se dividieron en dos categorías principales: pruebas de rendimiento y pruebas de funcionamiento.

Para las pruebas de rendimiento, se utilizó una herramienta de uso libre llamada **DNS Benchmark**[48]. Esta herramienta permitió obtener estadísticas detalladas del rendimiento del nuevo sistema, así como del sistema DNS en uso, lo que facilitó una comparación directa de ambos sistemas.

En cuanto a las pruebas de funcionamiento para la red móvil, se aprovechó la capacidad que ofrece una red móvil para definir diferentes Access Point Names (APN). Un APN en una red móvil actúa como una puerta de enlace entre la red móvil y otra red, generalmente Internet. A través de un APN se pueden definir los tipos de servicio que puede utilizar un usuario, el protocolo de red que se usará e incluso contener información sobre la autenticación, como un nombre de usuario y una contraseña.

[48] DNS Benchmark es una herramienta completa, precisa y gratuita para Windows y Linux diseñada para determinar el rendimiento de los servidores de nombres DNS locales y remotos.

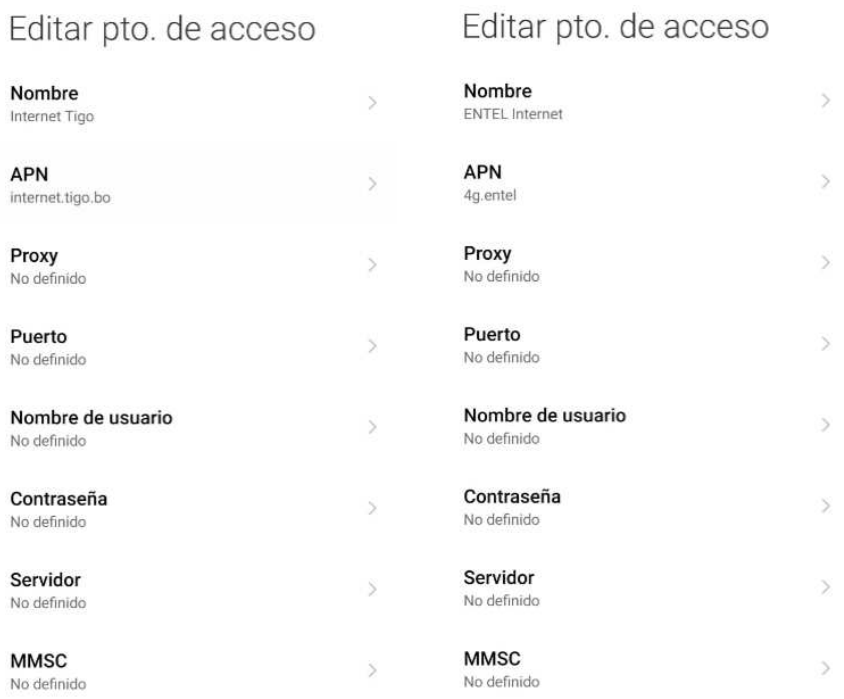
Los operadores de telefonía móvil pueden tener varios APNs, que los clientes pueden utilizar para diferentes servicios, como la navegación por Internet, MMS, servicios corporativos, entre otros. Estos APNs, se configuran y seleccionan en los terminales móviles de los usuarios.

En el contexto de este proyecto, se creó un APN de prueba, idéntico al APN para el acceso a Internet, pero con una dirección DNS diferente. Este APN de prueba fue configurado en un grupo aproximado de 20 dispositivos móviles pertenecientes a personal del ISP en las principales ciudades. Esta estrategia permitió realizar pruebas de funcionamiento en las principales ciudades donde el ISP tiene desplegado su servicio móvil, definiendo así un entorno de pruebas seguro dentro de la red móvil del operador, sin interferir en ningún momento con la red principal del ISP.

De esta forma, se pudo asegurar que la funcionalidad recursiva en el nuevo sistema DNS funcionaba correctamente y estaba listo para su implementación en la red principal, minimizando posibles problemas durante su puesta en marcha.

A modo de ejemplo, la figura muestra APNs de acceso a Internet de dos de los operadores móviles en Bolivia.

Figura 2.6.9 Configuración de APN en un Teléfono Inteligente



Fuente: Elaboración Propia

2.6.5.2 PRUEBAS EN AMBIENTE CONTROLADO EN LA RED FIJA

El ISP tenía desplegada una red de acceso a Internet domiciliario o red fija, basada en la tecnología de **Cable Modem**, que aprovecha la infraestructura existente de cable coaxial para proporcionar servicios de Internet de alta velocidad. Esta red se estructura en tres niveles: central, de distribución y de usuario.

En el nivel central se encuentran los sistemas de **Cable Modem Termination System (CMTS)**[49], ubicados en los centros de datos del ISP. El CMTS gestiona el tráfico de datos entre la red de banda ancha del proveedor de servicios y los módems de cable del usuario,

[49] CMTS (Cable Modem Termination System) es un componente que se utiliza en las redes de cable para proporcionar servicios de alta velocidad, como el acceso a Internet.

esencialmente actuando como el punto de acceso a Internet para los usuarios de cable módem.

El nivel de distribución está compuesto por nodos, instalados a nivel urbano, que distribuyen la señal a diferentes zonas de la ciudad. Estos nodos, a su vez, alimentan los sistemas de distribución de cable que llevan la señal de Internet a los hogares de los usuarios.

Finalmente, en el nivel del usuario, encontramos los equipos de **Cable Módems o CM**[50], instalados en los domicilios de los usuarios. Estos equipos reciben la señal del cable coaxial y tienen la capacidad de distribuir esta señal de Internet a través de puertos Ethernet y también WiFi en el hogar del usuario.

Es importante destacar que esta red, denominada Red **Híbrida de Fibra y Coaxial** (HFC), utiliza tanto fibra óptica como cable coaxial para transportar las señales de datos. Esto proporciona una solución robusta y de alta velocidad para los servicios de Internet de banda ancha.

En este contexto, el entorno de pruebas en la red fija fue construido para imitar tan de cerca cómo fue posible la red de producción, utilizando los mismos tipos de equipos y configuraciones. Para estas pruebas se utilizó un equipo CMTS que se disponía para estos fines, el cual fue conectado a equipos CM, que imitaban a los dispositivos de los clientes en sus hogares.

Para asegurar que las pruebas no afectaran a la red de producción y a los clientes reales, este entorno de pruebas estaba completamente aislado del resto de la red. Se estableció una configuración específica del DNS en el CMTS de prueba, similar a la configuración que se planeaba implementar en la red de producción. Esto permitió probar el nuevo sistema DNS en un entorno controlado y seguro, minimizando los riesgos antes de la implementación en la red de producción.

[50] Se refiere a los equipos que los ISP instalan en los domicilios de los usuarios, los cuales tienen reciben la señal de Internet y la distribuyen en el domicilio del usuario mediante conexiones Ethernet o WiFi.

Todas las pruebas se realizaron de manera exhaustiva, garantizando que la funcionalidad recursiva en el nuevo sistema DNS funcionara correctamente una vez implementado en la red de producción, tanto en términos de resolución de nombres de dominio como de rendimiento y escalabilidad.

2.6.5.3 PRUEBAS EN AMBIENTE CONTROLADO PARA LA FUNCIONALIDAD AUTORITATIVA

Para evaluar la funcionalidad autoritativa, se utilizó un dominio no activo comercialmente. En coordinación con NIC Bolivia, se modificaron las direcciones DNS del dominio en cuestión. Tras un período de 12 horas, tiempo necesario para su propagación a través de Internet, se procedió a probar el acceso al dominio, confirmando así su correcto funcionamiento.

2.6.5.4 PRUEBAS DEL PROVEEDOR

Al igual que el ISP, el proveedor también realizó sus propias pruebas una vez que el sistema estuvo completamente instalado y configurado. En resumen, el proveedor realizó las siguientes validaciones:

- Realizó pruebas de **ping**[51] a los servidores recursivos con el objetivo de medir el tiempo de respuesta.
- Efectuó pruebas de resolución DNS con herramientas como **nslookup y dig**[52] a contenido cacheado. Se esperaba que los tiempos registrados tengan similitud con los tiempos de un ping normal.
- Ejecutó pruebas de estrés en el sistema usando la herramienta **dnsperf**[53].

[51] Ping es una herramienta de diagnóstico que comprueba la conectividad entre dos nodos o dispositivos en una red. Funciona enviando un paquete de datos a un destino y luego esperando una respuesta. El tiempo que tarda la respuesta en llegar se conoce como tiempo de ping y es una medida de la latencia de la red.
[52] Nslookup y dig son herramientas utilizadas para realizar consultas DNS y obtener información de los servidores de nombres. Proporcionas detalles como las direcciones IP o los distintos registros de un dominio.
[53] Dnsperf es una herramienta de código abierto que se utiliza para realizar pruebas de estrés en servidores DNS.

- Confirmó que el servidor DNS autoritativo respondiera únicamente a las consultas de datos para los cuales tiene autoridad (es decir, las zonas DNS que tiene creadas), y que no estuviera tratando de resolver consultas para las que no tiene autoridad.
- Verificó que el servidor no rechazara una transferencia de zona. La transferencia de zona es un proceso en el cual un servidor DNS autoritativo secundario solicita toda la información de la zona de un servidor DNS autoritativo primario. Este caso puede darse, por ejemplo, si el servidor DNS secundario está iniciando por primera vez y necesita toda la información de la zona, o si el servidor secundario está realizando una actualización periódica de los datos de la zona.
- Comprobó que el servidor autoritativo respondiera a las consultas tanto a través del protocolo UDP como de TCP en el puerto 53. Cabe aclarar que la mayoría de las consultas DNS se realizan utilizando UDP porque es más eficiente y rápido. Sin embargo, el protocolo UDP tiene una limitación de tamaño de paquete de 512 bytes. Si la respuesta a una consulta DNS supera este tamaño, se utiliza TCP, que no tiene esa restricción. Por lo tanto, un servidor DNS debe estar configurado para manejar consultas tanto en UDP como en TCP para asegurar la correcta funcionalidad del servicio.
- Adicionalmente, antes de que el sistema fuera puesto en servicio comercial, el proveedor realizó una validación general de la integridad de cada uno de los servidores asegurando que el software estuviera correctamente instalado junto con sus correspondientes licencias, que todos los servicios estuvieran bien configurados y que cada vez que una máquina se reiniciara, todo el sistema se levantara sin intervención. También revisó que todo el direccionamiento IP estuviera correcto y que los puertos necesarios estuvieran abiertos en cada servidor. De igual forma, se aseguró de que las listas de acceso estuvieran correctas de acuerdo a la información provista por el ISP.

2.6.5.5 MATRIZ DE PRUEBAS

La siguiente tabla contiene los casos mínimos de pruebas que se tenían que completar para las pruebas preproducción, que también fueron utilizadas para las pruebas posproducción.

Tabla 2.6.5.5-1 Matriz de Pruebas

NAVEGACION	RESULTADO ESPERADO	ORIGEN	CIUDAD	RESPONSABLE	RESULTADO
www.google.com	Acceso normal al sitio	Dispositivo Movil			
www.facebook.com	Acceso normal al sitio	Dispositivo Movil			
www.youtube.com	Acceso normal al sitio	Dispositivo Movil			
www.twitter.com	Acceso normal al sitio	Dispositivo Movil			
www.baidu.com	Acceso normal al sitio	Dispositivo Movil			
www.bbc.co.uk	Acceso normal al sitio	Dispositivo Movil			
www.tigo.com.bo	Acceso normal al sitio	Dispositivo Movil			
Speedtest	Uso normal del aplicativo	Dispositivo Movil			
Whatsapp	Uso normal del aplicativo	Dispositivo Movil			
Tigo Shop	Uso normal del aplicativo	Dispositivo Movil			
Tigo Sports	Uso normal del aplicativo	Dispositivo Movil			
www.google.com	Acceso normal al sitio	Dispositivo Fijo			
www.facebook.com	Acceso normal al sitio	Dispositivo Fijo			
www.youtube.com	Acceso normal al sitio	Dispositivo Fijo			
www.twitter.com	Acceso normal al sitio	Dispositivo Fijo			
www.baidu.com	Acceso normal al sitio	Dispositivo Fijo			
www.bbc.co.uk	Acceso normal al sitio	Dispositivo Fijo			
www.tigo.com.bo	Acceso normal al sitio	Dispositivo Fijo			
www.micuenta.tigo.com.bo	Acceso normal al sitio	Dispositivo Fijo			

CORREOS	RESULTADO ESPERADO	ORIGEN	CIUDAD	RESPONSABLE	RESULTADO
Envio desde dominio @tigo.net.go	Correo recibido en destino	Dispositivo Movil			
Recepcion hacia dominio @tigo.net.go	Correo recibido en destino	Dispositivo Movil			
Envio desde dominio @tigo.net.go	Correo recibido en destino	Dispositivo Fijo			
Recepcion hacia dominio @tigo.net.go	Correo recibido en destino	Dispositivo Fijo			

Fuente: Elaboración Propia

2.6.5.6 PRUEBAS DE REDUNDANCIA

Para validar la redundancia del sistema, se simularon fallas en cada nodo individualmente al desconectarlos del Backbone de Internet. Ambos nodos pasaron la prueba, demostrando que el sistema puede tolerar fallos de un nodo sin afectar negativamente el rendimiento o la disponibilidad del servicio.

2.6.5.7 EJECUCIÓN DE LAS PRUEBAS PREPRODUCCIÓN

En relación a las pruebas de rendimiento, el equipo técnico llevó a cabo una serie de mediciones utilizando la herramienta de código abierto 'DNS Benchmark'. Los datos resultantes de estas pruebas, se recopilaron y promediaron a partir de múltiples mediciones realizadas con la mencionada herramienta.

Tabla 2.6.5.7-1 Resultados de las Pruebas de Rendimiento

DNS Nuevo	Mínimo (segundos)	Promedio (segundos)	Máximo (segundos)	Desviación Estándar (segundos)	Confiabilidad (%)
Cached Name	0,012	0,013	0,014	0,001	100,0
Uncached Name	0,054	0,167	0,330	0,055	100,0
DotCom Lookup	0,033	0,036	0,037	0,001	100,0
DNS Actual	Mínimo (segundos)	Promedio (segundos)	Máximo (segundos)	Desviación Estándar (segundos)	Confiabilidad (%)
Cached Name	0,011	0,012	0,014	0,000	100,0
Uncached Name	0,062	0,142	0,313	0,048	100,0
DotCom Lookup	0,185	0,187	0,190	0,001	100,0
DNS Google	Mínimo (segundos)	Promedio (segundos)	Máximo (segundos)	Desviación Estándar (segundos)	Confiabilidad (%)
Cached Name	0,159	0,160	0,162	0,000	100,0
Uncached Name	0,208	0,329	0,593	0,089	100,0
DotCom Lookup	0,231	0,313	0,367	0,055	100,0

Fuente: Elaboración Propia

Los términos utilizados en esta tabla son los siguientes:

Cached Name: Esta prueba mide el tiempo en segundos que tarda el servidor DNS en responder a una consulta para un nombre de dominio que ya tiene en su cache. El rendimiento es más rápido que para las otras dos categorías, como se esperaba, ya que el servidor DNS ya tiene la respuesta almacenada y no necesita buscarla.

Uncached Name: Mide el tiempo en segundos que el servidor DNS tarda en responder a una consulta para un nombre de dominio que no está en su cache. Esto implica que el servidor DNS tiene que realizar una serie de consultas a otros servidores DNS para obtener la respuesta. Como se esperaba, los tiempos de respuesta son más largos en comparación con las consultas de nombres en cache.

DotCom Lookup: Esta prueba mide el tiempo que tarda el servidor DNS en buscar los nombres de dominio de los servidores DNS de nivel superior '.com'. Estos tiempos de respuesta, deberían ser menores a los tiempos de las pruebas 'Uncached Name', pero esto no siempre es así ya que se depende de múltiples factores como la ubicación de los servidores, el momento de la ejecución de las pruebas, la carga de la red, la carga de trabajo del servidor DNS, entre otros.

2.6.5.8 ANÁLISIS DE RESULTADOS

Es relevante destacar que no existen normas internacionales estrictas que definan el tiempo de resolución óptimo para una consulta DNS. No obstante, diversas fuentes, incluida Google, ofrecen pautas generales. Se considera aceptable un tiempo de respuesta DNS inferior a 200 ms, mientras que un tiempo de respuesta DNS inferior a 50 ms se considera muy bueno, y un tiempo menor a 10 ms se cataloga como excelente. Estos tiempos actúan más como recomendaciones generales que como estándares estrictos, dada la influencia de múltiples factores como la ubicación geográfica, la calidad de la conexión a Internet y el rendimiento del hardware del servidor en los resultados.

En este contexto, y centrando la evaluación en los tiempos de respuesta promedio, todas las métricas obtenidas se sitúan por debajo de los 200 ms considerados como aceptables. En particular, la métrica 'Cached Name' arroja un tiempo promedio de 0,013 segundos, aproximándose a lo que se consideraría como excelente. La métrica 'Uncached Name' con 0,167 segundos se catalogaría como aceptable, y 'DotCom Lookup' con 0,036 segundos se consideraría muy bueno. En resumen, el nuevo sistema DNS no solo cumple con las pautas generales de tiempos de respuesta aceptables, sino que también se aproxima a las métricas que se considerarían excelentes.

En cuanto a una comparación directa con el sistema anterior, es importante resaltar la mejora significativa en el indicador 'DotCom Lookup', que muestra un aumento en el rendimiento del 80.75%.

En relación con la evaluación de incidentes y problemas de servicio, el grupo de 20 usuarios de prueba, que estuvo utilizando el nuevo DNS durante un período de dos semanas para acceder a Internet, no reportó problemas en la navegación web ni en el uso de aplicaciones que requieran conexión a Internet. Al contrario, los usuarios indicaron que experimentaron normalidad en el consumo de estos servicios, lo que sugiere un desempeño estable y fiable del nuevo sistema DNS.

En cuanto a la funcionalidad autoritativa del DNS, el proveedor confirmó que los datos de zona del ISP se configuraron correctamente en los servidores autoritativos. Estos datos de zona son esenciales para la resolución correcta de nombres de dominio. Además, se llevaron a cabo pruebas internas que verificaron que los servidores autoritativos respondían adecuadamente a las solicitudes de resolución de nombres. Estas pruebas también confirmaron que otras operaciones críticas, como la transferencia de zonas entre servidores, se ejecutaban de manera efectiva.

2.6.5.9 CONCLUSIONES DE LAS PRUEBAS PREPRODUCCIÓN

Basado en los tiempos de respuesta obtenidos y la alta confiabilidad durante las pruebas funcionales y de redundancia, la conclusión fue que el nuevo sistema DNS estaba listo para pasar a producción.

Los resultados y conclusiones se presentaron, tanto a los gerentes del área de **Aseguramiento de Servicio** como al área de **Planificación y Capacidad**, logrando una aprobación interna. Posteriormente, estos resultados se compartieron con el Director del área técnica y las gerencias comerciales relacionadas con Internet, logrando un consenso y aprobación final para poner el nuevo sistema en producción, dando por concluida exitosamente la etapa de pruebas preproducción del nuevo sistema DNS.

2.6.6 PUESTA EN PRODUCCIÓN

Para la implementación de un cambio significativo en la red técnica o para la puesta en marcha de un nuevo sistema, como fue el caso del nuevo sistema DNS, se cumplió con los siguientes requisitos:

- Aprobación del documento **MOP (Method of Procedure)**[54] por parte del personal técnico responsable. Este documento contiene los procedimientos para la implementación del nuevo sistema, así como los pasos a seguir para revertir los cambios en caso de detectar errores.
- Las fechas seleccionadas para la implementación fueron cuidadosamente revisadas y aprobadas de acuerdo al calendario de cambios técnicos de la empresa. Se tuvo en cuenta que no se debían ejecutar dos cambios importantes o de alto impacto en la red en la misma fecha, o incluso en fechas consecutivas, para asegurar que los recursos humanos estuvieran completamente enfocados en la actividad programada y que la parte de la red afectada estuviera estable.
- Áreas externas, como el servicio de atención al cliente y el **Call Center**[55], fueron informadas del cambio. Se solicitó la presencia de personal de turno para realizar pruebas y monitorear las consultas de los clientes después de la implementación del cambio.
- Aunque el proceso de puesta en servicio del nuevo sistema DNS fue pensado para no interrumpir los servicios de Internet Móvil e Internet Fijo, se tomó la precaución adicional de obtener un permiso de corte de servicio de la ATT. Este permiso, en línea con las políticas de la empresa y las normas del ente regulador boliviano.

Estos pasos se siguieron rigurosamente para garantizar el éxito de la implementación del proyecto y minimizar cualquier posible interrupción del servicio.

[54] MOP (Method of Procedure) es un documento detallado que proporciona instrucciones paso a paso sobre cómo realizar una tarea específica o actividad para asegurar que las tareas complejas se realicen de manera consistente y segura.

[55] Call Center es un centro de llamadas, la cual tiene como una de sus principales funciones la recepción de reclamos de los clientes en general.

2.6.6.1 DESCRIPCIÓN DEL CAMBIO EN LA RED MÓVIL

La ejecución del cambio en la red móvil consistió esencialmente en reconfigurar el APN definido en el elemento **MME**[56], parte integral del nodo de la red troncal de conmutación de paquetes, conocido como **EPC (Evolved Packet CORE)**[57] dentro de una red móvil LTE. Este cambio no requirió reiniciar el MME y fue transparente tanto para los usuarios como para la red móvil, es decir, no impactó en el servicio.

Es importante enfatizar que la reconfiguración realizada en el MME no significaba que los dispositivos móviles de los usuarios comenzarían a utilizar inmediatamente el nuevo sistema DNS. En una red móvil, los usuarios se conectan a través de un procedimiento conocido como **Establecimiento de Sesión**, durante el cual se les asigna un APN (Nombre del Punto de Acceso) que dirige su tráfico de datos. Este APN incluye información de DNS, y esta información se mantiene constante durante toda la sesión de datos del usuario. Sólo cuando la sesión de datos se termina y se inicia una nueva (por ejemplo, cuando se reinicia el dispositivo móvil o se desplaza entre diferentes áreas de cobertura celular) se consulta de nuevo la información del APN y, por lo tanto, la nueva configuración DNS se tomará en cuenta. Esto significa que la actualización completa a la nueva configuración DNS se realiza de forma gradual, a medida que los usuarios establecen nuevas sesiones de datos a lo largo del tiempo.

Una opción para que todos los usuarios adopten inmediatamente la nueva configuración DNS habría sido forzar una cancelación de registro masivo de todos los usuarios en la red, lo que les obligaría a establecer nuevas sesiones de datos y, por lo tanto, a obtener la nueva información del DNS. Sin embargo, este enfoque podría haber tenido consecuencias significativas. Al generar un alto volumen de solicitudes de establecimiento de sesión simultáneamente, habría supuesto una carga considerable para los nodos de la red móvil, y el nuevo sistema DNS entre otros, con la posibilidad de congestionar estos elementos.

[56] El MME (Mobility Management Entity) es un componente clave en una red LTE que se encarga de la gestión de la movilidad, incluyendo la autenticación de usuarios, el seguimiento de su ubicación y la gestión de las sesiones de datos.

[57] El EPC (Evolved Packet Core) es la infraestructura de red troncal de una red móvil LTE, que maneja el enrutamiento de datos y la conectividad a Internet para los usuarios de la red móvil. Es responsable de la gestión de la movilidad, el control de sesiones y la autenticación de los usuarios.

Además, también podría haber resultado en una serie de usuarios que, por una variedad de razones (como problemas de señal en el momento de la cancelación de registro forzado), no hubieran podido establecer una nueva sesión de datos, lo que podría haber llevado a una afectación al servicio de los usuarios y consecuentes reclamos.

En lugar de optar por este enfoque potencialmente disruptivo, se decidió implementar el cambio en la configuración del DNS en el MME y permitir que la adopción de la nueva configuración por parte de los usuarios se produjera de forma natural y gradual. Esto se basa en el entendimiento de que, debido a la naturaleza de la red móvil y al comportamiento habitual de los usuarios (como reiniciar sus dispositivos o desplazarse entre diferentes áreas de cobertura celular), los terminales móviles de los usuarios regularmente terminan y establecen nuevas sesiones de datos. Este enfoque ofreció la ventaja de un cambio transparente para los usuarios y un impacto mínimo en la red móvil y en el Backbone Internet.

2.6.6.2 DESCRIPCIÓN DEL CAMBIO EN LA RED FIJA

Para el caso de la red fija, es necesario considerar que los equipos CM que se instalan en los domicilios de los usuarios obtienen su configuración, incluyendo la dirección DNS, mediante un archivo de configuración, el cual se descarga desde un sistema de aprovisionamiento central a través de la conexión que los enrutadores tienen con sus respectivos CMTS.

Así como sucede en la red móvil, los CM no actualizan su configuración de DNS en tiempo real. Solo recibirán la nueva dirección DNS cuando se reinicien y se reconecten a la red, en cuyo momento descargarán un nuevo archivo de configuración con la nueva dirección DNS.

Por lo tanto, el proceso de cambio será gradual y depende de cuándo se reinicien los CM de los clientes. Al igual que en la red móvil, esto se consideró como una ventaja, ya que permitió un despliegue gradual y de bajo impacto en la red fija y el Backbone Internet.

A través de este enfoque el cambio se pudo implementar en fases para lo cual en una primera fecha se escogió un grupo de CMTS a los cuales se les aplico el cambio, para

posteriormente en una segunda fecha proceder con un segundo grupo y finalmente en una tercera fecha se concluyó la actividad. De esta forma se minimizaron los riesgos y se pudo monitorear el cambio gradual de los cambios realizados.

2.6.6.3 DESCRIPCIÓN DEL CAMBIO PARA LA FUNCIONALIDAD AUTORITATIVA

Las dos secciones anteriores hacen alusión a la funcionalidad recursiva. Para realizar el cambio en la funcionalidad autoritativa, fue necesario coordinar con la entidad NIC Bolivia, encargada de administrar todos los dominios que están bajo el dominio ccTLD **'.bo'**. Para una mejor comprensión se aclara que cuando una entidad requiere un dominio, como por ejemplo https://umsa.bo/, tal dominio debe ser solicitado a NIC Bolivia, quienes se encargan de su asignación, administración y control.

Dentro de los parámetros que se configuran en cada dominio están las direcciones DNS, como en el siguiente ejemplo:

Tabla 2.6.6.3-1 Configuración de DNS Autoritativos para el dominio umsa.bo

	SERVIDORES DNS
DNS1 :	marte.umsa.bo
IP1 :	200.7.160.10
DNS2 :	jupiter.umsa.bo
IP2 :	200.7.170.100

Fuente: Elaboración Propia

Las direcciones IP de DNS mostradas en la figura son las direcciones de los servidores autoritativos encargados de la resolución del dominio umsa.bo.

Los cambios realizados en NIC Bolivia toman un tiempo aproximado de 12 horas para propagarse en Internet, por este motivo se coordinó con ellos para que el cambio se aplique aproximadamente a las 14:00 horas del día anterior, de esa forma el cambio se haría efectivo a las 02:00 AM del día en que se realizaron los cambios de la funcionalidad recursiva.

2.6.6.4 PRUEBAS POSPRODUCCIÓN

Para las pruebas posproducción, se tomó como base la matriz planteada en la sección 2.6.5.5, la cual cumple con el objetivo de validar la efectividad del cambio y asegurar que todos los sistemas y servicios dependientes del DNS funcionaran correctamente, incluyendo pruebas de navegación a diferentes sitios web, pruebas de servicios que requerían conexión a Internet y pruebas de los servicios propios del ISP, como el acceso a su página principal y el envío y recepción de correos. De esta manera, se abarcó tanto las funcionalidades recursivas como autoritativas.

Se planificaron estas pruebas para ser realizadas desde varias ubicaciones geográficas, concretamente las principales ciudades donde opera el ISP, y se llevaron a cabo tanto en la red móvil como en la fija. El personal designado por el área comercial fue responsable de realizar estas pruebas y dar la aprobación final del cambio, asegurando que se mantuviera la calidad de servicio al cliente.

Antes, durante y después de los cambios, se mantuvo una estrecha comunicación con el personal de **Atención al Cliente,** quienes a través del **Call Center**, nos proporcionaron retroalimentación continua acerca de la cantidad de reclamos de clientes sobre el servicio de Internet, que se recibieron después de la implementación de los cambios. En cada etapa de los cambios fue posible confirmar que, en general, el volumen de reclamos no varió significativamente en comparación con los días previos al cambio. Esta validación formo parte de las pruebas posproducción.

Una vez concluidas estas pruebas el área comercial nos dio su visto bueno para dejar el cambio en producción comercial, con lo cual se dejó el sistema bajo monitoreo por parte de personal del **NOC (Network Operation Center)**[58], así como de personal del proveedor, para que en caso de que en horas posteriores se detectaran anomalías, se aplique el procedimiento de vuelta atrás o **Rollback**.

[58] NOC (Network Operation Center) es una unidad centralizada desde donde se supervisan, controlan y administran las operaciones de red de una organización. El NOC es fundamental para asegurar la máxima disponibilidad y rendimiento de la red, mediante el monitoreo de las alarmas, toma de medidas correctivas cuando sea necesario y, aplicación del escalamiento.

Después de realizar todas estas validaciones, no se tuvo ninguna afectación en los servicios de acceso a Internet, tanto Móvil como Fijo, siendo el cambio exitoso.

2.6.6.5 ANÁLISIS DE ESTADÍSTICAS DESPUÉS DEL CAMBIO

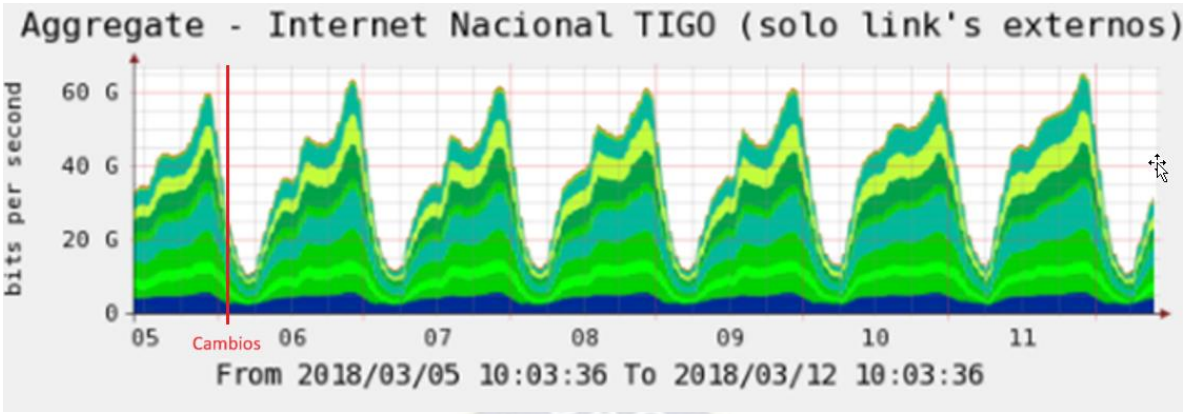
Para el análisis del rendimiento del nuevo sistema DNS, se emplearon datos estadísticos y de comportamiento provenientes tanto de los sistemas afectados por la implementación como del propio sistema DNS desplegado. Se maximizó el uso de aquellos sistemas que contaban con recursos estadísticos más robustos. Cabe señalar que las gráficas presentadas en este apartado son representativas de las gráficas reales con las que se trabajó durante el análisis. Debido a las políticas de confidencialidad del ISP, no se pueden presentar las gráficas completas.

2.6.6.5.1 VOLUMEN DE TRAFICO

Una de las verificaciones iniciales que se realizaron tras la implementación del nuevo sistema DNS consistió en asegurarse de que el volumen total de tráfico de la red no sufriera variaciones significativas. En este sentido, cabe mencionar que no se esperaba que la introducción del nuevo sistema DNS incrementara o disminuyera el tráfico global del ISP.

La siguiente gráfica, extraída del sistema de monitoreo, muestra el tráfico total del ISP durante la semana en que se realizó el cambio. Como se puede observar, no se registraron variaciones apreciables en relación al volumen de tráfico. Esta tendencia se mantuvo constante en las semanas posteriores a la implementación del cambio.

Figura 2.6.10 Trafico Nacional del ISP



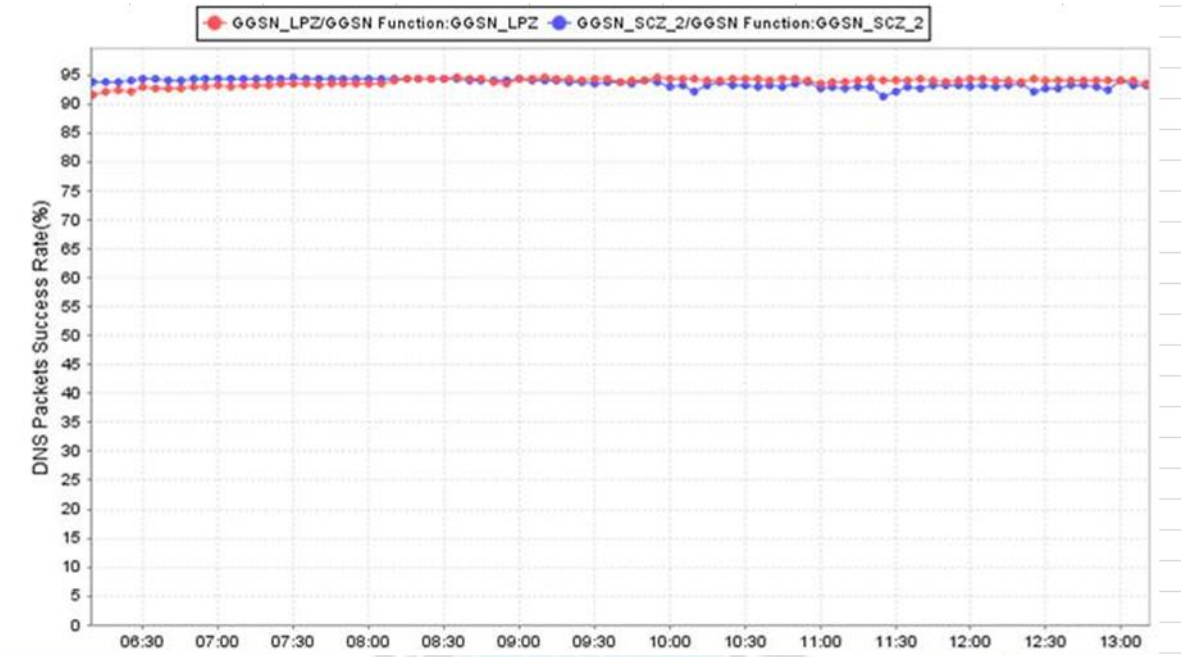
Fuente: Sistema de Monitoreo del ISP

2.6.6.5.2 RED MÓVIL

Uno de los indicadores más representativos en la red móvil para detectar anomalías a nivel de DNS es el **DNS Packet Success Rate**. Este indicador compara el número de paquetes DNS enviados desde la red móvil con el número de paquetes DNS recibidos como respuesta. Antes de la implementación del nuevo sistema DNS, el comportamiento histórico de este indicador mostraba una oscilación en el rango de 92% a 95%, estableciéndose así, como el rango de funcionamiento normal para la red móvil del ISP.

Después de implementar el nuevo sistema DNS, se observó que este indicador se mantuvo consistentemente dentro del rango previamente definido de 92-95%. Este resultado sugiere que la nueva implementación de DNS no tuvo un impacto negativo en la eficiencia de la resolución de DNS en la red móvil. La siguiente gráfica muestra la tasa de éxito de este indicador para la red móvil oriental y la red móvil occidental.

Figura 2.6.11 KPI DNS Packet Success Rate



Fuente: Sistema de Monitoreo del ISP

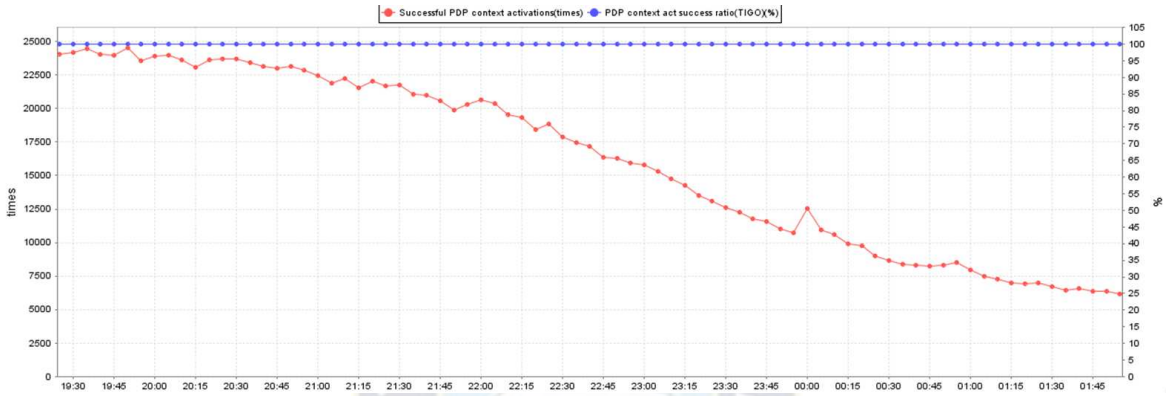
Otro indicador clave en la red móvil es el nivel de éxito en el establecimiento de los **contextos PDP**[59], el cual es conocido como PDP Context Success Rate. Este indicador es crítico porque mide la eficacia con la que se establecen conexiones de datos entre el dispositivo del usuario y la red. El proceso incluye la asignación de una dirección IP al dispositivo y la configuración de varios parámetros, como el servidor DNS para la resolución de nombres de dominio.

Si se producen anomalías en el servidor DNS, como tiempos de respuesta lentos o fallos en las consultas, este indicador se vería negativamente afectado. Tal situación se traduciría en una disminución de la capacidad del dispositivo para establecer una conexión de datos efectiva, lo que podría resultar en fallos en el establecimiento del contexto PDP o en un rendimiento de la conexión subóptimo.

[59] **PDP Context** (Contexto de Protocolo de Datos por Paquetes) es una estructura de datos que establece y gestiona una sesión de datos entre un dispositivo móvil y la red móvil. Este contexto contiene información crucial como la dirección IP asignada al dispositivo, parámetros de Calidad de Servicio (QoS) y el servidor DNS utilizado para la resolución de nombres de dominio.

Después de la implementación del nuevo servidor DNS, se realizó un seguimiento de este indicador para identificar cualquier cambio significativo. La siguiente gráfica muestra el indicador PDP Context Success Rate en color azul, y los datos indican claramente que el cambio en el servidor DNS no provocó fluctuaciones fuera del rango aceptable para este indicador.

Figura 2.6.12 KPI PDP Context Success Rate



Fuente: Sistema de Monitoreo del ISP

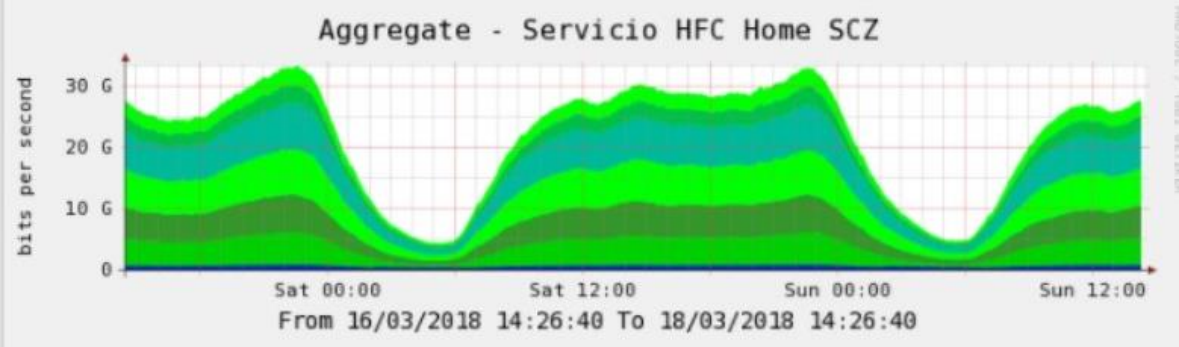
2.6.6.5.3 RED FIJA

Para la red fija, el enfoque estuvo en asegurar que los volúmenes de tráfico se mantuvieran estables durante y después de la implementación del nuevo sistema DNS. Este monitoreo se efectuó a nivel global de la red y también a nivel de cada uno de los CMTS específicos. Para ello, se controló que al momento del cambio no se registraran variaciones bruscas, por otra parte se comparó el volumen de tráfico con el volumen del mismo horario del día anterior y con el volumen del mismo horario del mismo día de la semana anterior, esperando encontrar valores similares. Las gráficas que se presentan a continuación sirven como ejemplos ilustrativos y muestran las mediciones de tráfico global y por CMTS.

En base a este enfoque, se pudo corroborar que tanto el volumen de tráfico general como el correspondiente a cada CMTS se mantuvieron sin alteraciones significativas y dentro de valores normales, validando así la eficacia de la nueva implementación de DNS en la red fija.

La siguiente grafica muestra el tráfico de la red fija oriental.

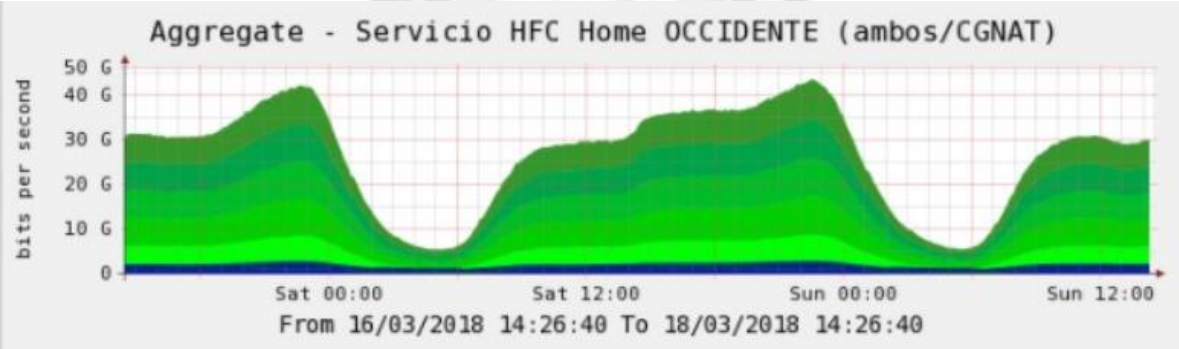
Figura 2.6.13 Trafico HFC Oriental



Fuente: Sistemas de Monitoreo del ISP

La siguiente grafica muestra el tráfico de la red fija occidental.

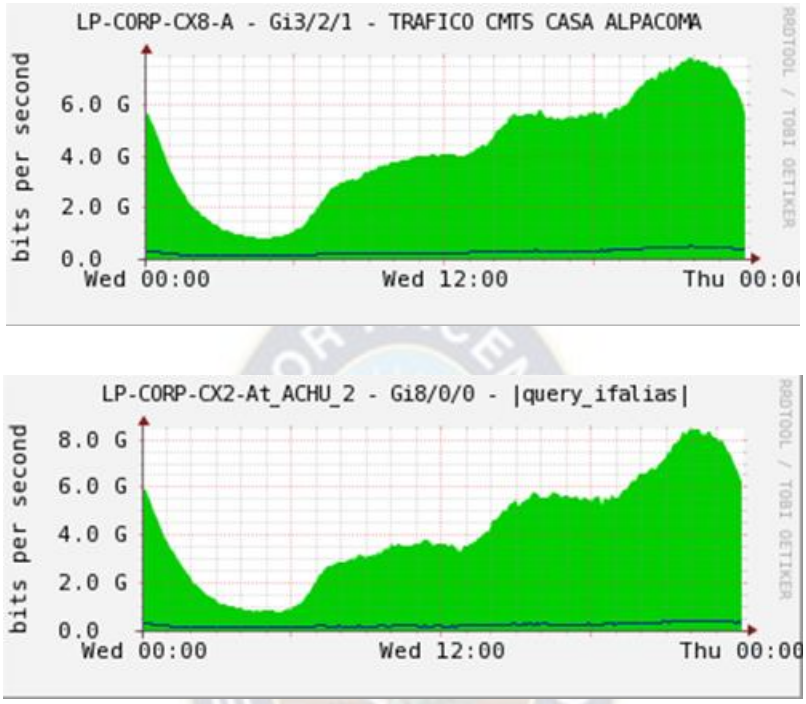
Figura 2.6.14 Trafico HFC Occidental



Fuente: Sistemas de Monitoreo del ISP

La siguiente grafica muestra el tráfico de dos CMTS de la ciudad de La Paz: Alpacoma y Achumani.

Figura 2.6.15 Ejemplos de Trafico Individual de dos CMTS

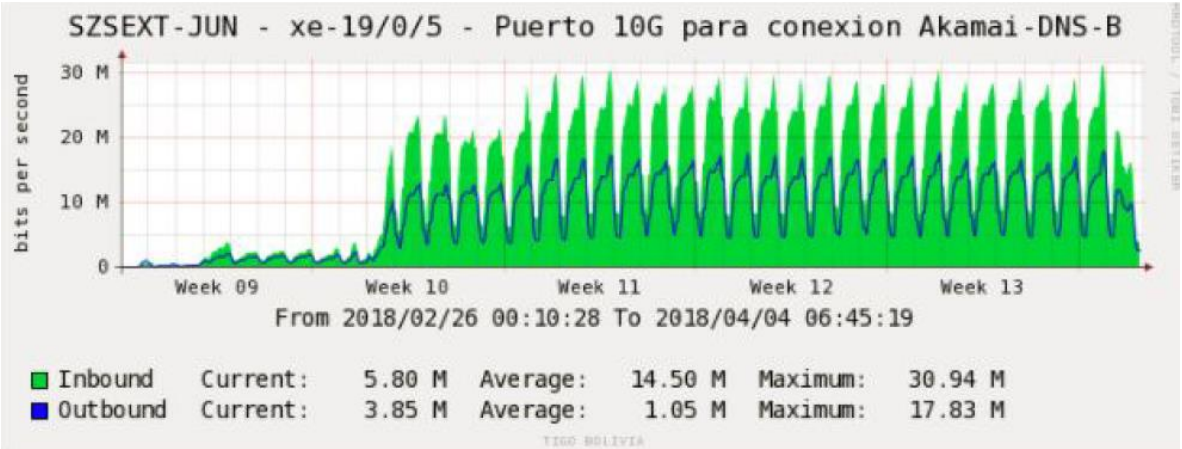


Fuente: Sistemas de Monitoreo del ISP

2.6.6.5.4 ESTADÍSTICAS DEL NUEVO SISTEMA DNS

La siguiente gráfica ilustra el tráfico de uno de los servidores recursivos. Como se puede apreciar, tras la puesta en servicio del nuevo sistema DNS, el volumen de tráfico aumenta significativamente. Esto se debe a que el nuevo servidor ahora está asumiendo el tráfico de Internet de la red del ISP.

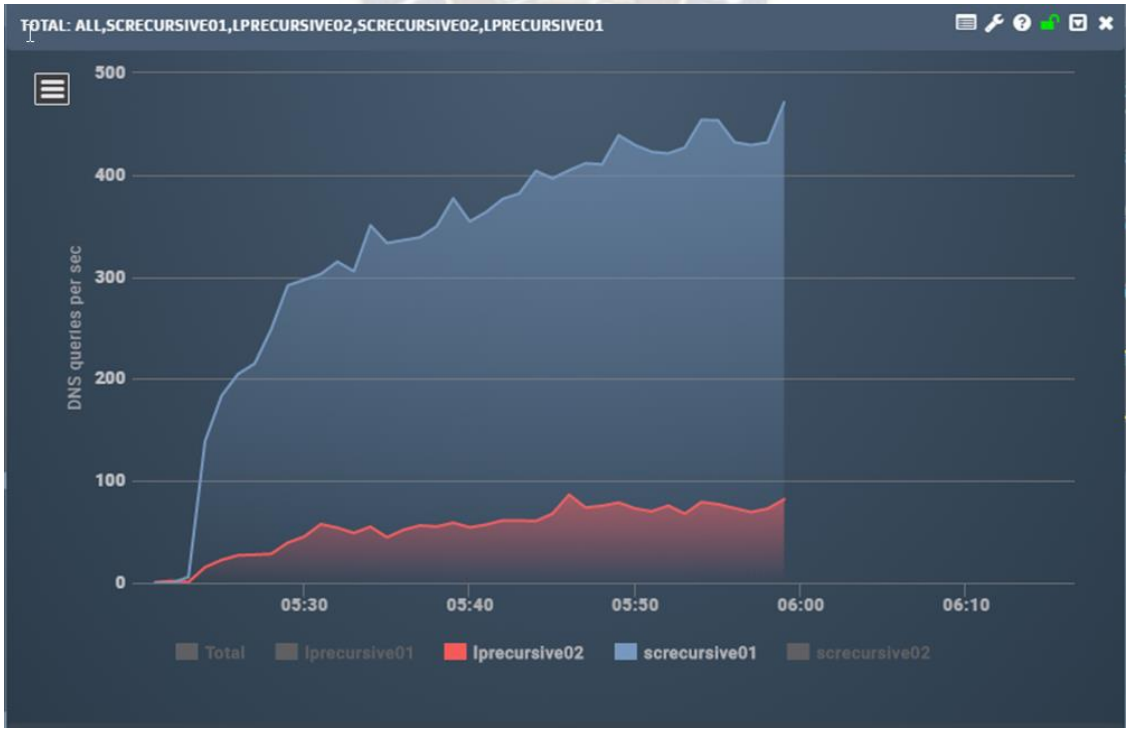
Figura 2.6.16 Ejemplo de Trafico Servidor Recursivo



Fuente: Sistemas de Monitoreo del ISP

Además, obtuvimos confirmación por parte del proveedor de que el nuevo sistema DNS estaba procesando adecuadamente los eventos de recursividad. Las siguientes gráficas muestran que el nuevo sistema ya estaba gestionando tráfico de forma efectiva.

Figura 2.6.17 Nuevo DNS: Consultas por Segundo



Fuente: Sistemas de Monitoreo del Sistema DNS

2.6.6.6 ACTIVIDADES COMPLEMENTARIAS

Se instruyó al NOC para poner en servicio las alarmas correspondientes a los servidores del nuevo sistema DNS en los sistemas de monitoreo existentes. Esto garantizaría que cualquier falla o anomalía en el funcionamiento del nuevo sistema DNS se detectara y se notificara de manera oportuna.

Una vez que el nuevo sistema DNS entró en servicio, el proveedor mantuvo un período de monitoreo cercano. Durante este tiempo, también se llevaron a cabo actividades de capacitación dirigidas al personal responsable del nuevo sistema y a los miembros de otras áreas relacionadas. Esta etapa fue importante para familiarizar al personal con el funcionamiento del sistema, sus características y su mantenimiento.

Cumpliendo la normativa de la ATT, en días posteriores se pasaron informes a este ente acerca de la actividad realizada, mencionando que la misma no produjo afectaciones al servicio de los usuarios.

2.6.7 RESUMEN Y RESULTADO

Al resumir el desarrollo del proyecto, se distinguen tres fases principales:

Fase de Implementación: El ISP suministró la infraestructura virtual conforme a las indicaciones del proveedor, asegurando también la conectividad de red requerida. Paralelamente, el proveedor realizó la instalación y configuración del sistema. Además, el ISP ajustó el Backbone Internet para garantizar conectividad con las redes Móvil y Fija, así como para proporcionar acceso a Internet al nuevo sistema.

Fase de Pruebas Preproducción: Se establecieron ambientes de prueba controlados para los servicios de Internet Móvil e Internet Fijo, en los cuales se realizaron las pruebas, tanto funcionales como de rendimiento y redundancia, cuyos resultados permitieron evaluar el nuevo sistema y generar la aprobación para proseguir con la siguiente fase.

Fase de Puesta en Producción: Se diseñó una estrategia que permitió la integración gradual del nuevo sistema sin interrupciones para los usuarios finales. Esta fase contó con

la validación de las áreas comercial y de atención al cliente y cumplió con las regulaciones y normas internas de la compañía. Se seleccionó cuidadosamente la fecha de transición para asegurar la disponibilidad total de recursos, tanto humanos como técnicos.

Una vez concluidas estas fases y gracias al esfuerzo conjunto de las áreas técnica, comercial y de atención al cliente, el proyecto culminó con éxito, dejando el nuevo sistema en producción.

Entre las lecciones aprendidas destaca la importancia de una planificación detallada, la comunicación constante y el monitoreo riguroso, que fueron esenciales para anticipar desafíos y solucionarlos a tiempo.

2.7 CONCLUSIONES Y RECOMENDACIONES

2.7.1 RESULTADOS PRINCIPALES

2.7.1.1 ELABORACIÓN DE LA ESTRATEGIA TÉCNICA

La estrategia de implementación y migración del nuevo sistema DNS se diseñó cuidadosamente para cumplir con el objetivo específico de modernizar la infraestructura DNS del ISP. Esta estrategia implicó varias fases clave:

Análisis Técnico: Se realizó un estudio técnico profundo para integrar el nuevo sistema en el Backbone Internet, identificando los posibles riesgos y soluciones.

Ambiente de Pruebas: Se estableció un entorno de pruebas controlado para validar la funcionalidad y el rendimiento del nuevo sistema, mitigando así cualquier riesgo asociado con la migración.

Implementación Gradual: La estrategia contempló la posibilidad de migrar los servicios del ISP por tipo de servicio y por ubicación geográfica. Esto redujo aún más el impacto en los servicios de Internet Móvil y Fijo, garantizando la continuidad del servicio para los usuarios finales.

Esta estrategia no solo aseguró una transición fluida, sino que también permitió un control riguroso durante cada fase del proyecto. En resumen, la implementación y migración se llevaron a cabo con éxito, confirmando plenamente la efectividad de la estrategia técnica.

2.7.1.2 IMPLEMENTACIÓN Y MIGRACIÓN DEL NUEVO SISTEMA DNS

Siguiendo la estrategia técnica delineada, se implementó el nuevo sistema DNS en el Backbone Internet de Telecel S.A. en una configuración paralela al sistema anterior. Tras completar con éxito el plan de pruebas y obtener la aprobación correspondiente, el nuevo sistema se puso en producción sin causar interrupciones ni degradaciones en los servicios de Internet Móvil y Fijo.

Una mejora técnica muy importante en este proyecto fue la adopción de una infraestructura virtual para el despliegue del nuevo sistema DNS, en contraste con la infraestructura física utilizada anteriormente. Este avance no solo aporta eficiencias económicas sino también flexibilidad técnica y administrativa, como se detalló en la sección 2.6.3.1.

2.7.1.3 INDICADORES DE CALIDAD

Se realizó una evaluación de los Indicadores Clave de Rendimiento (KPI) para cuantificar las mejoras en comparación con el sistema anterior. La evaluación arrojó resultados mixtos en los indicadores medidos, proporcionando datos para evaluar el alcance de las optimizaciones implementadas.

En el indicador DotCom Lookup se registró un significativo avance, con un incremento del 80.75% en su rendimiento. Específicamente, el tiempo de respuesta promedio disminuyó de 0.187 segundos a 0.036 segundos. Este resultado sugiere una deficiencia en el sistema DNS anterior, la cual se abordó con éxito en la nueva implementación.

Aparte del indicador DotCom Lookup, los demás indicadores no mostraron variaciones significativas con respecto al sistema preexistente. Esto podría interpretarse como un indicativo de que el sistema DNS anterior ya era eficiente en estos aspectos, o como una oportunidad para futuras investigaciones y optimizaciones.

En conclusión, aunque no se observaron mejoras en todos los indicadores clave, el notable avance en el indicador DotCom Lookup contribuye al objetivo general de mejorar la calidad de la resolución DNS. Este incremento en el tiempo de resolución de dominios comerciales populares se traduce directamente en una experiencia de navegación más rápida y eficiente para el usuario final.

2.7.2 RESULTADOS COMPLEMENTARIOS

2.7.2.1 BENEFICIO ECONÓMICO PARA EL ISP

A pesar de las restricciones de confidencialidad que impiden presentar cifras exactas, es pertinente destacar que se logró un beneficio económico en la adquisición del nuevo sistema DNS. Esta ventaja económica se obtuvo gracias a la compra coordinada de sistemas DNS para todas las filiales de Millicom en Latinoamérica. Adicionalmente, la implementación mediante tecnología de virtualización del nuevo sistema contribuyó a reducir costos operativos. Los sistemas virtuales, por su naturaleza, suelen ser más eficientes, flexibles y conllevan menores costos de mantenimiento y hardware en comparación con sistemas físicos tradicionales.

2.7.3 CONCLUSIÓN FINAL

El esfuerzo y tiempo que se invirtieron en el análisis técnico y en la planificación de todas las fases del proyecto, además de un arduo trabajo de coordinación, comunicación y colaboración entre los miembros del equipo del proyecto, el proveedor y colaboradores externos, tuvo como resultado la implementación e integración del proyecto en el Backbone Internet del ISP de forma exitosa. De esta manera, se cumplieron de forma satisfactoria los objetivos planteados al inicio del proyecto.

La monitorización continua del progreso del proyecto permitió prever desafíos, ajustar estrategias y asegurar una gestión efectiva. Con la culminación de esta implementación, se sentaron bases sólidas para futuras optimizaciones y mejoras en la infraestructura DNS del ISP. Este compromiso con la mejora continua posicionó a la empresa a la vanguardia en un entorno tecnológico en constante cambio.

2.7.4 RECOMENDACIONES

2.7.4.1 RECOMENDACIONES PARA EL ISP

Adopción del Protocolo IPv6: Es de suma importancia el protocolo IPv6 sea implementado en Backbone Internet del ISP, incluido el nuevo sistema DNS, así como las redes de servicios de Internet Móvil y Fijo. Esta transición, más allá de ser un estándar en la industria, ofrece ventajas tecnológicas significativas.

- **Eliminación de NAT (Network Address Translation)**: IPv6 disminuye la dependencia del NAT, un mecanismo que soluciona la escasez de direcciones IPv4 al permitir que varios dispositivos compartan una dirección IP pública. Al adoptar IPv6, se simplifica la infraestructura de red y se mejora el servicio al reducir la latencia asociada al proceso NAT.
- **Mejoras en la Implementación de QoS (Quality of Service) con IPv6**: Tanto IPv4 como IPv6 ofrecen soporte para QoS, sin embargo, IPv6 presenta en su diseño campos específicos para este propósito. Esta característica facilita una gestión de tráfico más eficiente, permitiendo al ISP ofrecer servicios diferenciados de alta calidad, cruciales para aplicaciones como VoIP, streaming y juegos en línea.
- **Avances en QoS (Quality of Service)**: IPv6 proporciona capacidades avanzadas de QoS en comparación con IPv4. Esto se traduce en una gestión de tráfico más eficaz, permitiendo al ISP ofrecer servicios diferenciados de alta calidad, esenciales para aplicaciones como VoIP, streaming y juegos en línea.
- **Seguridad con IPSec**: El protocolo IPSec protege la comunicación en redes IP al ofrecer autenticación y cifrado, y en IPv6 viene integrado por defecto. Esta característica asegura una robusta seguridad en la comunicación, esencial en la era actual de ciberseguridad.

Activación de Características Avanzadas del Nuevo Sistema DNS: El nuevo sistema DNS cuenta con características avanzadas cuya implementación es recomendable en fases posteriores del proyecto. Su activación no solo optimizaría la inversión del ISP, sino que también enriquecería los servicios a los usuarios finales. Es esencial priorizar las funcionalidades más alineadas al contexto y visión del ISP.

- **Funcionalidades de seguridad avanzadas**: El sistema tiene la habilidad de bloquear URLs y detectar sitios de phishing. También permite la implementación de controles parentales para restringir el acceso a ciertos tipos de contenido en Internet y ofrece la posibilidad de integración con organizaciones como la Internet Watch Foundation (IWF), Interpol, Symantec y otras, para obtener acceso a listas de sitios con contenido inapropiado o peligroso, como los sitios de abuso infantil o los que podrían infectar a los usuarios con malware.
- **Gestión de Tráfico basada en DNS**: Permite realizar restricciones en función del tipo de servicio. Por ejemplo, puede diferenciar entre servicios de streaming, llamadas por Internet y juegos en línea. Esta capacidad permitiría crear distintos tipos de servicios comerciales.
- **EDNS (Extension Mechanisms for DNS)**: Es una mejora del protocolo DNS estándar que amplía sus capacidades. Se incrementa la capacidad de datos que puede ser transferida en una sola consulta DNS, reduciendo la necesidad de otras consultas, resultando en una resolución de nombres más rápida y eficaz. Refuerza la seguridad mediante DNSSEC y provee optimizaciones que aseguran que los usuarios consuman el contenido geográficamente más cercano.

Desarrollo Profesional en Gestión de Proyectos: El equipo técnico del ISP mostró habilidad y destreza en la gestión de proyectos, para fortalecer estas habilidades se podría invertir en certificaciones como Project Management Professional, o programas similares orientados a telecomunicaciones. Esto aseguraría que el equipo técnico esté al día con las mejores prácticas de la industria y mejor preparado para afrontar desafíos futuros.

Pruebas de Redundancia Periódicas: Se recomienda ejecutar pruebas de redundancia en un intervalo regular de acuerdo a las políticas de recuperación contra desastres para garantizar que el sistema de redundancia geográfica entre los dos nodos del DNS sigue siendo efectivo. Además, estas pruebas deberían llevarse a cabo después de cualquier actualización significativa del sistema o adición de nuevos componentes.

2.7.4.2 RECOMENDACIONES ACADÉMICAS

Con un sentido de profundo respeto y gratitud hacia mi alma mater, me gustaría compartir ciertas observaciones que, en mi opinión, podrían contribuir a enriquecer el pensum académico de la carrera de Ingeniería Electrónica. Mi experiencia profesional me ha permitido identificar ciertas habilidades y conocimientos que considero podrían complementar de forma valiosa la formación actual:

Gestión de Proyectos: La realidad del mercado laboral actual demanda profesionales que puedan liderar, gestionar y participar en proyectos de forma efectiva. Incorporar módulos o cursos especializados en gestión de proyectos, quizá con la opción de obtener certificaciones reconocidas, añadiría un valor significativo a la formación de los estudiantes.

Sistemas de Comunicación y Redes: A lo largo de mi trayectoria profesional, he tenido la oportunidad de trabajar con una amplia gama de sistemas de telecomunicaciones e infraestructuras de TI. Una constante en todos estos entornos ha sido la presencia fundamental de redes IP, que actúan como columna vertebral para la comunicación y la conectividad. En el caso específico de proveedores de servicios de Internet (ISP), existen redes IP especializadas de alta capacidad como los Backbone de Internet, por ejemplo, y se componen de elementos como conmutadores, enrutadores y otros elementos que deben manejar grandes volúmenes de tráfico. En este contexto, considero que sería de mucho beneficio para los estudiantes contar con cursos introductorios a las redes IP tempranamente en la carrera, así como una mención o especialización en Sistemas de Comunicación y Redes Avanzadas en los últimos semestres de su formación académica. Este programa podría incluir temas avanzados como seguridad en redes, integración de servicios en la nube, y tecnologías emergentes como **SD-WAN**[60], IPv6, gestión de redes definidas por software, solo por mencionar algunas de las tecnologías que he encontrado en el ámbito laboral.

[60] SD-WAN (Software-Defined Wide Area Network) es una tecnología que optimiza el tráfico en redes de área amplia (WAN) mediante software. Mejora el rendimiento de la red y reduce costos al gestionar múltiples tipos de conexiones de forma eficiente.

Habilidades Socioemocionales y Profesionales: En el entorno laboral contemporáneo, no sólo las habilidades técnicas son valoradas, sino también las competencias socioemocionales y profesionales, comúnmente conocidas como **Habilidades Blandas**. Estas incluyen la comunicación efectiva, la empatía, la resolución de conflictos, el trabajo en equipo, y la gestión del tiempo y del estrés, entre otras. Estas habilidades son esenciales para una colaboración eficaz, la toma de decisiones informadas y la adaptabilidad en un mundo laboral en constante cambio. Sería altamente recomendable que la universidad considere la inclusión de cursos, seminarios o talleres optativos enfocados en el desarrollo de estas habilidades. Estos podrían estructurarse como cursos transversales o integrarse dentro de asignaturas técnicas existentes para fomentar una formación más holística de los futuros profesionales.

Estas sugerencias se presentan con la esperanza de aportar a la evolución continua de una institución que ha demostrado consistentemente su compromiso con la excelencia educativa.

3. ANÁLISIS DE LA ACTIVIDAD

3.1 DESEMPEÑO LABORAL

Al comenzar mi carrera laboral, mis primeros años fueron de constante aprendizaje, principalmente sobre la tecnología de telefonía móvil, que formaba la base del producto principal de Telecel S.A., la compañía que me dio mi primera oportunidad. Paralelamente a mi aprendizaje técnico, pude cultivar habilidades humanas fundamentales, como el trabajo en equipo, la responsabilidad, la integridad y la ética en el entorno laboral.

Con el tiempo, pasé de aprender de ingenieros más experimentados a enseñar a los nuevos ingenieros que se unían a nuestro equipo, y finalmente a liderar un grupo de profesionales, devolviendo de esta manera, la enseñanza que recibí.

Creo que a través de mi trabajo he podido contribuir a la sociedad boliviana, participando en la implementación de tecnologías que hoy disfrutamos como sociedad, como la Telefonía Móvil y el Acceso a Internet. Tuve la fortuna de ser parte de una empresa innovadora, que implementó sus servicios en base a tecnologías de punta, y generando un entorno competitivo, del cual considero que nuestra sociedad se benefició, ya que se logró ofrecer servicios móviles y de acceso a Internet de alta calidad a precios competitivos.

Mi ilusión para el futuro es continuar aprendiendo de las últimas tecnologías en telecomunicaciones y redes, así como también poder ejercer roles de docencia, que me permitan transmitir mis conocimientos a nuevos profesionales.

3.2 FORMACIÓN RECIBIDA EN LA UMSA

En mi opinión, la formación que recibí en la UMSA en la carrera de Ingeniería Electrónica fue de las mejores disponibles en la época en que estudié. Tuve el privilegio de aprender de excelentes catedráticos que se esforzaron al máximo para transmitirnos sus conocimientos. También fui expuesto a un alto nivel de exigencia académica, que cultivó en mí valores como la perseverancia y la responsabilidad. Estos atributos me han sido de gran utilidad en el entorno laboral.

Durante mi tiempo en la universidad, no pude aprovechar adecuadamente las materias de programación, siendo mi aprendizaje parcial en este campo. Aun así y equipado con un conocimiento básico, puedo decir que esta habilidad me resultó extremadamente útil en mis primeros años de trabajo, y basándome en esta experiencia y en la de otros profesionales que conozco, puedo decir que un Ingeniero Electrónico que tiene bien desarrollada esta habilidad tiene una ventaja significativa.

La tecnología está en constante crecimiento y evolución. Las tecnologías existentes no son estáticas, sino que se mejoran y optimizan constantemente. Además, surgen nuevas tecnologías a diario, como la inteligencia artificial, evidenciada por herramientas como ChatGPT. Por lo tanto, creo que las carreras técnicas, como la de Ingeniería Electrónica, deben actualizar constantemente sus contenidos para mantenerse al día. También deben ofrecer a los estudiantes la oportunidad de especializarse en las tecnologías emergentes, que quizás no puedan incluirse adecuadamente en el plan de estudios regular debido a limitaciones de tiempo y volumen.

ANEXOS

ANEXO A: LISTA DE REGISTROS DNS QUE MANEJA EL SISTEMA DNS

A: dirección IPv4.

AAAA: dirección IPv6.

AFSDB: base de datos AFS.

AKAMAICDN: registro de recurso privado de Akamai para el mapeo de dominios de nivel superior.

AKAMAITLC: registro de recurso privado de Akamai para CNAME de nivel superior. Solo puede ser configurado por soporte técnico. Akamai recomienda usar AKAMAICDN en su lugar.

CAA: autorización de la autoridad de certificación.

CERT: registro de certificado que almacena certificados de clave pública.

CDNSKEY: copia del registro DNSKEY del dominio hijo, para ser transferida al dominio padre. Para agregar conjuntos de registros de este tipo, se debe utilizar la API de gestión de zonas de Edge DNS.

CDS: copia secundaria del registro DS, para transferir al padre. Para agregar conjuntos de registros de este tipo, se utiliza la API de administración de zona de Edge DNS.

CNAME: nombre canónico.

DNSKEY: clave DNS. Almacena la clave pública utilizada para las firmas de conjunto de registros (RRset). Requerido para las extensiones de seguridad de DNS (DNSSEC).

DS: firmante de delegación. Puntero de la zona padre al DNSKEY de la zona hija. Requerido para DNSSEC.

HINFO: información del sistema.

HTTPS: protocolo de transferencia de hipertexto seguro.

LOC: ubicación.

MX: intercambio de correo.

NAPTR: puntero de autoridad de nombres.

NS: servidor de nombres.

NSEC: registro de seguridad subsecuente. Disponible solo para zonas secundarias autenticadas. NSEC3 es una opción más segura.

NSEC3: registro de seguridad subsecuente, versión 3. Utilizado para NXDOMAIN autenticado. Requerido para DNSSEC.

NSEC3PARAM: Parámetros NSEC3.

PTR: Puntero.

RP: persona responsable del dominio.

RRSIG: firma de conjunto de registros (RRset). Almacena la firma digital utilizada para autenticar los datos que están en el RRset firmado. Requerido para DNSSEC.

SSHFP: registro de huella digital de Secure Shell. Identifica claves SSH asociadas con un nombre de host.

SOA: registro de inicio de autoridad. Almacena información administrativa sobre una zona, incluidos los datos para controlar las transferencias de zona. Para agregar conjuntos de registros de este tipo, utiliza la API de administración de zona de Edge DNS.

SPF: marco de políticas del remitente.

SRV: localizador de servicios.

SVCB: vinculación de servicios.

TLSA: asociación de certificado de autenticación de seguridad de capa de transporte (TLS). Se utiliza para asociar un certificado o clave pública de servidor TLS con el nombre de dominio donde se encuentra el registro.

TXT: texto.

ZONEMD: Resúmenes de mensaje para zonas DNS. Para agregar conjuntos de registros de este tipo, se utiliza la API de administración de zona de Edge DNS.

BIBLIOGRAFÍA

Dordal, P. L. (2016). **An introduction to computer networks**. Recuperado de http://nmap.cs.loyola.edu/.

Grupo de Sistemas y Comunicaciones. (2016). Arquitectura de Redes de Ordenadores Arquitectura de Internet. Recuperado de https://docplayer.es/18815462-Dns-arquitectura-de-redes-de-ordenadores-arquitectura-de-internet.html.

ATT. (2020). **ESTADO DE SITUACION DEL INTERNET EN BOLIVIA. Primer Semestre de 2020.** Recuperado de https://www.att.gob.bo/sites/default/files/archivos_listados_pdf/2021-07-27/Bolet%C3%ADn%20-%20Estado%20de%20Situaci%C3%B3n%20de%20las%20Telecomun.pdf.

"**COMO FUNCIONA INTERNET**". (s.f.). **AREATECNOLOGIA**. Consultado el 12 de diciembre de 2022, de https://www.areatecnologia.com/informatica/como-funciona-internet.html.

"**PROTOCOLOS DE COMUNICACIÓN EN RED**". (s.f.). MASTER MOVILES UA. Consultado el 18 de diciembre de 2022, de https://mastermoviles.gitbook.io/tecnologias2/protocolos-de-comunicacion-en-red

"**TIPOS DE PROTOCOLO DE TCP/IP**". (s.f.). **BAUL DE LINUX**. Consultado el 3 de enero de 2023, de https://baulderasec.wordpress.com/analisis-software/linux/8-configuracion-basica-de-redes/8-1-las-redes-tcpip/8-1-5-tipos-de-protocolo-de-tcpip/.

"**QUE ES UN DOMINIO DE NIVEL SUPERIOR**". (s.f.). **CLOUDFARE**. Consultado el 10 de enero de 2023, de https://www.cloudflare.com/es-es/learning/dns/top-level-domain/.

"**QUE SON LOS REGISTROS DNS**". (s.f.). **IONOS**. Consultado el 12 de enero de 2023, de https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/registros-dns/.

HANS PAUL ZIZOLD DELGADO
C.I. 3383982
CEL. 77290032
hzizold@hotmail.com

BICENTENARIO DE BOLIVIA

senapi

ESTADO PLURINACIONAL DE BOLIVIA — MINISTERIO DE DESARROLLO PRODUCTIVO Y ECONOMÍA PLURAL

2023-TTES-1244-0-1

DIRECCIÓN DE DERECHO DE AUTOR
Y DERECHOS CONEXOS
RESOLUCIÓN ADMINISTRATIVA NRO. 1-2987/2023
La Paz, 16 de Octubre del 2023

VISTOS:

La solicitud de Inscripción de Derecho de Autor presentada en fecha **9 de Octubre del 2023**, por **HANS PAUL ZIZOLD DELGADO** con **C.I. Nº 3383982 LP**, con número de trámite **DA 1574/2023**, señala la pretensión de inscripción de la Memoria Laboral titulada: **"Implementación y Migración de un Sistema de Nombres de Dominio en el Backbone Internet de Telecel S.A."**, cuyos datos y antecedentes se encuentran adjuntos y expresados en el Formulario de Declaración Jurada.

CONSIDERANDO

Que, en observación al Artículo 4º del Decreto Supremo Nº 27938 modificado parcialmente por el Decreto Supremo Nº 28152 el *"Servicio Nacional de Propiedad Intelectual SENAPI, administra en forma desconcentrada e integral el régimen de la Propiedad Intelectual en todos sus componentes, mediante una estricta observancia de los regímenes legales de la Propiedad Intelectual, de la vigilancia de su cumplimiento y de una efectiva protección de los derechos de exclusiva referidos a la propiedad industrial, al derecho de autor y derechos conexos; constituyéndose en la oficina nacional competente respecto de los tratados internacionales y acuerdos regionales suscritos y adheridos por el país, así como de las normas y regímenes comunes que en materia de Propiedad Intelectual se han adoptado en el marco del proceso andino de integración".*

Que, el Artículo 16º del Decreto Supremo Nº 27938 establece *"Como núcleo técnico y operativo del SENAPI funcionan las Direcciones Técnicas que son las encargadas de la evaluación y procesamiento de las solicitudes de derechos de propiedad intelectual, de conformidad a los distintos regímenes legales aplicables a cada área de gestión".* En ese marco, la Dirección de Derecho de Autor y Derechos Conexos otorga registros con carácter declarativo sobre las obras del ingenio cualquiera que sea el género o forma de expresión, sin importar el mérito literario o artístico a través de la inscripción y la difusión, en cumplimiento a la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina, Ley de Derecho de Autor Nº 1322, Decreto Reglamentario Nº 23907 y demás normativa vigente sobre la materia.

Que, la solicitud presentada cumple con: el Artículo 6º de la Ley Nº 1322 de Derecho de Autor, el Artículo 26º inciso a) del Decreto Supremo Nº 23907 Reglamento de la Ley de Derecho de Autor, y con el Artículo 4º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina.

Que, de conformidad al Artículo 18º de la Ley Nº 1322 de Derecho de Autor en concordancia con el Artículo 18º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina, referentes a la duración de los Derechos Patrimoniales, los mismos establecen que: *"la duración de la protección concedida por la presente ley será para toda la vida del autor y por 50 años después de su muerte, a favor de sus herederos, legatarios y cesionarios".*

V°B° SENAPI

V°B° SENAPI

Que, se deja establecido en conformidad al Artículo 4º de la Ley Nº 1322 de Derecho de Autor, y Artículo 7º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina que: "*...No son objeto de protección las ideas contenidas en las obras literarias, artísticas, o el contenido ideológico o técnico de las obras científicas ni su aprovechamiento industrial o comercial*".

Que, el artículo 4, inciso e) de la ley 2341 de Procedimiento Administrativo, instituye que: "*... en la relación de los particulares con la Administración Pública, se presume el principio de buena fe. La confianza, la cooperación y la lealtad en la actuación de los servidores públicos y de los ciudadanos ...*", por lo que se presume la buena fe de los administrados respecto a las solicitudes de registro y la declaración jurada respecto a la originalidad de la obra.

POR TANTO

El Director de Derecho de Autor y Derechos Conexos sin ingresar en mayores consideraciones de orden legal, en ejercicio de las atribuciones conferidas

RESUELVE:

INSCRIBIR en el Registro de Tesis, Proyectos de Grado, Monografías y Otras Similares de la Dirección de Derecho de Autor y Derechos Conexos, la Memoria Laboral titulada: **"Implementación y Migración de un Sistema de Nombres de Dominio en el Backbone Internet de Telecel S.A."**, a favor del autor y titular: **HANS PAUL ZIZOLD DELGADO** con **C.I. Nº 3383982 LP**, bajo el seudónimo **HANS**, quedando amparado su derecho conforme a Ley, salvando el mejor derecho que terceras personas pudieren demostrar.

Regístrese, Comuníquese y Archívese.

Abg. Carlos Alberto Soruco Arroyo
DIRECTOR DE DERECHO DE AUTOR
Y DERECHOS CONEXOS
SERVICIO NACIONAL DE PROPIEDAD INTELECTUAL

CASA/lsxaq
c.c.Arch.