CAPITULO I

PRESENTACION DEL PROYECTO

I.- Capítulo I: Presentación del proyecto

I.1.- Presentación del Proyecto

Título del Proyecto: Mejorar la eficiencia y seguridad de la fiscalía departamental de Tarija mediante el rediseño y optimización de la infraestructura de red actual, con el uso de tecnologías MikroTik

Nombre del Postulante: David Rivera Ibarbol
Celular: 69317444
Carrera/Unidad: Departamento de Informática y Sistemas
Facultad: Ciencias y Tecnología
Correo Electrónico: riveraibarbol@gmail.com
Institución/Centro Cooperante: Fiscalía Departamental de Tarija
Duración del Proyecto: 8 meses
Área/línea de investigación priorizada: Redes

I.2.- Perfil del Proyecto

I.2.1.- Introducción

La infraestructura de red es un componente esencial para el funcionamiento eficiente de cualquier empresa pública y privada, incluyendo la Fiscalía Departamental de Tarija. Una red corporativa bien diseñada y optimizada puede mejorar significativamente el rendimiento, la escalabilidad y la seguridad de la red, el uso de tecnologías MikroTik ofrece una solución eficiente y rentable para el rediseño y optimización de la infraestructura de red corporativa de la Fiscalía Departamental de Tarija. En este proceso, se pueden aprovechar las características avanzadas de MikroTik, como su capacidad de gestión de ancho de banda, gestión de redes inalámbricas, seguridad y escalabilidad, para diseñar una infraestructura de red altamente eficiente y confiable.

La fiscalía es una institución del estado encargada de cualquier acción penal publica, significa que investiga y persigue cualquier delito, su función principal es llegar a dar justicia y que los culpables paguen sus delitos. Además, se encarga de la protección de los derechos de las víctimas y de garantizar un debido proceso para los acusados.

Se destacará cómo el uso de dispositivos de MikroTik permitirá la implementación de políticas de seguridad adecuadas, la configuración de los protocolos de red apropiados y gestión de la red, lo que mejorará la eficiencia y la eficacia de la red de la Fiscalía Departamental de Tarija.

I.2.2.- Descripción del Proyecto

I.2.2.1.- Antecedentes

I.2.2.2.- Antecedentes de Institución

En lo que respecta a la institución se planteó un rediseño de la red porque la red actual de la Fiscalía sufre de interrupciones frecuentes, lo que afecta la productividad y el acceso a los recursos críticos. Estas interrupciones pueden deberse a problemas de conectividad, configuración deficiente o equipos obsoletos también se ha observado que algunos usuarios de la Fiscalía han recurrido al uso de dispositivos como hubs no recomendados para ampliar el alcance de la red. Estos dispositivos pueden introducir inseguridad y comprometer la calidad de la red, la infraestructura actual no está correctamente ambientada a la red actual.

Estos problemas tienen un impacto significativo en la eficiencia y seguridad de la Fiscalía Departamental de Tarija. La falta de acceso confiable a la red obstaculiza la comunicación y el acceso a información crítica esto provocaría q los usuarios de la institución vean interrumpido su trabajo y esto derivaría en quejas para la institución, cuando hablamos de impacto a la eficiencia se atribuye principalmente de la partición mediante hub o algún parcheo , cuando hablamos de seguridad nos referimos principalmente a quien accede a los equipos ya sea por medio de los fiscales o la área informática de manera inalámbrica compromete el uso del ancho de banda mediante compartir el servicio inalámbrica abiertamente .

la Fiscalía para abordar estos problemas y mejorar la eficiencia y seguridad. Esto se logrará mediante la implementación de tecnologías MikroTik para construir un entorno de red eficiente y seguro que permita a la Fiscalía Departamental de Tarija operar de manera efectiva.

I.2.2.3.- Antecedentes de Trabajos Similares

La infraestructura de red de cualquier organización es crítica para su funcionamiento eficiente, ya que conecta a los usuarios y recursos de la organización y permite la comunicación y el intercambio de información. En particular, para la Fiscalía Departamental de Tarija, una infraestructura de red bien diseñada y optimizada es esencial para garantizar la eficiencia y la eficacia en la gestión de casos y la administración de justicia.

Anteriormente, la infraestructura de red de la Fiscalía Departamental de Tarija podría haber presentado desafíos en términos de rendimiento, escalabilidad y seguridad. Esto podría haber afectado la productividad de la organización y la satisfacción del usuario. Además, con el

aumento de la cantidad de casos y la necesidad de una gestión de datos más segura, la infraestructura de red existente podría no ser suficiente para satisfacer las necesidades actuales y futuras de la organización ya que presenta muchas deficiencias.

la implementación de tecnologías MikroTik puede ofrecer una solución eficiente y rentable para el rediseño y optimización de la infraestructura de red corporativa de la Fiscalía Departamental de Tarija. MikroTik es una solución de red de alta calidad y costo efectivo, que ofrece muchas funciones avanzadas.

En Bolivia los antecedentes principales de otros proyectos que se realizaron con aplicación de las tecnologías Mikrotik son principalmente de los departamentos de La paz, Cochabamba, Santa cruz para tomar en cuenta el uso de las tecnologías se consultó con el proveedor de estas tecnologías lo que se especifico es empresas proveedoras de servicio de internet realizan este uso para sus redes de control interno aplicando tecnologías mikrotik a las empresas me refiero a las de Tigo, Entel, Viva. También tomo en cuenta que se utilizan dispositivos enrutadores de tipo mediano y pequeño en el uso de áreas rurales y empresas pequeñas o grandes ya sean áreas educativas, municipales, hoteles y cibercafes.

Un proyecto con aplicación de tecnologías mikrotik es de la Universidad Mayor de San Andrés este Proyecto es ¨Diseño de un sistema de radio enlace por microondas utilizando Tecnología mikrotik para proporcionar sistema de seguridad y video vigilancia ¨ En este Proyecto se logra apreciar el uso de antenas de la marca mikrotik para la comunicación de 2 puntos uno con el hospital y otro con el pueblo para de allí tener una respuesta más rápida por parte de los efectivos policiales por emergencias en el hospital , en el caso de mi proyecto en la Fiscalía Departamental de Tarija esta posee muchas deficiencias en el servicio de internet y en su control y eso puede ocasionar bastantes aperturas en el caso de robo de la información.

I.2.3.- Justificación del Proyecto

I.2.3.1.- Tecnológica

Será escalable lo que significa que pueden adaptarse fácilmente a las necesidades de una organización en crecimiento. Esto permitirá que la infraestructura de red de la fiscalía sea escalable y pueda manejar un mayor tráfico de red y datos.

Las tecnologías MikroTik ofrecen un alto nivel de seguridad en la infraestructura de red, lo que

garantiza que los datos y la información confidencial estén protegidos contra posibles amenazas de seguridad. Las funciones avanzadas de seguridad incluyen cortafuegos, detección de intrusiones y control de acceso.

I.2.3.2.- Económica

La implementación de tecnologías MikroTik puede reducir los costos de la infraestructura de red a largo plazo. Las soluciones MikroTik son rentables y tienen un bajo costo de adquisición en comparación con otras tecnologías de red.

El rediseño y la optimización de la infraestructura de red permitirá a la fiscalía aumentar su eficiencia y productividad, lo que llevará a un aumento en los ingresos y en la eficiencia general de la organización.

La implementación de tecnologías MikroTik mejorará la seguridad de la infraestructura de red de la fiscalía, lo que reducirá los riesgos asociados a la pérdida de datos y la exposición a amenazas de seguridad. Esto puede prevenir la pérdida de ingresos asociada con posibles ataques.

I.2.3.3.- Social

Una infraestructura de red eficiente y optimizada permitirá a la fiscalía brindar un mejor servicio a la comunidad, ya que se reducirán los tiempos de respuesta y se mejorará la calidad de la atención al cliente.

La optimización de la infraestructura de red de la fiscalía permitirá agilizar los trámites para el ciudadano. Esto facilitará la detección y prevención de delitos y mejorar la capacidad de respuesta en caso de emergencias.

La optimización de la infraestructura de red permitirá a la fiscalía mejorar la eficiencia de sus procesos y reducir los costos asociados, lo que permitirá destinar más recursos a la mejora en otro aspecto en invertir más en otros aspectos que benefician al ciudadano.

I.2.3.4.- Desarrollo sostenible

La Fiscalía departamental de Tarija cuenta con el recurso tecnológico y humano para continuar sin inconvenientes el desarrollo del proyecto y su administración futura.

I.2.3.5.- Medio Ambiental

La optimización de la infraestructura de red permitirá a la fiscalía reducir los desplazamientos innecesarios de los empleados al lugar de trabajo, lo que reducirá la cantidad de emisiones de gases de efecto invernadero y la contaminación generada por los vehículos.

I.2.4.- Planteamiento del problema

En la fiscalía departamental de Tarija, la infraestructura de red corporativa actual presenta problemas de rendimiento y escalabilidad que afectan la eficiencia y la productividad de los usuarios. Estos problemas se deben a la falta de una arquitectura de red adecuada y en no realizar un rediseño en la red anteriormente y adaptarla para su funcionamiento sin tomar en cuenta las normas de cableado estructurado, otros problemas se presentan en el control del uso de aplicaciones de streming como también problemas en la asignación de más equipos con la red actual, los equipos actuales de la institución se encuentran sin protección expuestos al aire libre.

I.2.5.- Análisis del cuadro de involucrados

Grupos	Intereses	Problemas	Recursos y mandatos
Médicos forenses	Examinar y evaluar las pruebas médicas para determinar la causa y el momento de la muerte, así como cualquier otra información relevante para la investigación.	- Acceso limitado a registros médicos debido a problemas en la estabilidad de la red	Acceso seguro y controlado a registros médicos electrónicos y otros datos relevantes en la red. Cumplimiento de las regulaciones de privacidad y seguridad de datos.
Administrativos	Mantener y gestionar la documentación del caso, incluyendo informes, registros y archivos.	- Perdida de Información por equipos deteriorados -acceso interrumpido a la red	Almacenamiento y copias de seguridad seguras y fiables de archivos importantes. Cumplimiento de las regulaciones de privacidad y seguridad de datos.

Conciliadores	Ayudar a las partes a llegar a un acuerdo en caso de que haya discrepancias o conflictos.	-Falta de conexión estable a la red - perdida de datos de implicados en casos - Falla para comunicarse con implicados	Plataformas de comunicación seguras y confiables para facilitar la comunicación entre las partes involucradas. Cumplimiento de las regulaciones de privacidad y seguridad de datos.
Cuarto Policial	Análisis de pruebas y seguridad en la institución	- fallas en la red al momento de visualizar sus documentos	Herramientas y técnicas de análisis forense digital para recuperar y preservar la evidencia digital de manera segura y fiable. Cumplimiento de las regulaciones de privacidad y seguridad de datos.
funcionarios Fiscales	Presentar y analizar el caso ante el tribunal y acusar al acusado en nombre del Estado.	- fallas de red en análisis de casos - Perdida de conexión	Acceso seguro y controlado a evidencia y documentos relevantes en la red. Cumplimiento de las regulaciones de privacidad y seguridad de datos.
funcionarios Informáticos	Administrar todo el uso de tecnología en la institución y actualizar y mantener en mejores condiciones	- Fallas en la conexión de red de toda la institución - Tomas de cable vacías sin funcionamiento - Perdida de control de identificación de equipos - Perdida de identificación de cableado estructurado - Cableado Irrumpe el trabajo del personal de la institución -Falta de control en donde navegan los funcionarios	Herramientas y técnicas para el análisis y recuperación de datos de manera segura y confiable. Cumplimiento de las regulaciones de privacidad y seguridad de datos.
Funcionario de atención al cliente	Proporcionar información y asistencia a las partes interesadas en el proceso judicial, como los testigos y las víctimas, y responder a preguntas y preocupaciones relacionadas con el	- Perdida de red en Horario de atención al cliente - problema con el uso de etiquetas de atención	Plataformas de comunicación seguras y confiables para facilit

	caso.		

I.2.6.- Árbol de Problemas

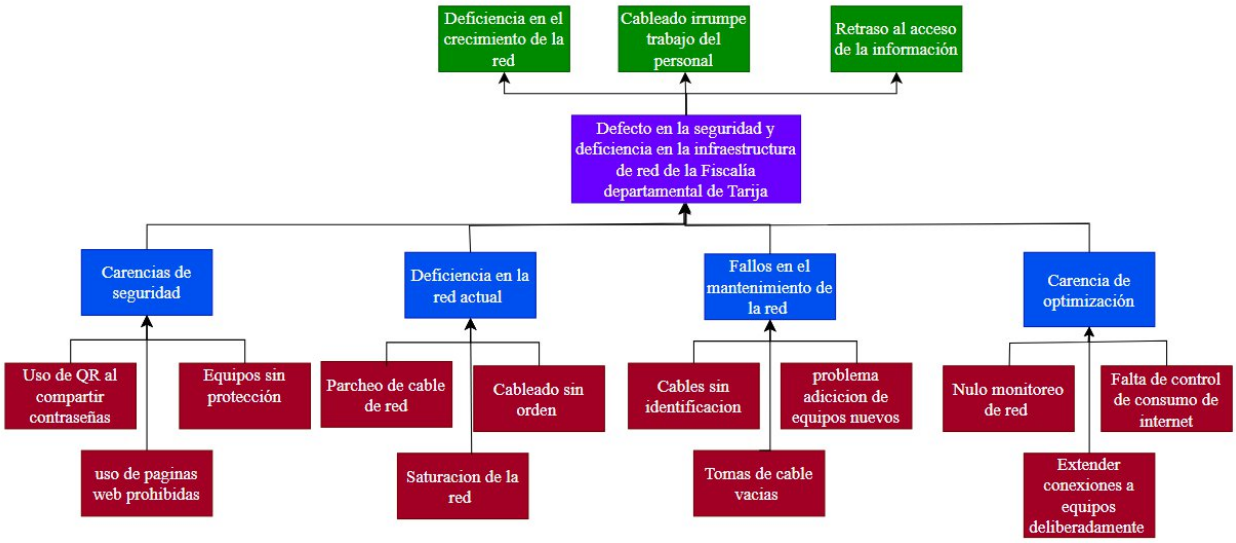


Figura 1. Árbol de Problemas

I.2.7.-Árbol de Objetivos

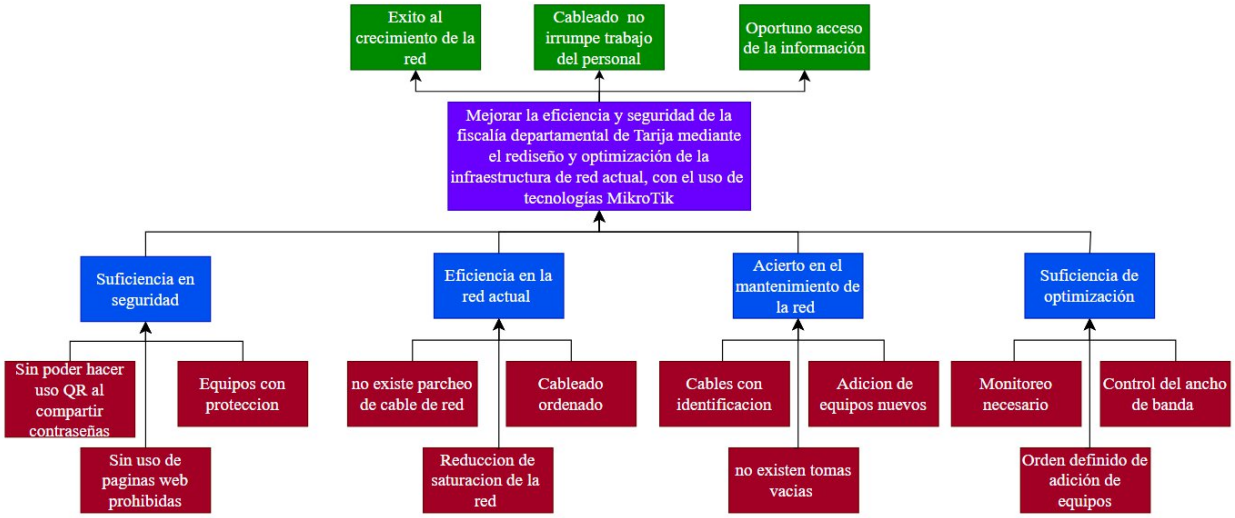


Figura 2. Árbol de Objetivos

I.2.8.- Objetivos

I.2.8.1.- Objetivo General

- Mejorar la eficiencia y seguridad de la fiscalía departamental de Tarija mediante el rediseño y optimización de la infraestructura de red actual, con el uso de tecnologías MikroTik

I.2.8.2.- Objetivos Específicos

- Implementación del rediseño de red
- Capacitación de los encargados de la institución

I.2.9.-Alcance

El alcance de este proyecto se plantea la implementación de dispositivos MikroTik como una solución integral para abordar desafíos clave en el ámbito de las redes de comunicación. El objetivo fundamental de este proyecto es optimizar la infraestructura de red en la Fiscalía Departamental de Tarija, se busca garantizar un acceso ininterrumpido a la red, eliminando problemas de conexión y pérdida de señal que han afectado la operatividad de la Fiscalía. establecer políticas de firewall que bloqueen el acceso a redes sociales y puertos no esenciales, fortaleciendo la seguridad de la red y reforzar las redes inalámbricas con el uso de hotspot para un mejor control en los usuarios la implementación redes segmentadas para diferentes departamentos y usuarios, lo que permitirá un control y gestión de manera más eficaz.

I.2.10.- Limitaciones

La realización del presente proyecto, se enfrenta a las siguientes limitaciones:

- No contar con un cuarto de Telecomunicaciones
- No contar con equipos nuevos y reutilizar los equipos de la anterior red en lo que se vea necesario (Dispositivos finales)
- La poca disponibilidad de tiempo del personal que labora en las diferentes dependencias, lo que dificulto de alguna manera la recolección de la información necesaria para la realización del proyecto.
- Inspecciones por parte de superiores en el momento de la ejecución de proyecto lo cual tuvo que parar el avance del proyecto
- Los usuarios fiscales nos ofrecen acceso limitado para realizar el trabajo y realiza reclamos por el corte de los servicios en la configuración de los equipos nuevos

I.2.11.- Matriz del marco Lógico (MML)

Resumen Narrativo del Proyecto	**Indicadores**	**Medios de Verificación**	**Supuestos**
Fin Mejora en la calidad y eficiencia de los servicios que proporciona la Fiscalía departamental de Tarija a los ciudadanos	A un año de finalizado el proyecto, la fiscalía departamental de Tarija se contará con menos reclamos tecnológicos por parte de los empleados en un 60%	Informe e documentación por parte del administrador en la fiscalía departamental de Tarija sobre los reclamos en la presente gestión	Se mantiene la misma infraestructura de red y edificio de la fiscalía departamental de Tarija
Propósito Mejorar la eficiencia y seguridad de la fiscalía departamental de Tarija mediante el rediseño y optimización de la infraestructura de red actual, con el uso de tecnologías MikroTik	Una vez finalizado el proyecto se cumplirá con al menos el 80% de los servicios propuestos Calculados por la siguiente formula: $\frac{\text{Cantidad de servicios Disponibles}}{\text{Cantidad de servicios Requeridos}} \times 100$ 1 conexión a la red de internet 2 optimización de la red de la fiscalía 3 conexión con otras áreas de la institución 4 seguridad y disponibilidad con sus datos en el sistema	Informe e documentación por parte del administrador en la fiscalía departamental de Tarija avalando los servicios implementados	Los empleados de la fiscalía departamental de Tarija cuentan con tiempo para proporcionar la información de manera oportuna
Componentes **1.** Implementación del Rediseño de red	1. Al Finalizar el proyecto se cumplen con las normas de cableado estructurado TIA/EIA-568 y TIA/EIA-569 2.Al finalizar el proyecto se entregará el	1. Carta de Aprobación del proyecto por parte del docente de Taller 3.	• Disponibilidad del equipo por parte del empleado realizando sus labores en la institución • Se cuenta con los equipos de manera

<table>
<tr>
<td>2. Capacitación de los encargados de informática de la administración de la institución</td>
<td>manual a los 2 encargados administrativos de informática en la fiscalía</td>
<td>2. Carta de administración de la fiscalía departamental de Tarija con aprobación de asistencia de capacitación de configuración de la red
3. Fotografía, imagen de capacitación</td>
<td>oportuna

• Se cuenta con los mismos encargados en la fiscalía departamental al finalizar el proyecto</td>
</tr>
<tr>
<td>Actividades
1. Implementación del Rediseño de red
1.1. Analizar Requerimientos

1.2. Desarrollar Diseño Lógico

1.3. Desarrollar Diseño Físico

1.4. Probar, optimizar y documentar diseño

1.5. Implementar</td>
<td>Resumen presupuesto

<table>
<tr><th>Componentes</th><th>Ap</th></tr>
<tr><td>Análisis de la infraestructura</td><td></td></tr>
<tr><td>Materiales electrónicos</td><td></td></tr>
<tr><td>E. de computación</td><td></td></tr>
<tr><td>E. de comunicación</td><td></td></tr>
<tr><td>Capacitación de Configuración de la red</td><td></td></tr>
<tr><td>Total</td><td></td></tr>
</table>
</td>
<td>Comprobantes de ingreso y egreso</td>
<td>La Fiscalía departamental de Tarija abona el dinero para la realización del proyecto de manera oportuna con los plazos previstos</td>
</tr>
</table>

y probar la red 1.6. Monitorear y Optimizar la Red **2. Capacitación del encargado de informática de la administración de la institución** 2.1. Análisis 2.2. Diseño 2.3. Desarrolló 2.4. Implementación 2.5. Evaluación			

I.2.12.- Metodología de desarrollo del proyecto

La metodología Top-Down se puede aplicar para el diseño de redes y consta de varias fases que permiten analizar los requerimientos y objetivos de negocio para desarrollar un diseño adecuado. Algunas de las fases de la metodología Top-Down para redes incluyen el análisis de requerimientos, el desarrollo del diseño lógico y la selección de tecnologías y dispositivos. Esta metodología se enfoca en partir de una visión general de la red y desglosarla en planes específicos para lograr los objetivos establecidos previamente. La metodología Top-Down puede ser útil para diseñar una red eficiente y adaptada a las necesidades del negocio o empresa.

La metodología está compuesta por estas fases:

Fase 1: Analizar Requerimientos

- Analizar metas del negocio
- Analizar metas técnicas
- Analizar red existente
- Analizar tráfico existente

Fase 2: Desarrollar Diseño Lógico

- Diseñar topología de red
- Diseñar modelos de direccionamiento y hostnames
- Seleccionar protocolos para Switching y Routing
- Desarrollar estrategias de seguridad
- Desarrollar estrategias de administración de red

Fase 3: Desarrollar Diseño Físico

- Seleccionar tecnologías y dispositivos para redes empresariales

Fase 4: Probar, optimizar y documentar diseño

- Probar el diseño de red
- Optimizar el diseño de red
- Documentar el diseño

Fase 5: Implementar y probar la red

- Realizar cronograma de implementación
- Implementación del diseño de red (final)
- Realizar pila de pruebas

Fase 6: Monitorear y Optimizar la Red

- Operación de la red en producción
- Monitoreo de la red
- Optimización de la red

la metodología ADDIE es un enfoque sistemático utilizado en el diseño instruccional para desarrollar programas efectivos de capacitación y aprendizaje en el proyecto como medio para elaborar la capacitación se tomarán en cuenta los puntos los que comprenden esta metodología los cuales son:

Fase de Análisis: En esta fase, se desarrolla una introducción al proyecto para ver para quien está dirigida la capacitación.

Fase de Diseño: En esta fase, se dispone de los métodos para el desarrollo de la capacitación ya sean medios o materiales necesarios para desarrollar la capacitación de la mejor manera.

Fase de Desarrollo: En esta fase, con los materiales dispuestos anteriormente se desarrolla o se gestiona el uso de los medios para la capacitación.

Fase de Implementación: En esta fase, se desarrolla un plan de contenidos de la capacitación para así brindarla a los capacitados.

Fase de Evaluación: En esta fase, se verifica según lo aprendido que tan beneficioso es el plan implementado con una comprobación de los resultados.

I.2.13.- Resultados esperados

Una vez implementado las nuevas tecnologías MikroTik se espera obtener:

- Implementación del rediseño de la red.
- Capacitación del encargado de informática de la fiscalía departamental de Tarija presencial o virtual.

MikroTik ofrecen opciones de seguridad avanzadas, por lo que se espera que la red de la fiscalía sea más segura y menos vulnerable a posibles ataques cibernéticos.

I.2.14.- Beneficiarios

I.2.14.1.- Beneficiarios Directos

los empleados y colaboradores de la Fiscalía Departamental de Tarija, quienes utilizan la red de la organización para llevar a cabo su trabajo diario. Al optimizar y mejorar el rendimiento de la infraestructura de red, estos empleados podrían beneficiarse de una mayor eficiencia y productividad en el trabajo, lo que a su vez podría mejorar la calidad de los servicios que ofrece la Fiscalía a la comunidad.

I.2.14.2.- Beneficiarios indirectos

Al mejorar la infraestructura de red de la Fiscalía Departamental de Tarija, es posible que se mejore el procesamiento y la administración de casos judiciales y legales, lo que podría tener un impacto significativo en la eficiencia y la acción del Sistema de justicia de Tarija con los diferentes casos tratados en el lugar.

I.2.15.- Cronograma de Actividades

N.º	Actividad	N.º días	Fecha inicio	Fecha Finalización	M1	M2	M3	M4	M5	M6	M7	M8
1	Implementación del rediseño de red.	**120**	**18/04/2022**	**07/10/2022**	**X**	**X**	**X**	**X**	**X**			
1.1	Analizar Requerimientos	**15**	**18/04/2022**	**06/05/2022**	**X**							
1.2	Desarrollar Diseño Lógico	**20**	**09/05/2022**	**03/06/2022**		**X**	**X**					
1.3	Desarrollar Diseño Físico	**35**	**06/06/2022**	**22/07/2022**			**X**					
1.4	Probar, optimizar y documentar diseño	**25**	**25/07/2022**	**26/08/2022**			**X**	**X**				
1.5	Implementar y probar la red	**25**	**05/09/2022**	**07/10/2022**				**X**	**X**			
1.6	Monitorear y Optimizar la Red							**X**	**X**			
2	Capacitación de los encargados de informática de la administración de la institución	**22**	**10/10/2022**	**15/11/2022**					**X**	**X**	**X**	**X**
2.1	Análisis	**2**	**10/10/2022**	**11/10/2022**					**X**	**X**	**X**	
2.2	Diseño	**5**	**11/10/2022**									

2.3	Desarrollo	**5**										
2.4	Implementación	**5**										
2.5	Evaluación	**5**	**07/11/2022**	**15/11/2022**								**X**

Tabla 1. Cronograma de Actividades

I.2.16.- Presupuesto general

PARTIDA	**FINALIDAD**				
25200	**Análisis de la infraestructura**				
#	**Recurso**	**Aporte UAJMS**	**Aporte Institucional**	**Bimestral**	**TOTAL (Bs)**
1	**Estipendio por el trabajo**	**0.00**	**2500.00**	**4**	**20000.00**
Sub total componente					**20000.00**

PARTIDA	**FINALIDAD**				
39700	**Útiles y Materiales Eléctricos.**				
#	**Recurso**	**Aporte UAJMS**	**Aporte Institucional**	**Cantidad**	**TOTAL (Bs)**
1	**Switch (48 puertos)**	**0.00**	**1240**	**2**	**2480**
2	**Switch (24 puertos)**	**0.00**	**680**	**3**	**2040**

3	**Adaptadores de wifi (mikrotik)**	**0.00**	**525**	**3**	**1575**
4	**Conectadores RJ-**	**0.00**	**2,50**	**75**	**187,50**
5	**Rack 22U**	**0.00**	**3220**	**1**	**3220**
6	**Rack 10U**	**0.00**	**1450**	**4**	**5800**
7	**Patch Pannel de 48 puertos**	**0.00**	**551**	**2**	**1102**
8	**Patch Pannel de 24 puertos**	**0.00**	**350**	**3**	**1050**
9	**Canaletas de 40x20**	**0.00**	**8,50**	**50**	**425**
10	**Canaletas de 70x40**	**0.00**	**66**	**8**	**528**
11	**Cable Caja de 305 metros**	**0.00**	**199**	**8**	**1592**
Sub total componente					**19999,50**

PARTIDA	**FINALIDAD**				
43120	**Equipos de Computación**				
#	**Recurso**	**Aporte UAJMS**	**Aporte Institucional**	**Cantidad**	**TOTAL (Bs)**
1	**Computadoras de Escritorio**	**0.00**	**1400**	**20**	**28000**
2	**impresoras**	**0.00**	**800**	**5**	**4000**

Sub total componente	**32000**

PARTIDA	**FINALIDAD**				
43500	**Servicios de Comunicación**				
#	**Recurso**	**Aporte UAJMS**	**Aporte Institucional**	**Anual**	**TOTAL (Bs)**
1	**Servicio de internet completo**	**0.00**	**2750**	**1**	**22000**
Sub total componente					**22000**

PRESUPUESTO TOTAL en Bs.	**94.999.50**

Tabla 2. Presupuesto de Proyecto

Condiciones

- El presupuesto tiene una duración de un año
- Sujeto a variación de precios por aumento en costos nivel nacional e internacional
- Tomando en cuenta el reutilizar los equipos de la anterior red en caso que sea necesario
- Equipos sujetos a Cambio en caso de fallo ya que son pedidos que llegan de otro departamento sede
- Entrega de equipos en 120 días

CAPITULO II COMPONENTES

II.- Capitulo II: Componentes

II.1.- Marco Teórico

II.1.1.- Introducción

Las agencias gubernamentales y las organizaciones en general dependen de una infraestructura de red confiable y eficiente para realizar sus operaciones diarias. En el caso de la Fiscalía de Tarija, se requiere implementar una nueva red informática para mejorar la eficiencia y seguridad de sus servicios.

Las nuevas redes informáticas ofrecen muchos beneficios que pueden impactar positivamente en la eficiencia y productividad de la fiscalía departamental de Tarija. En primer lugar, una infraestructura de red bien diseñada y optimizada proporciona una comunicación rápida y flexible entre los diferentes departamentos y funcionarios, lo que facilita la colaboración y agiliza los procesos internos. Esto aumenta considerablemente la eficiencia del trabajo y el tiempo de respuesta.

La nueva red informática también brindará mayor seguridad a la fiscalía y los ciudadanos que se benefician del servicio que ofrece. A medida que aumenta el riesgo de amenazas cibernéticas, las soluciones de seguridad avanzadas para proteger los datos confidenciales y garantizar la integridad de la información son esenciales. Una infraestructura de red mejorada respaldada por tecnologías de seguridad como las proporcionadas por MikroTik permite políticas de seguridad sólidas, detección y prevención de intrusiones y controles de acceso más estrictos.

La nueva red informática de la fiscalía departamental de Tarija es fundamental para mejorar la eficiencia operativa, mejorar la seguridad de los datos, optimizar el rendimiento de las aplicaciones y servicios y brindar una mejor experiencia a la ciudadanía. Esta moderna infraestructura permitirá que a la fiscalía se adapte a los avances tecnológicos modernos y permitir crecimiento óptimo de la infraestructura.

II.1.2.- Modelos de protocolos y de referencias

En lo que se refiere a la interconexión de los equipos los principios para la comunicación de redes son necesarios para garantizar una transmisión de datos eficiente y fiable en un entorno de red. Los dos principios fundamentales son el modelo de capas OSI y TCP/IP.

II.1.3.- Modelo TCP/IP

El modelo TCP/IP es un modelo teórico diseñado para que toda la comunicación entre computadoras y dispositivos se realice en el "mismo idioma" para que todos los dispositivos involucrados se entiendan entre sí y entreguen los mensajes correctamente.

TCP/IP (Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos ampliamente utilizado para la comunicación en redes. TCP/IP se basa en el modelo de capas TCP/IP, que se asemeja al modelo de capas OSI, pero con una estructura más simplificada. El modelo TCP/IP consta de cuatro capas:

Capa de red: Es responsable del direccionamiento y enrutamiento de los paquetes de datos en la red. El protocolo principal utilizado en esta capa es el Internet Protocol (IP).

Capa de transporte: Proporciona servicios de transporte confiable de extremo a extremo. El protocolo más utilizado en esta capa es el Transmission Control Protocol (TCP), que garantiza la entrega y el orden de los datos.

Capa de aplicación: Contiene los protocolos utilizados por las aplicaciones para comunicarse a través de la red, como el Hypertext Transfer Protocol (HTTP) para la navegación web, el Simple Mail Transfer Protocol (SMTP) para el correo electrónico, el File Transfer Protocol (FTP) para la transferencia de archivos, entre otros.

Capa de enlace de datos: Se ocupa de la transmisión de datos a nivel de bits a través del medio físico de la red. Incluye los protocolos Ethernet, Wi-Fi y otros protocolos de acceso a medios.

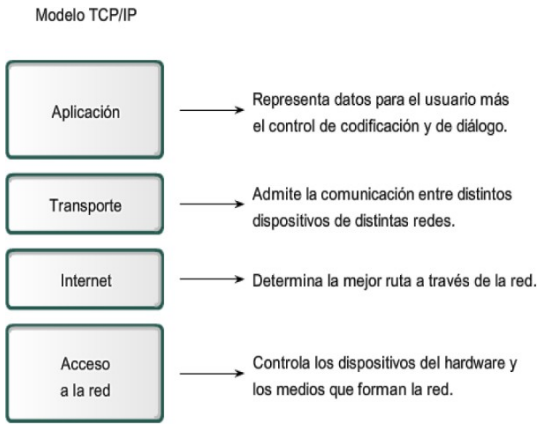


Figura 3. Modelo TCP/IP

II.1.3.1.- Modelo OSI

El modelo de capas OSI (Open Systems Interconnection) es un marco conceptual desarrollado por la Organización Internacional de Normalización (ISO) para definir una arquitectura de red de siete capas. Cada capa tiene una función específica y se comunica con las capas adyacentes para brindar servicios a las capas superiores o inferiores. El modelo OSI permite la interoperabilidad entre diferentes dispositivos y sistemas de red.

Capa física: Se ocupa de la transmisión y recepción de datos a nivel de bits a través de medios físicos.

Capa de enlace de datos: Proporciona la transferencia de datos confiable entre nodos adyacentes en una red.

Capa de red: Se encarga del enrutamiento de paquetes y la determinación de la mejor ruta para la transmisión de datos.

Capa de transporte: Ofrece servicios de segmentación, control de flujo y detección de errores para la entrega confiable de datos extremo a extremo.

Capa de sesión: Establece, mantiene y finaliza las conexiones entre aplicaciones en diferentes nodos.

Capa de presentación: Se encarga de la representación y el formato de los datos para que sean

comprensibles por las aplicaciones.

Capa de aplicación: Proporciona servicios de red a las aplicaciones y permite la interacción entre el usuario y la red.

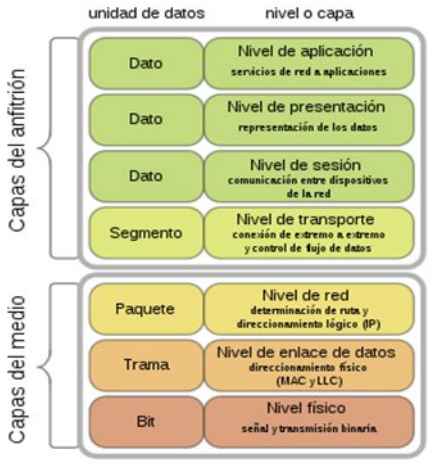


Figura 4. Modelo OSI

II.1.3.2.-Diferencias entre modelo OSI y modelo TCP/IP

La capa de aplicación del modelo TCP/IP representa a las capas 5, 6, 7 combinadas del modelo OSI, el modelo TCP/IP no tiene una capa de sesión. La capa de transporte de TCP/IP abarca las responsabilidades de la capa de transporte OSI y algunas de las responsabilidades de la capa de sesión OSI. La capa de acceso a la red del modelo TCP/IP abarca el enlace de datos y las capas físicas del modelo OSI.

El modelo OSI define un marco conceptual que divide el proceso de comunicación de la red en siete capas, cada una con funciones y responsabilidades específicas. El modelo de protocolos OSI permite que diferentes componentes de una red se comuniquen entre sí de forma estandarizada. El modelo OSI ayuda a diseñar, desarrollar y resolver problemas de redes al proporcionar una estructura modular que facilita la implementación de nuevas tecnologías y la interoperabilidad entre sistemas de diferentes proveedores.

Por otro lado, TCP/IP es un conjunto de protocolos más utilizado en la actualidad para la

comunicación en Internet y en muchas redes locales. TCP/IP se basa en un modelo de cuatro capas, que se alinea de manera general con el modelo OSI. TCP/IP proporciona un conjunto de protocolos para la transmisión y el enrutamiento de datos en una red. El protocolo IP, que forma parte de TCP/IP, es responsable del direccionamiento y enrutamiento de paquetes de datos en la red, permitiendo que los datos se transmitan entre diferentes dispositivos y redes. TCP, otro protocolo clave en TCP/IP, garantiza una entrega confiable de datos mediante la segmentación, el control de flujo y la detección de errores.

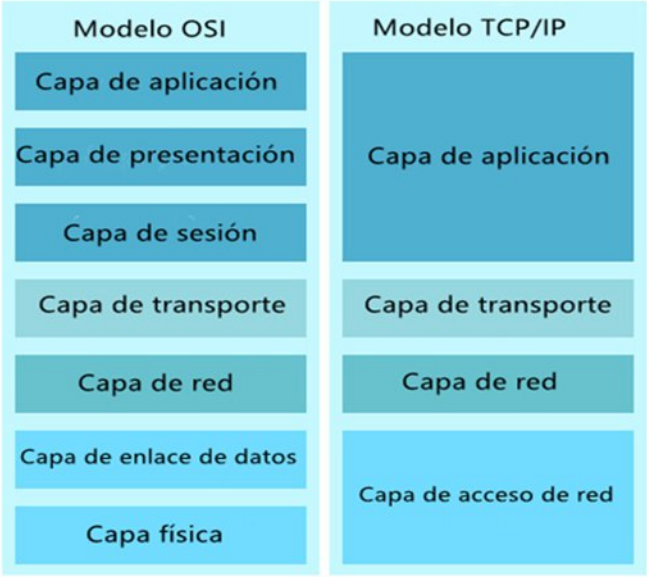


Figura 5. Diferencia de Modelo TCP/IP y OSI

II.1.4.- Red LAN (Red de Área Local)

Una red LAN (Local Área Network) es una red de área local que cubre un área geográfica relativamente pequeña, como una oficina, un edificio, una escuela o una casa. Estas redes están diseñadas para permitir la comunicación y el intercambio de datos entre dispositivos ubicados dentro de un área limitada. Algunas características de las redes LAN incluyen:

Cobertura limitada: Una red LAN está diseñada para cubrir un área geográfica relativamente

pequeña, como un edificio o una instalación.

Velocidad alta: Las redes LAN suelen ofrecer velocidades de transmisión de datos más altas debido a la proximidad física de los dispositivos conectados.

Propiedad privada: Por lo general, una LAN es propiedad y está controlada por una organización o entidad individual.

II.1.5.-Topología de una red

La Topología de red se conoce como la forma de interconectar y organizar físicamente y lógicamente los nodos y enlaces de comunicación que comprenden a la red. Esta organización determinara como se conectarán los diferentes dispositivos y como se comunican ellos entre sí.

Existen 5 topologías más utilizadas:

- **Topología de bus:** En esta topología, todos los dispositivos están conectados a un único medio de transmisión, conocido como "bus". Los datos se transmiten a lo largo del bus y son recibidos por todos los dispositivos conectados. Cualquier dispositivo puede enviar o recibir datos, pero solo el dispositivo destinatario procesa la información.
- **Topología de estrella:** En esta topología, todos los dispositivos están conectados a un nodo central, como un switch o un concentrador. Cada dispositivo tiene una conexión dedicada con el nodo central. Cuando un dispositivo envía datos, estos se transmiten directamente al nodo central, que luego los envía al dispositivo de destino. La falla de un dispositivo no afecta la comunicación de los demás.
- **Topología de anillo:** En esta topología, los dispositivos están conectados en forma de anillo cerrado, donde cada dispositivo está conectado directamente a los dos dispositivos adyacentes. Los datos se transmiten en una dirección alrededor del anillo. Cada dispositivo recibe los datos y los pasa al siguiente dispositivo en el anillo hasta que llegan al destino. La falla de un dispositivo puede interrumpir la comunicación en el anillo.
- **Topología de malla:** En esta topología, todos los dispositivos están conectados directamente entre sí, creando múltiples rutas de comunicación. Cada dispositivo tiene una conexión dedicada con todos los demás dispositivos. Esto proporciona redundancia y mayor confiabilidad, ya que, si una ruta falla, los datos pueden seguir una ruta alternativa.

- **Topología en árbol:** Esta topología utiliza una estructura jerárquica en forma de árbol, donde los dispositivos están conectados en niveles, comenzando desde un nodo raíz hasta los nodos hoja. El nodo raíz es el punto central de la red y los nodos hoja son los dispositivos finales. La comunicación se realiza a través del nodo raíz, y los datos se transmiten hacia abajo a través de los niveles del árbol.

II.1.6.- Cableado Estructurado (Medios Físicos de Transmisión)

El cableado estructurado es un sistema de cableado diseñado para proporcionar una infraestructura de telecomunicaciones que pueda soportar múltiples aplicaciones, como voz, datos y video, a través de una red de cableado integrada. El objetivo del cableado estructurado es proporcionar una solución de cableado flexible y escalable que pueda adaptarse a las necesidades cambiantes de la organización. El cableado estructurado se basa en estándares internacionales, como ANSI/TIA/EIA-568, que establecen las especificaciones técnicas para el diseño e implementación de sistemas de cableado estructurado. El cableado estructurado puede incluir elementos como cables de cobre y fibra óptica, conectores, paneles de parcheo, racks y gabinetes, y dispositivos de terminación.

II.1.7.- Cableado Estructurado

II.1.7.1.-Introducción

El cableado estructurado es un conjunto de cables, conectores, canalizaciones y dispositivos que componen la infraestructura de telecomunicaciones interior de un edificio o recinto. Que tiene como función transportar señales desde unos dispositivos (emisores) a otros (receptores) con el objetivo de crear la red de área local del mismo.

II.1.7.2.-Normas y Organismos:

Organismos

- ANSI: (American National Standards Institute)
- EIA: (Electronics Industry Association).
- TIA: (Telecommunications Industry Association)
- ISO: (International Standards Organization)

- IEEE: (Institute of Electrical and Electronics Engineers)

Normas

- ANSI/TIA/EIA-568-B: Cableado de Telecomunicaciones en Edificios Comerciales es un estándar técnico importante para el diseño e implementación de sistemas de cableado estructurado de cobre en redes informáticas

  - TIA/EIA 568-B1 Requerimientos generales
  - TIA/EIA 568-B2 Componentes de cableado mediante par trenzado balanceado

- ANSI/TIA/EIA-569-A: Normas de Recorridos y Espacios de Telecomunicaciones en
- Edificios Comerciales Este estándar establece los requisitos para la ubicación de los equipos de telecomunicaciones, las rutas de cableado, los espacios de entrada de servicios y las áreas de trabajo de telecomunicaciones.
- ANSI/TIA/EIA-569-A: Normas de Recorridos y Espacios de Telecomunicaciones en edificios Comerciales que la infraestructura de telecomunicaciones esté diseñada, instalada y mantenida adecuadamente para satisfacer las necesidades de los ocupantes del edificio.
- Cubre una amplia gama de temas, incluido el diseño y la construcción de caminos y espacios, la colocación de equipos de telecomunicaciones y la separación de cables de telecomunicaciones y de energía
- ANSI/TIA/EIA-570-A: Normas de Infraestructura Residencial de Telecomunicaciones establece los requisitos para la protección contra incendios, la seguridad y la ventilación de los equipos de telecomunicaciones.
- ANSI/TIA/EIA-606-A: Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales establece los requisitos para la identificación y etiquetado de los componentes de la infraestructura de telecomunicaciones, como los cables, los paneles de parcheo y los equipos de red.
- ANSI/TIA/EIA-607: Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales establece los requisitos para la protección contra descargas eléctricas y otros eventos adversos, como la interferencia electromagnética.

II.1.7.3.-Cableado Horizontal

El cableado horizontal en redes informáticas es la porción de cableado que conecta los paneles de parcheo en el cuarto de telecomunicaciones (gabinete) con los tomacorrientes de telecomunicaciones en las áreas de trabajo. Este tipo de cableado se utiliza en sistemas de cableado estructurado y es esencial para la transmisión de datos en una red informática. El cableado horizontal se debe diseñar e instalar de acuerdo con los estándares técnicos, como el estándar ANSI/TIA/EIA-568-B, para garantizar un rendimiento óptimo de la red.

El cableado horizontal abarca:

- Transmisión de datos: el cableado horizontal es esencial para la transmisión de datos en una red informática, ya que es el medio por el cual los datos se transmiten desde el cuarto de telecomunicaciones hasta las áreas de trabajo.
- Conexión de dispositivos: el cableado horizontal permite la conexión de dispositivos de finales y de transmisión, como computadoras, impresoras, scanners y otros en la red informática.
- Cumplimiento de estándares: el cableado horizontal debe cumplir con los estándares técnicos, como el estándar ANSI/TIA/EIA-568-B, para garantizar un rendimiento óptimo de la red.

II.1.7.4.-Cableado Vertical o Backbone

El cableado vertical o Backbone en redes informáticas es la porción de cableado que conecta los equipos de telecomunicaciones en el cuarto(gabinete) de telecomunicaciones con los paneles de parcheo en los diferentes pisos de un edificio. Este tipo de cableado se utiliza en sistemas de cableado estructurado y es esencial para la transmisión de datos en una red informática. El cableado vertical se debe diseñar e instalar de acuerdo con los estándares técnicos, como el estándar ANSI/TIA/EIA-569-A, para garantizar un rendimiento óptimo de la red. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos.

II.1.7.4.1.-Cuarto de Entrada de Servicios

En cables, accesorios de conexión, dispositivos de protección, y demás equipos es necesario para conectar el edificio a servicios externos. Puede contener el punto de demarcación.

Ofrecen protección eléctrica establecida por códigos eléctricos aplicables. Deben ser diseñadas

de acuerdo a la norma EIA/TIA-569-A. Los requerimientos de instalación son:

- Precauciones en el manejo del cable UTP
- Evitar tensiones en el cable
- Los cables no deben en distribuirse en grupos muy apretados
- Utilizar rutas de cable y accesorios apropiados 100 ohmios UTP y STP

II.1.7.4.2.-Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones es un espacio físico designado para albergar y organizar los equipos, cables y dispositivos necesarios para la infraestructura de la red. Es un espacio dedicado en un edificio donde se centralizan las conexiones y equipos de telecomunicaciones. Desde este lugar se distribuyen las conexiones hacia las áreas internas del edificio, permitiendo una gestión eficiente de las redes de comunicación y asegurando la conectividad necesaria para el funcionamiento de los servicios de telecomunicaciones.

- Alojamiento de equipos: El cuarto de telecomunicaciones es el lugar donde se instalan los dispositivos y equipos de red, como routers, switches, servidores, firewalls, unidades de almacenamiento, entre otros. Estos equipos son fundamentales para el enrutamiento, control y administración de la red.
- Conexión y terminación de cables: En el cuarto de telecomunicaciones se concentran los cables de red que conectan diferentes áreas de un edificio o instalación. Aquí se realiza la terminación de los cables, es decir, se conectan los extremos de los cables a los paneles de conexión o a los dispositivos activos de red.
- Administración y organización: El cuarto de telecomunicaciones proporciona un espacio organizado para la gestión y administración de la infraestructura de red. Los cables se enrutan y etiquetan adecuadamente para facilitar la identificación y el mantenimiento. Además, se pueden implementar racks y gabinetes para mantener los equipos ordenados y protegidos.

II.1.7.4.3.-Gabinete de Telecomunicaciones

Un gabinete de telecomunicaciones, también conocido como rack de telecomunicaciones o armario de comunicaciones, es una estructura diseñada para alojar y organizar los equipos y

dispositivos de telecomunicaciones en una red informática. El gabinete proporciona un entorno seguro y ordenado para montar los componentes de la infraestructura de red. Estos se usan principalmente con la función de alojar múltiples equipos, para mejorar el ordenamiento y la gestión de los cables de red, para mantener una temperatura estable en los equipos por medio de ventilación, seguridad y protección para solo acceso de personal autorizado y también para la escalabilidad por que suelen adaptarse a las necesidades.

Los gabinetes pueden ser de varios tipos los más comunes son:

- Gabinete de montaje en pared (Wall-mount Cabinet): Estos gabinetes están diseñados para ser montados en la pared, lo que los hace ideales para espacios reducidos o cuando se requiere una instalación compacta. Son utilizados para alojar equipos de red más pequeños, como switches, routers, patch panels y equipos de conexión.
- Gabinete de piso (Floor-standing Cabinet): También conocidos como gabinetes de pie libre o gabinetes de suelo, son estructuras independientes que se colocan en el suelo. Estos gabinetes son más grandes y ofrecen una mayor capacidad de alojamiento para equipos y dispositivos de red. Son adecuados para redes más extensas y alojan componentes como servidores, switches, unidades de almacenamiento, entre otros.

II.1.7.5.-Canalización del Cableado

La canalización del cableado se refiere al sistema de conductos o rutas utilizados para organizar y proteger los cables en una red de telecomunicaciones o en un entorno de cableado estructurado. La canalización del cableado es esencial para mantener un entorno ordenado, minimizar el desorden de cables y facilitar el acceso y la administración de los cables.

- Conductos físicos: Los conductos físicos son tubos o canales por donde se pasan los cables. Pueden ser conductos metálicos, conductos de PVC, bandejas porta cables, canaletas de plástico o incluso sistemas de piso elevado. Estos conductos proporcionan una ruta protegida y organizada para los cables, evitando enredos y daños.
- Canaletas y ductos de pared: Las canaletas y ductos de pared son utilizados para ocultar y proteger los cables que se dirigen a través de las paredes. Estos sistemas proporcionan una ruta interna en la pared y permiten una instalación limpia y estéticamente agradable.

Las canaletas y ductos de pared también facilitan la administración de los cables y minimizan los riesgos de daños accidentales.

- Etiquetado e identificación: Es importante etiquetar y marcar adecuadamente los cables y la canalización para facilitar su identificación y mantenimiento. El etiquetado proporciona información sobre la función, origen o destino de los cables, lo que ayuda a evitar confusiones y errores durante las tareas de administración y solución de problemas.

II.1.8.-Cable de red

Para determinar cuál es el mejor cable para un lugar determinado habrá que tener en cuenta distintos factores:

- Carga de tráfico en la red
- Nivel de seguridad requerida en la red
- Distancia que debe cubrir el cable
- Opciones disponibles del cable
- Presupuesto para el cable

Cuanto mayor sea la protección del cable frente al ruido eléctrico interno y externo, llevará una señal clara más lejos y más rápido.

El cable Ethernet también conocido como cable de par trenzado sin blindaje (UTP, por sus siglas en inglés), es el tipo de cable más utilizado en redes LAN (Local Area Network). Está compuesto por pares de hilos de cobre trenzados, lo que ayuda a reducir la interferencia electromagnética. Este se compone de pares de conductores eléctricos aislados en forma de espiral este reduce la interferencia electrónica y diafonía entre los pares y así mejora la calidad de la señal transmitida.

Dependiendo la velocidad de transmisión se divide como:

- Categoría 5: Es una de las categorías más antiguas y se utiliza en redes de baja velocidad. Soporta velocidades de hasta 100 Mbps.
- Categoría 5e: Es una versión mejorada de la categoría 5 y se utiliza en redes de velocidad media. Soporta velocidades de hasta 1 Gbps.

- Categoría 6: Es una categoría más moderna y se utiliza en redes de alta velocidad. Soporta velocidades de hasta 10 Gbps.
- Categoría 6a: Es una versión mejorada de la categoría 6 y se utiliza en redes de velocidad ultra alta. Soporta velocidades de hasta 10 Gbps a una distancia de hasta 100 metros.

El cable coaxial Es un tipo de cable utilizado para transmitir señales eléctricas de alta frecuencia. Está compuesto por dos conductores que se orientan de manera coaxial y están separados por una capa de aislamiento dieléctrico. Esto permite una transmisión eficiente y protegida minimizando la interferencia y la perdida de señal, este es comúnmente usado en señales de televisión, conexiones de banda ancha o de video.

El cable de fibra óptica Es un tipo de cable utilizado para transmitir datos a través de pulsos de luz. A diferencia de los cables de cobre tradicionales, los cables de fibra óptica ofrecen una mayor capacidad de ancho de banda y una menor atenuación, lo que permite transmitir datos a largas distancias con menos pérdida de señal. Este tiene bastantes usos principalmente en el manejo de telecomunicaciones servicio de internet, también se puede aplicar a redes de área local o transmisión de señales de televisión, pero su alto costo con relación al par trenzado de cobre no tan agradable para uso común.

II.1.8.1.-Longitud del cable

La longitud total del cable que se requiere para conectar un dispositivo incluye todos los cables desde los dispositivos finales del área de trabajo hasta el dispositivo intermediario en el cuarto de telecomunicaciones (generalmente un switch). Esto incluye el cable desde los dispositivos hasta el enchufe de pared, el cable a través el edificio desde el enchufe de pared hasta el punto de conexión cruzada, o patch panel, y el cable desde el patch panel hasta el switch.

Si el switch se ubica en los cuartos de telecomunicaciones en diferentes pisos de un edificio o en diferentes edificios, el cable entre estos puntos debe incluirse en la longitud total.

Para las instalaciones UTP, el estándar ANSI/TIA/EIA-568-B especifica que la longitud combinado total del cable que abarca las cuatro áreas enumeradas anteriormente se limita a una distancia máxima de 100 metros por canal. Este estándar establece que se pueden utilizar hasta 5 metros de patch cable para interconectar los patch pannel.

II.1.9.- Equipos Tecnológicos

Existen dos clasificaciones, la primera clasificación son los dispositivos de usuario final, como por ejemplo computadoras, impresoras, scanners y otros dispositivos que provean servicios directamente al usuario. La segunda clasificación son los dispositivos de red. Los dispositivos de red proveen la comunicación entre dispositivos de usuario final.

II.1.9.1.- Switches

Un switch o conmutador de red es un dispositivo hardware que opera en la segunda capa del modelo OSI (Capa de Enlace de Datos) su función principal es interconectar múltiples dispositivos en una red LAN y gestionar el tráfico de la red de una manera eficiente, con diferencia de un dispositivo como un hub que envía direcciones en todos sus puertos de manera indiscriminada un switch envía los datos solamente por el puerto configurado al dispositivo correspondiente.

A continuación, se pondrán características del switch:

- Los switches filtran y reenvían los datos únicamente al puerto especifico donde está conectado el usuario destino minimizando el tráfico innecesario.
- Los switches permiten una mejor segmentación de la red rediciendo congestión y mejorando el tráfico de la red.
- Los switches modernos pueden permitir transmisión y recepción de datos de manera simultánea.
- Determinados switches también controlan funciones más avanzadas de seguridad como listas de acceso por parte de los equipos como también el control de las Vlans.

II.1.9.2.- Routers

Un router es un dispositivo de red que se utiliza para conectar diferentes redes y permitir la comunicación entre ellas. El router se encarga de enrutar los paquetes de datos a través de la red, utilizando diferentes protocolos de red y tomando decisiones sobre la mejor ruta para enviar los datos. Además, el router puede proporcionar funciones de seguridad, como firewalls y filtrado de paquetes, para proteger la red de posibles amenazas externas. En resumen, el router es un componente esencial en cualquier red informática, ya que permite la comunicación entre

diferentes dispositivos y redes.

Su función es que pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias.

Trabajan en la capa de red del modelo OSI segmentan la red por puerto a nivel de capa 2 y 3.

II.1.9.3.- Access Point

Un Access point (AP) es un dispositivo de red inalámbrico que se utiliza para conectar dispositivos a una red mediante Wi-Fi. El AP actúa como un punto de acceso a la red, permitiendo que los dispositivos se conecten a la red inalámbrica y se comuniquen entre sí. El AP se conecta a una red cableada y transmite la señal inalámbrica a los dispositivos cercanos. El AP también puede proporcionar funciones de seguridad, como autenticación de usuarios y encriptación de datos, para proteger la red de posibles amenazas externas. Además, el AP puede ser administrado para realizar tareas como la configuración de dispositivos y el monitoreo del tráfico de red. En resumen, el AP es un componente esencial en cualquier red inalámbrica, ya que permite la conexión de dispositivos a la red mediante Wi-Fi y proporciona funciones de seguridad y administración de red.

II.1.9.4.- Diferencias y Similitudes entre Access point y un Router

Función principal: El router se encarga de enrutar los paquetes de datos a través de la red, tomando decisiones sobre la mejor ruta para enviar los datos y utilizando diferentes protocolos de red. Por otro lado, el Access point se utiliza para conectar dispositivos a una red mediante Wi-Fi, actuando como un punto de acceso a la red.

Conexión a la red: El router se conecta a una red cableada y transmite la señal inalámbrica a los dispositivos cercanos, mientras que el Access point se conecta directamente a la red cableada y transmite la señal inalámbrica a los dispositivos cercanos.

Administración de red: El router puede ser administrado para realizar tareas como la configuración de dispositivos y el monitoreo del tráfico de red, mientras que el Access point se enfoca principalmente en la conexión de dispositivos a la red inalámbrica.

Funciones de seguridad: El router puede proporcionar funciones de seguridad, como firewalls y filtrado de paquetes, para proteger la red de posibles amenazas externas, mientras que el Access point puede proporcionar funciones de seguridad, como autenticación de usuarios y encriptación de datos, para proteger la conexión inalámbrica.

II.1.10.-Dispositivo mikrotik

MikroTikRouterOS es el sistema operativo del hardware MikroTikRouterBOARD. Que tiene las características necesarias para un ISP.

- Firewall
- Routing
- Forwarding
- MPLS
- VPN
- Wireless
- HotSpot
- Calidad de Servicio (QoS)
- Web Proxy
- Herramientas
- TheDude

Licencias RouterOS:

Tenemos 6 tipos de licencias:

- -Nivel 0: Demo (24 Horas)
- -Nivel 1: Free (Muy limitada)
- -Nivel 3: WISP CPE (Clientes Wi-Fi)
- -Nivel 4: WISP (Requeridos para un Access Point)
- -Nivel 5: WISP (Mas Capacidades)
- -Nivel 6: Controlador (Capacidades ilimitadas)

Un dispositivo Mikrotik es un dispositivo de red que se utiliza para crear y administrar redes de

cualquier tamaño. Mikrotik ofrece una variedad de dispositivos, desde pequeños routers para el hogar hasta grandes switches para empresas.

- **Enrutamiento:** El dispositivo Mikrotik se utilizará para enrutar el tráfico entre la red de la institución y el Internet.
- **Switching:** El dispositivo Mikrotik se utilizará para conectar los dispositivos de la red de la institución entre sí.
- **Acceso inalámbrico:** El dispositivo Mikrotik se utilizará para proporcionar acceso inalámbrico a Internet a los usuarios de la institución.
- **Seguridad:** El dispositivo Mikrotik se utilizará para proteger la red de la Fiscalía de accesos no autorizados.

Estas son todas las funciones de mi dispositivo mikrotik:

- **Enrutamiento** El enrutamiento es el proceso de mover el tráfico entre diferentes redes. Los dispositivos Mikrotik se pueden utilizar para enrutar el tráfico entre redes de diferentes tamaños, desde redes domésticas pequeñas hasta redes empresariales grandes.
- **Switching** El switching es el proceso de conectar dispositivos entre sí en una red. Los dispositivos Mikrotik se pueden utilizar para conectar dispositivos de diferentes tipos, como computadoras, impresoras, cámaras de seguridad y teléfonos VoIP.
- **Acceso inalámbrico** El acceso inalámbrico permite a los usuarios conectarse a Internet de forma inalámbrica desde cualquier lugar dentro del alcance de la señal. Los dispositivos Mikrotik se pueden utilizar para proporcionar acceso inalámbrico a Internet a los usuarios de una red.
- **Seguridad** Los dispositivos Mikrotik ofrecen una variedad de funciones de seguridad para proteger las redes de accesos no autorizados, ataques de malware y otros tipos de amenazas.
- **VPN** Las redes privadas virtuales (VPN) permiten a los usuarios crear una conexión segura entre dos redes. Los dispositivos Mikrotik se pueden utilizar para crear VPN para conectar redes de diferentes ubicaciones o para proporcionar acceso remoto a recursos de la red.

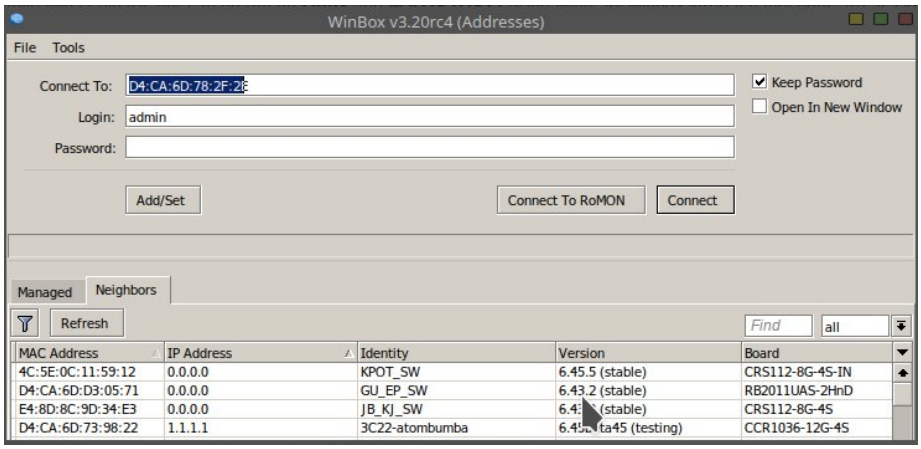


Figura 6. Herramienta winbox

II.1.11.-Vlans

Las Redes de Área Local Virtuales (VLAN, por sus siglas en inglés) son una tecnología de segmentación de redes que permite dividir una red física en múltiples redes lógicas aisladas entre sí. Esta segmentación se logra mediante la asignación de dispositivos y puertos de conmutación de red a grupos específicos, lo que facilita la administración, seguridad y eficiencia de la red.

La implementación de VLAN en la Fiscalía se justifica por los siguientes motivos:

- Mejora de la Seguridad: La separación de segmentos de red permitirá controlar y aislar el tráfico entre departamentos, protegiendo datos sensibles y mitigando amenazas internas.
- Optimización del Rendimiento: La segmentación de tráfico reducirá la congestión de la red y garantizará un rendimiento constante para aplicaciones críticas.
- Administración Eficiente: La administración de la red será más sencilla al agrupar dispositivos similares en segmentos lógicos, lo que facilitará la solución de problemas y cambios en la configuración.
- Preparación para el Futuro: La infraestructura de VLAN es escalable, lo que permitirá adaptarse fácilmente a las futuras necesidades de expansión de la red.

II.1.12.- Direccionamiento de Red

El direccionamiento de red se refiere al proceso de asignar identificadores únicos a dispositivos y recursos en una red de computadoras para que puedan comunicarse entre sí. En una red, cada dispositivo, ya sea una computadora, impresora, servidor o enrutador, se le asigna una dirección

única que le permite ser identificado y localizado en la red. Estas direcciones pueden ser direcciones IP (Protocolo de Internet) para redes IP, direcciones MAC (Control de Acceso al Medio) para redes locales, o incluso nombres de dominio en redes más grandes.

El direccionamiento de red es fundamental para que los dispositivos puedan intercambiar datos y servicios de manera eficiente. Permite enrutar paquetes de datos a su destino correcto y garantiza que la información llegue a donde debe. Además, el direccionamiento de red puede involucrar la segmentación de la red en subredes o VLANs para mejorar la gestión y la seguridad.

II.1.12.1.-Clases de direcciones IPv4

En el direccionamiento con IPv4 existen diferentes tipos de redes, estas fueron creadas con el objetivo de crear redes de tamaño grande, mediano y pequeño.

Existen direcciones de clase A, B, C que son las más utilizadas, también tenemos las clases E que son las direcciones de Multicast, y las de clase E que son para uso experimental o de pruebas. En la siguiente tabla se puede ver un resumen de las diferentes clases que tenemos:

Clase	Rango	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)	Información
A	0.0.0.0/8 to 127.0.0.0/8	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)	Para grandes redes con más de 16 millones de host addresses.
B	128.0.0.0 /16 - 191.255.0.0 /16	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)	Para soportar de medio a grandes redes.
C	192.0.0.0 /24 - 223.255.255.0 /24	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)	Soporta pequeñas redes con un máximo de 254 hosts.
D	224.0.0.0 to 239.0.0.0				Reservado para Multicasting
E	240.0.0.0 - 255.0.0.0				Experimental; usado para investigaciones

Figura 7. Ejemplos de direcciones ipv4

Tal y como se puede ver, tanto en las direcciones de clase A, B y C tenemos un rango de

direccionamiento IP privado que podemos utilizar en nuestro hogar o empresa sin problemas, pero siempre de manera local.

II.1.13.- Servicio de DHCP

El Servicio de Configuración Dinámica de Host (Dynamic Host Configuration Protocol o DHCP, por sus siglas en inglés) es un protocolo de red utilizado para automatizar y simplificar la asignación de direcciones IP y configuración de red a dispositivos en una red informática. Su función principal es gestionar de manera eficiente la distribución de direcciones IP, máscaras de subred, puertas de enlace, servidores DNS y otros parámetros de configuración a dispositivos, como computadoras, impresoras, y dispositivos móviles, cuando se conectan a una red.

DHCP opera de la siguiente manera:

- Cuando un dispositivo se conecta a la red, envía una solicitud DHCP para obtener una dirección IP y otros parámetros de configuración.
- Un servidor DHCP en la red recibe la solicitud y asigna una dirección IP disponible, junto con otros detalles de configuración, al dispositivo.
- El servidor DHCP responde al dispositivo con la información necesaria, permitiéndole conectarse a la red y comunicarse con otros dispositivos.

Los beneficios del DHCP incluyen la automatización de la asignación de direcciones IP, la prevención de conflictos de direcciones IP y la facilitación de la administración de la red, ya que reduce la necesidad de configurar manualmente cada dispositivo.

II.1.13.1.- Servicio de DHCP en mikrotik

Un dispositivo MikroTik ofrece una amplia gama de funciones relacionadas con el Servicio de Configuración Dinámica de Host (Dynamic Host Configuration Protocol o DHCP).

Asignación de Direcciones IP Dinámicas: El DHCP en MikroTik permite la asignación automática de direcciones IP a dispositivos en la red, lo que facilita la configuración de dispositivos sin necesidad de intervención manual.

- Asignación de Puertas de Enlace (Gateways): El DHCP permite asignar la puerta de

enlace predeterminada a los dispositivos, lo que facilita la comunicación con otras redes o Internet.

- Entrega de Servidores DNS: Puedes configurar servidores DNS para que se asignen automáticamente a los dispositivos, lo que garantiza que tengan acceso a la resolución de nombres de dominio.
- Tiempo de Arrendamiento de Direcciones (Lease Time): Puedes establecer el tiempo durante el cual una dirección IP asignada estará disponible para un dispositivo.
- Bloqueo de Direcciones IP: Puedes reservar direcciones IP específicas para dispositivos particulares, lo que garantiza que siempre reciban la misma dirección.
- Monitoreo y Registro de Actividad: MikroTik permite el monitoreo de las asignaciones de direcciones IP y mantiene registros de la actividad de DHCP.
- Configuración Avanzada de Red: Puedes realizar configuraciones más avanzadas, como el uso de múltiples subredes y segmentación de red.
- Seguridad: Puedes implementar medidas de seguridad, como la restricción de acceso a la asignación de direcciones IP por dirección MAC.
- Soporte para Redes VLAN: MikroTik es compatible con redes VLAN, lo que permite la segmentación de la red en múltiples dominios virtuales.
- Balanceo de Carga: Puedes implementar balanceo de carga para distribuir las solicitudes de DHCP en múltiples servidores, lo que mejora la redundancia y la disponibilidad del servicio.
- Configuración de Redes Inalámbricas: Puedes asignar direcciones IP a dispositivos inalámbricos en redes WLAN.

II.1.14.- Seguridad de la red

En que respecta a seguridad de una red todos los métodos y restricciones se llevaran a cabo en el dispositivo mikrotik:

II.1.14.1.- Firewall

Un firewall en un dispositivo MikroTik es una parte esencial de la seguridad de red que se encarga de controlar y regular el tráfico de datos entre redes. Proporciona una barrera de seguridad que filtra, bloquea o permite el paso de paquetes de datos en función de reglas y

políticas específicas.

- examina cada paquete de datos que entra o sale de la red y decide si se permite o se bloquea según reglas predefinidas.
- Las reglas de firewall son instrucciones que especifican cómo se debe tratar el tráfico. Pueden estar basadas en direcciones IP, puertos, protocolos u otras condiciones.

II.1.14.2.- Bloqueo de puertos

El bloqueo de puertos en un dispositivo MikroTik se refiere a la configuración de reglas de firewall que impiden o limitan el tráfico de red a través de puertos específicos. Este proceso se utiliza para reforzar la seguridad, controlar el acceso a servicios o aplicaciones, y proteger la red contra amenazas potenciales.

- Muchos protocolos y servicios utilizan puertos estándar, como el puerto 80 para HTTP, el puerto 443 para HTTPS y el puerto 22 para SSH. Las reglas de bloqueo pueden enfocarse en estos puertos estándar para controlar el acceso a servicios comunes.
- El bloqueo de puertos es una medida de seguridad esencial para prevenir ataques y proteger la red de amenazas como intrusiones, malware y denegación de servicio.

II.1.14.3.- Priorizar el ancho de banda

Es un conjunto de técnicas y políticas diseñadas para gestionar y asignar recursos de ancho de banda de manera eficiente, asegurando que ciertos tipos de tráfico o aplicaciones tengan un acceso preferencial a la capacidad de la red. Esta práctica es esencial para optimizar el rendimiento de la red y garantizar un funcionamiento adecuado, especialmente en entornos compartidos donde múltiples usuarios o aplicaciones compiten por recursos limitados.

- La priorización de ancho de banda permite garantizar un nivel mínimo de servicio para aplicaciones críticas.
- se asignan límites de ancho de banda a cada clase. Esto garantiza que ciertos tipos de tráfico reciban una cuota preferencial de ancho de banda cuando la red esté congestionada.

II.1.14.4.- Hotspot

Es un servicio que ofrece mikrotik que permite a los usuarios conectarse de manera inalámbrica a Internet o a una red local a través de una infraestructura de red inalámbrica, generalmente utilizando tecnología Wi-Fi. Los hotspots son comunes en lugares públicos como cafeterías, aeropuertos, hoteles y centros comerciales, así como en entornos empresariales.

Los hotspots pueden ser implementados de diversas maneras los dos modelos principales son:

- Hotspot Público: Estos hotspots se encuentran en lugares públicos como cafeterías, parques, estaciones de tren, aeropuertos y otros espacios públicos. Por lo general, ofrecen acceso gratuito o de pago a Internet y pueden requerir autenticación antes de la conexión.
- Hotspot Privado: Los hotspots privados son comunes en entornos empresariales y pueden requerir autenticación para el acceso. Las empresas pueden utilizar hotspots privados para proporcionar conectividad inalámbrica a empleados y visitantes.

II.1.14.5.- Estrategias de Administración de red

Las estrategias de administración de redes constituyen un conjunto de enfoques, políticas, y técnicas planificadas y coordinadas que se emplean para planificar, diseñar, implementar, supervisar y mantener una infraestructura de red de computadoras de manera efectiva y eficiente. Estas estrategias son esenciales en el ámbito de las tecnologías de la información (TI) y las comunicaciones, ya que permiten asegurar que las redes de datos funcionen de manera óptima, estén disponibles de forma continua, sean seguras y cumplan con los objetivos y requisitos del entorno en el que operan.

Unos puntos secciones a analizar en este punto son:

II.1.14.5.1.- Administración de cuentas de usuario Hotspot

La administración de cuentas de usuario en una red Hotspot es un aspecto crítico de la infraestructura de red, especialmente en entornos donde se ofrece acceso a internet inalámbrico de forma pública o privada. Una red Hotspot se utiliza comúnmente en hoteles, cafeterías, aeropuertos, instituciones educativas y otros lugares públicos para proporcionar conectividad a la red a los usuarios finales. La administración de cuentas de usuario en esta configuración implica una serie de procesos y políticas destinadas a gestionar, supervisar y controlar el acceso de los usuarios a la red. A continuación, se detalla este proceso:

Registro de Usuarios:

El proceso de administración de cuentas en una red Hotspot generalmente comienza con el registro de usuarios. Los usuarios deben proporcionar información básica, como nombres, direcciones de correo electrónico o números de teléfono, para crear una cuenta.

Autenticación:

La autenticación de usuarios es un paso crítico en la administración de cuentas. Los usuarios pueden autenticarse mediante diversos métodos, como contraseñas, códigos de acceso temporales, autenticación de dos factores (2FA) o incluso a través de redes sociales. Esta autenticación asegura que solo usuarios autorizados obtengan acceso a la red.

Asignación de Credenciales:

Cada usuario registrado recibe un conjunto de credenciales de acceso. Estas credenciales pueden ser un nombre de usuario y contraseña, estas credenciales deben ser asignadas a los equipos a los que se conectara.

Control de Acceso:

La administración de cuentas de usuario implica el control de acceso a la red. Esto puede incluir la restricción de ciertos servicios o sitios web, la limitación del ancho de banda disponible o la implementación de políticas de calidad de servicio.

Gestión de Tiempo de Sesión:

La administración de cuentas de usuario a menudo involucra la gestión del tiempo de sesión. Los usuarios pueden tener un tiempo limitado de acceso, después del cual se les desconecta automáticamente. Esto es común en cafeterías y lugares públicos.

Renovación de Cuentas:

Las cuentas de usuario en una red Hotspot pueden tener una fecha de vencimiento. La administración de cuentas incluye la renovación de cuentas para usuarios recurrentes o la eliminación de cuentas inactivas.

Seguridad:

La seguridad es un aspecto crítico de la administración de cuentas de usuario. Se deben implementar medidas para proteger las credenciales de usuario, cifrar la comunicación y prevenir el acceso no autorizado.

II.1.15.- Protección contra incendios

La protección contra el fuego es vital, por los daños materiales y sobre todo por las pérdidas humanas que puede ocasionar, por lo que un sistema de prevención contra el fuego tiene que ser eficaz para que se pueda prevenir, detectar y extinguir el incendio en su fase inicial. Para cumplir con este fin un sistema contra incendios involucra varias áreas de diseño que deben considerarse: hidráulica, eléctrica, mecánica, etc.

Las características se basan ciertas normativas reconocidas alrededor del mundo como por ejemplo la NFPA (Asociación Nacional de Protección contra el Fuego) cuyos códigos y normas son ampliamente adoptados debido a que son generados a través de un proceso abierto y consensuado.

II.1.15.1.-Extintores

Los extintores son elementos portátiles destinados a la lucha contra fuegos incipientes. Sirven para dominar o extinguir cualquier tipo de fuego generado para evitar así su transformación en incendios mayores. Existe un tipo de extintor recomendado para cada tipo de incendio y hoy desde Soler Prevención desglosaremos los tipos de extintores existentes y las recomendaciones específicas para sus usos.

Tipos de fuegos extintores

Para poder entender mejor la funcionalidad de cada tipo de extintor, es necesario saber primero qué tipos de fuegos existen:

- **Clase A:** fuegos con combustibles sólidos como madera, cartón, plástico, etc.
- **Clase B:** fuegos donde el combustible es líquido como por ejemplo el aceite, la gasolina o la pintura.
- **Clase C:** en este caso el combustible son gases como el butano, propano o gas ciudad.
- **Clase D:** en este tipo de fuegos el combustible es un metal: el magnesio, el sodio o el

aluminio en polvo.

II.1.16.- Pruebas en la red

Es un proceso crítico para garantizar que la red funcione de manera eficiente, segura y confiable antes de su implementación en un entorno de producción, estas son unas características a tomar en cuenta al implementar una nueva red.

- Pruebas de Conectividad: Se prueba la conectividad de red para garantizar que los dispositivos puedan comunicarse a través de la red sin problemas. Se verifica que no haya pérdida de paquetes y que la latencia sea aceptable.
- Pruebas de Rendimiento: Se evalúa el rendimiento de la red, incluyendo la velocidad de transferencia de datos, la capacidad de ancho de banda y la escalabilidad. Esto asegura que la red pueda manejar la carga prevista.
- Pruebas de Seguridad: Se realizan pruebas de seguridad para identificar y solucionar vulnerabilidades de red. Se verifica la efectividad de las medidas de seguridad, como cortafuegos y sistemas de detección de intrusiones.
- Pruebas de Tolerancia a Fallos: Se simulan fallos en la red para evaluar su capacidad de recuperación. Se verifica que la red pueda mantener la disponibilidad en caso de problemas.
- Pruebas de Calidad de Servicio (QoS): Si es necesario, se prueban las políticas de QoS para garantizar que se cumplan los requisitos de calidad de servicio para aplicaciones críticas.
- Pruebas de Interoperabilidad: Si la red se integra con sistemas de terceros, se realizan pruebas de interoperabilidad para garantizar que todos los sistemas funcionen juntos de manera eficiente.
- Pruebas de Documentación: Se revisa y actualiza la documentación de la red, incluyendo diagramas de red, políticas y procedimientos.

II.1.17.- Monitoreo de la red

El monitoreo de la red se describe como el proceso de supervisar y gestionar una red de computadoras para asegurar que funcione de manera eficiente, segura y confiable. Implica la

recopilación de datos sobre el tráfico de red, el rendimiento de dispositivos y la detección de posibles problemas o fallas el equipo mikrotik nos ofrece las siguientes opciones.

- The Dude: MikroTik proporciona una herramienta de monitoreo de red llamada "The Dude". Permite el descubrimiento de dispositivos en la red, el seguimiento de su estado y la creación de mapas de red. Puedes supervisar la disponibilidad de dispositivos y configurar alertas en caso de fallos.
- Snmp: MikroTik admite el protocolo SNMP (Simple Network Management Protocol), que te permite recopilar datos de dispositivos de red compatibles. Puedes utilizar software de gestión de red como Observium o Cacti para recopilar y mostrar estadísticas de rendimiento.
- Logs y Alertas: MikroTik permite configurar registros y alertas para eventos de red. Puedes supervisar eventos como intentos de inicio de sesión fallidos, cambios de configuración y más. Estos registros pueden enviarse a un servidor syslog externo o a través de correo electrónico para su monitoreo.
- Ancho de banda y Uso de Recursos: MikroTik ofrece herramientas integradas para monitorear el uso de ancho de banda y recursos del dispositivo. Puedes utilizar herramientas como Torch para visualizar el tráfico en tiempo real y el monitor de recursos para ver el uso de la CPU, la memoria y otros recursos.
- NetFlow: Puedes configurar el flujo de NetFlow en MikroTik para recopilar datos de tráfico de red y enviarlos a un servidor NetFlow para su análisis detallado.
- Firewall y Filtros: Utiliza las capacidades de firewall de MikroTik para establecer reglas de filtrado y registrar el tráfico no deseado o sospechoso. Esto te ayudará a mantener un ojo en la seguridad de la red.

COMPONENTE I

Desarrollo de la Configuración de la red

II.-Componente 1: Desarrollo de la Configuración de la red

II.2.- Metodología para diseño de red top-Down

La metodología Top-Down se puede aplicar para el diseño de redes y consta de varias fases que permiten analizar los requerimientos y objetivos de negocio para desarrollar un diseño adecuado. Algunas de las fases de la metodología Top-Down para redes incluyen el análisis de requerimientos, el desarrollo del diseño lógico y la selección de tecnologías y dispositivos. Esta metodología se enfoca en partir de una visión general de la red y desglosarla en planes específicos para lograr los objetivos establecidos previamente. La metodología Top-Down es por la que se optó para aplicar en este proyecto porque se adecua a lo que se plantea implementar en la fiscalía departamental de Tarija.

La metodología está compuesta por estas fases:

- Fase 1: Analizar Requerimientos
- Fase 2: Desarrollar Diseño Lógico
- Fase 3: Desarrollar Diseño Físico
- Fase 4: Probar, optimizar y documentar diseño
- Fase 5: Implementar y probar la red
- Fase 6: Monitorear y Optimizar la Red

En lo que respecta a esta metodología cubre todos los puntos para poner en funcionamiento la red desarrollada debido a eso para la propuesta de este proyecto se cubrirán completamente los puntos hasta la fase 4 y las otras fases se tomarán en cuenta los puntos que se puedan analizar tomando en cuenta la escala de desarrollo actual en la institución.

II.2.1.-Fase 1: Análisis de Requerimientos

II.2.1.1.-Análisis de metas del negocio

II.2.1.1.1.-Diagrama de funcionamiento de la institución

El proceso de funcionamiento de la fiscalía departamental de Tarija pasa por varios puntos intermedios pero los pasos mostrados en la figura describen el proceso por el que suele pasar un caso llevado por la institución y los procesos y tiempos que permanecen los casos en el sistema utilizado por la fiscalía

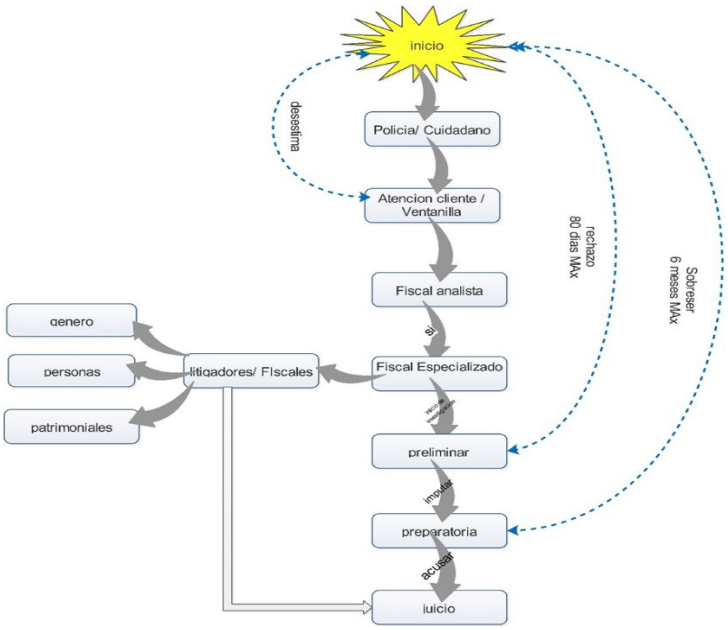


Figura 9. Diagrama de funcionalidad de la institución

Lo que se logra ver en la imagen es proceso de funcionamiento de la fiscalía departamental es un proceso se muestra en pasos que son:

- El proceso inicia donde ciudadano o policía se aproxima a ventanilla para informar sobre su caso y conocer los detalles principales del caso.
- Ventanilla o atención al cliente verifica los casos y pasa el detalle de los casos los fiscales analistas.
- El fiscal Analista es la persona que estima o desestima el caso según vea su experiencia en este ámbito si el caso procede este pasa a un fiscal especializado en el caso y este se desestima el caso vuelve a etapa de inicio hasta que sea presentado nuevamente.
- El fiscal especializado verifica y procede con informar a los afectados y al culpable y luego del análisis por su parte llega el caso a etapa preliminar.
- En la etapa preliminar se verifica por parte de otros involucrados en esta etapa el caso puede ser rechazado con un tiempo máximo de 80 días y si procede avanza a la etapa

preparatoria.

- En la etapa preparatoria es la culminación de los últimos preparativos en este punto para acercarse a acusar al involucrado el caso no puede sobrepasar los 6 meses como máximo y en caso de que continue el caso llega a una etapa de juicio y allí procede la autoridad a evaluarlo.

II.2.1.1.2.- Casos de uso de Negocio

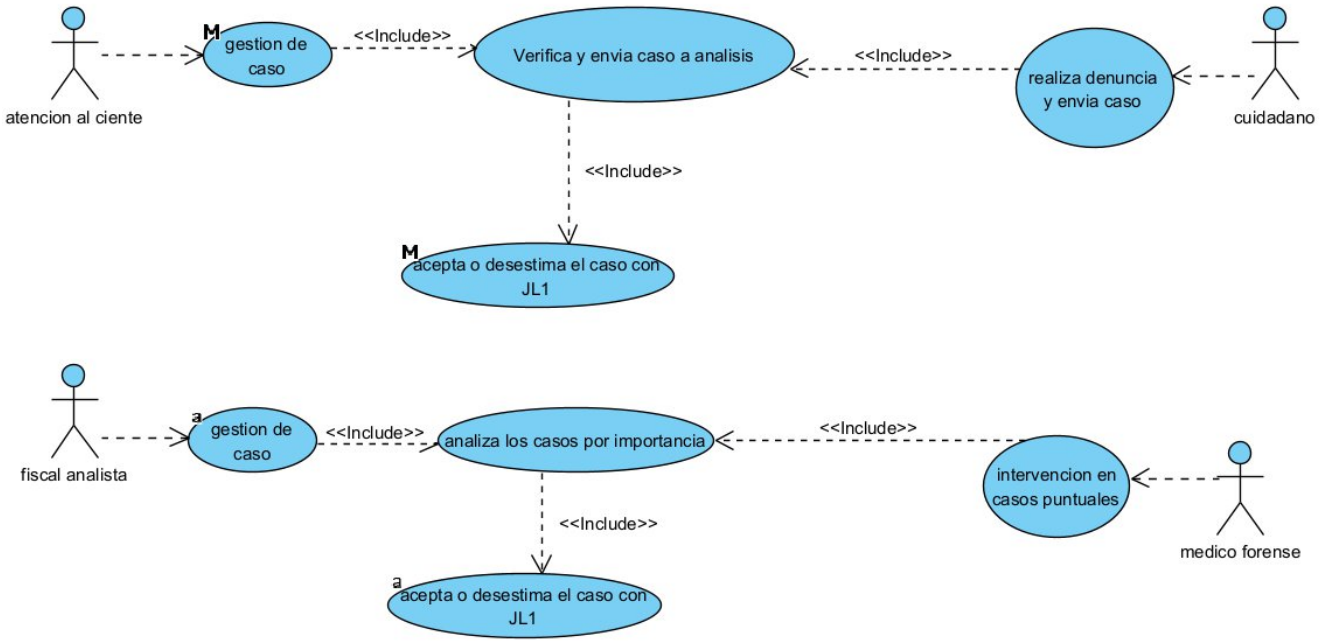


Figura 10. Caso de Uso de Negocio

En el caso de uso se logra ver el proceso principal que se repite al realizar una denuncia lo ya detallado en el diagrama de funcionalidad de la empresa, pero de una manera más detallada.

II.2.1.2.- Análisis de metas técnicas

La fiscalía departamental de Tarija para un mejor análisis de los datos opte por analizar cada piso de la institución cuenta con un total de 4 pisos:

la planta baja se cuenta con un aproximado de 16 empleados los cuales se distribuyen de la siguiente la siguiente manera:

- 4 en plataforma de ventanilla
- 1 en denuncias verbales
- 2 notificadores
- 1 conciliador
- 4 en Fiscal analista
- 3 médicos forense
- 1 policía

Planta Baja	Cantidad de host
plataforma de ventanilla	6
denuncias verbales	7
notificadores	4
conciliador	4
Fiscal analista	6
médicos forense	7
Policia	1
total	35

Tabla 3. Host de la planta baja

En la planta baja equipos de tipo terminal se encontrarían 35

La planta 1 se cuenta con un aproximado de 19 empleados los cuales se distribuyen de la siguiente la siguiente manera:

- 6 litigadores

- 2 psicólogos
- 5 fiscales de materia
- 6 auxiliares/abogados

Planta 1	Cantidad de host
litigadores	14
psicologos	2
fiscales de materia	10
auxiliares	11
total	37

Tabla 4. Host de la planta 1

En la planta 1 equipos de tipo terminal se encontrarían 37

La planta 2 se cuenta con un aproximado de 9 empleados los cuales se distribuyen de la siguiente la siguiente manera:

- 2 fiscales de materia
- 5 auxiliares/abogados
- 2 psicólogos

Planta 2	Cantidad de host
fiscales de materia	4
psicologos	2
auxiliares	7
total	13

Tabla 5. Host de la planta 2

En la planta 2 equipos de tipo terminal se encontrarían 13

La planta 3 se cuenta con un aproximado de 9 empleados los cuales se distribuyen de la siguiente la siguiente manera:

- 2 administración
- 1 fiscal de materia
- 3 informática
- 2 asistentes
- 1 secretaria

Planta 3	Cantidad de host
administracion	4
informatica	5
fiscales de materia	2
asistentes	4
secretaria	1
total	16

Tabla 6. Host de la planta 3

En la planta 3 equipos de tipo terminal se encontrarían 16

La planta 4 se cuenta con un aproximado de 6 empleados los cuales se distribuyen de la siguiente la siguiente manera:

- 4 asistentes de fiscal
- 2 fiscales

Planta 4	Cantidad de host
fiscal de materia	6
asistente fiscal	4
total	10

Tabla 7. Host de la planta 4

En la planta 4 equipos de tipo terminal se encontrarían 10

II.2.1.3.- Analizar red existente

En la fiscalía departamental de Tarija cuentan con una red esta red está dispuesta en una topología de hibrida la red actual de la fiscalía está compuesta que los servicios de internet por parte del proveedor se distribuyen al piso 3 en donde se encuentra su espacio acondicionado como su cuarto de telecomunicación desde este espacio se satisface a los empleados de la 3er y 4ta planta respectivamente sin un control de los cables distribuidos la red igual cuenta con un inconveniente y no cuenta con un control específico y etiquetas en los cables debido a que en el edificio usado todavía persiste un anterior cableado sin uso que se mezcla con el cableado de la institución.

II.2.1.3.1.- Diseño lógico de la antigua red

La organización de la antigua red de manera lógica se originaba con la configuración de un equipo Forigate 50e este dispositivo realizaba distribución de las 4 ethernet que estos estaban configurados cada uno con una distribución de red diferente estas cuatro pasaban atreves de cada piso para distribuir mediante switchs y alimentar a los demás pisos.

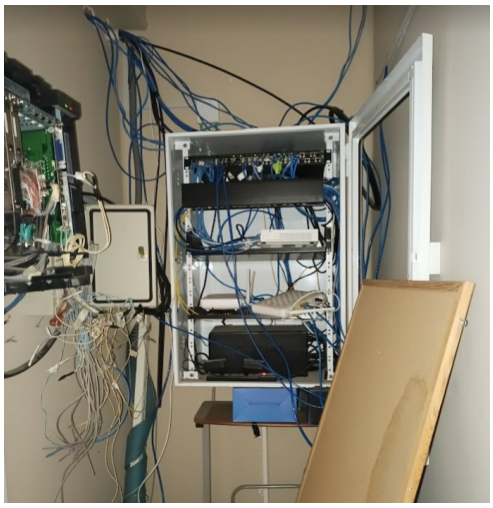


Figura 11. Estado del cuarto de telecomunicaciones actual

El gabinete de telecomunicaciones se encontraba en mal estado y los cables que distribuía al ampliar de puntos también contaban con hubs para extender más la red en este gabinete principal se manejaba tanto el fortigate 50e como 2 servicios de internet uno de hogar de una velocidad de 50 mbps de descarga y 50 mbps de subida y otro corporativo de una velocidad de 150 mbps de descarga 65 de subida aproximadamente medido durante uso en la antigua red ya que se contaba con el dispositivo fortigate 50e configurado solamente usando el internet corporativo y al contar con un acceso al dispositivo fortigate de solo visualización de la configuración se optó por realizar una nueva configuración en otro dispositivo para aprovechar el internet de tipo hogar que solo se usaba como ventana para acceso a wifi en el tercer piso de la institución.

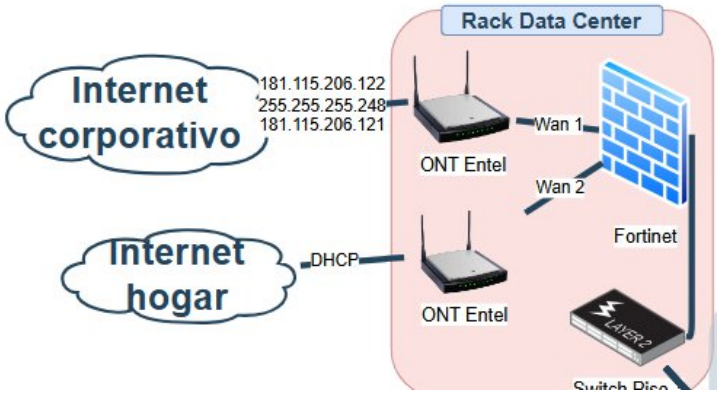


Figura 12. Representación del gabinete de telecomunicaciones

Para la distribución de la planta 2 se hace un tendido de cable para comunicarse desde la planta 3 con un switch alojado en la oficina fiscal y desde ese distribuye un puerto para comunicarse con el switch de la planta 1 se comunica con uno de los switchs de la planta baja y se encuentra divido en 2 switch de 12 y para los dispositivos faltantes se hace el uso de hubs para extender la red a los empleados faltantes principalmente a los médicos forenses.

Figura 13. Vista de los switchs de la planta baja,1,2

Para las plantas baja,1 y 2 los equipos se encuentran al aire libre y el cableado en ocasiones se encuentra por fuera y como se ve en este dispositivo solo hay 2 puertos libres y para amplificar se hace uso de los dispositivos hubs.

Equipos	**Descripción**	**Cantidad**
fortigate 50e	enrutador para toda la institución que puede soportar entre 50 usuarios	1
Modem	servicio de internet Entel	2
Organizador de cable	organizador de switch	1
Switch 24 ´puertos	switch de piso	2
Switch 12 ´puertos	switch de piso	4
ups iterativa forza	protege y suministra energía a los equipos	1

Tp link	proveer servicio inalámbrico	X

Tabla 8. Dispositivos presentes en la antigua red

Estos dispositivos se encontraban presentes en la antigua red para el uso de toda la institución está la composición que manejaba la antigua red de la institución.

II.2.1.3.1.- Distribución de la antigua red

II.2.1.3.1.1.- Distribución de la planta baja:

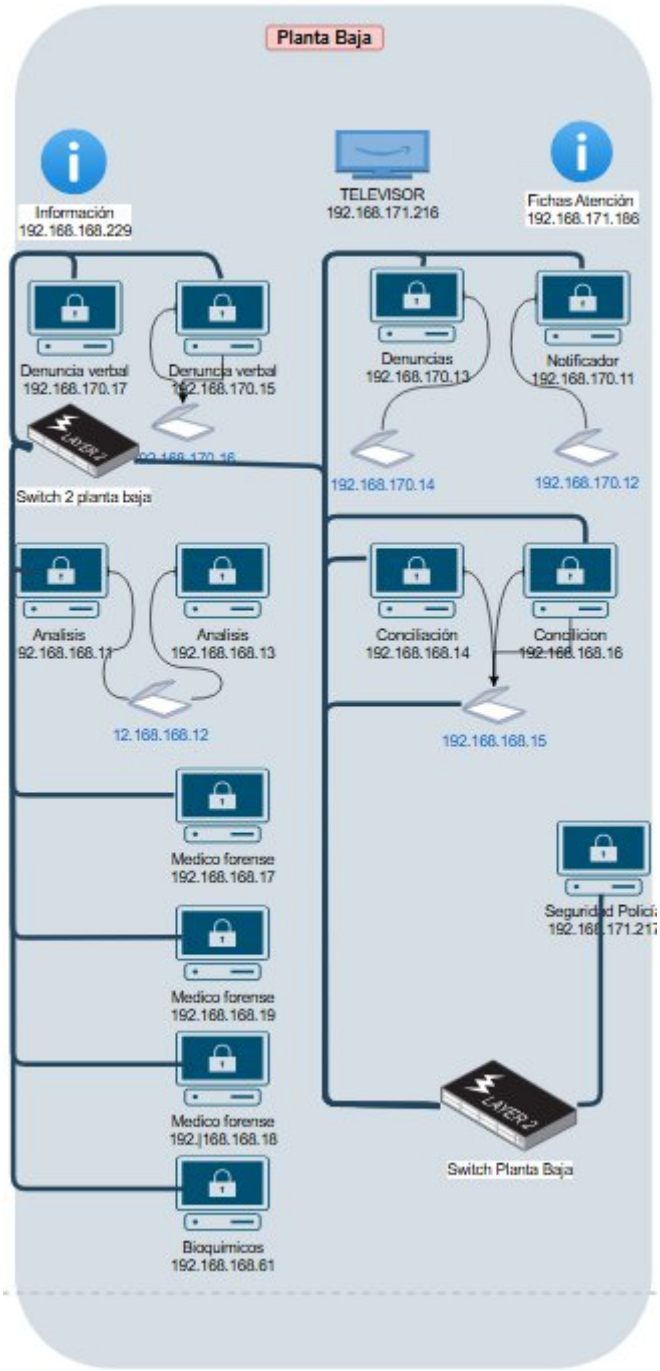


Figura 14. Distribución planta baja antigua red

II.2.1.3.1.2.- Distribución de la planta 1:

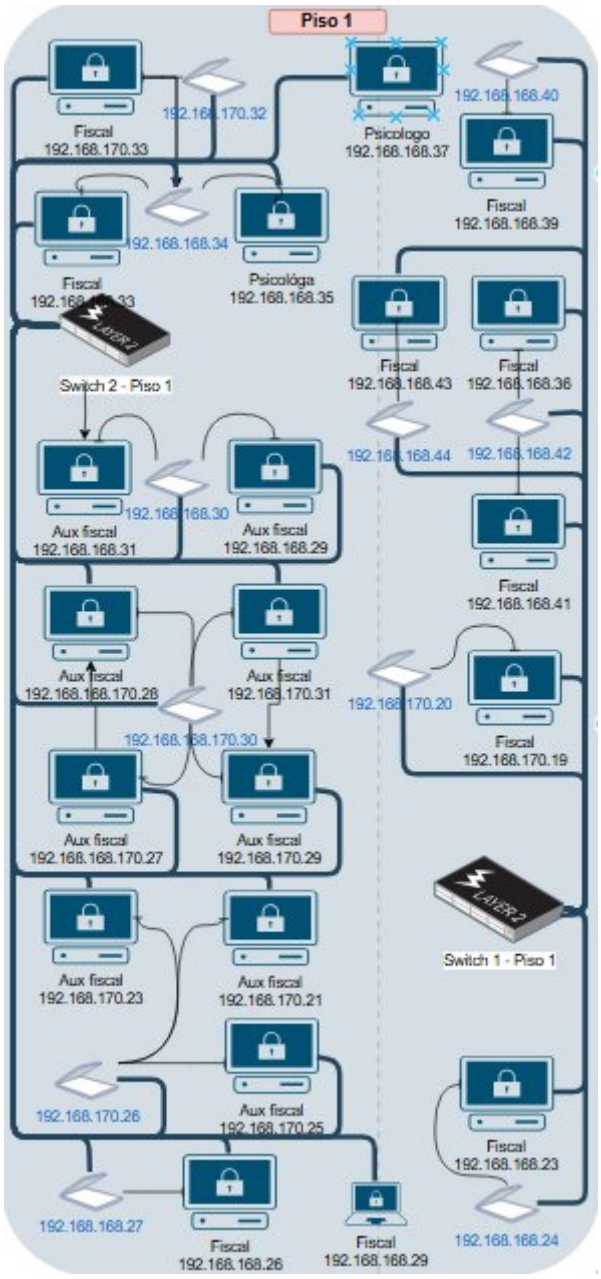


Figura 15. Distribución planta 1 antigua red

II.2.1.3.1.3.- Distribución de la planta 2:

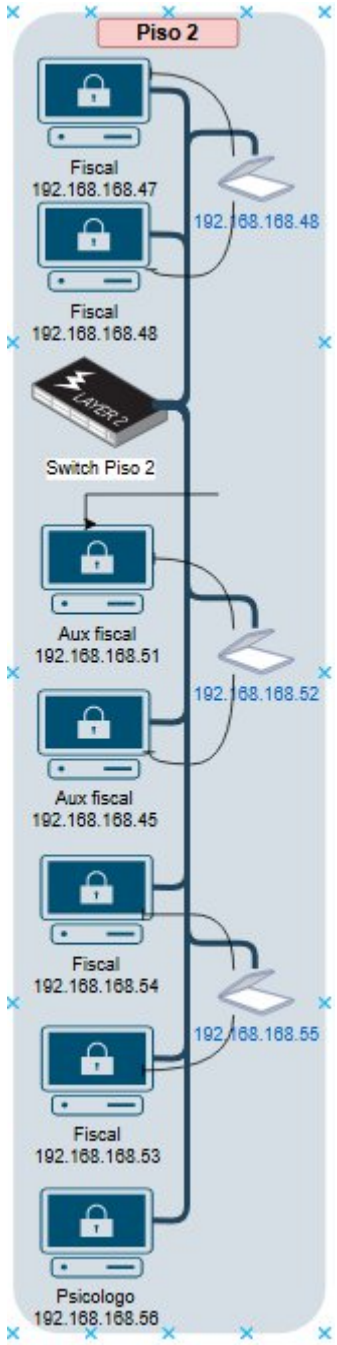


Figura 16. Distribución planta 2 antigua red

II.2.1.3.1.4.- Distribución de la planta 3:

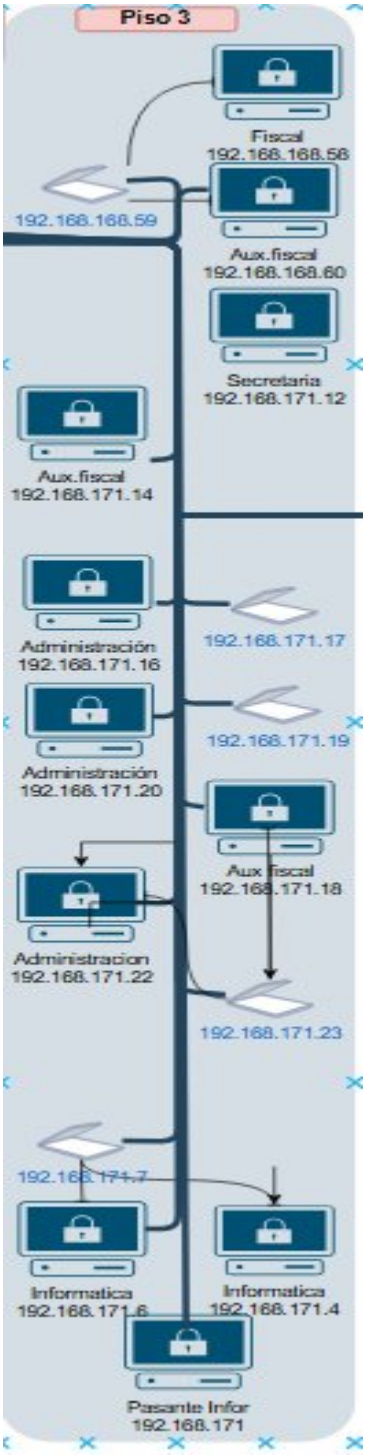


Figura 17. Distribución planta 3 antigua red

II.2.1.3.1.5.- Distribución de la planta 4:

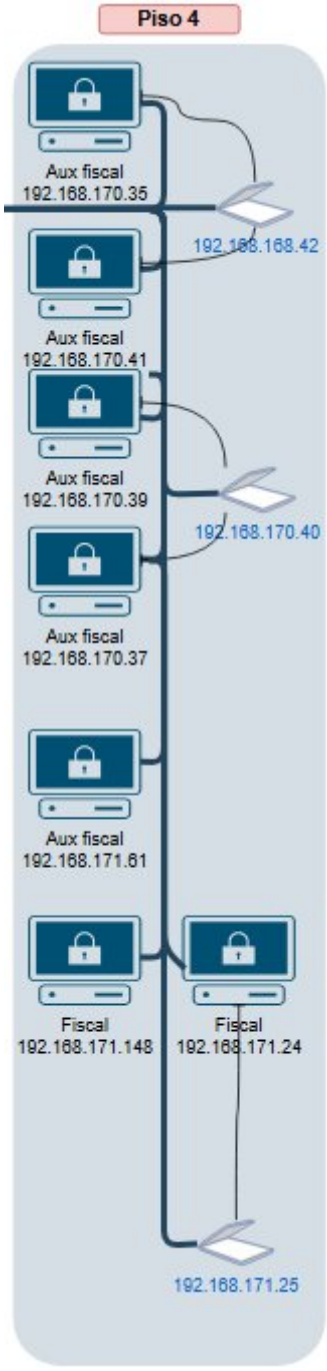


Figura 18. Distribución planta 4 antigua red

II.2.1.3.1.6.- Explicación de la antigua red

- La distribución de la planta baja en la antigua red de la fiscalía se encontraba dispuesta entre 2 switchs comunicados entre sí para distribuir conexión equipos estos no se encontraban ordenados porque para la verificación a cuál pertenecía el cableado al ser un cableado que se mezclaba causaba múltiples confusiones a la hora de instalar nuevos equipos por lo que hacían uso de hubs o medios para agilizar una conexión rápida.
- La distribución de la planta 1 en la antigua red de la fiscalía se encontraban 2 dispositivos switchs más grandes uno en conciliación y otro en la sala de fiscales de materia el primero de 24 puertos abastecía principalmente a los litigadores y conciliadores, el otro de 24 puertos principalmente para los fiscales y sus asistentes y los psicólogos no tenían acceso a internet al ser una parte difícil de acceder.
- La distribución de la planta 2 en la antigua red se encontraban un dispositivo pequeño que abastecía a todo el piso ubicado en la sala de la fiscal analista y en este piso tomando en cuenta a los psicólogos ellos no tenían acceso a internet eso por falta de puertos activos en el dispositivo de la planta 2 y optar por priorizar los que necesitan acceso rápido.
- La distribución de la planta 3 en la antigua red se encontraba un dispositivo grande solo un pequeño cuarto solo con aire acondicionado los equipos se encontraban en un mueble allí se encontraba la central donde llegaba el servicio de internet y de allí bajaba y distribuía a los demás pisos en este piso se encontraba un hub para los dispositivos del fiscal y sus auxiliares.
- La distribución de la planta 4 en la antigua red proviene desde el gabinete de la planta 3 le suministraba servicio de red a la planta 4 por medio de cableado directo desde la planta 3 al ser una cantidad reducida de equipos.

El direccionamiento ip de la antigua red se componía de 4 direcciones usadas las cuales eran:

- La 192.168.168.0 esta red era principalmente usada para asignarla a los asistentes.
- La 192.168.169.0 esta red era principalmente usada para asignarla a los fiscales.
- La 192.168.170. 0 esta red era para asignarla a equipos pertenecientes a informática
- La 192.168.171.0 esta red era para asignarla a dispositivos inalámbricos o dispositivos de

uso privado por parte de ingeniera informática.

Esta asignación como se ve en la distribución de la antigua red no está aplicada de esta manera en todo caso esta se encuentra desordenada y asignada de cualquier equipo lo cual es perjudicial al asignar cualquier red puede ser un grave error al darle acceso a otros equipos ubicados en la red que se le asigno.

II.2.1.4.-Análisis de tráfico existente

El flujo de datos puede ocurrir tanto a nivel interno de un sistema como a través de redes externas, como Internet. La transferencia de datos puede realizarse en diferentes direcciones, como en un sentido unidireccional o en ambos sentidos, dependiendo de la naturaleza de la comunicación.

En lo que respecta a la fiscalía sus análisis del flujo de datos radica en 2 sistemas principalmente:

- 1 JL1: este sistema tiene su función principal de administrar y gestionar los casos este se usa para que los abogados y partes hagan seguimiento de los casos, este sistema se comunica con instituciones como ser órgano Judicial, policía, segip, rejap, migración.
- 2 JL2: este sistema tiene su función principal administrando IDIF (Instituto de investigación forense), recursos humanos, unidad de protección de víctimas y testigos y seguimiento de ejecución financiera.
- 3 almacenes: este se encuentra en un servidor de manera local y solo se usa para el control de los almacenes de equipos y repuestos en la fiscalía.
- 4 gestión documental: correspondencia
- 5 correo institucional: cómo se puede ver es un correo institucional que pocos usan en la actualidad pero que se encuentra en la fiscalía
- 6 archivo Local: para administrar los casos archivados

Programas que usa la fiscalía:

solo se hace uso de Navegadores como Chrome, Firefox, Edge.

Any desk: para ofrecer asistencia técnica más por parte del área de informática

II.2.2.-Fase 2: Desarrollar Diseño Lógico

II.2.2.1.-Diseño de Topología de red

El diseño de una red es un proceso crucial para garantizar una conectividad eficiente y confiable en un entorno administrativo, público y de la fiscalía departamental de Tarija. Al recopilar información y presentar un modelo de diseño de red, es importante considerar diversos aspectos que influirán en la elección de la topología y la distribución de equipos. En este caso lo recomendable seria hacer el uso de una topología estrella, pero tomando en cuenta los datos y con los equipos que contara la fiscalía departamental de Tarija se optó por la topología de bus debido al uso del dispositivo mikrotik como enrutador principal todos los datos que se transmiten en la red pasan a través del cable compartido y son recibidos hacia los gabinetes colocados en cada piso al equipo distribuidor de cada piso para cuando llegue la señal del bus proceder con el cableado horizontal.

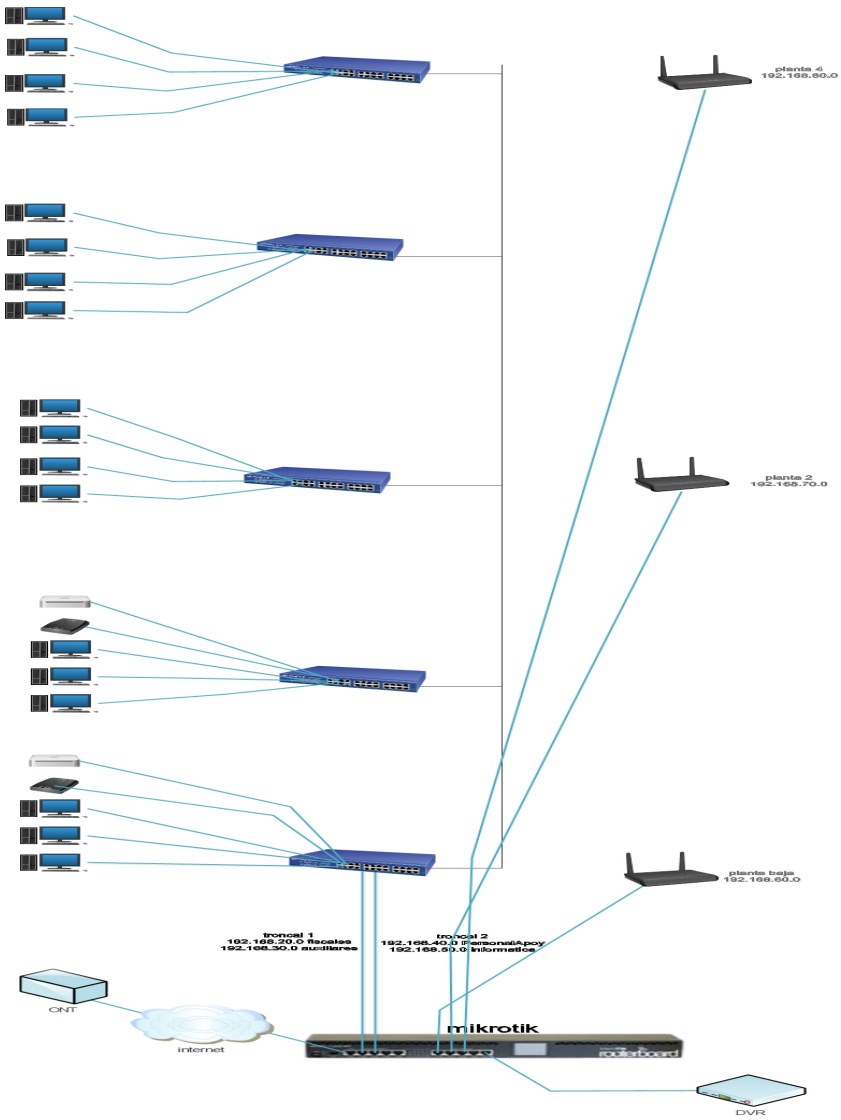


Figura 19. Topología de red de la institución

El uso de cableado estructurado mediante medios de transmisión es fundamental para satisfacer las necesidades de transporte de información en el diseño de nuestra red. En este sentido, el cableado estructurado se destaca como la opción más adecuada para esta tarea.

Optaremos por el cable de cobre o par trenzado, compuesto por hilos de cobre trenzados para asegurar su estabilidad a lo largo del tiempo y evitar interferencias. En particular, utilizaremos el tipo de cable par trenzado conocido como UTP, capaz de transmitir señales de voz o datos. Su bajo costo y facilidad de instalación lo hacen muy conveniente para nuestra red. Además, su

diámetro reducido permite su uso en espacios de dimensiones reducidas.

Es importante tener en cuenta que el UTP no cuenta con blindaje, lo cual lo excluye de áreas propensas a interferencias electromagnéticas. Asimismo, su alcance máximo está limitado a 100 metros. Por tanto, su implementación resultará adecuada para cubrir las necesidades de comunicación en nuestra red, garantizando una transmisión confiable y eficiente de datos y voz.

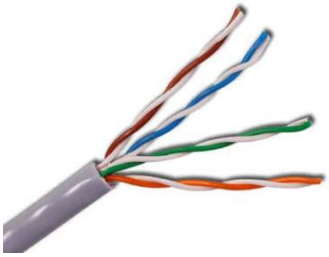


Figura 20. Cable UTP

El cable UTP utilizado en este diseño será de categoría 5e siguiendo los estándares TIA/EIA-568-B, 568-A y 568-B1, definiremos el orden de los conectores y colores en el conector RJ45. En este diseño, distinguiremos dos tipos de conexiones: el cable directo y el cable cruzado, cada uno con funciones específicas y distribución de cables en el conector.

En este apartado debemos distinguir dos tipos de conexión llamadas cable cruzado y cable directo cuyas funciones son diferentes, así como la distribución de cables en el conector.

Los cables directos tienen dos formas diferentes de cableado: T568A y T568B. Ambas formas son funcionales y no hay diferencia de rendimiento entre ellas.

Los cables cruzados tienen un cableado diferente al de los cables directos. Esto se debe a que los cables cruzados deben poder enviar y recibir datos al mismo tiempo.

Si no se ve seguro de qué tipo de cable usar, es mejor usar un cable directo. Los cables directos son compatibles con la mayoría de los dispositivos y se pueden utilizar en cualquier situación.

El cable que se opto para este proyecto es principalmente el cable cat5e de tipo directo cumpliendo con la norma ANSI TIA/EIA-568-B con un orden de colores naranja blanco, naranja, verde blanco, azul, azul blanco, verde, café blanco, café para la conexión de los equipos de manera horizontal.

El cableado horizontal es el cableado que conecta los puntos de conexión de telecomunicaciones en los puestos de trabajo a los paneles de distribución horizontal en el cuarto de telecomunicaciones. El cableado horizontal generalmente se realiza con cable de pares trenzados no blindado (UTP) o cable de fibra óptica.

En este caso en lo que respecta al edificio de la fiscalía que cuenta con un total de 4 pisos más la planta inferior serian 5 en cada piso se dispondría de un gabinete de distribución para el cableado horizontal cada piso de la fiscalía con excepción de la planta baja que en allí se encontrara un gabinete principal o cuarto de telecomunicación en este se almacenaran el dispositivo principal del trabajo que es el mikrotik.

El cableado horizontal debe cumplir con los requisitos de la norma ANSI/TIA/EIA-568. La norma establece que la distancia máxima de recorrido para el cableado no debe exceder los 90 metros de longitud entre el parcheo y la salida hacia el área de trabajo.

El cableado vertical es el cableado que conecta los paneles de distribución horizontal en los cuartos de telecomunicaciones a la red troncal. El cableado vertical generalmente se realiza con cable de pares trenzados no blindado (UTP) o cable de fibra óptica.

En este caso en lo que respecta al cableado vertical se comunicara con un enlace troncal este enlace en los cableados de tipo bus suele pasar por un solo cable a los gabinetes de los demás pisos

- Se instalaría un armazón de cableado vertical en el cuarto de telecomunicaciones de la planta baja.
- Se correría cable UTP o de fibra óptica desde el armazón de cableado vertical hasta los MDF en los cuartos de telecomunicaciones de los otros pisos.
- El cable se conectaría al MDF en cada piso utilizando conectores RJ-45.

No se cuenta con un cuarto de entrada de servicios por ende se realizará la distribución desde el gabinete de piso ubicado en la plata baja para la distribución en los demás pisos en sus gabinetes de pared que distribuirán servicio a los puntos de trabajo en la fiscalía departamental de Tarija.

En lo que respecta a la norma ANSI/TIA/EIA-568 para el cableado vertical o backbone establece que se puede hacer uso de cableado UTP en la conexión, pero al manejar un mayor volumen de datos al interconectar pisos de la institución se optó por hacer uso de cable UTP cat 6 al este contar con un mayor volumen de datos.

Figura 21. Rack Gabinet de 22U

El gabinete de piso es una caja grande y rectangular que se usa para almacenar y proteger dispositivos de red. Los gabinetes de piso para redes suelen estar hechos de acero o aluminio y tienen puertas que se pueden cerrar con llave para evitar el acceso no autorizado debe tener 1 metro libre para el espacio de apertura de la puerta y en los laterales de 0,6 metros para la manipulación. También pueden tener ruedas o patas para facilitar el movimiento esto establecido por la Norma ANSI TIA/EIA 569 para los gabinetes de piso.

Luego se dispondrá de un gabinete de pared más pequeño en los demás pisos este alojara dispositivos conmutadores como son los switchs principalmente para proveer el servicio a los

dispositivos, dando cumplimiento a la normativa ANSI TIA/EIA 569 para los dispositivos de pared establece que deben encontrarse en un lugar de acceso moderado a una distancia de 2 metros desde el borde del piso.

II.2.2.2.-Diseño modelos de direccionamiento y host-name

II.2.2.2.1.-Direccionamiento

Para el definir este punto lo que necesitamos conocer es principalmente cuanto host y/o equipos necesitan direccionamiento Ip en la red.

Los equipos que necesitan dirección ip son:

- Computadoras
- Impresoras
- Scanners
- Dispensadores
- Access points

Una vez definido los equipos que utilizaran ip en la red se procede a ejecutar el plan de direcciones ip necesarias que satisfagan lo que requiere la fiscalía como la fiscalía requiere un control determinado dependiendo cada grupo de trabajo se llevó a cabo que se necesitan un total de 4 segmentos de red de clase C.

	Ip de red	Mascara
Segmento	192.168.20.0/24	255.255.255.0
Segmento	192.168.30.0/24	255.255.255.0
Segmento	192.168.40.0/24	255.255.255.0
Segmento	192.168.50.0/24	255.255.255.0

Tabla 9. Direcciones ip usadas

- El segmento de red 192.168.20.0 se les asignara a los usuarios de tipo fiscales
- El segmento de red 192.168.30.0 se les asignara a los usuarios de tipo asistente
- El segmento de red 192.168.40.0 se les asignara a los usuarios de tipo Idif o personal de

apoyo

- El segmento de red 192.168.50.0 se les asignara a los usuarios de tipo informática

Tomando en cuenta lo que comprende a los equipos inalámbricos se dispondrá de los siguientes segmentos de red:

	Ip de red	Mascara
Segmento	192.168.60.0/24	255.255.255.0
Segmento	192.168.70.0/24	255.255.255.0
Segmento	192.168.80.0/24	255.255.255.0

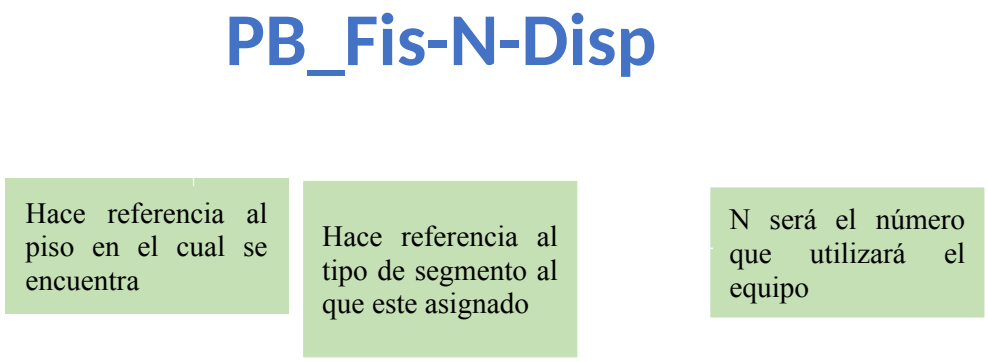
Tabla 10. Direcciones ip usadas inalámbricamente

- El segmento de red 192.168.60.0 se dispondrá para el uso de los dispositivos inalámbricos correspondientes a la planta baja, planta 1
- El segmento de red 192.168.70.0 se dispondrá para el uso de los dispositivos inalámbricos pertenecientes a la planta 2 y planta 3
- El segmento de red 192.168.80.0 se dispondrá para el uso de los dispositivos inalámbricos pertenecientes a la planta 4

En el caso de los dispositivos inalámbricos se tomará en cuenta la ubicación de los equipos en un área donde pueda cubrir en su totalidad el radio de alcance del área de trabajo.

II.2.2.2.2.-Host-name

Con respecto al host-name esta será una característica que nos permitirá identificar los equipos conectados a la red se tomará en cuenta a que piso pertenece y a que segmento de red este asignado.



Con respecto a la identificación de que **Dips** este se refiere al tipo de dispositivo al que se refiere que está conectado esto tomando en cuenta si se trata de una Pc de escritorio (**PC**), dispensador (**Dis**), impresora (**Pri**), scanner (**Scan**).

II.2.2.3.- Seleccionar protocolos para Switching y Routing

Los protocolos de switching y routing son los protocolos que permiten que los dispositivos de red se comuniquen entre sí. Los protocolos de switching se utilizan para conectar dispositivos en una misma red, mientras que los protocolos de routing se utilizan para conectar redes diferentes.

En lo que comprende de Switching en el proyecto actual si se aplicara por que el dispositivo switch nos permite administrar y dirigir todos los puertos y funciona de modo que utilizan los datos Mac para dirigir los datos al dispositivo internamente el dispositivo switch trabaja con el protocolo RSTP (Rapid Spanning Tree Protocol) principalmente se encuentra en la capa de enlace del modelo TCP/IP ya que este realiza la tranferencia de tramas utilizando las direcciones Mac.

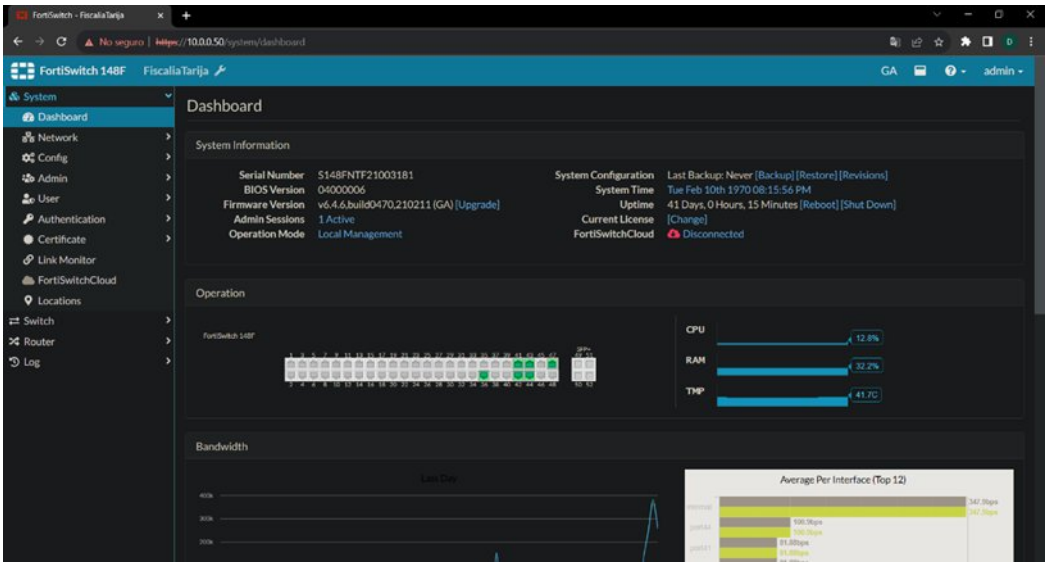


Figura 22. Administración del switch

En este apartado se logra ver cómo se administrará puerto por puerto para que se direccione a la vlan correspondiente al tipo de usuario en la cual estará dispuesto ese puerto, otra función que manejara el dispositivo switch es pasar un puerto como troncal hacia el gabinete del siguiente piso para allí distribuir usuarios de la misma manera.

EL manejo principal para llevar a cabo la configuración de la vlans que son parte fundamental en el switching se realizara en el mikrotik con la creación y la asignación de los puertos para el paso de las vlans para así pueda ser recibido y gestionado por parte del switch asignarlas y administrarlas para los dispositivos finales de la red.

Los protocolos de Routing principalmente es en mover datos entre diferentes redes estos mueven demasiado tráfico principalmente el dispositivo mikrotik que es el enrutador este interactúa principalmente con la red de servicio proveedor de internet, el dispositivo enrutador interactúa para proveer direcciones Ip a toda la red tanto a todos los dispositivos de ethernet al estar configurada las 2 troncales que poseen las 4 vlans de toda la red, también a su vez maneja la configuración de los 3 Access point que ofrecen conexión inalámbrica, Este trabaja principalmente en la capa de internet del modelo TCP/IP al encargarse principalmente de él envió de paquetes y el enrutamiento de los mismos.

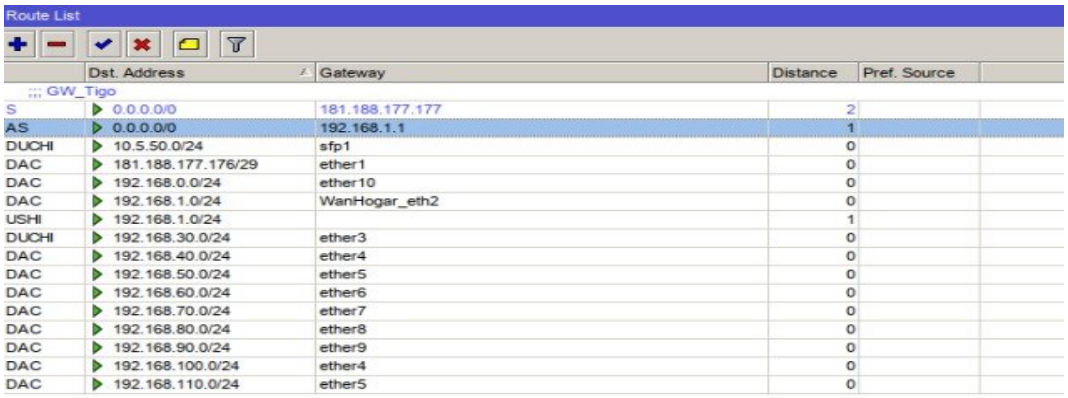


Figura 23. Definición de rutas de acceso a internet

Con respecto al routing la interacción de la red con otros proveedores de internet dispone principalmente estas alimentaran todas las funciones de la red, las redes wan conectadas al dispositivo mikrotik se encuentran con el Gateway 181.188.177.177 esta es la red respaldo en caso de falla es la red del proveedor de internet de Tigo, la red 192.168.1.1 la red principal que alimenta a todos los equipos conectados a la fiscalía que es la red de Entel.

Figura 24. Servicio de internet de Entel

Velocidad de internet del proveedor de servicio de Entel que gestionará el uso principal y abastecerá a toda la institución en la conexión a sus equipos finales.

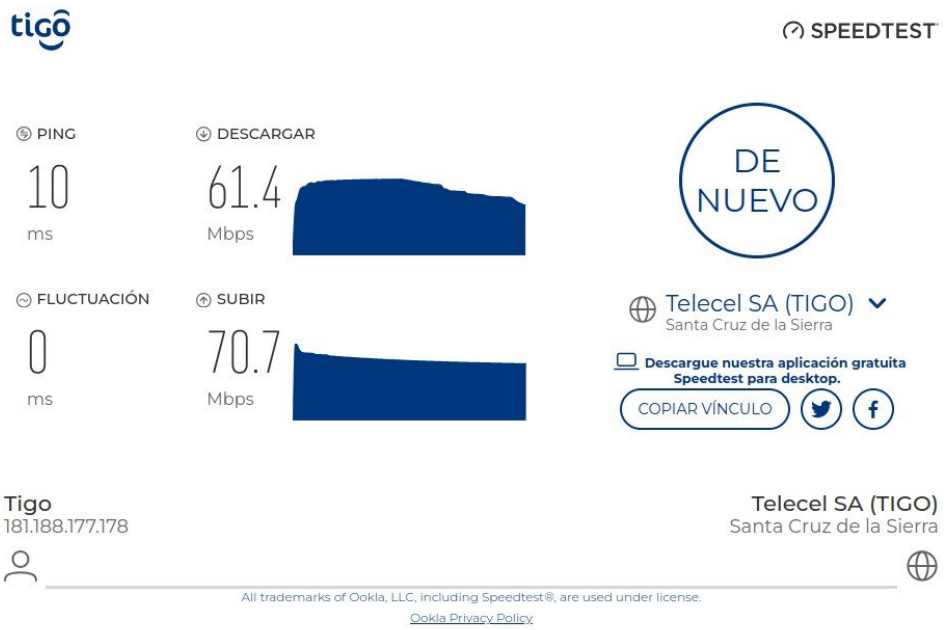


Figura 25. Servicio de internet de Tigo

Velocidad de internet del proveedor de servicio de Tigo que gestionara como respaldo y gestionara tareas secundarias para disminuir el uso del ancho de banda del servicio principal de internet.

II.2.2.4.-Desarrollo estrategias de seguridad

Las estrategias de seguridad son muy importantes tanto de manera inalámbrica y vía ethernet las estrategias que se utilizarán serán:

Firewall

Medio de proteger la red de ataques externos o de redes que no son de confianza que son las externas lo que el dispositivo mikrotik cuenta con su propio firewall este manejara reglas necesarias para su buen funcionamiento esta interviene principalmente en la capa de transporte del modelo TCP/IP.

Regla Nro. 1 Permitir conexiones establecidas y relacionadas

Esta regla es fundamental para que las conexiones ya establecidas por los usuarios el firewall no negara las respuestas a sitios ya asociados tengan respuesta más rápida asi reducir ataques externos y al asociar sitios seguros mejorar la optimización de la red ante este tipo de respuestas

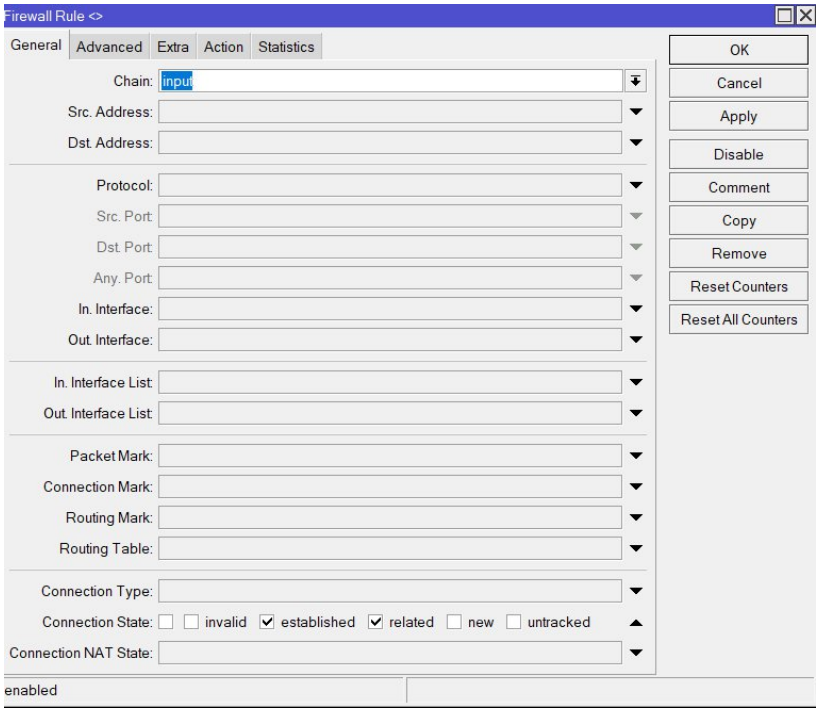


Figura 26. Regla Nro.1 firewall

Se asegura de las conexiones la establecidas en toda la red y asi mejorar en aspectos fundamentales de la red.

Regla Nro. 2 Permitir acceso a winbox desde una ip especifica

Esta regla es una que permite tener una ip específica para acceder desde ese punto siempre y no permanezcan puertas abiertas contra cualquier usuario que pueda ingresar a la red siempre es recomendable realizar una ip para acceder solamente de esa dirección ip.

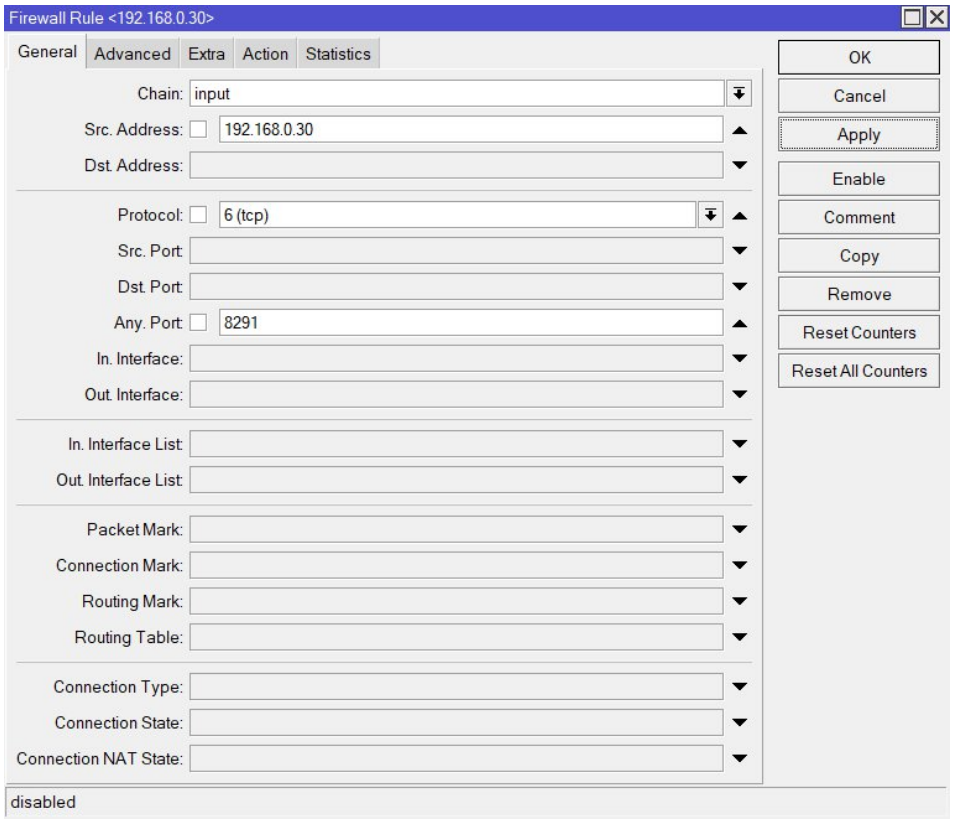


Figura 27. Regla Nro.2 firewall

Regla especifica que solamente desde la ip en este caso la ip 192.168.0.30 solamente tendrá acceso al winbox y el puerto de acceso del winbox es el 8291 y así tener un acceso más personalizado desde una ip en la misma red de la institución.

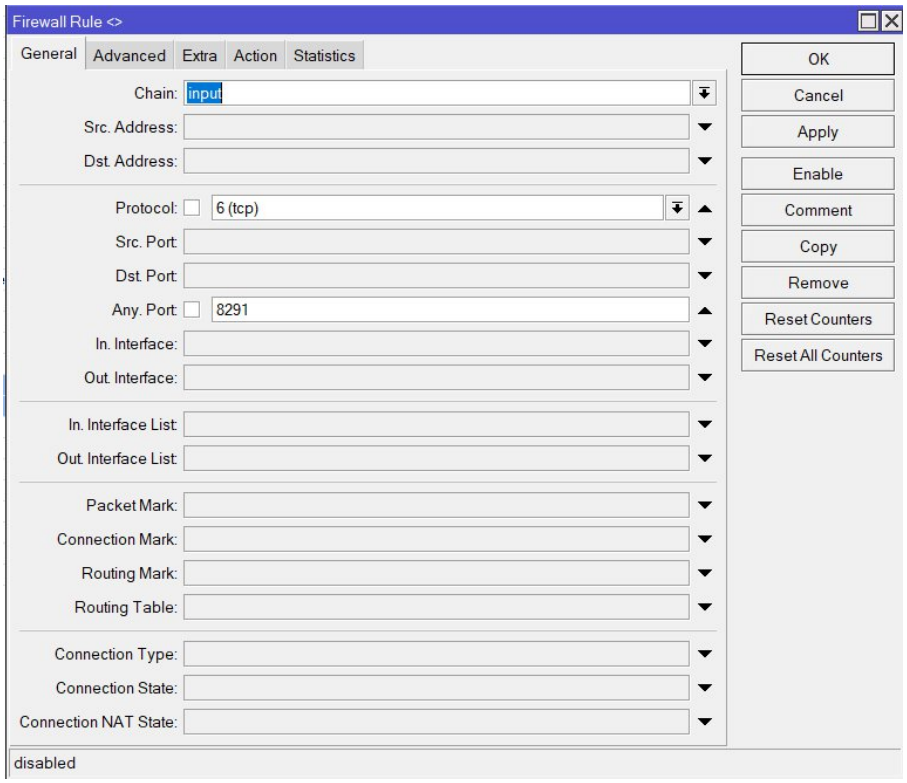


Figura 28. Regla Nro.2 firewall

Esta regla especifica una acción de drop(eliminar) a todo aquella ip a la que intente acceder al puerto 8291 no perteneciente a la anterior regla esta para las demás ips que quieran entrar al winbox.

Regla Nro. 3 Bloquear el acceso mediante SHH

El SHH puede ser seguro a la hora de acceder, pero también suele ser el blanco más común para ataques de fuerza bruta al ingresar de un área de manera remota, es una buena practicar al realizar una red LAN bloquear el acceso por este medio.

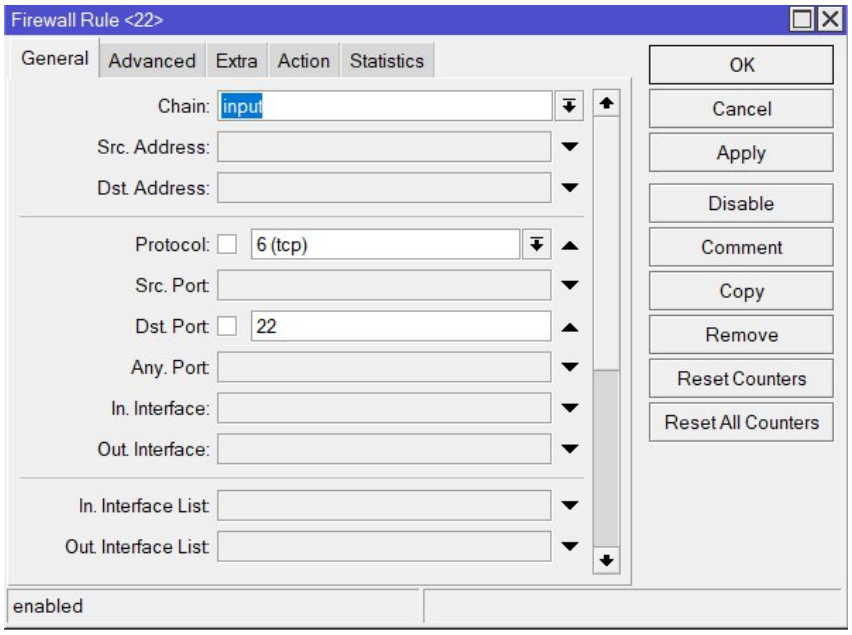


Figura 29. Regla Nro.3 firewall

Esta regla realiza una acción de drop(eliminar) en todo caso de que una ip quiera ingresar por este medio y la lleva a una lista negra de bloqueo.

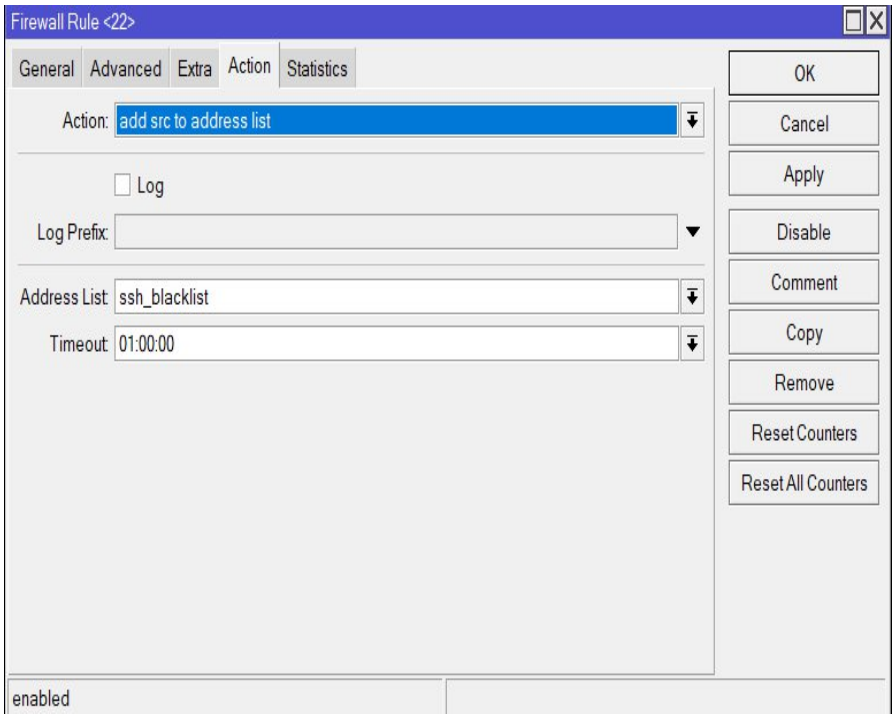


Figura 30. Regla Nro.3 firewall

Esta regla lo que realiza un listado a todas aquellas ips que se encuentren intentando entrar por este medio y tengan más de 3 intentos fallidos las agrega a una lista negra para allí proceder a bloquear el acceso por este medio a esa ip.

Regla Nro. 4 limitar el acceso por ips

El limitar el acceso por ip nos permite un mayor control de todos los dispositivos conectados a la misma al restringir un numero de ips disponibles por cada dirección y así protegerme de ataques que quieran saturar mi dispositivo a base de solicitudes de conexión y así evitar caídas en la red.

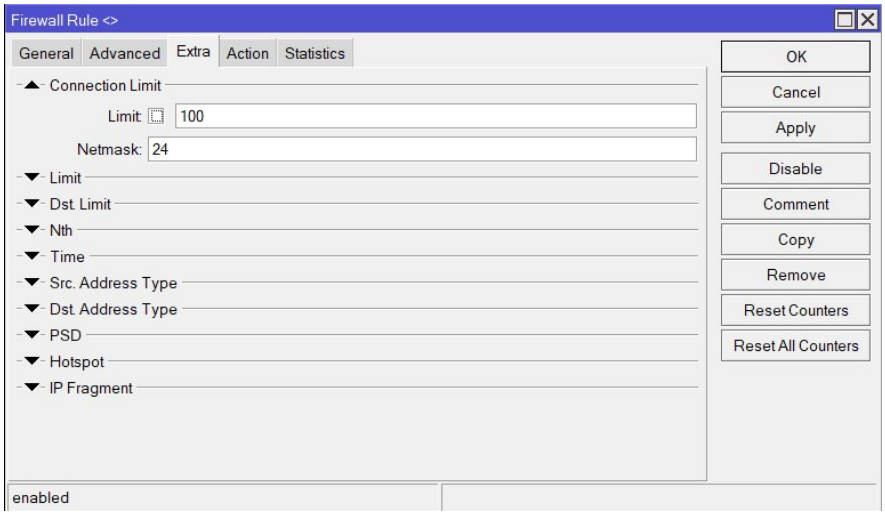


Figura 31. Regla Nro.4 firewall

Limita el número de conexiones a 100 por cada dirección y así evitar ataques masivos de direcciones al pasar el límite establecido en este caso 100 se toma la acción de borrado para quitar todas las conexiones después de la 100.

Regla Nro. 5 limitar el acceso de nuevas conexiones

Esto para evitar ataques masivos en este caso ataques de tipo DDos o ataques que consisten en mandar múltiples solicitudes de conexión de manera simultánea y esto satura al equipo y provoca reinicios constantes.

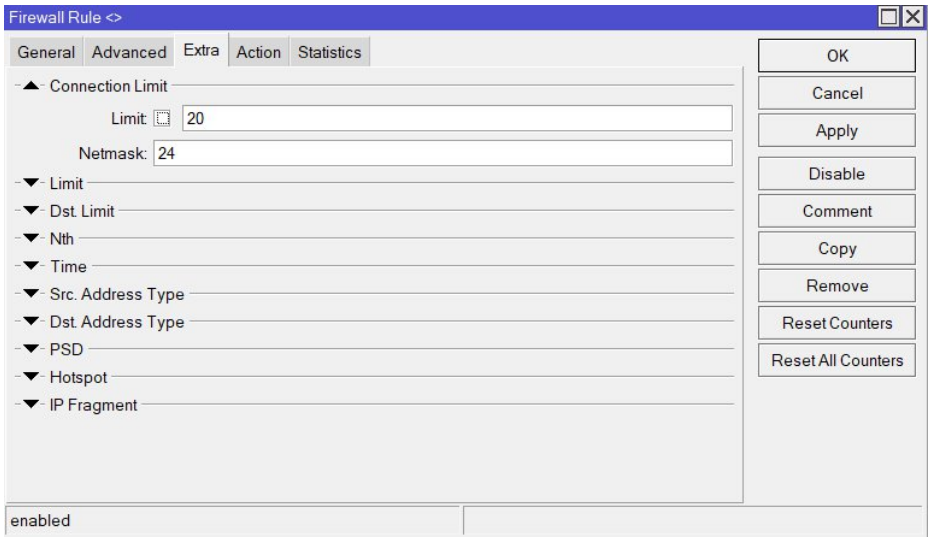


Figura 32. Regla Nro.4 firewall

Limitar el acceso a nuevas conexiones a un límite de 20 un número más limitado ya que un número mayor a 50 de manera simultánea provocaría que el dispositivo colapse con las solicitudes y se reinicie constantemente entorpeciendo el trabajo de la institución.

Administración de usuarios

En lo que respecta a administración de usuarios nos referimos a los usuarios que son capaces de conectarse al equipo mikrotik solo debe tener un acceso al dispositivo con los permisos totales o como lo maneja el mikrotik con acceso full.

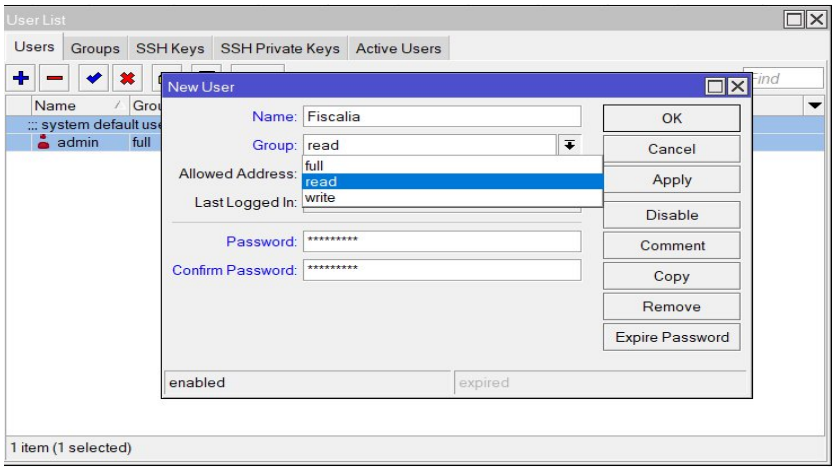


Figura 33. Administración de usuarios Mikrotik

Se logra ver que existen 3 tipos de usuarios por lo general solo se debe contar con un usuario de tipo Full este posee acceso a todo el equipo y puede realizar modificaciones los otros tipos de read, write son usados normalmente en caso de revisión la creación de un usuario de este tipo para que puedan leer, pero sin modificar lo que este hecho.

Bloqueo de tráfico en la red

En lo que respecta al tráfico permitido en la red el dispositivo tiene distintos métodos para restringir el tráfico en la red como ser prerouting, marcado de paquetes, layer7, este método para limitar el consumo y restringirlo en aplicaciones no deseadas.

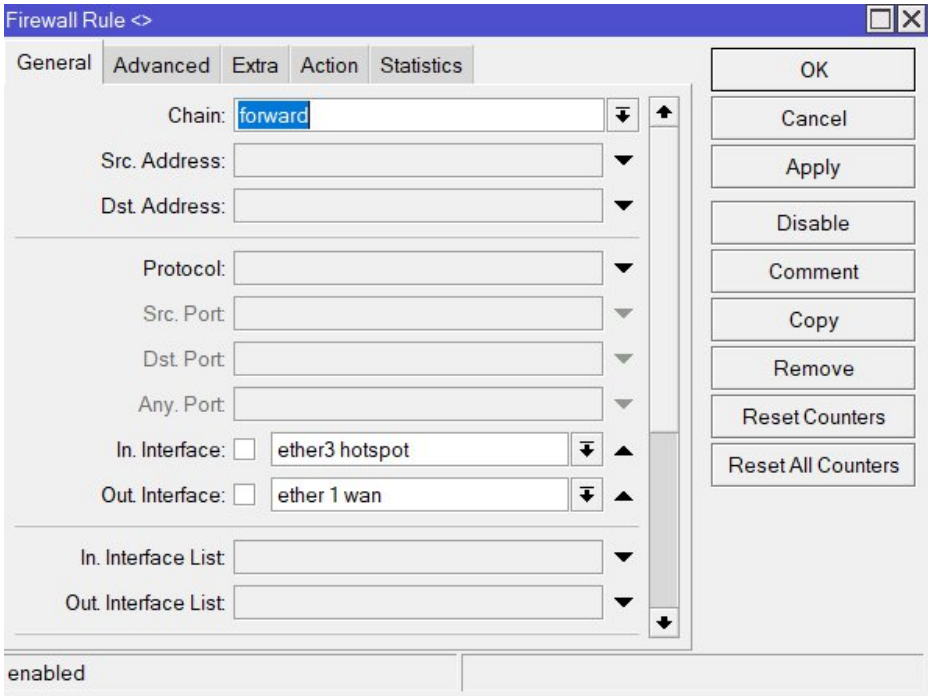


Figura 34. Bloqueo de acceso a apps

En este caso limitar el acceso por la WAN 1 a toda conexión que se realice desde el puerto Ether 3 en este caso el hotspot.

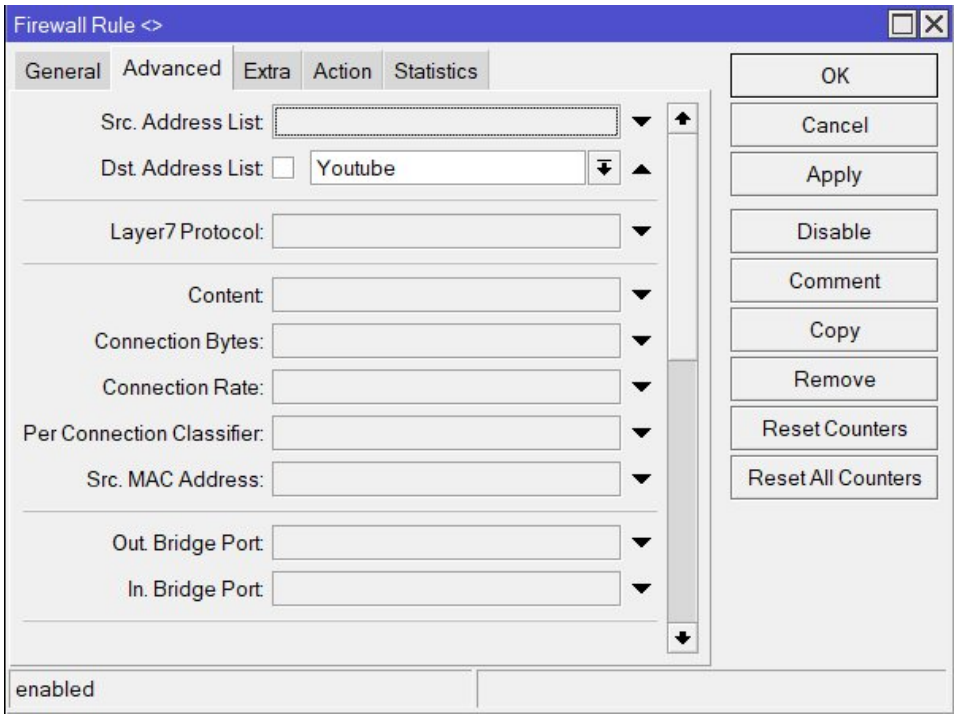


Figura 35. Bloqueo de acceso a apps

Limitando el acceso a YouTube mediante una lista de servidores que proveen el servicio de YouTube y así creada en una lista de direcciones ips bloqueadas.

Seguridad inalámbrica

La gran mayoría empresas de opta por wpa2-personal en este proyecto se optara por hacer uso del dispositivo mikrotik que nos permite tener control del Access point por medio de un redireccionamiento a una página editable en el mikrotik que nos solicita una autentificación por usuario y contraseña por cada usuario esta misma solo puede ser usada por un usuario porque enlaza la Mac del dispositivo al que se conecte primero estos usuarios solo los puede crear quien tenga el acceso al dispositivo mikrotik.

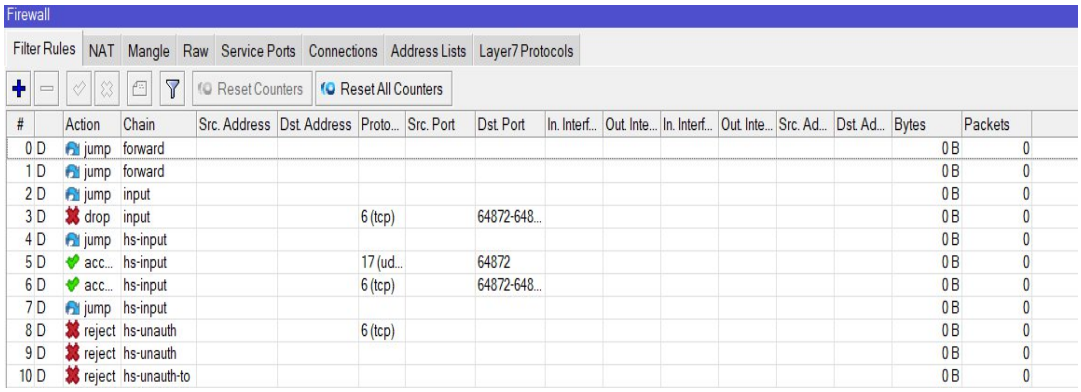


Figura 36. Reglas para el acceso a la red inalámbrica

Reglas para acceder al hotspot que permiten la visualización de la página para acceder mediante el usuario y contraseña estas son reglas que realizan la autentificación los saltos tcp y udp para acceder a la cuenta correspondiente.

II.2.2.5.-Desarrollo de estrategias de administración de red

En lo que se trata de administración de una red un dispositivo mikrotik es una excelente opción el sistema operativo de Mikrotik, es un sistema operativo basado en Unix que ofrece una amplia gama de funciones para administrar redes.

Ofrece distintos servicios muy importantes en la administración de una red como, por ejemplo:

- Gestión de usuarios y dispositivos: RouterOS ofrece una variedad de herramientas para gestionar usuarios y dispositivos en su red. Puede crear cuentas de usuario, asignar permisos a las cuentas de usuario y monitorear el uso de dispositivos. En lo respecta al proyecto esta función se utilizará en los usuarios de la institución que necesitan una conexión inalámbrica esto se llevara a cabo con un orden respectivo deben solicitar un acceso al administrador del dispositivo mikrotik.
- Seguridad de red: RouterOS incluye una variedad de funciones de seguridad para proteger su red de ataques. Puede configurar un firewall, bloquear acceso a puertos no utilizados y utilizar la autenticación de dos factores (2FA). En este proyecto se identificarán puertos no usados para bloquearlos con una regla de entrada en el firewall

puertos por los que se puede entrar un posible intruso.

- Rendimiento de red: RouterOS ofrece una variedad de herramientas para monitorear el rendimiento de su red. Puede recopilar datos sobre el uso de ancho de banda, la latencia y la pérdida de paquetes. Para este proyecto se separado en segmentos de red justamente para aprovechar esta función que es importante para identificar un problema o consumo excesivo por parte de qué tipo de usuario y solucionar problemas con mayor efectividad.

II.2.3.- Fase 3: Desarrollar Diseño Físico

II.2.3.1.- Seleccionar tecnologías y dispositivos para redes empresariales

II.2.3.1.1.-Descripcion de la institución

El proyecto estará diseñado para la institución pública la fiscalía departamental de Tarija esta institución cuenta con 5 plantas en todas las plantas deben estar conectadas al dispositivo mikrotik.

Planta Baja: En la planta baja se encuentra recepción tanto denuncias verbales como escritas, notificadores, fiscalía analista, médicos forenses, conciliadores, bióloga. También se toma en cuenta que en la planta baja se encontrara el gabinete de piso principal que actuara como puesto de telecomunicaciones.

Planta 1: En la planta 1 se encuentran recepciones de casos, fiscales especialistas en áreas antes mencionadas y apoyos como ser psicólogos. También en esta planta se dispondrá de un gabinete de pared pequeño empotrado en la pared fuera del alcance de las personas que distribuirá el servicio a esta área.

Planta 2: En la planta 2 se encuentran lo que son fiscales especialistas en sus áreas personal de apoyo como psicólogos en esta área se contará igualmente con un gabinete de pared pequeño que distribuirá servicio en todo el piso.

Planta 3: En la planta 3 se encuentran lo que son administración, informática también almacenes y recursos humanos esta contara con un gabinete de piso igual al ser un área donde se encontrara informática pensando a futuro pueden disponer de otros equipos en el área.

Planta 4: En la Planta 4 se encuentran los secretarios y los fiscales de más alto rango de la

institución como fiscales de distrito y de materia en esta área se dispondrá de un gabinete de pared pequeño que distribuirá el servicio en todo el piso.

II.2.3.1.2.-Estimación total de la infraestructura física

La estimación de la distancia de la infraestructura se realizó tanto de manera física con un dispositivo de medida como con la ayuda de los planos dispuestos para este trabajo.

Para la estimación que se utilizara la herramienta metro se midió distancia por distancia tomando en cuenta por donde pasara el cableado detallado en el plano de la institución.

Planta baja:

En este caso esta planta contará con un total de equipos de 35 tomas las cuales se midieron de manera manual

Nodos	Distancia (m)
1	25.8
2	25.8
3	21.8
4	21.8
5	21.8
6	21.8
7	21.8
8	21.5
9	21.5
10	19
11	19
12	18.5
13	18.5
14	14.5
15	14.5
16	14.5
17	14.5
18	19.5
19	19.5
20	17
21	17
22	17

23	17
24	17
25	21
26	21
27	21
28	21
29	21
30	21
31	10
32	10
33	10
34	4.5
35	21.5
Total	599

Tabla 11. Medidas de Planta baja

Ahora calcularemos la longitud total del cable a utilizar:

Metros de cable PB: 599m * 1.20 = 718 metros de cable

Planta 1:

En este caso esta planta contará con un total de equipos de 37 tomas las cuales se midieron de manera manual

Nodos	Distancia (m)
1	9.5
2	9.5
3	13.5
4	13.5
5	14.5
6	14.5
7	15.5
8	17
9	18.5
10	13.5
11	13.5
12	18.5
13	18.5
14	18.5

15	15.5
16	15.5
17	15.5
18	13.5
19	17.5
20	17.5
21	19.5
22	20
23	24.5
24	24.5
25	24.5
26	24.5
27	8
28	8
29	12
30	12
31	12
32	12
33	10
34	15.5
35	15.5
36	15.5
37	17.5
Total	565.5

Tabla 12. Medidas de Planta 1

Ahora calcularemos la longitud total del cable a utilizar:

Metros de cable P1: 565.5 metros *1.20 = 678 metros de cable

Planta 2:

En este caso esta planta contará con un total de equipos de 13 tomas las cuales se midieron de manera manual.

Nodos	Distancia (m)
1	2.5

2	4.5
3	4.5
4	8
5	3.5
6	5.5
7	5.5
8	8
9	11
10	11
11	13.5
12	17
13	17
Total	

Tabla 13. Medidas de Planta 2

Ahora calcularemos la longitud total del cable a utilizar:

Metros de cable P2: 111.5 metros *1.20 = 133.8 metros de cable

Planta 3:

En este caso esta planta contará con un total de equipos de 16 tomas las cuales se midieron de manera manual.

Nodos	Distancia (m)
1	4.2
2	8.5
3	8.5
4	10.5
5	17
6	14.5
7	15.5
8	17
9	6
10	14
11	16
12	16
13	18.5

14	18.5
15	24
16	24
Total	

Tabla 14. Medidas de Planta 3

Ahora calcularemos la longitud total del cable a utilizar:

Metros de cable P3: 232.7 metros *1.20 = 279.24 metros de cable

Planta 4:

En este caso esta planta contará con un total de equipos de 10 tomas de distribución con este dato y la distancia real se dispondrá a él calculo

Nodos	Distancia (m)
1	9.5
2	9.5
3	6.5
4	2.5
5	2.5
6	3.5
7	13.5
8	20
9	24
10	24
Total	

Tabla 15. Medidas de Planta 4

Ahora calcularemos la longitud total del cable a utilizar:

Metros de cable P4: 115.5 metros *1.20 = 138.6 metros de cable

En total lo que se llegaría a usar en toda la institución seria de 1950 metros.

II.2.3.1.3.-Descripción detallada de la canalización

En la distribución de para la llegada de los equipos terminales en el presente proyecto se realizó un cableado con canaletas de PVC de 2 tipos esto en el caso del cableado horizontal, en el cableado vertical se utilizará los canales de paso de piso dejados en anteriores instalaciones en el edificio este canal es necesario el paso del cable ya que es una disposición de topología de tipo bus y se contara con un cable troncal de datos.

En lo que se refiere a la canalización por pisos se dispondrá del uso de ellas en las oficinas se dispondrá de un tendido principalmente por la pared y en los pasillos de la institución por temas estéticos se buscaría hacerlo por techo en las oficinas se dispondrá por las paredes ya que no son paredes de concreto sino de una madera en la cual es fácil el paso de los cables a través de ella y llegar de manera más fácil al punto del usuario, Según norma ANSI TIA/EIA 569 que todo equipo de red debe instalarse con una distancia de 30 cm con respecto a uno electrónico y si los conductos eléctricos tiene protección metálica esa distancia reduce a unos 6 cm.

II.2.3.1.4.-Material de canalización

Descripción: CANALETA PLÁSTICA 32 x 12 mm

Canaleta 70x40 mm:

para la canalización se hará material canaletas de 70x40 mm estas se utilizarán como principal salida desde los gabinetes de comunicación ya que llega el máximo grupo de cableado para la distribución a los equipos de salida.

Figura 37. Canaleta de PVC 70x40mm ranurada

Canaleta 40x20 mm:

Este tipo de canaleta se utilizará para la llegada a los equipos al ser más pequeñas con una capacidad de 10 cables se usarán para la distribución dentro de las habitaciones para los dispositivos finales.

Figura 38. Canaleta de PVC 40x20mm

II.2.3.1.5.-Cableado

Para el presente proyecto se optó por utilizar el tipo de cableado UPT para esta instalación, ya que el coste no supone una inversión muy descomunal. El modelo elegido fue:

Modelo de cable UTP Cat.5e

- Velocidad de transmisión de hasta 1 Gbps
- Frecuencia de funcionamiento de 100 a 350 MHz
- Cuatro pares de hilos de cobre trenzados
- Cubierta exterior de plástico

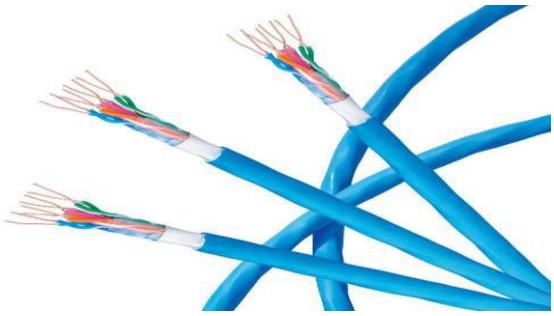


Figura 39. Cableado UTP 4 pares Cat.5e

II.2.3.1.5.1.-Latiguillos de parcheo.

Latiguillo de parcheo de 4 pares sin apantallar (UTP). Desarrollado principalmente para la conexión entre los puestos de trabajo, o para la distribución entre repartidores. Soporta frecuencias de hasta 350 MHz y velocidades de hasta 1000 Mbps.

- Supera las condiciones de Cat. 6 marcados por la norma.
- Alta protección contra las interferencias electromagnéticas.
- Baja propagación de retardo.
- Altos valores ACR y error mínimo de velocidad.

Figura 40. Latiguillo de parcheo

II.2.3.1.5.2.-Rosetas y conectores.

En lo que respecta a las rosetas se instalaran justo en el espacio más conveniente en la pared baja cerca del dispositivo final sean de 4 slot o de 2 slot siempre que sea conveniente.

Conectores:

El conector RJ45 es un tipo de conector modular utilizado para conectar cables de par trenzado a dispositivos de red. Tiene ocho pines o conexiones eléctricas, que se utilizan para conectar los pares de hilos del cable a los terminales del dispositivo.

- Ocho pines o conexiones eléctricas
- Dos tipos principales: macho y hembra
- Se utiliza para conectar cables de par trenzado a dispositivos de red
- Se puede conectar utilizando un crimpador de cables

Figura 41. Conector RJ45

II.2.3.1.6.-Descripción de los armarios de telecomunicaciones

Rack de distribución planta baja

Gabinete de piso es un gabinete principal en este proyecto este será el gabinete más fundamental para su desarrollo por lo que se procuró que este en un lugar bien ambientado y espacioso. Sus dimensiones normalizadas según la especificación EIA-310 permiten que sea compatible con

equipos de cualquier marca o fabricante.

- Altura: La altura de un gabinete de piso se mide en unidades de rack (RU). Un gabinete de 23 unidades tiene una altura de 23 RU
- Ancho: El ancho de un gabinete de piso se mide en pulgadas este es de un ancho de 19 pulgadas.
- Material: Los gabinetes de piso suelen estar fabricados con acero o aluminio.
- Refrigeración: Los gabinetes de piso para servidores suelen tener un sistema de refrigeración incorporado para mantener los equipos a una temperatura adecuada.
- Accesibilidad: Los gabinetes de piso para servidores suelen tener puertas y paneles laterales que se pueden abrir para acceder a los equipos.
- Organización: Los gabinetes de piso para servidores suelen tener bandejas y soportes para organizar los equipos.

Figura 42. Rack de piso 22U

Equipo	Tamaño	Unidades	Total
Ventilador	2U	1	2U
Patch Pannel 24 puertos	1U	1	1U
switch 48 puertos	3U	1	3U
switch 24 puertos	2U	1	2U
Patch Pannel 48 puertos	2U	1	2U
Regleta de fuerza	1U	2	2U
organizador de cable	3U	2	6U
Mikrotik RouterBoard	2U	1	2U
Total	16U	10	20U=19U+24%=23U

Tabla 16. Componentes del Rack planta baja

Rack de distribución planta 1

El gabinete del piso 1 se optó por el uso de gabinete de pared ya que estos dispositivos solo reciben el puerto troncal configurado en un dispositivo switch este gabinete debe regirse según la especificación EIA-310 permiten que sea compatible con equipos de cualquier marca o fabricante.

- Altura: La altura de un gabinete de pared se mide en unidades de rack (RU). Un gabinete de 10 unidades tiene una altura de 10 RU
- Ancho: El ancho de un gabinete de piso se mide en pulgadas este es de un ancho de 19 pulgadas.
- Material: Los gabinetes de pared suelen estar fabricados con acero o aluminio.
- Accesibilidad: Los gabinetes de pared para servidores suelen tener puertas y paneles laterales que se pueden abrir para acceder a los equipos.
- Organización: Los gabinetes de pared para servidores suelen tener bandejas y soportes para organizar los equipos.

Figura 43. Rack de pared 10U

Equipo	Tamaño	Unidades	Total
Ventilador	2U	1	2U
Pach panel 48 puertos	2U	1	2U
Switch de 48 puertos	3U	1	3U
regleta de fuerza	1U	1	1U
Organizador de cable	1U	1	1U
Total	9U	5	9U=8U+24%=10U

Tabla 17. Componentes del Rack planta 1

Rack de distribución planta 2,3,4

El gabinete del piso 2,3,4 se manejará gabinetes de pared ya que estos dispositivos solo reciben el puerto troncal configurado en un dispositivo switch este gabinete debe regirse según la especificación EIA-310 permiten que sea compatible con equipos de cualquier marca o fabricante.

- Altura: La altura de un gabinete de pared se mide en unidades de rack (RU). Un gabinete de 8 unidades tiene una altura de 8 RU
- Ancho: El ancho de un gabinete de piso se mide en pulgadas este es de un ancho de 19 pulgadas.
- Material: Los gabinetes de pared suelen estar fabricados con acero o aluminio.

- Accesibilidad: Los gabinetes de pared para servidores suelen tener puertas y paneles laterales que se pueden abrir para acceder a los equipos.
- Organización: Los gabinetes de pared para servidores suelen tener bandejas y soportes para organizar los equipos.

Figura 44. Rack de pared 8U

Equipo	Tamaño	Unidades	Total
Ventilador	2U	1	2U
Pach panel 24 puertos	1U	1	1U
Switch de 24 puertos	2U	1	2U
regleta de fuerza	1U	1	1U
Organizador de cable	1U	1	1U
Total	7U	5	7U=6U+24%=8U

Tabla 18. Componentes del Rack planta 2,3,4

II.2.3.1.7.- Switches

Un Switch utilizada para conectar equipos, formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

El Switch que utilizaremos serán 2 de 48 puertos y 3 de 24 puertos para conectar los equipos

finales los que se contempló e el análisis de la institución este switch estos dispositivos en los pisos están pensados para una ampliación o en caso de que los fiscales contraten ayudantes no tengan problemas a ingresar a la red de la institución.

Características a que utilizara este switch es:

- Número de puertos: 48 RJ45 Ethernet.
- Velocidad de transferencia de datos: gigabit (10/100/1000).
- Protocolo de interconexión de datos Ethernet, Giga Ethernet.
- Alimentación externa.

Figura 45. Switch de 48 puertos

- Número de puertos: 24 RJ45 Ethernet.
- Velocidad de transferencia de datos: Mbps (10/100).
- Protocolo de interconexión de datos Ethernet, Fast Ethernet.
- Alimentación externa.

Figura 46. Switch de 24 puertos

II.2.3.1.8.-Router

Es un enrutador (router) de la marca MikroTik que ofrece una amplia gama de características y funcionalidades diseñadas para redes pequeñas y medianas, este enrutador se hará uso para toda la distribución y control de los equipos.

Características de equipo:

- Código de Producto RB2011UiAS-RM

- CPU Frecuencia Nominal 600 MHz
- CPU número de núcleos de 1
- Tamaño de RAM 128 MB
- Puertos Ethernet 10/100 5
- Puertos Ethernet 10/100/1000 5
- Voltaje de Entrada 8 V - 30 V
- Dimensiones 214mm x 86mm para PCB
- Sistema Operativo RouterOS
- Temperatura Ambiente Probado -35C a + 65C
- Nivel de Licencia 6
- CPU AR9344
- Puertos SFP Sí
- Tipo de Ranura USB microUSB tipo AB
- Tipo de almacenamiento NAND
- Tamaño de almacenamiento 128 MB
- Puerto Serial RJ45
- Conector de alimentación 1

Figura 47. RouterBoard Mikrotik

II.2.3.1.9.-Access Point

El Access Point dispositivo que establecerá una conexión inalámbrica entre equipos y puedan formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas.

Usos que tendrá:

- Dar acceso a una red inalámbrica a los usuarios que lo requieran.
- Llevar una conexión a internet a donde no había antes, sin perder ancho de banda con repetidores.
- Cubrir grandes áreas con una conexión de calidad, reduciendo el uso de cableado.
- Permite interconexiones entre dispositivos convencionales e inalámbricos si se conecta el

AP al dispositivo mikrotik.

Figura 48. Wireless cAP RouterOs

El proveedor de servicios de internet será la empresa encargada de suministrar a sus clientes una conexión de banda ancha, a través de tecnologías como cable coaxial entre otras, ya sea de servicio como Tigo o Entel eso se dependerá que tipo de paquetes empresariales tenga.

II.2.3.1.10.-Regleta de fuerza

Están fabricadas con un perfil de aluminio de alta calidad preparado para soportar temperaturas elevadas estos componentes normalmente llegan con la compra de un dispositivo como rack o gabinete.

El electroblock suministra alimentación al switch, repetidores y router mikrotik dentro del distribuidor.

Referencia F2109.

- 1U.
- 8 tomas.
- Interruptor bipolar de 16 amperios.

Figura 49. Regleta de fuerza.

II.2.3.1.11.-Organizador de cableado

La función principal de un organizador de cables en un gabinete es mantener los cables ordenados, organizados y debidamente gestionados. Esto es esencial para garantizar un entorno de TI limpio, seguro y eficiente en un gabinete o rack de equipos. Algunas de las ventajas del uso del organizador de cable son: mejora de la ventilación y refrigeración, prevención de enredos y confusión de cables.

Figura 50. Organizador de cables

II.2.3.1.12.-Ventilador rack

En lo que comprende el ventilador es un dispositivo primordial su función es la de mantener una temperatura adecuada y constante dentro del gabinete. Los gabinetes informáticos albergan componentes electrónicos sensibles, como servidores, equipos de red y sistemas de almacenamiento, que generan calor durante su funcionamiento.

Figura 51. Ventilador rack

II.2.3.1.13.-Patch pannel

El uso de un patch pannel puede beneficiar mucho a mejorar la durabilidad de los dispositivos como switchs para reducir las conexiones y desconexiones constantes y evitar el desgasto.

Para este Proyecto se debe disponer de ambos tamaños de patch pannel dependiendo el uso del dispositivo switch de cuanta capacidad será en cada piso en los pisos B,1 se hará uso 48 puertos de capacidad, en los pisos 2,3,4 se usarán de los de 24 puertos. Llevan los cables de datos de los diferentes puestos de trabajo para conectarlos mediante latiguillos de parcheo directamente al switch.

Figura 52. Patch Pannel.

II.2.3.1.14.-Etiquetado de la infraestructura de red

En el sistema de cableado estructurado, es necesario el etiquetado de todo el material que pueda causar confusión y permita facilitar de forma eficaz y eficiente además de ayudar con los temas de mantenimiento de la red.

La duración del etiquetado tiene que ser a ambos extremos y con ayuda de distintas herramientas los elementos que deben ser etiquetados son:

- Cableado horizontal y vertical. Como mínimo ambos extremos del cable, y si es posible en tramos regulares.
- Repetidores y switch.
- Rosetas o tomas de usuario.
- Espacios donde se localicen terminales.
- Asegurarse que las etiquetas no sean visibles para los usuarios

Abreviaturas:

- **Fis:** Sala de Telecomunicaciones.
- **Aux:** Oficina de Mancomunidad de municipios Héroes de la Independencia.
- **Idif:** Oficina de Técnicos.
- **Inf:** Oficina de funcionarios Públicos.

Puerto	RJ45	Puerto	RJ45	Puerto	RJ45	Puerto	RJ45
1	Pb_Fis_1	13	Pb_Aux_9	25	Pb_Aux_21	37	LIBRE
2	Pb_Fis_2	14	Pb_Aux_10	26	Pb_Idif_1	38	LIBRE
3	Pb_Fis_3	15	Pb_Aux_11	27	Pb_Idif_2	39	LIBRE
4	Pb_Fis_4	16	Pb_Aux_12	28	Pb_Idif_3	40	LIBRE
5	Pb_Aux_1	17	Pb_Aux_13	29	Pb_Idif_4	41	LIBRE
6	Pb_Aux_2	18	Pb_Aux_14	30	Pb_Idif_5	42	LIBRE
7	Pb_Aux_3	19	Pb_Aux_15	31	Pb_Idif_6	43	LIBRE
8	Pb_Aux_4	20	Pb_Aux_16	32	Pb_Idif_7	44	LIBRE
9	Pb_Aux_5	21	Pb_Aux_17	33	Pb_Idif_8	45	LIBRE
10	Pb_Aux_6	22	Pb_Aux_18	34	Pb_Inf_1	46	LIBRE
11	Pb_Aux_7	23	Pb_Aux_19	35	Pb_Inf_2	47	LIBRE
12	Pb_Aux_8	24	Pb_Aux_20	36	Pb_Inf_3	48	LIBRE

Tabla 19. Etiquetas de la Planta Baja

Puerto	RJ45	Puerto	RJ45	Puerto	RJ45	Puerto	RJ45
1	Pb_Fis_6	13	Pb_Aux_24	25	Pb_Aux_36	37	Pb_Inf_5
2	Pb_Fis_7	14	Pb_Aux_25	26	Pb_Aux_37	38	LIBRE
3	Pb_Fis_8	15	Pb_Aux_26	27	Pb_Aux_38	39	LIBRE
4	Pb_Fis_9	16	Pb_Aux_27	28	Pb_Aux_39	40	LIBRE
5	Pb_Fis_10	17	Pb_Aux_28	29	Pb_Aux_40	41	LIBRE
6	Pb_Fis_11	18	Pb_Aux_29	30	Pb_Aux_41	42	LIBRE
7	Pb_Fis_12	19	Pb_Aux_30	31	Pb_Aux_42	43	LIBRE
8	Pb_Fis_13	20	Pb_Aux_31	32	Pb_Aux_43	44	LIBRE
9	Pb_Fis_14	21	Pb_Aux_32	33	Pb_Aux_44	45	LIBRE
10	Pb_Fis_15	22	Pb_Aux_33	34	Pb_Idif_9	46	LIBRE
11	Pb_Aux_22	23	Pb_Aux_34	35	Pb_Idif_10	47	LIBRE
12	Pb_Aux_23	24	Pb_Aux_35	36	Pb_Inf_4	48	LIBRE

Tabla 20. Etiquetas de la Planta 1

Puerto	RJ45	Puerto	RJ45
1	Pb_Fis_16	13	Pb_Idif_12
2	Pb_Fis_17	14	LIBRE
3	Pb_Fis_18	15	LIBRE
4	Pb_Fis_19	16	LIBRE
5	Pb_Aux_44	17	LIBRE
6	Pb_Aux_45	18	LIBRE
7	Pb_Aux_46	19	LIBRE
8	Pb_Aux_47	20	LIBRE
9	Pb_Aux_48	21	LIBRE

10	Pb_Aux_49	22	LIBRE
11	Pb_Aux_50	23	LIBRE
12	Pb_Idif_11	24	LIBRE

Tabla 21. Etiquetas de la planta 2

Puerto	RJ45	Puerto	RJ45
1	Pb_Fis_20	13	Pb_Inf_9
2	Pb_Fis_21	14	Pb_Inf_10
3	Pb_Aux_51	15	Pb_Idif_13
4	Pb_Aux_52	16	Pb_Idif_14
5	Pb_Aux_53	17	LIBRE
6	Pb_Aux_54	18	LIBRE
7	Pb_Aux_55	19	LIBRE
8	Pb_Aux_56	20	LIBRE
9	Pb_Aux_57	21	LIBRE
10	Pb_Inf_6	22	LIBRE
11	Pb_Inf_7	23	LIBRE
12	Pb_Inf_8	24	LIBRE

Tabla 22. Etiquetas de la planta 3

Puerto	RJ45	Puerto	RJ45
1	Pb_Fis_22	13	LIBRE
2	Pb_Fis_23	14	LIBRE
3	Pb_Fis_24	15	LIBRE
4	Pb_Aux_58	16	LIBRE
5	Pb_Aux_59	17	LIBRE
6	Pb_Aux_60	18	LIBRE
7	Pb_Aux_61	19	LIBRE
8	Pb_Aux_62	20	LIBRE

9	**Pb_Aux_63**	**21**	**LIBRE**
10	**Pb_Aux_64**	**22**	**LIBRE**
11	**LIBRE**	**23**	**LIBRE**
12	**LIBRE**	**24**	**LIBRE**

Tabla 23. Etiquetas de la planta 4

II.2.4.- Fase 4: Probar, optimizar y documentar diseño

II.2.4.1.- Probar el diseño de red

En el desarrollo de las pruebas para el diseño de red se realizó la misma configuración en un equipo mikrotik con el que se contaba la empresa para tomar en cuenta su uso antes de pasar al dispositivo grande ubicado en la fiscalía.

Otra manera de realizar pruebas es que el dispositivo mikrotik se puede manejar en programas como VirtualBox para hacer correr su ISO una de las desventajas de hacer correr de este modo es que la licencia llega solo válida para el uso de 24 horas con el dispositivo en uso para realizar la configuración de este modo es un poco complicada pero de manera de practicar y aprender de su uso contribuyo muchísimo en para los primeros pasos en este dispositivo.

En el dispositivo mikrotik mini se tomó en cuenta trabajar en el desarrollo del bloqueo de puertos, en la disposición del uso de hotspot y a configurar las vlans principalmente estos aspectos.

Figura 53. Mikrorik RB750

- Firewall para el desarrollo del firewall se analizó puertos de bloqueo por los cuales se pueda penetrar la integridad de la institución para ser aprendió que puertos como el 21,22,23,8729,8728 son puertos que al realizar la configuración que se debe desactivar porque estos puertos elevan el consumo de CPU en el dispositivo y permite que múltiples intrusos acceder al mikrotik.

- En la disposición del uso de hotspot se realizaron pruebas como la conexión correcta de los dispositivos inalámbricos verificar la carga y la descarga de internet si le llega de manera correcta probar con la carga de video conferencias principalmente y con la página de la fiscalía la Jl1 y Jl2 y realizar el bloqueo de aplicaciones que consumen elevado ancho de banda.
- En lo que respecta a la disposición de las vlans para la institución se tomó en cuenta en aplicarlo si en el dispositivo switch o en el dispositivo miktotik se probó en ambos para ver en cual corría de mejor manera y tomar en cuenta si es viable hacerlo de ese modo.

En la etapa de probar el diseño surgen muchos fallos o es un ensayo de prueba y error por lo que para esta etapa se realizó arto el uso de backup cargarlo y volverlo a cargar en caso de que se llegue a un error que no se llegue a una solución rápida por ejemplo cuando aplicas las reglas algunas de las reglas limitan el acceso o pueden llegar a saturar el equipo de manera drástica por ende se optaba por reiniciarlo de fábrica y de allí cargar el backup hecho previamente.

El uso del dispositivo mikrotik se optó por este dispositivo al tener bastantes libros dedicados a su uso y por recomendación del encargado o tutor de ayuda para la realización de este proyecto.

II.2.4.2.- Optimizar el diseño de red

En esta el desarrollo de la optimización de la red una vez hechas las pruebas se tomó en cuenta en esta parte se buscará corregir o definir porque tipo de configuración de red se tomará en el dispositivo mikrotik.

En lo que respecta a la optimización de la red se contempló en primer lugar el dispositivo mikrotik ya que este controlara todas las funciones de la red.

- En lo que respecta al firewall con lo realizado del bloqueo de puertos y activado tanto si es necesario o no solo si se usara esta función.
- En lo que comprende al desarrollo inalámbrico con el hotspot para optimizar se tomó en cuenta mucho lo que viene siendo el bloqueo de aplicaciones de streaming y en el desarrollo de la ventana para registro de los usuarios que se conectaran en la red también en corregir los errores que se produjeron al probar los host inalámbricos usando de

prueba a los fiscales y a los usuarios de la institución para ver si tenían problemas ya que se presentaron algunos dispositivos de marcas en particulares que no lograron conectarse a la red

- En la configuración de las vlans se optó por realizar la configuración en el equipo mikrotik no se cuenta con ningún problema una vez hecho la prueba el dispositivo soporta 24 horas continuas en funcionamiento con la configuración y no presenta interrupciones en la calidad del internet.

II.2.4.3.- Documentar el diseño de red

En esta parte se tomará en cuenta los aspectos que se tuvieron en cuenta en el diseño de la red como la simulación y todos lo que viene siendo el orden de los equipos de red en la distribución del gabinete y la distribución de los equipos por toda la institución.

II.2.4.3.1.- Red detallada por capas

En lo que respecta a este punto se mostrara según el modelo de tcp/ip que aspectos del proyecto intervienen en cada capa de la siguiente manera:

Capa de Acceso a la Red (Capa de Enlace)

En esta capa, es responsable de la transferencia de los datos de manera física principalmente son el cableado las señales inalámbricas también interceden los equipos.

- Todos los equipos que interceden cableado conexión con los equipos y medios de manera física que interceden en el proceso de la transmisión de paquetes.
- Cableado de cat 5e en el cableado horizontal, backbone cableado de cat 6 para cableado vertical.
- Señales wifi que replican el hotspot de tipo inalámbrica.
- Conexión de una dirección ip a una maquina física fija.

Capa de Internet (Capa de Red)

En esta capa, Se encarga del direccionamiento, enrutamiento y encaminamiento de los paquetes de datos desde el origen hasta el destino.

- Configurar el enrutamiento inter-VLAN para permitir la comunicación entre las diferentes VLAN para llegar de un punto a otro punto.
- Implementar el enrutamiento entre las dos conexiones WAN para lograr el balanceo de carga y la redundancia.

Capa de Transporte

La capa de transporte se enfoca en la entrega confiable de datos. En este nivel, podrías configurar reglas de calidad de servicio (QoS) y optimización de rendimiento.

- Implementar QoS para priorizar el tráfico de fiscales e informática, garantizando un buen rendimiento para estas áreas críticas.
- Configurar reglas de firewall a nivel de transporte para filtrar o priorizar el tráfico.

Capa de Aplicación

La capa de aplicación se refiere a las aplicaciones y servicios de red que los usuarios utilizan. Aquí es donde se aplican las políticas de seguridad y se optimiza el rendimiento.

- Configurar reglas de firewall a nivel de aplicación para bloquear el acceso a redes sociales y otros sitios web no deseados.
- Asegurarse de que las aplicaciones utilizadas por fiscales, asistentes de fiscales y otros se ejecuten de manera eficiente y segura.
- Acceso al servicio de manera inalámbrica o hotspot.

II.2.4.3.2.- Simulación del diseño de red

La distribución del diseño de simulación se aprecia la topología de red que se visualizara ya que en la implementación de la red se verá todo lo que viene siendo el aspecto de configuración de la red.

Figura 54. Gabinete de planta baja

En la imagen se logra visualizar como se dispondrán los equipos en la planta de abajo que será la que reciba los servicios de internet justo en el puerto WAN es decir el puerto 1 del dispositivo mikrotik.

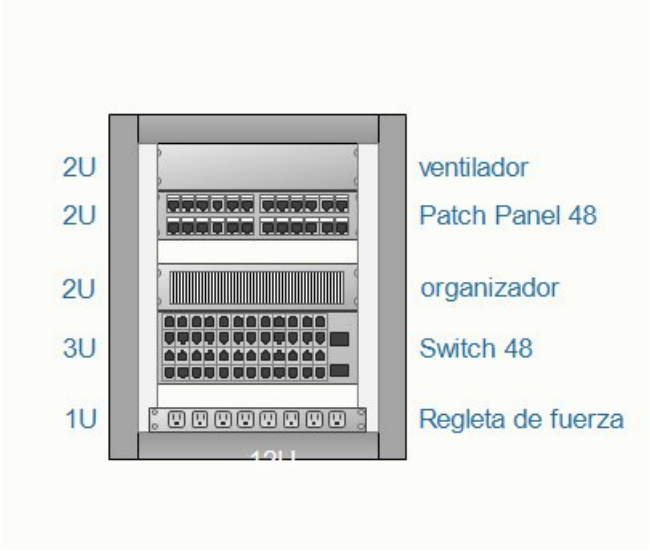


Figura 55. Gabinete de planta 1

En la se logra ver la distribución en el gabinete de la planta 1 en esta llegara un cable troncal que llegara al dispositivo switch para luego redireccione a los dispositivos finales.

Figura 56. Gabinete de planta 2,3,4

En la se logra ver la distribución que tendrán los gabinetes de la planta 2,3,4 se verá un cable troncal que llegara al dispositivo switch para luego redireccione a los dispositivos finales.

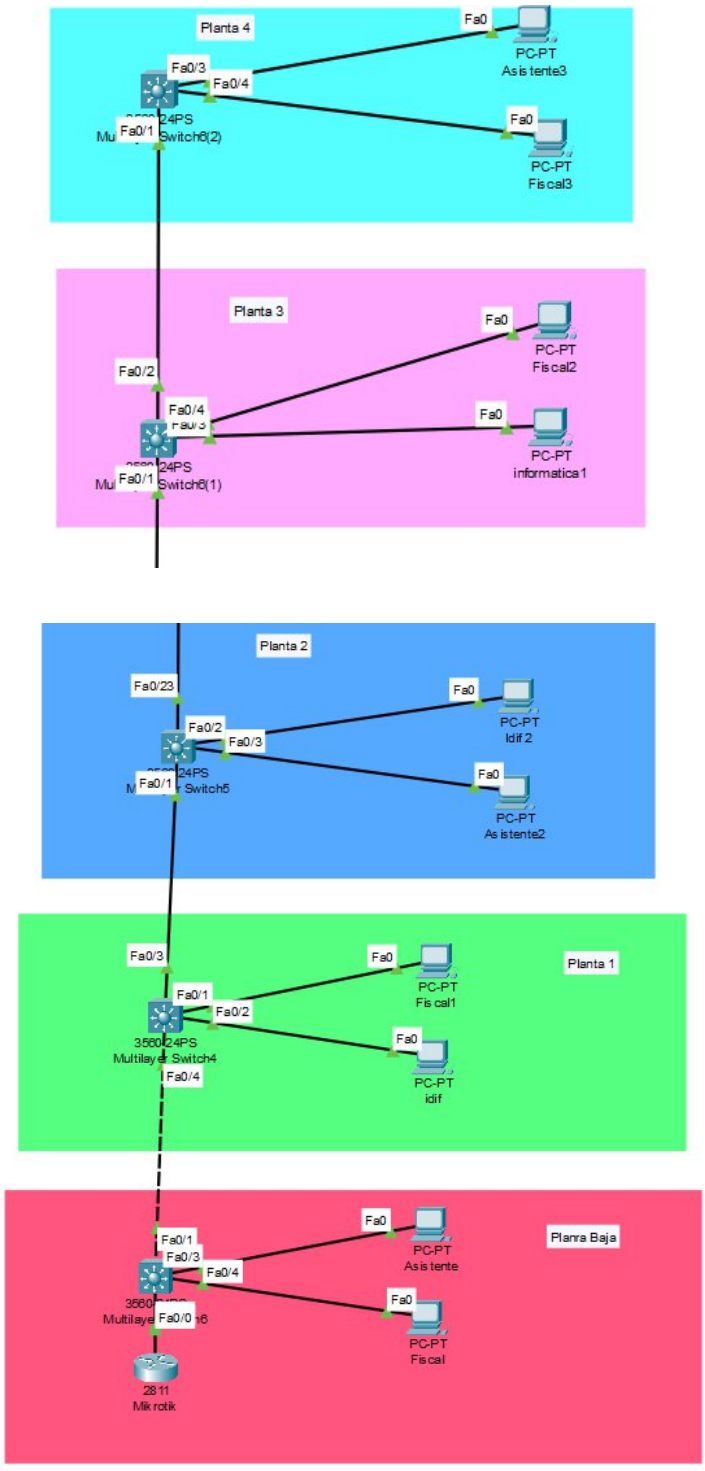


Figura 57. Simulación en Packet Tracer de la red

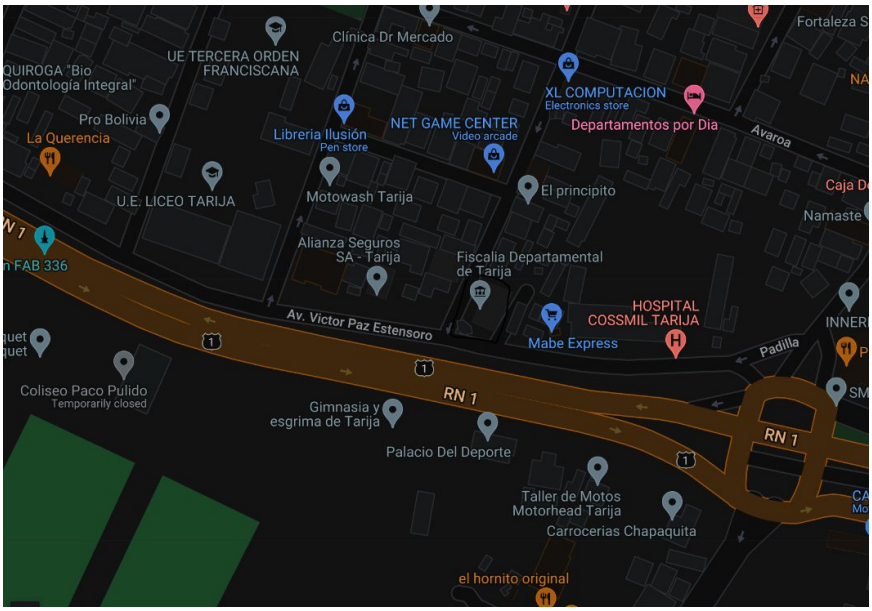


Figura 58. Ubicación de la institución

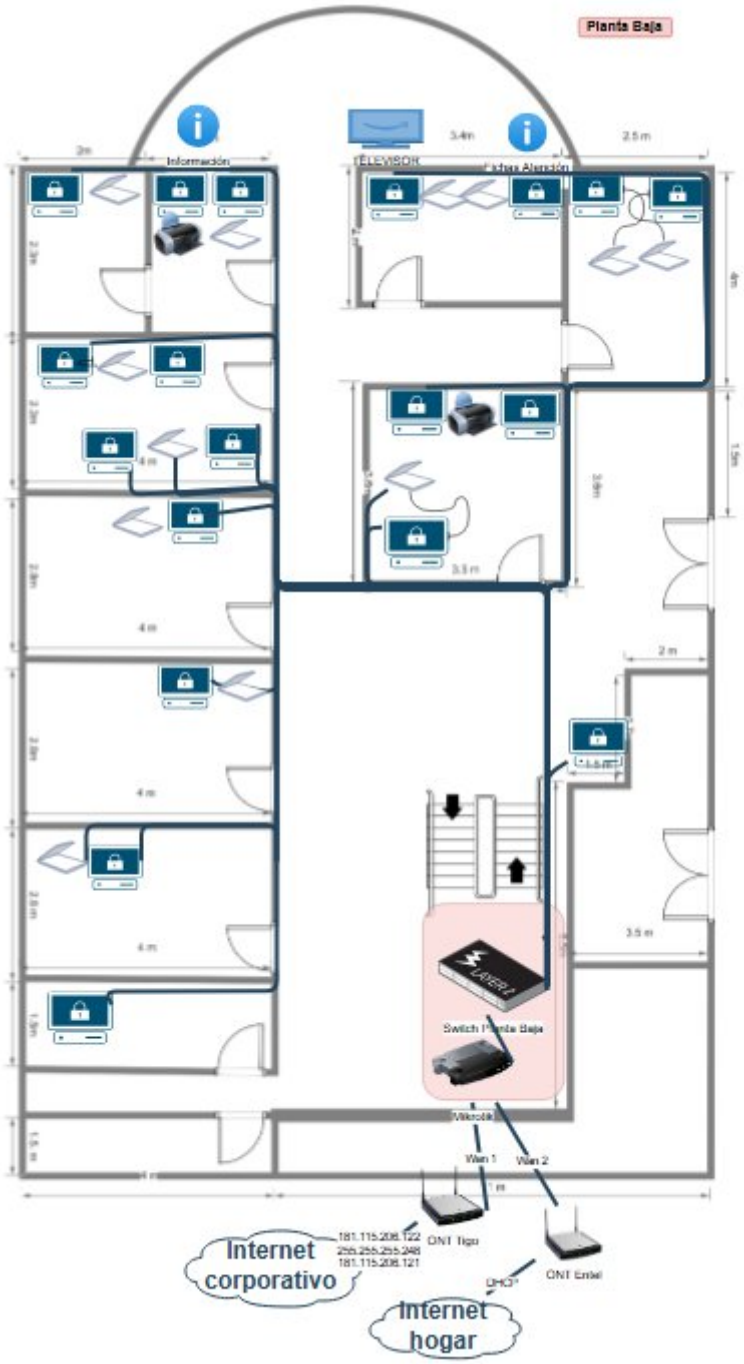


Figura 59. Distribución de la planta baja

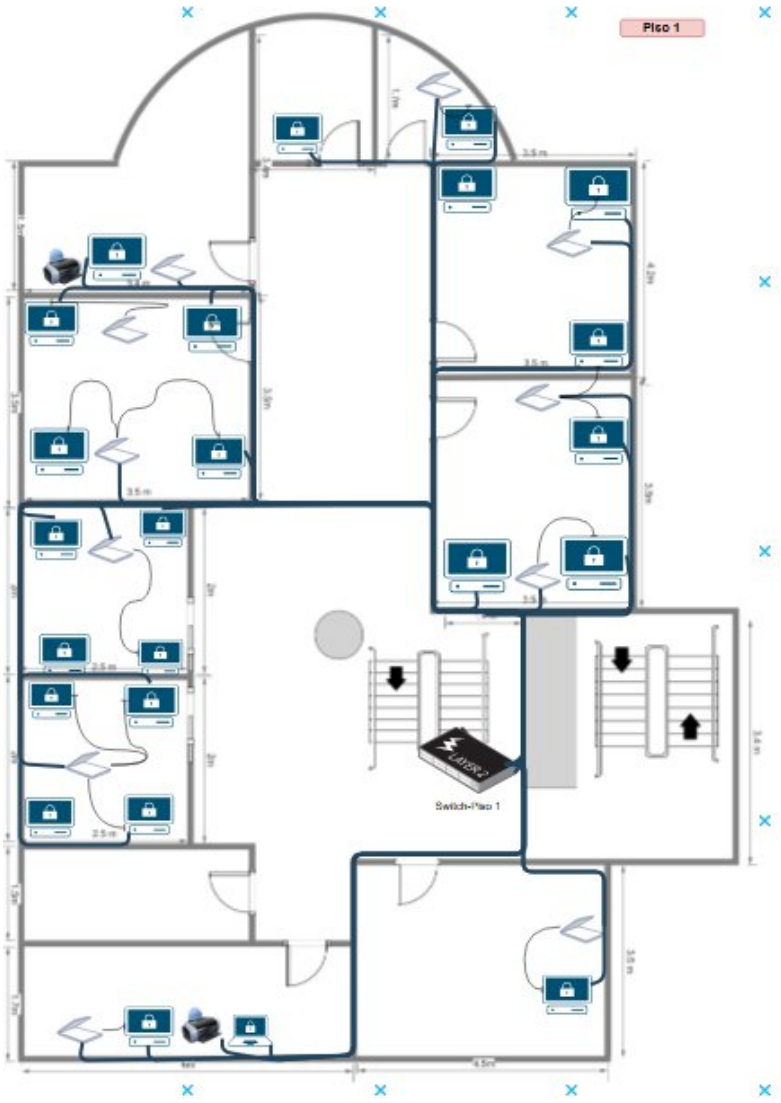


Figura 60. Distribución de la planta 1

Figura 61. Distribución de la planta 2

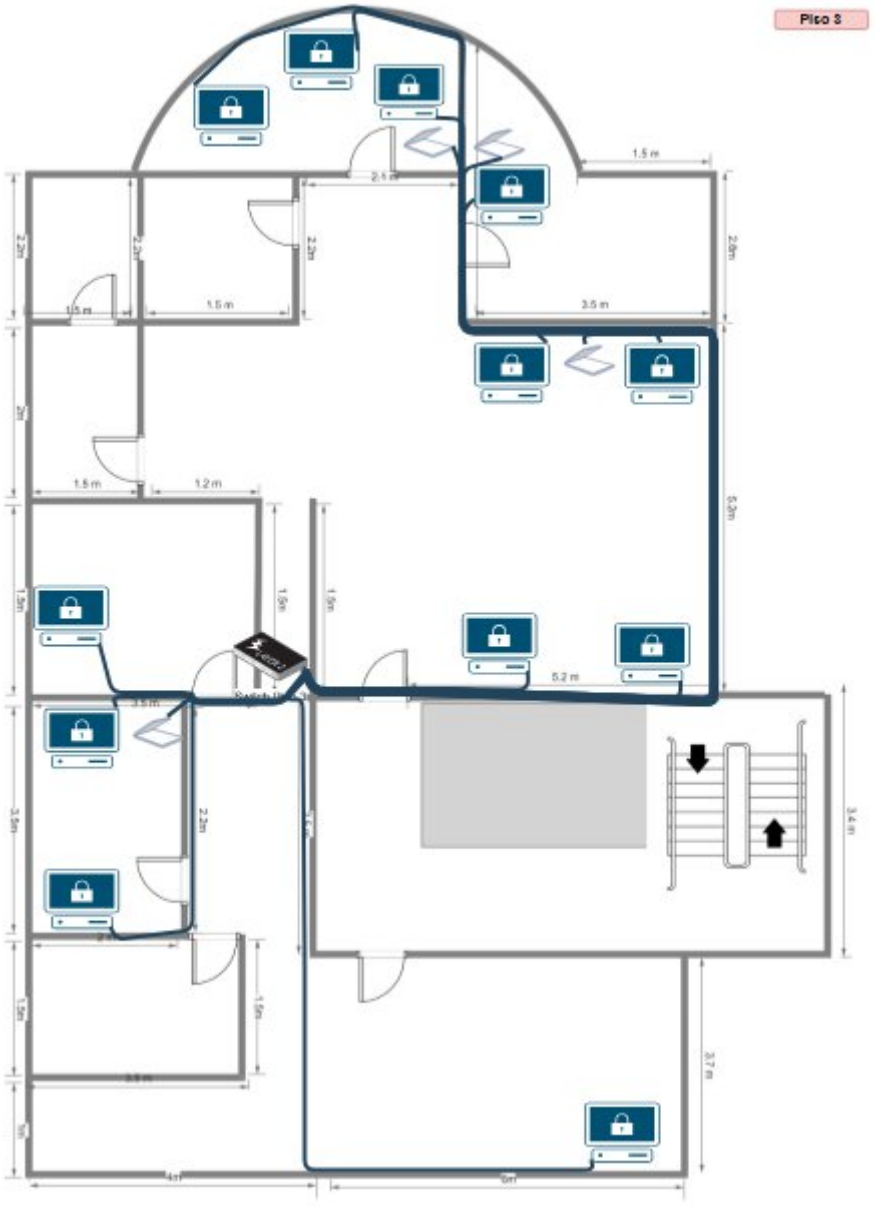


Figura 62. Distribución de la planta 3

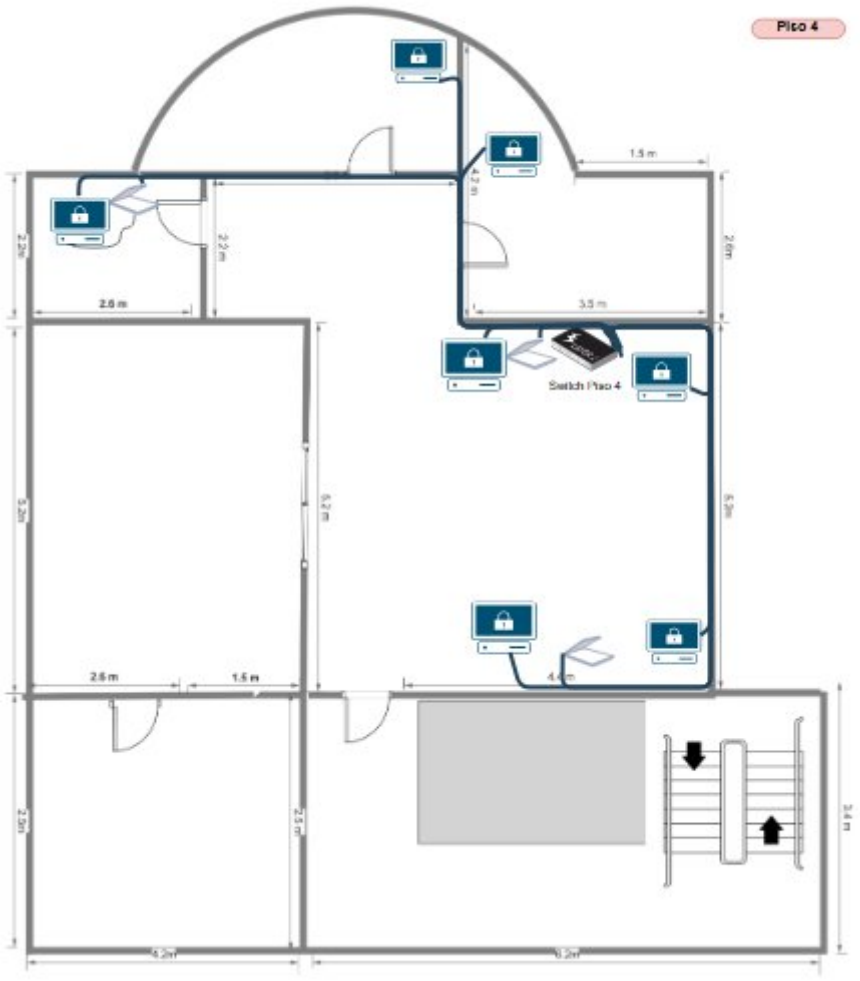


Figura 63. Distribución de la planta 4

II.2.4.3.3.-Descripcion de dispositivos finales

Lenovo ThinkCentre M900 SFF

Características:

Marca: Lenovo **Memoria RAM:** 8 GB **Almacenamiento:** 1Tera **Procesador:** Intel Core i7
Velocidad de la CPU: 4.0 GHz
Sistema Operativo: Windows 10 (1 año de Garantía)
Conector a Ethernet: Incluido **Tarjeta de Video**: 4GB
Teclado y Mouse: Incluido
Monitor: Pantalla Plana Led incluido

Figura 64. Computadora de escritorio

Impresora Multifuncional Inalámbrica EcoTank L805

Características:

La Impresora multifuncional 3 en 1 Epson EcoTank L805 Imprime hasta 3000 páginas en negro o 6000 páginas a color Conectado con WiFi, celulares y tablets

Capacidad de bandeja de 120 hojas.

Figura 65. Impresora

II.2.5.- Fase 5: Implementar y probar la red

II.2.5.1.- Cronograma de implementación de la red

N.º	Actividad	N.º días	Fecha inicio	Fecha Finalización	S 1	S 2	S 3	S 4	S 5
1	Implementar los servicios requeridos.	**25**	**05/08/2023**	**07/08/2023**	**X**	**X**	**X**	**X**	**X**
1.1	Conexión del cableado Estructurado de la red	**6**	**08/08/2023**	**15/08/2023**	**X**	**X**			
1.2	Configuración de los equipos de Computación a la Red por cableado	**4**	**16/09/2023**	**21/09/2023**		**X**	**X**		
1.3	Configuración del equipo mikrotik	**30**	**01/09/2023**	**30/09/2023**			**X**	**X**	
1.4	Configuración de los dispositivos distribuidores e inalámbricos	**29**	**02/10/2023**	**30/10/2023**				**X**	
1.5	Verificar cumplimiento de los requisitos	**5**	**03/11/2023**	**07/11/2023**					**X**

Tabla 24. Cronograma de Implementación

II.2.5.2.- Implementación de la red

Para la implementación del rediseño de red tomando en cuenta la topología antes vista para la implementación principalmente se configurará el dispositivo Mikrotik con la entrada del servicio de internet correspondiente.

II.2.5.2.1.- Mikrotik

En lo que se refiere al mikrotik para la implementación del equipo se debe configurar como una salida a internet siempre en el puerto eth1 en este caso con el uso de una ip privada dada por la empresa de telecomunicaciones.

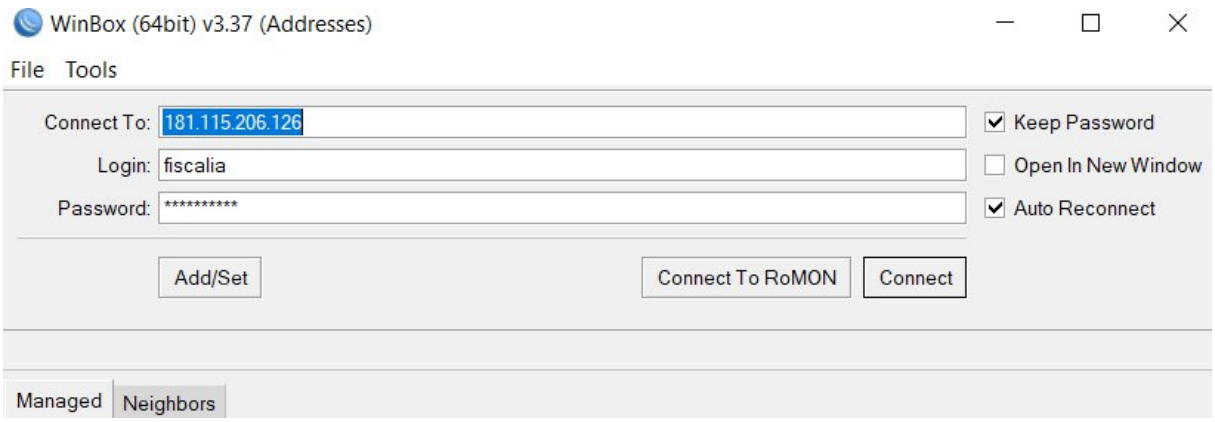


Figura 66. Pantalla de acceso al mikrotik

En esta imagen se muestra que para el acceso al equipo principal en esta se logra ver la ip privada proporcionada por el servicio de internet una vez en esta fase el dispositivo mikrotik una vez conectado agarra una ip de manera automática y una vez dentro del equipo puede editarse la dirección.

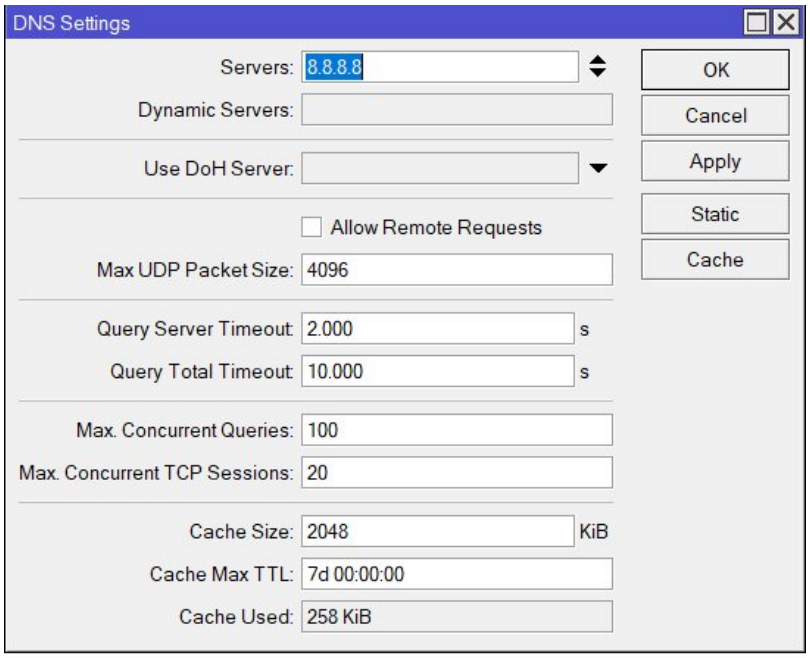


Figura 67. Pantalla de DNS

En esta pantalla es una de las opciones fundamentales para el acceso a internet ya que en este caso lo fundamental es tomar la ip de un servidor de tipo publica para que el dispositivo tenga acceso a internet.

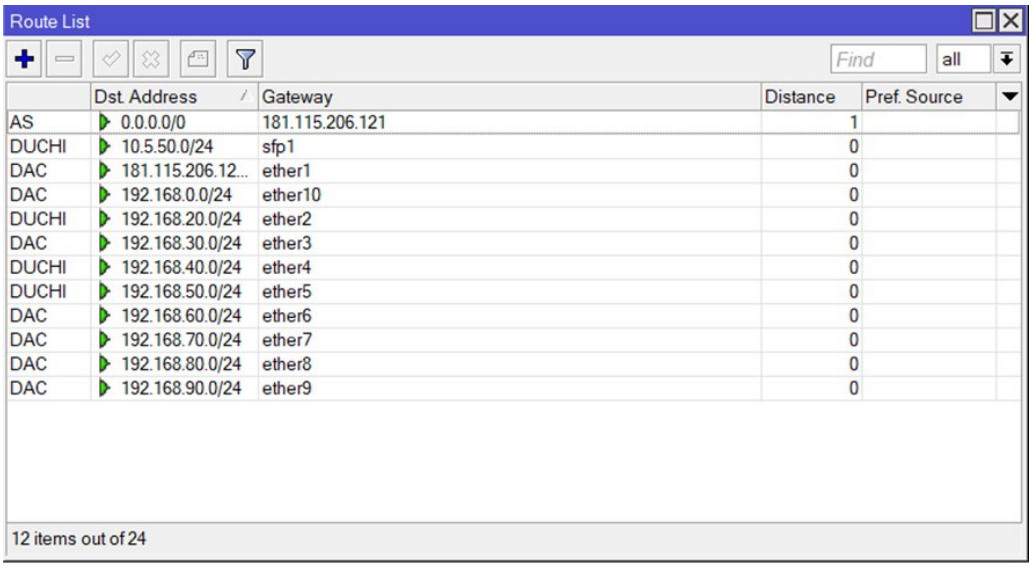


Figura 68. Pantalla de gateway

Esta pantalla es fundamental para el dispositivo mikrotik porque en este apartado se le da acceso a las ip configuradas en el equipo para que puedan tener salida por la ip privada en este caso.

Con estas configuraciones realizadas en el dispositivo mikrotik en estos apartados puede dar funcionamiento al primer paso de la red.

II.2.5.2.2.- Servicio DHCP

Para el servicio de DHCP se realizará la configuración mediante el dispositivo mikrotik principalmente con las direcciones de tipo ethernet ya que la configuración de las troncales para se realizará en el mismo dispositivo mikrotik.

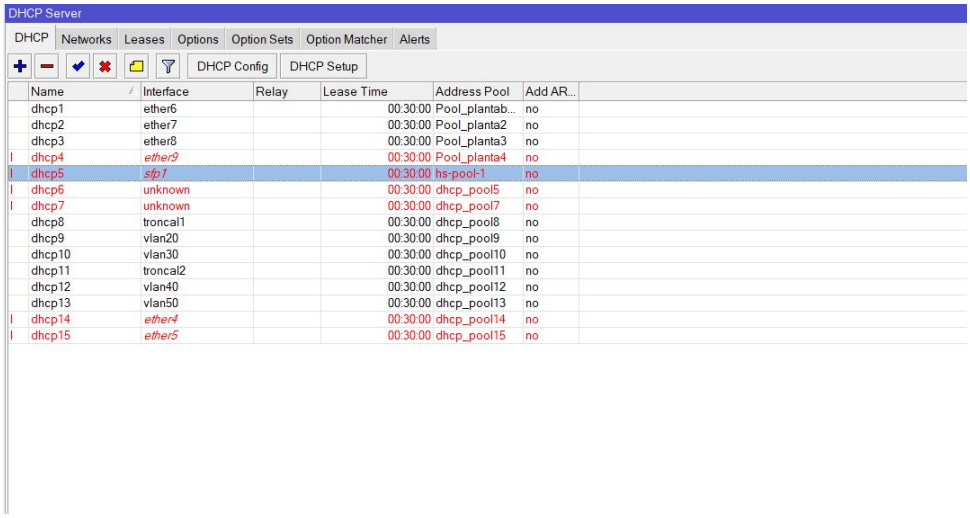


Figura 69. DHCP

En esta pantalla de elaboración propia se logra apreciar la configuración de las troncales y asi mismo se le asignan las vlans a cada troncal como se ve ordenada cada troncal se le asignara 2 vlans.

Para el apartado inalámbrico se realizó la configuración de la misma manera, pero en un apartado en que la configuración de los inalámbricos debe ser unitaria por ende se realiza la configuración por ethernet 6,7,8 cada puerto controlara únicamente un dispositivo inalámbrico.

Figura 70. Puerto de alimentación Cap Mikrotik

En el caso de los dispositivos inalámbricos para su conexión en el apartado de Data tiene 2 salidas una para acceder de manera directa al puerto configurado en el mikrotik y otra entrada en modo de energía directamente conectado esto para abastecer el dispositivo hotspot.

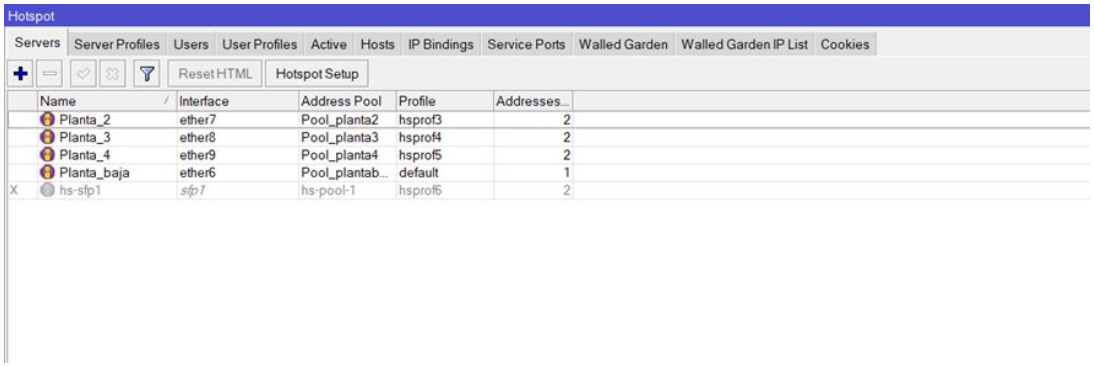


Figura 71. Hotspot

En este apartado se logra ver los puertos del dispositivo mikrotik configurados de manera que puedan brindar el servicio de hotspot de manera inalámbrica.

II.2.5.2.3.- Distribución del cableado

Con esta configuración dispuesta en el dispositivo mikrotik se procedería en la adaptación del ambiente en este caso la implementación se realizó solo en la planta baja para la disposición de cómo se ubicarán los equipos en el cableado horizontal.

Figura 72. Disposición de Cableado Horizontal

En la siguiente imagen de elaboración propia se logra apreciar por donde se realizará la distribución de los equipos en la planta baja por donde se distribuye el cableado horizontal y en que parte de ubicaran los equipos exactamente.

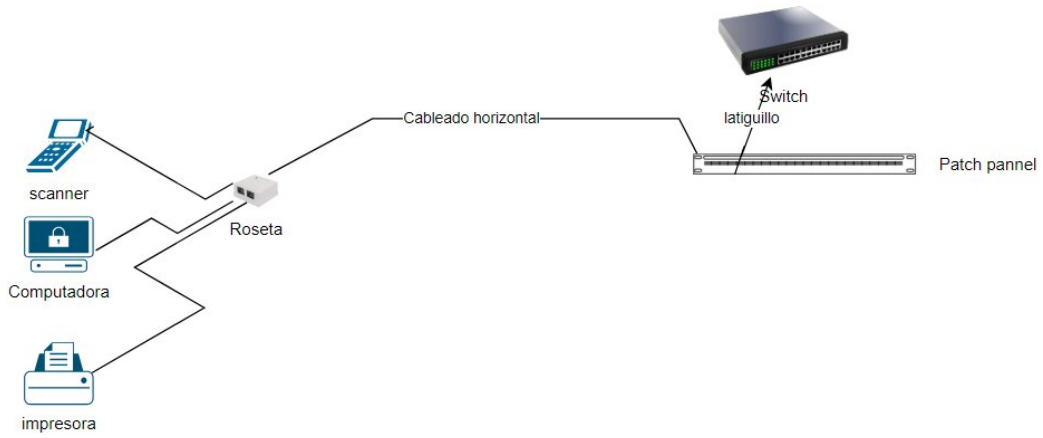


Figura 73. Como se realizará el tagget

En esta imagen se puede ver el proceso por el cual se montará el cableado horizontal en cada uno de los hosts a los cuales se distribuirá red en todas las plantas desde el gabinete de piso.

II.2.5.2.4.- Pilas de pruebas

En lo que respecta a las pruebas realizadas en la implementación de la red fueron realizadas con la muestra de la planta baja de la institución.

Prueba de funcionamiento

En lo que respecta al funcionamiento del equipo soportar tanto ethernet como inalámbricamente el equipo en su momento de arranque puede soportar un funcionamiento las 24 horas del dia esto controlado mediante winbox en su momento de configuración ingresar al equipo a altas horas de la noche el dispositivo respondía de manera satisfactoria y en funcionamiento en horas de 10 am y las 3 pm donde el trafico de red era mayor el equipo solo alcanzaba el 23% de su funcionamiento con 37 equipos conectados de manera ethernet y aproximadamente 25 equipos inalámbricos conectados.

Prueba de rendimiento

Al recibir un ataque de tipo Doss el dispositivo mikrotik respondió de manera satisfactoria en una carga de 200 usuarios y al sobrepasar el limite el dispositivo paso su rendimiento de CPU a

un 80% para proceder a apagarse

Prueba de Seguridad

En lo que respecta a seguridad se probo cada una de las reglas aplicando lo que deberían hacer en el caso de las reglas del firewall al ser reglas aplicadas de conocimientos previos de libros y internet funcionaron de manera satisfactoria.

Al momento de la creación de la regla para bloqueo de redes sociales el punto analizado fue YouTube al realizar un bloqueo convencional no se logro solucionar nada al ser teléfonos inteligentes capaces de ocultar al conectarse lograban tener acceso a la aplicación en un momento por eso se hizo uso de herramienta una pagina web para lograr ver las direcciones ips que maneja YouTube y allí recién restringir el acceso mediante las direcciones ips.

En termino de seguridad sobre el uso de contraseñas seguras tanto para ingresar de manera inalámbrica como al dispositivo mikrotik en lo inalámbrico se hizo uso de carnet de identidad.

Ejemplo: RoLo^Garec10661595

En caso del dispositivo mikrotik solo el acceso mediante una cuenta y con la contraseña dada por el encargado de la fiscalía departamental.

Ejemplo:BocA**479800

II.2.6.- Fase 6: Monitorear y optimizar la red

II.2.6.1.- Operación de la red en producción

En lo que presenta a este punto se tomara en cuenta lo realizado durante la configuración esta será la planta baja y los dispositivos de red inalámbricos por lo que se tomara en cuenta las funciones que posee el mismo mikrotik.

II.2.6.1.1.- Rendimiento del equipo en funcionamiento

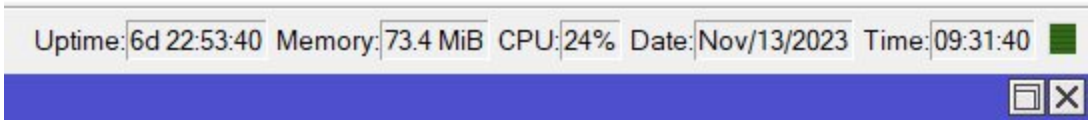


Figura 74. Visualización del rendimiento de la red en producción

En la imagen se logra ver que una vez hecha toda la configuración a la fecha 13 de noviembre la red solo consume un 24% del rendimiento del equipo mikrotik con todas las funciones puestas actualmente. Otra manera de ver la satisfacción con el funcionamiento es el uso prolongado de algunos usuarios al servicio de red inalámbrico también se toma en cuenta que aunque los equipos se encuentren en la red habrá momentos en donde los dispositivos saquen el máximo rendimiento de la red llegando a alcanzar un 50% de la potencia del equipo estas siendo horas de más trabajo laboral.

II.2.6.1.2.- Diseño de hotspot

La pantalla inicial para login para los usuarios inalámbricos mikrotik nos proporciona un modelo funcional base que cumple la función inicial.

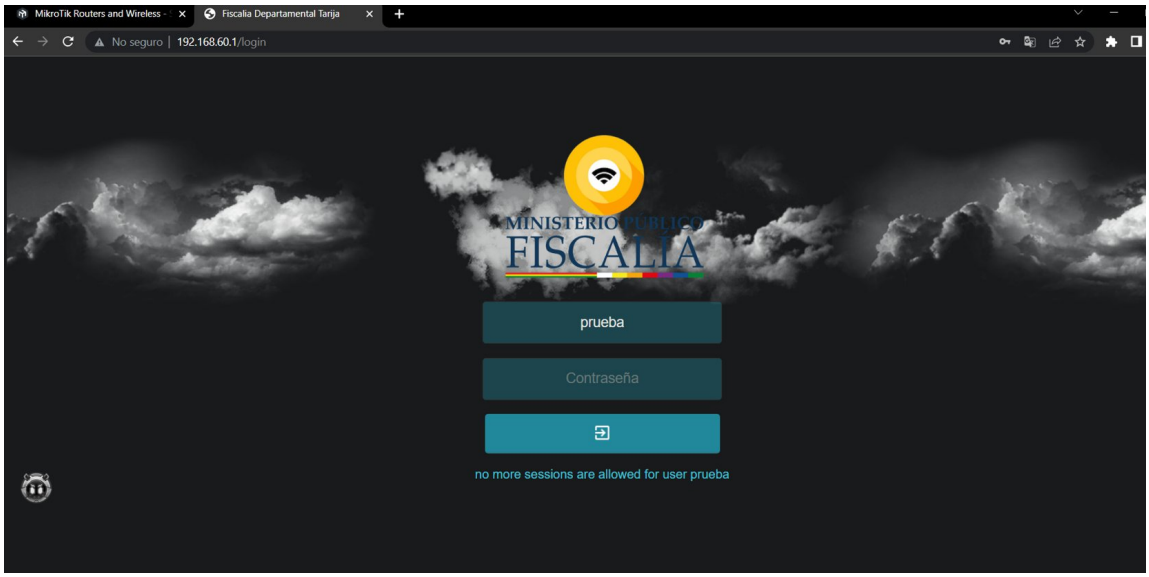


Figura 75. Diseño modificado para el hotspot

Como se logra ver en la imagen en este caso se realiza de manera estética para conocimiento que

a la red que se desean conectar es de propiedad de la fiscalía.

II.2.6.2.- Monitoreo de la red

Para monitorear una red informática se pueden utilizar distintos programas esto con el fin de garantizar un crecimiento optimo en la red y así poder mejorar la misma las funciones que nos proporciona tener un buen monitoreo de red son:

- Detección temprana de problemas de red, evitando interrupciones costosas.
- Optimización del rendimiento, garantizando un flujo de datos eficaz.
- Identificación de cuellos de botella y planificación de recursos.
- Mayor seguridad, mediante la detección de amenazas y vulnerabilidades.
- Toma de decisiones informadas basadas en datos en tiempo real.

II.2.6.2.1.- Trafico de la red

En el dispositivo mikrotik se puede realizar el monitoreo de las distintas maneras uno es el análisis de los puertos "RX" y "TX" son abreviaturas utilizadas para referirse a las direcciones de datos y la transferencia de información. Estas abreviaturas provienen del inglés y representan "Receive" (Recibir) y "Transmit" (Transmitir). En la comunicación de red, "RX" se refiere a la dirección de recepción de datos, "TX" se refiere a la dirección de transmisión de datos.

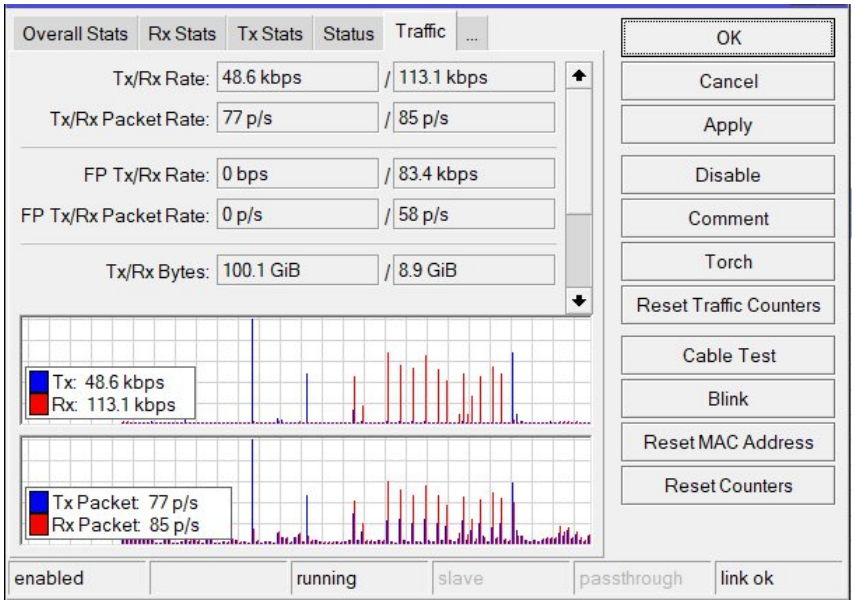


Figura 76. Trafico de la red

El tráfico de red se logra ver de distintas formas se puede ver el tráfico que pasa por uno de los puertos del mikrotik o también por usuario conectado por su usuario en el hotspot.

II.2.6.2.2.- Tiempo de conexión

Server	User	Domain	Address	Uptime	Idle Time	Session Time ...	Rx Rate	Tx Rate
Planta_2	JorgeMiran...		192.168.70.5	00:46:00	00:00:05		0 bps	0 bps
Planta_2	SergioCent...		192.168.70.56	01:38:14	00:00:04		0 bps	0 bps
Planta_baja	AdrianaPaz...		192.168.60.6	01:01:39	00:00:02		789 bps	894 bps
Planta_baja	PatriciaAyar...		192.168.60.37	01:30:23	00:00:09		0 bps	0 bps
Planta_baja	LorenaFern...		192.168.60.60	01:12:09	00:00:08		0 bps	0 bps
Planta_baja	BryanMaldo...		192.168.60.69	02:21:30	00:00:09		0 bps	0 bps
Planta_baja	FabiolaGar...		192.168.60.99	01:40:58	00:00:01		302.4 k...	4.1 Mbps
Planta_baja	VanesaRod...		192.168.60.109	01:31:56	00:00:03		476 bps	500 bps
Planta_baja	DavidGallar...		192.168.60.110	01:11:48	00:00:09		0 bps	0 bps
Planta_baja	MarcoRical...		192.168.60.174	02:13:13	00:00:01		162.2 k...	24.7 kbps
Planta_baja	JimenaFlor...		192.168.60.190	01:20:12	00:00:30		0 bps	0 bps
Planta_baja	AlvaroPere...		192.168.60.196	01:25:57	00:00:04		0 bps	0 bps
Planta_baja	ArturoMoral...		192.168.60.215	01:36:23	00:00:02		20.0 kbps	29.6 kbps
Planta_baja	milenca		192.168.60.216	01:25:17	00:00:01		199 bps	0 bps

Figura 77. Verificación del tiempo de conexión de los usuarios inalámbricos

En la imagen se logra ver la conexión de los usuarios de la fiscalía y su tiempo en el que permanecen activos en el hotspot este tipo de conexiones nos permite que mientras se encuentren en la fiscalía permanezcan conectados según se vea su rol se le asignara el tipo de usuario y en donde tiene acceso y a que piso se podrá conectar.

II.2.6.3.- Optimización de la red

Para realizar la optimización de una red informática se debe hacer una evaluación de los problemas de la red en lo que respecta a la nueva red podemos ver que tenemos ya un método de monitoreo para ver posibles fallas o algún inconveniente los inconvenientes.

II.2.6.3.1.- Bloqueo de apps

Al momento de la implementación de las reglas para bloqueo de streaming las cuales se solucionaron de haciendo uso de otro método de bloqueo de red uno que analiza el tráfico de los paquetes les coloca una marca y de allí limita el paso de los mismos en lo que respecta la optimización de la red se trabajó.

Con la optimización de esta red se hizo uso de herramientas que generan todas las ips disponibles con las que trabajan los servicios que se desean bloquear y así obtener listas de distintos servidores.

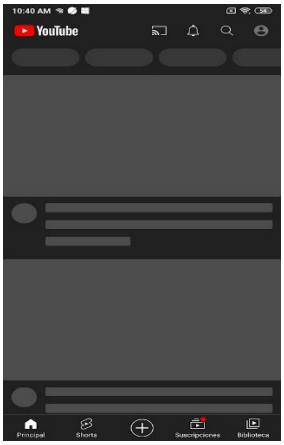


Figura 78. bloqueo de app de YouTube

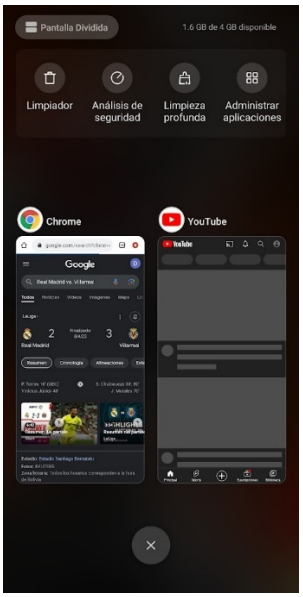


Figura 79. Funcionamiento en conjunto

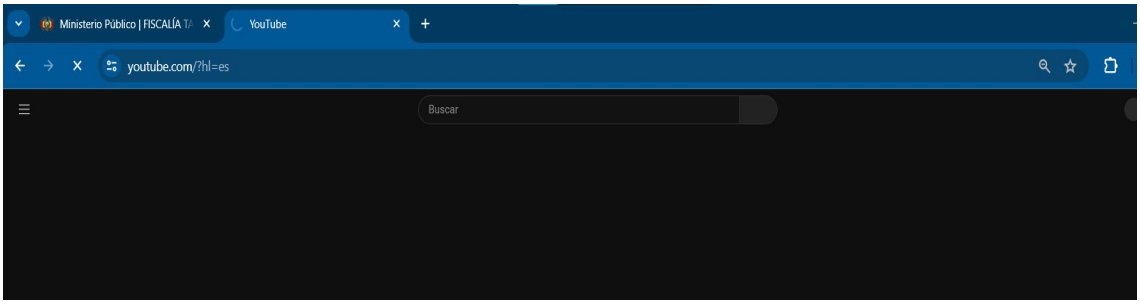


Figura 80. Funcionamiento en conjunto desde navegador

II.2.6.3.2.- Control de ancho de banda

Para el control del ancho de banda se realizó un análisis de las aplicaciones usadas por los usuarios y por el medio inalámbrico se requiere mayor ancho de banda por el uso de aplicaciones de video llamada y en máquinas ethernet menor medida ya que solo la usan para ver el estado de los casos o descargar archivos no muy grandes.

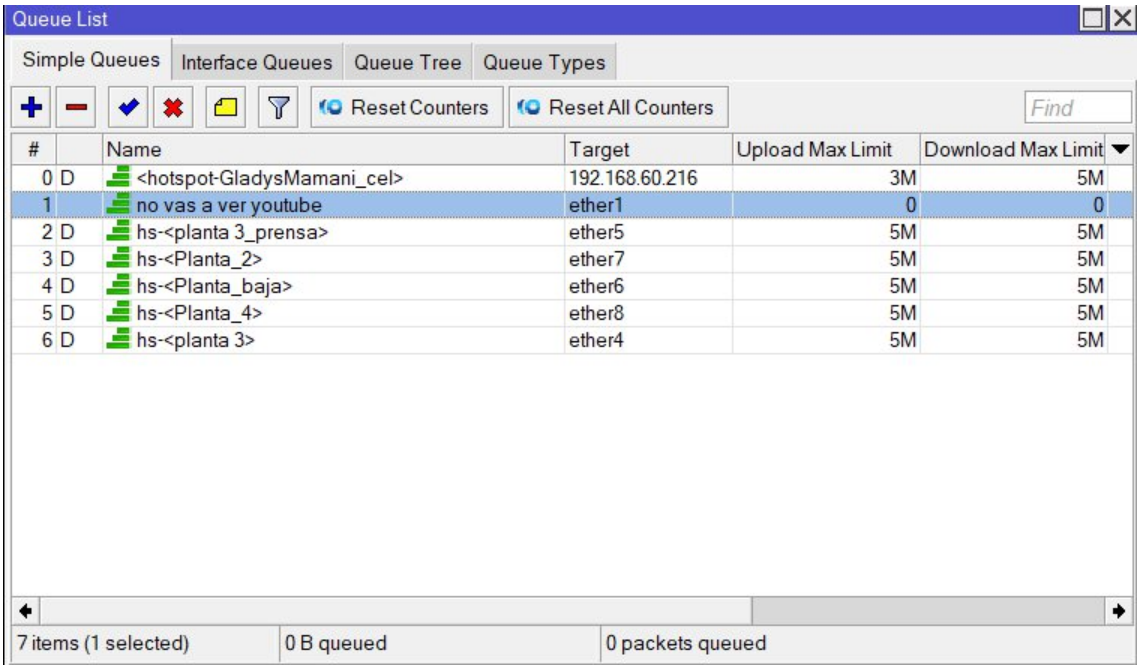


Figura 81. Configuración de ancho de banda

Se definirían el ancho de banda con 5M de descarga y 5M de carga para los dispositivos inalámbricos y con los dispositivos ethernet se configuraría con 3M de descarga y 3M de carga por que requiere menor ancho de banda.

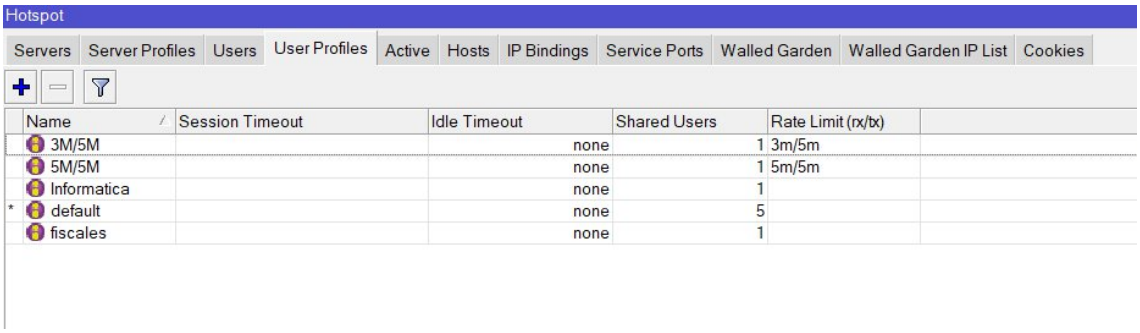


Figura 82. Asignación de ancho de banda para el hotspot

II.2.6.3.3.- Failover

El failover es un medio redundante para hacer un respaldo de uso de internet aplicando 2 WAN en un dispositivo mikrotik en caso de fallo de alguno el otro reemplaza automáticamente todas

sus funciones de trabajo configurado.

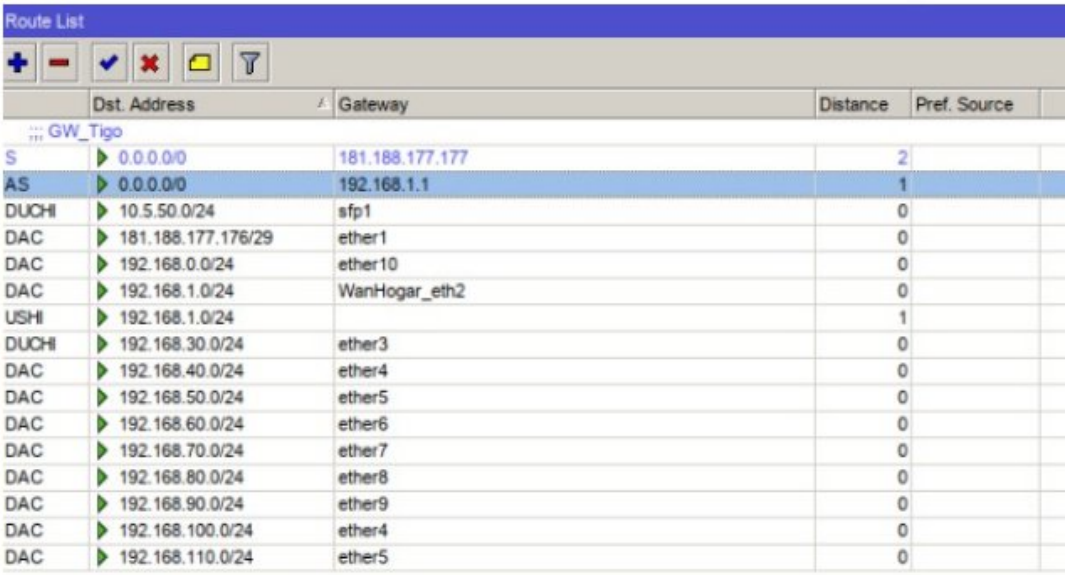


Figura 83. Asignación de ancho de banda para el hotspot

Se asigna la configuración de ambas WANs con una dirección perteneciente la WAN 1 para el acceso a todas las rutas de la red mediante 0.0.0.0/0 con una distancia de 1 al ser la principal y con una dirección gateway hacia 181.188.177.177 al servicio de tigo, la WAN 2 para el acceso a todas las rutas de la red mediante 0.0.0.0/0 con una distancia de 2 al ser la de respàldo en contra de caída de la wan1 y con una dirección gateway hacia 192.168.1.1 al servicio de entel en este caso la Wan 1 estará en constante funcionamiento y la Wan 2 en caso de respaldo asumirá todas sus funciones automáticamente.

II.3.-Requerimientos de la Red

Definiciones, acrónimos y abreviaturas

FDT	Fiscalía Departamental De Tarija
NewRI	Nueva Red de la Institución

II.3.1.-Resumen

El presente Proyecto de redes está adaptado para su trabajo bajo la norma ERS IEEE 830 por

ende se tomarán en cuenta unos puntos con mayor referencia como el punto 3 de requisitos no funcionales y algunos puntos no forman parte en este proyecto.

II.3.2.-Perspectiva del producto

El objetivo de la realización de ese proyecto es para reducir las quejas otro es mejorar la seguridad de la red ya que es una red que maneja asuntos delicados e información de vital importancia.

Lo que se espera es que no se necesite al personal de mantenimiento de la red como actualmente que en la fiscalía en el horario laboral en un día se aproxima tener entre 5 a 10 fallas que el personal informático debe ir a solucionar.

II.3.3.-Funcionalidad del producto

La nueva red lo que se espera que cumpla con los siguientes puntos:

-Mejorar el rendimiento una reacción más rápida para él envió de datos

-Mayor seguridad incluir características de seguridad mejoradas para proteger los datos y la información de la organización

-Escalabilidad puede adaptarse y crecer junto con las necesidades de la organización, sin requerir una reestructuración importante.

- Reducción de costos esto incluye al equipo de mantenimiento y al momento de la escalabilidad.

II.3.4.-Características de los usuarios

Tipo de usuario	Notificador
Formación	Universitaria
Habilidades	Abogado
Actividades	Trato con personas sobre sus casos

Tipo de usuario	Médico Forense

Formación	Universitaria
Habilidades	Doctor
Actividades	Evalúa estado de paciente en caso de algún daño físico

Tipo de usuario	Psicólogo/trab social
Formación	Universitaria
Habilidades	Psicología
Actividades	Manejo de palabra con los afectados en el caso

Tipo de usuario	Administración
Formación	Universitaria
Habilidades	Contabilidad, administración
Actividades	Evaluación de personal, Registro de equipamiento y Pedidos de equipo nuevo

Tipo de usuario	Encargado Informático
Formación	Universitaria
Habilidades	Conocimientos informáticos
Actividades	Encargado de reparación, instalación, implementación de proyectos en la institución

Tipo de usuario	Auxiliar Fiscal
Formación	Universitaria
Habilidades	Abogado
Actividades	Colabora en actividades y casos

Tipo de usuario	Fiscal de Materia
Formación	Universitaria
Habilidades	Abogado con doctorado

Actividades	Encarga de recibir y Dirigir los casos aceptados

II.3.5.-Restricciones

El proyecto debe cumplir con el documento de los protocolos de trabajo que maneja la fiscalía departamental de Tarija la red debería realizarse con forme a lo dice el documento si se desea garantizar el funcionamiento de la misma.

Solo los usuarios pertenecientes a la FDT del área de informática tendrán en posesión la documentación.

II.3.6.-Suposiciones y dependencias

En caso de la adición de nuevos dispositivos inalámbricos se previó que el mikrotik puede alojar o enlazarse a otros dispositivos de la misma marca para realizar su expansión.

II.3.7.-Evolución previsible

En el futuro la red podrá estar dispuesta para posible ampliación de la red inclusive manejo de vpn también si existen modificaciones en la institución dispuesta para una reorganización por parte del encargado de administrar el dispositivo.

II.3.8.-Requisitos no funcionales

II.3.8.1.-Requisitos de rendimiento

REQ1.-Division de ancho de banda

Tomando en cuenta en rendimiento el ancho de banda debo realizar una repartición mínima de al menos 5 Mbps por cada usuario.

- Implementar tecnologías de gestión de ancho de banda: Control de uso de ancho de banda ya sea por usuario o por grupos de usuarios.
- Establecer políticas de uso de ancho de banda: Define políticas claras y específicas sobre el uso del ancho de banda en la red. Estas políticas deben incluir límites de consumo de ancho de banda para ciertas aplicaciones o usuarios, así como la identificación de

actividades no permitidas o de bajo valor que puedan afectar el rendimiento general.

REQ2.-Verificacion de latencia

La latencia se refiere al tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino y regresar teniendo eso en cuenta una latencia aceptable es de debajo de 100 milisegundos.

REQ3.-Perdida de paquetes

la perdida de paquetes en lo que se espera cumplir con mantener la pérdida de paquetes por debajo del 1% es lo recomendado para cualquier institución.

- Mikrotik: posee una cantidad de herramientas para medir el uso general del internet ya sea por puerto o por un periodo de tiempo.

II.3.8.2-Seguridad
REQ4.-Control de acceso

El dispositivo Mikrotik plantea una mejora en la seguridad de toda la institución en lo que respecta la restricción a los usuarios en los horarios laborales de prohibir el uso de determinadas acciones en sus equipos en horario laboral.

REQ5.-Backup al equipo

Realización de respaldo periódicamente de los datos e información de los equipos.

REQ6.-Contraseñas

Configurar el uso de contraseña de usuarios par el acceso en las maquinas usuarios y contraseña. Emplear un mínimo de 8 caracteres, con letras mayúsculas y minúsculas, así como símbolos y signos de puntuación.

Estas son unas aplicaciones que ayudan en lo que respecta este punto:

- LastPass: es una aplicación de administración de contraseñas que no solo genera contraseñas seguras, sino que también almacena y autocompleta tus credenciales de inicio de sesión en diferentes sitios web y aplicaciones.
- Dashlane: es otra herramienta de gestión de contraseñas que genera contraseñas seguras y las guarda en una bóveda encriptada. También ofrece autocompletado y sincronización

entre dispositivos.

- 1Password: 1Password es una aplicación de administración de contraseñas que genera contraseñas fuertes y seguras. Además, cuenta con características como el almacenamiento seguro de datos y la autenticación de dos factores.
- KeePass: es un administrador de contraseñas de código abierto que permite generar contraseñas seguras y las guarda en una base de datos encriptada. Puedes utilizarlo en diferentes plataformas y sincronizar la base de datos mediante servicios en la nube.
- Bitwarden: es una aplicación de gestión de contraseñas de código abierto que genera contraseñas seguras y las almacena en una bóveda encriptada. También ofrece funciones de autocompletado y sincronización entre dispositivos.

REQ7.-Cambio de contraseñas

Cambiar las contraseñas de manera regular, y procurar que sean siempre muy distintas.

REQ8.-Control de incendios

Lo que comprende al control de incendios se toma en cuenta solo en un aspecto el uso de extintores que sean para metales seria extintores de clase D para objetos electrónicos y en caso de un incendio existen policías vigilando todos los 7 días de la semana por lo que un sistema d incendios no sería necesario.

II.3.8.3.-Disponibilidad
REQ9.-Acceso a la red

Permitir que los usuarios tengan acceso a la red las horas de trabajo y en horario 24/7 para los administradores para mejorar el servicio.

II.3.8.4.-Mantenibilidad
REQ10.-Mantenimiento

Contar con un cronograma anual de mantenimientos de los equipos de computación para evitar problemas cuando estén en usos además brindar seguridad a los mismos equipos con respaldos de datos de información.

Mensualmente:

Actualización de software: Verifica y aplica las actualizaciones de software disponibles para los

equipos, incluyendo sistemas operativos, aplicaciones y controladores.

Trimestralmente:

Limpieza física: Limpia físicamente los equipos para eliminar el polvo y la suciedad acumulados en los ventiladores, teclados, pantallas, etc. Utiliza productos de limpieza adecuados y evita el uso de líquidos directamente sobre los equipos.

Verificación de cables: Revisa y asegura que todos los cables estén correctamente conectados y en buen estado. Repara o reemplaza los cables dañados o desgastados.

Semestralmente:

Respaldo de datos: Realiza copias de seguridad de todos los datos importantes almacenados en los equipos. Asegúrate de que los respaldos sean completos y se almacenen en ubicaciones seguras y fuera del sitio.

Actualización de antivirus: Actualiza y escanea los equipos con el software antivirus para garantizar que estén protegidos contra las últimas amenazas.

Anualmente:

Mantenimiento preventivo: Realiza un mantenimiento preventivo más exhaustivo, que puede incluir desmontar los equipos, limpiar los componentes internos, aplicar pasta térmica en los disipadores de calor, verificar los ventiladores, etc.

REQ11.-Solucion rápida

Tomar en cuenta solución de manera rápida a equipos que influyan en el trabajo de la institución

Los equipos que influyen más en el trabajo y que no pueden estar ni un momento sin sus equipos son los que se encuentran en ventanilla en contacto directo con los cuidadnos estos son: auxiliares/abogados, ventanilla de atención al cliente estos requieren reparación inmediata en otros casos con los demás usuarios se puede demorar más o proporcionar un equipo de reserva de almacén.

II.3.8.4.-Portabilidad
REQ12.-Administrar mikrotik

En lo que respeta de portabilidad solo se manejara en la institución para los usuarios comunes con excepción de administración en el equipo informático que posee mayor control en equipos personales dispuestos por la empresa y pueden acceder desde su domicilio en algún caso de emergencia.

Se puede ver que los dispositivos mikrotik son muy portátiles para su manejo ya que estos se pueden administrar desde un dispositivo celular al contar con una aplicación para administrar desde el móvil.

II.3.9.-Otros requisitos

Se debe Tomar en cuenta que en esta especificación de software que este documento está adaptado para el control en una de redes.

COMPONENTE II
Capacitación de los encargados de informática de la administración de la institución

II.-Componente 2: Capacitación de los encargados de informática de la administración de la institución

II.3.- Capacitación a los encargados de informática.

II.3.1.-Analisis

El análisis de la capacitación nos demuestra que al ser personal de informática a los que vamos a capacitar y tienen buen conocimiento del tema entonces se tomaría en cuenta la enseñanza según lo aplicado con ayuda de conceptos del proyecto, pero dirigido principalmente a los encargados que se quedaran a cargo de administrar el seguimiento de la evolución del proyecto.

El personal que se encuentra a cargo del gabinete de telecomunicaciones obtendrá conocimientos sobre el uso fundamental de las tecnologías implementadas en la nueva estructuración, haciendo uso de métodos de enseñanza para el aprendizaje para la administración y mantenimientos requeridos en un futuro.

Este componente asegura la transferencia de conocimientos sobre el trabajo del personal involucrado que conlleva a mejorar los conocimientos del personal que recibe la capacitación.

II.3.1.2-Propósito

El propósito del componente es finalizar el proyecto con la capacitación, para contar con los encargados capacitados en caso de algún error o falla pueda resolverse y no tenga de realizarse ninguna nueva configuración desde 0.

II.3.1.3-Objetivos Generales

II.3.1.4.-Objetivo

- Capacitar al personal principalmente sobre el funcionamiento del gabinete de telecomunicaciones, dispositivo mikrotik y uso de los dispositivos finales.

II.3.1.5.-Objetivos Específicos

- Definir métodos visuales para enseñanza del gabinete de telecomunicaiones.
- Capacitación sobre uso del dispositivo Mikrotik.

II.3.2.-Diseño

La capacitación se desarrollará por la guía que tomara en cuenta las diferentes tecnologías que se usaron para la instalación y estructuración de los diferentes equipos tecnológicos. El rol de las capacitaciones va en función de las funciones de los administradores del cuarto de telecomunicaciones; que por lo expuesto solo se cubrirá el nivel Técnico. Debido a que son los únicos encargados se hará uso presencial del equipo para la enseñanza del mismo y así su fácil comprensión y pruebas correspondientes.

II.3.2.1.-Propuesta Pedagógica

Para la propuesta pedagógica a utilizar sobre los servicios en la nueva infraestructura tecnológica dada las características de los usuarios directos que son funcionarios administradores del cuarto de telecomunicaciones.

El método de enseñanza será el aprendizaje Significativo: Debido a que este método se caracteriza que los mismos técnicos de la institución se les incorporará nuevos conocimientos previamente tomando en cuenta que los funcionarios capacitados tengo alguna relación sobre las nuevas tecnologías implementadas que generará interés por aprender el uso de las herramientas para su trabajo cotidiano comprender para los casos y el funcionamiento general de los equipos en caso de posible cambio o mejora a futuro.

II.3.3.-Desarrollo

Lo que comprende con el desarrollo o el análisis de las herramientas que se utilizaran para el aprendizaje de los encargados de informática de la institución se usara como herramienta principal de manera visual y el uso de backups hechos durante la configuración de los equipos como medio de explicación cargarla en un equipo o dispositivo y someterlo a pruebas de su funcionamiento tomando en cuenta la explicación del proceso de configuración.

II.3.4.-Implementacion

II.3.4.1.-Puntos de capacitación

- Lección 1: Configuración los equipos de computación usuarios.
- Lección 2: Asignación de Licencias para los programas de computación.
- Lección 3: Administración del Router.
- Lección 4: Configuración de los Access Point.
- Lección 5: Asignación de IP a los equipos.

- Lección 6: Administración del gabinete de telecomunicaciones.

II.3.4.2.-Plan de capacitación

Nro.	CONTENIDO	OBJETIVO	FECHA	DURACION (horas)	MATERIAL DIDACTICO	MEDIOS DE ENSEÑANZA Y APRENDIZAJE	DESTINATARIO
1	Configuración los equipos de computación usuarios.	Que los encargados puedan configurar correctamente y se ubiquen en la red	08 – NOV – 2023	2	Demostración n Real	Equipo de computación	Informáticos encargados de la nueva red
2	Asignación de Licencias para los programas de computación.	Sepan correctamente el tipo de licencias que manejan sus equipos y los periodos de actualización	09 – NOV – 2023	2	Demostración n Real	Equipo de computación	Informáticos encargados de la nueva red
3	Administración del Router mikrotik.	Sepan encontrar errores en el dispositivo mikrotik	10 – NOV – 2023	2	Demostración n Real	Equipo de computación	Informáticos encargados de la nueva red
4	Configuración de los Access Point.	Sepan corregir fallas en los equipos inalámbricos	13 – NOV – 2023	2	Demostración n Real	Equipo de computación	Informáticos encargados de la nueva red
5	Asignación de IP a los equipos.	Manejen correctamente la configuración de los equipos de la fiscalía	14 – NOV – 2023	2	Demostración n Real	Equipo de computación	Informáticos encargados de la nueva red
6	Administración del Gabinete de telecomunicaciones.	Sepan el orden de los equipos y su funcionamie	15 – NOV – 2023	2	Demostración n Real	Equipo de computación	Informáticos encargados de la nueva

		nto para futuros mantenimientos del equipo					red

Tabla 25. Plan de Capacitación

II.3.5.-Evaluacion

II.3.5.1.-Resultados

Se tiene como resultados la capacitación a los administradores del área de informática de la institución, y se tornan capaces en el manejo de los equipos de red en el uso del dispositivo mikrotik.

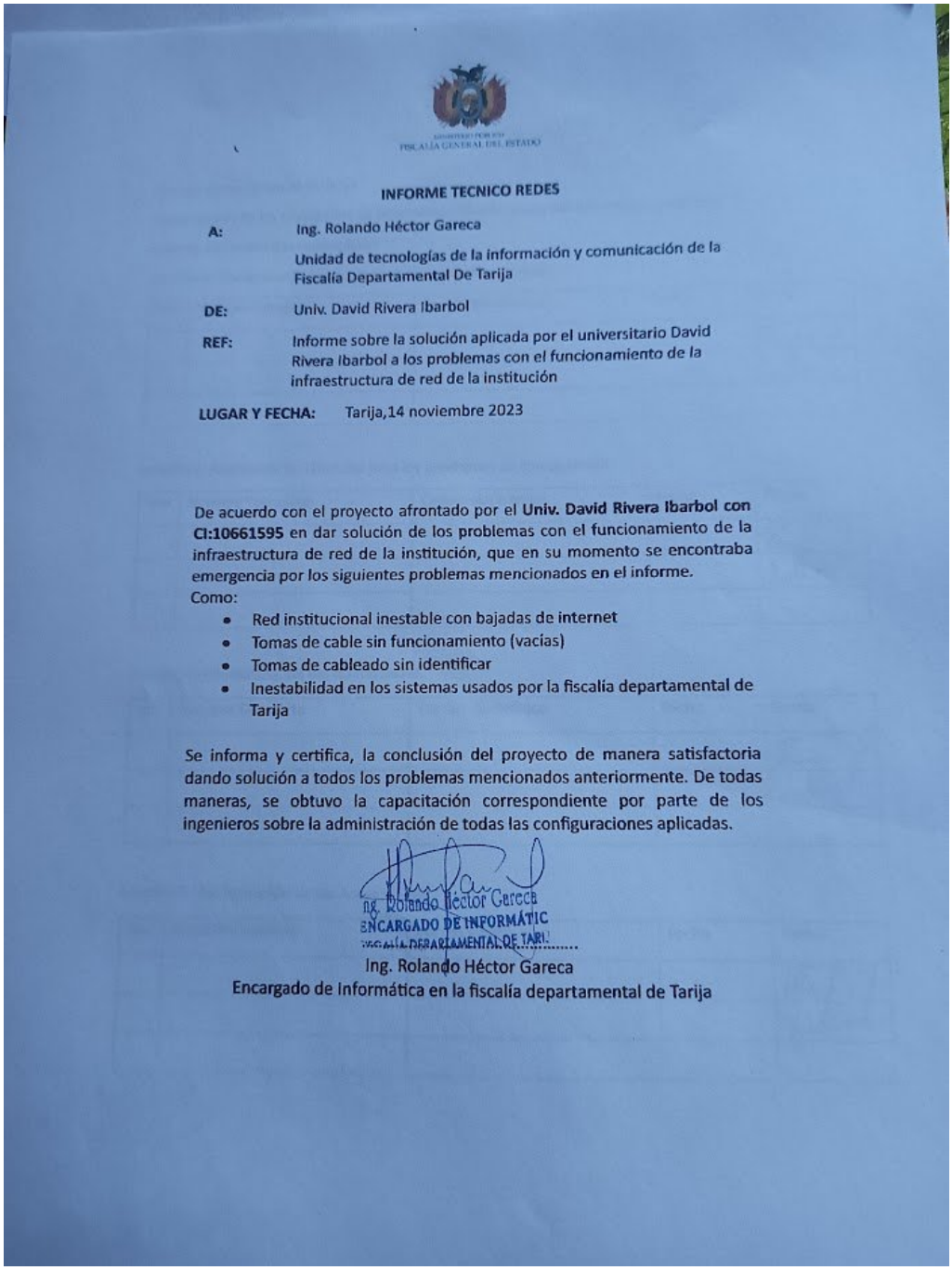
II.3.5.2.-Conclusiones

Después de que se realizará la capacitación se concluirá de esta manera la etapa de capacitación de manera exitosa con la Socialización de la explicación de la infraestructura de red y principalmente con el manejo del dispositivo mikrotik.

II.3.6.-Medios de Verificación

- Carta de conformidad de informe técnico sobre los servicios prestados en la institución por parte del encargado de Informática
- Informe de los asistentes para la capacitación

II.3.6.1.- Carta de conformidad de informe técnico sobre los servicios prestados en la institución por parte del encargado de Informática.



FISCALÍA GENERAL DEL ESTADO

INFORME TECNICO REDES

A: Ing. Rolando Héctor Gareca
Unidad de tecnologías de la información y comunicación de la Fiscalía Departamental De Tarija

DE: Univ. David Rivera Ibarbol

REF: Informe sobre la solución aplicada por el universitario David Rivera Ibarbol a los problemas con el funcionamiento de la infraestructura de red de la institución

LUGAR Y FECHA: Tarija,14 noviembre 2023

De acuerdo con el proyecto afrontado por el **Univ. David Rivera Ibarbol con CI:10661595** en dar solución de los problemas con el funcionamiento de la infraestructura de red de la institución, que en su momento se encontraba emergencia por los siguientes problemas mencionados en el informe.
Como:

- Red institucional inestable con bajadas de internet
- Tomas de cable sin funcionamiento (vacías)
- Tomas de cableado sin identificar
- Inestabilidad en los sistemas usados por la fiscalía departamental de Tarija

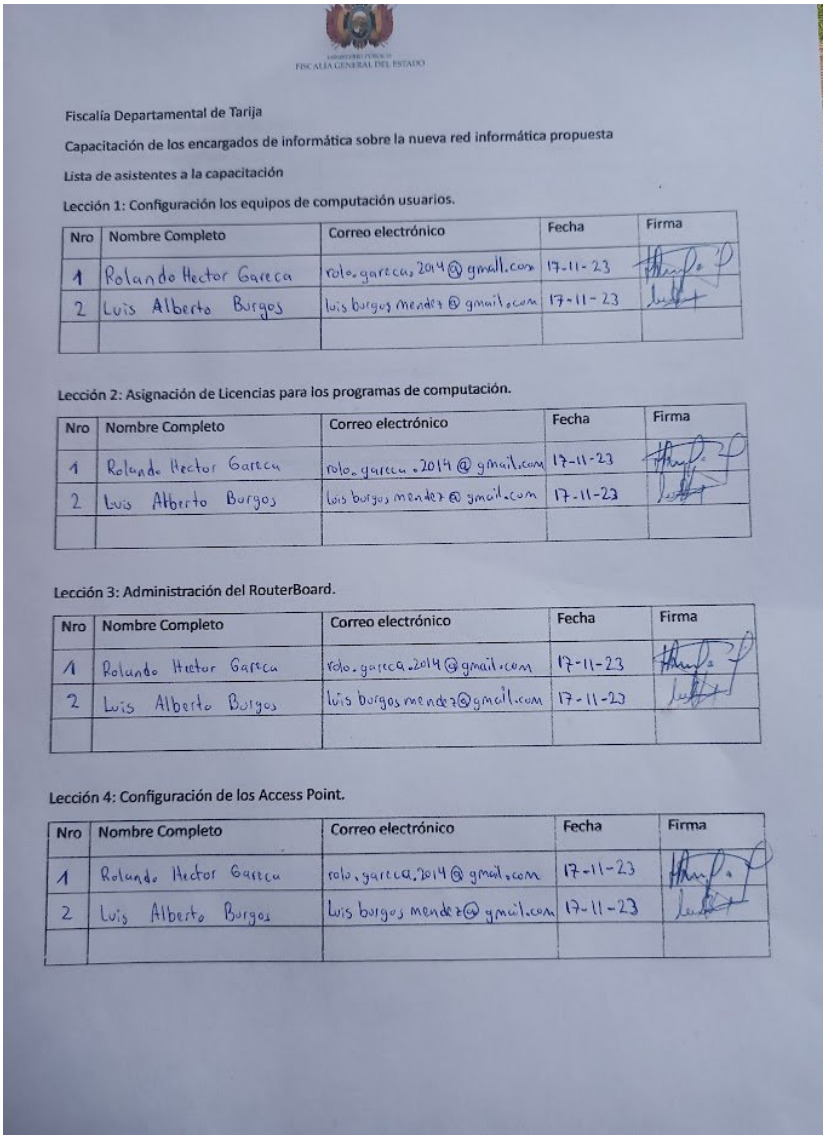
Se informa y certifica, la conclusión del proyecto de manera satisfactoria dando solución a todos los problemas mencionados anteriormente. De todas maneras, se obtuvo la capacitación correspondiente por parte de los ingenieros sobre la administración de todas las configuraciones aplicadas.

Ing. Rolando Héctor Gareca
ENCARGADO DE INFORMÁTIC
FISCALÍA DEPARTAMENTAL DE TARI

Ing. Rolando Héctor Gareca
Encargado de Informática en la fiscalía departamental de Tarija

Figura 84. Carta de conformidad de informe técnico sobre los servicios prestados en la institución por parte del encargado de Informática

II.3.6.2.- informe de los asistentes para la capacitación



FISCALÍA GENERAL DEL ESTADO

Fiscalía Departamental de Tarija

Capacitación de los encargados de informática sobre la nueva red informática propuesta

Lista de asistentes a la capacitación

Lección 1: Configuración los equipos de computación usuarios.

Nro	Nombre Completo	Correo electrónico	Fecha	Firma
1	Rolando Hector Garreca	rolo.garreca.2014@gmail.com	17-11-23	
2	Luis Alberto Burgos	luis burgos mendez@gmail.com	17-11-23	

Lección 2: Asignación de Licencias para los programas de computación.

Nro	Nombre Completo	Correo electrónico	Fecha	Firma
1	Rolando Hector Garreca	rolo.garreca.2014@gmail.com	17-11-23	
2	Luis Alberto Burgos	luis burgos mendez@gmail.com	17-11-23	

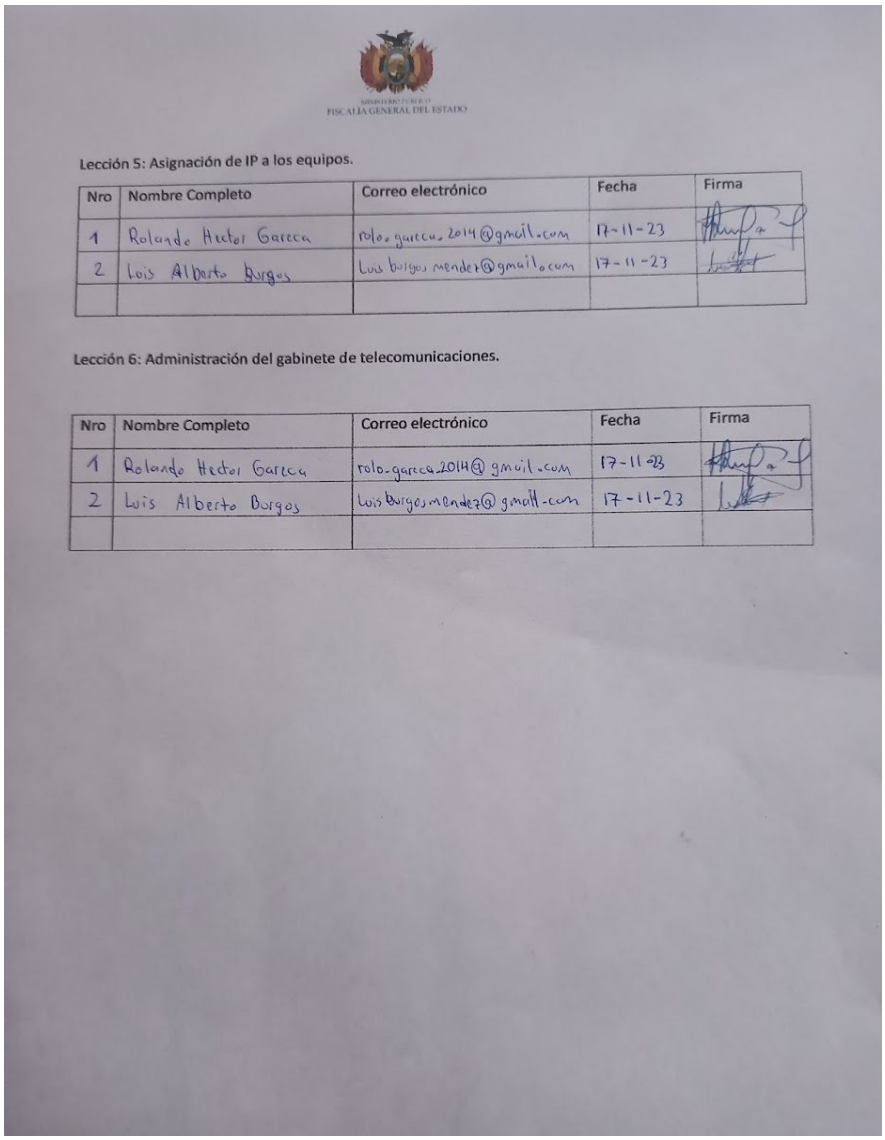
Lección 3: Administración del RouterBoard.

Nro	Nombre Completo	Correo electrónico	Fecha	Firma
1	Rolando Hector Garreca	rolo.garreca.2014@gmail.com	17-11-23	
2	Luis Alberto Burgos	luis burgos mendez@gmail.com	17-11-23	

Lección 4: Configuración de los Access Point.

Nro	Nombre Completo	Correo electrónico	Fecha	Firma
1	Rolando Hector Garreca	rolo.garreca.2014@gmail.com	17-11-23	
2	Luis Alberto Burgos	luis burgos mendez@gmail.com	17-11-23	

Figura 85. Lista de asistencia a la Capacitación I



MINISTERIO PÚBLICO
FISCALÍA GENERAL DEL ESTADO

Lección 5: Asignación de IP a los equipos.

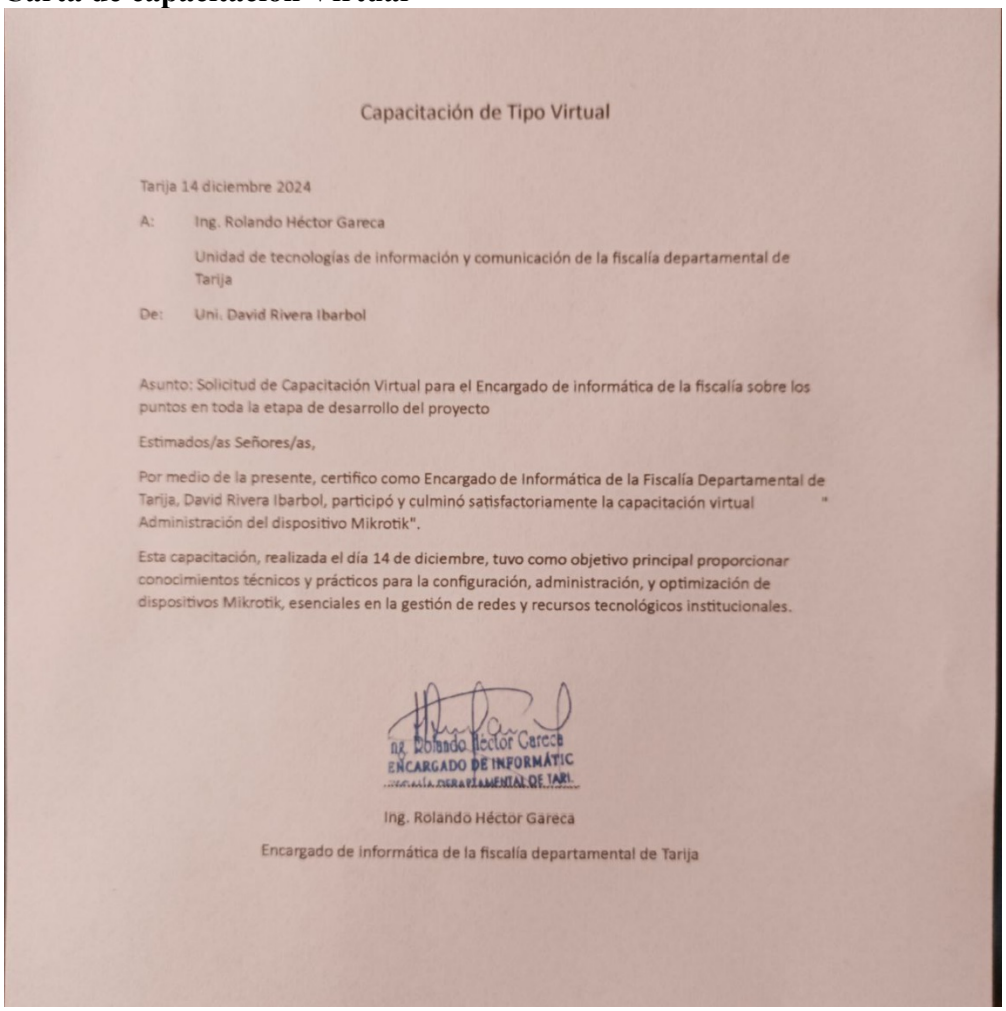
Nro	Nombre Completo	Correo electrónico	Fecha	Firma
1	Rolando Hector Garcca	rolo.garcca.2014@gmail.com	17-11-23	
2	Luis Alberto Burgos	Luis burgos.mendez@gmail.com	17-11-23	

Lección 6: Administración del gabinete de telecomunicaciones.

Nro	Nombre Completo	Correo electrónico	Fecha	Firma
1	Rolando Hector Garcca	rolo-garcca.2014@gmail.com	17-11-23	
2	Luis Alberto Burgos	Luis Burgos.mendez@gmail.com	17-11-23	

Figura 86. Lista de asistencia a la Capacitación II

II.3.6.3.- Carta de capacitación Virtual



Capacitación de Tipo Virtual

Tarija 14 diciembre 2024

A: Ing. Rolando Héctor Gareca

Unidad de tecnologías de información y comunicación de la fiscalía departamental de Tarija

De: Uni. David Rivera Ibarbol

Asunto: Solicitud de Capacitación Virtual para el Encargado de informática de la fiscalía sobre los puntos en toda la etapa de desarrollo del proyecto

Estimados/as Señores/as,

Por medio de la presente, certifico como Encargado de Informática de la Fiscalía Departamental de Tarija, David Rivera Ibarbol, participó y culminó satisfactoriamente la capacitación virtual " Administración del dispositivo Mikrotik".

Esta capacitación, realizada el día 14 de diciembre, tuvo como objetivo principal proporcionar conocimientos técnicos y prácticos para la configuración, administración, y optimización de dispositivos Mikrotik, esenciales en la gestión de redes y recursos tecnológicos institucionales.

Ing. Rolando Héctor Gareca
ENCARGADO DE INFORMÁTIC
FISCALÍA DEPARTAMENTAL DE TARI

Ing. Rolando Héctor Gareca

Encargado de informática de la fiscalía departamental de Tarija

Figura 87. Carta Avalando la capacitación virtual

II.3.6.4.- Fotografía de capacitación

Figura 88. Fotografía de capacitación 2

CAPITULO III
CONCLUSIONES Y RECOMENDACIONES

III.1.-Conclusiones

Mediante la mejora de la nueva red para la fiscalía departamental de Tarija se pudo concluir:

- La configuración de la red en la Fiscalía Departamental de Tarija ha permitido la optimización de la infraestructura de comunicación, garantizando un rendimiento eficiente y una gestión efectiva de los recursos de red.
- El uso de la metodología Top-Down nos permitió un mejor orden en el apartado de la implementación de la nueva red al trabajar en la configuración de los equipos.
- Los beneficios obtenidos por elegir esta topología son tanto económicos como beneficiosos para permitir el crecimiento de la institución y la instalación de nuevos equipos a futuro.
- La implementación de políticas de calidad de servicio (QoS) ha priorizado el tráfico de los usuarios críticos, como los fiscales y el personal de informática, garantizando un acceso rápido y sin interrupciones a los recursos de red.
- La configuración del firewall y las políticas de seguridad han fortalecido la protección de la red contra amenazas cibernéticas, lo que ha contribuido a salvaguardar la confidencialidad de la información en la Fiscalía.
- La segmentación de la red en VLANs ha permitido una administración más efectiva y un aislamiento adecuado de los diferentes grupos de usuarios, mejorando la seguridad y el rendimiento.

III.2.-Recomendaciones

- Establece un plan de mantenimiento regular para el dispositivo MikroTik que incluya actualizaciones de firmware, parches de seguridad y copias de seguridad periódicas de la configuración.
- Refuerza la seguridad del dispositivo MikroTik mediante la configuración de contraseñas fuertes y el acceso limitado a través de SSH o Winbox.
- Mantén el sistema operativo RouterOS actualizado con las últimas versiones. Realiza pruebas en un entorno de laboratorio antes de aplicar actualizaciones en producción.
- Ten en cuenta la planificación para futuras expansiones de red y la adición de nuevos servicios. Asegúrate de que el dispositivo MikroTik sea escalable y flexible para

adaptarse a las necesidades cambiantes.