

**UNIVERSIDAD NACIONAL DE CHIMBORAZO**

**FACULTAD DE INGENIERÍA**

**ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN**

**“ESTUDIO COMPARATIVO DE PORTALES CAUTIVOS BASADOS EN SOFTWARE LIBRE PARA AUTENTIFICAR Y CONTROLAR UNA RED INALÁMBRICA DE LA ESCUELA GABRIEL GARCÍA MORENO”**

**TESIS DE GRADO**

**Previa a la obtención del título de**

**INGENIERO EN SISTEMAS Y COMPUTACIÓN**

**AUTOR (ES):**

CARLOS MAURICIO ESTRADA ARÉVALO

ADRIANO ESCUDERO WILLIAM ADRIANO

**TUTOR:**

Ing. Gonzalo Allauca Mgs

**RIOBAMBA-ECUADOR**

**2014**

Los miembros del Tribunal de Graduación del proyecto de investigación de título:

**“ESTUDIO COMPARATIVO DE PORTALES CAUTIVOS BASADOS EN SOFTWARE LIBRE PARA AUTENTIFICAR Y CONTROLAR UNA RED INALÁMBRICA DE LA ESCUELA GABRIEL GARCÍA MORENO”**

Presentado por:

CARLOS MAURICIO ESTRADA ARÉVALO

ADRIANO ESCUDERO WILLIAM ADRIANO

Y dirigida por:

ING. GONZALO ALLAUCA MGS

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

**Para constancia de lo expuesto firman:**

**Presidente del Tribunal (nombre) Firma ----------------------------------**

**Miembro del Tribunal (nombre) Firma ----------------------------------**

**Miembro del Tribunal (nombre) Firma ----------------------------------**

**AGRADECIMIENTO**

**DEDICATORIA**

**CAPITULO 1**

1. **MARCO REFERENCIAL**
   1. **Antecedentes**

La tecnología inalámbrica cobra más fuerza día a día, en el mundo donde la información digital forma parte indispensable de las actividades diarias de todas las personas, permitiendo la interconectividad entre computadoras, PDA`s, etc. Sin la necesidad de permanecer en un solo lugar, cada vez son más las instituciones tanto públicas como privadas las que ofrecen disponibilidad de usar una red, como aeropuertos, centros de educación, hoteles, etc.



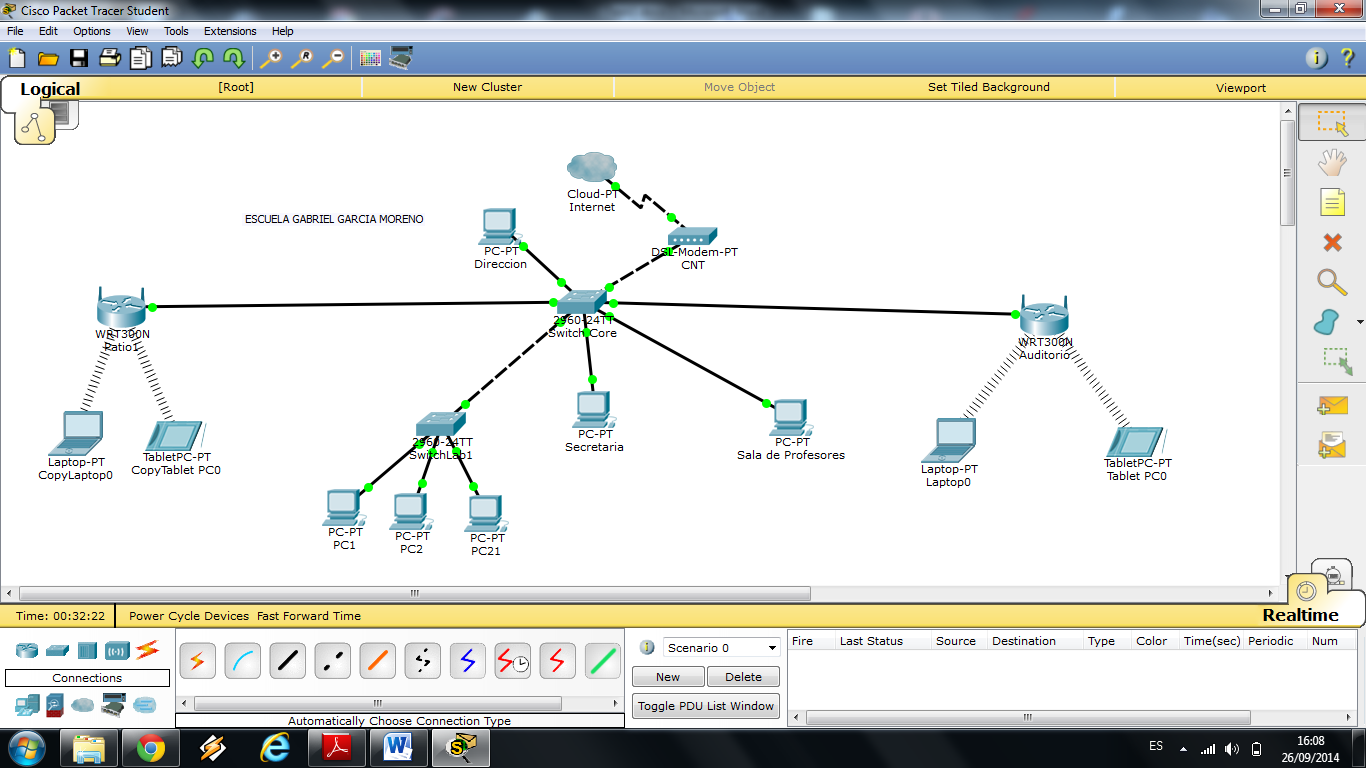
Figura 1. Zona Wifi

En la Actualidad existen muchas herramientas tanto gratuitas como de paga, para administrar la tecnología inalámbrica, entre las más utilizadas se encuentran los Hotspots, sin embargo estas aplicaciones pueden ser inseguras, y utilizadas por personas maliciosas que solo desean hacer daño a los usuarios de la red inalámbrica o a la misma empresa que presta este servicio.

La Escuela Gabriel García Moreno es una institución educativa Fisco misional con un elevado número de estudiante y docentes donde la educación interactiva así como la descarga de información digital forma parte de las actividades diarias a realizar. La institución educativa no pudo quedar fuera del avance tecnológico por tal motivo han implantado el servicio WIFI. En sus instalaciones para brindar acceso a internet a todos los miembros de la institución gracias al ancho de banda de 10MB.

Uno de los mayores inconvenientes del servicio inalámbrico de la institución es el de poseer una sola contraseña para la autenticación de la red en cualquier dispositivo móvil, lo que facilita el uso del internet inalámbrico a terceras personas que no están relacionadas con la institución educativa de tal manera que pueden consumir recursos de la escuela

La infraestructura que actualmente posee la institución educativa es:



La escuela Gabriel García Moreno Posee un Hotspot vulnerable y sin ningún tipo de seguridad, lo que provocaría la perdida de ancho de banda que podría ser utilizada por los miembros de la institución, y podría ser víctima de ataques por personas maliciosas.

Conocemos que existe un amplio ámbito de portales cautivos que ofrecen distintos, tanto de paga, en hardware u Open Source entre los cuales tenemos:

* CoovaChilli
* ChilliSpot
* EasyhotSpot
* ZeroShell
* WifiDog

Los cuales formaran parte del estudio a realizar.

* 1. **Justificación**

Con el pasar del tiempo la tecnología ha ido evolucionando cada día más y más, en la actualidad tanto como las computadoras portátiles y dispositivos móviles poseen tecnología que le permiten acceder alguna red inalámbrica e incluso tener acceso al internet. Lo cual implica tener un control seguro y fácil de manejar por parte de los administradores de red.

Las instituciones tanto públicas como privadas ofrecen a sus trabajadores un acceso inalámbrico que les permita tener acceso a la red y al internet para realizar su trabajo con calidad y eficiencia. Pero el principal problema de la mayoría de las instituciones que poseen ese servicio a sus trabajadores es la seguridad y el control de autenticación de usuario ya que sus trabajadores para poder tener acceso a dicho servicio en su computadoras personales o dispositivos móviles tiene que acercarse al administrador de la red para que el personal autorizado de acceso al servicio.

Por otra parte, en este proyecto de investigación se trata de analizar y determinar un método factible que ayude al administrador de red tener un mejor control de los usuarios que necesiten del servicio de internet inalámbrico, lo cual determinaremos con la comparación de portales cautivos basados en software libre que son una herramienta segura, gratuita, fácil de implementar , lo que le facilitara al administrador de la red el manejo y control sobre la red, también proporcionara a los usuario tener un registro automatizado para acceder al servicio de internet

* 1. **Objetivos**
     1. **Objetivo General**

Determinar un estudio comparativo de portales cautivos basados en software libre para autentificar y controlar la red inalámbrica de la Escuela Gabriel García Moreno.

* + 1. **Objetivo Especifico**
* Investigar, comparar los diferentes tipos de portales cautivos basados en software libre que existen en la actualidad.
* Determinar las medidas de seguridad que poseen los portales cautivos a la hora de ser implementados en una red inalámbrica.
* Analizar el estado en que se encuentra la red inalámbrica de una institución pública o privada
* Determinar un portal cautivo que se adapte a las necesidades de la red inalámbrica de una institución.
  1. **Hipótesis**

La implementación del portal cautivo permitirá obtener un mejor control de las redes inalamricas.

**CAPITULO II**

1. **MARCO REFERENCIAL**
   1. **TECNOLOGIAS Y SEGURIDADES INALAMBRICAS**
      1. **Redes inalámbricas**

Es la interconexión de distintos dispositivos con la capacidad de compartir información entre ellos, pero sin un medio físico de transmisión. Estos dispositivos pueden ser de muy variadas formas y tecnologías entre ellos [3]:

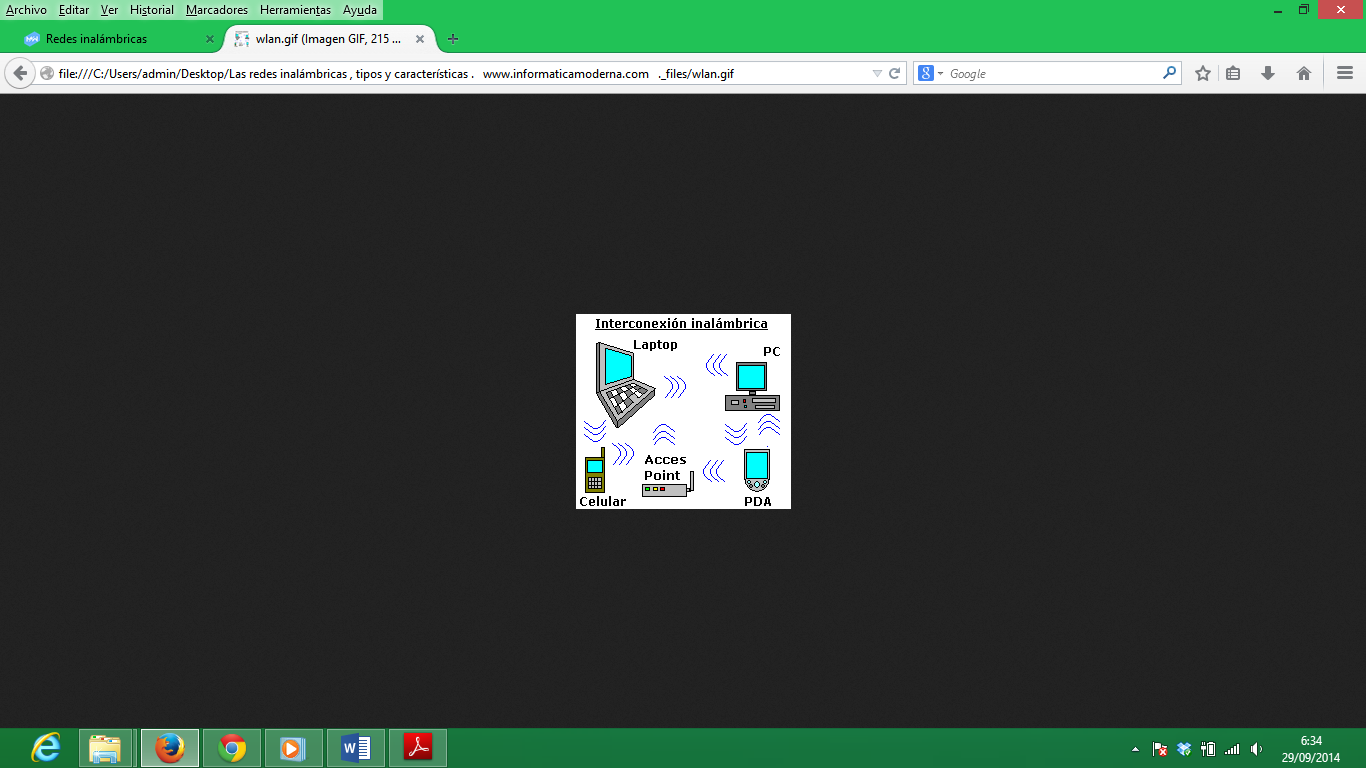


Ilustración 1: interconexión inalámbrica entre dispositivos

Permitiendo una mayor movilidad y versatilidad en la conexión a la red. Sin embargo, la red inalámbrica no pretende ser nunca un sustituto de la red cableada, y nunca se debe utilizar para puestos de trabajo permanentes. [2]

La infraestructura inalámbrica puede ser construida a muy bajo costo en comparación con las alternativas tradicionales de cableado. Pero construir redes inalámbricas se refiere sólo en parte al ahorro de dinero. Proveyendo a su comunidad con un acceso a la información más sencillo y económico, la misma se va a beneficiar directamente con lo que Internet tiene para ofrecer [1].

* + 1. **Tecnologías actuales para red inalámbrica**

1. **Wi-Fi ("*Wireless Fidelity*")**

En español significa literalmente fidelidad sin cables. También se les denomina WLAN ("*Wireless Local Area Network*") ó redes de área local inalámbricas, se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio con muy buena calidad de emisión para distancias cortas (hasta teóricamente 100 m). Este tipo de transmisión se encuentra estandarizado por la IEEE [3].

Para la transmisión es necesario el uso de antenas integradas en las tarjetas, además este tipo de ondas son capaces de traspasar obstáculos sin necesidad de estar frente a frente el emisor y el receptor.

- Actualmente son 3 estándares básicos:

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Tecnología | Velocidad de Transmisión | Características |
| Wireless B | IEEE 802.11b | 11 Mbps (Megabits por segundo) | Trabaja en la banda de frecuencia de 2.4 GHz solamente, compatible con velocidades menores. |
| Wireless G | IEEE 802.11g | 11 / 22 / 54 Mbps | Trabaja en la banda de frecuencia de 2.4 GHz solamente. |
| Wireless N | IEEE 802.11n | 300 Mbps | Utiliza una tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente. |

**Que utilidades tiene una Red WiFi?**

Las Redes WiFi pueden tener muchas utilidades prácticas para todo tipo de entidades, empresas o negocios.

* Acceder a una red empresarial desde cualquier punto.
* Acceder a Internet sin necesidad de cables.
* Conectarse sin cables con un pc, un portátil, una pda, un teléfono móvil o videoconsola con conexión WIFI.
* Servicio de HotSpot para acceso restringido por tiempo o volumen.
* Acceder a servicios de VoIP sin cables [2].

1. **Infrarrojos**

Es posible transmitir y recibir información mediante rayos infrarrojos, esta disciplina se engloba dentro de las comunicaciones ópticas no guiadas, IrDA es un estándar que define una forma de implementar el uso de la tecnología infrarroja por los fabricantes [4]. Es una tecnología de transmisión inalámbrica por medio de ondas de calor a corta distancia (hasta 1 m), capaces de traspasar cristales [3].

Esta tecnología, basada en rayos luminosos que se mueven en el espectro infrarrojo. Los estándares IrDA soportan una amplia gama de dispositivos eléctricos, informáticos y de comunicaciones, permite la comunicación bidireccional entre dos extremos a velocidades que oscilan entre los 9.600 bps y los 4 Mbps. Esta tecnología se encuentra en muchos ordenadores portátiles, y en un creciente número de teléfonos celulares, sobre todo en los de fabricantes líderes como Nokia y Ericsson.

1. Bluetooth

Es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz [5].

Los principales objetivos son:

* Facilitar las comunicaciones entre equipos móviles y fijos.
* Eliminar los cables y conectores entre éstos.
* Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

1. **Microondas:**

Se trata de comunicaciones a gran escala, muy caras y con poco uso doméstico. Las hay de dos tipos:

* **Satelitales:** se realizan a través de bases terrestres con antenas que envían señales al satélite, este se encarga de direccionarlas hacia la estación receptora con la onda amplificada para evitar pérdidas.
* **Terrestres:** se basan en conexiones denominadas punto a punto, ya que sus antenas deben estar sin obstáculos físicos para evitar fallas en la transmisión.
  + 1. **MECANISMOS DE SEGURIDAD INALAMBRICAS**
* WEP (Wired Equivalent Protocol)

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio.

Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionado por RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama.

* OSA (Open System Authentication)

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aun activando WEP, por lo tanto es un mecanismo poco fiable.

* ACL (Access Control List)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

* CNAC (Closed Network Access Control)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

* 1. **PORTALES CAUTIVOS**

Un portal cautivo es un software o hardware conectado a una red que vigila y controla el tráfico http y fuerza a los usuarios a pasar por una página especial si quieren navegar por internet. El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifique. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede controlar el ancho de banda usado por cada cliente

Generalmente, el sistema portal cautivo utiliza un navegador web como un dispositivo de autenticación que presentan las condiciones de uso y política de la empresa.

Un portal cautivo se suele utilizar en las redes públicas en donde un cliente es obligado a pasar por una página web de autenticación. Los portales cautivos normalmente se encuentran en las redes públicas como hoteles, bibliotecas, aeropuertos entre otras como una manera para que el proveedor fuerce a un usuario a aceptar los términos de servicio, a pagar por el uso, o autenticar antes de acceder a internet [6].

Un portal cautivo es muy útil a la hora de gestionar una red inalámbrica Wi-Fi, ya que podremos controlar los usuarios que se conectan a nuestra red, asignándoles un nombre de usuario y contraseña, ancho de banda y un tiempo limitado, con lo cual estamos brindándole el acceso a internet por el tiempo y forma que nosotros queramos[6].

* + 1. **Tipos de portales cautivos**
       1. **Por Software**

Entre los distintos sistemas de portal cautivo con software libre podemos señalar

* Easy HotSpot
* CoovaChilli
* ChilliSpot
* ZeroShell
* Wifi Dog
  + - 1. **Por Hardware**

Son equipos que se implementa sin necesidad de un ordenador:

* Cisco BBSM-Hotspot
* Nomadix Gateway
* Antamedia Hotspot Gateway
* Aptilo Access Gateway
* Mikrotik RouterOS