

## **Portal Cautivo Utilizando Equipos Mikrotik en el Laboratorio de Telecomunicaciones y Redes**

### **Captive portal using Mikrotik equipment in the Telecommunications and Networks laboratory**

---

**Para citar este trabajo:**

Zambrano, D., Bonilla, J., y Barberán, J., (2024) Portal Cautivo Utilizando Equipos Mikrotik en el Laboratorio de Telecomunicaciones y Redes. *Reincisol*, 3(6), pp. 1856-1870.  
[https://doi.org/10.59282/reincisol.V3\(6\)1856-1870](https://doi.org/10.59282/reincisol.V3(6)1856-1870)

---

#### **Autores:**

**Damaris Yulexi Zambrano Rosado**

Instituto Superior Tecnológico Tsa`chila

Ciudad: Santo Domingo, País: Ecuador

Correo Institucional: [damariszambranorosado@tsachila.edu.ec](mailto:damariszambranorosado@tsachila.edu.ec)

Orcid <https://orcid.org/0009-0007-3034-4997>

**Jefferson Javier Bonilla Camisan**

Instituto Superior Tecnológico Tsa`chila

Ciudad: Santo Domingo, País: Ecuador

Correo Institucional: [jeffersonbonillacamisan@tsachila.edu.ec](mailto:jeffersonbonillacamisan@tsachila.edu.ec)

Orcid <https://orcid.org/0009-0002-0744-9794>

**Ing. Jeneffer Joselin Barberán Moreira, Mg**

Instituto Superior Tecnológico Tsa`chila

Ciudad: Santo Domingo, País: Ecuador

Correo Institucional: [jenefferbarberan@tsachila.edu.ec](mailto:jenefferbarberan@tsachila.edu.ec)

Orcid <https://orcid.org/0000-0001-9103-6858>

**RECIBIDO:** 20 junio 2024    **ACEPTADO:** 15 julio 2024    **PUBLICADO** 22 agosto 2024

## Resumen

El proyecto se centra en la implementación de un portal cautivo utilizando equipos Mikrotik, para el laboratorio de Telecomunicaciones y Redes. El proyecto puesto que en el Laboratorio no hay un sistema que controle la red Wi-Fi, lo cual dificulta la seguridad y conlleva varios inconvenientes, incluyendo la falta de gestión de ancho de banda. Este proyecto se basa en la implementación de un portal cautivo con Mikrotik para el laboratorio de Telecomunicaciones y Redes. Se utilizó la metodología en cascada con tres etapas: a) Análisis de los requisitos técnicos y selección de los equipos mediante una tabla comparativa. b) Configuración del portal cautivo mediante la autenticación de usuarios y la designación de ancho de banda. c) validación del portal cautivo mediante pruebas de autenticación, ancho de banda y el acceso a usuarios concurrentes. Se constató el ingreso exitoso de los usuarios al portal cautivo, y se verificó que la asignación de ancho de banda y el tiempo de conexión se llevaron a cabo de manera satisfactoria. Esto permitió administrar eficientemente el acceso de los usuarios, garantizando al mismo tiempo la seguridad de la red.

**Palabras claves:** Portal cautivo, Hotspot, Mikrotik.

### Abstract

The project focuses on the implementation of a captive portal using Mikrotik equipment, for the Telecommunications and Networks laboratory. The project arose because in the Laboratory there is no system that controls the Wi-Fi network, which makes security difficult and entails several inconveniences, including the lack of bandwidth management. This project is based on the implementation of a captive portal with Mikrotik for the Telecommunications and Networks laboratory. The waterfall methodology was used with three stages: a) Analysis of the technical requirements and selection of equipment using a comparative table. b) Configuring the captive portal through user authentication and bandwidth designation. c) validation of the captive portal through authentication tests, bandwidth and concurrent user access. The successful entry of users to the captive portal was verified, and it was verified that the bandwidth allocation and connection time were carried out satisfactorily. This allowed user access to be efficiently managed, while ensuring network security.

**Keywords:** Captive portal, Hotspot, Mikrotik.

## INTRODUCCIÓN

La aparición de las Tecnologías de la información y la comunicación (TIC) índice en las funciones del sistema de educación (García, Reyes, & Godinez, 2017). Hoy en día, el uso de internet representa una prioridad en las instituciones de Educación Superior, por varios motivos claves. En primer lugar, facilita el acceso a recursos educativos en línea, permitiendo a estudiantes y profesores aprovechar al máximo herramientas de aprendizaje digital, plataformas de colaboración y recursos educativos interactivos. Además, promueve la flexibilidad y la movilidad en el entorno, facilitando la conectividad, fomentando la colaboración y el intercambio de ideas (Laguna, 2013). En última instancia, una red Wi-Fi confiable y segura contribuye significativamente a mejorar la experiencia educativa, preparando a los estudiantes para un mundo digitalizado y promoviendo la innovación y la excelencia académica (Zarate & Villero, 2020).

Actualmente, las personas consumen internet de manera inalámbrica, es decir, sin necesidad de disponer de un cable de red, a pesar, de que tienen una menor velocidad de conexión y una menor estabilidad. Además, una red donde todos los usuarios desean ingresar al mismo tiempo genera saturación de la red, donde tendrán una conexión con baja velocidad y exponiendo sus datos a terceros en caso de que la red no sea segura (Zarate & Villero, 2020). La pregunta clave aquí es ¿existe una manera de generar una solución ante esto?, es allí cuando los equipos Mikrotik con sus funcionalidades de Hotspot y portales cautivos entrar en dar solución.

El uso de internet de manera inalámbrica es bastante utilizado en cafeterías, hospitales, hoteles, aeropuertos, terminales y entre otros. Sin embargo, muchas personas desconocen que es un hotspot y portal cautivo. De acuerdo con Prieto (2015), un Hostpot es un lugar donde se ofrece el servicio de internet de manera gratuita, donde varios usuarios podrán conectarse de manera inalámbrica, para lo cual se debe contar de varios puntos accesos. Los Hostpot van de la mano del portal cautivo, donde Cruz (2011), considera que un portal cautivo es una máquina en una red para vigilar el tráfico HTTP, obligando al usuario a ingresar a una página web para la autenticación mediante usuario y contraseña, para poder ingresar a internet, de esta manera poder controlar los tiempos de conexión, los sitios a los

que pueden ingresar, controlar el ancho de banda y contar con un registro de los usuarios conectados a la red.

Actualmente, el Laboratorio de Telecomunicaciones y Redes en la carrera de Tecnología Superior Electrónica del Instituto Superior Tecnológico Tsa'chila carece de un sistema centralizado para autenticar y gestionar el acceso a su red inalámbrica, lo que puede llevar a problemas de seguridad, con gestión de la red y dificultades en la asignación de ancho de banda para actividades académicas y administrativas. Además, el laboratorio no cuenta con un sistema de control y gestión eficiente para su red Wi-Fi, generando diversos inconvenientes como el acceso no controlado, en el cual cualquier persona puede acceder a la red sin autorización, poniendo en riesgo la seguridad de la información.

Ante, esta problemática, surge la necesidad de realizar un portal cautivo utilizando equipos Mikrotik en el Laboratorio de Telecomunicaciones y Redes para gestionar eficientemente el acceso a su red Wi-Fi, permitiendo autenticar a los usuarios de manera centralizada, controlar el acceso basado en políticas predefinidas y proporcionar una experiencia de navegación personalizada a través de la configuración de páginas de inicio personalizadas. Además, como una herramienta para comunicar información importante, eventos y políticas institucionales a los usuarios al conectarse a la red, mejorando así la experiencia general del usuario y fortaleciendo la seguridad de la red.

### **MATERIALES Y MÉTODOS**

Para el presente trabajo de titulación se adoptó la metodología en cascada, consiste en ciertas etapas. Se identificaron las necesidades técnicas del portal cautivo para determinar los requisitos de autenticación de usuarios, asignación de ancho de banda y personalización de páginas de inicio. Se elaboró un diagrama de red donde se integran los equipos Mikrotik con la infraestructura existente. Además, se configuró el portal cautivo de acuerdo con las políticas de autenticación, asignación de ancho de banda y página de inicio personalizado. Finalmente, se realizaron pruebas funcionales para asegurar de que el portal cautivo se autentica correctamente y se asigne el ancho de banda según lo previsto. Además, se simuló el uso del portal cautivo por parte de los usuarios para verificar la fluidez de la experiencia, de esta manera poder detectar y corregir cualquier fallo.

## **Análisis de Requisitos**

### **Requisitos técnicos del portal cautivo**

La tabla 1 detalla los requisitos técnicos esenciales para la implementación de un portal cautivo, enfatizando la capacidad para manejar al menos 30 usuarios concurrentes, soporte para autenticación mediante usuario/contraseña, y la gestión del ancho de banda. Estos elementos son fundamentales para garantizar un rendimiento óptimo y una experiencia de usuario personalizada.

**Tabla 1.** Requisitos Técnicos del Portal Cautivo

<b>Requisito</b>	<b>Descripción</b>	<b>Prioridad</b>
Número de Usuarios Concurrentes	Capacidad para manejar al menos 30 usuarios concurrentes en el portal cautivo.	Alta
Métodos de Autenticación	Soporte para autenticación mediante usuario/contraseña	Media
Gestión de ancho de banda	Capacidad para asignar límites de ancho de banda por usuarios o grupo de usuarios.	Alta
Personalización de página de inicio	Posibilidad de diseñar y configurar páginas de inicio personalizadas para los usuarios.	Media
Registro y monitoreo	Funcionalidades para registrar actividad de usuarios y monitorear el rendimiento del portal.	Alta
Integración con infraestructura existente	Compatibilidad con los switches y routers actualmente en uso en el laboratorio.	Alta

### **Especificaciones de equipo Mikrotik**

En la tabla 2, se compara diversas opciones de routers Mikrotik, evaluando características como CPU, RAM, puertos Ethernet, Wi-Fi y precio. El hAP ac2, con un procesador de 716 MHz y 128 MB de RAM, destaca por su doble banda Wi-Fi integrada (2.4/5 GHz) y un precio competitivo de \$103.00. Este dispositivo se presenta como una opción compacta y eficiente, ideal para entornos donde se

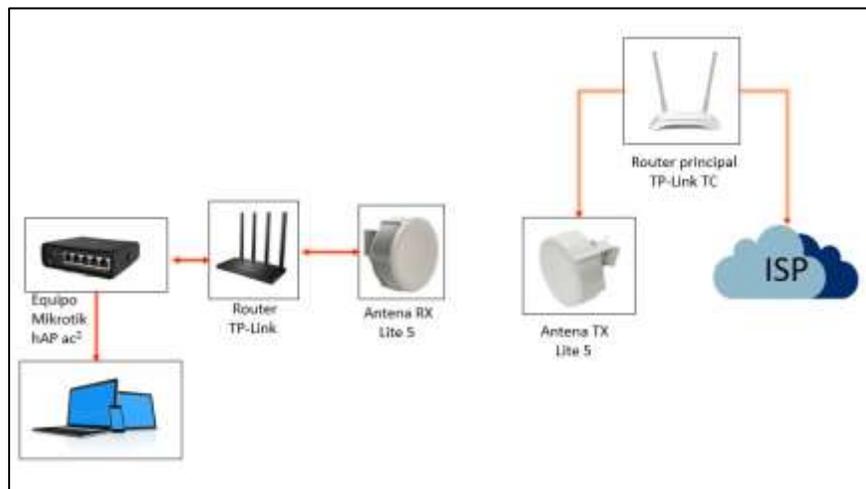
requiere una configuración con Wi-Fi integrado, y se busca un balance entre costo y funcionalidad.

**Tabla 2.** Especificaciones de Equipos Mikrotik

<b>Modelo</b>	<b>CPU</b>	<b>RAM</b>	<b>Puerto Ethernet</b>	<b>Puerto SFP</b>	<b>Wi-fi</b>	<b>Precio</b>	<b>Comentarios</b>
RouterBOARD 3011UiAS	1.4 GHz Dual Core	GB	10x Gigabit	1	No	\$175.00	Buena relación costo-beneficio, adecuado para laboratorios .
RouterBOARD RD RB4011	1.4 GHz Quad Core	1 GB	10x Gigabit	1	No	\$379.99	Mayor rendimiento , útil si se espera expansión futura.
RouterBOARD HEX S	880 MHz Dual Core	256 MB	5x Gigabit	1	No	\$99.99	Más económico, pero con limitaciones en rendimiento .
RouterBOARD RD hAP ac2	716 MHz Quad Core	128 MB	5x Gigabit	0	Dual-band 24/5 GHz	\$103.00	Compacto, ideal para configuraciones que requieren

### Diseño de la red con portal cautivo

Actualmente, en el Laboratorio de Telecomunicaciones y Redes no se posee una red inalámbrica para los estudiantes, por lo cual se optó por una solución para brindar el servicio de internet y al mismo tiempo tener un registro de usuarios conectados a la red, lo que permite la gestión y asignación de ancho de banda. En la figura 6, se visualiza la topología actual de la red.



**Figura 1.** Diseño de la red con portal cautivo

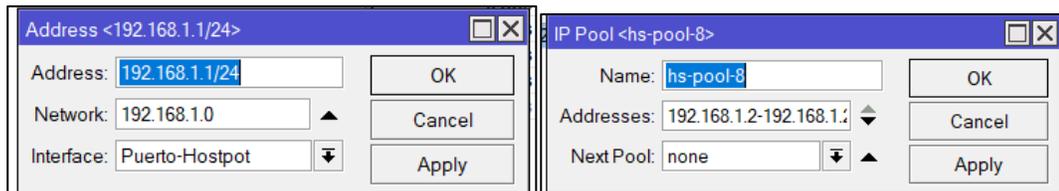
### Configuración de la red para el hotspot

Se configuró el puerto ether1-WAN para que reciba una IP de manera dinámica desde el router principal, para lo cual se selecciona el puerto y luego Apply. Posteriormente, se observa, como de manera automática le asigna la IP 172.16.20.244/24 a partir de la conexión WAN, como se muestra en la figura 2.



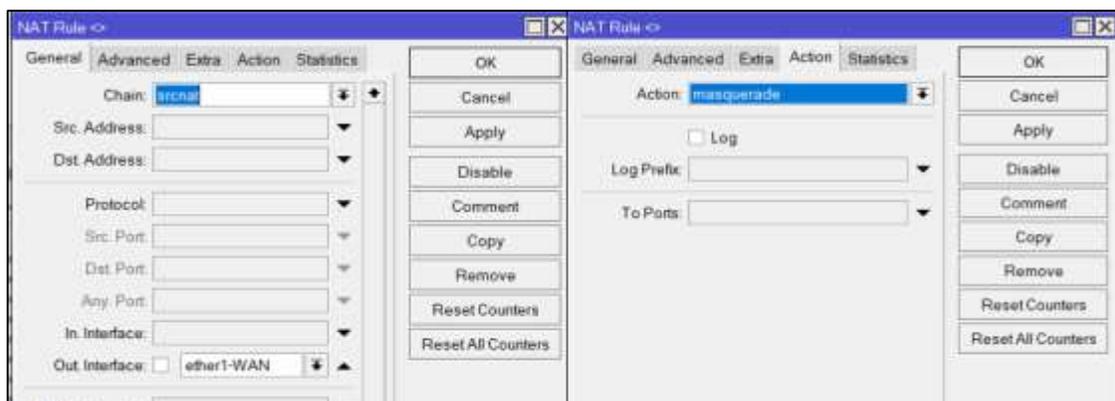
**Figura 2.** Configuración y designación de DHCP Cliente

Se configuró el Bridge con el nombre Puerto-Hostpot para que los equipos conectados de manera inalámbrica la red del equipo hAP ac2 y los puertos ethernet sobrantes del equipo estén en una misma red. Luego se configura la red para el Hostpot, en este caso será 192.168.1.0/24. Los dispositivos que se conectan al Hotspot, deben tener una IP asignada para que puedan tener conexión a la red, para lo cual se configuró un servidor DHCP. El servidor tendrá un rango de IPs de 192.168.1.2 a 192.168.1.254



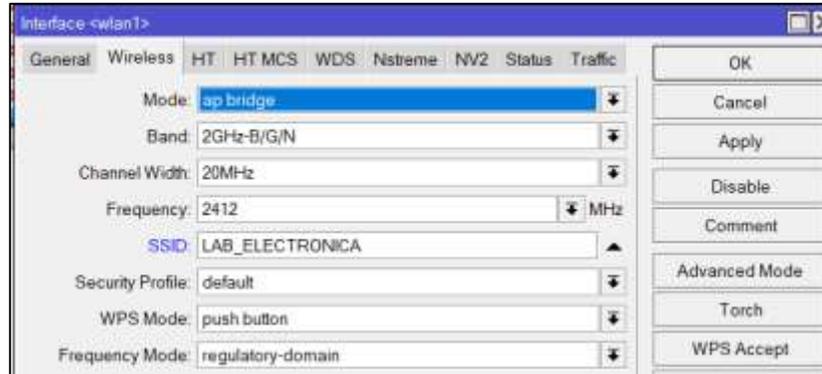
**Figura 3.** Configuración de a) IP al Hostpot b) pool para el rango de IPs

Además, se generó una regla en el firewall para que exista la traducción de IP privadas a públicas y poder tener conexión a internet, para ello se realizó un enmascaramiento, seleccionando la opción **masquerade**.



**Figura 4.** Traducción NAT

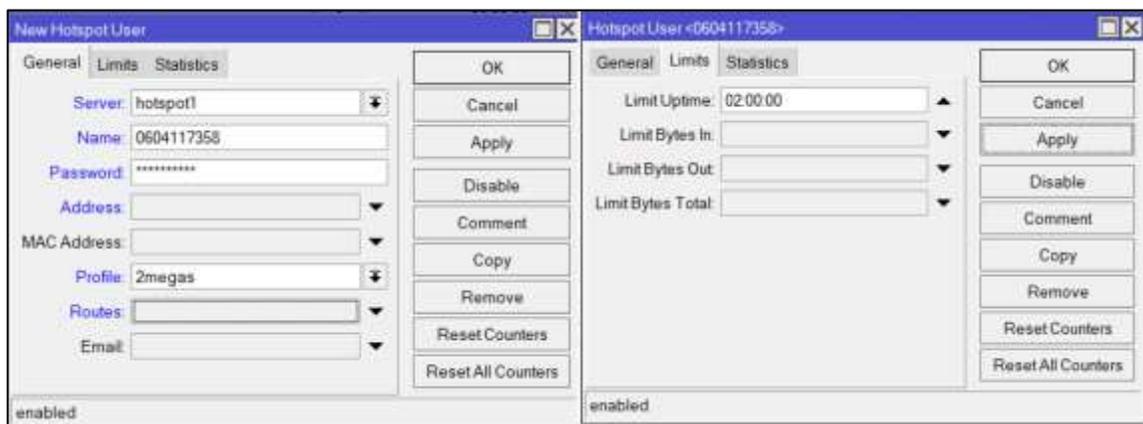
Para realizar la configuración inalámbrica, se generó una red con el SSID: LAB\_ELECTRONICA, en la banda de 2GHz-B/G/N, con un ancho de banda de 20 MHz, como se observa en la figura 5.



**Figura 5.** Configuración de red inalámbrica

### Configuración del servidor y perfil hotspot

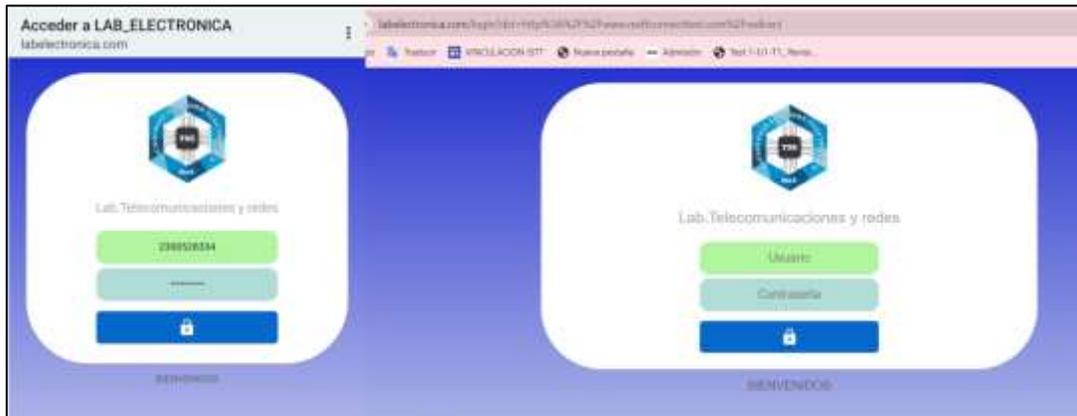
Para la configuración Hotspot, se creó el perfil del servidor Hotspot con el nombre hspot1 con la IP de gateway 192.168.1.1. El DNS con el que van a ingresar desde el buscador es labelectronica.com para logearse en el portal cautivo. Además, se configuró un ancho de banda 2 Mbps, junto con el tiempo de conexión de 2 horas por día, una vez pasado ese tiempo de conexión, automáticamente el hotspot lo inactiva hasta después de ver pasado 24 h. Adicional, se creó una plantilla de inicio cuando deseen acceder a la red.



**Figura 6.** Configuración a) usuario b) límite de conectividad 2 horas

### Prueba de métodos de autenticación

Se realizaron pruebas de conexión desde el celular y desde un computador, al inicio no pide contraseña para conectarse a la red, pero si pide logearse para acceder a la red.



**Figura 7.** Ingreso al portal cautivo a) celular b) computadora

### Prueba de gestión de ancho de banda a cada usuario

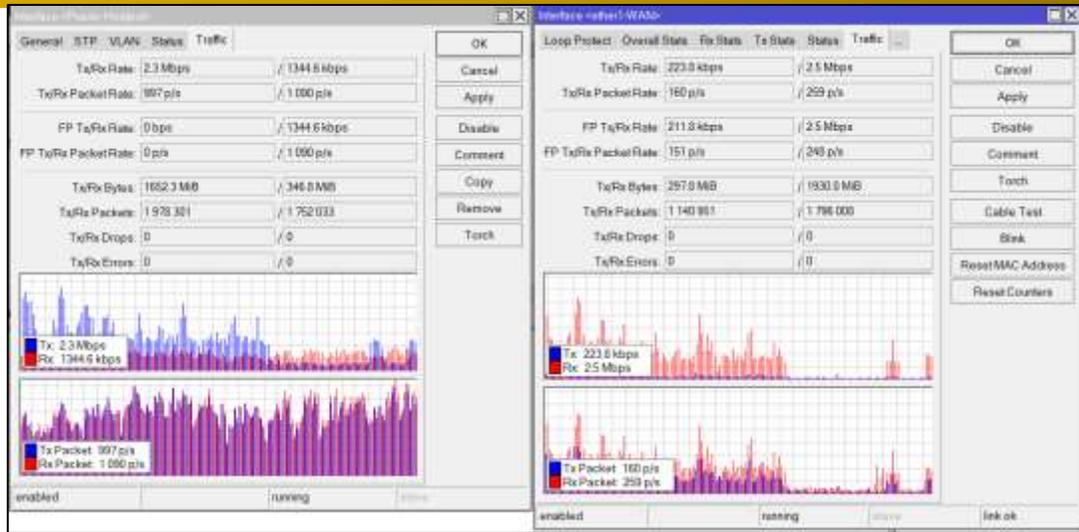
Se configuró para que los usuarios que se conecten al hotspot con una tasa de transmisión de 2 Mbps de bajada y 2Mbps de subida, como se observa en la figura 20. El tiempo que el usuario está conectado a la red se configuró de 2 horas, pasado ese tiempo el equipo se desconecta de la red y deberá esperar 24 horas para que pueda volver a conectarse.

User	Username	Address	Uptime	Idle Time	Session Time	Up Rate	Down Rate
Hotspot1	230000000	192.168.1.211	00:00:00	00:00:00	00:01:52	260.1 kb	1300.0 kb
Hotspot1	230000000	192.168.1.210	00:00:00	00:00:00	00:01:50	195.0 kb	954.0 kb
Hotspot1	170000000	192.168.1.210	00:00:00	00:00:00	00:01:30	195.0 kb	954.0 kb
Hotspot1	230000000	192.168.1.211	00:00:00	00:00:00	00:01:28	240.0 kb	1130.0 kb
Hotspot1	170100000	192.168.1.202	00:00:00	00:00:00	00:01:21	102.0 kb	1307.0 kb
Hotspot1	080500000	192.168.1.203	00:00:00	00:00:00	00:01:10	74.1 Mbps	623.0 kb
Hotspot1	080400000	192.168.1.204	00:00:00	00:00:00	00:01:10	74.0 Mbps	623.0 Mbps
Hotspot1	230000000	192.168.1.202	00:00:00	00:00:00	00:01:17	186.0 kb	1301.0 kb
Hotspot1	030000000	192.168.1.206	00:00:00	00:00:00	00:01:17	22.0 Mbps	461.0 kb
Hotspot1	170400000	192.168.1.207	00:00:00	00:00:00	00:01:14	140.0 Mbps	1700.0 kb
Hotspot1	230000000	192.168.1.208	00:00:00	00:00:00	00:01:12	96.0 Mbps	1700.0 kb
Hotspot1	230000000	192.168.1.205	00:00:00	00:00:00	00:01:08	74.0 Mbps	1701.0 kb
Hotspot1	230000000	192.168.1.200	00:00:00	00:00:00	00:01:05	100.0 kb	700.0 kb
Hotspot1	230000000	192.168.1.203	00:00:00	00:00:00	00:01:00	80.0 Mbps	1077.0 kb
Hotspot1	230000000	192.168.1.200	00:00:00	00:00:00	00:01:00	0.0 kb	0.0 kb
Hotspot1	230000000	192.168.1.200	00:00:00	00:00:00	00:01:00	0.0 kb	0.0 kb

**Figura 8.** Verificación de la limitación de la tasa de transmisión

### Prueba de usuarios concurrentes

Se realizó la verificación de la red al tener varios usuarios conectados al mismo tiempo, esto para observar que no se genere fallos en la red y puedan traficar sin ningún problema, cada uno con su ancho de banda destinado.



**Figura 9.** Tráfico de datos a) red del Hotspot b) Red WAN

## DISCUSIÓN

En la implementación de la metodología en cascada para el desarrollo del portal cautivo en el Laboratorio de Telecomunicaciones y Redes, se evidenció un enfoque secuencial y estructurado que facilitó la identificación de las necesidades técnicas y la integración de la infraestructura existente. El análisis detallado de los requisitos del portal cautivo, incluyendo la capacidad para manejar 30 usuarios concurrentes y la personalización de la experiencia del usuario, permitió definir con claridad los objetivos del proyecto. Además, la selección cuidadosa del equipo Mikrotik, como el hAP ac2, demostró ser una elección eficiente y económica para cumplir con los requisitos técnicos sin comprometer la funcionalidad.

Durante la fase de implementación, se destacaron las configuraciones específicas necesarias para establecer el portal cautivo, desde la integración del equipo con la infraestructura actual hasta la configuración detallada de las interfaces y la asignación de IPs. Las pruebas funcionales realizadas aseguraron la correcta autenticación de los usuarios y la adecuada asignación de ancho de banda, garantizando una experiencia fluida y libre de fallos. Este proceso meticuloso reflejó la importancia de un diseño de red bien planificado y una configuración precisa, lo que resultó en un sistema robusto y eficiente, adecuado para las necesidades del laboratorio.

## **CONCLUSIÓN**

Para la selección de los equipos para la implementación del portal cautivo se realizó un análisis de los requisitos técnicos para el portal cautivo. Luego, se realizó una tabla comparativa para determinar el equipo Mikrotik óptimo de acuerdo con los requisitos técnicos, donde se determinó que el equipo hAP ac<sup>2</sup>, con un procesador de 716 MHz y 128 MB de RAM, destaca por su doble banda Wi-Fi integrada (2.4/5 GHz). Este dispositivo se presenta como una opción compacta y eficiente, ideal para entornos donde se requiere una configuración con Wi-Fi integrado, y se busca un balance entre costo y funcionalidad.

En el portal cautivo se integró la autenticación de usuarios con el número de cedula como usuario y contraseña, sólo los usuarios dentro de la base del Mikrotik podrán conectarse generando de esta manera seguridad dentro de la red. Además, se asignó un ancho de banda de 2 Mbps de subida, como de bajada para que puedan tener una conexión de 2 horas cada día, generando el reinicio del contador de tiempo de uso a medianoche, de esta manera el usuario podrá tener una conexión de dos horas diarias cada día.

Para realizar la validación del funcionamiento del portal cautivo se realizaron pruebas de autenticación de manera satisfactoria. El ancho de banda de 2Mbps de subida y bajada fue designado con éxito, logrando un tráfico estable dentro de los rangos permitidos. Además, se realizaron pruebas de usuarios concurrentes donde se observó un tráfico constante.

## **REFERENCIAS BIBLIOGRÁFICAS**

- Cruz, D. (2011). *Diseño e implementación de un portal cautivo que permita la venta de tickets de internet*. Quito: Escuela Politécnica Nacional. Obtido de <https://bibdigital.epn.edu.ec/bitstream/15000/3953/1/CD-3714.pdf>
- García, M., Reyes, J., & Godinez, G. (2017). *Las Tic en la educación superior, innovaciones y retos* (Vol. 6). (R. I. Humanistas, Ed.) México. doi:<http://dx.doi.org/10.23913/ricsh.v6i12.135>

- Laguna, M. (2013). *Estudio sobre el uso de internet y sus aplicaciones en el alumnado e último año de carrera de la Universidad de Alicante*. Alicante: Universidad de Alicante. Obtido de [https://rua.ua.es/dspace/bitstream/10045/35701/1/Tesis\\_Laguna\\_Segovia.pdf](https://rua.ua.es/dspace/bitstream/10045/35701/1/Tesis_Laguna_Segovia.pdf)
- Prieto, E. (2015). *Implementación de un hotspot y una aplicación web para su gestión*. Madrid: Universidad Carlos III de Madrid. Obtido de <https://e-archivo.uc3m.es/rest/api/core/bitstreams/e668365c-8596-4e76-8c47-5b64e1a00db5/content>
- Zarate, E., & Villero, S. (2020). *El uso de los portales cautivos en redes WLAN a traves de dispositivos Mikrotik como la mejor herramienta para controlar el tráfico de datos*. La Guajira-Colombia: Revista Interdisciplinar de Estudios en Ciencias Básicas e Ingenierías. Obtido de <file:///C:/Users/jenef/Downloads/Dialnet-ElUsoDeLosPortalesCautivosEnRedesWLANATravesDeDisp-8742453-1.pdf>

**Conflicto de intereses**

Los autores indican que esta investigación no tiene conflicto de intereses y, por tanto, acepta las normativas de la publicación en esta revista.

**Con certificación de:**

