PROYECTO FIN DE CARRERA

INGENIERÍA TÉCNICA INFORMÁTICA DE GESTIÓN

Implementación de un hotspot y una aplicación web para su gestión.

Leganés, Octubre 2015

Autor: Eduardo José Prieto del Valle

Tutor: Juan Miguel Gómez Berbís

Director: Jose María Alvarez Rodríguez

Resumen

El auge de las nuevas tecnológicas y la creciente necesidad de conectividad a Internet han impulsado a muchas empresas e instituciones a ofrecer el servicio de conexión inalámbrica como un valor añadido. Para cubrir dicha necesidad surge el concepto de hotspot.

Pero no es solo necesario ofrecer dicho servicio, si no poder gestionarlo de una manera sencilla y eficiente.

Este proyecto realiza una búsqueda de soluciones para ambas necesidades; por un lado, creando un acceso gratuito a Internet y con el que cualquier persona, sin necesidad de tener nociones sobre informática, puede verse beneficiada del servicio. Por otro lado, facilitando que su gestión sea accesible y manejable por cualquier usuario mediante el uso de las tecnologías actuales y en cualquier situación.

Finalmente, se pretende que tanto los equipos hardware usados en el proyecto, como la solución software desarrollada no tengan un coste muy elevado y sean fácilmente ampliables con funciones futuras.

Palabras clave

Hotspot, redes de comunicaciones, redes inalámbricas, aplicación web, gestión.

Abstract

The rise of new technologies and the growing need for an internet connection have motivated many companies and institutions to offer wireless access service as an added value. To meet this need appears the hotspot concept.

But it is not only necessary to provide this service, it is important to manage the hotspot in a simple and productive way.

This project searches for solutions for both needs; on one hand, it makes a free internet access for anyone, even those who do not have knowledge of computing. This service can be used by anyone. On the other hand, it makes an easy to use and understandable way of management this system. This management can be applied in many situations and is supported by the new technologies.

Finally, the hardware devices, chosen for the project and the software solutions developed are a low cost design. Also they are easily expandable to future purposes.

Keywords

Hotspot, telecommunications networks, wireless networks, Web application, management.

Índice

Índice de figuras

Índice de tablas

1. INTRODUCCIÓN

Con los últimos dispositivos y tecnologías desarrollados en el entorno de las telecomunicaciones se dispone de la capacidad de poder estar conectado en cualquier momento a Internet. Lo que lleva a poder navegar por páginas web, revisar el correo electrónico o la agenda, establecer comunicaciones con amigos y familiares o simplemente disfrutar de un rato de ocio.

Entre los dispositivos que brindan dicha capacidad estarían los dispositivos móviles, y como tecnologías, se puede citar las redes inalámbricas. Dichas redes se implantaron, en primer lugar, en ámbito doméstico pero cada vez es más habitual que estas redes proporcionen acceso a Internet en lugares públicos en los que se desarrolla una parte importante de la vida.

Ofrecer acceso a Internet de manera gratuita puede ser una característica de diferenciación en negocios como hoteles y restaurantes. Puede hacer más ameno y llevadero ese tiempo de espera en estaciones y aeropuertos o en el trayecto realizado en medios de transporte, como aviones o trenes, y puede ser una necesidad a cubrir en eventos como ferias y convecciones que tengan que ver o no con las tecnologías. Para ello se puede proporcionar este acceso a internet desde un *hotspot* o punto de acceso público.

Pero no solo es importante el desarrollo y la implementación de este punto de acceso público si no también el modo de gestionarlo. Habitualmente si este punto de acceso se proporciona en equipos hardware, estos requieren de unos conocimientos para ser manejados. La idea es desarrollar un sistema de gestión que sea de fácil manejo para cualquier usuario y que no requiere de conocimientos avanzados en informática o redes.

Este proyecto intenta realizar una búsqueda de soluciones que permitan poner en funcionamiento tanto el punto de acceso público hotspot y brindar un acceso a internet, como su entorno de gestión accesible y manejable por cualquier usuario mediante el uso de las tecnologías actuales.

1.1 Problemática y necesidad

Para explicar la problemática de este proyecto es preciso definir anteriormente una serie de términos y conceptos que son la base sobre la que se desarrolla. Con este punto se quiere facilitar la compresión de lo escrito así como acercar al lector los conceptos y términos que se van a tratar en los puntos posteriores de la memoria y sentar las bases para que comprenda la utilidad y el funcionamiento del sistema.

1.1.1 ¿Qué es un hotspot?

Se puede denominar hotspot a un lugar en el que se ofrece acceso a internet de manera pública. Para ello se dispone de una red inalámbrica con uno o varios puntos de acceso y de un dispositivo enrutador que se encarga de realizar la conexión con el proveedor de internet.

En muchas situaciones se define hotspot como el equipo o dispositivo hardware que se encarga de autorizar a los usuarios para que puedan acceder a algunos recursos de la red.

De forma habitual los hotspot suelen ser usados en sitios públicos, como pueden ser aeropuertos, cafeterías, hoteles y bibliotecas, donde los usuarios disponen de un acceso a internet, ya sea de forma gratuita o mediante algún pago.

Este servicio de acceso a internet, suele ser ofrecido mediante redes inalámbricas. Para ello se utilizan los puntos de acceso, que crean la red de datos inalámbrica a la cual se conectan los dispositivos clientes. Estas transmisiones de datos se suelen efectuar en la frecuencia de 2.4 Ghz, aunque también puede ofrecerse en la frecuencia de 5 Ghz.

Los dispositivos clientes usados pueden ser: ordenadores portátiles, teléfonos móviles con capacidad de navegación (smartphones), PDA o tablet; aunque hoy en día cada vez más dispositivos cuentan con capacidad de conexión a redes inalámbricas y de navegación, por lo que también podrían ser usados para disfrutar dicho servicio de internet.

Se puede ver en el siguiente esquema un ejemplo de configuración de un hotspot.

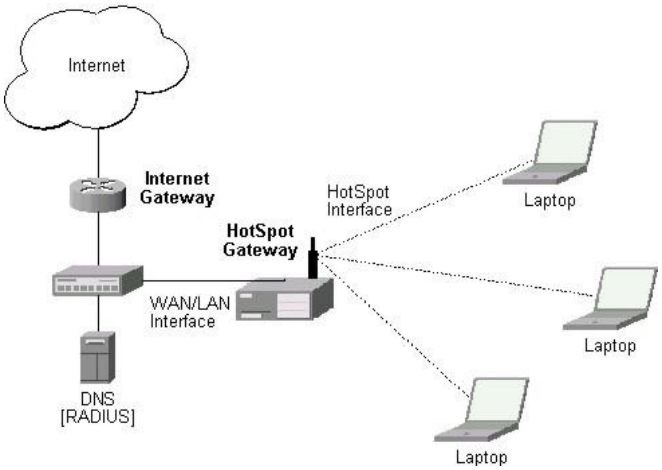

Figura 1 – Esquema de un hotspot [hot]

1.1.2 ¿Cómo funciona un hotspot? Concepto de portal cautivo.

El funcionamiento habitual de los hotspot es que dispongan de un portal cautivo. Se puede entender como portal cautivo una máquina o software que se encarga de controlar el tráfico de navegación y obliga a los usuarios a pasar por una página web de validación para habilitar el tráfico de manera normal. Con este método se consigue poder controlar tanto la navegación de los usuarios, refiriéndose al tipo de tráfico que generen, el número de usuarios concurrentes, el tiempo que se quiere que los usuarios puedan disfrutar de dicho acceso a internet, así como el ancho de banda o la cantidad de tráfico (numero de bytes) del cual disponen en el acceso.

Esta página web funciona a modo de pasarela permitiendo el acceso a la navegación a los usuarios. El método de validación más habitual suele ser mediante el uso de un usuario y contraseña proporcionados por la entidad que gestiona el hotspot. Por ejemplo, en el caso de un hotel, facilitados en recepción en el momento de la entrada o entrega de llaves de la habitación. Existen otros métodos de validación (usando la dirección física, dirección mac, del dispositivo cliente que realiza la conexión con el portal cautivo) que también se pueden usar aunque seguramente el método de usuario y contraseña sea el más extendido y habitual.

Para acceder a este portal cautivo y poder usar el servicio, los usuarios pueden utilizar cualquier navegador web, por tanto lo están obligados a instalar ningún software adicional en su sistema o en sus dispositivos.

El portal cautivo puede contener información sobre la entidad que gestiona el hotspot así como las condiciones de uso del servicio (tipo de tráfico permitido, responsabilidad legal, etc.) En muchos ámbitos también puede ser interesante introducir información relacionada con la entidad, por ejemplo, se puede usar el portal cautivo para publicitar otros servicios que ofrezca la entidad. Este punto puede ser aplicable en el caso de negocios de hostelería o restauración o en el caso de entidades o instituciones.

También se puede citar que los sistemas hotspot suelen ofrecer la posibilidad de permitir la navegación a algunas páginas web a los usuarios sin haber accedido al sistema. Esta característica suele denominarse lista de páginas blancas o walled garden en inglés.

Como se ha comentado anteriormente el hotspot realizar una validación de los datos de acceso que introduce el usuario, estos datos de acceso tienen que estar almacenados en algún lugar para que puedan ser comparados con los que introduce el usuario y permitirle el acceso si son correctos o no.

Este almacenamiento de datos de acceso, puede realizarse en una base de datos local en el hotspot o puede realizar en un servidor externo, lo que se llama servidor radius. De igual manera si se quiere establecer unas políticas de acceso particulares para cada usuario estas deberán ser almacenadas en la misma base de datos interna o en el servidor externo.

1.1.3 ¿Para qué se usa un hotspot?

Como se ha comentado anteriormente el uso de hotspot suele ser habitual en lugares públicos en los que se quiere brindar un acceso a internet. Este acceso a internet se hace mediante redes abiertas por lo que se debe controlar y vigilar el tráfico que generan los usuarios.

Se puede usar el hotspot para controlar que los usuarios no generen tráfico con contenido ilícito o ilegal, de manera que se puede aplicar un filtro por contenidos o limitar el uso de determinados programas de descarga P2P. Se puede incluso permitir cierto tipo de tráfico a unos determinados usuarios pero no permitirlo para otros. Este ejemplo se puede aplicar en lugares como bibliotecas o centros de estudios donde los usuarios pueden ser profesores o alumnos.

También se aplica el uso de hotspot para limitar el tiempo de acceso de los usuarios al servicio, con lo que se controla que no se realice un abuso de este acceso público a internet.

Otro uso que se debe citar es el control del ancho de banda, un punto muy importante para asegurar el éxito y la calidad del servicio que se quiere ofrecer. Si se asegura a cada usuario un ancho de banda se evitan tanto problemas de sobrecarga como el mal uso de la red por parte de algunos usuarios con programas de descarga.

1.1.4 Conclusiones preliminares

Teniendo en cuenta todos los puntos anteriores se puede concluir cual es el problema a tratar en este proyecto, se desea ofrecer un servicio de acceso a internet para usuarios en una institución, entidad o negocio. Para resolver dicho problema se va a utilizar un hotspot.

Con el problema definido se puede tratar las necesidades a cubrir, se necesita que dicho acceso a internet pueda ser controlado, de manera que solo puedan acceder usuarios autorizados. Se necesita por tanto poder crear esos datos de autorización para los usuarios y almacenarlos, así como sus policitas de acceso.

También se apunta como necesidad poder realizar la gestión del hotspot sin tener que acceder al dispositivo donde esta implementado, de modo que una persona de la entidad, negocio o institución pueda realizar tareas de administración y de gestión sobre el hotspot.

1.2 Motivación y objetivos

La integración de un servicio gratuito de acceso a internet en un negocio puede ser un elemento diferenciador respecto a la competencia de otros negocios. Hoy en día el acceso a Internet se ha convertido en algo necesario e importante para muchas personas, ya sea por motivos de trabajo o porque desean estar siempre conectadas a Internet.

Las redes sociales han promovido esta necesidad de acceso a Internet permanente, de igual manera han contribuido los dispositivos móviles y las aplicaciones desarrolladas para ellos como pueden ser las de mensajería instantánea, intercambio de ficheros, imágenes o videos.

Para este acceso a Internet permanente por parte de los usuarios se puede dotar a un negocio, entidad o institución del sistema hotspot a desarrollar, lo que puede dar lugar a que los clientes se decidan o elijan un negocio por el hecho de ofrecer este acceso a Internet de forma permanente y gratuita.

Los sistemas hotspot habitualmente se desarrollan en equipos hardware bastante cerrados y costosos. Con cerrados se quiere decir que la empresa que los desarrolla incluye las funcionalidades que desea, que en muchos casos pueden no adaptarse a las necesidades del cliente. En este caso, se desarrollará un sistema teniendo en cuenta las necesidades más habituales para todo tipo de situaciones, pero este desarrollo podría ser ampliado en cualquier momento, ya que su realización con lenguaje de código abierto facilita su ampliación e inclusión de nuevas funciones.

Normalmente el equipo hardware en el cual se configura y se gestiona un hotspot, se llaman controladores. Estos controladores suelen tener un elevado coste. En este caso se ha apostado por dispositivos de bajo coste al alcance de cualquier persona y por código abierto para el desarrollo del proyecto.

Estos sistemas hotspot que se incluyen en controladores suelen requerir un cierto grado de experiencia o formación para su configuración y gestión. Para este proyecto se apuesta por entornos de fácil acceso para cualquier persona, dejando a un lado lo visualmente espectacular para centrarse en la facilidad de uso y la sencillez.

Una vez implementado el hotspot, se realizará el desarrollo del portal cautivo. Este portal cautivo puede ser personalizado para que se pueda incluir información de la entidad que maneja el punto de acceso u otra información que se desee.

Una vez completados estos dos desarrollos el hotspot estaría funcionando y podría ser útil en cualquier situación. Pero se tiene que tener en cuenta que para la gestión del hotspot se tendría que realizar accediendo al dispositivo.

Para evitar tener que formar a una persona en ese aspecto y también evitar que pueda cambiar algún parámetro de la configuración que provoque un mal funcionamiento del hotspot, o de la configuración de las redes de comunicaciones, se realizará la implementación de un entorno web para la gestión del hotspot, denominado portal de gestión.

Este entorno web sería mucho más amigable e intuitivo y podría ser gestionado por cualquier persona sin que sea necesario que tenga conocimientos de configuración de dispositivos para redes como pueden ser enrutadores o puntos de acceso.

Dentro de este entorno web existirían varias opciones de gestión. Una primera opción para ver el estado del servicio, para comprobar el funcionamiento del hotspot. Después, se tendrían opciones de consulta para ver los usuarios y perfiles de usuario que existen creados en el hotspot, así como una consulta de usuarios conectados en el momento actual.

Pero seguramente las funciones más deseables y que más facilidad proporcionarían, sería la creación de datos de acceso para usuarios del hotspot. Esta función se podría llevar a cabo introduciendo unos datos determinados para el nombre de usuario y contraseña que se le quiera proporcionar al usuario del hotspot o generando de manera aleatoria tanto el usuario como la contraseña de acceso.

Una vez generados estos datos de acceso para hacer más cómoda su comunicación al usuario, existiría la posibilidad de realizar la impresión de los mismos.

También dentro de la creación de datos de acceso para los usuarios del hotspot, otra función interesante a desarrollar sería la generación de un número determinado de datos de acceso para un perfil de usuario, determinado por el tiempo.

Es decir, generar aleatoriamente nombre de usuario y contraseña para un total de 10 usuarios, que van a usar el servicio durante 24 horas. Este punto sería especialmente útil para usos del hotspot en lugares como hoteles. Ya que permitiría poder ajustar el uso del servicio a la estancia del cliente en el hotel o en lugares donde el hotspot pueda tener muchos usuarios ya que habría que invertir mucho tiempo en la generación de un usuario aleatorio cada vez que se solicite.

De igual manera que en el apartado anterior, para facilitar la comunicación los datos de acceso generados estarían disponibles para su impresión.

Por último, se podría añadir alguna función más para la mejora de la gestión del hotspot, como por ejemplo, llevar a cabo la eliminación de manera automática de los datos de acceso de usuarios cuyo tiempo de uso del servicio ya haya caducado.

Como función a tener en cuenta para su desarrollo y que podría ser de utilidad, existiría la posibilidad de bloquear a un usuario mediante sus datos de validación, de tal manera que si se desea, sea posible denegar el servicio a dicho usuario por algún motivo.

Pensando que este sistema pueda ser fácilmente escalable, se podrían añadir más funciones que se consideren útiles para la gestión del hotspot mediante el entorno web.

En mi modesta opinión, en algunos de los casos donde se ofrece un acceso gratuito a Internet pero es necesario obtener una clave de acceso para disfrutar de dicho servicio, el usuario desiste de este uso ya que no está dispuesto a preguntar para obtener dicha clave. Simplemente por problemas de idioma al estar en el extranjero, porque haya que dirigirse a un punto o persona concreta para obtener dichos datos, o porque haya que facilitar varios datos,

como puede ser el número de teléfono para poder disfrutar de dicho servicio. Este inconveniente se piensa resolver en el proyecto realizando una página web para que los usuarios puedan darse de alta en el sistema por ellos mismos. Lo que llevará a poder usar el sistema en tres simples pasos acortando y minimizando las molestias tanto para el usuario como para el gestor del sistema.

Se incluyen en esa parte las molestias al gestor, ya que tampoco es muy productivo que una persona en el desarrollo de su actividad laboral, por ejemplo en un hotel, restaurante o convención tenga que estar interrumpiendo sus actividades para atender las peticiones de obtención de datos de acceso al servicio de Internet. Tampoco sería productivo dedicar a una persona exclusivamente a esta actividad. Aunque este punto puede que en muchas situaciones no sea visto como una molestia y sea una manera o modo de controlar un poco más el acceso al servicio de Internet.

Una parte importante a desarrollar sería implementar la opción en el portal cautivo para que los usuarios puedan obtener los datos de acceso al hotspot mediante el registro en un formulario web. De manera que se realice por ellos mismos y no sea necesaria la intervención de un gestor para la creación de usuarios. A este desarrollo se le dará el nombre de portal de registro.

Esta opción puede ser especialmente útil en el caso de lugares públicos en los que no se disponga de un punto al que acudir para solicitar los datos de acceso y en los que pueda haber un gran número de usuarios como puede ser ferias o convenciones.

Además se debe tener en cuenta que los tres desarrollos: el portal cautivo, el portal de gestión y el portal de registro deben estar adaptados para su correcta visualización en todo tipo de dispositivos, ya que como se ha citado anteriormente, es habitual que dispositivos móviles o tablet usen el hotspot.

Así, se pueden especificar los siguientes objetivos para el desarrollo del proyecto que serán tomados como metas a conseguir:

- Ofrecer un servicio de acceso a internet controlado mediante la implementación de un hotspot.

- Desarrollar el portal cautivo que solicitará los datos de acceso a los usuarios y se encargará de enviarlos al hotspot para la validación.

- Poder gestionar y administrar el hotspot sin tener que acceder a él, mediante el desarrollo de un acceso externo llamado portal de gestión.

- Ofrecer a los usuarios del hotspot poder realizar un registro automático para obtener los datos de acceso al sistema mediante un portal de registro.

2. ESTADO DEL ARTE

El acceso público a redes inalámbricas fue propuesto por primera vez por Henrik Sjödin en la conferencia NetWorld + Interop en el Moscone Center de San Francisco en agosto de 1993. Sjödin no utilizó el término punto de acceso, pero se refirió a redes inalámbricas de acceso público.

La primera aventura comercial para tratar de crear una red de acceso público fue realizada por una empresa fundada en Richardson, Texas conocida como PLANCOM (Public Local Area Network Communications). Los fundadores de esa empresa, Mark Goode, Greg Jackson, y Brett Stewart disuelven la firma en 1998, mientras que Goode y Jackson crearon MobileStar Networks. Dicha empresa fue pionera en establecer redes de acceso público en lugares como Starbucks, American Airlines y Hilton Hotels. La compañía fue vendida a Deutsche Telecom en 2001, quien la convirtió en "T-Mobile Hotspot". Fue entonces cuando el término "hotspot" se hizo un hueco en la terminología de redes de comunicaciones como una referencia a una ubicación donde existe una red inalámbrica de acceso público. [wik]

Durante los primeros años del siglo XXI con la expansión de las nuevas tecnologías, muchas empresas han pensado que la tecnología inalámbrica puede ser un gran negocio. Para ello se han desarrollado dispositivos para la emisión de redes inalámbricas de acceso de público, ya sean gratuitas o de pago.

Hoy en día estas redes de acceso público siguen creciendo, siendo muy habituales en lugares como campus universitarios, hoteles o aeropuertos.

El mapa interactivo iPass 2014 [ipa], que muestra los datos proporcionados por los analistas Maravedis Rethink, muestra que en diciembre de 2014 existen 46.000.000 de hotspot en todo el mundo. Más de 10.900 puntos de acceso están en trenes, aviones y aeropuertos (Wi-Fi en movimiento) y más de 8,5 millones son hotspot situados en comercios, cafeterías y hoteles. La región con el mayor número de puntos de acceso públicos es Europa, seguida de América del Norte y Asia.

Los dispositivos de Mikrotik [mik] ofrecen la posibilidad de implementar un hotspot, así como muchas otras funciones de red, por ejemplo, la creación de rutas, funciones de firewall, control de ancho de banda y calidad de servicio, VPN, etc.

Estos dispositivos ofrecen grandes posibilidades de configuración para las redes de comunicaciones, se dispone de un único dispositivo para poder realizar varias funciones y tienen capacidad suficiente para poder realizarlas.

Con este punto se ahorra en costes, ya que se evita tener que colocar varios dispositivos; directamente con el router de Mikrotik se tiene todo en uno y se evita tener que adquirir un dispositivo específico para cada función. De manera que con este dispositivo se tiene el hotspot y el portal cautivo en el mismo dispositivo, así como el router o firewall para gestionar la red y el punto de acceso que emitirá la red inalámbrica a la que podrán conectarse los clientes.

El sistema operativo del que disponen se denomina RouterOS, es un sistema basado en GNU/Linux que permite implementar funcionalidades para la creación, gestión y mantenimiento de redes de comunicaciones. Así mismo permite que mediante el uso de script se pueda automatizar muchas de las funciones que se puedan requerir.

El sistema operativo RouterOS también puede ser instalado en un ordenador, y por tanto permite realizar las funciones citadas anteriormente usando dicho dispositivo.

2.1 ¿Por qué implementarlo con un dispositivo de Mikrotik?

El sistema operativo RouterOS ofrece la posibilidad de implementar y configurar un hotspot con muchas opciones de las citadas anteriormente y por eso se ha elegido para su implementación. Se puede usar uno de sus modelos de productos, llamados *Routerboard,* para llevar a cabo dicha implementación. En ese mismo dispositivo podría configurarse una de sus interfaces de red para conectar con el proveedor de servicios de internet y/o utilizar otra de las interfaces de red para gestionar la red interna de la entidad que quiere dar servicio a internet con el sistema hotspot.

Figura 2 – Dispositivo Routerboard de Mikrotik [dis]

Dicha implementación abarcaría diferentes parámetros de configuración, como por ejemplo, la creación de perfiles de conexión determinados por el tiempo de uso del servicio, La configuración del ancho de banda del cual van a disfrutar los usuarios del hotspot, la creación de los datos de acceso determinados para que los usuarios accedan al servicio, la configuración del bloqueo a determinados programas de descarga o determinado tipo de tráfico.

Una vez implementado el hotspot, se configuraría el portal cautivo. De modo que se pueda incluir alguna personalización acerca de la entidad que ofrece el servicio de acceso a internet o

cualquier otra información que se desee, como puede ser temas de responsabilidad legal o avisos de acuerdo a las leyes vigentes en cada país o estado.

2.2 Sistemas y aplicaciones similares

A continuación se enumeran algunos de los sistemas hotspot existentes actualmente en el mercado. Por lo general se pueden dividir en sistemas software y sistemas hardware, aunque realmente los sistemas software necesitan después de un soporte hardware en el que sean implementados, el cual no está incluido. Los sistemas hardware integran tanto el dispositivo físico donde se implementa como el software para realizar las funciones. La lista que se detalla a continuación incluye sistema hotspot de ambos tipos.

También se especifica las ventajas y desventajas que pueden tener estos dispositivos si se les compara con el desarrollo del sistema hotspot que se hará en este proyecto.

- Unifi Controller de Ubiquiti Networks [ubi]

Se trata de un software desarrollo por la empresa Ubiquiti Networks cuyo principal objetivo es la configuración y gestión centralizada de puntos de acceso inalámbricos. Dentro de estas opciones de creación existe la posibilidad de poder configurar un hotspot para la red inalámbrica emitida por los puntos de acceso que están gestionados. Este hotspot también dispone de portal cautivo y opciones de configuración como limitación de ancho de banda para los usuarios. Este software está disponible para ser instalado tanto en Windows como Linux o Mac OS. La desventaja que tiene es que para las funciones de hotspot, el dispositivo donde se instala el software debe estar encendido siempre para que las funciones de hotspot estén activas, por lo que se tendría que sumar un elemento más a la arquitectura de red. Además, las funcionalidades de las que dispone para filtrado de tráfico son limitadas, no se puede realizar filtrado de tráfico P2P ni se puede denegar el acceso a una dirección ip concreta. Esta configuración se tendría que realizar con otro dispositivo cortafuegos.

En lo citado anteriormente este proyecto tiene una clara ventaja ya que con el dispositivo de Mikrotik se tiene todo de uno, sirve de router central de la red, de dispositivo cortafuegos y de dispositivo donde se implementará el hotspot. De manera que se pasa de tener con el software anterior tres dispositivos, a tener solo uno, con el consiguiente ahorro de costes de adquisición y mantenimiento.

Al tratarse de un dispositivo software, hay que sumar otro dispositivo hardware para la emisión de la red inalámbrica a la que se conectarán los usuarios del hotspot. Este dispositivo hardware es un punto de acceso inalámbrico pero también existe la desventaja de que el software solo es compatible con los puntos de acceso de su misma marca y solo está disponible para redes inalámbricas no para redes cableadas.

Otra ventaja que suma este proyecto es que el dispositivo de Mikrotik, también es capaz de realizar la emisión de la red inalámbrica para los usuarios del hotspot, es decir además de las funciones anteriores de router, cortafuegos y hotspot se suma la de punto de acceso inalámbrico. También se puede citar como ventaja que el dispositivo de Mikrotik permite realizar la implementación del hotspot tanto en redes cableadas como en redes inalámbricas y que permite el uso de puntos de acceso inalámbricas de cualquier fabricante.

En cuanto a las funcionalidades que incluye dicho software se puede citar que no es muy personalizable a la hora de crear diferentes perfiles para los usuarios, ya que por defecto vienen unos predefinidos para usar.

En este proyecto se piensa desarrollar como una de las funciones, la posibilidad de creación de diferentes perfiles según lo requieran los usuarios, de manera que se adapten a las necesidades de cada uno.

En el software no existe la posibilidad de realizar ningún proceso de registro automático del usuario, este siempre tiene que solicitar el acceso al gestor del sistema para que le proporcione unos datos de acceso. Unos de los puntos principales de este proyecto será la realización de un portal de registro para que el usuario pueda registrarse sin intervención del gestor del sistema.

Quizá la ventaja de este software reside en que su interfaz es muy amigable y que no requiere altos conocimientos de redes de comunicaciones para su puesta en marcha. Estos puntos se espera que se vean solventados al realizar la implementación del portal de gestión para realizar las tareas de administración y mantenimiento del hotspot de Mikrotik.

- CoovaChilli de Coova.org [coo]

Es un software para el control de acceso en hotspot, implementa el portal cautivo y su principal ventaja es que es de código abierto. Para realizar la autenticación de los clientes se utiliza un servidor radius.

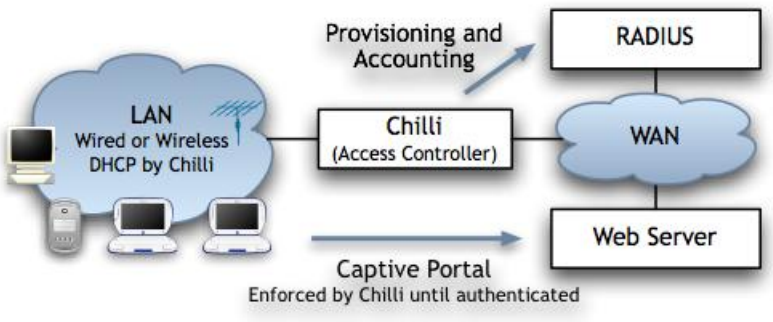

Figura 3 – Funcionamiento de CoovaChilli [fcc]

El funcionamiento es el siguiente, los usuarios sin autorizar son enviados al portal cautivo donde se le piden los datos de acceso. Una vez introducidos, el portal cautivo enviará estos datos al controlador que será el encargado de realizar la autenticación en el servidor radius. Si la autenticación es correcta, cambiará el estado del usuario a autenticado y este podrá navegar por Internet.

En este caso las desventajas de este software es que se debe dedicar un ordenador con el sistema operativo Linux para su funcionamiento y que tanto su implementación como mantenimiento requiere de conocimientos tanto en sistemas GNU/Linux como en redes de comunicaciones.

- Connectify Hotspot de Connectify [con]

Se trata de otro hotspot mediante software, aunque en este caso está más pensado para el uso de compartir conexión entre diferentes dispositivos. La opción que ofrece es la de compartir la conexión, ya sea inalámbrica o cableada, a internet desde un ordenador, de modo que otros dispositivos puedan conectarse a él y usar dicho servicio.

Convierte un ordenador en un router que funcionaría como puerta de enlace entre la conexión a internet y la red de comunicaciones donde estén conectados los demás dispositivos. Este funcionamiento se consigue mediante un software que implementaría las rutas necesarias para redirigir el tráfico de una red a otra.

Este software puede ser usado en ordenadores que cuenten con sistema operativo Microsoft Windows 7 o superior. Existen diferentes paquetes dependiendo de las características que se quieren usar.

Pero en cualquier caso, no dispone de opción para crear cuentas de usuario ni perfiles, simplemente está pensado para poder compartir la conexión.

- Wireless Hotspot Gateway HSG327 de 4ipnet [4ip]

En este caso se trata de un dispositivo hardware que permite implementar las funcionalidades de hotspot. Este dispositivo funcionaría como puerta de enlace entre el acceso a internet y la red inalámbrica a la cual estén conectados los clientes. Tendría incluido el portal cautivo de tal manera que los clientes deberían autenticarse para acceder a Internet. También ofrece la posibilidad de crear diferentes usuarios y diferentes roles (grupos de usuarios) a los que aplicar diferentes políticas. Estas políticas pueden estar basadas en el tiempo de uso o en la cantidad de tráfico que pueden generar los clientes.

Por otro lado también dispone de algunas funcionalidades de cortafuegos, aunque no dispone de filtro de contenidos o de filtrado por tipo de tráfico.

Como indica en su nombre, el dispositivo también incluye parte interfaz inalámbrica, por lo que desde el propio dispositivo es posible emitir la red inalámbrica para que se conecten los usuarios al hotspot.

Su uso estaría indicado para negocios de restauración, oficinas o comercios que deseen ofrecer una red inalámbrica a sus clientes para acceder a Internet. También dispone de una parte de monitorización para ver el estado de los usuarios y las conexiones que hay en uso en el hotspot.

- Wireless Hotspot HS1200N de NetCommWireless [net]

También se trata de un dispositivo hardware que funciona a modo de puerta de enlace entre la salida a internet y la red inalámbrica o cableada a la que estén conectados los usuarios del hotspot. Dispone de portal cautivo que también es personalizable para inclusión de información o avisos.

Permite crear usuarios y asignar diferentes políticas según el rol que tenga asignado cada usuario. También se puede limitar el uso del sistema por tiempo. Dispone de funciones de cortafuegos.

En este dispositivo también viene incluida la parte inalámbrica para la emisión de la red a la que se conectarán los usuarios del hotspot. Por lo que se evita el uso de más dispositivos.

En general, se puede decir que estos equipos hardware son bastante completos en las funcionalidades que ofrecen, con ellas se podrían adaptar a muchas de las entidades, instituciones o negocios donde se desea tener un hotspot, pero quizá esa sea una de sus desventajas ya que son equipos cerrados con funcionalidades definidas y que no son ampliables como puede ser el desarrollo de este proyecto.

Además, cabe tener en cuenta que para la gestión de este tipo de dispositivos se requiere conocimientos en redes de comunicaciones, lo que también se cuenta como desventaja ya que se desea un sistema que sea fácilmente usable por cualquier persona con unos conocimientos mínimos en informática.

También existe la desventaja que para su gestión se debe acceder a la misma interfaz que para su configuración con el consiguiente riesgo de realizar algún cambio en la configuración que provoque un mal funcionamiento del sistema.

3. ANÁLISIS

En este punto se realiza un estudio de las funciones que debería tener el sistema. Será efectuado a partir de unos requisitos que debe cumplir, especificando entre funcionales y no funcionales. Con este análisis se pretende conocer que debe hacer el sistema.

3.1 Especificación de requisitos

Se va a realizar en este apartado la especificación de los requisitos que tiene el desarrollo para el sistema completo, es decir, tanto para la parte de implementación del hotspot como para el desarrollo del portal de gestión.

Se debe tener en cuenta que estos requisitos se han pensando intentando cubrir las mayores necesidades posibles, pero que dependiendo del caso o entidad en la que se va a desarrollar el sistema podría tener que llevarse a cabo alguna adaptación en alguno de ellos.

A continuación, se muestra una lista de ideas que se han especificado en un primer acercamiento a los posibles requisitos que tiene que tener el proyecto:

1. El sistema controlará el acceso al servicio de Internet mediante un nombre de usuario y contraseña. (caracteres alfanuméricos y longitud comprendida entre 4 y 20 caracteres).
2. El sistema permitirá el acceso al servicio de Internet durante un tiempo limitado, indicado en el perfil del usuario.
3. El sistema impedirá la navegación a páginas web con contenido para adultos o con contenidos violentos.
4. El sistema impedirá el tráfico con contenido P2P.
5. El sistema limitará el ancho de banda para el tráfico de acuerdo a los límites establecidos.
6. El sistema impedirá el acceso de los usuarios al portal de gestión.
7. El sistema será accesible desde todo tipo de dispositivos, ya sean ordenadores, tablet o dispositivo móvil.
8. El sistema permitirá la conexión inalámbrica con todo tipo de dispositivos, ya sean ordenadores, tablet o dispositivo móvil.
9. El sistema impedirá a un usuario el acceso al servicio de Internet cuando se elimine sus datos.
10. El sistema impedirá el acceso de los usuarios al portal de registro una vez que se hayan registrado.
11. El sistema validará todos los datos introducidos de acuerdo a las restricciones especificadas.
12. El gestor accederá al portal de gestión para administrar el sistema sin necesidad de identificarse.
13. El gestor creará un usuario, introduciendo nombre de usuario (caracteres alfanuméricos y longitud comprendida entre 4 y 20 caracteres), contraseña (caracteres

alfanuméricos y longitud comprendida entre 4 y 20 caracteres) y perfil (seleccionado de la lista de perfiles creados en el sistema).

14. El gestor eliminará un usuario creado seleccionando nombre de usuario de la lista de usuarios creados.
15. El gestor consultará los usuarios creados en el sistema, mostrándose nombre de usuario, perfil y tiempo de conexión (1-31 días y/o 1-23 horas y/o 1-59 minutos).
16. El gestor creará un usuario con nombre de usuario y contraseña generados de manera aleatoria. (caracteres alfanuméricos y longitud comprendida entre 4 y 20 caracteres).
17. El gestor creará un número determinado de usuarios (1-32), con un perfil (seleccionado de la lista de perfiles creados en el sistema), con nombre de usuario y contraseña generados de manera aleatoria. (caracteres alfanuméricos y longitud comprendida entre 4 y 20 caracteres).
18. El gestor creará un perfil, introduciendo tiempo de uso (1-31 días y/o 1-23 horas y/o 1-59 minutos) cuyo nombre de perfil será generado con los valores de tiempo introducidos.
19. El gestor consultará los perfiles creados en el sistema, mostrándose nombre de perfil y tiempo de uso. (1-31 días y/o 1-23 horas y/o 1-59 minutos).
20. El gestor consultará los usuarios conectados al sistema en un momento determinado, mostrándose nombre de usuario, dirección ip (0-255.0-255.0-255.0-255), tiempo de conexión y tiempo restante. (1-31 días y/o 1-23 horas y/o 1-59 minutos).
21. El gestor eliminará un usuario conectado al sistema, seleccionando su dirección ip (seleccionado de la lista de usuarios conectados al sistema).
22. El gestor consultará información sobre el estado del sistema, como por ejemplo número de usuarios creados y número de usuarios conectados.
23. El gestor establecerá los límites de ancho de banda para el tráfico, tanto de descarga como de subida, de los usuarios conectados al sistema. (seleccionando lento, normal, rápida, sin límite).
24. El gestor borrará los límites de ancho de banda establecidos en el sistema.
25. El gestor añadirá una página web introduciendo su dirección (url), para ser visitada por los usuarios sin que estos tengan que introducir nombre de usuario y contraseña.
26. El gestor imprimirá un ticket, en el cual aparecen nombre de usuario, contraseña y perfil asignado (tiempo de uso).
27. El usuario accederá al servicio de Internet con un coste de 0 euros. (forma gratuita).
28. El usuario introducirá nombre de usuario y contraseña (caracteres alfanuméricos y longitud comprendida entre 4 y 20 caracteres) para acceder al servicio de Internet.
29. El usuario se registrará generando su propio nombre de usuario y contraseña. (caracteres alfanuméricos y longitud comprendida entre 4 y 20 caracteres).
30. El usuario accederá a la página web de la entidad que ofrece el servicio de Internet sin necesidad de introducir nombre de usuario y contraseña.

3.2 Definiciones

A continuación se muestra una lista de definiciones que se han obtenido con la lista de ideas realizada en el punto anterior que ayudarán a comprender mejor el sistema y realizar una especificación de requisitos funcionales:

- Usuario: se caracteriza por un nombre y una contraseña que son los datos para acceder al sistema. Tiene asignado un perfil.
- Perfil: se caracteriza por el tiempo de validez y se asocia al usuario.
- Gestor: realiza las funciones de gestión del sistema.
- Tráfico: comunicación del usuario hacia internet u otro destino.
- Ancho de banda: cantidad de tráfico que se puede enviar/recibir.

3.3 Requisitos funcionales

Con la lista de ideas obtenida como especificación de requisitos, a continuación, mediante una tabla, se indica los requisitos funcionales que han sido extraídos durante el análisis.

Id	Título	Descripción	Prioridad	Casos de uso
RF01	Acceder a internet	El sistema proporcionará acceso al servicio de Internet con un coste de 0 euros. (forma gratuita).	Alta	Acceder a internet
RF02	Solicitar usuario	El sistema tendrá una salida web en la que mostrará un formulario simple donde introducir los datos para acceder a internet.	Alta	Acceder a internet
RF03	Validar usuario	El sistema deberá validar los datos introducidos en el formulario para permitir el acceso a internet.	Alta	Acceder a internet
RF04	Limitar tiempo de uso	El sistema permitirá el acceso al servicio de Internet durante un tiempo limitado, indicado en el perfil del usuario.	Alta	Acceder a internet
RF05	Filtrar contenido web	El sistema impedirá la navegación a páginas web con contenido para adultos o con contenidos violentos.	Media	Acceder a internet
RF06	Filtrar tráfico P2P	El sistema impedirá el tráfico con contenido P2P.	Media	Acceder a internet
RF07	Limitar ancho de banda	El sistema limitará el ancho de banda para el tráfico de acuerdo a los límites establecidos	Alta	Acceder a internet
RF08	Bloquear portal de gestión	El sistema impedirá el acceso de los usuarios al portal de gestión.	Media	Acceder a internet

RF09	Bloquear acceso	El sistema impedirá a un usuario el acceso al servicio de Internet cuando se elimine sus datos.	Alta	Acceder a internet Borrar usuario Borrar conexión
RF10	Bloquear registro	El sistema impedirá el acceso de los usuarios al portal de registro una vez que se hayan registrado.	Alta	Acceder a internet
RF11	Validar datos	El sistema deberá validar todos los datos introducidos mediante formularios.	Alta	Varios
RF12	Portal de gestión	El gestor accederá al portal de gestión para administrar el sistema sin necesidad de identificarse.	Alta	Varios
RF13	Crear usuario	El sistema añadirá un usuario (con los datos introducidos por el gestor) al sistema.	Alta	Crear usuario
RF14	Borrar usuario	El sistema eliminará un usuario (seleccionado por el nombre) del sistema.	Alta	Borrar usuario
RF15	Consultar usuarios	El sistema mostrará un listado de los usuarios creados.	Media	Consultar usuarios
RF16	Generar aleatorio	El sistema añadirá un usuario generado aleatoriamente a la estructura de datos existente.	Alta	Generar usuario aleatorio
RF17	Generar aleatorios	El sistema añadirá un número determinado de usuarios generados aleatoriamente a la estructura de datos existente.	Alta	Generar numero usuarios aleatorios
RF18	Crear perfil	El sistema añadirá un perfil especificado por el tiempo a la estructura de datos existente.	Alta	Crear perfil
RF19	Consultar perfiles	El sistema mostrará un listado de los perfiles creados.	Media	Consultar perfiles
RF20	Consultar usuarios conectados	El sistema mostrará un listado de los usuarios conectados.	Media	Consultar conexiones
RF21	Borrar usuario conectado	El sistema eliminará un usuario de la lista de usuarios conectados.	Alta	Borrar conexión
RF22	Consultar información	El sistema mostrará información sobre el estado del mismo.	Media	Consultar información
RF23	Establecer limites	El sistema establecerá como limites de ancho de banda para el tráfico, el valor introducido por el gestor.	Alta	Establecer limites
RF24	Borrar limites	El sistema borrará los límites de ancho de banda que estén especificados, dejándolos como sin límite.	Media	Establecer limites
RF25	Añadir pagina blanca	El sistema mostrará una salida web con un formulario simple donde introducir los datos para añadir una página web.	Media	Añadir web a lista blanca

RF26	Imprimir ticket	El sistema imprimirá un ticket, en el cual aparecen nombre de usuario, contraseña y perfil asignado (tiempo de uso).	Alta	Varios
RF27	Portal de registro	El sistema tendrá una salida web en la que mostrará un formulario simple donde introducir los datos para realizar el registro de un usuario.	Alta	Registrarse
RF28	Registrar usuario	El sistema creará un usuario con los datos introducidos por el usuario asignando a dichos datos el perfil por defecto.	Alta	Registrarse
RF29	Visitar página blanca	El sistema permitirá el acceso a la página web de la entidad que ofrece el servicio de Internet sin necesidad de introducir nombre de usuario y contraseña por parte del usuario.	Media	Acceder a internet

Tabla 1 – Requisitos funcionales

3.4 Requisitos no funcionales

A continuación, mediante una tabla, se indica los requisitos no funcionales del proyecto.

Código	Nombre	Descripción	Prioridad	Casos de uso
RNF01	Apariencia	Las interfaces visuales del sistema estarán adaptadas para su correcta visualización en todo tipo de dispositivos.	Alta	Todos
RNF02	Compatibilidad	El sistema será compatible con todo tipo de dispositivos que dispongan de conexión inalámbrica o Ethernet.	Alta	Todos
RNF03	Lenguaje	Todos los menús del sistema estarán disponibles en lenguaje español.	Alta	Todos
RNF04	Escalabilidad	El sistema debe ser escalable, de tal manera que pueda adaptarse a nuevas funciones.	Alta	
RNF05	Robustez	La información almacenada en el sistema debe ser fiable permitiendo la introducción de nuevos datos, modificación y eliminación de los mismos.	Alta	Todos
RNF06	Eficiencia	El sistema debe ser eficiente especialmente en la recuperación de información para las consultas y debe proporcionar un acceso concurrente a un número considerable de usuarios.	Media	Acceder a internet Consultar conexiones Consultar perfiles Consultar usuarios

Tabla 2 – Requisitos no funcionales

3.5 Diagrama de casos de uso

Teniendo en cuenta los requisitos que se han especificado se pueden tratar de organizar las funciones que podrá manejar el agente gestor, en el siguiente diagrama de casos de uso.

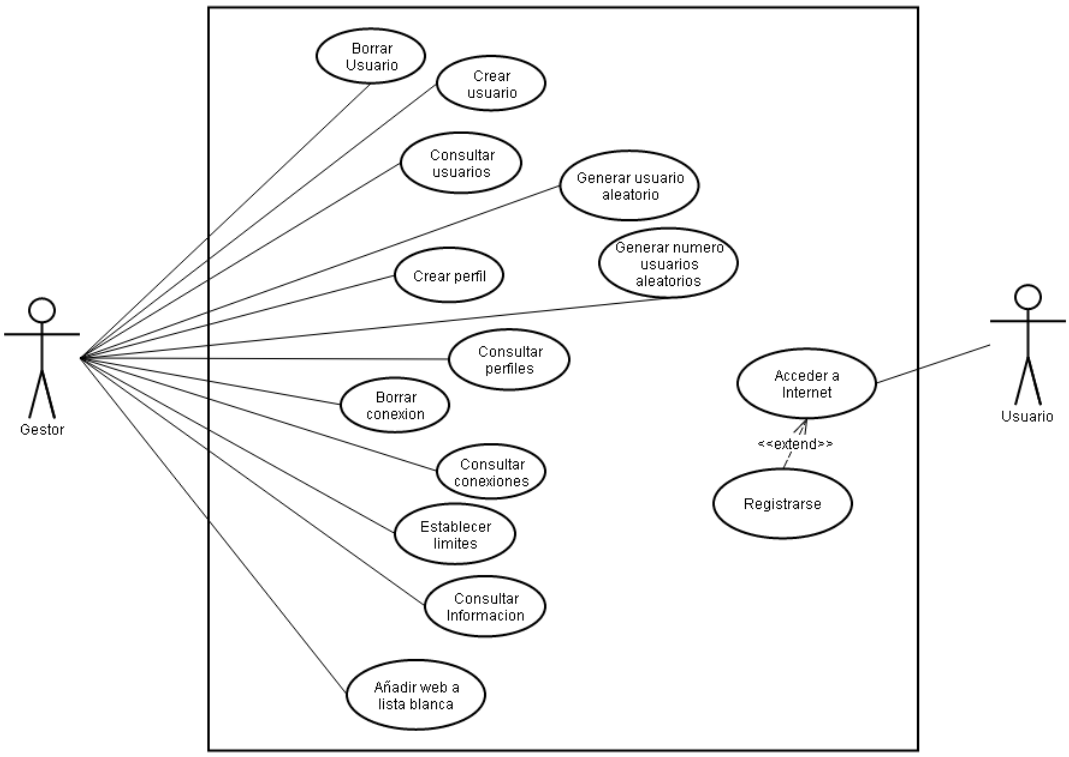

Figura 4 – Diagrama de casos de uso

Se pretende que en el momento de realizar el diseño de las funciones este diagrama sea de utilidad, que ayude a entender mejor qué funciones del sistema son accesibles para el gestor.

Para el otro agente que existe en el sistema, que será llamado usuario, porque será el que use el servicio propiamente dicho, solo tiene un caso de uso como se muestra en el diagrama, ya que la función que tendrá disponible será únicamente acceder a internet. Dependiendo de la página web de destino y del estado del usuario (si ya ha accedido o no al sistema) se le permitirá navegar a la página (aplicándole los distintos requisitos que se han especificado) o será redirigido a la página donde se le solicitarán los datos de acceso, conocida como portal cautivo. Desde el portal cautivo el usuario también tendrá la opción de registrarse por sí mismo, por lo que se ha añadido en el diagrama como una extensión del caso de uso acceder a internet.

3.6 Matriz de trazabilidad

A continuación se muestra la relación entre requisitos y casos de uso.

	Borrar usuario	Crear Usuario	Consultar usuarios	Generar usuario aleatorio	Generar numero usuarios aleatorios	Crear perfil	Consultar perfiles	Borrar conexión	Consultar conexiones	Establecer limites	Consultar información	Añadir web a lista blanca	Acceder a internet	Registrarse
RF 01													X	
RF 02													X	
RF 03													X	
RF 04													X	
RF 05													X	
RF 06													X	
RF 07													X	
RF 08													X	
RF 09	X							X					X	
RF 10													X	
RF 11	X	X		X	X	X		X		X		X	X	X
RF 12	X	X	X	X	X	X	X	X	X	X	X	X		
RF 13		X												
RF 14	X													
RF 15			X											
RF 16				X										
RF 17					X									
RF 18						X								
RF 19							X							
RF 20									X					
RF 21								X						
RF 22											X			
RF 23										X				
RF 24										X				
RF 25												X		
RF 26		X		X	X									
RF 27														X

RF 28														X
RF 29													X	
RNF01	X	X	X	X	X	X	X	X	X	X	X	X	X	X
RNF02	X	X	X	X	X	X	X	X	X	X	X	X	X	X
RNF03	X	X	X	X	X	X	X	X	X	X	X	X	X	X
RNF04		X				X		X					X	X
RNF05	X	X	X	X	X	X	X	X	X	X	X	X	X	X
RNF06			X		X		X		X				X	

Tabla 3 – Matriz de trazabilidad

4. DISEÑO

En el siguiente apartado, se realizará un análisis exhaustivo de todos los elementos que intervienen en el sistema. En este análisis se incluyen los elementos software que deberán ser desarrollados, las estructuras de datos y los medios físicos donde se almacenarán así como la arquitectura general del sistema para una futura implantación.

Se expondrán todos los aspectos relativos al diseño de este proyecto. En este caso, tanto del desarrollo del hotspot y su portal cautivo como del desarrollo del portal web para su gestión.

4.1 Elementos que intervienen en el sistema

Las entidades que componen el sistema son las siguientes:

- **Usuario**
  Es la persona que accede al servicio gratuito de acceso a Internet. Se caracteriza por tener un nombre de usuario y contraseña que son los datos que tendrá que introducir para poder acceder al sistema. Esta información de acceso será almacenada en el hotspot donde se realiza la comprobación de validez de los datos.
- **Perfil**
  Se puede definir un perfil como un grupo de usuarios que comparten características comunes, en este caso el tiempo de validez de sus datos de acceso. Esta información será almacenada en el hotspot donde se realiza la comprobación de validez del tiempo de validez. Para el tiempo de validez se tiene que especificar que dicho tiempo se pone en marcha desde la primera vez que se use el servicio, desde el primer acceso al sistema. Es decir si un usuario tiene asignado un perfil cuyo tiempo de validez es de veinticuatro horas, podrá usar el servicio desde el primer acceso con éxito hasta la misma hora del día siguiente.
- **Ticket**
  Relacionando los dos elementos anteriores, un usuario y el perfil al que pertenece, se puede llamar ticket al conjunto del nombre de usuario, contraseña y tiempo de validez. En el caso de nombre de usuario y contraseña, son datos necesarios para acceder al sistema y el tiempo de validez especifica el tiempo que se podrá usar el servicio. Serán presentados de manera que sean legibles para el usuario y tienen que estar disponibles para su impresión. En la siguiente imagen se puede ver un ejemplo de ticket:

Figura 5 – Ejemplo de datos de acceso

- **Conexión**
  Se entiende como conexión, la comunicación de un usuario con el sistema hotspot. Esta conexión estaría definida por el nombre de usuario y la dirección ip que le ha sido asignada en el momento de conectarse. Se tiene que explicar que esta conexión se almacena una vez que el usuario se ha validado correctamente en el hotspot. De tal manera que ya se disponga de su nombre de usuario para realizar la correcta relación comentada anteriormente. Esta conexión será almacenada en el hotspot.
- **Gestor**
  Será el agente encargado de usar el portal de gestión para realizar las diferentes tareas de gestión, administración y mantenimiento del hotspot.
- **Servidor web**
  El concepto de servidor web se puede detallar como el dispositivo o máquina donde se almacenará el portal de gestión. A este servidor será donde se conecte el gestor para realizar las tareas de administración del hotspot.
- **Router**
  En el sistema el router sería el dispositivo o maquina encargado de dirigir el tráfico entre las diferentes redes de comunicaciones. En este caso entre la red del hotspot, la red interna donde se aloja el servidor web y para ambos casos generar la salida a internet. También será el encargado de realizar tareas de cortafuegos para el bloqueo de tráfico.
- **Hotspot**
  Es la pieza clave del sistema, será el encargado de almacenar los datos de usuarios y perfiles, se encargará de captar todas las peticiones de páginas web de los usuarios para redirigirlas al portal cautivo, dicho portal cautivo estará alojado en el hotspot. También se encargará de realizar la validación de usuarios comprobando los datos introducidos en el portal cautivo con los que tiene en su base de datos.

4.2 Arquitectura de red del sistema

En el siguiente esquema se puede ver el esquema de la red y los dispositivos que la componen, así como los principales agentes que van a hacer uso de las funcionalidades del sistema. Con el esquema de la red se pretende ofrecer una consistencia del sistema y un rendimiento óptimos, evitar posibles ataques desde fuera de la red y ofrecer la posibilidad de aumentar las funcionalidades del sistema si se requieren.

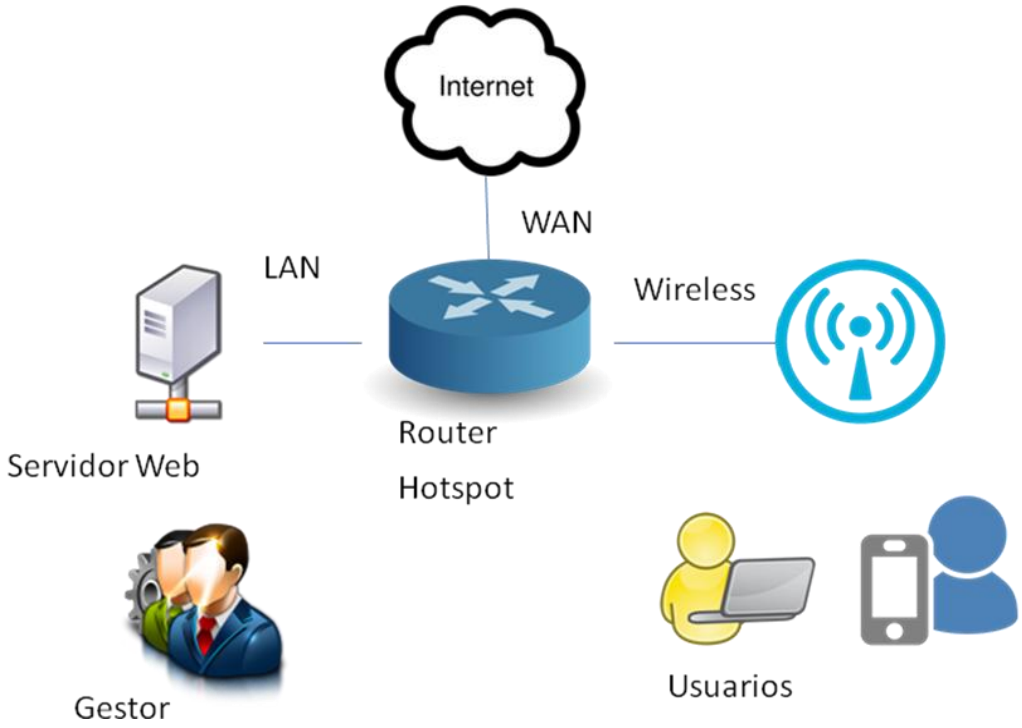

Figura 6 – Arquitectura de red del sistema

Se puede apreciar que el dispositivo router será el encargado de las comunicaciones entre las diferentes redes, permitiendo o denegando la comunicación cuando sea necesario. En el propio dispositivo que funciona como router también estará implementado el hotspot asociado a su interfaz inalámbrica.

El otro elemento importante de la red, será el servidor web, en el estarán alojados el portal de gestión y el portal de registro automático para los usuarios. Dicho servidor estará conectado al router por una de sus interfaces Ethernet, al igual que estará conectado a otra de sus interfaces Ethernet el ordenador del gestor con el que podrá acceder al portal de gestión al estar conectado en la misma red.

Los usuarios del hotspot se conectarán en este caso a la interfaz inalámbrica del router, donde estará activado el hotspot, de este momento al conectarse serán redirigidos al portal cautivo.

Para finalizar otra de las interfaces Ethernet del router estará conectada con el proveedor de internet para permitir el acceso a la red de redes.

4.3 Comunicación entre los elementos del sistema

En este punto se va a mostrar mediante un esquema donde están alojados los elementos del sistema y como se comunican entre ellos.

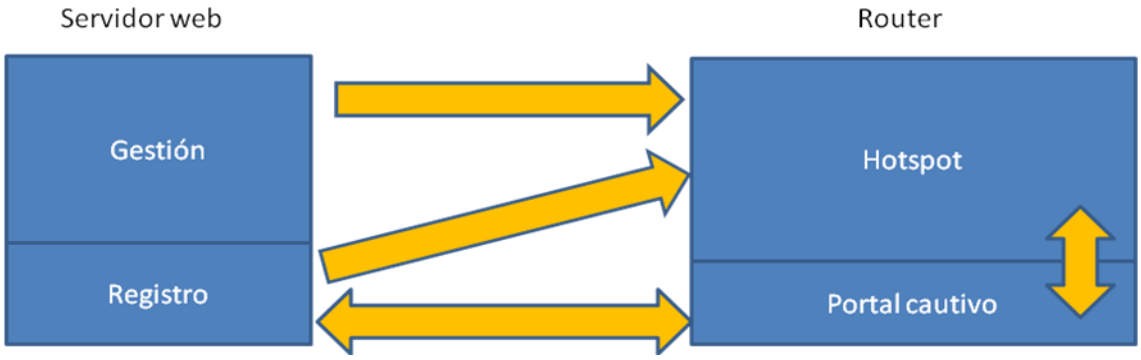

Figura 7 – Comunicación entre los elementos del sistema

Como se ha explicado anteriormente en el router estará implementado el hotspot y el portal cautivo, estos dos elementos se comunicación entre sí, el hotspot envía al usuario al portal cautivo y este será el encargado de solicitar al usuario los datos de acceso y enviarlos de nuevo al hotspot para realizar la comprobación de su validez o no. Si son correctos el hotspot permitirá al usuario la navegación por internet.

Desde el portal cautivo se podrá acceder al portal de registro, de tal manera que si un usuario acceder al portal cautivo y no dispone de datos de acceso, pueda llegar al portal de registro para obtenerlos.

Si decide registrarse el portal cautivo iniciará una comunicación con el hotspot para que esos datos sean introducidos como un nuevo usuario. De tal manera que devolviendo la comunicación al portal cautivo este usuario pueda acceder al sistema.

El portal de gestión será el encargado de realizar las comunicaciones con el hotspot, ya sea para introducir nuevos usuarios o perfiles, para realizar consultas de usuarios conectados o creados o para cambiar valores como los límites de ancho de banda.

También iniciará las comunicaciones para borrar usuarios creados o conectados, de cualquier manera siempre será el portal de gestión quien inicie la comunicación, por tanto la flecha que se ha colocado es unidireccional ya que el hotspot nunca iniciará por el mismo una comunicación con el portal de gestión sin que este la haya solicitado primero.

También se puede tener en cuenta el siguiente diagrama de componentes, donde se ven los componentes en los que se divide el sistema y las relaciones entre ellos.

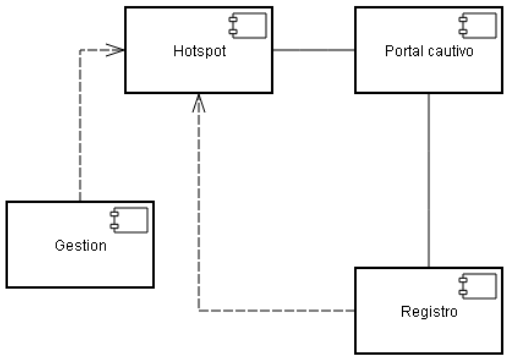

Figura 8 – Diagrama de componentes del sistema.

4.4 Diseño de los elementos del sistema

En este apartado se va a llevar a cabo una explicación de cómo realizan las funciones del sistema cada elemento que lo compone. Este paso es importante para después poder desarrollar la implementación, cuanto más detalle se ponga en el diseño más fácil será después realizar la implementación de cada elemento.

Para algunos de los dispositivos se realizará el diseño en pseudocódigo, en otros se explicará con el mayor detalle posible y en otros también será necesario definir la apariencia que tendrán al tratarse de las interfaces del sistema con las que interactuaran los agentes.

4.4.1 Diseño del router

En primer lugar se trata el diseño del router, encargado de proporcionar el acceso a internet y realizar la comunicación entre las redes. También será el encargado de realizar las funcionas habituales de un router, como puede ser la asignación de direcciones ip mediante un servidor de DHCP o la resolución de nombre de dominio, DNS.

- Configuración del acceso a Internet en una de las interfaces Ethernet mediante una dirección ip estática.
- Configuración de traducción de direcciones de red (NAT).
- Configuración de puerta de enlace por defecto (Gateway).
- Configuración de rutas de tráfico por defecto.
- Configuración de servidor de resolución de nombre de dominio (DNS).

- Configuración de cliente horario (SNTP).
- Configuración de interfaces Ethernet como red LAN para conexión del servidor web y del ordenador del gestor.
- Configuración de interfaz inalámbrica.
- Configuración de servidores de DHCP.
- Creación de perfil de seguridad para la red asociada a la interfaz inalámbrica.
- Activación de la interfaz para la emisión de la red inalámbrica.
- Configuración de puentes entre una interface Ethernet y la interfaz inalámbrica.
- Configuración de cuenta de acceso para la gestión del router.
- Configuración de reglas de cortafuegos, bloqueo de tráfico.
- Configuración de protección contra ataques de denegación de servicio (DoS).
- Configuración de protección a los clientes de la red.
- Configuraciones adicionales de seguridad para el router.

4.4.2 Diseño del hotspot

Una vez que se tiene especificado el diseño del router, el siguiente paso sería implementar en el router todo lo necesario para que el hotspot funcione de manera correcta.

- Configuración de reglas de direccionamiento de tráfico del hotspot. Con esta configuración lo que se hará es direccionar todo el tráfico del hotspot para que pase por el portal cautivo. De este modo, controlando si el usuario es autorizado o no, es decir si ha introducido sus datos de acceso, se le mostrará el portal cautivo o se le permitirá la navegación.
- Configuración de reglas de filtrado de tráfico. Con esta configuración se hace que se denieguen las comunicaciones de clientes que no estén autenticados. En cambio sí que son aceptadas las comunicaciones de clientes autenticados y que se realicen contra el portal cautivo.
- Configuración de la dirección ip del hotspot, con dicha ip se accedería al portal cautivo.
- Configuración de servidor de DHCP para asignación de direcciones ip en la red del hotspot.

- Configuración de nombre de dominio que se corresponde a la dirección ip, mediante ese nombre de dominio también se accederá al portal cautivo.

- Asignación de la interfaz inalámbrica del dispositivo Mikrotik como interfaz para el hotspot.

- Configuración de reglas de tráfico para permitir visitar una página web sin haber accedido al hotspot, esta configuración se realiza para que los usuarios puedan acceder al portal de registro y obtener así los datos de acceso.

- Configuración del método de autenticación de usuarios.

- Configuración del filtro de contenidos.

- Configuración de bloqueo de tráfico con destino a la red LAN privada donde se encuentra el portal de gestión y el ordenador del gestor.

- Configuración de bloqueo de tráfico con destino al portal de registro para usuarios que ya han accedido a internet mediante el portal cautivo.

- Configuración de filtrado de tráfico P2P.

- Creación de un perfil por defecto, con tiempo de uso de un día y de un usuario de pruebas.

- Creación de script para borrado automático de usuarios cuyo tiempo de validez ya se haya cumplido.

4.4.2.1 Métodos de autenticación

Para el desarrollo del portal cautivo del hotspot, una parte muy importante es el método de autenticación que se use para comprobar los datos de acceso de los usuarios. Existen varios métodos de autenticación que se podrían aplicar para validar dichos datos de acceso e incluso existen métodos en los que no sería necesario introducir ningún dato de acceso, ya que se obtendrían los datos del dispositivo que ha realizado la conexión. También se tiene que tener en cuenta que es posible configurar varios métodos de autenticación al mismo tiempo.

Se pasa a explicar cuales serian los métodos de autenticación que se podrían utilizar:

- **HTTP PAP**
  Se trata del método de autenticación más simple de todos los disponibles. Se trata de mostrar la página del portal cautivo y obtener los datos de acceso mediante un formulario, en este caso sería nombre de usuario y contraseña, en texto plano. En este caso se tiene que tener en cuenta que tanto el nombre de usuario como la contraseña no están cifrados al ser enviados por la red.

- **HTTP CHAP**

  En este caso es un método algo más complejo de autenticación. También consiste en mostrar la página del portal cautivo y obtener los datos de acceso mediante un formulario. Pero en este caso para validar los datos se usaría el protocolo de autenticación por desafío mutuo, llamado CHAP. En el siguiente esquema se puede ver cómo funciona este método:

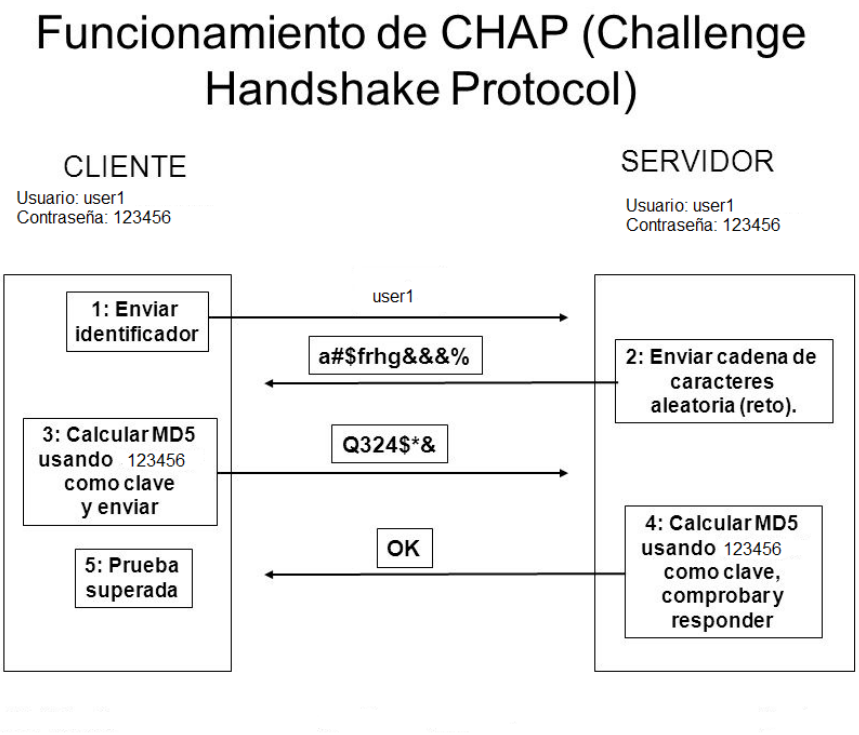

Figura 9 – Funcionamiento de protocolo CHAP [cha]

Para el sistema hotspot se usaría de tal manera que el portal cautivo se encargaría de generar la cadena de caracteres aleatoria, reto, En el momento que el usuario introduzca la contraseña, se realizaría la función MD5 usando el reto y la contraseña introducida. Este resultado serían los datos que se envían por la red para realizar la validación, de tal manera que la contraseña no viaja en claro por la red.

Una vez enviados los datos al hotspot, este se encargaría de realizar la misma función pero con los datos que tiene almacenados, si el resultado es el mismo permitiría el acceso al sistema.

Esta función MD5 se desarrollara en lenguaje Javascript de tal manera que pueda ser incluida en el código HTML del portal cautivo.

- **HTTPS**

  Este método es el más seguro en cuanto a la comunicación y confidencialidad de los datos, ya que los datos introducidos por el usuario serían encriptados con el protocolo SSL. Para que este método sea funcional es necesario disponer de un certificado que permita cifrar las comunicaciones.

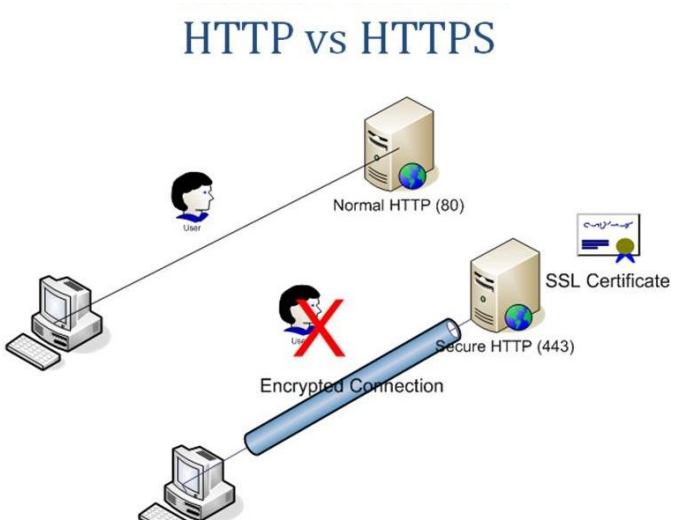

Figura 10 – HTTP vs HTTPs [htt]

- **HTTP cookie**
  En este método entran en juego las cookies, se puede definir una cookie como pequeña información enviada por un sitio web y almacenada en el navegador del usuario. En este caso cuando un usuario realiza el acceso con éxito, una cookie se envía a su navegador y también es almacenada en la base de datos del hotspot en la lista de cookies activas. Para la siguiente vez que el usuario intente acceder al hotspot se compara la cookie que envía el navegador y la almacenada en la base de datos, si la información que contiene ambas cookies concuerda se realizará el acceso automático del usuario con los mismos datos que la vez anterior. Este método está pensando para facilitar el acceso en intentos posteriores por lo que debe ser usado con alguno de los tres métodos anteriores que permitan al usuario acceder por primera vez y por tanto poder generar la cookie.
- **Dirección MAC**
  En cuanto un usuario se conecta al hotspot, es decir en cuanto envié el primer paquete de comunicación, ya ha enviado la información acerca de la dirección física del dispositivo que está usando para dicha conexión, por lo que se puede usar dicha dirección física como nombre de usuario para realizar el acceso.

- **Acceso de prueba (trial)**
  Se puede permitir a los usuarios usar el servicio durante un periodo de evaluación sin tener que tener datos de acceso. Por ejemplo se puede fijar un tiempo de acceso determinado para cada dirección física de dispositivo que se conecte. Este método estaría más pensado para casos en los que se vaya a cobrar por el acceso y se quiera poder disponer de un periodo de evaluación.

Teniendo en cuenta los puntos anteriores, con las ventajas y desventajas de cada método de autenticación, se ha decidido diseñar el hotspot con el método de autenticación de **HTTP CHAP**. Se ha considerado que este método es válido para el

desarrollo de este proyecto, ya que con él se evita que las contraseñas viajen en claro y puedan ser interceptadas.

Además como el desarrollo del proyecto se realiza sin saber específicamente en que entidad, institución o negocio podría usarse el hotspot, se ha optado por este método de autenticación, HTTP CHAP, que cubriría las necesidades básicas de todas ellas. No se descarta que si el proyecto se desarrolla para una instalación concreta se opte por HTTPS, que es más seguro, como método de autenticación.

Para este último caso tratado, habría que tener en cuenta si la entidad, institución o negocio estaría dispuesta a obtener un certificado SSL o habría que realizar uno autofirmado.

4.4.2.2 Filtrado por contenidos

Para el diseño del filtro de contenidos se han valorado diferentes opciones:

- El dispositivo de Mikrotik donde se implementará el hotspot, también ofrece la posibilidad de realizar un filtrado de direcciones IP mediante las capacidades de firewall de las que dispone. Para ello habría que configurar las direcciones IP de las páginas web que no se desean que sean visitables o configurar las que se desea que sean visitables para después añadir una regla donde se bloquee todo lo demás. También se podría realizar este bloqueo usando una palabra contenida en la url, de tal manera que el cortafuegos se encargaría de analizar cada paquete generada para ver si contiene la palabra que se desea bloquear. Esta opción no se aplicará ya que las páginas o palabras a permitir/bloquear pueden ser un número elevado lo que conlleva demasiadas reglas de firewall que sobrecargarán al equipo en el procesamiento de datos.
- Implementación de un filtro de contenido, también el dispositivo de Mikrotik ofrece la posibilidad de implementar un filtro de contenidos mediante un proxy. Esta opción permitiría filtrar por palabras dentro de la url, lo que daría opción por ejemplo de filtrar todas las url que contengan la palabra “sex”. Esta opción no se aplicará ya que siempre se va a escapar algún sitio web, dado que no filtra por el contenido del sitio solicitado, sino por la URL del mismo. La regla que se h aplicado anteriormente se cumpliría con la siguiente url de wikipedia: http://es.wikipedia.org/wiki/Sexo. La cual no necesariamente tendría que ser bloqueada, dado que no es sexo del tipo explicito.
- Implementación de un filtro de contenido utilizando las peticiones de DNS realizadas por los usuarios que estén conectados a la red inalámbrica del hotspot. Este filtro de contenidos es ofrecido por un servicio externo. Este tipo de filtrado si sería por contenidos propiamente dichos, lo que sería su principal ventaja, pero como inconveniente cabe citar que se depende de la actualización periódica, por parte del servicio externo, del tipo de páginas que se pueden visitar o no dependiendo del contenido y que es un servicio externo el cual no podrá ser gestionado.

A pesar de los inconvenientes citados, se ha optado por realizar el filtro de contenido mediante la tercera opción, usando las peticiones DNS de los usuarios. Para poder entender las cuestiones de diseño, se debe entender en primer lugar cómo funcionan las solicitudes DNS en Internet, con ayuda del siguiente esquema:

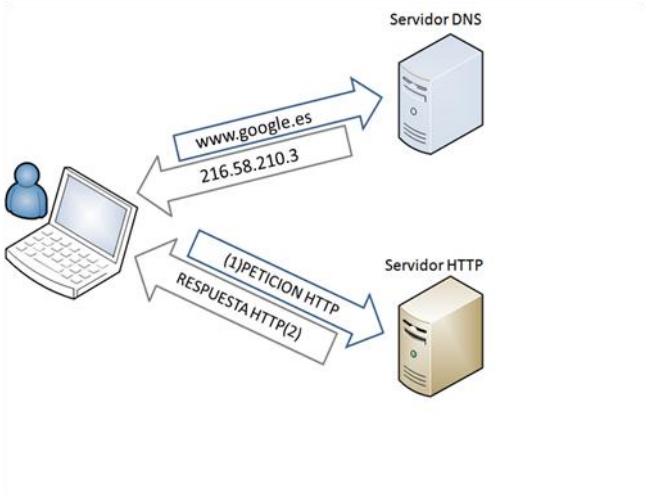

Figura 11 – Funcionamiento de DNS

En primer lugar el usuario introduce en la barra de direcciones del navegador la dirección www.google.es, si el ordenador no dispone de la dirección ip a la que corresponde dicha dirección solicitará al servidor DNS la dirección ip de www.google.es de manera transparente para el usuario. Este paquete es lo que se llama una petición DNS y en lo que se basa el filtro de contenidos por peticiones de DNS.

Habitualmente el servidor DNS devolverá al ordenador la dirección ip, en este caso 216.58.210.3 que es la correspondiente a www.google.es. Una vez que el ordenador tiene dicha dirección ip es cuando estará preparado para realizar la petición http al servidor www.google.es

En este caso el filtrado de contenido por DNS consiste en que la dirección IP correspondiente a una url, será facilitada o no por el servidor de DNS externo dependiendo de si se encuentra bloqueada o no. Este bloqueo se puede configurar mediante grupos de contenido, por lo que en este caso no se bloquea por la url del recurso si no por el contenido que tiene dicho recurso.

Uno de los servicios más populares para el filtrado por DNS es OpenDNS. Ofrece diferentes paquetes de acceso a su servicio, desde uno gratuito hasta servicios con coste pensados para empresas con más de 1000 usuarios y que permite no solo realizar el filtrado web si no proteger contra otras amenazas de la red. Para el desarrollo se va a utilizar el servidor DNS gratuito que cuenta con los grupos de contenido más habituales ya configurados para su bloqueo (por ejemplo contenido sexual o violencia).

En el caso de otras situaciones puede usarse el paquete de siguiente nivel que permite configurar los grupos y el nivel de bloqueo que se desea aplicar, para lo cual será necesario registrarse en su servicio.

Para que este filtrado por contenido basado en las peticiones de DNS, este funcionando en el hotspot, se llevará a cabo la siguiente configuración:

- Configuración de la ip del hotspot como servidor DNS para cualquier petición de DNS que se realice por usuarios conectados a la red del hotspot.

- Redirección de toda petición DNS en la red inalámbrica de hotspot a la ip del hotspot, tanto si es para usuarios que ya han accedido al sistema como si son usuarios que no han accedido.

- Configuración de los servidores DNS del servicio de OpenDNS como servidores externos para cualquier petición de DNS en el router.

Se ha considerado explicar las funciones de métodos de validación y filtrado por contenido ya que para ambas necesidades se han evaluado diferentes opciones de diseño.

Con este diseño se tendría un hotspot que llevaría a los usuarios al portal cautivo para realizar su validación. Estaría preparado para filtrar tráfico dependiendo del contenido, tipo o destino y sería capaz de aceptar clientes mediante conexión inalámbrica y asignarles una dirección ip.

Para que el hotspot este plenamente funcional, se necesita que el portal cautivo se muestre y sea capaz de realizar la validación de los usuarios.

4.4.3 Diseño del portal cautivo

El hotspot se encargará de direccionar todo el tráfico de los usuarios al portal cautivo de tal manera que estos puedan realizar la validación de sus datos de acceso.

Como se ha comentado antes se ha elegido como método de autenticación HTTP CHAP de modo que se implementará en la página web el código necesario para realizar dicho método de autenticación, para ello se utilizará la función MD5, implementada en código Javascript. Se realizará dicha llamada a la función con el valor introducido en contraseña y el valor de desafío. El resultado, así como el nombre de usuario, serán enviados al hotspot para realizar la autenticación.

También se incluirá un enlace al portal de registro para que los usuarios puedan obtener dichos datos de acceso si no los poseen.

Con estas dos ideas se diseña la apariencia del portal cautivo, una página web con un formulario web donde se pide introducir la información acerca del nombre de usuario y contraseña. Con un enlace en la parte inferior para comunicar con el portal de registro.

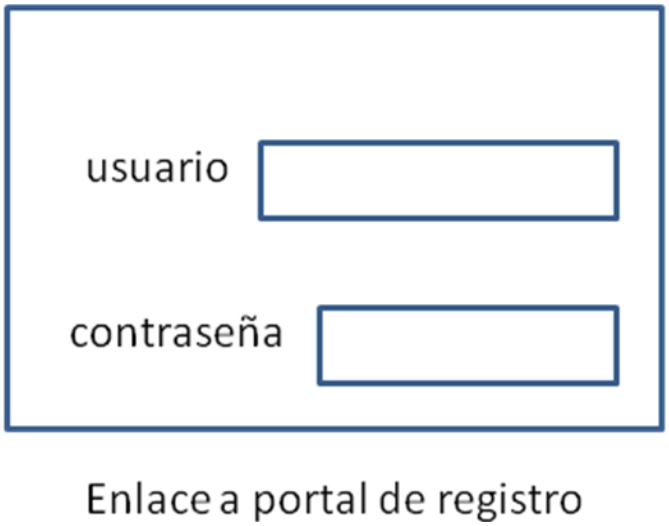

Figura 12 – Apariencia del portal cautivo

También debe adaptarse el desarrollo de las páginas del portal cautivo a todo tipo de dispositivos, de manera que se muestre correctamente en todos ellos.

4.4.4 Diseño del portal de gestión

En este apartado se trata el diseño del portal de gestión, el cual se comunicará con el hotspot para poder crear nuevos usuarios, borrar los usuarios existentes, crear nuevos perfiles o cambiar parámetros de configuración como los limites de ancho de banda.

A continuación se explicará de la manera más detallada el desarrollo e las funciones que son necesarias para la gestión y administración del hotspot.

4.4.4.1 Creación de usuarios

Para dar de alta a un usuario en el sistema de hotspot, el gestor solo tendrá que acceder al portal de gestión, mediante el menú de usuarios podrá llegar a la opción de crear. Una vez en dicha página se le solicitarán los datos correspondientes mediante un formulario. Estos datos necesarios son el nombre de usuario y la contraseña. Una vez introducidos deberá pulsar en el botón de crear para dar de alta al usuario.

Este acceso al portal de gestión por parte del gestor podrá realizarlo desde el ordenador que utilice para sus tareas habituales ya que la configuración desarrollada ha contemplado que el servidor web donde se encuentra el portal de gestión está conectado en la misma red local que el ordenador del gestor. Usando un navegador web podrá acceder al portal y realizar la

creación del usuario. Siendo el portal de gestión el encargado de realizar la comunicación con el hotspot de manera totalmente transparente para el usuario.

De este modo se evita al gestor tener que acceder al hotspot para la creación de un usuario y no se le obliga a tener que conocer la terminología que use el sistema tanto para la configuración o funcionamiento.

Volviendo al proceso de alta de un usuario, se le pedirán en un formulario web los valores que desea introducir como usuario y contraseña. Estos datos serán validados una vez introducidos, de manera que solo contengan caracteres alfanuméricos y su longitud esté comprendida entre cuatro y veinte caracteres. Si se cumplen dichas condiciones serán usados por el hotspot para crear el usuario. Estos valores deberán ser proporcionados por el gestor al usuario para que pueda acceder al sistema hotspot y acceder al servicio de Internet.

Para comunicarle estos datos de acceso al usuario que los ha solicitado se habilitará un botón de impresión. De este modo se generará un ticket con los datos de acceso, que será entregado al usuario para que pueda disfrutar del servicio.

Si se desea tener algo más de control sobre los usuarios que existen en el sistema, se recomienda como una buena práctica, pedir al usuario que introduzca su correo electrónico personal como nombre de usuario. Lo que también puede ofrecer ventajas para el envío de avisos, publicidad o comunicaciones de la entidad que ofrece el servicio. Este punto se puede aplicar o no dependiendo del tipo de entidad en el cual se haya desarrollado el sistema hotspot.

En otros casos, como puede ser servicios de hostelería y hospedaje, se recomienda como una buena práctica para facilitar el control de acceso u obtener estadísticas, colocar como nombre de usuario el número de habitación donde se aloja el huésped que ha solicitado el acceso al sistema hotspot.

Junto con los datos de usuario y contraseña, también se tiene que introducir el perfil al cual se desea que pertenezca el usuario. Este valor aparecerá en el formulario web como una opción de selección. Dependiendo de cada perfil el cliente podrá usar el sistema durante un tiempo determinado, por defecto aparecen creados los perfiles validos durante ocho horas, un día y tres días.

Este tiempo, durante el cual podrá el usuario acceder al sistema, será también especificado en el ticket que se le entregará con los datos de acceso para que en todo momento tenga disponibles sus datos de acceso y el tiempo para el cual son validos.

4.4.4.2 Visualización de usuarios

Mediante esta funcionalidad de visualización de usuarios, el gestor podrá ver los usuarios que están registrados en el sistema hotspot. Para acceder a dicha información solo tendrá que navegar desde los menús del portal de gestión. Dentro del apartado de usuarios se encuentra la opción de Ver.

Dicha información será presentada en formato tabla, en las columnas se presentará la siguiente información:

- nombre de usuario.
- perfil que tiene asignado.
- tiempo de uso (este tiempo se refiere al tiempo que ha estado usando el servicio, no al tiempo de validez).

En cada fila se presentará la información de un usuario registrado en el sistema hotspot.

Esta información puede ser útil para identificar posibles usuarios que estén registrados en el sistema y que no hayan usado todavía el servicio. También sería de gran ayuda para comunicar a un usuario el tiempo que ha estado usando el servicio.

4.4.4.3 Eliminación de usuarios

Mediante esta funcionalidad de eliminación de usuarios, el gestor podrá eliminar un usuario que este registrado en el sistema hotspot.

Para acceder a dicha información solo tendrá que navegar desde los menús del portal de gestión. Dentro del apartado de usuarios se encuentra la opción de Borrar.

En este caso se mostrará un formulario con la lista de usuarios que están registrados en ese momento en el sistema hotspot, seleccionando un usuario de la lista y pulsando el botón de borrar, se procederá a la eliminación del usuario.

De este modo el usuario ya no podrá utilizar dicho nombre de usuario y contraseña como datos de acceso al servicio y por tanto tendrá que solicitar unos nuevos datos de acceso.

Esta funcionalidad se ha pensado que puede ser útil para eliminar a usuarios que estén haciendo un uso no adecuado o indebido del acceso a internet. También se podría utilizar para eliminar los datos de acceso que hayan sido solicitados en algún momento pero que finalmente no hayan sido usados.

4.4.4.4 Generación de un usuario aleatorio

En el apartado de conceptos fundamentales del hotspot se ha explicado el concepto de ticket, sabiendo que se compone del nombre de usuario, contraseña y tiempo de validez se puede desarrollar esta funcionalidad. La posibilidad que ofrece sería la de generar de manera automática un ticket de acceso al sistema hotspot, simplemente navegando a la opción Aleatorios--uno desde los menús del portal de gestión.

No sería necesario introducir ningún dato por parte del gestor, ya que el nombre de usuario y la contraseña serían generados de manera aleatoria, de modo que será necesario el desarrollo de una función específica para este cometido, siempre teniendo en cuenta las reglas de validez

que se ha especificado en el momento de la creación de usuarios (caracteres alfanuméricos y longitud comprendida entre cuatro y veinte caracteres).

El tiempo de validez del ticket generado vendría determinado por el tiempo que tenga asignado el perfil que está marcado como opción por defecto en el sistema hotspot. Para este caso, el perfil por defecto tendría un tiempo de validez de un día.

Para facilitar al usuario este ticket que se acaba de generar, se habilitará un botón de impresión. De este modo se generará un ticket con los valores, que será entregado al usuario para que pueda disfrutar del servicio.

4.4.4.5 Generación de un número determinado de usuarios aleatorio

Esta funcionalidad sería una extensión de la funcionalidad número cuatro ya que se ofrece la posibilidad de crear un número determinado de tickets para acceso al sistema. Simplemente navegando a la opción Aleatorios--Varios desde los menús del portal de gestión.

En este caso los datos a introducir por parte del gestor del sistema, en el formulario web, serían el número de tickets que desea generar y el perfil al cual quiere asignarlos. De este modo serían generados de manera aleatoria tantos tickets de acceso como se haya especificado. Para la introducción del número de tickets también se tendrá en cuenta que se debe validar que se ha introducido un número y no otro carácter cualquiera. Además de que dicho número deberá ser mayor que cero y no superior a treinta y dos. En este caso se elegido treinta y dos como número máximo para evitar que el tiempo de generación sea excesivo y como medida para evitar tener muchos tickets registrados en el hotspot que todavía estén sin usar.

El tiempo de validez del ticket generado vendría determinado por el tiempo que tenga asignado el perfil que se ha asignado. Para realizar esta selección se ha habilitado en el formulario una lista con los perfiles que hay creados en el hotspot para que el gestor pueda seleccionar el que desea fácilmente.

Estos tickets serán generados teniendo en cuenta los tipos validos para los datos de nombre de usuario y contraseña, es decir caracteres alfanuméricos y longitud comprendida entre cuatro y veinte caracteres.

Una vez generados todos los tickets solicitados se mostrarán en una tabla. Se habilitará un botón de impresión que generará un archivo con todos los tickets. De este modo se podrán imprimir y estarán disponibles para facilitarlos en formato papel a los usuarios que soliciten datos de acceso sin tener que acceder al sistema para generarlos.

4.4.4.6 Creación de perfiles

Tanto en el momento de dar de alta un usuario en el sistema hotspot como en el momento de generar tickets con datos de acceso aleatorios, se ha hablado del perfil asignado.

En este caso la información más importante que se almacena en el perfil es el tiempo de validez, es decir el tiempo durante el cual se puede usar el servicio. Por tanto si se habla de creación de usuarios y que estos tienen un perfil asignado, también se debe ofrecer la posibilidad de crear un perfil especificando el tiempo que se quiere que este en uso.

Para dicho cometido será desarrollada esta funcionalidad. De igual manera que todas las funcionalidades anteriores estará disponible desde los menús de navegación del portal de gestión. Estará disponible en la parte de perfiles dentro de crear.

Se habilitará un formulario web para que el gestor, pueda crear un nuevo perfil. Para ello se le solicitarán los datos de tiempo de validez. Estos datos serán separados en días, horas y minutos, pudiendo especificarse al menos uno de ellos o los tres. Teniendo en cuenta los valores introducidos en estos campos se genera automáticamente un nombre para el perfil.

De modo que si se crea un nuevo perfil con tiempo de validez de 12 horas, este perfil será llamado 12 horas para que sea más fácil su identificación. En el momento de la introducción de los datos estos serán validados de tal manera que cumplan las restricciones de tiempo, por ejemplo que los días estén comprendidos entre 1 y 31, que las horas estén entre 1 y 23 y que los minutos estén comprendidos entre 1 y 59.

Si no se cumplen estos valores se mostraran mensajes de error en los campos donde no se haya cumplido la restricción. Si todo es correcto se crear el perfil con el tiempo de uso que se haya introducido.

4.4.4.7 Consulta de perfiles

Se desarrollará la funcionalidad de visualización de perfiles. Con ella el gestor podrá ver los perfiles que están creados en el sistema hotspot. Para acceder a dicha información solo tendrá que navegar desde los menús del portal de gestión. Dentro del apartado de perfiles se encuentra la opción de Ver.

Dicha información será presentada en formato tabla, en las columnas se presentará la siguiente información:

- nombre del perfil.
- tiempo de validez (en el formato Xdhh:mm:ss, la x corresponde con un número de días y los demás valores se corresponden con formato horario).

En cada fila se presentará la información de un perfil creado en el sistema hotspot. Esta información puede ser útil para comprobar si ya se tiene un perfil creado con un tiempo determinado, en el momento de crear un nuevo perfil se puede ver si ya existe alguno creado con ese tiempo de validez o es posible usar alguno que tenga un tiempo de validez similar.

4.4.4.8 Consulta de conexiones

Repasando el diagrama de casos de uso realizado en la parte de análisis, se encuentra la posibilidad de ver las conexiones que hay actualmente en el hotspot. Es decir los usuarios que están conectados al hotspot y están usando el servicio en ese momento.

Para dicha información sería de utilidad, obviamente el nombre de usuario, pero también la dirección ip con la que está conectado al hotspot. Esta información puede resultar útil a modo de resumen, para ver las conexiones que hay en el hotspot. Esta información se mostrará en una tabla.

También se mostrará la información del tiempo de conexión que lleva consumido el usuario desde su primer acceso y el tiempo restante que le falta para que su ticket deje de ser válido.

4.4.4.9 Eliminación de conexiones

En el punto anterior se ha tratado la visualización de conexiones, pero también puede resultar útil una función para eliminar dichas conexiones.

Se puede eliminar un usuario del hotspot mediante la funcionalidad de eliminación de usuarios, de este modo el usuario ya no podrá volver a usar su usuario y contraseña para poder acceder. Pero también se quiere poder eliminar la conexión de un usuario sin tener que eliminar sus datos de usuario, de manera que sea forzado a validarse de nuevo en el hotspot. Esta funcionalidad puede ser útil para evitar la acumulación y realizar un control de los usuarios que estén utilizando el servicio.

4.4.4.10 Consulta de información del sistema.

En cualquier sistema siempre es recomendable tener una página que muestre algo de información sobre el estado del sistema. Esta funcionalidad viene a cubrir esa necesidad. Desde los diferentes menús de la aplicación, se podrá acceder a la zona de información, ubicada en el apartado de herramientas.

En esta página se mostrará información sobre el sistema donde está funcionando el hotspot, por ejemplo la velocidad del procesador. También se mostrará a modo de resumen el número de usuarios que están registrados en el hotspot, independientemente de si están usando el servicio o no.

También se mostrará a modo de resumen el número de conexiones que hay en ese momento en el hotspot, esto quiere decir el número de usuarios que estén usando el servicio en ese momento.

4.4.4.11 Limitar ancho de banda.

En cualquier sistema que proporciona un acceso a una red de comunicaciones o a Internet es muy importante tener en cuenta el ancho de banda que se proporciona a cada usuario. Es una cuestión de vital importancia ya que puede determinar el número de usuarios a los que es posible ofrecer el servicio y la calidad con la cual se da dicho servicio.

También puede resultar muy útil para limitar las descargas de contenido P2P o descargas masivas así como el envío de correo electrónico spam. Con el establecimiento de unos límites de ancho de banda tanto para la descarga como para la subida de datos se asegura que no haya usos abusivos del sistema hotspot.

Esta funcionalidad viene a cubrir dicha necesidad. En los menús del portal de gestión aparecerá en el apartado de herramientas, llamándose limites. Mediante un formulario web el gestor podrá fijar unos límites de ancho de banda para todos los usuarios del hotspot de tal manera que los límites introducidos serán las velocidades máximas que podrá obtener el usuario en su conexión de bajada y subida de datos.

Como la intención es que el gestor no tenga que estar familiarizado con configuraciones o terminología de redes de comunicaciones, se han establecido una serie de niveles para asignar a los límites de ancho de banda. De tal manera que estos límites equivalgan a una velocidad que no tiene porque ser conocida por el gestor.

También se ofrece la posibilidad de borrar los límites que se hayan establecido anteriormente o de fijar que no haya límites en el ancho de banda.

Los niveles que se han fijado y las velocidades a las cuales equivalen se pueden ver en la siguiente tabla. Estos valores se han pensado también para el servicio que se quiere ofrecer así por ejemplo los niveles lentos podrían equivaler a un uso de aplicaciones de mensajería que no consumen mucho ancho de banda. El nivel normal se podría equiparar a un uso de navegación web y correo electrónico. Por último el nivel rápido se podría equiparar a un uso de visionado de videos en web que requiere mayor ancho de banda.

Nivel de descarga	Velocidad	Nivel de subida	Velocidad
Lento	128 Kbps	**Lento**	64 Kbps
Normal	512 Kbps	**Normal**	256 Kbps
Rápida	1024 Kbps	**Rápida**	512 Kbps

Tabla 4 – Límites de ancho de banda

4.4.4.12 Añadir página para visitar sin haber accedido al hotspot.

Como se ha explicado en el funcionamiento del hotspot, el sistema no deja acceder a ninguna página web de Internet a menos que el usuario realice primero el acceso al sistema en el portal cautivo. De este modo al intentar visitar cualquier página se redirige a dicho portal para que el usuario introduzca sus datos de acceso.

Este comportamiento puede ser modificado añadiendo las páginas, que se desean que puedan ser visitadas sin haber accedido al sistema hotspot, en el llamado walled garden. Se puede definir este walled garden como una lista de páginas blancas que se pueden visitar sin autorización.

Por ejemplo puede ser que una institución, como el caso de una universidad, quiera que su página web pueda ser visitada sin tener que acceder al sistema hotspot, por tanto es necesario añadir una funcionalidad que permita introducir estas páginas en la lista de acceso sin autorización.

Para ello se desarrollará esta funcionalidad accesible desde todos los menús del portal de gestión. En un formulario web se pedirá que se introduzca la web a la que se desea dar acceso., estos datos serán validados de modo que se correspondan con una dirección web o url válida y si lo es será añadida a la lista de páginas blancas.

4.4.4.13 Interfaz del portal de gestión

Para el desarrollo de una aplicación web, como es en este caso el portal para la gestión del hotspot, es conveniente definir una plantilla o maqueta que seguirán las paginas que se vayan desarrollando. En este caso se puede dividir el portal en dos tipos de páginas:

- página de acceso al portal con menús para acceder a cada función. Sería la página principal del portal y seguiría el siguiente esquema:

Figura 13 – Apariencia del menú principal del portal de gestión.

- página de función. Con menú de navegación en la parte superior para navegar de una función a otra, desarrollo de la función en la parte central y acceso al menú principal en la parte inferior. Seguiría el siguiente esquema.

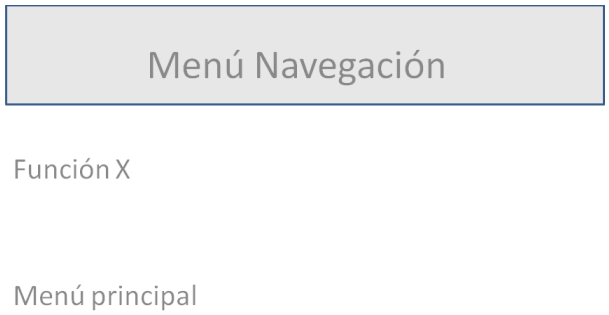

Figura 14 – Apariencia de páginas de función del portal de gestión

Una vez que se tiene definido el diseño para el portal de gestión y están definidas sus funcionalidades, así como la apariencia que van a tener las páginas web que componen dicho portal, se pasa a definir las tecnologías con las que se llevara a cabo el desarrollo.

En primer lugar, al tratarse de una aplicación web es imprescindible usar el lenguaje HTML para su implementación. Para hacer más fácil el desarrollo y obtener páginas web adaptadas a las nuevas tecnologías, se ha decidido usar un framework para el desarrollo del código HTML de las páginas.

Un framework es un marco de trabajo que contiene soluciones a problemas que ya han sido planteados y resueltos. En este caso, un framework para páginas web contiene especificaciones para el desarrollo de los menús de navegación, para las rejillas que sirven de base a la maquetación de la página web, así como funciones para cambiar la apariencia de la pagina en funciona del dispositivo en el cual es visualizada.

Este último concepto ha venido a llamarse diseño web responsive o adaptativo que consiste en una técnica de diseño web que busca la correcta visualización de una misma página en distintos dispositivos. Desde ordenadores de escritorio a tablet y móviles. Se trata de redimensionar y colocar los elementos de la web de forma que se adapten al ancho de cada dispositivo permitiendo una correcta visualización y una mejor experiencia de usuario.

Para el desarrollo del portal de gestión se ha valorado la utilización de diferentes framework para finalmente decidir que se utilizará el framework conocido como Bootstrap. Este framework contiene un conjunto de herramientas de software libre para diseño de sitios y aplicaciones web. Contiene plantillas de diseño con tipografía, formularios, botones, cuadros, menús de navegación y otros elementos de diseño basado en HTML y CSS, así como, extensiones de JavaScript opcionales adicionales.

Este framework fue creado por dos desarrolladores en Twitter como herramienta de patrón de diseño en el desarrollo de aplicaciones dentro de la compañía. Actualmente se ha convertido en uno de los marcos de diseño de páginas web más populares del mundo, usado incluso en la NASA para el desarrollo de sus aplicaciones.

Ya que se trata de un framework muy popular, son muchas las páginas web desarrolladas con él, y que ya había realizado su manejo en el desarrollo de otras aplicaciones por lo que sea ha decidido usar este framework en lugar de otros.

Con las clases y funciones ya desarrolladas en este framework se llevará a cabo el desarrollo de todos los elementos de las páginas web del portal de gestión:

- Maquetación de la página.
- Menú de navegación.
- Menú principal.
- Formularios.
- Botones.

4.4.4.14 Comunicación del portal de gestión con el hotspot.

Para el desarrollo de este entorno web para la gestión del hotspot y poder realizar todas las funciones que son necesarias, el portal de gestión debe poder comunicarse con el hotspot. De tal manera que pueda acceder a su configuración para realizar lecturas y escrituras y así crear nuevos usuarios o consultar lo que están creados.

Esta comunicación será iniciada por el portal de gestión, estableciendo en primer lugar la comunicación, después dependiendo de la función que le haya solicitado hacer el gestor, hará una lectura o escritura de la configuración. Para terminar deberá cerrar la comunicación.

Estas comunicaciones con el hotspot se van a desarrollar en lenguaje PHP, se trata de un lenguaje de programación diseñado para el desarrollo web de contenido dinámico. Es un lenguaje de código abierto muy popular, adecuado para desarrollo web y que puede ser incrustado en HTML.

Se llama páginas dinámicas a aquellas cuyo contenido no es siempre el mismo, por ejemplo en este caso una consulta de usuarios conectados no siempre generara la misma salida. El proceso sería el siguiente, mediante un navegador web, cliente, se envían los datos de la solicitud al servidor que los procesa, reúne la información necesaria realizando una comunicación con el hotspot (por eso se denomina como proceso dinámico) y el servidor devolverá una página HTML con la información solicitada.

Para realizar dichas comunicaciones con el hotspot se dispone de una API (biblioteca con funciones y procedimientos) para ser usada con el lenguaje de programación PHP. De tal manera que realizando la conexión con el hotspot permite consultar y modificar los valores de configuración y poder así presentarlos y manejarlos desde el entorno web.

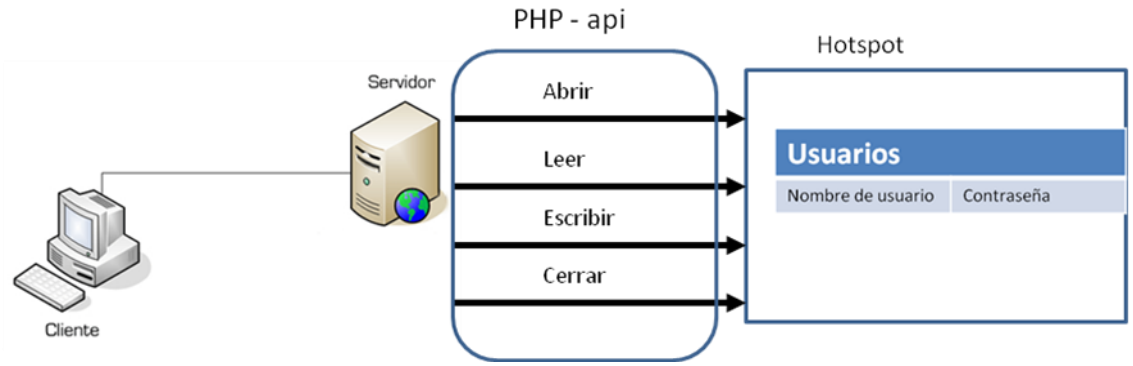

Figura 15 – Comunicación del portal de gestión con el hotspot

Como se ve en el esquema superior, las principales funciones de esta api son cuatro, las cuales van a permitir manejar la configuración del hotspot y poder realizar las funciones de gestión y administración desde el portal de gestión:

- Abrir: esta función permite iniciar una conexión con el hotspot. Para ello se tendrán que facilitar los datos de comunicación, ip del hotspot, puerto en el que se realizará la comunicación así como los datos de identificación.
- Leer: esta función realiza una lectura de datos del hotspot y guardar el resultado en una variable.
- Escribir: esta función escribe el valor de una variable en un parámetro de configuración del hotspot.
- Cerrar: esta función cierra la comunicación con el hotspot.

Para poder utilizar esta api, se tendrá que configurar en el hotspot el puerto de escucha que se quiere utilizar, así como los datos de identificación de tal manera que se puedan abrir conexiones desde el portal de gestión.

De este modo la comunicación entre el portal de gestión y el hotspot se hace de manera transparente para el gestor. Con esto se consigue que no sea necesario para el gestor tener unos conocimientos en redes de comunicaciones ni que tenga que conocer ni manejar parámetros de configuración del hotspot. Simplemente se le ofrece de manera simple e intuitiva las funciones que necesitara realizar para administrar y gestionar el sistema.

4.4.5 Diseño del portal de registro

Con esta funcionalidad se pretende que los usuarios del hotspot puedan realizar el registro por ellos mismos de tal manera que no tengan que solicitarlo al gestor.

En este caso por registro se entiende la creación de unos datos de acceso formados por usuario y contraseña para poder acceder al hotspot y empezar la navegación por Internet.

Este portal de registro tiene que estar accesible para los usuarios en el momento de mostrarles el portal cautivo por primera vez, de tal manera que se incluirá un enlace a dicho portal en la página principal del portal cautivo. La misma en la cual el usuario deberá introducir los datos de acceso al hotspot si ya los posee.

Con este enlace se asegura que si un usuario no está registrado en el hotspot y no dispone de datos de acceso, no tenga que pedírselos al gestor, si no que pueda obtenerlos de manera automática.

Este portal de registro estará compuesto por un formulario donde se le pedirá al usuario que introduzca los datos que desea que se generen como nombre de usuario y contraseña. Siempre teniendo en cuenta los tipos validos para ambos campos.

Una vez introducidos y validados esos datos se realizará la comunicación con el hotspot para crearlos en las tablas correspondientes, en este caso se generará una nueva entrada en la lista de usuarios.

Esta comunicación con el hotspot se realizará de igual manera que las comunicaciones que realiza el portal de gestión, es decir se hará en código PHP utilizando las funciones que ofrece la API.

Para evitar proporcionar al usuario del hotspot más información de la que necesita, no se le pedirá que introduzca nada relacionado con el tiempo que vaya a usar el servicio. Para ello se le asignará el perfil marcado como por defecto en el hotspot, de manera que tendrá acceso al hotspot durante el tiempo de uso especificado en dicho perfil.

Si la creación de los datos de acceso es correcta se le mostrarán al usuario los datos que se han introducido y que se han creado como nombre de usuario y contraseña y se le proporcionará la opción de acceder directamente al hotspot sin tener que volver a mostrar el portal cautivo, e introducir de nuevo los datos creados.

Con esto se consigue que el usuario no tenga que memorizar los datos para introducirlos de nuevo en la página de acceso del portal cautivo. Se realiza de forma transparente para el usuario, el acceso al sistema hotspot.

En el momento que el usuario pulsa el botón de acceso se realiza una redirección, del portal de registro pasando los datos de acceso al portal cautivo, que será el encargado de procesarlos. El portal cautivo realizará la comunicación con el hotspot para comprobar que esos datos de acceso están almacenados en sus tablas y si son correctos le permitirá el acceso al usuario.

Una vez que el usuario ha usado el portal de registro para obtener los datos de acceso al sistema, no debe poder acceder al portal de registro de nuevo. Con esto se evita que un usuario pueda crear varios datos de acceso, simplemente se le permite crear uno para que use el hotspot. Para evitar dicho acceso, se configurarán las reglas de cortafuegos necesarias para impedir el acceso al portal de registro una vez que el usuario haya accedido al hotspot.

Para que esta funcionalidad del portal de registro quede lo más clara posible y facilitar su desarrollo e implementación, se ha realizado el siguiente diagrama de secuencia, teniendo en cuanta los agentes que intervienen y las funciones que realizan:

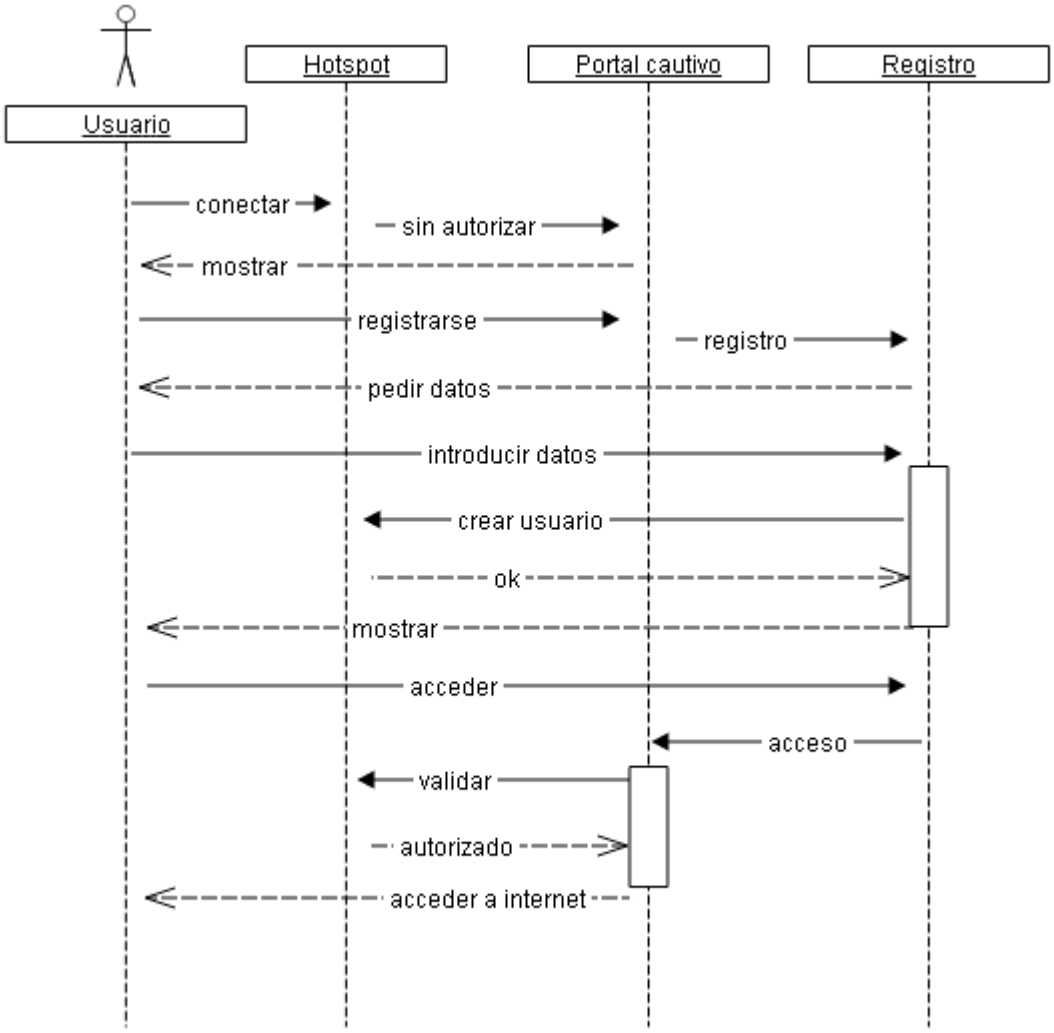

Figura 16 – Diagrama de secuencia del portal de registro

De igual modo que para el portal de gestión, esta página debe ser visionada correctamente en todo tipo de dispositivos, por lo que su desarrollo se realizará con el framework Twitter Bootstrap.

4.5 Recursos externos

En este punto, se van a especificar los recursos externos que serán necesarios para el desarrollo y la implementación del proyecto. Dichos recursos ya se han ido citando en muchos de los apartados tratados anteriormente, pero se considera que es necesario realizar un resumen de los mismos para tener claras las necesidades.

Por recursos externos se entiende tanto los lenguajes de programación con los que se desarrollará el proyecto como las plataformas donde se implementará. Para que quede lo más claro posible se va a realizar una separación de los elementos del sistema por las plataformas donde están alojados y se citará para cada punto, que sistema operativo tiene la plataforma y con qué lenguaje de programación se realizará el desarrollo que se aloja.

4.5.1 Routerboard

En el dispositivo Routerboard se realizará la implementación del router, del hotspot y el desarrollo del portal cautivo. Esta plataforma es un producto de la empresa Mikrotik, son dispositivos hardware que disponen del sistema operativo RouterOS basado en GNU/Linux y que va a permitir realizar la implementación de los elementos que se han citado.

Mediante las capacidades del sistema operativo RouterOS se va a poder realizar funciones de redes de comunicaciones, como enrutamiento, bloqueo de tráfico, asignación de ip, servidor de DNS y por supuesto todo lo necesario para implementar el hotspot.

También este dispositivo dispone de una interfaz inalámbrica que servirá para emitir la red a la cual se conectarán los clientes del hotspot. Es un dispositivo muy completo que asume las funcionalidades de varios dispositivos en uno.

También dispone de un directorio FTP donde se puede alojar el portal cautivo. El desarrollo el portal cautivo será realizado mediante lenguaje de programación HTML, ya que se trata de una página web, se usará CSS para mejorar su apariencia y también será utilizado el lenguaje de programación Javascript para el desarrollo del método de validación de los usuarios.

4.5.2 Servidor HTTP

En el servidor HTTP estará alojado tanto el portal de gestión como el portal de registro. Este servidor HTTP tendrá que atender las peticiones del gestor o del usuario, procesarlas y además ofrecer una respuesta. Existen múltiples servidores web en el mercado entre los cuales existen algunos que son ampliamente utilizados y que además son de código abierto. Teniendo en cuenta estas características se ha optado por Apache HTTP Server que es un servidor HTTP ampliamente conocido por su temprana aparición en 1995. Este servidor, es utilizado en el 54,2% de los sitios web del mundo.

La peculiaridad de este servidor HTTP es que se ha pensado para su instalación en un ordenador de placa reducida llamado Raspberry Pi. Este dispositivo dispone del sistema operativo Raspbian basado en GNU/Linux, por lo que la instalación y configuración de Apache

se realizaría de igual manera que en cualquier otro ordenador con un sistema operativo GNU/Linux.

Como se ha comentado en la parte de diseño de cada elemento, tanto para el portal de gestión como para el portal de registro se utilizará el código HTML para la presentación de la web. Se usará hojas de estilo de CSS para su apariencia y se utilizará el lenguaje PHP para las comunicaciones con el hotspot y obtener así los datos dinámicos.

Se utilizará el marco de trabajo o framework de Twitter Bootstrap para el desarrollo del código HTML y las hojas de estilo que proporciona este marco de trabajo para la apariencia de la web. Haciendo así más sencillo la generación de los elemento de la web, tanto formularios como menús y botones.

También cabe citar que se utilizará el lenguaje PHP para las comunicaciones con el hotspot, usando la api llamada RouterOS PHP API class v1.4 desarrollada por Denis Basta y que esta accesible en la web.

Para realizar las impresiones de datos desde el portal de gestión también se usará una api para generar un fichero de extensión PDF. En este caso la api se llama FPDF, la versión utilizada será la 1.7 y ha sido desarrollada por Olivier Plathey. Ofrece las funcionalidades de crear ficheros PDF mediante código PHP.

Se ha tenido en cuenta que se debe realizar una validación de los campos introducidos en los diferentes formularios web del portal de gestión y del portal de registro, por lo que se realizará comprobaciones con el lenguaje de programación Javascript para validar los tipos de datos introducidos y si se detectan errores comunicárselos al usuario.

5. PRUEBAS Y VALIDACIÓN

En cualquier proyecto de desarrollo de software es importante que el resultado final sea adecuado a los requisitos que se han especificado para ello se realizarán una serie de pruebas para comprobar el correcto funcionamiento de todos los componentes.

En este apartado se establecen una serie de pruebas que se realizaran sobre el desarrollo obtenido. En primer lugar pruebas enfocadas al funcionamiento y proceso de ejecución de las diferentes funciones que componen el sistema y en segundo lugar, una serie de pruebas realizadas contra el sistema completo, es decir poniendo en funcionamiento muchos de los procesos que lo componen, de modo que se compruebe si tanto el usuario final del hotspot como el gestor son capaces de manejar el sistema.

5.1 Pruebas realizadas del router

Una vez se ha completado la implementación de las configuraciones necesarias para el funcionamiento del router, se ha comprobado que el funcionamiento es correcto. Se ha comprobado que el router disponía de dirección ip para ser alcanzando por los dispositivos conectados a él. Se ha conectado a las diferentes interfaces Ethernet del dispositivo y se ha comprobado que asignaba direcciones ip de la red privada que se había configurado. También se ha comprobado que el dispositivo era alcanzable desde esa red mediante el comando ping. La comprobación de la salida a internet se ha realizado mediante el comando ping, en este caso se ha efectuado a la dirección ip de una de los servidores DNS de Google (dirección ip 8.8.8.8) para comprobar si había conexión con el exterior. Se puede comprobar el funcionamiento en dicha captura.

```
[admin@MikroTik] > ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56  56 10ms
    1 8.8.8.8                                    56  56 16ms
    2 8.8.8.8                                    56  56 12ms
    3 8.8.8.8                                    56  56 11ms
    4 8.8.8.8                                    56  56 11ms
    sent=5 received=5 packet-loss=0% min-rtt=10ms avg-rtt=12ms max-rtt=16ms
```

Figura 17 – comando ping a servidor DNS de Google.

Una vez que se tiene acceso a internet, se ha comprobado que el dispositivo dispone de una fecha y hora correctas y que es capaz de resolver peticiones de DNS, para lo cual realizará una consulta externa a servidores DNS, si no dispone de dicha información en su caché de DNS.

```
[admin@MikroTik] > ping www.google.es
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 216.58.210.131                             56  55 11ms
    1 216.58.210.131                             56  55 12ms
    2 216.58.210.131                             56  55 10ms
    3 216.58.210.131                             56  55 12ms
    4 216.58.210.131                             56  55 9ms
    sent=5 received=5 packet-loss=0% min-rtt=9ms avg-rtt=10ms max-rtt=12ms
```

Figura 18 – resolución del nombre de DNS www.google.es

Con un ordenador conectado al router, se ha comprobado que dicho PC es capaz de tener acceso a internet, tanto en navegación web como realizando otras peticiones. Por tanto la configuración del router se da validada y comprobada.

5.2 Pruebas realizadas del hotspot

Terminada la implementación del hotspot, se pasa a comprobar su funcionamiento, en este caso como se ha asignado una interfaz inalámbrica en la que funcionará, se tiene que comprobar si los dispositivos inalámbricos son capaces de conectar a dicha red.

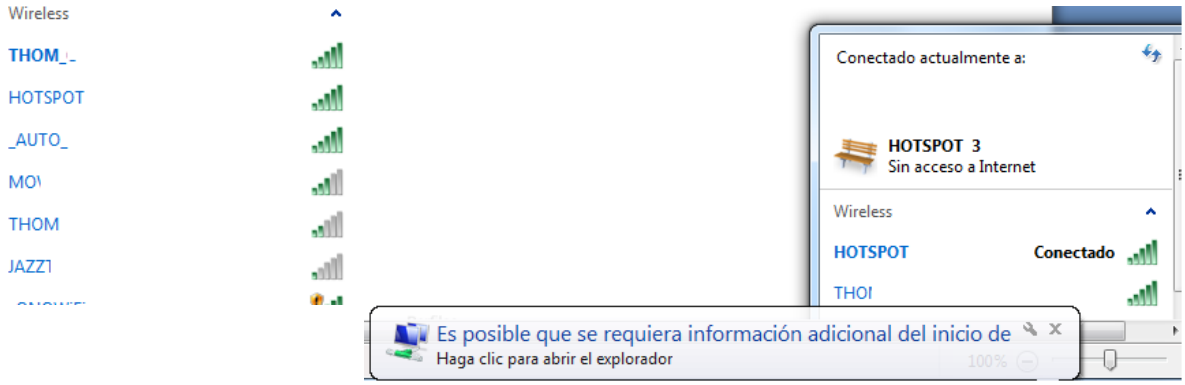

Figura 19 – Captura de funcionamiento del hotspot

Como se puede ver en las capturas, los dispositivos inalámbricos son capaces de conectar a la red y muchos de ellos detectarán que para usar la conexión a internet hay que introducir información para el inicio de sesión. Por tanto se comprueba que el funcionamiento del hotspot es correcto. Con esta prueba se valida el requisito no funcional RNF02 y como se aprecia en la captura es necesario introducir información para iniciar sesión con lo cual se valida también el requisito funcional RF02.

Las demás implementaciones de configuración del hotspot, como puede ser la redirección al portal cautivo o el método de validación del los usuarios, se van a realizar en las pruebas del portal cautivo ya que implicas parte de desarrollo de ambos elementos del sistema.

5.3 Pruebas realizadas del portal cautivo

En primer lugar antes de comprobar que el portal cautivo aparece una vez que los usuarios se conectan al hotspot, se valida su apariencia en varios dispositivos. Se valida el requisito no funcional RNF01.

Figura 20 – Visualización en dispositivo móvil del portal cautivo.

Después se repite la prueba anterior realizada en el caso del hotspot pero en este caso se pulsará para abrir el navegador y comprobar si aparece el portal cautivo. Se valida de nuevo el requisito funciona RF02.

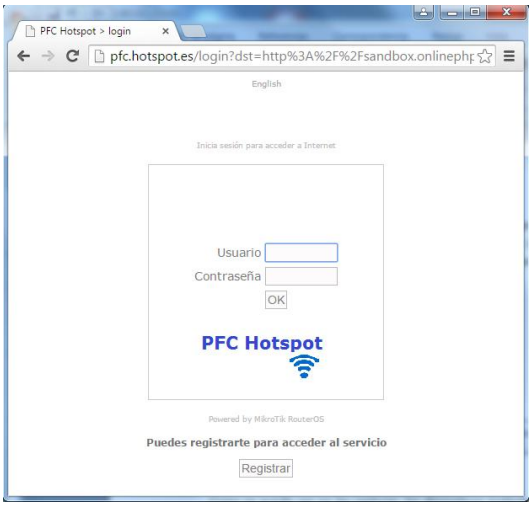

Figura 21 – Captura de funcionamiento del portal cautivo

Con este paso se comprueba que el portal cautivo está funcionando y que el hotspot redirige a él al detectar cualquier tráfico de usuarios que no están autenticados.

Como se dispone de un usuario de pruebas, se va a proceder a realizar la autenticación en el hotspot, también se comprobará la introducción de un dato erróneo para ver el control de errores. En la captura se aprecia el aviso que se muestra al introducir un date erróneo. Se valida en este caso el requisito funciona RF11.

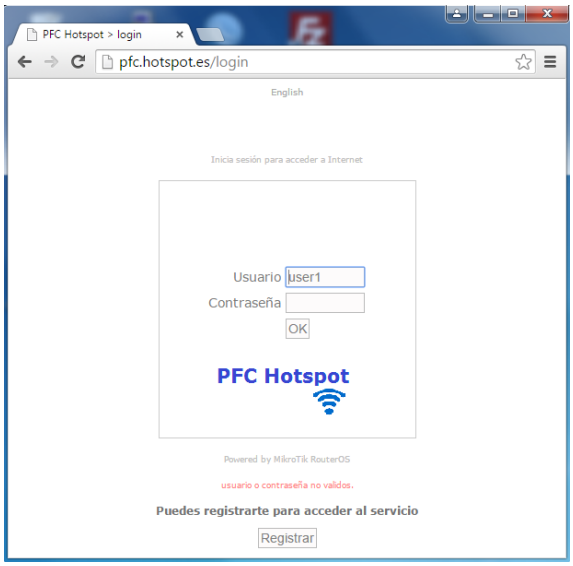

Figura 22 – Captura de error en la introducción de datos

Si el acceso se produce de manera correcta se muestra la página de éxito para segundos después redirigir a la página origen que el usuario ha solicitado. La página que el usuario quería visitar antes de ser interceptada la comunicación con el portal cautivo. Se validan de este modo los requisitos funcionales RF01 y RF03.

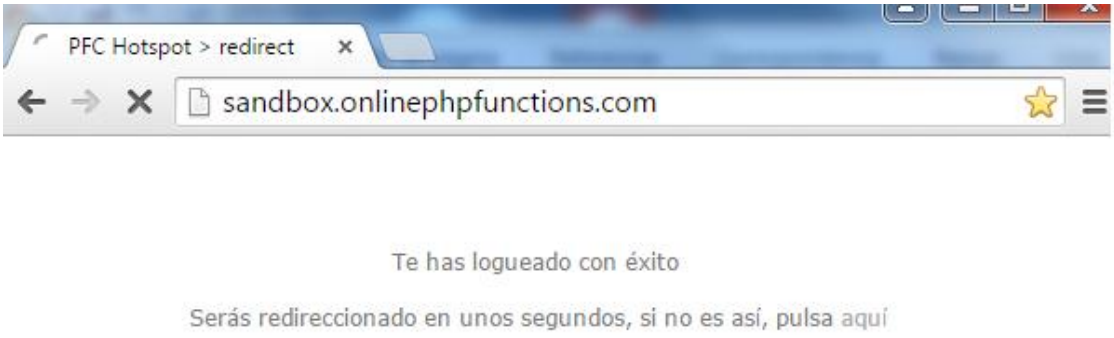

Figura 23 – Captura de acceso con éxito

5.4 Pruebas realizadas del portal de gestión

Para empezar las pruebas con el portal de gestión se debe comprobar si la apariencia de dicho portal está adaptada a cualquier tipo de dispositivo ya sea un ordenador, una tablet o un dispositivo móvil. Para lo cual se debe acceder al portal de gestión desde cada uno de los diferentes dispositivos, en las siguientes capturas se ven cada una de las diferentes versiones. Se validan así los requisitos no funcionales RNF01, RNF02, RNF03 y el requisito funciona RF12.

Figura 24 – Visualización del portal de gestión en ordenador

Figura 25 – Visualización del portal de gestión en tablet

Figura 26 – Visualización del portal de gestión en dispositivo móvil

Se valida con esta primer primera prueba que el portal de gestión se visualiza correctamente en todo tipo de dispositivos.

Se ha comprobado desde la interfaz de usuario que todos los enlaces del portal de gestión dirigen a páginas que existen, es decir que no hay ningún enlace roto. También se comprueba que desde todas las páginas se puede volver al menú principal.

Figura 27 – Navegabilidad hacia el menú principal

Se pasa a comprobar el funcionamiento de las funciones de consulta, en este caso de la información del sistema, de los usuarios creados y conectados y de los perfiles creados. Con estas cuatro capturas se puede ver que el portal de gestión se comunica correctamente con el hotspot obteniendo información de él y mostrándola correctamente en el interfaz web. Se validan los requisitos funcionales RF22, RF15, RF20 y RF19.

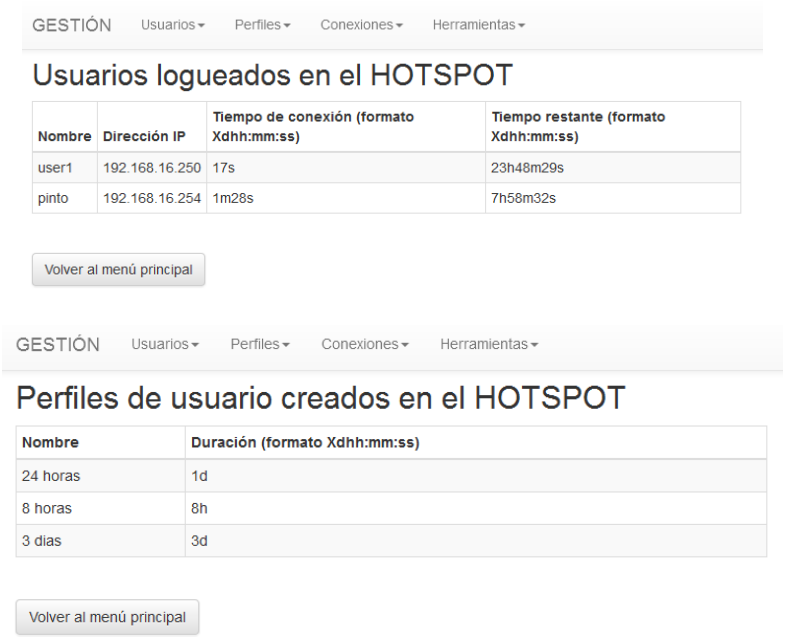

Figura 28 – Capturas de funciones de consulta

La siguiente prueba consiste en utilizar una de las funciones de creación, en este caso se va a crear un nuevo usuario para poder usar el hotspot. Una vez que el usuario este creado como se dispone de una función de consulta se puede comprobar si el proceso ha funcionado correctamente. En este caso el usuario creado se llamará pruebas. Se valida el requisito funcional RF13.

Figura 29 – Captura de creación de usuario

Como se puede comprobar el usuario se ha creado correctamente y aparece la opción de imprimir tal y como se había solicitado en uno de los requisitos. Si se usa el botón se abre un fichero PDF para poder imprimir los datos de acceso. Se valida el requisito funcional RF26.

Figura 30 – Captura de impresión

Para comprobar que el usuario se ha creado correctamente se puede ver si aparece en la lista de usuarios creados. En la captura siguiente se ve como el usuario aparece en la última posición de la lista ya que ha sido el último usuario creado.

Figura 31 – Captura de usuarios registrados

Con estas pruebas se ve que la función de creación de usuarios cumple con los requisitos solicitados, la comunicación entre el portal de gestión y el hotspot en el momento de realizar escrituras sobre parámetros de configuración funciona del modo correcto. Se validan con esta prueba los requisitos no funcionales RNF05 y RNF06.

Estas pruebas han sido repetidas para la creación de perfiles de usuario. Se ha comprobado que introduciendo el tiempo que se desea asignar al perfil, se genera un nombre adecuado a dicho tiempo. Se valida el requisito funcional RF18.

Figura 32 – Captura de creación de perfil

De igual modo se puede comprobar que el perfil ha sido creado correctamente y que aparece tanto en la lista de perfiles creados como en la opción de perfil asignado al crear un usuario.

Figura 33 – Captura de perfiles creados

Para las dos funciones que cambian parámetros de configuración del hotspot se ha comprobado que realizan lo esperado. Para ver si el valor que se quiere modificar cambia en el hotspot se accederá a su configuración y se comprueba el éxito de la función.

En primer lugar para el establecimiento de los límites de ancho de banda. Se validan los requisitos funcionales RF23, RF24 y RF07.

Figura 34 – Captura de límites de ancho de banda

Y en segundo lugar para añadir una página web para ser visitada sin autorización en el hotspot.

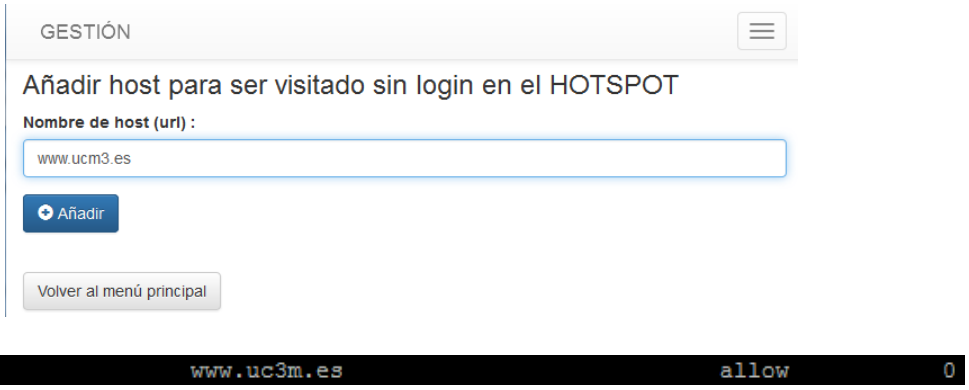

Figura 35 – Captura de página permitida

También se comprueba que estas funciones realizan los requisitos solicitados. Validando los requisitos funcionales RF25 y RF29.

La siguiente prueba se realiza con la generación de usuarios aleatorios. Introduciendo el número de usuarios que se quieren generar y el perfil asignado, estos se generan correctamente.

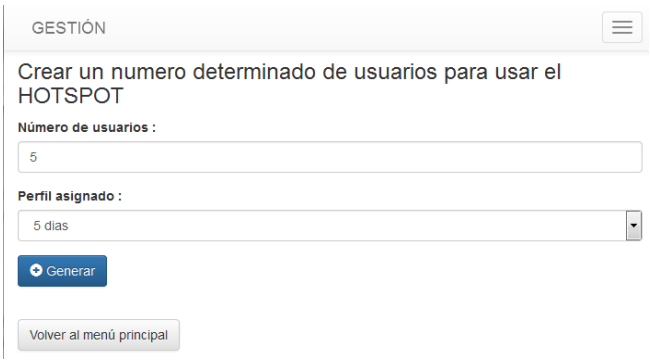

Figura 36 – Captura de generación de usuarios aleatorios

Figura 37 – Captura de usuarios aleatorios generados

Con estas capturas también se comprueba que la función generada para crear nombre de usuario y contraseña aleatorios funciona correctamente. Se validan los requisitos funcionales RF16 y RF17.

Con uno de los usuarios que se han creado aleatoriamente, en este caso el último, se va a comprobar el funcionamiento de la función de borrado. Se selecciona el usuario que se quiere borrar de una lista.

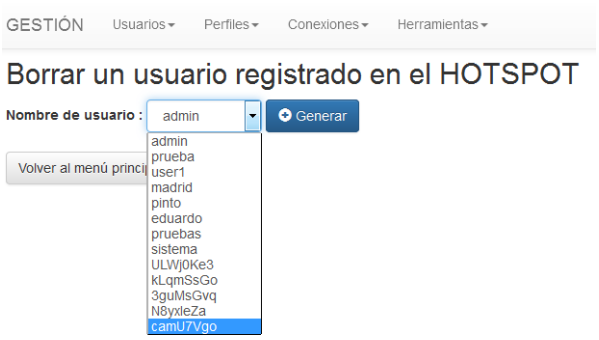

Figura 38 – Captura de eliminación de usuario

Si se realiza posteriormente una consulta de usuarios, se comprueba que el usuario ha sido borrado.

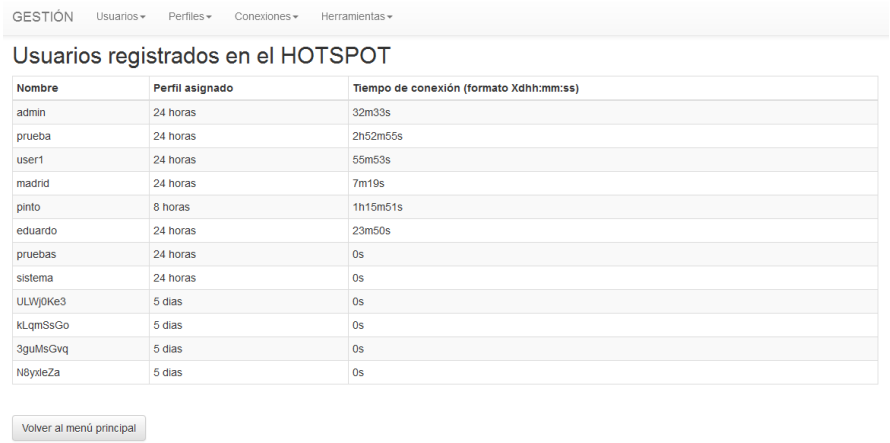

Figura 39 – Captura de usuarios registrados tras eliminar

Los pasos anteriores han sido repetidos con la función que se encarga de eliminar a los usuarios conectados al hotspot, también se comprueba y valida su resultado, no se ha considerado incluir capturas ya que son similares a las expuestas en el caso anterior. Con estas pruebas se validan los requisitos funcionales RF14 y RF21, además de validar de nuevo los no funcionales RNF05 y RNF06

Por último queda comprobar que los datos son validados de acuerdo a sus tipos. Se adjunta diferentes campos donde se comprueba la correcta implementación de esta validación. Por lo que el requisito funcional RF11 queda comprobado.

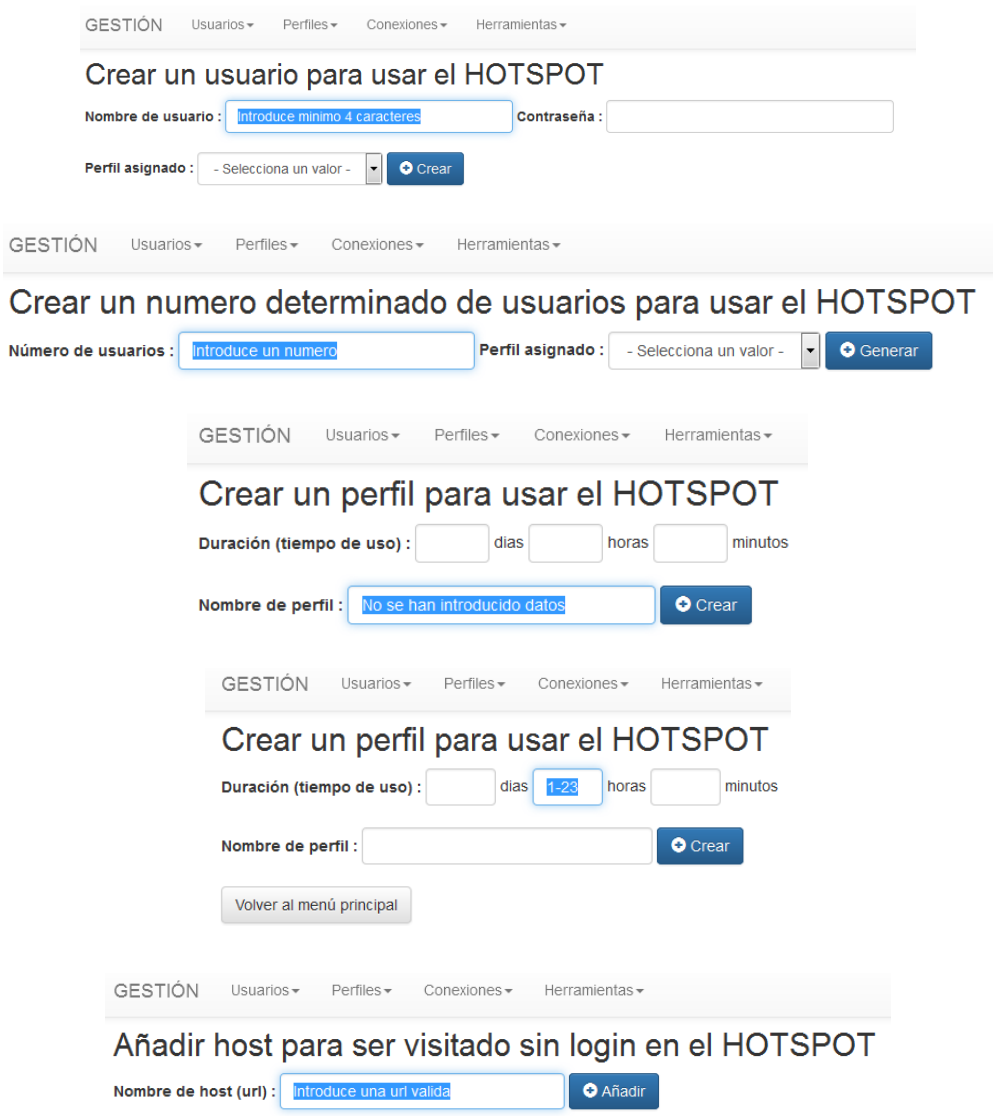

Figura 40 – Validación de tipo de datos

5.5 Pruebas realizadas del portal de registro

Para el portal de registro se comprueba en primer lugar su correcta visualización en todo tipo de dispositivos. Se adjunta la captura de pantalla desde un dispositivo móvil. Se validan de nuevo los requisitos no funcionales RNF01 y RNF02, además de los requisitos funcionales RF27 y RF28.

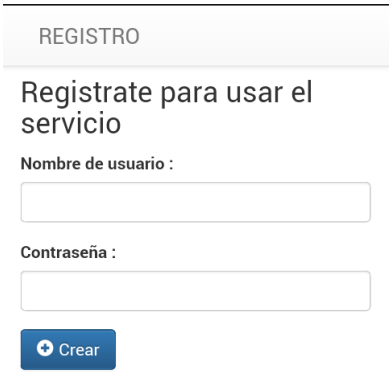

Figura 41 – Visualización del portal de registro en dispositivo móvil

Se comprueba que introduciendo unos datos el usuario es creado de forma correcta.

Figura 42 – Captura de funcionamiento del portal de registro

Si en ese momento el usuario pulsa el botón acceder, se devolverá la comunicación al portal cautivo para realizar la validación del usuario que se acaba de crear.

5.6 Pruebas realizadas del sistema completo

En este punto que se ha comprobado el funcionamiento de los elementos del sistema por separado, se va a proceder a realizar una prueba del sistema completo. Aunque en alguno de los puntos anteriores ya se ha comprobado el correcto funcionamiento de varios elementos del sistema interactuando entre sí ya que están relacionados o realizan comunicaciones entre ellos. Se validan los requisitos RF01, RF02, RF03, RF11, RF27, RF28, RNF01, RNF02, RNF03 y RNF06.

Se va a probar el proceso de acceder a internet desde un teléfono móvil. En primer lugar se conecta al hotspot, se le solicitan los datos en el portal cautivo pero como no se dispone de ellos, se realiza el registro en el portal de registro, una vez obtenidos se puede acceder a internet. Este proceso se ve en las siguientes capturas:

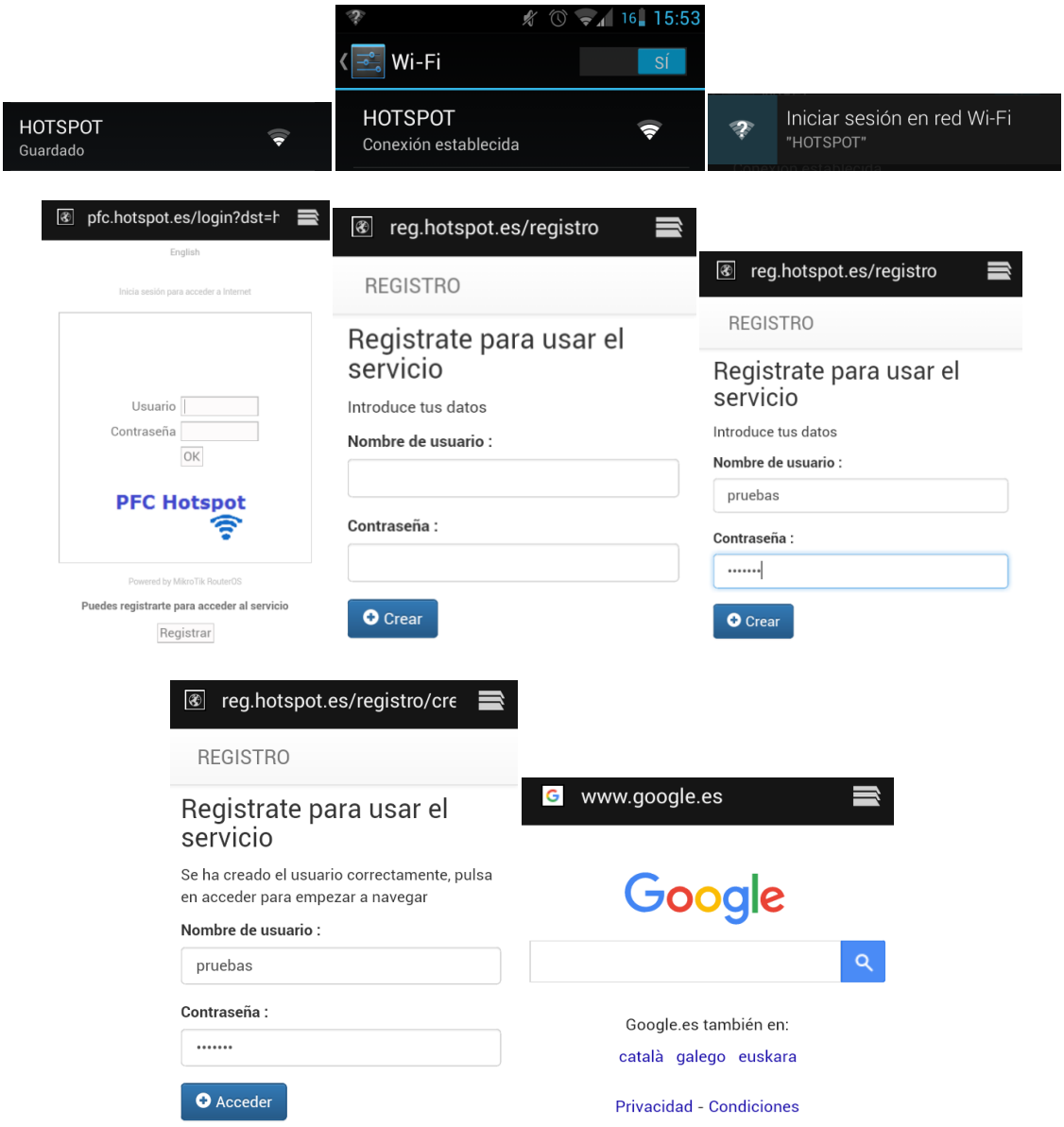

Figura 43 – Captura de pasos para registro y posterior acceso

Para comprobar el correcto funcionamiento del portal de gestión, se puede comprobar que el usuario que acabe de realizar el registro por medio del portal de registro, aparece como usuario registrado y como está conectado en el hotspot también aparece como usuario conectado.

Figura 44 – Captura de comprobación de funcionamiento del sistema

Se puede utilizar la función de borrado de usuarios conectados para validar el funcionamiento del portal de gestión. Con este paso en el momento que el usuario intente acceder de nuevo a internet se le mostrará el portal cautivo. Se validan los requisitos RF14 y RF09.

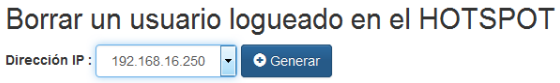

Figura 45 – Captura de eliminación de usuario que ha realizado el registro

Se va comprobar si el sistema limita correctamente el tiempo de uso que tiene asignado el usuario para disfrutar del acceso a internet. Se crea un usuario con tiempo de uso de 4 minutos y se comprueba que pasado ese tiempo el usuario ya no aparece como conectado en el sistema. Se valida con éxito el requisito funcional RF04.

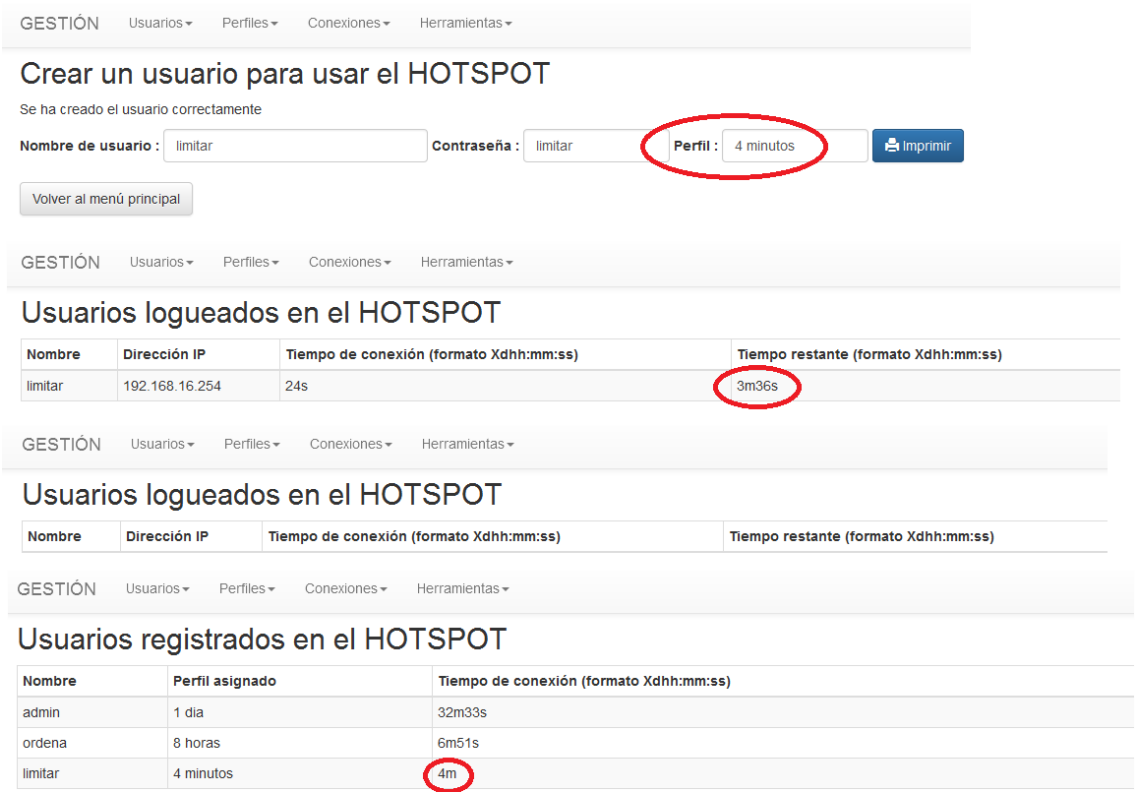

Figura 46 – Captura de usuario limitado por tiempo.

Se valida también el filtro por contenidos, intentado acceder a la página divxtotal.com, podemos ver en la captura que aparece bloqueada. Se valida el requisito funcional RF05.

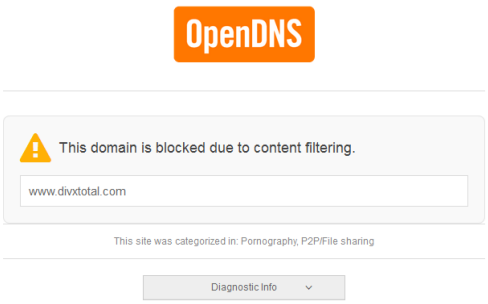

Figura 47 – Página bloqueada. [dns]

Se comprueba de igual modo la limitación de ancho de banda para el tráfico con los límites configurados anteriormente, validándose el requisito funcional RF07.

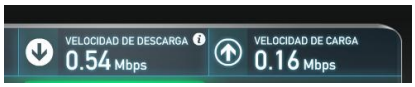

Figura 48 – Límite de ancho de banda. [spe]

Se pasa a comprobar los filtrados de tráfico, en primer lugar el filtrado de tráfico P2P, por ejemplo se ve en la captura como estando conectado a la red del hotspot no se permite la descarga por torrent. Se valida el requisito funciona RF06.

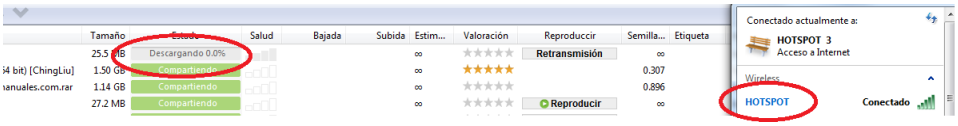

Figura 49 – Bloqueo de tráfico P2P.

Como últimas pruebas se ve que no se puede acceder al portal de gestión ni al portal de registro una vez se ha accedido al servicio de Internet. Validándose los requisitos funcionales RF08 Y RF10.

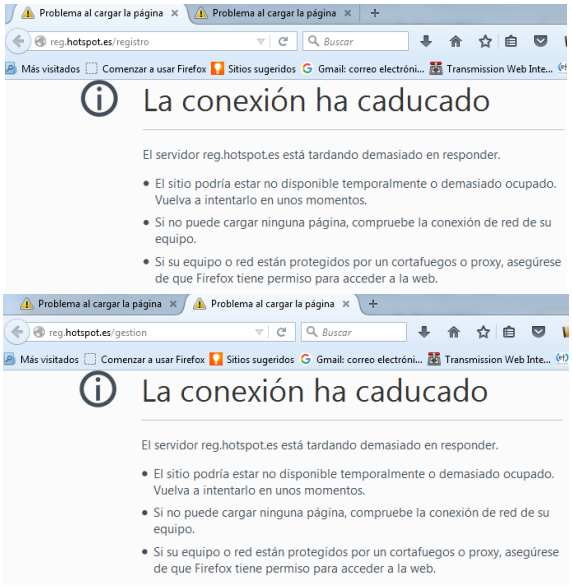

Figura 50 – Bloqueo a portal de registro y gestión.

Con todas las pruebas realizadas se puede concluir que el sistema cumple con los requisitos que se habían solicitado, de igual modo si en algún momento del uso del sistema se encuentra fallos o problemas, se destinará una partida en los costes del proyecto para tareas de mantenimiento sobre la aplicación, lo que incluiría posibles mejoras que haya que realizar en el desarrollo.

6. PLANIFICACIÓN Y PRESUPUESTO

En este punto se desarrollará la planificación del proyecto tanto en los apartados relativos a los recursos humanos que serán necesarios para su desarrollo e implantación como los recursos económicos que serán necesarios para su funcionamiento. De igual manera, se detallarán las tareas principales del proyecto con el objetivo de poder estimar una duración del mismo.

Para cualquier tipo de proyecto, pero más con los relacionados con informática y comunicaciones siempre se debe realizar una planificación para poder desarrollar el proyecto con garantías y alcanzar los objetivos marcados.

En este aspecto de alcanzar los objetivos, entran en juego dos factores muy importantes a tener en cuenta, en primer lugar los costes, para lo cual se hará una estimación del impacto económico que supone el desarrollo del proyecto y en segundo término, la duración, para lo cual se necesita definir las tareas y los tiempos estimados en cada una de ellas.

Con ambos factores definidos se podrá saber si es factible y asumible llevar a cabo el proyecto.

6.1 Planificación

Teniendo en cuenta las tareas principales que componen un proyecto software se pueden definir las siguientes para la estimación temporal de este proyecto:

Tarea	Duración
Especificación de requisitos	3 días
Análisis	7 días
Diseño	30 días
Implementación	40 días
Pruebas	20 días
Documentación	12 días
TOTAL	**112 días**

Tabla 5 - Planificación

La planificación ofrece la necesidad de tener 112 días, 16 semanas de desarrollo para la generación de los componentes necesarios para otorgar al sistema de un funcionamiento adecuado.

6.2. Recursos humanos

Será necesario cubrir los siguientes recursos:

Recurso	Número	Descripción
Jefe de proyecto	1	Será la persona encargada de realizar la supervisión del proyecto, controlar que se van cumpliendo los objetivos y las fechas estimadas para las tareas. Tendrá una dedicación parcial un 10 %.
Analista/desarrollador	2	Serán los encargados de desarrollar el proyecto siguiendo las pautas del jefe de proyecto tanto en los objetivos como en las tareas a realizar. Es conveniente que uno de ellos tenga conocimientos y experiencia en desarrollos con redes de comunicaciones. Mientras que la otra persona tenga habilidades para el desarrollo de páginas web. Ambos estarán dedicados al 100 % en el proyecto.
Probador/tester	1	Será el encargado de realizar las pruebas para comprobar el correcto funcionamiento del sistema. Estará dedicado parcialmente en un 25%.

Tabla 6 – Recursos humanos

6.3 Recursos materiales

Para la elaboración del proyecto han sido necesarios los siguientes recursos materiales:

Recurso	Descripción
Mikrotik Routerboard RB/951Ui-2HnD	600Mhz CPU, 128MB RAM, 5xLAN, 2.4Ghz 802b/g/n
Raspberry Pi 2	Kit de iniciación Raspberry Pi 2 Modelo B CPU quad-core 900MHz 1 GB RAM. Micro SD 8gb. Fuente alimentación.
Equipo de desarrollo	HP Pavilion 500-524NS CPU Intel Core i5-4460. RAM 4GB. Disco duro 1TB
Dispositivo móvil (Smartphone)	Samsung Galaxy Prime
Cableado	Cableado para redes de comunicaciones
Conexión a Internet	ONO 50 Mb/5Mb. Router Thomson TWG-870

Tabla 7 – Recursos materiales

6.4. Recursos económicos

A continuación se establecen los recursos económicos necesarios por un lado para cubrir los costes relativos a los recursos humanos asignados al proyecto y por otro para aquellos relativos a los recursos materiales.

En el primero de los casos es necesario tener en cuenta que las tarificaciones se especifican en euros por hora, por tanto se tendrán un total de 640 horas, teniendo en cuenta que se tendrán 5 días laborables de 8 horas para las 16 semanas especificadas. También se debe aplicar a esas horas totales el porcentaje de dedicación de cada miembro del equipo. Además hay que tener en cuenta los impuestos aplicables a estos costes.

Tipo de Recurso	**Tarifa**	**Horas trabajadas**	**Unidades**	**Coste**
Jefe de proyecto	18,00 €/h	64	1	1.152 €
Analista/desarrollador	15,00 €/h	640	2	19.200 €
Probador/tester	11,00 €/h	160	1	1.760 €
SUBTOTAL				**22.112 €**
Impuesto: IVA	21%		1	4.646,52 €
TOTAL				**26.755,52 €**

Tabla 8 – Costes en recursos humanos

En la siguiente tabla se muestran los costes relativos a los recursos materiales. Se ha establecido una relación de costes según las previsiones de costes del mercado actual.

Tipo de Recurso	**Coste Unitario**	**Unidades**	**Coste**
Mikrotik Routerboard RB/951Ui-2HnD	49,9 €	1	49,90 €
Raspberry Pi 2	62,2 €	1	62,20 €
Equipo de desarrollo	399 €	2	798 €
Dispositivo móvil (Smartphone)	150 €	1	150 €
Cableado	30 €	1	30 €
Conexión a Internet	39,9 €/mes	4	159,60 €
SUBTOTAL			**1.249,70 €**
Impuesto: IVA	21%	1	262,44 €
TOTAL			**1.512,14 €**

Tabla 9 – Costes en materiales

Como último punto se detallan los costes finales, también se ha añadido una partida para mantener el servicio al menos un año, que se destinará a mejoras en caso en el caso de que se encuentra problemas en la aplicación. El importe fina es de **29.767,66 €.**

Concepto	**Coste**
Recursos humanos	**26.755,52 €**
Recursos materiales	**1.512,14 €**
Costes de mantenimiento	1.500 €
TOTAL	**29.767,66 €**

Tabla 10 – Resumen de costes

7. CONCLUSIONES Y TRABAJOS FUTUROS

Para el desarrollo del proyecto he querido tener muy en cuenta elementos tanto de hardware como de software que sean actuales. Se puede citar el framework de Twitter Bootstrap en el desarrollo del elemento software y los dispositivos Mikrotik y Raspberry Pi en la parte de hardware.

Como ya se ha comentado en la parte de diseño, el framework de Twitter Bootstrap es muy común para el desarrollo actual de aplicaciones web, es uno de los más usados y ofrece muchas de las posibles funcionalidades que se requieren para las páginas web actuales. Sobre todo con la tendencia a ser vistas desde dispositivos móviles o tablet.

En cuanto a los dispositivos de Mikrotik, cabe comentar, que por mi experiencia laboral estos dispositivos se están usando en gran medida en el mundo de las redes de comunicaciones tanto cableadas como inalámbricas. Las grandes posibilidades de configuración, desarrollo e implementación que tienen, los hacen unos dispositivos muy adecuados para diferentes entornos. Desde entornos domésticos, funcionando como router que suministra el acceso a Internet conectado a la red del proveedor de servicios, hasta entornos empresariales y de grandes comunicaciones, ya que existen dispositivos de esta marca con gran capacidad de procesamiento de datos.

El dispositivo Raspberry Pi también se ha puesto muy de moda en diferentes entornos tanto en el mundo educativo, para dar los primeros pasos en el desarrollo de aplicaciones de arquitectura de computadores, como en el mundo de ocio, a modo de gestor de contenido audiovisual. También ofrece grandes posibilidades de configuración, en este caso se ha pensado su utilidad como servidor web de muy bajo coste comparado con un ordenador que estuviera exclusivamente dedicado a ese servicio.

También cabe decir que gran parte de las funcionalidades desarrolladas se han pensando para entidades, instituciones o negocios que quieren dar el acceso a Internet como un complemento adicional al desarrollo de su actividad habitual. Teniendo en cuenta que puede ser que no quieran dedicar una gran inversión de dinero y/o tiempo para este desarrollo.

De este punto anterior se deriva, que si la entidad institución o negocio se dedica exclusivamente como actividad, a la comercialización de este acceso a Internet, habría que desarrollar un modulo para las funcionalidades de facturación. Una línea futura de investigación que podría tratarse. Esta integración podría realizar con sistemas de pago en línea como puede ser Paypal o SafetyPay.

Para dotar de mayor seguridad a todas las comunicaciones entre los diferentes dispositivos del sistema y para evitar que las comunicaciones del usuario puedan ser interceptadas y vulneradas por terceras persona, se podría dotar a todo el sistema de transferencia segura de datos mediante el protocolo HTTPs.

Para lo cual sería necesario obtener certificados SSL para los diferentes elementos de la red. Tanto para el portal cautivo del hotspot, lo que daría opción de poder utilizar el método de autenticación mediante HTTPs, como para el portal de gestión y registro con lo que se

conseguiría que las comunicaciones del gestor con el portal de gestión se realizaran cifradas y las del usuario con el portal de registro también se realicen cifradas.

Para la creación de los certificados SSL, se podrían obtener emitidos por una autoridad de certificación de confianza. Autoridades de certificación como Verisign (ahora Symantec), GeoTrust, Comodo, Go Daddy o similares pueden ofrecer certificados SSL para cifrar las comunicación. [SSL]

Otra posible línea futura de desarrollo sería la integración del sistema de validación de datos con redes sociales o con Google. Con esto se quiere decir que el usuario pueda acceder al servicio de internet, introduciendo como datos de acceso, los que ya tenga registrados como cuenta personal en alguna red social ya sea Facebook o Twitter o la cuenta personal de la que dispongan en Google.

En este caso, los datos introducidos por el usuario en el portal cautivo en lugar de ser comparados con los que están almacenados en la base de datos local del hotspot, se mandarían a un servidor externo para realizar dicha validación. Se puede ver esta funcionalidad en la página web de Tripadvisor.

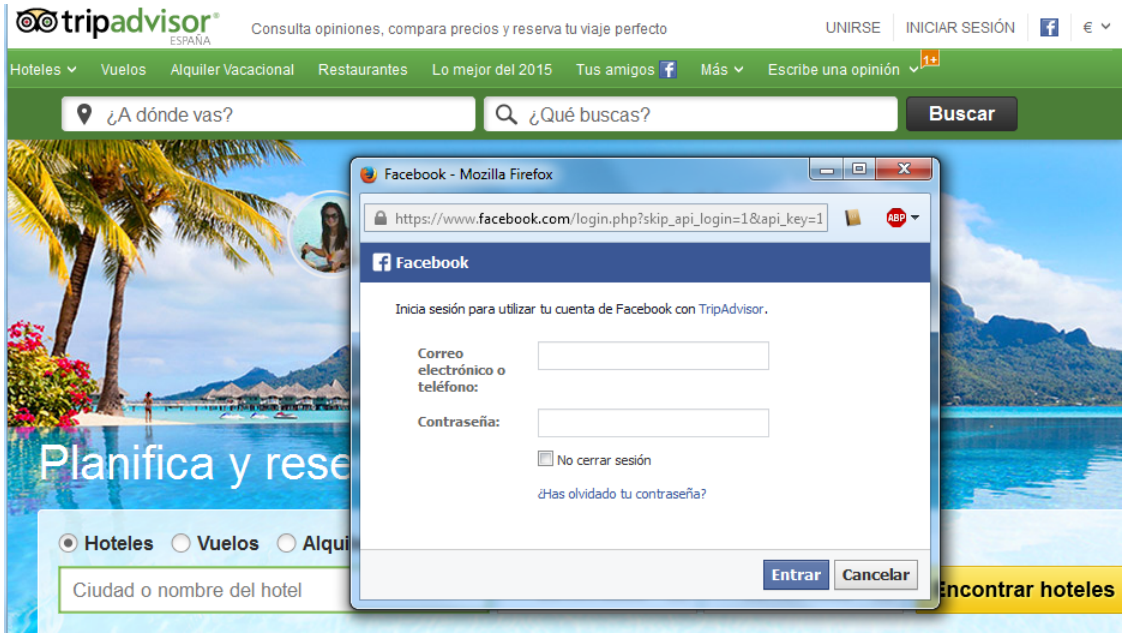

Figura 51 – Acceso mediante Facebook [tri]

Cabe citar como última línea futura de trabajo adaptar este hotspot a todas las posibles leyes o reales decretos que le puedan afectar.

Una vez finalizado el desarrollo del proyecto cabe decir que se han plasmado en él los conocimientos adquiridos a lo largo de la carrera. Con el desarrollo del sistema y la documentación se adquieren las habilidades para poder afrontar otros proyectos en el mundo laboral. También el proyecto me ha servido para darme cuenta que tareas que en un principio parecen triviales han llevado bastante trabajo y esfuerzo realizarlas.

Tengo que decir que es un proyecto que me ha resultado interesante realizar ya que trata de diferentes aspectos dentro del mundo de la informática. Especialmente de la redes de comunicaciones. El proyecto me ha servido para familiarizarme con nuevos lenguajes de programación como PHP y para conocer nuevas herramientas de desarrollo.

Pienso que este proyecto puede ser de utilidad en diferentes ámbitos y que su desarrollo ha sido pensado para que su uso se lleve a cabo por todo tipo de persona que no necesariamente tengan conocimientos en informática.

Todas las tareas relacionadas con el proyecto se han desarrollado con entusiasmo y dedicación, realizando un gran esfuerzo para su alcanzar su finalización.

8. DEFINICIONES Y TÉRMINOS

En el presente documento se pueden encontrar algunos términos que resulten desconocidos para el lector o que puedan resultar ambiguos. En adelante se enumeran algunos de ellos con su definición.

Redes de comunicaciones: Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos. Las redes o infraestructuras de comunicaciones proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o una comunicación. [1]

Redes inalámbricas: El término red inalámbrica (en inglés: wireless network) se utiliza en informática para designar la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada. Una de sus principales ventajas es notable en los costes, ya que se elimina el cableado Ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar a los intrusos. [2]

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Enrutador/router: Un router —anglicismo; también conocido como enrutador o encaminador de paquetes, y españolizado como rúter, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red), y que por tanto tienen prefijos de red distintos. [3]

Ghz: El gigahercio (GHz) es un múltiplo de la unidad de medida de frecuencia hercio (Hz) y equivale a 1 000 000 000 Hz.

Smartphone: El teléfono inteligente (en inglés: smartphone) es un tipo de teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar actividades, semejante a la de una minicomputadora, y con una mayor conectividad que un teléfono móvil convencional.

Tablet: Una tableta, en muchos lugares también llamada tablet (del inglés: tablet o tablet computer), es una computadora portátil de mayor tamaño que un teléfono inteligente o un PDA, integrada en una pantalla táctil con la que se interactúa con los dedos sin necesidad de teclado físico ni ratón.

1 http://wikitel.info/wiki/Redes_de_comunicaciones
2 https://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica
3 https://es.wikipedia.org/wiki/Router

Dirección MAC: En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. [4]

Radius: RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Service). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos. [5]

Implementación: Una implementación es la instalación de una aplicación informática, realización o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política.

Mikrotik: Mikrotīkls Ltd., conocida internacionalmente como MikroTik, es una compañía letona proveedora de tecnología disruptiva de hardware y software para la creación de redes. MikroTik se dedica principalmente a la venta de productos de hardware de red como routers denominados routerboards y switches también conocidos por el software que lo integra, denominado RouterOS y SwOS. [6]

RouterOS: Mikrotik RouterOS es un software que funciona como un Sistema Operativo para convertir un PC o una placa Mikrotik RouterBOARD en un router dedicado. [6]

Routerboard: La división de hardware de la marca MikroTik es caracterizada por incluir su sistema operativo RouterOS por defecto y actualizaciones de por vida. Estos dispositivos tienen la ventaja de tener una relación calidad/precio buena. [6]

GNU/Linux: Es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux con el sistema operativo GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera.[7]

Portal cautivo: Un portal cautivo (o captivo) es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede empezar a controlar el ancho de banda usado por cada cliente (haciendo lo que se llama Calidad de Servicio).[8]

4 https://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC
5 https://es.wikipedia.org/wiki/RADIUS
6 https://es.wikipedia.org/wiki/MikroTik#RouterOS
7 https://es.wikipedia.org/wiki/GNU/Linux
8 https://es.wikipedia.org/wiki/Portal_cautivo

Unix: Registrado oficialmente como UNIX®, es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969, por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Dennis Ritchie, Ken Thompson y Douglas McIlroy. [9]

Interfaz: Es lo que se conoce en inglés como interface ("superficie de contacto"). En informática se utiliza para nombrar a la conexión física y funcional entre dos sistemas o dispositivos de cualquier tipo dando una comunicación entre distintos niveles. [10]

Ethernet: Es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones (CSMA/CD). Su nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI. [11]

Wi-Fi: El wifi (nombre común en español proveniente de la marca Wi-Fi) es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con wifi —tales como una computadora personal, un televisor inteligente, una videoconsola, un teléfono inteligente o un reproductor de música— pueden conectarse a internet a través de un punto de acceso de red inalámbrica.[12]

VPN: Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.[13]

Windows: Microsoft Windows (conocido generalmente como Windows o MS Windows), es el nombre de una familia de distribuciones de software para PC, smartphone, servidores y sistemas empotrados, desarrollados y vendidos por Microsoft, y disponibles para múltiples arquitecturas.

MAC OS: Mac OS (del inglés Macintosh Operating System, en español Sistema Operativo de Macintosh) es el nombre del sistema operativo creado por Apple para su línea de computadoras Macintosh.

9 https://es.wikipedia.org/wiki/Unix
10 https://es.wikipedia.org/wiki/Interfaz
11 https://es.wikipedia.org/wiki/Ethernet
12 https://es.wikipedia.org/wiki/Wifi
13 https://es.wikipedia.org/wiki/Red_privada_virtual

Dirección IP: Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red.[14]

DNS: Domain Name System o DNS (en español «Sistema de Nombres de Dominio») es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.[15]

DHCP: Siglas en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de host», es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes.[16]

Gateway/puerta de enlace: La pasarela (gateway) o puerta de enlace es el dispositivo que permite interconectar redes de computadoras con protocolo de comunicaciones y arquitecturas diferentes a todos los niveles de comunicación.[17]

DoS: En seguridad informática, un ataque de denegación de servicios, también llamado ataque DoS (de las siglas en inglés Denial of Service) o DDoS (de Distributed Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.[18]

Javascript: JavaScript (abreviado comúnmente "JS") es un lenguaje de programación. Se utiliza principalmente en su forma del lado del cliente, implementado como parte de un navegador web permitiendo mejoras en la interfaz de usuario y páginas web dinámicas.[19]

HTML: Siglas de HyperText Markup Language («lenguaje de marcas de hipertexto»), hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que sirve de referencia para la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código (denominado código HTML) para la definición de contenido de una página web, como texto, imágenes, videos, entre otros.[20]

14 https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP
15 https://es.wikipedia.org/wiki/Domain_Name_System
16 https://es.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
17 https://es.wikipedia.org/wiki/Puerta_de_enlace
18 https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
19 https://es.wikipedia.org/wiki/JavaScript
20 https://es.wikipedia.org/wiki/HTML

CSS: Hoja de estilo en cascada o CSS (siglas en inglés de cascading style sheets) es un lenguaje usado para definir y crear la presentación de un documento estructurado escrito en HTML. [21]

PHP: Es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. [22]

Cookie: Una cookie (o galleta informática) es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

URL: Un localizador de recursos uniforme (conocido por la sigla URL, del inglés Uniform Resource Locator) es un identificador de recursos uniforme (Uniform Resource Identifier, URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo. [23]

URI: Un identificador de recursos uniforme o URI —del inglés Uniform Resource Identifier— es una cadena de caracteres que identifica los recursos de una red de forma unívoca. [24]

Firewall/cortafuegos: Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. [25]

OpenDNS: OpenDNS es una empresa que ofrece el servicio de resolución de nombres de dominio (DNS) gratuito (para uso privado en el hogar) y abierto en su versión más básica y original. Fue fundada en noviembre de 2005 por David Ulevitch. Más tarde añadió características opcionales gratuitas: corrección de errores ortográficos, filtrado de contenidos, protección contra phishing y robo de identidad, configurables a través de un panel de control, previo registro en su sitio web.

Framework: La palabra inglesa "framework" (marco de trabajo) define, en términos generales, un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar. [26]

Responsive: El diseño web adaptable o adaptativo, conocido por las siglas RWD del inglés Responsive Web Design, es una filosofía de diseño y desarrollo cuyo objetivo es adaptar la apariencia de las páginas web al dispositivo que se esté utilizando para visualizarla. [27]

21 https://es.wikipedia.org/wiki/Hoja_de_estilos_en_cascada
22 https://es.wikipedia.org/wiki/PHP
23 https://es.wikipedia.org/wiki/Localizador_de_recursos_uniforme
24 https://es.wikipedia.org/wiki/Identificador_de_recursos_uniforme
25 https://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29
26 https://es.wikipedia.org/wiki/Framework
27 https://es.wikipedia.org/wiki/Dise%C3%B1o_web_adaptable

Twitter Bootstrap: Es un framework o conjunto de herramientas de software libre para diseño de sitios y aplicaciones web. Contiene plantillas de diseño con tipografía, formularios, botones, cuadros, menús de navegación y otros elementos de diseño basado en HTML y CSS, así como, extensiones de JavaScript opcionales adicionales. [28]

API: La interfaz de programación de aplicaciones, abreviada como API (del inglés: Application Programming Interface), es el conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción. [29]

Raspberry Pi: Es un ordenador de placa reducida o (placa única) (SBC) de bajo coste desarrollado en Reino Unido por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas. [30]

Raspbian: Es una distribución del sistema operativo GNU/Linux y por lo tanto libre basado en Debian Wheezy (Debian 7.0) para la placa computadora (SBC) Raspberry Pi, orientado a la enseñanza de informática. [31]

HTTP: Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). El resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc. 32

HTTPs: Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP. Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales y/o contraseñas. 33

28 https://es.wikipedia.org/wiki/Twitter_Bootstrap
29 https://es.wikipedia.org/wiki/Interfaz_de_programaci%C3%B3n_de_aplicaciones
30 https://es.wikipedia.org/wiki/Raspberry_Pi
31 https://es.wikipedia.org/wiki/Raspbian
32 https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol
33 https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure

P2P: Una red peer-to-peer, red de pares, red entre iguales o red entre pares (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados. Normalmente este tipo de redes se implementan como redes superpuestas construidas en la capa de aplicación de redes públicas como Internet. El hecho de que sirvan para compartir e intercambiar información de forma directa entre dos o más usuarios ha propiciado que parte de los usuarios lo utilicen para intercambiar archivos cuyo contenido está sujeto a las leyes de derechos de autor, lo que ha generado una gran polémica entre defensores y detractores de estos sistemas. Las redes peer-to-peer aprovechan, administran y optimizan el uso del ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, y obtienen así más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación. [34]

Correo electrónico: (en inglés: e-mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante sistemas de comunicación electrónica. Para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales dependiendo del sistema que se use. [35]

Spam: Los términos correo basura y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La palabra equivalente en inglés, spam, proviene de la época de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada; entre estas comidas enlatadas se encontraba una carne enlatada llamada spam, que en los Estados Unidos era y sigue siendo muy común. Este término comenzó a usarse en la informática décadas más tarde al popularizarse, gracias a un sketch de 1970 del grupo de comediantes británicos Monty Python, en su serie de televisión Monty Python's Flying Circus, en el que se incluía spam en todos los platos. Aunque se puede hacer spam por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

34 https://es.wikipedia.org/wiki/Peer-to-peer
35 https://es.wikipedia.org/wiki/Correo_electr%C3%B3nico

Modelo OSI: El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como "modelo OSI", (en inglés, Open System Interconnection) es un modelo de referencia para los protocolos de red y la arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization). [36]

PDA: del inglés personal digital assistant, asistente digital personal, computadora de bolsillo, organizador personal o agenda electrónica de bolsillo, es una computadora de mano originalmente diseñada como agenda personal electrónica (para tener uso de calendario, lista de contactos, bloc de notas, recordatorios, dibujar, etc.) con un sistema de reconocimiento de escritura.

IP: Internet Protocol,en español 'Protocolo de Internet', es un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo OSI. Su función principal es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma OSI de enlace de datos. [37]

LAN: Una red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.[38]

WAN: Una red de área amplia, o WAN, (Wide Area Network en inglés), es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales, llamadas LAN, por lo que sus miembros no están todos en una misma ubicación física. [39]

Servidor: Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como "el servidor". [40]

Cliente: El cliente es una aplicación informática o un ordenador que consume un servicio remoto en otro ordenador conocido como servidor, normalmente a través de una red de telecomunicaciones. [41]

Debian: Debian o Proyecto Debian (en inglés: Debian Project) es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. El sistema se encuentra precompilado, empaquetado y en un formato deb para múltiples arquitecturas de computador y para varios núcleos. [42]

36 https://es.wikipedia.org/wiki/Modelo_OSI
37 https://es.wikipedia.org/wiki/Internet_Protocol
38 https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local
39 https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia
40 https://es.wikipedia.org/wiki/Servidor
41 https://es.wikipedia.org/wiki/Cliente_%28inform%C3%A1tica%29
42 https://es.wikipedia.org/wiki/Debian

WWW: En informática, la World Wide Web (WWW) o red informática mundial es un sistema de distribución de documentos de hipertexto o hipermedios interconectados y accesibles vía Internet. Con un navegador web, un usuario visualiza sitios web compuestos de páginas web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de esas páginas usando hiperenlaces. [43]

Punto de acceso inalámbrico: Un punto de acceso inalámbrico (en inglés: Wireless Access Point, conocido por las siglas WAP o AP), en una red de computadoras, es un dispositivo de red que interconecta equipos de comunicación alámbrica para formar una red inalámbrica que interconecta dispositivos móviles o con tarjetas de red inalámbricas. Los WAP son dispositivos que permiten la conexión inalámbrica de un dispositivo móvil de cómputo (computadora, tableta, smartphone) con una red. Normalmente, un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. [44]

Internet: Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen funcionen como una red lógica única de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como Arpanet, entre tres universidades en California (Estados Unidos). [45]

Proxy: Un proxy, o servidor proxy, en una red informática, es un servidor (un programa o sistema informático), que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la petición a C; de esta forma C no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, mejorar el rendimiento, mantener el anonimato, proporcionar Caché web, etc; este último sirve para acelerar y mejorar la experiencia del usuario mediante permisos que guardará la web, esto se debe a que la próxima vez que se visiten las páginas web no se extraerá información de la web si no que se recuperara información de la caché. [46]

Caché: En informática, la caché es la memoria de acceso rápido de una computadora, que guarda temporalmente los datos recientemente procesados (información). La memoria caché es un búfer especial de memoria que poseen las computadoras, que funciona de manera similar a la memoria principal, pero es de menor tamaño y de acceso más rápido. [47]

43 https://es.wikipedia.org/wiki/World_Wide_Web
44 https://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico
45 https://es.wikipedia.org/wiki/Internet
46 https://es.wikipedia.org/wiki/Proxy
47 https://es.wikipedia.org/wiki/Cach%C3%A9_%28inform%C3%A1tica%29

Comunicación inalámbrica: La comunicación inalámbrica o sin cables es aquella en la que la comunicación (emisor/receptor) no se encuentra unida por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio. En este sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, entre los cuales se encuentran: antenas, portátiles, PDA, teléfonos móviles, etc. [48]

TCP/IP: La familia de protocolos de Internet es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen, que fueron de los primeros en definirse, y que son los dos más utilizados de la familia: TCP (Transmission Control Protocol), Protocolo de Control de Transmisión, e, IP (Internet Protocol), Protocolo de Internet. La familia de protocolos de Internet puede describirse por analogía con el modelo OSI (Open System Interconnection), que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. [49]

TCP: Transmission Control Protocol (TCP) o Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por redes de computadoras, pueden usar TCP para crear "conexiones" entre sí a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. [50]

Puerto: Un puerto de red es una interfaz para comunicarse con un programa a través de una red. En el modelo OSI quien se preocupa de la administración de los puertos y los establece en el encabezado de los segmentos es la capa de transporte o capa 4, administrando así el envío y re-ensamblaje de cada segmento enviado a la red haciendo uso del puerto especificado. Un puerto suele estar numerado para de esta forma poder identificar la aplicación que lo usa. [51]

SSL: Transport Layer Security (TLS; en español «seguridad de la capa de transporte») y su antecesor Secure Sockets Layer (SSL; en español «capa de conexión segura») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet. Se usan certificados y por lo tanto criptografía asimétrica para autentificar a la contraparte con quien se están comunicando, y para intercambiar una llave simétrica.

48 https://es.wikipedia.org/wiki/Comunicaci%C3%B3n_inal%C3%A1mbrica
49 https://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet
50 https://es.wikipedia.org/wiki/Transmission_Control_Protocol
51 https://es.wikipedia.org/wiki/Puerto_de_red
52 https://es.wikipedia.org/wiki/Transport_Layer_Security

9. REFERENCIAS

[hot] Mikrotik. (2008) The diagram below shows a sample HotSpot setup. [Figura]. Recuperado de https://www.mikrotik.com/testdocs/ros/3.0/pnp/hotspot.php

[wik] Wikpedia. *Hotspot (Wi-Fi)* [en línea]. Disponible en https://en.wikipedia.org/wiki/Hotspot_%28Wi-Fi%29

[ipa] iPass. *Wi-fi Growth Map* [en línea]. Disponible en https://www.ipass.com/wifi-growth-map/

[mik] Mikrotik. *Mikrotik router and wireless* [en línea]. Disponible en http://www.mikrotik.com/

[dis] Mikrotik. (2015). RB951G-2HnD.[Fotografía]. Recuperado de http://routerboard.com/RB951G-2HnD

[ubi] Ubiquiti Networks. *Unifi* [en línea]. Disponible en https://www.ubnt.com/enterprise/software/

[coo] Coova.org. *CoovaChilli* [en línea]. Disponible en https://coova.github.io/

[fcc] ITSYOURIP.COM. (2007). CoovaChilli – Opensource Software Access Controller. [Figura]. Recuperado de http://www.itsyourip.com/Security/coovachilli-opensource-software-access-controller/

[con] Connectify. *Connectify Hotspot* [en línea]. Disponible en http://www.connectify.me/

[4ip] 4ipnet. *Wireless Hotspot Gateway* [en línea]. Disponible en http://www.4ipnet.com/products/wireless-hotspot-gateway

[net] NetCommWireless. *HS1200NPAK* [en línea]. Disponible en http://www.netcommwireless.com/product/wifi/hs1200npak

[cha] Montañana, R. (2009). Funcionamiento de CHAP (Challenge Handshake Protocol). [Figura]. Recuperado de http://slideplayer.es/slide/106504/ ,modificado para su mejor interpretación.

[htt] Fahrudin, A. (2014). HTTP vs HTTPS. [Figura]. Recuperado de http://www.slideshare.net/aldifahrudin/open-ssl-certificate-https-for-hotspot-mikrotik

[dns] Open DNS. (2015). [Captura de pantalla].Recuperado de https://www.opendns.com/

[spe] Speedtest. (2015). [Captura de pantalla]. Recuperado de http://www.speedtest.net/es/

[ssl] Sumastre, Michael Gabriel. *The Top 7 Most Reliable SSL Certificate Providers* [en línea]. Pluralsight blog. Disponible en http://blog.pluralsight.com/top-reliable-ssl-certificates

[tri] Tripadvisor. (2015). [Captura de pantalla]. Recuperado de http://www.tripadvisor.es/

10 - BIBLIOGRAFÍA

- Mikrotik. *Mikrotik documentation* [Wiki en Internet]. Disponible en http://wiki.mikrotik.com/wiki/Main_Page

- *Mikrotik Forum* [en línea]. Disponible en http://forum.mikrotik.com/

- W3schools*. PHP 5 Tutorial* [Wiki en Internet]. Disponible en http://www.w3schools.com/php/

- W3schools *Javascript Tutorial* [Wiki en Internet]. Disponible en http://www.w3schools.com/php/

- Eguiluz, Javier. *Introducción a JavaScript* [en línea].Disponible en http://librosweb.es/libro/javascript/>

- Otto,Mark; Thornton, Jacob. *Bootstrap 3, el manual oficial* [en línea]. Disponible en https://librosweb.es/libro/bootstrap_3/

- *Twitter Bootstrap* [en línea]. Disponible en http://getbootstrap.com/

- Powers, David. *PHP Solutions: Dynamic Web Design Made Easy.* 2014.

- Gralla, Preston. *Cómo funcionan las redes inalámbricas.* 2006.

-Tanenbaum, Andrew S. *Redes de ordenadores.* 2ª ed., 1ª ed. en español, 1991.

- Geier, Eric. *Wi-Fi hotspots.* 2007.

- Cowburn, Peter (ed). *Manual de PHP* [en línea]. Disponible en https://secure.php.net/manual/es/

- *Tutoriales FPDF* [en línea]. Disponible en http://www.fpdf.org/

- MRCELHW. *Tutorial Raspberry Pi – Crear servidor web* [en línea]. 2013. Disponible en https://geekytheory.com/tutorial-raspberry-pi-crear-servidor-web/