“AÑO DE LA CONSOLIDACIÒN DEL MAR DE GRAU”
UNIVERSIDAD PERUANA LOS ANDES
FACULTAD DE INGENIERÍA
ESCUELA ACADÉMICA PROFESIONAL DE INGENIERÍA DE
SISTEMAS Y COMPUTACIÓN

DISEÑO DE UN SISTEMA DE PUNTOS DE ACCESO INALÁMBRICOS DE ACCESO PÚBLICO (HOTSPOT) PARA LA DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL

INFORME TÉCNICO

PRESENTADO POR EL BACHILLER:

ROBLES CÓRDOVA ERICK JONATAN

PARA OPTAR EL TÍTULO PROFESIONAL EN:

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

HUANCAYO – PERÚ

2016

Dr. Rubén Darío Tapia Silguera
Presidente

Jurado

Jurado

Jurado

Mg. Miguel Ángel Carlos Canales
Secretario Docente

DEDICATORIA

A Dios, quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mi familia quienes por ellos soy lo que soy.

Para mis padres por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

A mi hermano por estar siempre presente, acompañándome para poderme realizar. A mis sobrinos Axel y Camila quienes han sido y son mi motivación, inspiración y felicidad.

RESUMEN

El presente Informe Técnico plantea una propuesta para el diseño de un Sistema de Puntos de Acceso Inalámbricos de Acceso Público (Hotspot), para las instalaciones de la Dirección de Titulación de Tierras y Catastro Rural, que al no contar con dicho sistema, el personal sufre problemas a la hora de querer conectarse a la red y por ende la falta de información oportuna, pérdida de tiempo e incomodidad en las personas. Dada la problemática, es indispensable el uso de una alternativa tecnológica económica y eficiente a fin de asegurar que el personal tenga acceso a Internet, cuente con la información oportuna en tiempo real y sean más eficientes incrementando la productividad.

El objetivo principal del presente Informe Técnico es diseñar un Sistema de Puntos de Acceso Inalámbricos de Acceso Público (Hotspot) para la Dirección de Titulación de Tierras y Catastro Rural, por tal motivo, se realizará un estudio de las principales tecnologías y estándares de comunicaciones inalámbricas en la actualidad como: IEEE 802.11 en sus especificaciones 802.11a, 802.11b y 802.11g, se describirá los principales métodos de seguridad inalámbricos, se seleccionará la tecnología y un estándar de seguridad, teniendo en consideración los requerimientos de la institución.

Para el diseño de un Sistema de Puntos de Acceso Inalámbricos de Acceso Público (Hotspot) el presente Proyecto tiene cuatro capítulos:

El primer capítulo define los aspectos generales del presente informe, y los objetivos que se desea lograr. El segundo capítulo define el marco teórico y describe la tecnología a usar. El tercer capítulo describe la Institución en estudio. El cuarto capítulo menciona el análisis actual de la Red y describe su funcionamiento. El quinto capítulo define la arquitectura y el diseño de la red a realizar.

INTRODUCCIÓN

La gran aceptación en el mercado y el rápido desarrollo de las tecnologías inalámbricas 802.11 (Wi-Fi), 802.15. (Bluetooth), 802.16 (Wimax) etc, ha revolucionado las comunicaciones a nivel mundial al brindar gran flexibilidad y movilidad a usuarios que necesitan acceder a Internet, a su información en cualquier lugar, parte y a cualquier hora.

Cualquier usuario legítimo puede conectarse a una red inalámbrica fácilmente y así puede transmitir y recibir datos, voz y video en tiempo real.

En la actualidad la Dirección de Titulación de Tierras y Catastro Rural. Cuenta con una red que está conectada a la red LAN de la Dirección Regional de Agricultura Junín la cual se encuentra de manera desordenada, esto impide el buen desempeño de las labores de los trabajadores de la misma. Esta red genera dificultad para acceder a la información de manera oportuna y en tiempo real, sumándole a esto la lentitud de la red LAN. La Institución no cuenta con puntos de acceso inalámbricos y esto representa un problema ya que la Dirección de Titulación de Tierras y Catastro Rural al igual que muchas de las entidades de la Región deben de estar a la vanguardia en lo que se refiere a tecnología.

Ante los posibles requerimientos de la Institución y dada la necesidad de contar con un Hotspot, éste debe brindar servicios como el acceso a Internet, seguridad, segmentación de usuarios, manejo centralizado, gran cobertura, versatilidad de infraestructura y escalabilidad. Por otro lado el de mejorar la calidad del servicio a Internet. Entonces resulta necesario el diseño de un Hotspot que permita brindar y satisfacer los servicios antes mencionados para el personal de la Dirección de Titulación de Tierras y Catastro Rural

ÍNDICE

Índice de Figuras

Capítulo I

Capítulo II

Capítulo III

Capítulo IV

Capítulo V

Índice de Tablas

Capítulo II

Capítulo V

Índice de Cuadros

Capítulo V

CAPÍTULO I

ASPECTOS GENERALES

1.1. IDENTIFICACIÓN DEL PROBLEMA

La constante expansión de las redes de área local y el crecimiento que se viene dando en el desarrollo de las comunicaciones móviles ha motivado la búsqueda de nuevas soluciones de conectividad. Este crecimiento continúa a paso acelerado a medida que se desarrollan mercados emergentes.

Una de las soluciones que comienza a tener auge importante son las Redes Inalámbricas ó Wireless LAN (WLAN), basadas en el estándar IEEE 802.11, una de las principales funciones de este tipo de redes es proporcionar conectividad y acceso a las redes cableadas (Ethernet) proveyéndoles de la flexibilidad y de la movilidad que ofrecen las comunicaciones inalámbricas.

El reciente aumento en la implementación de redes inalámbricas nos obliga a contemplar con más cuidado el aspecto de la seguridad en este tipo de redes. Así como en el caso de las típicas redes de datos con cables, tiene que asegurarse que los usuarios de una red inalámbrica se encuentren conectados a ésta de una manera segura, teniendo en cuenta que ahora el medi de transmisión ya no se restringe a un cable, sino que se encuentra en todo el ambiente que lo rodea. Debe de comprobarse que el usuario sea quien dice ser (autenticación), que solo tenga acceso a los recursos que le

corresponda (autorización) y también llevar a cabo un registro de las actividades que haga dentro de la red (contabilidad); realizando todo esto de una manera segura y sin que sujetos ajenos a la red puedan estar leyendo información confidencial ni mucho menos tratar de modificarla.

En la Institución existen servicios que requieren ser usados por el personal como acceso a internet, correo electrónico, descarga y trasferencia de archivos, etc. De igual manera existen actividades propias de la institución que necesitan de puntos de acceso a la red alámbrica pero solo se cuenta con puntos de acceso limitados con lo cual surge incomodidad y malestar no solo por el personal sino también por las personas ajenas a la institución.

En la actualidad la Institución en la cual se diseñará el Hotspot, no cuenta con una red inalámbrica de acceso a Internet, la problemática de diseño se extiende desde implementar una topología nueva y seleccionar los equipos necesarios para añadir a la red, porque es importante la confidencialidad de la información y debido a múltiples ataques de personas mal intencionadas a nivel mundial que buscan borrar, manipular, espiar y dañar archivos importantes así como obtener contraseñas y usarlas a su beneficio es necesario implementar un sistema de seguridad robusto que pueda eludir de manera confiable los ataques de personas no autorizadas, así el diseño será eficiente y confiable.

Por otro lado existe una consideración importante que se debe tener presente con este trabajo es que las redes inalámbricas no pretenden sustituir a las redes tradicionales, sino complementarlas. En este sentido, buscamos proporcionar facilidades no disponibles en los sistemas cableados y permitir la coexistencia de ambos tipos de red.

1.2. FORMULACIÓN DEL PROBLEMA

¿En qué medida el diseño de un Sistema de Puntos de Acceso Inalámbricos de Acceso Público (Hotspot) contribuirá en beneficio de la Dirección de Titulación de Tierras y Catastro Rural?

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Diseñar un Sistema de Puntos de Acceso Inalámbricos de acceso público (Hotspot) que garantice los niveles de cobertura, seguridad y rendimiento para la Dirección de Titulación de Tierras y Catastro Rural.

1.3.2. OBJETIVOS ESPECÍFICOS

- **Seleccionar la tecnología adecuada**: Es necesario la utilización de tecnologías inalámbricas especialmente diseñadas para redes de computadoras de área local y buscar la adaptación de éstas para una aplicación en particular. La red de computadoras debe tener como características: la fácil instalación y adaptación de la red a nuevas infraestructuras, así como modularidad, escalabilidad y políticas de seguridad.
- **Determinar la ubicación de las estaciones (Access Point):** Se debe elaborar un plan de ubicación que debe considerar la cobertura de señal tanto como la utilización mínima de Access point; una vez definido el plan de ubicación se debe realizar el reconocimiento de la infraestructura para ver si es posible ubicarlo en ese punto. La ubicación de cada estación dependerá de la infraestructura.

- **Establecer la viabilidad económica**: se debe buscar un diseño con tecnologías adecuadas a bajo costo tomando en cuenta las necesidades, el entorno y capacidades adquisitivas.

1.4. JUSTIFICACIÓN

Es por eso que las instituciones públicas y privadas tanto como las empresas, han optado por este sistema de red tan innovador que les permitirá alcanzar un rendimiento más óptimo en el desempeño de sus múltiples labores que a diario realizan. Todo esto con el fin de satisfacer sus necesidades y al mismo tiempo poder competir en el mercado que hoy en día busca soluciones más rápidas y eficaces para sus demandas. Ya que el diseño de un Hotspot permitirá la mejora en cuanto a transmisión y comunicación de datos entre sus áreas, trayendo consigo un mejor servicio.

Hoy en día las entidades en mención se dan cuenta de que la manera más fácil de ahorrar tiempo, dinero y esfuerzo en el manejo de información es haciéndolo mediante el uso de una red y que mejor si ésta, utiliza dispositivos inalámbricos, ya que es un problema reestructurar su red mediante un tendido de cableado, por lo que en

ocasiones se tienen que perforar y ranurar paredes, techos y muchas veces la estructura de los edificios.

Este diseño de un Hotspot permitirá a la Dirección de Titulación de Tierras y Catastro Rural intercomunicarse con todas sus áreas minimizando costos y mejorando el desempeño de sus labores. Por ello es indispensable contar con una red inalámbrica que complemente el uso del cableado, para contar con un sistema moderno, seguro, rápido y efectivo que le den la tan ansiada solución a todos sus problemas.

Por eso se propone instalar tres puntos de acceso (Access point) D-link DWL – 2100 AP, y a cada máquina que estará en la red se le colocará una tarjeta de red PCI D-Link DGE-528T Gigabit Ethernet 10/100/1000 Mbps, las antenas se colocaran estratégicamente, con esto se tendrá señal en todo el espacio de la institución y de esta manera las máquinas y el equipo inalámbrico tendrán conexión.

1.5. PLANTEAMIENTO DE LA SOLUCIÓN TECNOLÓGICA

La solución para el presente trabajo de investigación es realizar el diseño de un Sistema de Puntos Acceso Inalámbricos de Acceso Público (Hotspot) que permita el acceso a internet, la transferencia de información y de comunicación en tiempo real.

1.6. METODOLOGÍA

El presente Informe está enmarcado dentro de una serie de pasos que guían el desarrollo del Proyecto, después de la revisión de algunas metodologías enfocadas en el tema de redes se ha decidido aplicar la metodología para el Análisis, Arquitectura y Diseño de Redes de James McCabe Tercera Edición, que consta de tres fases: Análisis, Arquitectura y Diseño.

Fase de Análisis

- Recabar requerimientos.
- Definir las aplicaciones que se ejecutarán en forma distribuida.
- Caracterizar como usan los usuarios las aplicaciones, definir métricas para medir el desempeño.
- Distinguir entre requerimientos de servicio: Entradas y Salidas.
- Definir flujos, establecer las fronteras de flujo.

Fase de Arquitectura

- Evaluar opciones de diseño del cableado
- Seleccionar la ubicación de los equipos
- Realizar el diagrama físico de la red
- Incorporar las estrategias de enrutamiento con base en los flujos
- Optimizar flujos de enrutamiento
- Desarrollar una estrategia de asignación de direcciones, asignar las direcciones
- Desarrollar una estrategia detallada de enrutamiento
- Entrada: algoritmos de enrutamiento disponibles

Fase de Diseño

- Establecer metas de diseño.- Desarrollar criterios para evaluación de tecnologías:
  Costo, rapidez, confiabilidad, etc.
- Realizar la selección de tecnologías.
- Integrar mecanismos de interconexión.
- Integrar aspectos de administración y seguridad al diseño.
- Incorporar análisis de riesgos y planificación de contingencias.
- Evaluar opciones de diseño del cableado.
- Seleccionar la ubicación de los equipos.
- Realizar el diagrama físico de la red.
- Incorporar las estrategias de enrutamiento con base en los flujos.
- Optimizar flujos de enrutamiento.
- Desarrollar una estrategia detallada de enrutamiento.

CAPÍTULO II

MARCO TEÓRICO

2.1. CONCEPTO DE REDES

Las redes de computadoras no son más que un conjunto de medios para proporcionar servicios de telecomunicación entre cierto número de ubicaciones. Una ubicación (fija o móvil) es conocida como punto de terminación de red o simplemente "ptr". Así pues, podríamos ver una red como algo abstracto que ofrece un determinado servicio en puntos de terminación de red. También puede definirse como un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios. En la figura 2.1 se muestra el diseño de una Red. [1]

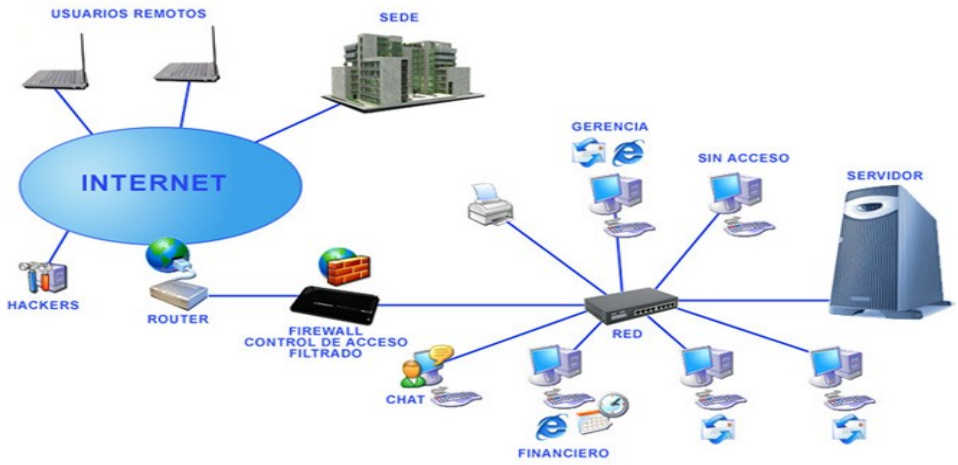


Figura 2.1 - Gráfico de Red de computadoras.
Fuente: Cisco Redes

2.2. ANTECEDENTES

En 1990 se formó en EE.UU el grupo de trabajo IEEE 802.11, para el estudio y desarrollo de estándares de redes WLAN. Su principal tarea fue el desarrollo de un estándar mundial para equipos y redes inalámbricas que trabajasen en la banda de frecuencias ISM (Industry, Science and Medicine), alrededor de 2,4 GHz y con tasas de transmisión de 1 a 2 Mbits/s. En cierto modo, con este estándar se pretendía unificar el mercado WLAN, bastante confuso y repleto de soluciones propietarias. La especificación original permitía tres tipos diferentes de técnicas de transmisión: espectro ensanchado por secuencia directa (DSSS), espectro ensanchado por salto de frecuencia (FHSS), e infrarrojos, si bien el mayor desarrollo se ha realizado para DSSS.

El estándar IEEE 802.11 fue adoptado finalmente en 1997. Todos los equipos que implementan esta tecnología (Tarjeta de red, puntos de acceso, etc.) se basan en una estructura de capas de acuerdo con el modelo de referencia OSI. La primera capa es el medio de transmisión o nivel físico. Por otro lado la siguiente capa (nivel de enlace) define el control de acceso al medio (MAC) y el control de enlace lógico (LLC). Este último está definido por el estándar IEEE 802.2 por lo que para las capas superiores una red 802.11 es equivalente a una red Ethernet, facilitándose de este modo la interconexión entre redes heterogéneas basadas en distintos estándares IEEE. La tasa de transmisión que permite el estándar IEEE 802.11 son de 1 y hasta 8Mbits/s. EK esquema de modulación propuesto para velocidades de 1 hasta 11 Mbits/s es BPSK, mientras que para 1 hasta 108 Mbits/s es QPSK. [13]

Desde 1985 hasta 1990 se consiguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbits/s, el mínimo establecido por el IEEE 802.2 para que la red sea considerada realmente una LAN, con aplicación empresarial.

Las redes WLAN se componen fundamentalmente de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como un concentrador o hub que reciben y envían información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente una PC o un ordenador portátil con una tarjeta de red inalámbrica, con o sin antena que se instala en uno de los slots libres o bien se enlazan a los puertos USB de los equipos.

En la actualidad los puntos de conexión son áreas de alto uso de tecnología de redes de área local (LAN) inalámbricas públicas. Con más y más personas que han aprendido a disfrutar de esta tecnología, los puntos de acceso están proliferando frenéticamente en el hogar, la oficina y en todo el mundo. La firma de analistas Gartner, predice que habrán más de 600.000 puntos de conexión de LAN Inalámbricas (WLAN) públicas y más de 90 millones de usuarios en dichos puntos de conexión para el año 2012. [3]

2.3. REDES INALÁMBRICAS

Las redes inalámbricas (Wireless Network) son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

En un principio las redes inalámbricas se desarrollaron en base a radioenlaces, y posteriormente desde el año 1996 aparecieron las primeras redes propietarias portátiles, estando el desarrollo actual normado para que la tecnología pueda ser utilizada independientemente de cuál es el fabricante de los equipos. Las normas han surgido en base a estándares regulados por la IEEE (Institute of Electrical and Electronics Engineers), una entidad sin fines de lucro, que reúne a más de 360.000 miembros de 175 países (base de datos de IEEE).

Las empresas telefónicas celulares por su parte también han ingresado al mercado de redes de datos, pero su enfoque hasta ahora ha sido como adicional a su servicio principal que es la comunicación de voz. Es probable que las redes de telefonía celular se dediquen cada vez más a los datos, mejorando el ancho de banda disponible para ello, para telefonía existe una dificultad el ancho de banda, es muy costoso; en el Perú es regulado por el Ministerio de Transportes y Telecomunicaciones; en el documento PNAF (Plan Nacional de Atribución de Frecuencias). En redes de computadoras inalámbricas se usan las frecuencias libres estandarizadas conocidas como bandas ISM 2.4 GHZ. [4]

Ha habido varios intentos de desarrollo de redes inalámbricas con diferentes tecnologías. Una de ellas es basada en la denominada tecnología infrarrojo, que se ha utilizado exitosamente para comunicación de dispositivos entre sí, como calculadoras portátiles o bien la comunicación de una computadora (PC) con otros equipos tal como una impresora, una agenda electrónica (Palm o PDA), y no tanto

para acceder a redes. Su alcance es limitado debido a que las ondas infrarrojas no pueden atravesar objetos opacos.

Otra tecnología inalámbrica exitosa es Bluetooth, creada para comunicar una PC con un teléfono celular o bien con micrófonos, mouse u otros. Es también de corto alcance, pero tienen la ventaja de requerir muy poca energía, razón por la cual es muy popular en los audífonos inalámbricos de los celulares.

Si bien, Wi-Fi se creó para acceder a redes LAN en forma inalámbrica, hoy se utiliza mayormente para acceder a internet. Recientemente han surgido los llamados "Hot-Spots" o redes públicas inalámbricas, establecidas en determinados lugares para conectarse a internet, basadas en Wi-Fi, que corresponde al estándar IEEE 802.11. Dichos lugares son en general zonas de uso público como aeropuertos, restaurantes y cafeterías, universidades, etc., en donde es posible acceder a internet en forma inalámbrica. Hay lugares en que el acceso es compartido gratuitamente, y sólo es necesario acceder a la red inalámbrica para tener acceso a Internet (Free Hot-Spot).

También hay espacios en que se debe realizar un pago por el acceso. Pero indudablemente una importante aplicación del denominado Wi-Fi es en el hogar, en las empresas, centros de esparcimiento, donde puede establecerse fácilmente una red inalámbrica de bajo costo; mediante la cual se puede compartir la impresora o el acceso a internet desde cualquier ubicación de su casa o departamento y sin tener que romper murallas o desplegar cables, esta tecnología permite conectarse a una distancia de 100 metros o más.

Ya que todas estas tecnologías están disponibles para el usuario final, debemos advertir que para un mundo convulsionado como el actual, se deben tener precauciones de seguridad para prevenirnos de un uso malintencionado.

Así como una persona tiene acceso a una red en particular en forma inalámbrica, cualquiera que esté en las cercanías también lo tiene. Si no se implementan medidas de seguridad adecuadas, al desplegar redes inalámbricas como en cualquier red, es factible que se vulnere la privacidad de la información.

De nada sirve que una empresa tenga cortafuegos y adopte medidas de seguridad extremas para su red cableada, si alguno de sus empleados instala un acceso inalámbrico en su puesto de trabajo sin protección adecuada. Al instalar una red

inalámbrica, preocúpese de activar las protecciones de acceso que la tecnología también le ofrece.

En la actualidad existen muchas maneras de implementar redes inalámbricas y distintos estándares, existen organizaciones internacionales que ya formalizaron estándares para el uso de redes inalámbricas la IEEE (INSTITUTO DE INGENIEROS ELECTRICOS Y ELECTRONICOS), UIT (UNION INTERNACIONAL DE TELECOMUNICACIONES) y la IETF (INTERNET ENGINEERING TASK FORCE) y que dicta normas llamadas RFC que son las normas que rigen el tráfico de internet (red de redes), por recomendación de la UIT en la actualidad para redes inalámbricas de corto alcance y de largo alcance todas están normalizadas. [2]

2.3.1. DEFINICIÓN DE RED INALÁMBRICA

Una Red Inalámbrica es un sistema flexible de comunicaciones que puede implementarse como una extensión o una alternativa a una red cableada. Este tipo de redes utiliza tecnología de radio frecuencia, minimizando así la necesidad de conexiones cableadas. Esto proporciona al usuario movilidad sin perder conectividad de la red. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la eliminación del medio de transmisión cableado. Las WLAN son la alternativa ideal para hacer llegar una red LAN cableada a lugares donde el cableado no lo permite. [5]

2.3.2. ¿PORQUE UTILIZAR REDES INALÁMBRICAS?

En la actualidad, prácticamente todas las instituciones, entidades y empresas necesitan de una red de comunicación, por lo tanto parece sencillo comprender que si esta comunicación se realiza sin una conexión física, esto hará que compartir información sea mucho más cómodo y además nos permita una mayor movilidad de los equipos. Esta movilidad se observa claramente cuando se desea cambiar la colocación de los equipos en una oficina conectada a una red por medio de cables. Este cambio provocaría tener que redistribuir la colocación de los cables en dicha oficina. Sin embargo con una red inalámbrica este trabajo no sería necesario realizarlo.

2.3.3. BENEFICIOS DE LAS REDES INALÁMBRICAS

Respecto a la red tradicional la red sin cable ofrece los siguientes beneficios:

- **Basada en estándares y con certificación Wi-Fi.** Es un robusto estándar de redes, comprobado a nivel de la industria de transmisión de datos, que asegura que los productos inalámbricos ínter operarán con otros productos certificados Wi-Fi de otros fabricantes de redes. Con un sistema basado en Wi-Fi, los usuarios gozarán de compatibilidad con el mayor número de productos inalámbricos y evitarán los altos costos y la selección limitada de las soluciones patentados por un sólo fabricante. Además, la selección de una solución inalámbrica basada en estándares, que sea totalmente ínter operable con redes Ethernet y Fast Ethernet, le permitirá al usuario que su red inalámbrica trabaje sin interrupciones con su sistema existente de LAN tradicional.

- **Instalación simple.** La solución inalámbrica debe ser del tipo plug and play; tomando solamente unos minutos para su instalación. Al conectarla, los usuarios empezarán a gozar de inmediato de los servicios en red. Para obtener una instalación aún más fácil, su solución deberá soportar el protocolo denominado Dynamic Host Configuration Protocol (DHCP), el cual asignará automáticamente direcciones IP a los clientes inalámbricos. En lugar de instalar un servidor DHCP en algún aparato independiente para obtener esta capacidad de ahorro de tiempo, los usuarios deben seleccionar Hubs inalámbricos que ofrezcan servidores DHCP incorporados. Si un usuario está agregando un sistema inalámbrico a su red Ethernet, sería una buena opción potenciar un punto de acceso a través de cables estándares de Ethernet; esto le permitirá hacer que el punto de acceso funcione utilizando un voltaje bajo de corriente en el mismo cable que es usado para transmitir datos: eliminando la necesidad de tener una toma de poder local y un cable para cada dispositivo de puntos de acceso. Una WLAN es rápida, fácil y elimina la necesidad de tirar cables a través de paredes y techos, permitiendo a la red llegar a puntos de difícil acceso para una LAN cableada.

- **Robusta y confiable.** Considera soluciones inalámbricas robustas que tienen alcances de por lo menos 100 metros. Estos sistemas les ofrecerán a los empleados de una institución una considerable movilidad dentro de sus instalaciones. Un usuario puede optar por un sistema superior que automáticamente detecte el ambiente, para seleccionar la mejor señal de

frecuencia de radio disponible y obtener máximos niveles de comunicaciones entre el punto de acceso y las PC cards. Para garantizar una conectividad a las velocidades más rápidas posibles incluyendo largo alcance o ambientes ruidosos el usuario debe asegurarse que su nuevo sistema pueda hacer cambios dinámicos de velocidades, basándose en las diferentes intensidades de señal y distancias del punto de acceso. Además, el usuario debe seleccionar PC cards inalámbricas para computadoras portátiles que ofrezcan antenas retractables para prevenir rupturas durante la movilización de los aparatos.

- **Escalabilidad.** Un buen hub inalámbrico deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas en computadoras adicionales e impresoras listas para ser conectadas a la red. Las impresoras u otros dispositivos periféricos que no puedan conectarse en red tradicional, se conectan a su red inalámbrica con un adaptador USB inalámbrico o un Ethernet Client Bridge.

- **Facilidad de uso.** Si un usuario planea conectar múltiples puntos de acceso inalámbricos a una red existente de cables, debe considerar una solución que ofrezca conexiones automáticas a la red. Cuando un usuario se desplace fuera de los límites de un Hub al campo de otro, una capacidad automática de conexión a la red transferirá sus comunicaciones sin interrupciones al siguiente aparato, aún al cruzar límites de routers, sin siquiera tener que reconfigurar la dirección IP manualmente. Esto resulta ser especialmente útil para aquellas compañías con múltiples instalaciones que están conectadas por medio de una red de área amplia (WAN). Como resultado, los usuarios podrán movilizarse libremente dentro de sus instalaciones y más allá y permanecer conectados a la red.

- **Servidor web para una administración más fácil.** Un usuario simplificará la administración de su red inalámbrica si selecciona un punto de acceso con un servidor web incorporado. Esto le permitirá acceder y definir parámetros de configuración, monitorear el rendimiento y hacer diagnósticos desde un navegador web.

- **Seguridad.** Si un usuario escoge una solución inalámbrica que ofrezca múltiples niveles de seguridad, incluyendo encriptación y autenticación de usuarios. Una solución segura es utilizar una encriptación de por lo menos 40 bits. Sin embargo, para su facilidad de uso y para una protección más fuerte, se debe seleccionar una solución superior que automáticamente genere una clave nueva de 128 bits para cada sesión de red inalámbrica, sin tener que ingresar la clave manualmente. Además, el usuario debe considerar un sistema que ofrezca autenticación del usuario, requiriendo que el personal presente una contraseña antes de acceder a la red.

- **Una aplicación que detecte localidades.** Una solución de redes inalámbricas deberá incluir una aplicación para la detección de instalaciones. Esta aplicación podrá ayudar al usuario a determinar la posición óptima de los Hubs inalámbricos y el número de Hubs que necesita para soportar a sus usuarios. Además, ayudará a implementar una solución inalámbrica en forma efectiva y eficiente.

- **Costo de propiedad reducido.** Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida pueden ser significativamente inferiores, ya que en ambientes dinámicos se requieren acciones y movimientos frecuentes, lo cual abarata los costos debido a que no hay instalaciones físicas.

- **Facilidad de configuración para el usuario.** La persona que se va a conectar a la red sólo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red está abierta no es necesario configurar nada, pues la tarjeta detecta la red automáticamente. [2]

2.3.4. FUNCIONAMIENTO DE LAS REDES INALÁMBRICAS

Para transformar la información de un punto a otro de la red sin necesidad de un medio físico, se utilizan ondas de radio, al hablar de ondas de radio nos referimos normalmente a ondas portadoras de radio sobre las que se transporta la información (trasladando la energía a un receptor remoto)

La transmisión de datos entre dos computadoras se realiza por medio de un proceso conocido como modulación de la portadora, el aparato transmisor agrega datos a una onda de radio (onda portadora) esta onda al llegar al receptor es analizada por este, el cual separa los datos útiles de los inútiles. [16]

La frecuencia de radio es la parte del espectro electromagnético donde se generan ondas electromagnéticas, mediante la aplicación de corriente alterna a una antena, si las ondas son transmitidas a distintas frecuencias de radio, varias ondas portadoras pueden existir en igual tiempo y espacio sin inferir entre si, siempre que posean una frecuencia distinta, para extraer los datos el receptor debe situarse en una determinada frecuencia (frecuencia portadora) e ignorar el resto.

En una configuración típica de LAN sin cables, los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado.

El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

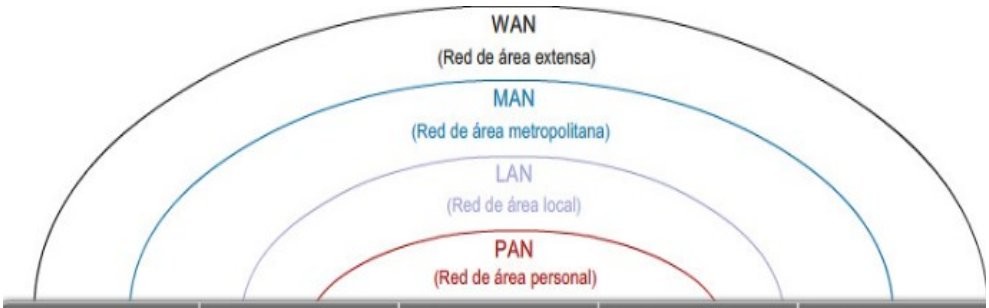
El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena.

La naturaleza de la conexión sin cable es transparente a la capa del cliente. [5]

2.4. CLASIFICACIÓN DE REDES INALÁMBRICAS

Las redes inalámbricas se pueden clasificar teniendo en cuenta como parámetro principal su rango de cobertura. El término inalámbrico hace referencia a la tecnología sin cables que permite conectar varias máquinas entre sí. Las redes inalámbricas se pueden clasificar teniendo en cuenta como parámetro principal su rango de cobertura.

En la figura 2.2 se muestra la clasificación de las principales tecnologías usadas en la actualidad.



	PAN	LAN	MAN	WAN
Estándares	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satélite
Velocidad	< 1 Mbps	de 11 a 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Intervalo	Cortocircuito	Medio	Medio-Largo	Largo
Aplicaciones	Punto a punto Dispositivo a dispositivo	Redes de empresas	Acceso de última milla	Datos móviles Dispositivos

Figura 2.2 – Clasificación de las tecnologías inalámbricas.

Fuente: CCNA 3 Cisco Networking Academy

2.4.1. RED DE ÁREA AMPLIA (WAN)

Es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías de teléfono.

Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

2.4.2. RED DE ÁREA METROPOLITANA (MAN)

Es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa. Esta red puede ser pública o privada, puede soportar tanto voz como datos, sobre medios de transmisión tales como fibra óptica y par trenzado. Utiliza medios de difusión al igual que las Redes de Área Local. Las redes de área metropolitana permiten alcanzar un diámetro en torno a los 50 km, dependiendo el alcance entre nodos de red del tipo de cable utilizado, así como de la tecnología empleada.

2.4.3. RED DE ÁREA LOCAL (LAN)

Una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización.

Nota: Para los propósitos administrativos, la red LAN grande se divide generalmente en segmentos lógicos más pequeños llamados los Workgroups. Un Workgroups es un grupo de las computadoras que comparten un sistema común de recursos dentro de una LAN.

2.4.4. RED DE ÁREA PERSONAL (PAN)

Wireless Personal Área Networks (Red Inalámbrica de Área Personal) es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a Internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella. [5]

2.5. TOPOLOGÍAS DE RED

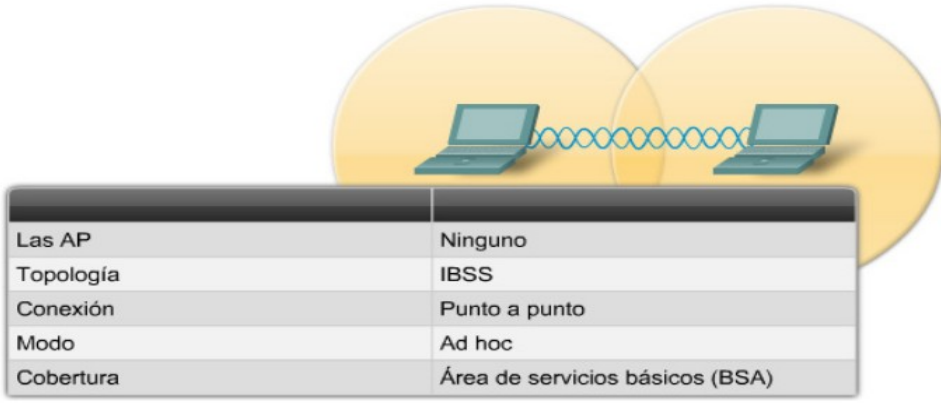
Las redes inalámbricas basadas en el estándar 802.11 pueden operar bajo tres topologías de red distintas: Topología Ad-Hoc, Topología de Infraestructura, Topología Roaming.

Dentro de cada una encontramos el Conjunto de Servicio Básico (BSS, siglas en inglés), que consiste de dos o más nodos, también llamados estaciones. Cada nodo o estación es una plataforma individual, como un AP o una tarjeta de usuario (tarjetas PCMCIA).

Un BSS cuenta con dispositivos que reconocen y trabajan en conjunto para minimizar la cantidad de colisiones que existen dentro del dominio del BSS.

2.5.1. LAS REDES AD-HOC

Es la configuración más sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas. En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red. La figura 2.3 nos muestra un ejemplo de una red Ad-Hoc.



Las AP	Ninguno
Topología	IBSS
Conexión	Punto a punto
Modo	Ad hoc
Cobertura	Área de servicios básicos (BSA)

Figura 2.3 - Topología de red Ad-Hoc.
Fuente: CCNA 3 Cisco Networking Academy

2.5.2. LAS REDES DE INFRAESTRUCTURA

Estas configuraciones utilizan el concepto de celda, ya utilizado en otras comunicaciones inalámbricas, como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva. A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión es posible combinar las celdas de estas señales para cubrir de forma casi total un área más extensa.

La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados "puntos de acceso", que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso.

Los puntos de acceso son colocados normalmente en alto, pero solo es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros. La figura 2.4 nos muestra un ejemplo de una red con topología de Infraestructura.

Las AP	Uno
Topología	BSS
Conexión	Cliente a AP
Modo	Infraestructura
Cobertura	Área de servicios básicos (BSA)

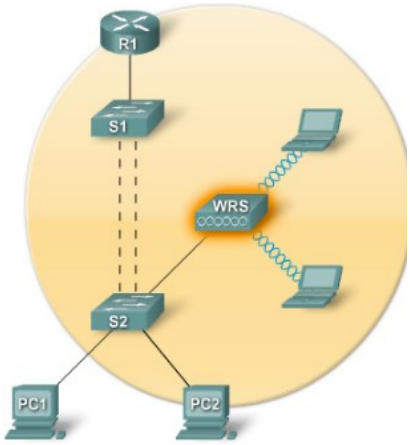


Figura 2.4 – Topología de red Infraestructura.

Fuente: CCNA 3 Cisco Networking Academy

2.5.3. LAS REDES ROAMING

Es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra. El concepto de roaming o itinerancia, utilizado en las redes inalámbricas, significa que el dispositivo Wi-Fi cliente puede desplazarse e ir registrándose en diferentes bases o puntos de acceso.

Este concepto se extiende para telefonía móvil, para que sea posible, tiene que haber una pequeña superposición (overlapping) en las coberturas de los puntos de acceso (Access Points), de tal manera que los usuarios puedan desplazarse por las instalaciones y siempre tengan cobertura.

Los puntos de acceso incorporan un algoritmo de decisión que decide cuando una estación debe desconectarse de un punto de acceso y conectarse a otro.

Esto es muy visto en campus universitarios con facultades distintas que tienen diferentes puntos de acceso y nombres, al caminar entre ellas se desconecta de

una pero se conecta a otra red. La figura 2.5 nos muestra un ejemplo de una red con topología Roaming. [5]

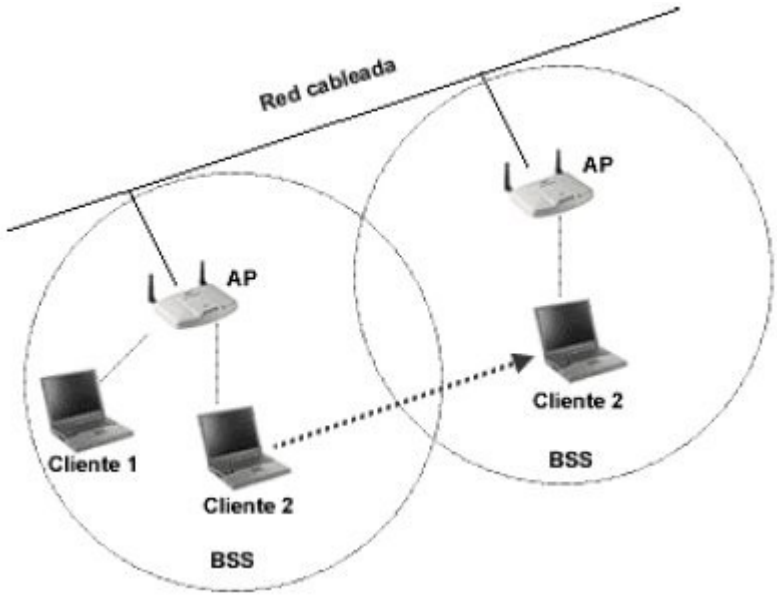


Figura 2.5 – Topología de red Roaming.
Fuente: CCNA Redes Cisco

2.6. TECNOLOGÍAS CSMA (ACCESO ALEATORIO AL MEDIO)

En informática, se entiende por Acceso Múltiple por Detección de Portadora (Carrier Sense Multiple Access) el escuchar el medio para saber si existe presencia de portadora en los momentos en los que se ocupa el canal. La finalidad es evitar colisiones, es decir que dos host hablen "al mismo tiempo". Por otro lado define el procedimiento que estos dos host deben seguir si llegasen a usar el mismo medio de forma simultánea.

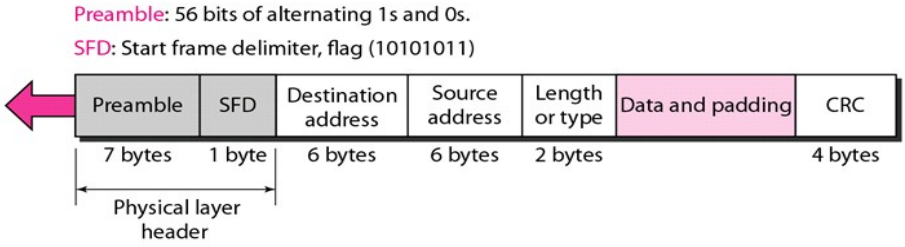
Distintos tipos de CSMA que podemos encontrar:

- CSMA/CD.
- CSMA/CA.

2.6.1. CSMA/CD

Siglas que corresponden a "Acceso Múltiple con escucha de Portadora y Detección de Colisiones", es una técnica usada en redes Ethernet para mejorar sus prestaciones. Anteriormente a esta técnica, se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones. Por eso apareció en primer lugar la técnica CSMA, que fue posteriormente mejorada con

la aparición de CSMA/CD. En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados o no. En la figura 2.6 se muestra la trama para la transmisión de datos usado por protocolo Ethernet.



2.6.2. CSMA/CA

En redes informáticas CSMA/CA "Acceso múltiple por detección de portadora con evasión de colisiones" es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente).

De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. CSMA/CA es utilizada en canales en los que por su naturaleza no se puede usar CSMA/CD. CSMA/CA se utiliza en 802.11 basada en redes inalámbricas.

Básicamente, este proceso se puede dividir en tres fases en las que el emisor puede:

- Escuchar para ver si la red está libre.
- Transmitir el dato.
- Esperar un reconocimiento por parte del receptor.

Este método asegura así que el mensaje se recibe correctamente. Sin embargo, debido a las dos transmisiones, la del mensaje original y la del

reconocimiento del receptor, pierde un poco de eficiencia. Este sistema incrementa el volumen de tráfico en el cable y reduce las prestaciones de la red, motivo por el que se usa poco. En redes inalámbricas, no se puede escuchar a la vez que se trasmite: no pueden detectarse colisiones. En la figura 2.7 se muestra la trama para transmisión en redes inalámbricas. [6]

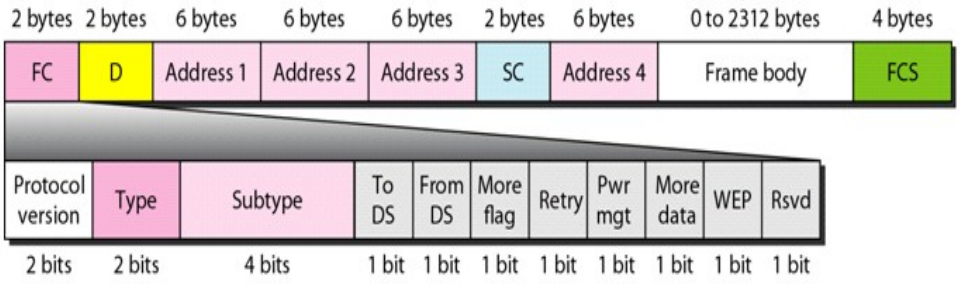


Figura 2.7 – Trama usado por Wireless IEEE 802.11.
Fuente: Textos Científicos Control de acceso al medio IEEE 802.3 CSMA/CA

2.7. MODULACIÓN PARA ESTÁNDARES IEEE 802.11

2.7.1. MODULACIÓN ESPECTRO ENSANCHADO

También llamado espectro esparcido, espectro disperso, spread spectrum o SS es una técnica por la cual la señal transmitida se ensancha a lo largo de una banda muy ancha de frecuencias, La tecnología de espectro ensanchado, utiliza todo el ancho de banda disponible, en lugar de utilizar una portadora para concentrar la energía a su alrededor.

Tiene muchas características que le hacen sobresalir sobre otras tecnologías de radiofrecuencias (como la de banda estrecha, que utiliza microondas), ya que, por ejemplo, posee excelentes propiedades en cuanto a inmunidad a interferencias y a sus posibilidades de encriptación. En la tabla 2.1 se muestra diferentes técnicas de modulación por cada estándar IEEE 802.11.

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

Tabla 2.1 – Diferentes técnicas de Modulación.
Fuente: Estándar IEEE 802.11

Tanto DSSS como FHSS están definidos por la IEEE en el estándar 802.11 para redes de área local inalámbricas WLAN.

2.7.1.1. MODULACIÓN DSSS

El espectro ensanchado por secuencia directa es una técnica de modulación que utiliza un código de pseudo ruido para modular directamente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral (es decir, el nivel de potencia en cualquier frecuencia dada). La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radiorreceptores les parecerá ruido, menos al que va dirigida la señal.

2.7.1.2. MODULACIÓN FHSS

El espectro ensanchado por salto de frecuencia (del inglés Frequency Hopping Spread Spectrum o FHSS) es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits. Una transmisión en espectro ensanchado ofrece 3 ventajas principales:

- Las señales en espectro ensanchado son altamente resistentes al ruido y a la interferencia.
- Las señales en espectro ensanchado son difíciles de interceptar. Una transmisión de este tipo suena como un ruido de corta duración, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor.
- Transmisiones en espectro ensanchado pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia.

2.7.1.3. MODULACIÓN OFDM

La Multiplexación por División de Frecuencias Ortogonales, (OFDM), también llamada modulación por multitono discreto, en inglés Discrete

Multitone Modulation (DMT), es una modulación que consiste en enviar un conjunto de portadoras de diferentes frecuencias donde cada una transporta información la cual es modulada en QAM o PSK.

Normalmente se realiza la modulación OFDM tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos en la transmisión, entonces esta modulación se denomina COFDM, del inglés Coded OFDM.

Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles de portadoras equi espaciadas que forman una modulación OFDM, los procesos de modulación y demodulación se realizan en tiempo discreto mediante la IDFT y la DFT respectivamente. [6]

Algunos sistemas donde es usado la modulación OFDM:

- El protocolo de enlace ADSL.
- El protocolo de red de área local IEEE 802.11a/g/n, también conocido como Wireless LAN.
- El sistema de transmisión inalámbrica de datos WiMAX.
- El sistema de transmisión de datos basados en PLC.

2.8. ESTÁNDARES DE RED INALÁMBRICA DE ÁREA LOCAL IEEE 802.11

El protocolo IEEE 802.11 es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación, todas las cuales utilizan los mismos protocolos.

El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11 legacy". En la tabla 2.2 se muestran estándares IEEE 802.11 y su descripción: [7]

Revisión	Título	Descripción
802.11	IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications	Estandar básico, define las capas MAC (control de acceso al medio) y PHY (capa física).
802.11b	Higher Speed Physical Layer (PHY) Extension in the 2,4 GHz band	WLAN, Wi-Fi.
802.11e	Medium Access Method (MAC) Quality of Service Enhancements	Mejora de la capa MAC actual para soportar Calidad de Servicio, con vistas a proporcionar aplicaciones como voz, audio o video.
802.11g	Further Higher Data Rate Extension in the 2,4 GHz Band	Nueva capa física como extension de 802.11b. Ya disponible comercialmente, alcanza 54 Mbit/s.
802.11i	Medium Access Method (MAC) Security Enhancements	Mejoras de los mecanismos de seguridad y autentificacion de la capa MAC 802.11.
802.11k	Radio Resource Measurement of Wireless LANs	Esta revisión definirá las interfaces para proporcionar medidas de gestión de recursos radio a las capas superiores.
802.11n	Enhancements for Higher Throughput	Mejoras de las capas PHY y MAC de 802.11 para alcanzar tasas de bit de más de 100 Mbit/s.

Tabla 2.2 – Estándares de IEEE 802.11.

Fuente: Estándar IEEE 802.11

2.8.1. IEEE 802.11a

El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 sub portador orthogonal frequency división multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede inter operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

2.8.2. IEEE 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s

sobre UDP.

Aunque también utiliza una técnica de ensanchado de espectro basada en DSSS en realidad la extensión 802.11b introduce CCK (Complementary Code Keying) para llegar a velocidades de 5,5 y 11 Mbps (tasa física de bit).

2.8.3. IEEE 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. que es la evolución del estándar 802.11b. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aproximadamente el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas. [6]

2.9. BANDAS ISM

ISM (Industrial, Scientific and Medical) son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (Wi-Fi) o WPAN (Bluetooth), cuando se usan estas bandas no se paga el espectro radioeléctrico a ningún ministerio, se sabe que el espectro radio eléctrico es un recurso natural de cada país y que si se usa se debe alquilar a este país. [6]

En el Perú la asignación de bandas se da en el documento llamado PNAF (PLAN NACIONAL DE ATRIBUCION DE FRECUENCIAS) con las bandas ISM, estas frecuencias son gratuitas. La figura 2.8 muestra las bandas de frecuencias que son asignadas para ISM de uso libre. [4]

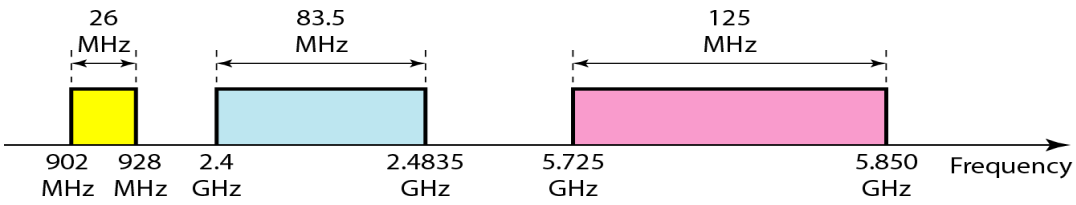


Figura 2.8 - Frecuencias usadas para ISM.

Fuente: PNAF Plan Nacional de Atribución de frecuencias

2.10. CAPA FÍSICA DE IEEE 802.11

La Capa Física de cualquier red define la modulación y la señalización característica de la transmisión de datos. IEEE 802.11 define tres posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa o DSSS (Direct Sequence Spread Spectrum),
- Espectro expandido por salto de frecuencias o FHSS (Frecuency Hopping Spread Spectrum) ambas en la banda de frecuencia 2.4 GHz ISM
- Luz infrarroja en banda base o sea sin modular.

En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación por un lado, y prestaciones y fiabilidad, por otro. No obstante, es previsible que, al cabo de un cierto tiempo, alguna de las opciones acabe obteniendo una clara preponderancia en el mercado. Entretanto, los usuarios se verán obligados a examinar de forma pormenorizada la capa física de cada producto hasta que sea el mercado el que actúe como árbitro final. [6]

2.11. CAPA DE ENLACE (MAC) DE IEEE 802.11

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas. Ya que deben de tenerse en cuenta las dos topologías de una red inalámbrica:

- Ad-hoc: redes peer-to-peer. Varios equipos forman una red de intercambio de información sin necesidad de elementos auxiliares. Este tipo de redes se utilizan en grupos de trabajo, reuniones, conferencias.
- Basadas en infraestructura: La red inalámbrica se crea como una extensión a la red existente basada en cable. Los elementos inalámbricos se conectan a la red cableada por medio de un punto de acceso o un PC Bridge, siendo estos los que controlan el tráfico entre las estaciones inalámbricas y las transmisiones entre la red inalámbrica y la red cableada.

Además de los dos tipos de topología diferentes se tiene que tener en cuenta:

- Perturbaciones ambientales (interferencias)
- Variaciones en la potencia de la señal
- Conexiones y desconexiones repentinas en la red
- Roaming: Nodos móviles que van pasando de celda en celda.

La capa de enlace de datos del estándar 802.11 se compone de dos subcapas: la capa de control de enlace lógico (LLC) y la capa de control de acceso al medio (MAC).En la figura 2.9 se muestra las subcapas de la capa de enlace de datos para el estándar IEEE 802.11. [6]

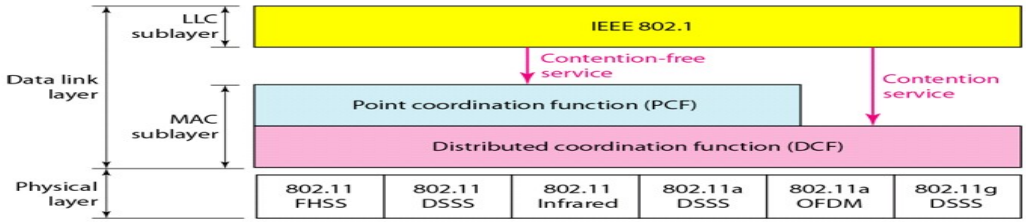


Figura 2.9 - Muestra las subcapas de la capa de enlace de datos.

Fuente: Redes inalámbricas 802.11 - Rogelio Montañana

2.12. DEFINICIÓN DE TAREAS 802.11

IEEE 802.11 es un grupo de trabajo perteneciente a IEEE que se encarga de estandarizar todo lo referente a redes inalámbricas. En 1997 802.11 se hizo realidad como estándar, definiendo dos tipos de transmisiones posibles. (Transmisión en la banda IR y Transmisión en RF). [14]

Destacar que todos los protocolos que se usan en 802.3 a partir de la capa MAC, es

decir, LLC, IP, TCP, UDP, BGP, OSPF, RIP, etc. son válidos para una red WLAN 802.11. Es decir, lo único que va a cambiar en una red inalámbrica frente a una cableada es la capa física y la capa MAC. De hecho este es el objetivo del grupo de trabajo 802.11, ya que se debe asegurar la inter operatividad de ambas redes.

El alcance de este proyecto incluye todos los estándares 802.11 para redes WLAN, dejando al margen los demás estándares. El grupo de trabajo 802.11 creó varios grupos de tareas para facilitar la labor de estandarización, así como un avance continuado. [8]

2.13. VELOCIDADES DE DATOS EN UNA RED INALÁMBRICA

Comúnmente se promociona una velocidad de datos máxima de 11Mbps, es importante notar que el estándar 802.11b soporta en realidad cuatro velocidades de datos: 1, 2, 5.5 y 11Mbps. Estas velocidades están disponibles en el mismo medio físico, específicamente, en una porción de 80MHz de amplitud del espectro de frecuencia de radio, iniciando en la frecuencia de 2.400 GHz que luego se divide en 11, 13 y 14 canales, dependiendo de la cantidad exacta del espectro asignado por las distintas agencias gubernamentales. En Ethernet, el medio físico permanece igual cuando las velocidades de datos aumentan o disminuyen, el mismo concepto se aplica para Wi-Fi, aumentar o disminuir el desempeño de la red inalámbrica no es una función de incrementar o disminuir el tamaño de la capa física o cambiar el ancho de banda, por el contrario, es una función del tipo de modulación que se utilice.
Las bases para las cuatro velocidades de datos que proporciona el estándar 802.11 b son tres técnicas de modulación distintas: [6]

- Modulación BPSK para proporcionar velocidades de hasta 1 Mbps.
- Modulación QPSK para proporcionar velocidades de hasta 2 Mbps.
- Modulación CCK para proporcionar velocidades de hasta 5.5 y 11 Mbps.

¿Porque si la mayor velocidad siempre es mejor, la industria y los estándares se preocupan por proporcionar soporte para cualquier otro tipo de modulación que no sea CCK? , la respuesta se resume en una palabra: rango.

Para entender mejor esto, podemos observar la figura 2.10 donde se aprecia como varía la velocidad y el rango dependiendo del tipo de modulación que se utiliza. [8]

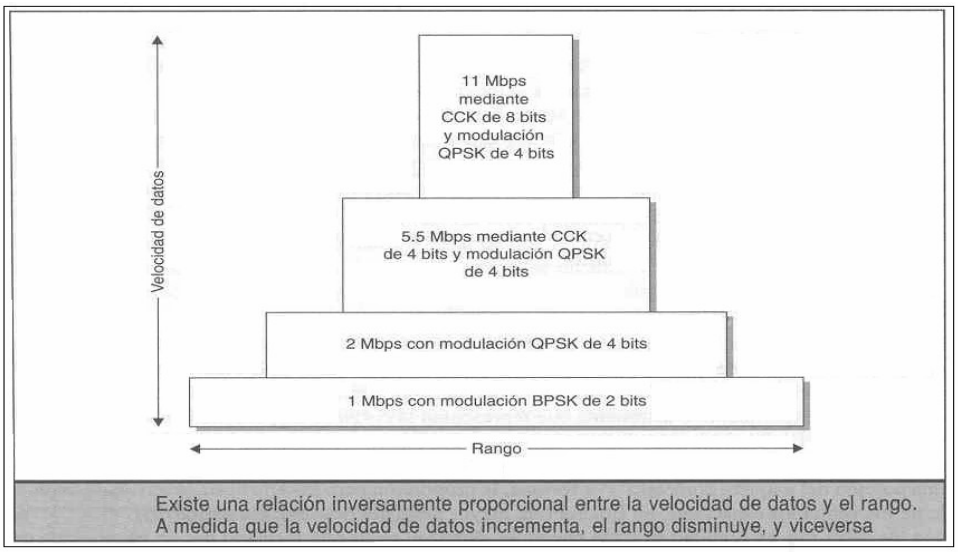


Figura 2.10 – Relación de velocidad de datos contra rango de alcance.

Fuente: Cisco CCNA

2.14. SEGURIDAD EN REDES INALÁMBRICAS

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad, la salida de estas señales fuera de los edificios donde está ubicada la red permite que un pirata informático sin poseer un equipo sofisticado, se introduzca en una red empresarial. Y una brecha de seguridad en una red es un grave problema para cualquier empresa. Una vez dentro, el pirata informático puede tener acceso a contraseñas, introducirse en los servidores y robar información, cambiar la página Web de la empresa o hacer que la red entera deje de funcionar.

¿Qué es lo que hace que las redes inalámbricas sean más vulnerables que las redes cableadas? La respuesta es sencilla: desconocimiento de las herramientas de seguridad disponibles para las redes inalámbricas. El término “seguridad inalámbrica” no tiene por qué ser una expresión contradictoria, de hecho son muchas las personas que piensan que es más difícil violar la seguridad en una red cableada que en una red inalámbrica. En el mercado podemos encontrar las herramientas de seguridad, funciones y protocolos para proporcionar una adecuada protección a las WLAN.

Las redes inalámbricas pueden tener un impacto positivo en una empresa cuando el resultado de implementarlas produce mejoras en la eficiencia organizacional, en la

toma de decisiones y en la productividad en general, pero pueden tener un impacto negativo cuando pone en riesgo no solo la seguridad de la WLAN, sino de toda la red (cableada e inalámbrica).

Las redes basadas en el estándar IEEE 802.11 presentan un crecimiento espectacular, ello incide en ver cada vez más necesaria la seguridad de este tipo de redes. IEEE, consciente de esta necesidad, aprobó en junio de 2001 el estándar IEEE 802.1X-2001 que especifica el control de acceso a la red basada en puertos el cual utiliza las características físicas de la infraestructura de las redes locales IEEE 8002.11 para facilitar una forma de autentificación y autorización de dispositivos conectados a un puerto de la red en modo punto a punto y de impedir el acceso a dicho puerto si falla el proceso de autenticación y autorización.

El objetivo del estándar es especificar un método general de provisión de control de acceso a la red basado en puertos. Entre su contenido cabe destacar que: describe un marco de referencia en el que se produce la autenticación, define los principios de funcionamiento de los mecanismos de control de acceso, los niveles de control de acceso y el comportamiento asociado a ellos (en cuanto a transmisión y recepción de tramas), los requisitos del protocolo entre Autenticador - Solicitante y entre Autenticador y Servidor de Autenticación.
También especifica los mecanismos y procedimientos que soportan control de acceso a la red por medio de protocolos de autorización y autenticación, la codificación de las unidades de datos del protocolo (PDU, siglas en inglés) utilizadas por dichos protocolos, establece los requisitos de gestión del control de acceso basado en puerto y el acceso remoto a las operaciones de administración de la red mediante el protocolo de administración de red simple (SNMP, siglas en inglés).

Explicaremos un escenario típico de autenticación 802.1x. Existen tres actores principales en la autenticación 802.1x: El Solicitante (Usuario), el Autenticador (AP), y el Servidor de Autenticación, en la figura 2.11, se pueden apreciar estos tres actores de acuerdo con una configuración básica de red.

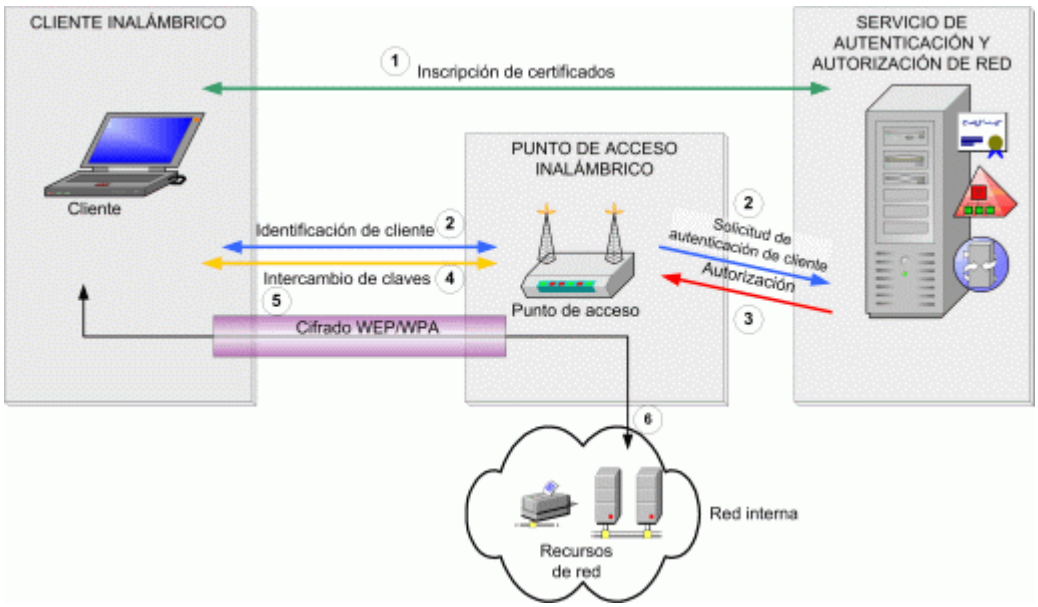


Figura 2.11 – Actores de la autenticación 802.1x.

Fuente: Seguridad en Redes Wireless

La comunicación comienza con un solicitante no autenticado que desea conectarse con un AP, el AP responde permitiendo al puerto pasar solamente paquetes del protocolo de Autenticación Extensible (EAP, siglas en inglés) desde el usuario hacia el servidor de autenticación situado en la red cableada, en ese momento pone al puerto en estado de "No Autorizado", el AP bloquea cualquier otro tipo de tráfico como paquetes del protocolo de transferencia de hipertexto (HTTP, siglas en inglés) o POP3.

El usuario envía un paquete EAP – inicio, el AP responde con EAP- solicitud de identidad para obtener la identificación del usuario, este contesta con su identidad y el AP envía este mensaje al servidor de autenticación, la autenticación se realiza de acuerdo con el algoritmo de autenticación seleccionado y el resultado es enviado al AP. Una vez autenticado el usuario, el AP abre el puerto del usuario para otro tipo de tráfico.

El estado del puerto pasa a "Autorizado". Para desconectar, el usuario enviará un mensaje EAP- desconexión, con lo que el AP pone el puerto en estado "No Autorizado" nuevamente. Este procedimiento puede apreciarse en la figura 2.12. [17]

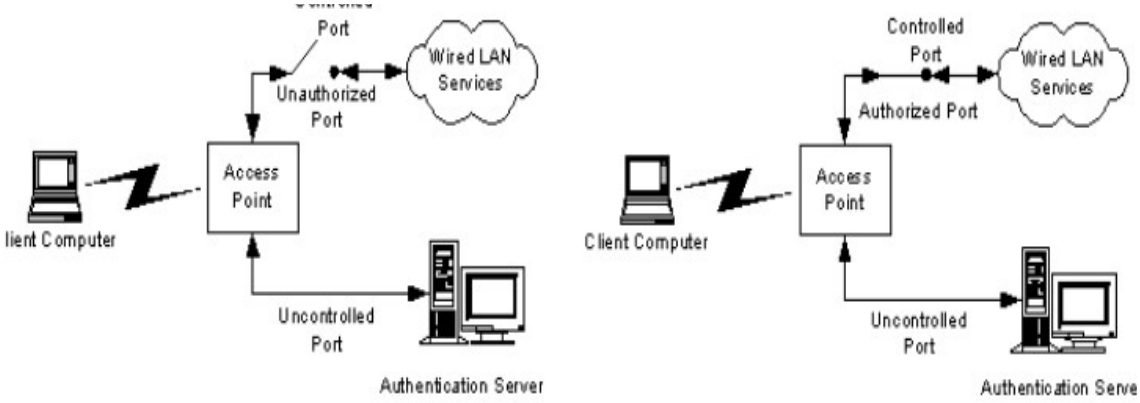


Figura 2.12 – Procedimiento de autenticación.

Fuente: Seguridad en Redes Inalámbricas Universitat de Valencia

A continuación se resumen las funciones de las entidades que intervienen:

- **Autenticador (AP):** Equipo en el extremo de un segmento punto a punto de una LAN que facilita la autentificación de la entidad conectada al otro extremo del enlace.
- **Servidor de Autenticación**: Equipo que facilita servicio de autenticación al autenticador. Puede estar situada junto al autentificador o remotamente en él se implementa el mecanismo de autentificación.
- **Puerto de Acceso a la Red (Puerto):** Es el punto de conexión de un sistema a una LAN. Puede ser un puerto físico MAC o un puerto lógico como una asociación IEEE 802.11 entre un AP y una estación inalámbrica.
- **Extensible Authentication Protocol (EAP):** Es el protocolo asociado con un puerto. Puede incluir la funcionalidad de autenticador, solicitante o ambas funcionalidades.
- **Solicitante (Usuario):** Es aquel en un extremo de un segmento LAN punto a punto que está siendo autenticado por un autenticador al otro extremo del enlace.

Como hemos visto, cuando se discuten los sistemas de seguridad, las dos áreas principales son: Autenticación y Cifrado, aunque están interrelacionadas, la veremos por separado ya que constituyen aspectos diferentes de una arquitectura general de seguridad.

La autenticación es el proceso en que se determina que un usuario es quien dice ser. Un ejemplo sencillo de este proceso es cuando una persona que llega a una oficina, primero muestra una tarjeta de identificación con su foto, luego mira a través de un visor que examina el patrón de su retina y por último tiene que teclear una secuencia

numérica para poder acceder al edificio. [17]

Los AP pueden configurarse de manera que usen contraseñas, conocidas como SSID, usualmente están compuestos por una sola palabra, y ya vienen predeterminados por el fabricante de los AP. Las herramientas administrativas, como por ejemplo NetStumbler, proporcionan la capacidad de registrar todos los SSID que se pueden recibir en el equipo del usuario y luego permitir que el usuario se asocie al AP seleccionado.

Algunos fabricantes proporcionan la capacidad de deshabilitar los SSID de los AP, por un lado esto resuelve un problema de seguridad, pero por el otro deshabilita la capacidad de que un usuario pueda encontrar la red adecuada con la cual puede conectarse. Un SSID debe considerarse más como un nombre que como una contraseña, debe actuar como un medio de identificación del AP o como la identificación de toda una WLAN.

La mayoría de los fabricantes proporcionan la capacidad de restringir el acceso a las redes basándose en la tabla de direcciones MAC, la programación de las direcciones MAC son los únicos identificadores numéricos que usan los fabricantes para los equipos de las redes. Mediante esta característica se puede introducir un rango de direcciones MAC dentro de los AP y solo permitir que los equipos que cuenten con esas direcciones accedan a la red. A pesar de que este método proporciona cierto nivel de seguridad presenta dos problemas importantes:

- Las direcciones MAC pueden ser falsificadas. Un pirata informático puede usar un analizador de protocolo inalámbrico para revisar el tráfico y encontrar una dirección valida, luego solo debe copiarla en un equipo de usuario y hacerse pasar por un usuario válido.
- Las bases de datos separadas crean problemas administrativos, cada tabla de direcciones que se ubica en AP individuales representan una base de datos separada. Algunos fabricantes proporcionan medios para aplicar las tablas de direcciones a lo largo de un grupo de AP, pero esta solución rompe la sincronización y crea problemas de actualización. [9]

2.15. MECANISMO DE SEGURIDAD

En las redes Wireless los datos circulan a través del aire, con lo que pueden ser fácilmente interceptados sin necesidad de estar en el interior de las instalaciones de la Institución. Esto provoca un riesgo en la transmisión de datos "sensibles" a través de una red Wireless. Para ello existen diferentes soluciones para evitar la interceptación de los datos. Todas ellas, de una manera o de otra, se basan en la encriptación de los datos que circulan por la red, de manera que aunque sean interceptados, no puedan ser descifrados, proporcionando además, de manera implícita, un control de acceso a la red.

También hay que tener en cuenta los protocolos y aplicaciones que se usan a la hora de transmitir datos. Muchas aplicaciones ya utilizan sus propios sistemas de cifrado, ya que están preparadas para que esos datos puedan circular por redes públicas sin problemas de seguridad. El caso más común es el del protocolo (Secure Sokets Layer) SSL utilizado en la Web. El protocolo SSL se encarga de cifrar los documentos que circulan a través de la conexión Web. El uso de este tipo de protocolos evita la posible interceptación del contenido de los datos que circulan a través de la red, independientemente del resto de medidas de seguridad que adoptemos.

- **WEP (Wired Equivalent Privacy):** Es una técnica de encriptación de datos, que se encarga de cifrar cada uno de los paquetes 802.11 antes de su transmisión, usando el algoritmo de cifrado RC4. Este algoritmo puede usar claves de 40 a 128 bits, aumentando la seguridad usando claves de mayor tamaño. WEP no provee mecanismos para el control de claves.
  Todos los cambios deben hacerse de forma manual en cada dispositivo wireless. Se ha demostrado que esta técnica tiene una serie de vulnerabilidades que permite que dicha clave pueda ser descubierta. Por esta razón actualmente se han diseñado nuevas técnicas (WPA, WPA2), que basadas en WEP, solucionan sus problemas de seguridad. WEP es una manera sencilla de evitar el acceso no controlado a nuestra red wireless, pero es inadecuada si se requieren unas mínimas medidas de seguridad.

- **WPA (Wi-Fi Protected Access):** Aparece para solucionar las limitaciones de la seguridad proporcionada por WEP, proporcionando una compatibilidad con los dispositivos existentes. WPA es un subconjunto de la especificación IEEE 802.11i, el estándar de la seguridad en la redes Wi-Fi, y aparece como una

medida intermedia hasta que el estándar 802.11i estuviera preparado (WPA aparece en Abril del 2003 y mientras que el estándar completo 802.11i fue ratificado en junio de 2004).

Las características principales son:

- Uso del protocolo Temporal Key Integrity Protocol (TKIP) para evitar la reutilización de claves (una de las vulnerabilidades de WEP).
- Testeo de la integridad de los paquetes enviados (Message Integrity Check o MIC) para evitar errores de transmisión o manipulado de datos.

Tiene dos versiones: La personal que controla el acceso usando una contraseña denominada Pre Shared Key (PSK), y la empresarial que provee un nivel de seguridad mayor, usando claves de sesión dinámicas y verificación de usuarios usando el protocolo 802.1X EAP. Al igual que su predecesor WEP utiliza el algoritmo de cifrado RC4 usando claves de 128 bits.

- **WPA2 (Wi-Fi Protected Access 2):** Se basa en su predecesor WPA, con las mismas características pero aumentando el nivel de seguridad, es la implementación completa de la especificación IEEE 802.11i. Una de las principales mejoras es el cambio del algoritmo de encriptado usado por WEP y WPA (RC4) por otro más avanzado, el Advanced Encryption Standard (AES). Como su predecesor el WPA tiene dos versiones: la personal que controla el acceso usando una contraseña denominada Pre Shared Key (PSK), y la empresarial que utiliza la verificación de usuarios usando el protocolo 802.1X EAP.
- **VPN (Virtual Private Network):** Es una extensión de una red privada que pasa a través de enlaces compartidos de redes públicas como Internet o una red wireless. Una VPN permite enviar datos entre dos puntos a través de una red compartida o pública de tal manera que emula una conexión punto a punto. Para emular un enlace privado los datos enviados estarán cifrados para evitar la lectura de los paquetes que puedan ser interceptados.

  La parte de la conexión en la que los datos circulan encapsulados es conocida como túnel. Para la creación de estos canales seguros se utilizan una serie de protocolos como el IPsec o SSL. En la figura 2.13 se muestra una conexión punto a punto de una VPN: [17]

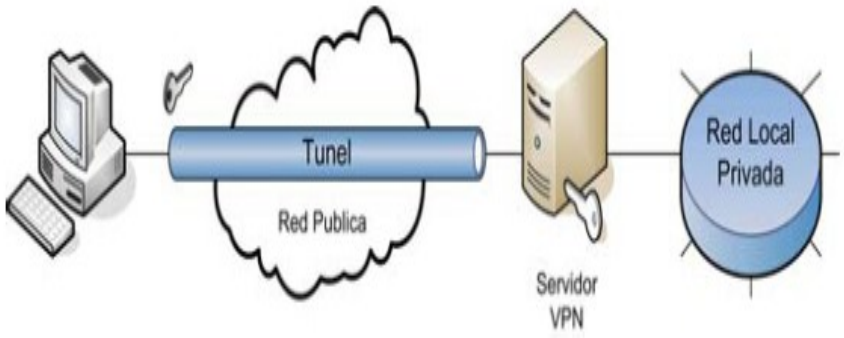


Figura 2.13 – Conexión punto a punto de una VPN.

Fuente: CCNA Cisco

Desde el punto de vista del usuario la conexión VPN es una conexión punto a punto con un servidor corporativo, de manera que la naturaleza de las redes por las que circulan los datos es irrelevante. El proceso que sigue el establecimiento de una conexión wireless a través de una VPN suele ser el siguiente:

- Al conectarse a la red wireless se obtiene automáticamente una dirección IP restringida. Con esta dirección no tenemos ningún tipo de acceso a la red local, sólo al servidor VPN.
- Conecta con el Servidor VPN y se realiza la autentificación con el nombre de usuario y contraseña.
- El servidor crea el canal de datos seguro y le asigna una IP "virtual" con acceso a la red local.

- **SEGURIDAD DE ACCESO.-** Con la seguridad de acceso se trata de controlar que dispositivos se conectan a nuestra red inalámbrica, de manera que evitemos posibles accesos externos no autorizados. Dependiendo del nivel de seguridad que necesitemos para nuestra red, podremos utilizar algunos de los diferentes métodos que explicaremos a continuación.

- **FILTRADO DE MAC.-** Cada tarjeta de red Wi-Fi tiene un identificador MAC

único asignado por el fabricante (al igual que las tarjetas de red Ethernet). Este identificador puede ser utilizado por parte de los puntos de acceso, para aceptar solo a un grupo de direcciones MAC e ignorar la señal del resto.
Esta técnica puede ser un poco engorrosa para grandes empresas, con un número importante de computadores, ya que tendrían que dar de alta, una por una, todas las direcciones MAC de los dispositivos wireless, pero es muy efectiva para un grupo reducido de ordenadores, ya que permite tener controlado en todo momento desde que dispositivos se accede a nuestra red inalámbrica.

Además tiene el inconveniente de que existen aplicaciones de dominio público que son capaces de cambiar la dirección MAC de los dispositivos de forma ágil y eficiente. De este modo, utilizando algún medio para obtener una dirección que tenga el acceso permitido será fácil obtener acceso a la red.

- **EAP (Extensible Authentication Protocol):** Es un protocolo de autenticación flexible, que es utilizado por el estándar IEEE 802.1X de control de acceso en las LAN's. El protocolo provee a las redes wireless de un entorno para elegir un método específico de autenticación. Existen diferentes variantes del EAP:
  - **EAP-MD5:** Es la versión menos segura del protocolo EAP, utiliza el nombre de usuario y contraseña para realizar la autenticación, usando la función hash MD5 de la contraseña para la verificación.
    - Al no comprobar la identidad del servidor es muy vulnerable a ataque del tipo Man-in-the-Middle.
  - **EAP-LEAP:** Es un sistema EAP propietario de Cisco. Al igual que la versión MD5, utiliza el nombre de usuario y contraseña para realizar la autenticación. Como servidor de autenticación utiliza un servidor RADIUS (explicado en apartados posteriores). Utiliza autenticación mutua pare evitar ataques Man-in-the-Middle como en el caso anterior.
  - **EAP-TLS:** Usa certificados X.509 tanto para el usuario como para el servidor para la autenticación mutua y el cifrado de las comunicaciones. Este sistema permite una autenticación con un nivel de seguridad muy alto, pero necesita la generación de certificados para todos los usuarios, lo cual puede ser un inconveniente para organizaciones pequeñas.

- **EAP-TTLS/PEAP:** En estas versiones se elimina la necesidad del certificado por parte del usuario necesario en el caso de la versión TTLS. La identidad del servidor se establece usando su certificado y la del usuario mediante un nombre de usuario y contraseña usando un servidor RADIUS.

- **RADIUS (Remote Authentication Dial-In User Service):** Es un sistema de autenticación y control de usuarios usado por muchos proveedores de acceso a Internet. Actualmente RADIUS forma parte de los mecanismos de seguridad del protocolo EAP (comentado anteriormente). El servidor RADIUS es el encargado de validar el acceso de los usuarios de forma centralizada usando nombres de usuario y contraseña.

  El cliente que desea conectarse a la red wireless utiliza alguna de las variantes para autentificarse. Dicha petición EAP llega al punto de acceso el cual se encargará de transmitir la petición al servidor RADIUS, el cual se encarga de validar al usuario, usando su nombre de usuario y contraseña o su certificado. El resultado de la validación es devuelto al cliente wireless, aceptando o denegando el acceso.

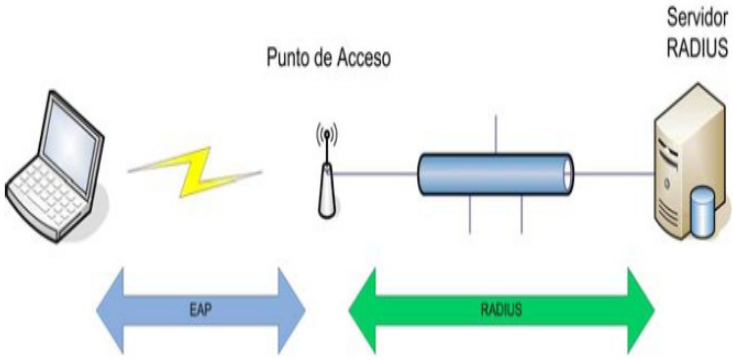


Figura 2.14 – Autenticación EAP con RADIUS.
Fuente: Autenticación EAP con servidor RADIUS Cisco

Algunos puntos de acceso permiten realizar filtrados de MAC usando servidores RADIUS, de manera que la MAC de la máquina que desea conectarse a la red wireless debe pasar por el servidor para ser validada.

- **KERBEROS:** Es un protocolo de seguridad desarrollado en el Instituto de Tecnología de Massachusetts (MIT), para autenticar usuarios y clientes en una red, y distribuir claves de encriptación, de forma segura. Permite que entidades

que se comunican a través de una red, puedan probar su identidad, evitando que puedan ser suplantadas.

También proporciona capacidades de integridad de datos (detección de modificaciones) y seguridad de datos (para evitar lecturas no autorizadas) usando sistemas criptográficos como DES. Kerberos funciona proporcionando a los participantes (usuarios o servicios) "tickets" digitales, que pueden usar para identificarse en la red y como clave criptográfica para hacer las comunicaciones de forma segura.

- **FIREWALLS:** Los firewall o cortafuegos son dispositivos hardware o software, que funcionan como barrera entre redes, permitiendo o denegando las transmisiones de una red a la otra en función de las características de las conexiones que se pretendan establecer y las políticas de seguridad establecidas.
En este tipo de dispositivos se puede configurar el tipo de máquinas que pueden entablar conexiones con las de la red a la cual protegen, el protocolo de comunicación que pueden utilizar para ello, etc. De forma recíproca se utilizan para limitar el acceso al exterior por parte de los equipos de la red a la que protegen. En ambos casos, se definen una serie de reglas que reflejan la política de seguridad de la red. En el caso de las redes wireless, los firewalls se establecen como barrera de separación entre los dispositivos wireless y el resto de la red cableada, para evitar accesos no autorizados a zonas comprometedoras de la red, como se muestra en la Figura 2.15.

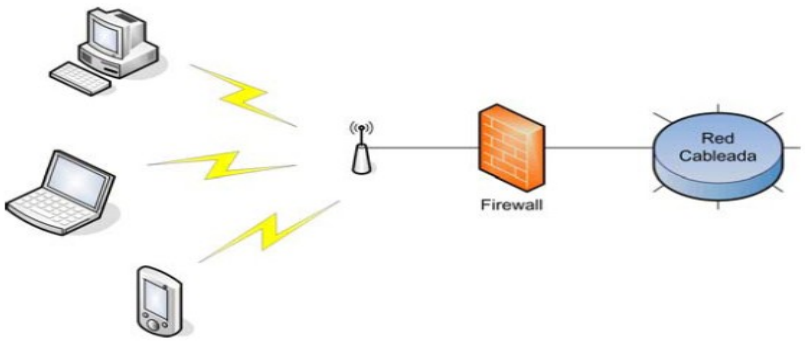


Figura 2.15 – Uso de Firewalls en una red Wireless.

Fuente: Comunicación y Ciencias digitales informática

Algunos puntos de acceso y gateways incorporan capacidades de firewall, permitiendo crear reglas básicas que pueden ser suficientes para un entorno de red sencillo. [9]

2.16. METODOLOGÍA DE ANÁLISIS, ARQUITECTURA Y DISEÑO DE REDES

Análisis, Arquitectura y Diseño de Redes de james D. McCabe es la tercera edición de un enfoque disciplinado en la arquitectura y diseño de redes, James McCabe aborda los elementos críticos necesarios para diseñar y desplegar redes en un entorno en constante cambio y complejo.

Día a día se presentan nuevos requerimientos para nuevas funciones y servicios, al mismo tiempo que aumenta la calidad de los servicios existentes y la seguridad de la red. Así mismo las fuerzas del mercado están presionando a los operadores de red para gestionar las nuevas infraestructuras y reducir los costos de operación y mantenimiento.

Desde la primera edición de esta tecnología el panorama ha cambiado radicalmente, los servicios convergentes, servicios VoIP y los nuevos despliegues del IPv6 están obligando a los arquitectos de red para volver a los fundamentos de las mejores prácticas de Ingeniería.

James D. McCabe ha desarrollado una metodología madura, repetible que cuando se sigue correctamente produce redes bien diseñadas y escalables, es una guía práctica basada en la riqueza de la experiencia de James. Los conceptos descritos se han demostrado con éxito en la implementación de numerosas redes de datos

Esta edición de la metodología ayuda a definir y comprender la arquitectura y diseño de la red. Analiza todo el sistema, los usuarios y sus aplicaciones, los dispositivos y las redes que los apoyan. Esta metodología está siendo aplicada en la formación en pre-grado y post-grado en ingeniería de redes, también es utilizada por los ingenieros de TI y de gestión en la implementación profesional de redes.

Está estructurado de manera que siguiendo la progresión lógica de análisis, desarrollo y validación de los requisitos permite tomar decisiones para el diseño de la red. El análisis, arquitectura y diseño de redes ayuda a identificar y aplicar los servicios de red y los niveles de rendimiento necesarios para satisfacer a los usuarios.

A través de estos procesos se puede entender los problemas y determinar los objetivos

de servicio y rendimiento necesarios para enfrentar los problemas de la red, la arquitectura y diseño de la red proporciona los servicios deseados y los niveles de rendimiento.

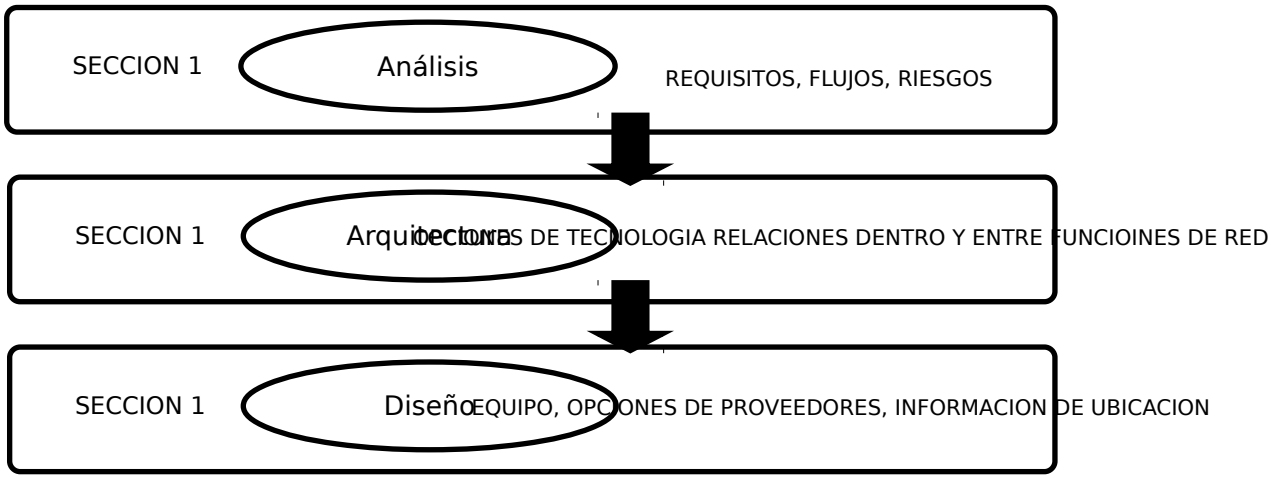


Tabla 2.3 – Flujo de información entre el análisis, arquitectura y diseño de redes.

Fuente: **análisis, arquitectura y diseño de redes, James Mccabe**

2.17. PFSENSE

PFSense es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Router. Se caracteriza por ser de código abierto, puede ser instalado en una gran variedad de computadores y además cuenta con una interfaz web sencilla para su configuración. El proyecto es sostenido comercialmente por BSD Perimeter LLC.

2.17.1. HISTORIA

El proyecto pfSense se inició en septiembre del 2004 por Chris Buechler Ullrich Scott como un fork de monowall, enfocado a las instalaciones en PC y Servidores (al contrario de monowall que se orientaba a ambientes embebidos y ordenadores de bajos recursos). Se calcula que para diciembre del 2010, PFSense contaba con más de un millón de descargas.

De acuerdo a su página oficial, se ha instalado exitosamente en distintos ambientes, que van desde redes domésticas hasta grandes corporaciones, universidades y otros tipos de organizaciones.

2.17.2. INSTALACIÓN Y USO

PFSense puede instalarse en cualquier ordenador o servidor que cuente con un mínimo de dos tarjetas de red, el proceso de instalación es similar a FreeBSD. Una vez copiados los archivos del sistema al disco duro se procede a configurar las direcciones IP de las tarjetas de red. Una vez concluido lo anterior, se puede

acceder al sistema desde un explorador web.

El portal de administración está basado en PHP y teóricamente todas las configuraciones y administración se pueden realizar desde allí, por lo tanto no es indispensable contar con conocimientos avanzados sobre la línea de comandos UNIX para su manejo.

2.17.3. CARACTERÍSTICAS

La siguiente lista muestra algunas funcionalidades que se incluyen por defecto en el sistema:

- Firewall
- State Table
- Network Address Translation (NAT)
- Balance de carga
- VPN que puede ser desarrollado en IPsec, OpenVPN y en PPTP
- Servidor PPPoE
- Servidor DNS
- Portal Cautivo
- Servidor DHCP

PFSense cuenta con un gestor de paquetes para ampliar sus funcionalidades, al elegir el paquete deseado el sistema automáticamente lo descarga e instala. Existen alrededor de setenta módulos disponibles entre los que se encuentran el proxy Squid, IMSpector, Snort, ClamAV, entre otros.

2.17.4. SOPORTE Y DESARROLLO

Al poseer software de código abierto la comunidad de desarrolladores y usuarios puede dar soporte y asistencia. BSD Perimeter ofrece soporte y capacitación a cambio de un costo.

Cualquier persona es libre de modificar el sistema a sus necesidades e incluso vender sus derivaciones de PFSense (bajo ciertas condiciones). Para el caso de los componentes para el núcleo, distribución y switch los precios son referenciales y variables según los proveedores donde se adquieran. Los servicios profesionales están considerados en horas hombres (HH), un costo para la elaboración del estudio y el detalle de la infraestructura a implementar y el otro costo para la supervisión durante la implementación con el fin que se supervise el cumplimiento de los estándares establecidos en el presente informe. [10]

CAPÍTULO III

DESCRIPCIÓN DE LA EMPRESA EN ESTUDIO "DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL"

3.1. ANTECEDENTES Y CREACIÓN

La Dirección de Titulación de Tierras y Catastro Rural es la unidad orgánica encargada de realizar el saneamiento físico legal de la propiedad agraria, mantener la información catastral rural actualizada, proporcionar la seguridad jurídica a los propietarios de predios rurales y generar las condiciones básicas para el desarrollo ágil y transparente del mercado de tierras de uso agrario, su acceso al crédito formal y por ende el incremento de inversiones privadas del agro. Mantiene relación de dependencia jerárquica y administrativa de la Dirección Regional de Agricultura. [11]

3.1.1. RESEÑA HISTÓRICA

Mediante la Octava Disposición Complementaria del Decreto Ley N° 25902, Ley Orgánica del Ministerio de Agricultura, del 27 de noviembre de 1992, se creó El Proyecto Especial Titulación de Tierras y Catastro Rural - PETT.

El PETT es una institución especializada del Ministerio de Agricultura, que asumió dentro de sus responsabilidades las funciones de la ex Dirección de Tenencia de Tierras y Estructura, el Programa Nacional de Catastro (PROCNAC) e integró el Proyecto Especial de Desarrollo Cooperativo y Comunal (PRODACC).

El PETT se creó como un proyecto dentro del marco de la reforma institucional del Sector Público Agrario, básicamente con el objeto de realizar las acciones necesarias para impulsar y perfeccionar la titulación y el registro de los predios rurales expropiados y adjudicados durante la vigencia de las normas contenidas en Texto Único Concordado del Decreto Ley N° 17716, complementarias y conexas; culminando los procedimientos de adjudicación y titulación que habían quedado inconclusos. Además de realizar la titulación de los predios de propiedad del Estado y lo que adjudique o transfiera con posterioridad a la vigencia del Decreto Legislativo N° 653.

La Constitución Política de 1993, sirvió de contexto a la dación de la Ley N° 26505, Ley de Inversión Privada en el desarrollo de las actividades económicas en las tierras del territorio nacional y de las Comunidades Campesinas y Nativas promulgada con fecha 17 de julio de 1995, conocida mayoritariamente como "Ley de Tierras". Esta ley marcó un giro radical en la normatividad que rigió la vida del agro nacional desde los años de la reforma agraria, fundamentalmente por la eliminación de las restricciones que lo limitaban. Su objetivo fue alentar la inversión privada en el sector agrario, eliminando las restricciones que impedían a los inversionistas orientarse a la agricultura. Fue modificada por las Leyes N° 26570, 26597, 26681.

Posteriormente, con fecha 15 de agosto de 1996, se expidió el Decreto Legislativo N° 838, mediante el cual se facultó al Ministerio de Agricultura para que adjudique en forma gratuita los predios rústicos de libre disponibilidad del Estado, en zonas de economía deprimida, a partir de los 2000 metros sobre el nivel del mar; su reglamento fue aprobado por Decreto Supremo N° 018-98-AG. Esta norma estuvo vigente hasta el 31 de diciembre de 2000, actualmente se

viene trabajando un proyecto de norma que regule el tratamiento legal de los predios rústicos en general.

En este entorno, y con el propósito de fortalecer y apoyar la culminación del proceso de Reforma Agraria - asignada al PETT mediante la titulación-, el 08 de mayo de 1996 el Estado Peruano suscribió el Contrato de Préstamo N° 906/OC-PERU con el Banco Interamericano de Desarrollo - BID, para la ejecución del Proyecto Titulación y Registro de Tierras - PTRT a cargo del Ministerio de Agricultura a través de la Unidad de Ejecución del Proyecto, con la participación del PETT, la SUNARP y el INRENA en calidad de organismos subejecutores. El PETT tenía a su cargo los componentes de Regularización Predial y Catastro; la SUNARP, el registro de los predios rurales y el Instituto Nacional de Recursos Naturales - INRENA, la administración y monitoreo de los recursos naturales.

Más adelante, a inicios de su etapa de implementación, el PTRT amplió sus objetivos hacia la generación de las condiciones para el desarrollo de un mercado de tierras rural, ágil y transparente, mediante el saneamiento físico-legal de la propiedad de todos los predios rurales, la modernización del catastro rural y el sistema único y automatizado de registro de la propiedad rural.

Mediante el decreto legislativo 1089, que establece el régimen temporal extraordinario de formalización y titulación de predios rurales, se declara de interés público nacional la formalización y titulación de predios rústicos y tierras eriazas habilitados en el ámbito nacional por un periodo de cuatro años a partir de junio del 2008. Se crea además el régimen temporal extraordinario de formalización y titulación de predios rústicos y eriazos habilitados, precisándose que las acciones de formalización serán iniciadas de oficio sobre las jurisdicciones que el Organismo de Formalización de la Propiedad Informal (COFOPRI) determine. Se precisa además que esta entidad generará, modernizará, consolidará, conservará y actualizará el catastro rural del país, creándose también el Tribunal Administrativo de la Propiedad del COFOPRI, siendo las oficinas zonales de esta entidad la primera instancia.

Asimismo, de acuerdo a lo establecido en la ley 27867, ley orgánica de gobiernos regionales, artículo 51, literal n), los gobiernos regionales serán los encargados de promover, gestionar y administrar el proceso de saneamiento

físicolegal de la propiedad agraria, con la participación de los actores involucrados, cautelando el carácter imprescriptible, inalienable e inembargable de las tierras de las comunidades campesinas y nativas. Mediante el decreto supremo 074-2007-PCM se prorroga el plazo para la transferencia a los gobiernos regionales de esta función específica y se modifica el decreto supremo 012-2007-VIVIENDA. El plazo se prorroga hasta el 31 de diciembre de 2008. Posteriormente, a través del régimen excepcional establecido por el decreto legislativo 1089, se establece que por el plazo de cuatro años, COFOPRI será quien realizará las labores de formalización, suspendiendo el proceso de transferencia de competencias hacia los gobiernos regionales. Se menciona, sin embargo, que dichas competencias podrán ser transferidas a los gobiernos regionales, inclusive dentro de ese régimen cuando estos lo soliciten, y que COFOPRI brindará asesoría técnica en materia de formalización rural a esos gobiernos, siempre que la pidan. Respecto de esta norma, es necesario precisar que se encuentra cuestionada por la población indígena y sus organizaciones de base, quienes solicitan su derogatoria.

Mediante decreto supremo 088-2008-PCM se prorrogó hasta el 30 de junio 2009, el plazo para la transferencia a los gobiernos regionales de la función prevista en el literal n) del artículo 51 de la ley orgánica de gobiernos regionales. Asimismo, se precisó que COFOPRI era la institución responsable de la transferencia a los gobiernos regionales de dicha función.

Posteriormente, mediante resolución de Secretaria de Descentralización 006-2009-PCM-SD se conforma la comisión intergubernamental para coordinar y ejecutar las acciones derivadas del procedimiento establecido para la transferencia a los gobiernos regionales de la función prevista en el literal n) del artículo 51 de la ley orgánica de los gobiernos regionales, en el marco del decreto supremo 088-2008-PCM.

Los ministerios de Agricultura y de Vivienda, Construcción y Saneamiento determinarán los alcances y condiciones pertinentes para el ejercicio compartido con los gobiernos regionales de la función establecida en el literal n) del artículo 51 de la ley orgánica de gobiernos regionales. Por ello, deberán establecerse los mecanismos de articulación con los gobiernos regionales en el marco del proceso de transferencia que sean los más convenientes, para concluir dicho

proceso dentro del plazo establecido por el decreto supremo 088-2008-PCM. En función de ello, la Secretaría de Descentralización aprobó lo siguiente:

a. Resolución de secretaria de descentralización 017-2009-PCM-SD, acreditan a los gobiernos regionales de Ayacucho, Ica, Madre de Dios, Moquegua, Cajamarca, Ucayali, Pasco, La Libertad, Apurímac y Huancavelica.

b. Resolución de secretaria de descentralización 028-2009-PCM-SD, acreditan a gobiernos regionales de Piura, Ancash, Callao, Cusco, Puno, Tumbes, Tacna, Junín, Amazonas y Lima para transferencia de función n) del artículo 51 de la ley orgánica de gobiernos regionales.

c. Resolución de secretaria de descentralización 031-2009-PCM-SD, acreditan a COFOPRI y los gobiernos regionales de Arequipa, Lambayeque y Loreto para la transferencia de la función n), artículo 51 de la ley orgánica de gobiernos regionales, en materia agraria.

d. Resolución de secretaria de descentralización 038-2009-PCM-SD, acreditan a los gobiernos regionales de Huánuco y San Martín para la transferencia de función n), artículo 51 de la ley orgánica de gobiernos regionales en materia agraria.

Asimismo, mediante decreto supremo 056-2010-PCM se transfieren a favor de los gobiernos regionales la función de formalización y titulación de predios rústicos de tierras eriazas habilitadas al 31 de diciembre de 2004, así como la reversión de predios rústicos adjudicados a título oneroso por el Estado ocupados por asentamientos humanos.

Resulta de suma importancia realizar las transferencias a los gobiernos regionales, a fin de que estos apliquen de manera eficiente herramientas de gestión, tales como la zonificación ecológica económica, en sus procesos de ordenamiento territorial. [12]

3.2. ÁMBITO DE RESPONSABILIDAD

La DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL, se desarrolla geográficamente en el departamento de Junín, el cual se ubica en la zona central del país. La Institución tiene domicilio legal en la Calle Real N° 507 El Tambo - Huancayo. La Institución es la encargada de realizar el saneamiento físico legal de la

propiedad agraria, mantener la información catastral rural actualizada, proporcionar la seguridad jurídica a los propietarios de predios rurales y generar las condiciones básicas para el desarrollo ágil y transparente del mercado de tierras de uso agrario, su acceso al crédito formal y por ende el incremento de inversiones privadas del agro. [11]

3.3. PERSPECTIVAS DE DESARROLLO

MISIÓN

Formalizar de manera definitiva la propiedad de la tierra de uso agrario, levantando un catastro moderno y formando expedientes de saneamiento legal, que permitan registrar la propiedad de los predios rurales, individuales, comunales y eriazos en desarrollo, dando seguridad jurídica a sus propietarios y propiciando el desarrollo de un mercado de la tierra ágil y transparente.

VISIÓN

La Dirección de Titulación de Tierras y Catastro Rural (DTT) tiene como visión ser una institución con tecnología de avanzada, eficiente y de prestigio, que consolide la formalización de la propiedad rural a nivel nacional.

OBJETIVOS

La DTT tiene como objetivo estratégico propiciar la seguridad jurídica de los propietarios de predios rurales, y generar las condiciones básicas para el desarrollo del mercado de tierras de uso agrario, el incremento de la inversión privada en el agro y su acceso al crédito formal

Son objetivos específicos de la DTT, los siguientes:

a) Efectuar el saneamiento físico – legal de predios individuales, tanto de la titulación de todos los predios resultantes de la Ley de Reforma Agraria, como de la regularización en forma definitiva de la propiedad y posesión de los predios individuales del área no reformada y de los que provengan de la individualización de las ex – cooperativas parceladas.

b) Elaborar, actualizar y promocionar la información cartográfica y catastral – Formación del Catastro Rural – de los predios rurales existentes en el país,

estableciendo su ubicación, extensión y propiedad a fin que los propietarios y posesionarios legítimos obtengan su título de propiedad debidamente saneados e inscritos en los Registros Públicos.

c) Efectuar el saneamiento físico – legal del territorio de todas las Comunidades Campesinas y Nativas del país.

d) Efectuar el saneamiento físico – legal de las tierras eriazas otorgadas mediante el procedimiento de denuncio, contrato de otorgamiento e identificación de tierras de libre disponibilidad del Estado a fin de integrarlas a la explotación agrícola e ingresarlas al mercado de tierras. [11]

FUNCIONES

- ✓ Planear, proponer, organizar, integrar, coordinar y controlar la política, planes, programas, proyectos y actividades en materia del proceso de saneamiento físico – legal de la propiedad agraria, territorio de las comunidades campesinas y nativas y adjudicación de tierras eriazas con aptitud agropecuaria, según corresponda.
- ✓ Establecer y proponer lineamientos, procedimientos, especificaciones, sistemas y políticas que deberían sujetarse las operaciones y funciones en actualización catastral, que sirva de base, modelo y/o aplicación para futuros planes de actualización en el ámbito de acción de otros entes.
- ✓ Formular, ejecutar y evaluar el Plan Anual.
- ✓ Levantar, conservar y actualizar el catastro rural de las tierras de uso agrario de la región.
- ✓ Evaluar y opinar sobre acciones de formalización de la propiedad de todos los predios del territorio de comunidades campesinas y nativas y de tierras eriazas con aptitud agropecuaria de libre disponibilidad del Estado.
- ✓ Elaborar una base cartográfica catastral precisa y actualizada bajo un sistema de representación que asegure una correcta ubicación geográfica y condición jurídica de los predios.
- ✓ Coordinar con las instituciones públicas y privadas para obtener la información necesaria para la formación y conservación del sistema de información geo referencial.

- ✓ Conservar y actualizar los registros catastrales mediante el uso de modelos y dar cumplimiento a directivas establecidas por la Dirección Nacional de Catastro.
- ✓ Procesar, editar y divulgar la información territorial de interés público, manteniendo la red institucional que permita la actualización de la base de datos y habilitar un sitio Web que facilite la postulación a integrarse al catastro nacional a través de Internet.
- ✓ Brindar capacitación, asesoría, información, apoyo técnico y servicios óptimos en materia catastral.
- ✓ Otras que se le asigne y corresponda.[11]

3.1. ORGANIGRAMA ESTRUCTURAL DE LA DIRECCION DE TITULACION DE TIERRAS Y CATASTRO RURAL

ORGANIGRAMA ESTRUCTURAL DE DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL

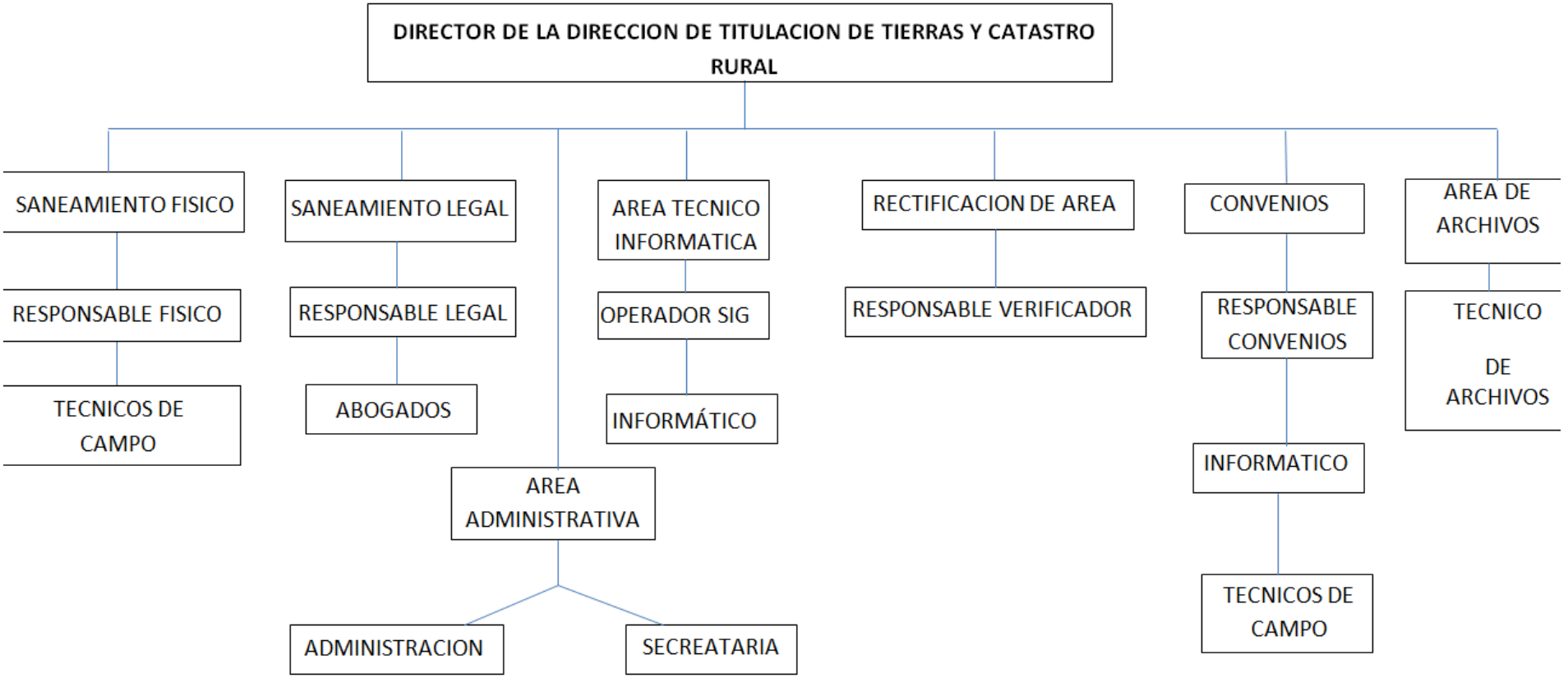


Figura 3.1 – Organigrama Estructural de la Dirección de Titulación de Tierras y Catastro Rural
Elaboración propia fuente: Dirección Regional de Agricultura Junín

3.5 ORGANIZACIÓN Y FUNCIONES

La estructura organizacional de la Dirección de Titulación de Tierras y Catastro Rural y las funciones ejercidas por esta son las siguientes:

3.5.1 ESTRUCTURA ORGANICA Y FUNCIONES

Se detalla la Estructura Orgánica de la DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL.

A. DIRECTOR

- ✓ Proponer a la Alta Dirección de la Dirección Regional de Agricultura las políticas, planes, programas, mecanismos y reformas institucionales, legales, presupuesto, cuadro de asignación de personal, reglamento de organización y funciones.
- ✓ Proponer a la Alta Dirección de la Dirección Regional de Agricultura la designación de los funcionarios responsables de los órganos de control, apoyo, línea, y asesores.
- ✓ Representar legalmente a la Dirección de Titulación de Tierras y Catastro Rural (DTT)
- ✓ Ejercer la titularidad de la Unidad Ejecutora DTT.
- ✓ Aprobar el Manual de Organización y Funciones MOF de DTT.
- ✓ Aprobar y resolver la contratación de funcionarios y personal necesario para el cumplimiento de los objetivos de DTT.
- ✓ Programar, dirigir, coordinar, supervisar y evaluar las acciones y actividades Técnicas, administrativas y de gestión de DTT.
- ✓ Aprobar y supervisar la ejecución de los Planes Operativos, Presupuestos, Memorias, Balances y Estados Financieros de DTT.
- ✓ Informar al Director de la Dirección Regional de Agricultura sobre el avance de Las actividades y cumplimiento de metas y recomendar a los órganos de DTT las medidas que resulten necesarias para su mejor desarrollo.
- ✓ Solicitar a las Unidades Orgánicas de DTT, los informes que sean necesarios para el cumplimiento de sus funciones.
- ✓ Emitir Resoluciones Directorales Ejecutivas dentro de su competencia y de acuerdo a las disposiciones legales vigentes;

- ✓ Ejecutar las políticas y estrategias diseñadas para la formalización de la propiedad rural y el levantamiento del catastro rural a nivel nacional, reportando su cumplimiento al Presidente Regional.
- ✓ Suscribir convenios y acuerdos de cooperación técnica y financiera que se requieran para el cumplimiento de los fines institucionales con instituciones nacionales y extranjeras;
- ✓ Disponer las acciones necesarias para la conservación del acervo documentario, control de títulos y contratos emitidos, etc.;

B. SANEAMIENTO FÍSICO Y LEGAL

RESPONSABLE FÍSICO Y LEGAL

- ✓ Formular y proponer a la Dirección las normas técnico legales, directivas y recomendaciones técnico legales relativas a la titulación de tierras y saneamiento legal de los predios rurales, tierras eriazas, comunidades campesinas y nativas.
- ✓ Planificar, organizar, conducir y evaluar a nivel regional el proceso de titulación y saneamiento legal de predios rurales, así como de las tierras eriazas con aptitud agropecuaria de libre disponibilidad del Estado.
- ✓ Planificar, organizar, conducir y evaluar el proceso de deslinde y titulación de las Comunidades Campesinas, así como de demarcación y titulación de las Comunidades Nativas y su posterior inscripción registral.
- ✓ Asesorar a la Dirección y a las demás unidades Orgánicas de la DTT en los asuntos relativos a su competencia.
- ✓ Efectuar el seguimiento y hacer cumplir la normatividad en el proceso de titulación de adjudicatarios, propietarios y posesionarios que se lleva a cabo simultáneamente con la formación del nuevo catastro.
- ✓ Asesorar, apoyar y supervisar a las Oficinas DTT de Ejecución Regional en la aplicación de las normas técnicas y legales, así como en la ejecución de las acciones de titulación y saneamiento legal de predios rurales, tierras eriazas con aptitud agropecuaria de libre disponibilidad del Estado y de las comunidades campesinas y nativas en los lugares donde la DTT haya asumido competencia.
- ✓ Absolver las consultas técnico legales, emitir opinión especializada y elaborar proyectos de Resolución en los asuntos de su competencia.
- ✓ Organizar y conducir el Archivo Técnico del proceso de titulación de tierras.
- ✓ Llevar a cabo la verificación, clasificación, organización, registro, control, seguimiento y archivo de los títulos, contratos y otros documentos que acreditan

la propiedad de predios rurales, así como de los expedientes remitidos para su custodia.

- ✓ Llevar el control de los formatos de títulos en blanco y anulados en coordinación con la Oficina de Administración.
- ✓ Emitir informes técnico-legales y proyectos de resolución, relacionados a los denuncios de tierras eriazas.
- ✓ Identificar los terrenos eriazos con aptitud agropecuaria de libre disponibilidad del Estado.
- ✓ Supervisar y evaluar los expedientes de tierras eriazas y contratos de adjudicación otorgados con fines de irrigación y/o drenaje y otros usos agrícolas por las Oficinas DTT de Ejecución Regional.
- ✓ Hacer de conocimiento de la Dirección Ejecutiva las tierras eriazas determinadas como de libre disponibilidad del Estado, que serán puestas a disposición de la Comisión de Promoción de la Inversión Privada - COFOPRI para su transferencia al sector privado mediante subasta pública.
- ✓ Mantener actualizados, los registros o padrones relativos a la titulación y saneamiento físico legal de los predios rurales, así como de las tierras eriazas, en coordinación con la Dirección de Catastro Rural.
- ✓ Mantener actualizado el Directorio de Comunidades Campesinas y Nativas, tituladas e inscritas.

C. OFICINA DE INFORMÁTICA

- ✓ Planificar, organizar, desarrollar, controlar y evaluar los procesos de automatización del sistema de información de la Institución.
- ✓ Implantar un sistema de información integrado, cuyas características sean compatibles con el grado de complejidad o tamaño de la institución, que permita disponer la información en forma rápida y confiable.
- ✓ Entender y dar solución a los problemas relacionados a la automatización e implantación de los sistemas automatizados, equipos y software en general, con eficiencia y calidad.
- ✓ Asesorar a la Dirección y unidades orgánicas en la aplicación y operación de los sistemas automatizados y el uso adecuado del software y equipos de cómputo de la institución.
- ✓ Elaborar proyectos para el diseño, programación e implantación de nuevos sistemas de información, aplicando metodología y técnicas de última generación.
- ✓ Programar y desarrollar el mantenimiento de los sistemas de información, equipos, dispositivos auxiliares y de la red de información.

- ✓ Distribuir en forma racional y equitativa los equipos de cómputo, el software de aplicación y dispositivos auxiliares a las unidades orgánicas.
- ✓ Programar, coordinar y desarrollar los eventos de capacitación en materia de informática, computación, manejo de GPS, telemática e internet.
- ✓ Formular normas internas para el uso adecuado de la base de datos de los sistemas automatizados, para el almacenamiento, resguardo y confidencialidad de los datos y programas implantados, como también de uso racional y adecuado de los equipos de cómputo.
- ✓ Efectuar periódicamente el control de calidad de los sistemas automatizados en funcionamiento.

D. OFICINA DE ATENCIÓN AL USUARIO

- ✓ Orientar sobre los requisitos, procedimientos a seguir para conseguir los servicios y/o otras demandas solicitadas por los usuarios.
- ✓ Atender de manera eficiente las demandas y consultas de los usuarios respecto a los servicios que brinda la institución.
- ✓ Canalizar y solucionar la demanda de los usuarios de manera eficiente, satisfactoria y oportuna.

E. AREA DE ADMINISTRACIÓN

OFICINA DE LOGÍSTICA

- ✓ Proporcionar a las unidades orgánicas de la institución los materiales, bienes, servicios e insumos necesarios para el cumplimiento de sus metas y objetivos.
- ✓ Programar y adquirir los bienes y contratar los servicios aprobados en el Plan Anual de Adquisiciones y Contrataciones de Bienes y Servicios.
- ✓ Almacenar adecuadamente los bienes adquiridos hasta su distribución a las dependencias de la institución para su uso racional y equitativo.
- ✓ Brindar los servicios de transporte, mantenimiento preventivo y correctivo de los equipos, maquinarias, herramientas y unidades móviles de la institución.

F. OFICINA DE SECRETARÍA

- ✓ Planificar, organizar, ejecutar y evaluar las actividades del trámite documentario, difusión y archivo general de la Institución.
- ✓ Organizar y programar la agenda de sesión de Dirección, así como registrar, comunicar sobre los acuerdos tomados en sesión.
- ✓ Mantener al día el Acta de Sesiones de Dirección.
- ✓ Desarrollar con eficiencia, oportunidad y calidad el trámite documentario de la Institución.

3.6 OFICINA GENERAL DE INFORMÁTICA Y COMPUTACIÓN

La oficina General de Informática y Computación, es el Órgano de Apoyo, encargada de automatizar los sistemas de información susceptibles de ello, del mantenimiento de los sistemas automatizados, de la operación de los sistemas implantados y la administración del Sistema de Información Geo referencial.

La Oficina de Informática y Computación está a cargo de un jefe de área, quien depende jerárquicamente del Director de la DTT.

3.7 PERSPECTIVAS DE DESARROLLO

OBJETIVOS

- ✓ Mantener todos los equipos de cómputo en estado óptimo de utilización.
- ✓ Sistematizar los procesos de las secciones de los diferentes Sistemas con los que cuenta la institución.

FUNCIONES

- ✓ Mejorar la seguridad informática de las oficinas a fin de contrarrestar los riesgos de robo, asalto u otros.
- ✓ Proporcionar mayor seguridad a los archivos de carácter institucional.
- ✓ Lograr un eficiente uso de los Sistemas Informáticos.
- ✓ Mantener actualizado la documentación de la Oficina
- ✓ Mejorar la red local de datos
- ✓ Mantener la Seguridad de los datos.
- ✓ Repotenciar el parque informático de impresoras y computadoras de última tecnología.
- ✓ Garantizar el mantenimiento de los equipos de cómputo y de los servidores.

ANÁLISIS FODA

FORTALEZAS

- ✓ Personal con conocimiento y experiencia en temas informáticos y de soporte técnico.
- ✓ Responsabilidad en el manejo de información.
- ✓ Deseo e iniciativa del personal informático en actualizarse en las nuevas tecnologías informáticas.
- ✓ Personal plenamente identificado con la Institución.

- ✓ Infraestructura tecnológica moderna propia.
- ✓ Proyección de una imagen positiva y eficiente a nivel institucional.
- ✓ Acceso a información referente a recursos informáticos de última generación.
- ✓ Personal responsable en la utilización y manejo de materiales a su cargo.

DEBILIDADES

- ✓ Escasos convenios y programas de capacitación al personal de esta oficina.
- ✓ Ambientes reducidos y mal ubicados para la realización de las actividades.
- ✓ Falta de recursos económicos para disponer de una infraestructura informática acorde a las necesidades.
- ✓ Cultura organizacional de la Institución orientada a las funciones que constituye obstáculo en la innovación de procesos a través de la aplicación de tecnologías y comunicaciones.
- ✓ Sistema no acorde con nuevas herramientas de seguridad informática.

OPORTUNIDADES

- ✓ El avance Tecnológico proporciona un abanico de posibilidades que pueden ser aplicadas en los procesos sistemáticos
- ✓ Disponibilidad de encontrar en el mercado tecnologías de punta
- ✓ Interés creciente por parte de los trabajadores a asistir a cursos informáticos.
- ✓ Existencia de centros de especialización informática
- ✓ Creciente demanda por servicios informáticos relacionados a consultas masivas.

AMENAZAS

- ✓ Situación económica del País, que se expresa en el escaso presupuesto para la adquisición de equipos de cómputo y Licencias de software.
- ✓ Exigencia de los usuarios de una atención oportuna y segura.
- ✓ Constantes amenazas de virus en la red.
- ✓ Falta de confidencialidad con respecto a las claves de acceso, por parte del personal que labora con los sistemas de información
- ✓ Rechazo por parte de los trabajadores a utilizar sistemas de información desconocidos.
- ✓ Fallas constantes de los equipos, ya sea por su antigüedad u obsolescencia.
- ✓ Elevados costos de hardware y software
- ✓ Creciente demanda por servicios informáticos relacionados a consultas masivas.
- ✓ Retraso en la entrega de insumos y repuestos necesarios para las actividades.

3.8 ORGANIGRAMA DE LA OFICINA DE INFORMÁTICA Y

COMPUTACIÓN

Figura 3.2 – Organigrama de la Oficina de Informática
Elaboración propia Fuente: Dirección Regional de Agricultura Junín

3.9 ORGANIZACIÓN, OBJETIVOS, FUNCIONES

La estructura organizacional, los objetivos, sus funciones y los recursos humanos de la Oficina de Informática y Computación son las siguientes:

- **UNIDAD DE DESARROLLO DE SISTEMAS**

OBJETIVOS

- ✓ Desarrollar sistemas computacionales con el objeto de simplificar el manejo de información en los procesos administrativos y mantener en óptimas condiciones el funcionamiento del equipo de cómputo, así como la red local de las oficinas.

FUNCIONES

- ✓ Desarrollar sistemas informáticos, de acuerdo a las necesidades de las Unidades Administrativas de la institución.
- ✓ Organizar y realizar el mantenimiento preventivo y correctivo de los sistemas informáticos y del equipo de cómputo.
- ✓ Realizar el análisis técnico sobre nueva tecnología en hardware y software aplicable a las necesidades de la institución.
- ✓ Proponer proyectos de actualización del hardware y software de la institución e identificar en el mercado los avances de las tecnologías de la información.
- ✓ Administrar el uso de las licencias de software utilizadas en la institución.

- ✓ Asegurar el adecuado almacenamiento de la Información histórica registrada, y procesada por la institución en medios ópticos y electrónicos.

➢ UNIDAD DE SOPORTE TÉCNICO Y MANTENIMIENTO

OBJETIVOS

- ✓ Instalar, mantener en funcionamiento y actualizar el hardware y software, proporcionar mantenimiento preventivo y correctivo de emergencia a los equipos de cómputo de la institución; evaluar y controlar los servicios de mantenimiento que ofrezcan los proveedores como garantía de servicio.

FUNCIONES

- ✓ Instalar, actualizar y mantener los paquetes y programas básicos de las computadoras personales con que cuenta la institución.
- ✓ Realizar instalaciones menores de hardware y proporcionar mantenimiento preventivo y correctivo de emergencia a los equipos de cómputo y periféricos.
- ✓ Realizar pruebas para verificar la operación y rendimiento a los equipos de cómputo, comunicación y auxiliares en proceso de adquisición.
- ✓ Elaborar y mantener actualizado el inventario del equipo de cómputo, de comunicaciones y software que posea la institución; y resguardar las licencias de uso, manuales y medios físicos del software adquirido.

CAPÍTULO IV

ANÁLISIS DE LA RED ACTUAL

4.1. DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL

La Dirección de Titulación de Tierras y Catastro Rural se encuentra ubicada en la Calle Real N° 507 – El Tambo - Huancayo.

Es la unidad orgánica encargada de realizar el saneamiento físico legal de la propiedad agraria, mantener la información catastral rural actualizada, proporcionar la seguridad jurídica a los propietarios de predios rurales y generar las condiciones básicas para el desarrollo ágil y transparente del mercado de tierras de uso agrario

En la figura 4.1 se muestra un pequeño mapa con las principales avenidas para su correcta ubicación y una foto de la institución. [11]

Figura 4.1 – Ubicación de la Institución.

Elaboración propia Fuente: Google maps Dirección Regional de Agricultura Junín

Figura 4.2 – Ubicación de la Institución.

Fuente: Dirección Regional de Agricultura Junín

4.2. DESCRIPCIÓN DE LA INFRAESTRUCTURA

La DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL desarrolla sus actividades administrativas y de operaciones en su local, ubicado en la Calle Real N° 507 – El Tambo - Huancayo donde se encuentran concentradas las oficinas administrativas, las áreas: legal, técnica y de informática. [11]

En la actualidad los ambientes se encuentran separados por no contar con una estructura adecuada, todos estos ambientes se han acondicionado según las necesidades que surgían por el crecimiento año tras año, según lo planificado en unos meses se iniciara los trabajos de remodelación prevista donde se acondicionaran las oficinas en un solo ambiente.

La implementación y crecimiento de la red no ha sido planificado, ha sido implementado sobre tecnología Ethernet y cuenta con una gran variedad de dispositivos de diferentes capacidades, el cableado está hecho con UTP CAT 5e, el cableado está estructurado, cuentan con dos switchs principales, ambos switchs están conectados al router que brinda el servicio de internet, a estos switchs se conectan otros que alimentan a las diferentes áreas tanto de la Dirección Regional de Agricultura como a la Dirección de Titulación de Tierras y Catastro Rural, muchos de estos switchs están operando satisfactoriamente.

El uso principal que se le da a la red es el de poder conectarse a Internet y a los Sistemas, también se utiliza para compartir información e impresoras en una misma oficina

La figura 4.2 muestra el plano de la infraestructura de la Dirección Regional de Agricultura y las áreas correspondientes a la Dirección de Titulación de Tierras y Catastro Rural como son:

1. Área técnica e informática
2. Dirección, secretaria y administración
3. Área de archivos
4. Área legal - saneamiento físico
5. Área de atención al usuario

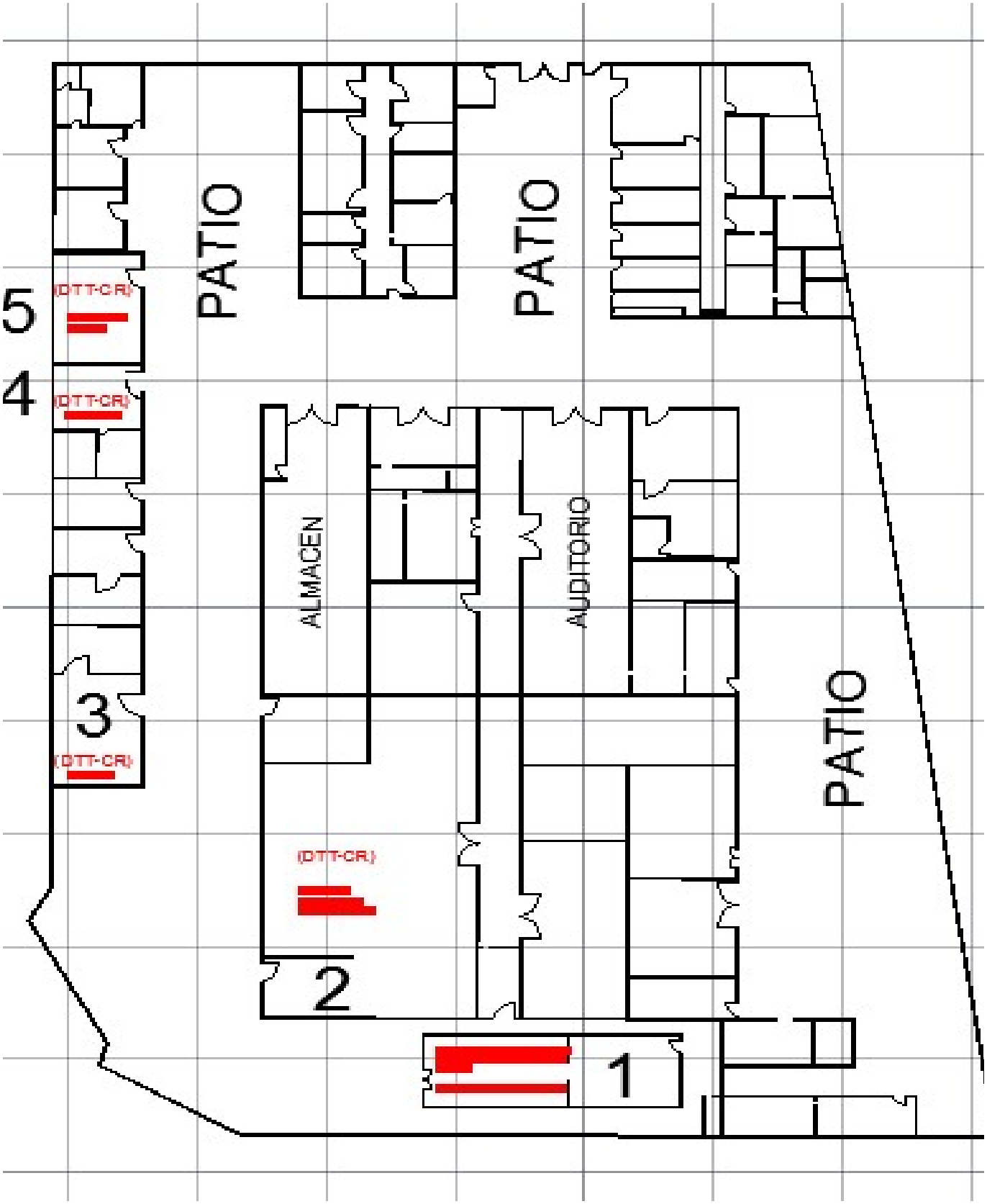


Figura 4.3 – Plano actual de la Dirección Regional de Agricultura y las áreas de la Dirección de Titulación de Tierras y Catastro Rural
Elaboración propia Fuente: Autocad Plano de infraestructura Dirección Regional de Agricultura

4.3. DESCRIPCIÓN DE LA RED EXISTENTE

En la actualidad la Dirección de Titulación de Tierras y Catastro Rural. cuenta con una topología estrella extendida de acuerdo con la tecnología IEEE 802.3 con conexión directa hacia un switch Cisco de la Serie Catalyst 2690 con 24 puertos 10/100 Mb + 2 puertos 10/100/1000 Mb, conectores RJ45 luego este, se conecta a un router (zyxel 660hw T1 wi-fi) 4 puertos con conectores RJ45, este, se conecta directamente con una línea telefónica a través de un conector RJ11 usando la tecnología ADSL, tiene un spliter (filtro pasa bajo y pasa altos para que la señal de voz y datos viajen ordenados) a través de la línea telefónica se conectan a Internet.

En la figura 4.4 se muestra la distribución de equipos físicos en las oficinas que pertenecen a la Dirección Regional de Agricultura, a nivel de la Dirección el cableado de red es Horizontal distribuyéndose desde el switch correspondiente a las estaciones de trabajo, en todas las áreas mencionadas

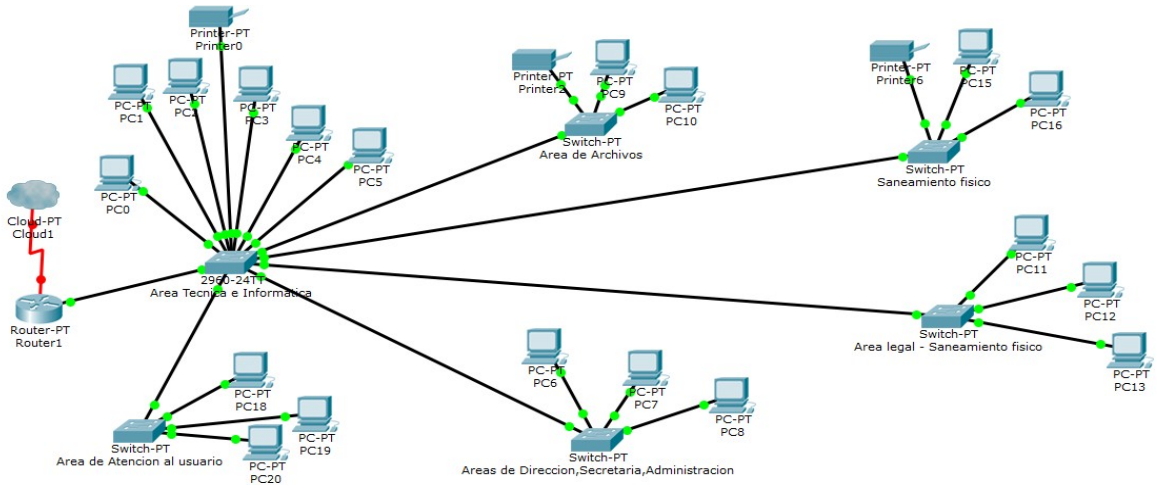


Figura 4.4 – Descripción de la topología de la red actual en la Institución.
Elaboración propia Fuente: Cisco Packet Tracer

La institución cuenta en la actualidad con 60 Pc´s que utilizan los sistemas operativos Windows XP y Windows 7, están conectados vía red a través del switch que tiene ésta capacidad.

4.4. CONECTIVIDAD EXTERNA

En la ciudad de Huancayo existen dos proveedores de telecomunicaciones: Movistar y Claro, los servicios que utiliza la institución son del proveedor Movistar. En Movistar cuenta con dos tipos de líneas de comunicación:

- Una línea ADSL Speedy Negocios de 3Mb al 10%, para el acceso a internet para los usuarios administrativos. Esta línea debería traducirse en un máximo de velocidad de 768 Kbps Downstream y 512 Kbps Upstream sobre cualquier

protocolo sin embargo las velocidades son mucho menores debido a que el proveedor solo garantiza la velocidad contratada hasta sus circuitos de transmisión y no más allá de internet.

4.5. PROBLEMAS EXISTENTES DE CONECTIVIDAD

La red de la Institución presenta muchos problemas, continuamente se han venido observando diferentes inconvenientes que afectan el normal funcionamiento de las actividades. Los problemas son reportados a la oficina de Informática, desde donde se han recopilado éstas incidencias:

- Todos los días el personal reporta que no hay acceso a internet, en una frecuencia de 2 a 4 veces al día, o el servicio se encuentra muy lento siendo necesario reiniciar el router para poder volver a recuperar el servicio. Al realizarse el análisis respectivo de la falla se puede identificar que los servicios ICMP responden favorablemente a las pruebas y los demás servicios presentan saturación.
- Muy a menudo se presenta conflicto de direcciones Ip, la red de la institución está configurado con direccionamiento lpv4 en todos sus equipos, generando desconexión de las computadoras debiendo modificarse manualmente las direcciones para que retome el servicio de Internet.
- El personal de las distintas agencias que visitan la institución conectan sus equipos personales como laptops a la red y configuran manualmente sus propias direcciones, generando conflicto de direcciones IP y al incrementar el número de equipos generan colisiones de broadcast del dominio.
- Los usuarios que logran conectarse al internet no tienen ningún control y en caso de que se intentaba controlarlos los usuarios utilizaban otros métodos para saltar estos mecanismos y seguían utilizando el internet sin restricción alguna.
- Los usuarios de las oficinas administrativas utilizan el internet para acceder a los distintos sistemas de la Institución pero también lo utilizan de forma generalizada para ingresar a páginas de ocio (video, audio, chats, imágenes, radios, juegos, etc) incluso utilizan programas que les permiten realizar descargas de programas, videos y música que saturan completamente el servicio de Internet.

Incidente	Alcance	Dispositivo	Tiempo de recuperación	Causa
Averías en el router Fecha 02 de marzo 2013 a horas 9:00 a.m.	Área técnico legal	Router	4 horas	fallos de energía, anomalías eléctrica subida y bajada de tensión
ejo contraseñas de usuarios Fecha 05 de marzo 2013 a horas 8:00 a.m.	Área legal - saneamiento físico	Pc´s, servicios, recursos, sistemas informáticos	30 minutos	perdida, olvido de contraseñas, no permitiendo el acceso a sistema, recurs servicios
Existencia de software malicioso(virus) Fecha 8 de marzo 2013 a horas 11:00 a.m.	Administración	PC´s	2 horas	a través del correo electrónico, al desca ficheros anexados infectados, memoria
verías en pc´s(hardware) Fecha 09 de marzo 2013 a horas 8:30 a.m.	Área de archivos	PC´s, fuente de poder, disco duro	3 horas	avería en la fuente de poder, disco du
o conectividad de medios Fecha 10 de marzo 2013 a horas 3:00 p.m.	Área de saneamiento físico	Router, PC´s.	45 minutos	cable utp deteriorado, gastado, Conecto RJ 45 (mal ponchado en cable UTP

erías en pc´s(hardware) echa 26 de marzo 2013 a horas 3:00 p.m.	Área de saneamiento físico	PC´s, fuente de poder, ventiladores, motherboard	2 horas	fallo de componentes del hardware, cooler(ventilador), falta de mantenimie físico
onexión a internet lenta Fecha 03 de abril 2013 a horas 11:30 a.m.	Área legal	PC´s	30 minutos	Exceso de aplicaciones que operan sobr red, uso de páginas de ocio(videos, mús redes sociales, chat)
Existencia de software malicioso(virus) Fecha 8 de abril 2013 a horas 11:00 a.m.	Administración	PC´s	2 horas	a través del correo electrónico, al desca ficheros anexados infectados, por comp archivos y carpetas infectadas
conectividad de medios Fecha 15 de abril 2013 a horas 9:00 a.m.	Administración	switch, pc´s	1 ½ hora	Conectores RJ 45 (mal ponchado en ca UTP), cables utp deteriorado,
onexión a internet lenta Fecha 18 de abril 2013 a horas 10:00 a.m.	Área de atención al usuario	PC´s	30 minutos	equipos obsoletos, poco espacio en dis duro, la pc está saturada de programas ocupan la poca capacidad de memoria c que cuenta
falla en el manejo de privilegios Fecha 21 de abril 2013 a horas 2:30 p.m.	Área de atención al usuario	Sistema	30 minutos	Manejo de información sin restriccion permisos ni privilegios

Existencia de software malicioso(virus) Fecha 23 de abril 2013 a horas 3:00 p.m.	Secretaria de Dirección	PC´s	2 horas	a través de la navegación por internet visitar ciertas páginas web con conten malicioso, y por compartir archivos v memoria USB,
Perdida de servicio Fecha 7 de mayo 2013 a horas 3:00 p.m.	perdida de servicio en toda la institución	router, switch, pc´s	2 horas	perdida de servicio de internet por parte empresa proveedora
rías en pc´s (hardware) Fecha 13 de mayo 2013 a horas 10.00 a.m.	Área de archivos	Pc´s, tarjeta de red	3 horas	antigüedad de equipos, obsolescenci
Perdida de servicio Fecha 21 de mayo 2013 a horas 2:30 p.m.	perdida de servicio en toda la institución	router, switch, pc´s	1 hora	perdida de servicio de internet por parte empresa proveedora
fallas en el suministro ctrico u otras anomalías eléctricas Fecha 24 de mayo 2013 a horas 2:30 p.m.	perdida de servicio de internet y fluido eléctrico en toda la institución	router, switch, pc´s	2 horas	Corte de fluido eléctrico

Figura 4.5 – Organigrama Estructural de la Dirección de Titulación de Tierras y Catastro Rural

Elaboración propia fuente: Direcci Region cultura Junín - Nomas ISO 17799

ASIGNACIÓN DE DIRECCIONES IP

Asignación de direcciones IP para Trabajadores

Área de la Institución	Nombre Pc	Dirección IP
Dirección	DTT - 1	192.168.1.151
Administración	DTT - 2	192.168.1.152
Secretaria de Dirección	DTT - 3	192.168.1.153

Área de la Institución	Nombre Pc	Dirección IP
Área Legal	DTT - 4	192.168.1.154
	DTT - 5	192.168.1.155
	DTT - 6	192.168.1.156
	DTT - 7	192.168.1.157
	DTT - 8	192.168.1.158

Área de la Institución	Nombre Pc	Dirección IP
Atención al Usuario	DTT - 9	192.168.1.160

Área de la Institución	Nombre Pc	Dirección IP
Área Saneamiento Físico	DTT - 10	192.168.1.161
	DTT - 11	192.168.1.162
	DTT - 12	192.168.1.163
	DTT - 13	192.168.1.164
	DTT - 14	192.168.1.165

Área de la Institución	Nombre Pc	Dirección IP
Área de Informática	DTT - 15	192.168.1.166
	DTT - 16	192.168.1.167
	DTT - 17	192.168.1.168
	DTT - 18	192.168.1.169
	DTT - 19	192.168.1.170

Figura 4.6 – Asignación de direcciones IP

Elaboración propia fuente: Dirección Regional de Agricultura Junín

4.6. DESCRIPCIÓN DEL SISTEMA DE SEGURIDAD DE LA EMPRESA

La existencia de amenazas y riesgos, en la infraestructura de red y recursos informáticos en una institución hace que deban estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración de riesgo. En la actualidad la institución no cuenta con ningún sistema de seguridad serio contra ataques de personas mal intencionadas que pueden hacerle espionaje, borrar archivos, entre otros ataques, por esto se propone un sistema de seguridad para la Institución.
Pero si cuenta con políticas de seguridad establecidas como:

Políticas para el control de acceso del usuario

- ✓ **Registro de usuarios**
  Elaborar un procedimiento formal de registro de usuarios para otorgar accesos a los sistemas y servicios de información.
  - Eliminar de manera inmediata los derechos de acceso de los usuarios que hayan cambiado de trabajo o hayan dejado la institución - Norma ISO 17799 - Registro del usuario.
  - Chequear de manera periódica y eliminar los IDS de cuentas usuario redundantes - Norma ISO 17799 - Registro del usuario.

- ✓ **Permisos de usuarios**
  Restringir y controlar la asignación y uso de los privilegios a los usuarios, el uso inapropiado de los privilegios del sistema con frecuencia es un importante factor que contribuye a la falla de los sistemas que se han violado.
  - Identificar los privilegios asociados con el sistema, así como la asignación de los privilegios a las personas sobre una base "lo que necesitan saber" y "evento por evento"; es decir el requerimiento mínimo para su rol funcional solo cuando se necesita - Norma ISO 17799 - Manejo de privilegios.
  - Mantener un proceso de autorización y un registro de todos los privilegios asignados, los que no se deberían otorgar sino hasta que se complete el proceso de autorización - Norma ISO 17799 - Manejos de privilegios.

- ✓ **Manejo de contraseñas del usuario**
  Las claves secretas son medios comunes para validar la identidad del usuario para tener acceso al sistema o servicio de información.

La asignación de contraseñas secretas se debería controlar a través de un proceso de gestión formal.

- ✓ **Uso de contraseñas por parte de los usuarios**
  - Mantener sus contraseñas secretas en forma confidencial - Norma ISO 17799 - Uso de claves secretas.
  - Evitar mantener un registro escrito de sus contraseñas secretas a no ser que se puedan guardar con seguridad - Norma ISO 17799 - Uso de clave secreta.

Políticas para el manejo de la información

- ✓ **Educación y capacitación en seguridad de la información**

Todos los empleados de la institución deberían recibir una capacitación apropiada y actualizaciones regulares sobre las políticas y procedimientos institucionales.

- Los usuarios deberán utilizar únicamente los servicios para los cuales están autorizados. Los usuarios no pueden utilizar las cuentas de otras personas ni intentar apoderarse de las claves de acceso, como tampoco intentar burlar los sistemas de seguridad bajo ningún punto de vista.

- ✓ **Mantenimiento de registro de actividades**

El personal operacional debe mantener un registro de sus actividades en el sistema y registrar las fallas reportadas por los usuarios de los sistemas de procesamiento de la información y comunicaciones. Los registros deben incluir: (Norma ISO 17799 – Registros del operador).

- Momento de inicio y fin de los sistemas
- Errores del sistema y las acciones correctivas tomadas
- El nombre de la persona que está realizando en ingreso de registros

Políticas para manejo de equipos

- ✓ **Mantenimiento de equipo**

El equipo debería ser mantenido correctamente para asegurar la disponibilidad e integridad continua.

- Realizar las reparaciones y servicio al equipo con el personal de mantenimiento de hardware de la institución - Norma ISO 17799 Mantenimiento de equipo.

- Mantener registros de todas las fallas sospechosas o reales y de todo el mantenimiento preventivo y correctivo - Norma ISO 17799 Mantenimiento de equipos.

- Prohibir a los usuarios abrir las maquinas, hacer cambios no autorizados en el hardware, sea cambios de memorias, discos y más partes constitutivas del equipo.

✓ **Suministro de energía**

El equipo debería ser protegido de fallas de energía y otras anomalías eléctricas, se debería proporcionar un suministro eléctrico adecuado que satisfaga las especificaciones de la red.

- Incluir múltiples alimentadores para evitar un solo punto de falla en el suministro de energía - Norma ISO 17799 - Suministros de energía.
- Utilizar un suministro de energía sin interrupciones (ups) realizando un chequeo regularmente para asegurar que tiene la capacidad adecuada.

✓ **Cableado**

El cableado de energía y telecomunicaciones que lleva datos o sostiene los servicios de información de deben proteger de la interceptación o daño.

- Proteger el cableado de la red de una interceptación no autorizada o daño, utilizando conductos porta cables o al evitar las rutas a través de áreas públicas - Norma ISO 17799 - Seguridad en el cableado.

Políticas para el manejo de la información

✓ **Debilidades en la seguridad**

Requerir que los usuarios de los servicios de información noten y reporten cualquier debilidad de seguridad observada o las amenazas en los sistemas o servicios, indicando a su jefe inmediato - Norma ISO 17799 – Reporte de debilidades en la seguridad.

✓ **Mal funcionamiento del software**

Establecer los procedimientos para reportar cualquier mal funcionamiento en el software.

- Prohibir a los usuarios que no eliminen el software en sospecha, a no ser que se le autorice a eso.

  El personal capacitado y experimentado debería llevar a cabo la recuperación de esta - Norma ISO 17799 - Seguridad de los sistemas de oficina electrónicos.

Políticas de acceso al internet

- ✓ **Uso del internet**
  - No se deben descargar archivos con títulos atractivos pero sospechosos, de ninguna vía.
  - El personal apropiadamente capacitado debería llevar a cabo la eliminación constante de cookies, archivos temporales e historial de internet con la finalidad de liberar espacio en el disco.

- ✓ **Software malicioso**

La protección contra software malicioso se debería basar en la conciencia de seguridad, acceso apropiado al sistema mediante controles de detección y prevención.

- Instalar y actualizar antivirus, para analizar las computadoras y medios ya sea como un control de precaución o de manera rutinaria Norma ISO 17799 - Controles contra el software malicioso.
- Chequear antes de usar cualquier archivo en los medios electrónicos de origen incierto o no autorizado o los archivos recibidos a través de redes no confiables, para verificar si tiene virus - Norma ISO 17799 - Controles contra el software malicioso.
- Chequear antes de usar cualquier archivo adjunto en el correo electrónico y las descargas para ver si tienen algún software malicioso Norma ISO 17799 - Controles contra el software malicioso.

- ✓ **Correo electrónico**

La institución debe controlar en el uso del correo electrónico:

- Ataques por correo electrónico (virus intercepción) - Norma ISO 17799 - Políticas sobre correos electrónicos.
- Protección de los archivos adjuntos del correo electrónico - Norma ISO 17799 - Políticas sobre correos electrónicos.

- No descargar archivos con extensión .exe, .vbs, avi, protectores de pantalla, etc. Que no provengan de un usuario conocido. En estos casos, se les recomienda borrar inmediatamente el mensaje sin abrirlo y de ser detectados por el administrador serán borrados.

CAPÍTULO V

ARQUITECTURA Y DISEÑO DE LA RED

5.1. ARQUITECTURA DE LA RED

La arquitectura de la red es de alto nivel, a través del modelo respectivo se muestran las relaciones entre los principales componentes de la red para el logro de los objetivos. La arquitectura planteada pretende mejorar el rendimiento de la red y garantizar el uso de las aplicaciones según sus propios requerimientos de esta, se garantiza estabilidad y confiabilidad en la red.

5.1.1. DIRECCIONAMIENTO/ENRUTAMIENTO

El direccionamiento planteado se basa en IPv4 en direcciones de la clase C, también llamadas privadas, esto es debido a que solo se cuenta con una salida al servicio de Internet y que debe ser realizada a través de un mecanismo llamado NAT.

ID Red	Rango Sub Red	Uso	Observaciones

A	192.168.1.0/24 GW:192.168.1.1	Speedy Negocios	Servicio de Internet
B	192.168.5.0/24 GW:192.168.7.1	Administrativos	Red LAN para los trabajadores de la institución
C	192.168.7.0/24 GW:192.168.7.1	Red Inalámbrica	Red WLAN para el personal con dispositivos móviles en la institución

Tabla 5.1 – Direccionamiento IPv4 de la Red WLAN de la Institución
Elaboración propia Fuente: Dirección Regional de Agricultura área informática

En la siguiente tabla 5.2 se muestra la asignación de las direcciones IPv4 según el cuadro anterior:

ID Red	Área	N° Usuarios	Dirección IPv4 Inicial	Dirección IPv4 Final
C	Red Inalámbrica	50	192.168.7.10	192.168.7.99
C	Red Inalámbrica del personal visitante a la Institución	200	192.168.7.100	192.168.7.239

Tabla 5.2 – Asignación de las direcciones IPv4 por Áreas.
Elaboración propia Fuente: Dirección Regional de Agricultura área informática

Las direcciones IPv4 serán asignadas de la siguiente manera:

Para la red inalámbrica se creara una red a la que llamaremos WIFIDTT, la asignación de las direcciones del ID C será de forma automática en función a lo siguiente:

Se registrara la dirección MAC del personal que labora en la Institución previamente identificados y en función a ello se le asignara una dirección IP del rango que le corresponda y para el caso del personal que en ocasiones llega de las diferentes sedes de la Institución el sistema le asignara una dirección de forma automática y para que pueda tener

acceso a Internet deberá ingresar un código que tendrá validez por un determinado tiempo, luego del cual se cortara la conexión.

5.1.2. GESTIÓN DE LA RED

La arquitectura de la red está pensada en un modelo Cliente-Servidor, esto es debido a que la principal aplicación a utilizar esta en Internet y en servicios locales de la Institución.
La gestión de la red se divide en tres actividades: Monitoreo, Instrumentación y Gestión. Para este caso se utilizara el sistema PFSense como sistema central para la administración de la red, el cual permitirá aplicar las configuraciones necesarias y realizar las gestiones de administración de red requeridas.

- **Mecanismos de Monitoreo:** Se recogerán los datos que influyen a través de la red y se mostraran en herramientas graficas accesibles vía un entorno web. Se podrá apreciar el grafico en tiempo real identificando las direcciones de origen y destino, el estado de la conexión, el tiempo, la cantidad de paquetes que se transfieren y el consumo que cada conexión acumula. Acumulación del trafico según días y frecuencia de horas, estado del tráfico actual en tiempo real con salidas a internet identificando el host de origen y el ancho de banda utilizado, estado de los servicios del servidor de administración de red. Monitoreo de la asignación de direcciones IPv4 a través del servidor DHCP del servidor de administración de red.

- **Mecanismos de Instrumentación:** Los mecanismos de instrumentación son el conjunto de herramientas y utilidades necesarias para el seguimiento y sondeo de la red. Las herramientas de monitoreo incluyen utilidades como: ping, traceroute y TCPdump y también mecanismos de conexión remota como FTP, TFTP, SSH vía consola. Todos estos mecanismos viene por default en el servidor de administración de red PFSense.

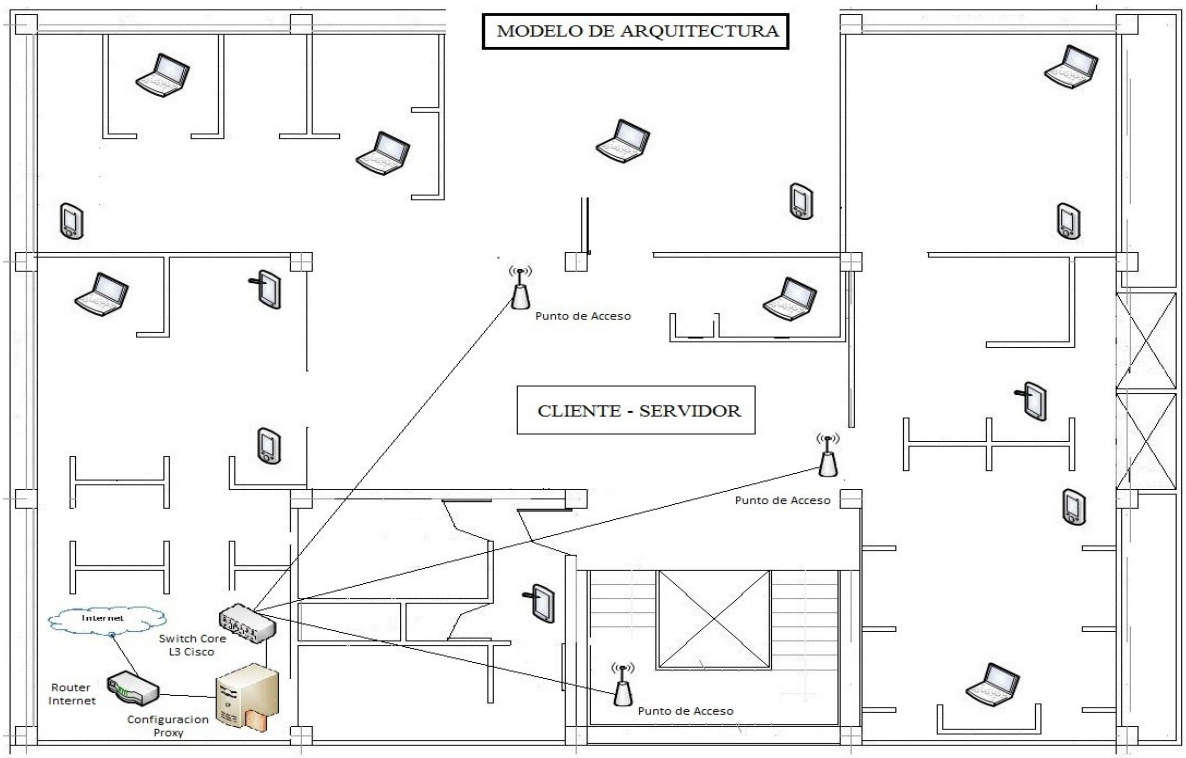
- **Mecanismos de Configuración:** El servidor de administración de red PFSense se encargara de gestionar toda la red, para ello cuenta con herramientas para la configuración remota o local. De forma remota tiene acceso vía web a una interfaz desde donde se puede realizar la

configuración y ajustes de toda o parte de la red. También de forma remota se tiene acceso vía SSH para la gestión de toda configuración del sistema, incluso dispone del servicio SNMP para poder realizar el monitoreo y configuración de red remota.

5.2. MODELO DE ARQUITECTURA

La arquitectura de una red viene definida por su topología, el método de acceso a la red y los protocolos de comunicación. Antes de que cualquier estación de trabajo pueda utilizar el sistema de red ya establecido debe definirse con cualquier otro nodo de la red.

La topología sobre la cual se diseñara dicho sistema de red es la topología de estrella extendida, también conocida como acceso/distribución/núcleo (Access/distribution/core) y teniendo en cuenta el flujo de datos el modelo está basado sobre Cliente- Servidor.



Elaboración propia Fuente: Autocad - Topología estrella extendida – arquitectura de red cliente servidor

5.3. DISEÑO DE LA RED

El diseño de la red es el objetivo final del presente informe, la culminación de los procesos de análisis y arquitectura de redes, el análisis proporciona la comprensión y la arquitectura de red proporciona las descripciones conceptuales (en tecnología y topología) por lo que el diseño se basa en estos.

5.3.1. Tecnología inalámbrica

La tecnología de redes inalámbricas basada en el estándar IEEE 802.11 tiene varios beneficios incuestionables en el mundo empresarial. Algunos de estos beneficios son la flexibilidad, movilidad, reducción de costes de infraestructura de red, integración con dispositivos móviles y PDAs, y mejor escalabilidad de la red.

Sin embargo para conseguir estos beneficios se debe definir la arquitectura y tecnología más apropiada y con el menor impacto tecnológico y económico. Si la red Wi-Fi no es fácil de usar y no presenta todas las facilidades de rendimiento, cobertura, seguridad y capacidad para el usuario ésta red se convierte en un problema en vez de una solución.

5.3.2. Selección de la Tecnología Inalámbrica

Para definir qué tecnología de red inalámbrica es la más favorable para la DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL es necesaria la comparación de los estándares de alto rendimiento de Wi-Fi 802.11 A y 802.11 G.

Características	802.11 A	802.11 G
Desempeño	Solo OFDM, banda de 5 GHZ y la ausencia de células mixtas proporciona una mejor capacidad de salida	Soporte para los estándares de alto rendimiento, células mixtas y operación en la banda de 2.4 GHZ tiene una capacidad de salida ligeramente menor que la de 802.11 A
Capacidad	Con ocho canales no solapados proporciona una capacidad total de 432 Mbps	Con tres canales no solapados proporciona una capacidad total de 162 Mbps
Rango	Una longitud de onda más corta y restricciones en la potencia de transmisión deterioran el rango de cobertura	Permiten un rango de cobertura de mayor tamaño que con 802.11 A
Interferencia	A 5 GHZ se tiene menos saturación del espectro	A 2.4 GHZ se presentan problemas de saturación con otros dispositivos
Compatibilidad	No proporciona compatibilidad con dispositivos anteriores de 802.11 B	Proporciona características importantes de compatibilidad con productos anteriores de 802.11 B
	Las regulaciones FCC que se	

Flexibilidad de instalación	aplican a los cuatro canales interiores de 802.11 A restringen a los fabricantes al uso exclusivo de antenas integradas que no pueden ser desconectadas	Al igual que 802.11 B permite antenas de 2.4 GHZ auxiliares que pueden estar directamente conectadas o conectadas a través de cables
Implementación	Para dar cobertura a un área se necesitan de varios puntos de acceso adicionales comparados con 802.11 G	Se tiene que para un área de cobertura grande es suficiente la implantación de pocos puntos de acceso

En la tabla se muestra los 2 estándares más utilizados para redes inalámbricas en instituciones.

Tabla 5.3 – Estándares más utilizados para redes inalámbricas en instituciones.
Elaboración propia Fuente: Estándares en tecnologías inalámbricas Alberto Escudero

Como parte del proyecto de la DIRECCIÓN DE TITULACIÓN DE TIERRAS Y CATASTRO RURAL se considera al estándar 802.11G, por ser el más adecuado y tener mayores prestaciones.

5.4. DISTRIBUCIÓN DE LA RED

- **Diagrama lógico:** El primer diagrama lógico muestra el diseño del núcleo y los switchs de distribución, apreciamos como elemento central a un servidor Firewall, se han realizado pruebas con PFSense y cumple muy bien los requerimientos de gestión. El servicio de internet se conectara al servidor Firewall, el servidor tendrá 3 tarjetas de red FastEthernet: 1 para la red Administrativa y una para la red Inalámbrica. El cableado del backbone debe ser implementado sobre tecnología Gigabyte con cable UTP 6.

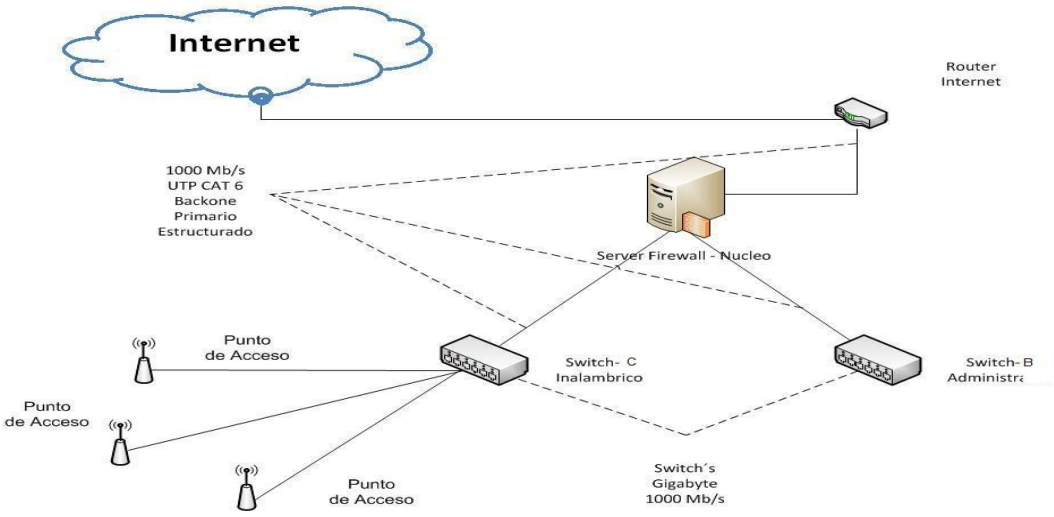
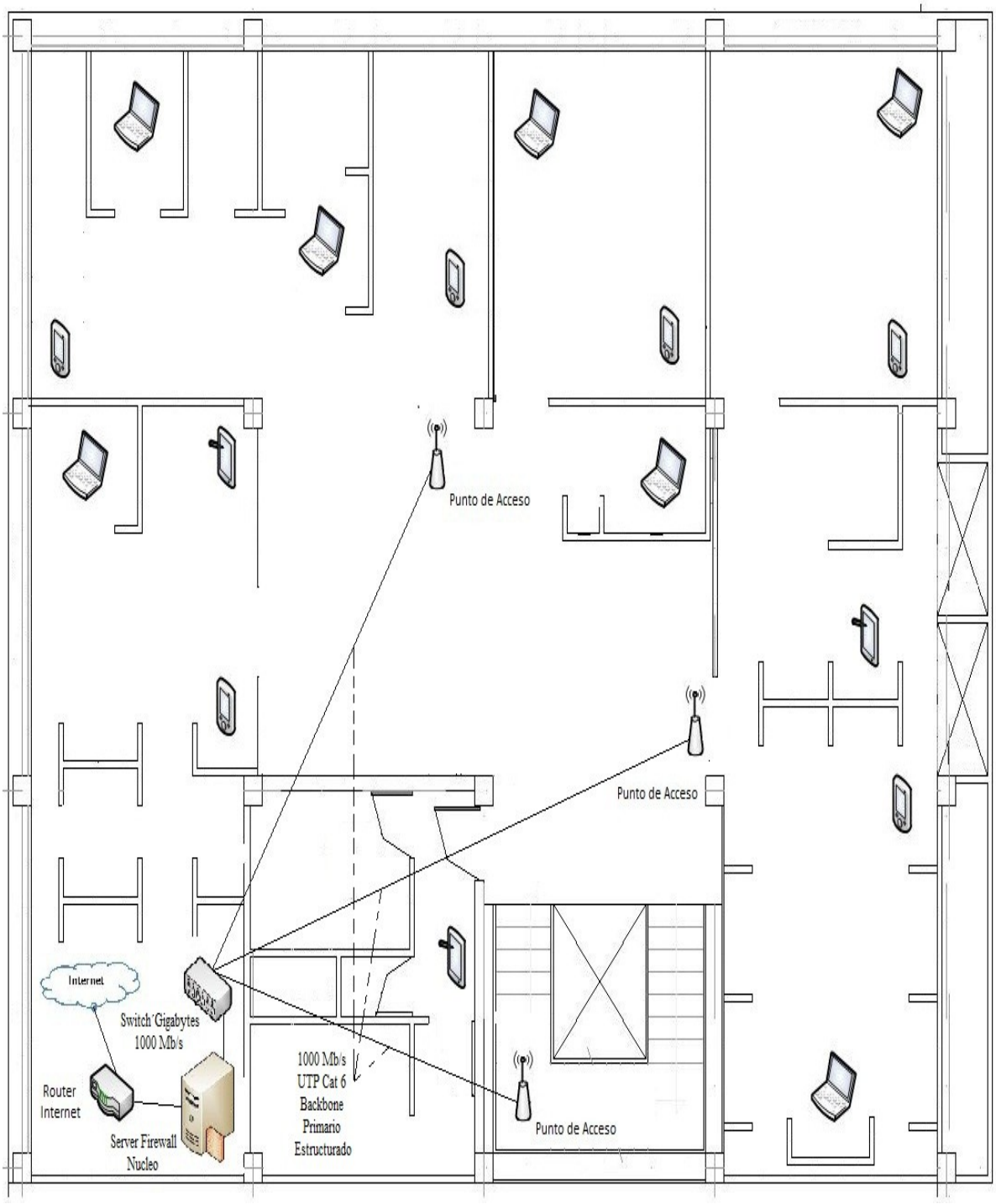


Figura 5.2 – Diagrama lógico del núcleo y distribución principal.
Elaboración propia Fuente: CCNA

La red inalámbrica para la Dirección de Titulación de Tierras y Catastro Rural y ocasionales visitantes contará con tres Access point que permitirán repartir la señal y dar acceso a los equipos móviles en una red totalmente separada de la otra red.

Figura 5.3 – Diagrama lógico de la red inalámbrica para la nueva oficina de la Dirección



de Titulación de Tierras y Catastro Rural.
Elaboración propia Fuente: AutoCAD – Dirección Regional de Agricultura Junín

- **Planos de la Red:** Los planos de la red nos muestran la ubicación estratégica de los equipos en la Institución. A continuación se muestran los planos de red del primer nivel.

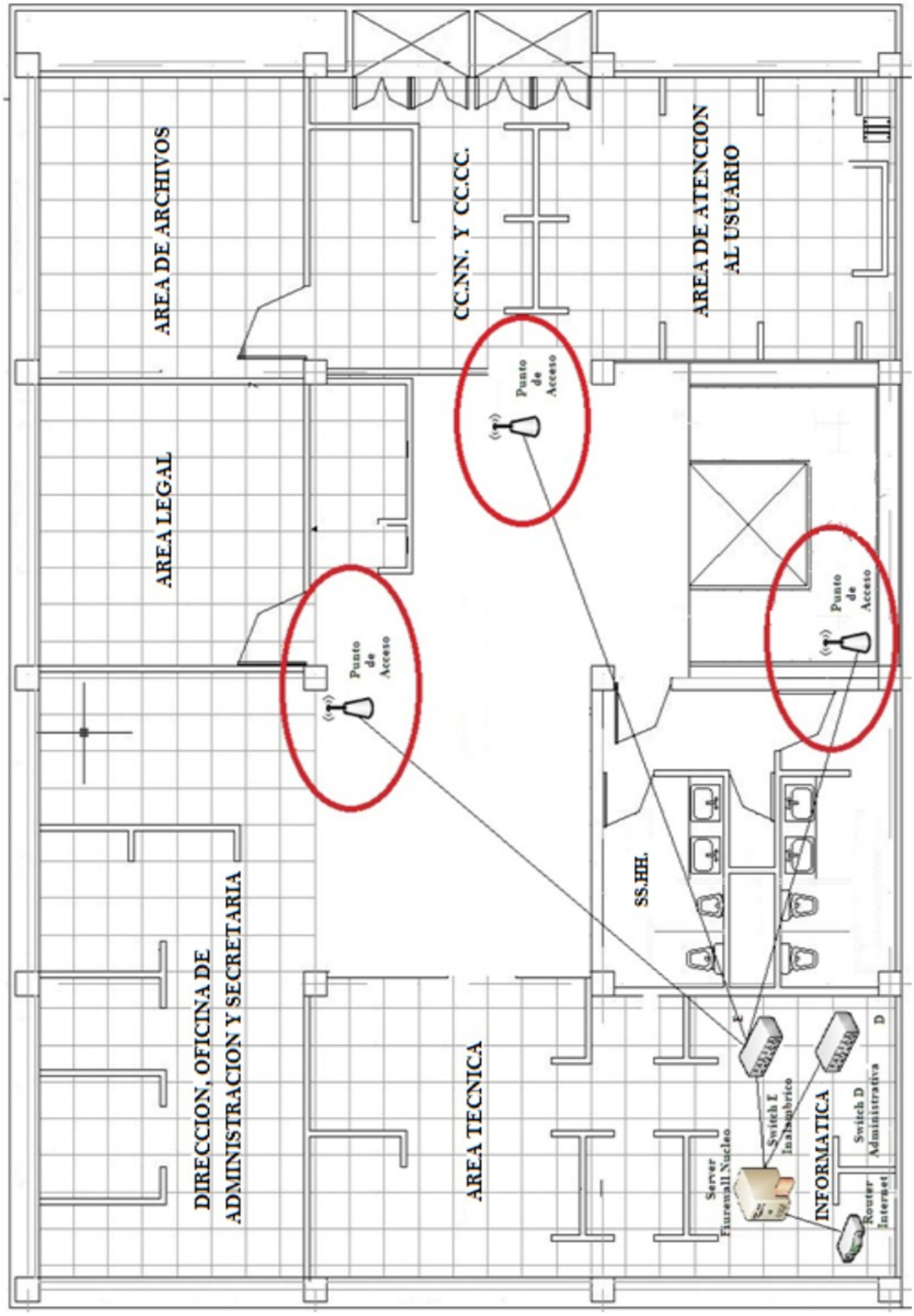


Figura 5.4 – Plano de red de la nueva oficina, núcleo y distribución.
Elaboración propia Fuente: AutoCAD – Dirección Regional de Agricultura Junín

5.5. SERVIDOR PARA LA GESTIÓN DE LA RED

En el punto 5.1.2. se definió los requerimientos para la gestión de la red, se implementara un servidor basado en PFSense, que es un sistema personalizado de FreeBSD adaptado para su uso como Firewall y Router. La elección se basa en las limitaciones financieras para adquirir nuevos equipos por su elevado costo; además se podrá actualizar las políticas de gestión de la red según necesidades y ampliar la funcionabilidad en base a paquetes de software del PFSense. Las características que se utilizarán del PFSense serán las siguientes:

- **Firewall**.- Pfsense se puede configurar como un cortafuego permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también haciendo filtrado avanzado de paquetes por protocolo y puerto.
- **State Table**.- PFSense es un stateful firewall, el cual como característica principal guarda el estado de las conexiones abiertas en una tabla. La mayoría de los firewall no tienen la capacidad de controlar con precisión la tabla de estado. Pfsense tiene un enorme número de características que permiten una granularidad muy fina para el manejo de la tabla de estado.
- **Network Address Translation (NAT)**.- Es un mecanismo utilizado por direccionadores (routers) IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo, un uso común es permitir utilizar direcciones privadas, si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada, para que solo puedan salir a Internet con una sola dirección IP.
- **Portal Cautivo**.- Este servicio consiste en forzar la autenticación de usuarios redirigiéndolos a una página especial de autenticación y/o para aceptar los términos de uso, realizar un pago etc. para poder tener acceso a la red. El portal cautivo es usado comúnmente para control de accesos a la red en los puntos de accesos inalámbricos de los hoteles, restaurantes, parques y kioscos.

- **Servidor DHCP**.- Especifica un método para configurar dinámicamente los parámetros de red necesarios para que un sistema pueda comunicarse efectivamente. También funciona como servidor de DHCP, se puede también implementar VLAN desde Pfsense.

- **Monitor y Gestión de la Red**.- Información en tiempo real, a través de los gráficos RDD Pfsense muestra el estado de los siguientes componentes:
  - ✓ Utilización de CPU
  - ✓ Rendimiento Total
  - ✓ Estado del Firewall
  - ✓ Rendimiento individual por cada interface
  - ✓ Paquetes enviados y recibidos por cada interface
  - ✓ Manejo de tráfico y ancho de banda.

5.5.1. CARACTERÍSTICAS DE HARDWARE

El hardware utilizado como servidor tiene las siguientes características:

Case	ATX
Procesador	Intel Core 2 Quad
Mainboard	Intel DP67
Memoria RAM	4 GB DDR2
Disco Duro	250 GB Seagate SATA
Lectoras	Lector CD/DVD
Conectividad	Tarjeta de red Intel Gigabyte Network D-Link Fast Ethernet DFE-520TX PCI (Administrativa) D-Link Fast Ethernet DFE-520TX PCI (Inalambrica)

Cuadro 5.1 – Características de hardware del servidor.
Elaboración propia Fuente: Intel, D-link

Con los requerimientos que se muestra en la tabla anterior hacemos énfasis que para virtualizar se necesita de un hardware especial que reúna ciertos criterios para su implementación, a continuación se describe el por qué utilizarlo con ciertas características sofisticadas:

El microprocesador Quad Core integra cuatro núcleos a cada ordenador y ofrece la velocidad y capacidad de respuesta inmensas que se requieren cada vez más para procesar las aplicaciones, con un uso intenso de medios más exigentes en la actualidad.

Además ofrece un excelente desempeño escalable y la mejor virtualización de su clase para la consolidación de servidores. Dentro de sus cualidades fuertes se mencionan:

- Desempeño hasta dos veces mayor respecto de los procesadores Dual-Core de la generación anterior.
- Rendimiento por vatio más de dos veces superior a los procesadores Dual Core de la generación anterior.
- Las máximas relaciones de consolidación de cualquier procesador Intel Xeon.
- Ayuda a proteger los datos mediante funciones avanzadas de redundancia y comprobación de errores

- ✓ Motherboard Intel DP67, ofrece nuevos niveles de rendimiento y fiabilidad para el hogar, instituciones educativas, usuarios empresariales, etc., también está diseñado para apoyar una gama de procesadores incluidos en el procesador Intel 2 Quad y el procesador Intel Core 2 Dúo.
- ✓ Esta placa puede soportar hasta 4 GB de doble canal DDR2 800/667 MHZ SDRAM. Así mismo, ofrece conexión de la red integrada 10/100/1000 y amplios conectores USB para todos los ordenadores.
- ✓ El disco duro propuesto está destinado para la instalación del sistema operativo FreeBSD.
- ✓ Case ATX, necesario para el montaje del hardware antes mencionado.
- ✓ Lector de CD/DVD, se utiliza para la realización de las instalaciones y los respaldos de mantenimiento de los sistemas.
- ✓ Evaluación del hardware existente con el que cuenta la institución, y tomando en cuenta la configuración de los servidores, es necesario adquirir equipo que cumpla con los requerimientos para ser virtualizados, ya que se necesita de un hardware con requerimientos sofisticados, para que soporten todos los servicios para su funcionamiento.

5.5.2. CONFIGURACIÓN GENERAL

Se instaló el PFSense v.2.0.1, es un proceso de instalación estándar, luego se procede a asignarle las siguientes direcciones:

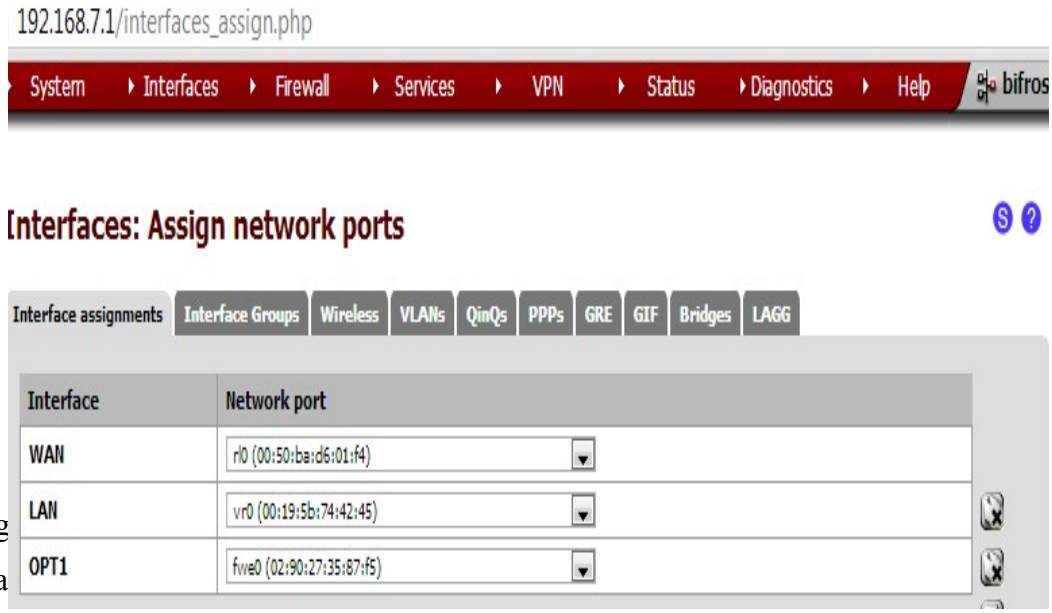
Red	Direccionamiento IPv4		
	IP	Máscara	Gateway
WAN	192.168.1.15	/24	192.168.1.1
Administrativ	192.168.5.1	/24	---

a			
Inalámbricos	192.168.7.1	/24	---

Tabla 5.4 – Direcciones IP de las tarjetas del pfSense.

Elaboración propia Fuente: Instalación y configuración de pfsense

Primero se procederá a asignar un nombre a cada dispositivo de red, de esta manera podremos identificarlos fácilmente, se realizara haciendo clic en el menú INTERFACES ␣ ASSIGN NETWORKS:



Lueg

toma

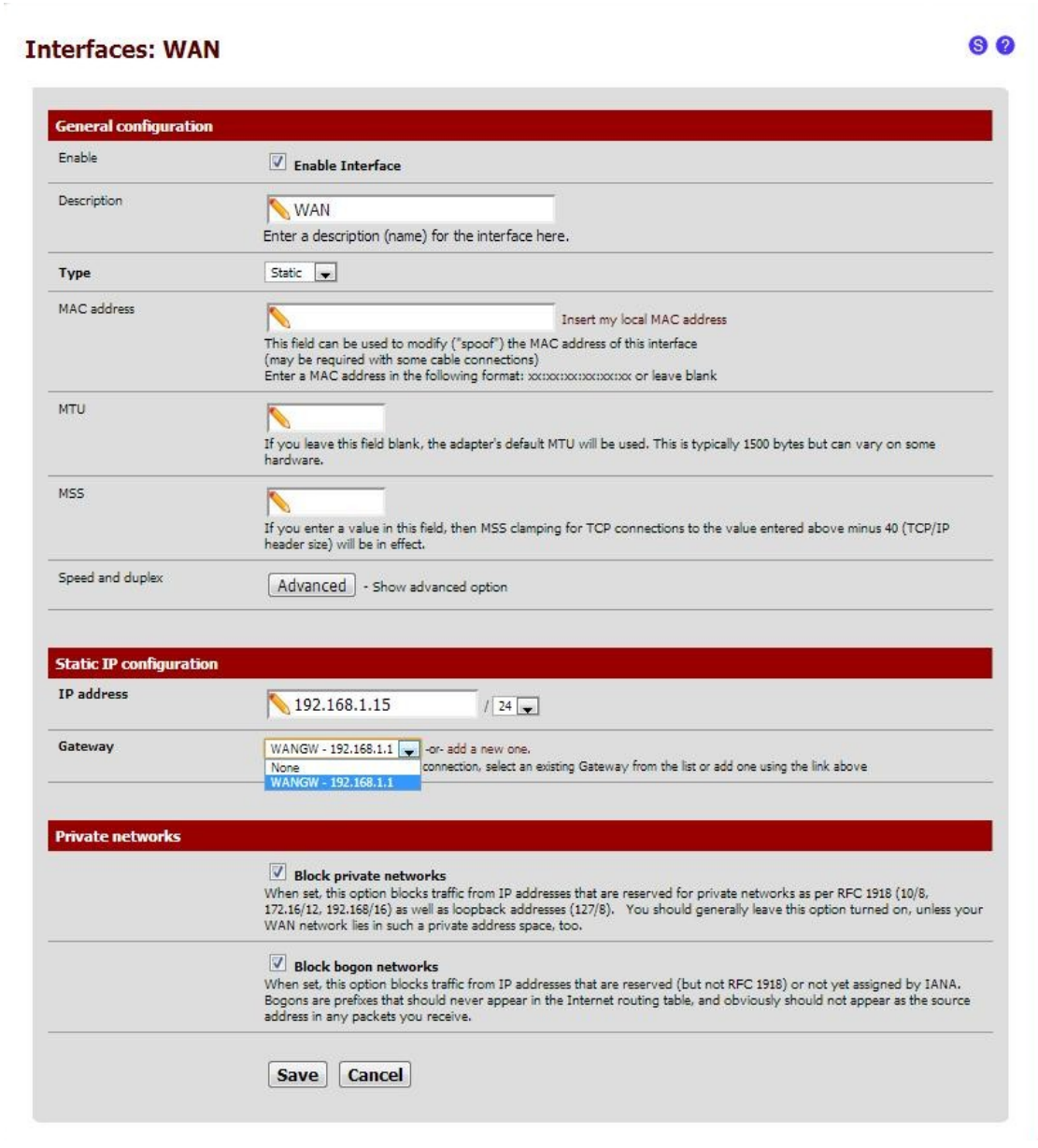


Figura 5.6 – Asignar direcciones IP a un dispositivo de red.

Elaboración propia Fuente: Instalación y configuración de pfsense

Luego asignamos un nombre al servidor, específicamente el dominio a utilizar y fijamos los DNS del proveedor de Internet para la resolución de los DNS. SYSTEM ␣ GENERAL SETUP:

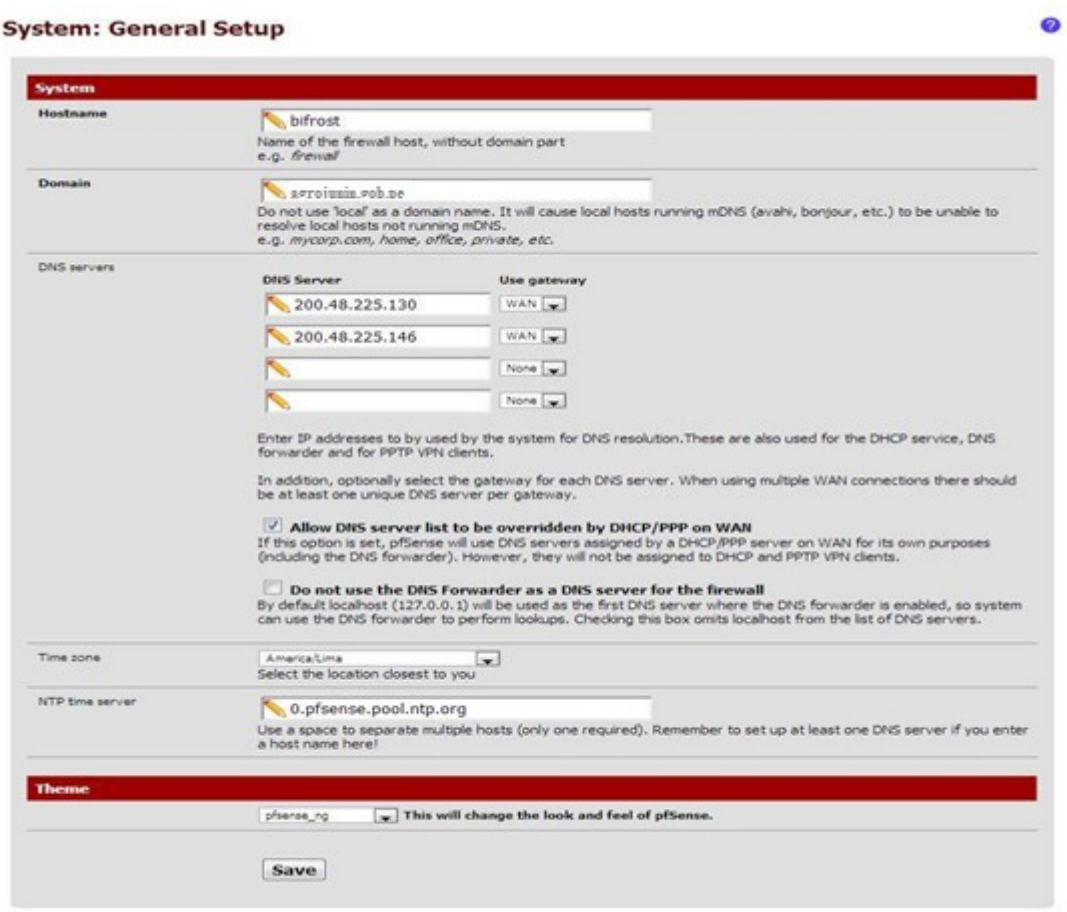


Figura Figura 5.7 – Configuración general Hostname.

Elaboración propia Fuente: Instalación y configuración de pfsense

Instalamos los paquetes adicionales que utilizaremos para el filtrado de contenidos y reportes, SYSTEM ␣ PACKAGES, instalamos los paquetes Lighsquid, squid y squid Guard:

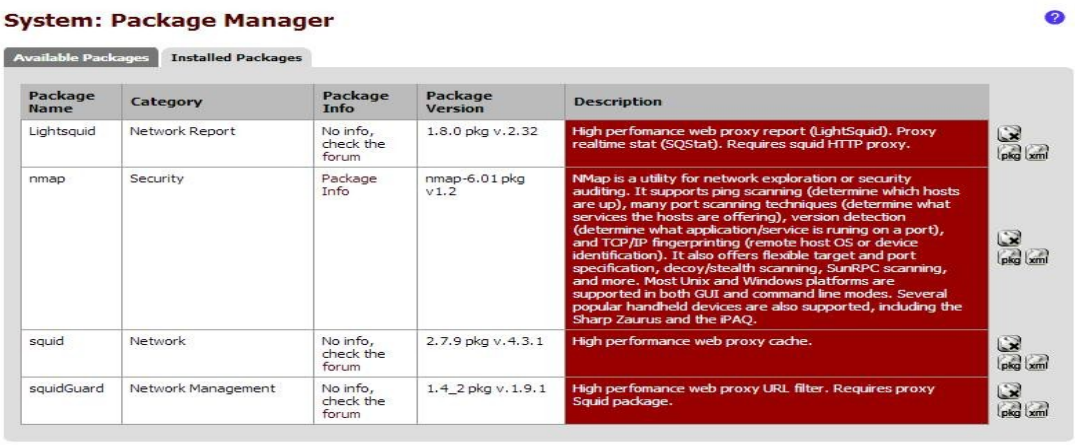


Figura 5.8 – Paquetes adicionales instalados en el pfSense.

Elaboración propia Fuente: Instalación y configuración de pfsense

5.5.3. CREACIÓN DE ALIAS

Una de las características de PFSense es la creación de Aliases que es la agrupación de un conjunto de direcciones para identificarlos de forma más rápida, aquí creamos los aliases tanto para los usuarios de la red, como para direcciones específicas o por grupos que se bloquearán o se darán acceso, FIREWALL ␣ ALIASES:

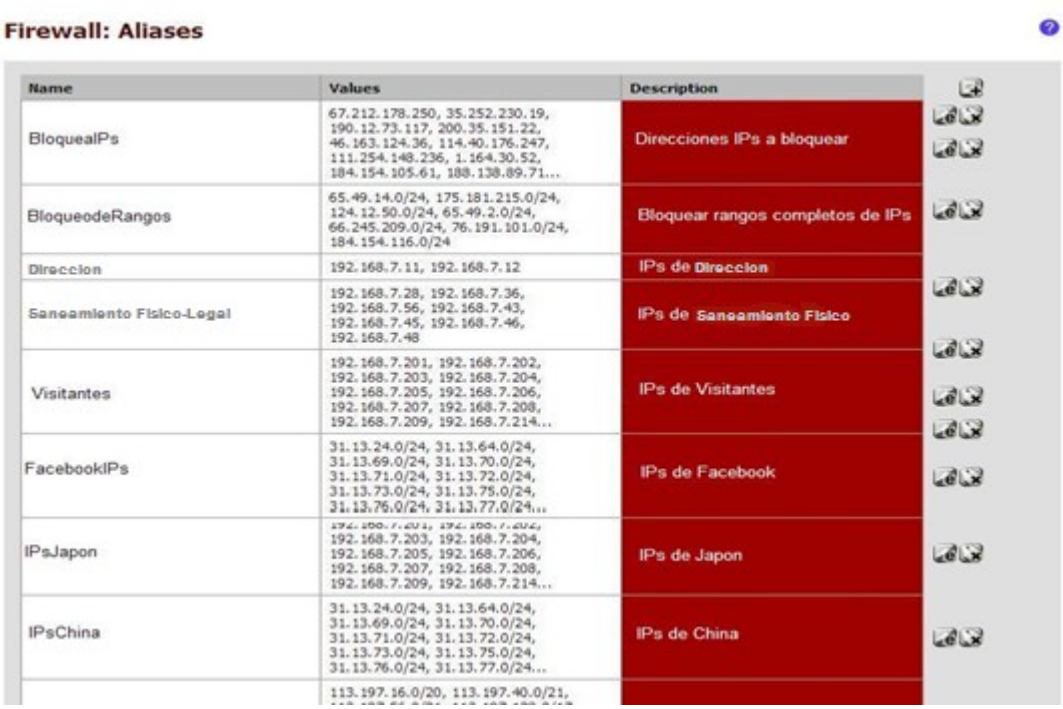


Figura 5.9– Listado de aliases creados en el Firewall.

Elaboración propia Fuente: Instalación y configuración de pfsense

En nuestro caso los aliases nos permitirán identificar y agrupar fácilmente a nuestros usuarios, y destinos y orígenes de red.

5.5.4. CONFIGURACIÓN DE LA RED INALÁMBRICA

La red Inalámbrica será gestionada a través del servicio CAPTIVE PORTAL, este servicio permite gestionar a los usuarios y la asignación de direcciones IP.

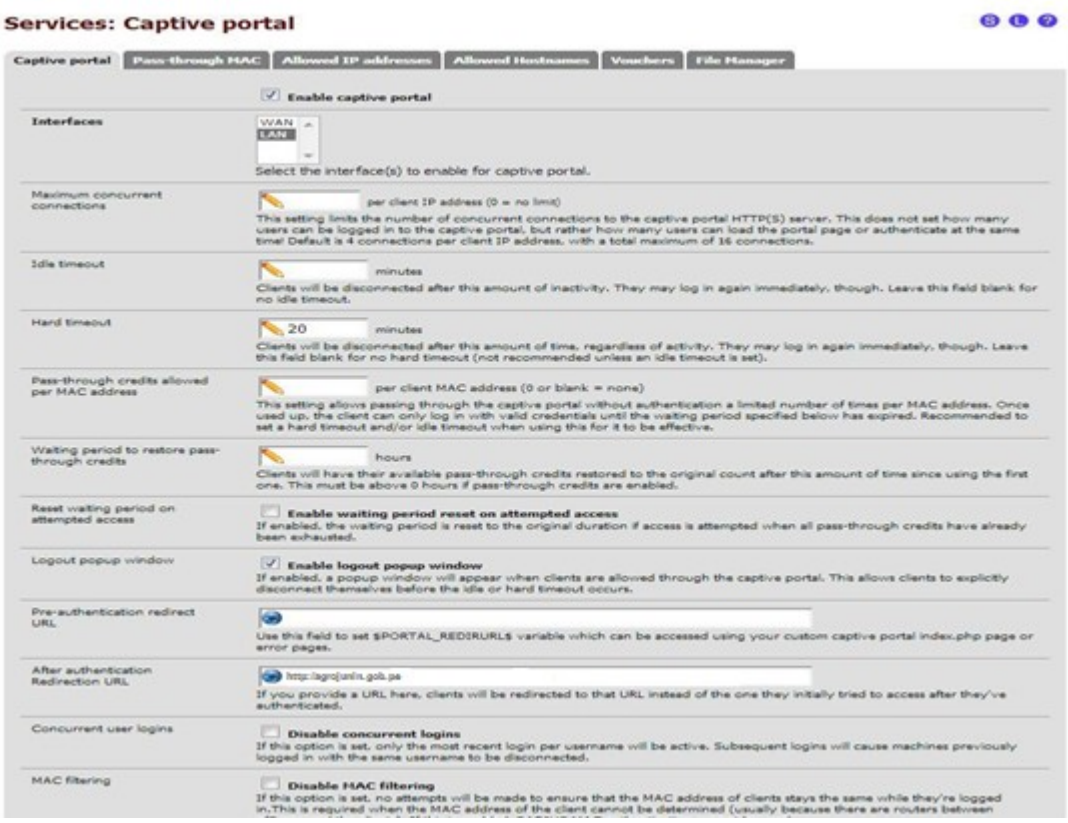
La política establecida, es que los equipos móviles del personal de la institución puedan conectarse a la red inalámbrica de forma automática, para ello es

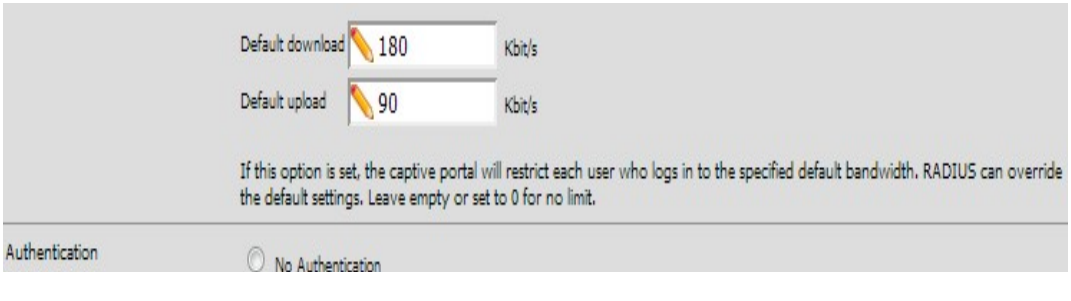
necesario que dichos usuarios se apersonen para registrar la dirección MAC de su equipo móvil.

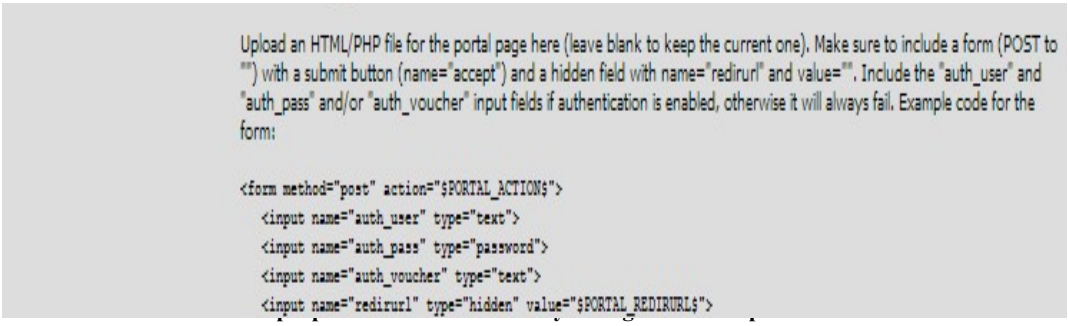
Para el caso de los ocasionales visitantes a la Institución podrán hacer uso de la red inalámbrica previo ingreso de un código, este código tendrá un tiempo de vida en minutos y luego de pasado ese tiempo se bloqueara el acceso a internet, de esta manera podremos garantizar la conectividad de cualquier personal de la Institución y que no saturen la red cuando no estén haciendo uso de la misma.

En el formulario de configuración de CAPTIVE PORTAL activamos el servicio, luego identificamos sobre que interface se aplicara este servicio, en este caso se selecciona, ingresamos la dirección web a donde se redirigirán los usuarios cuando logren el acceso a internet, activamos la opción que permitirá generar los códigos para el ingreso de los ocasionales visitantes a la institución, cargamos una página web por default para que muestre un mensaje informativo a los usuarios que deben ingresar su código para navegar, con estas consideraciones se guarda su configuración, ya tenemos la configuración general de la conexión inalámbrica.

Hacemos clic en SERVICES ⌴ CAPTIVE PORTAL






Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "") with a submit button (name="accept") and a hidden field with name="redirurl" and value="". Include the "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail. Example code for the form:
<form method="post" action="$PORTAL_ACTION$">
<input name="auth_user" type="text">
<input name="auth_pass" type="password">
<input name="auth_voucher" type="text">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
Los vouchers son el nombre técnico que Captive Portal le da para identificar la generación de códigos para acceso a Internet, primero activamos los vouchers, luego especificamos los caracteres que tendrán los códigos a generar, los demás valores se dejan por defecto, y se guarda la configuración, luego se procede a generar los vouchers según se va necesitando.
Services: Captive portal: Vouchers
Captive portal
Pass-through MAC
Allowed IP addresses
Allowed Hostnames
Vouchers
File Manager
Enable Vouchers
Voucher Rolls
Roll #
Minutes/Ticket
# of Tickets
Comment
Voucher private key
-----BEGIN RSA PRIVATE KEY-----
MD4CAQACCQDwHmQQ2bvuxwIDAQABAgh7X5IXX/MDKQIFAPq0geUCBQD1VdQbAgQW
//4BAgUAvEMvrwIEKcbqxQ==
-----END RSA PRIVATE KEY-----
Paste an RSA private key (64 Bit or smaller) in PEM format here. This key is only used to generate encrypted vouchers and doesn't need to be available if the vouchers have been generated offline. Generate new key.

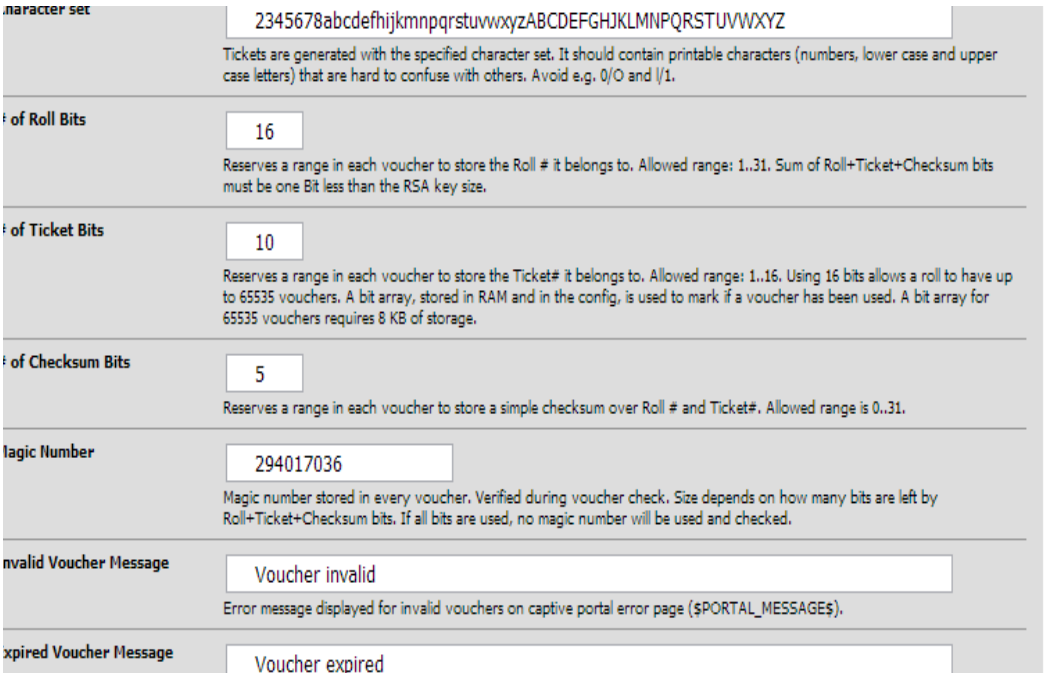


Figura 5.11 – Configuración y generación de vouchers.

Elaboración propia Fuente: Instalación y configuración de pfsense

Para poder registrar las direcciones MAC de los usuarios que estén autorizados se utilizará el formulario de la opción PASS-THROUGH MAC, donde se podrá especificar el equipo de cada usuario:

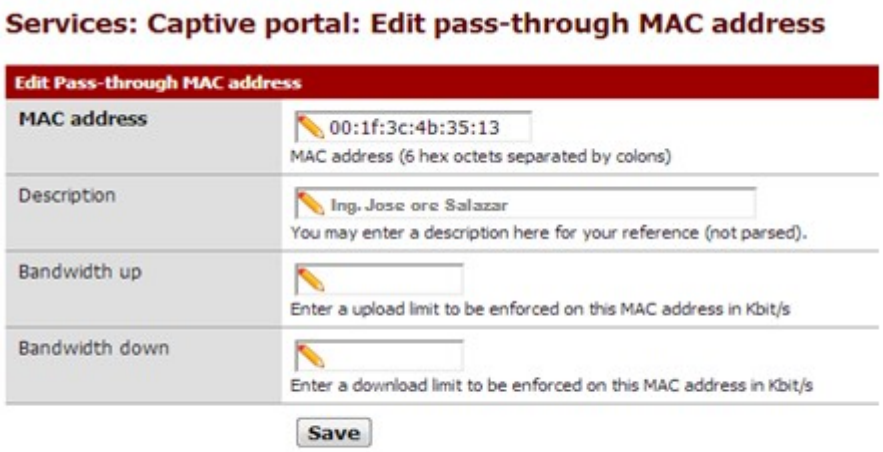
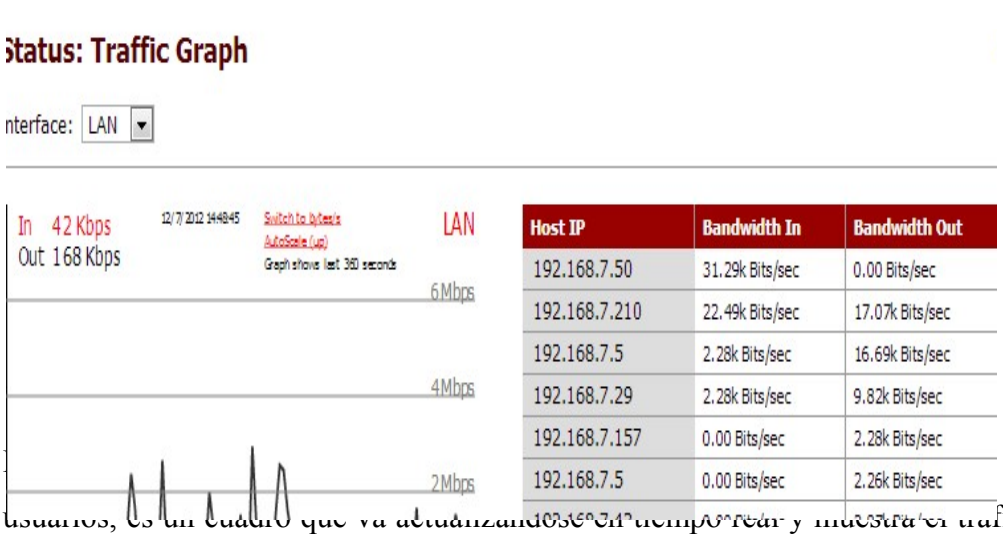


Figura 5.12 – Formulario para registro de MAC de los usuarios móviles.

Elaboración propia Fuente: Instalación y configuración de pfsense

5.5.5. MONITOREO Y SEGUIMIENTO

PFSense dispone de varias herramientas para poder realizar el monitoreo y seguimiento a la red, en la opción STATUS ▭ TRAFFIC GRAPH se mostrara una gráfica estadística que muestra en tiempo real el tráfico de la red hacia internet a través del tiempo, viene acompañado de una tabla donde se muestra las direcciones IP que originan el tráfico y su consumo:



los usuarios, es un cuadro que va actualizándose en tiempo real y muestra el tráfico en la red identificando el protocolo utilizado, el origen y fuente del tráfico, estado de la conexión, tiempo en milisegundos, numero de paquetes y el trafico

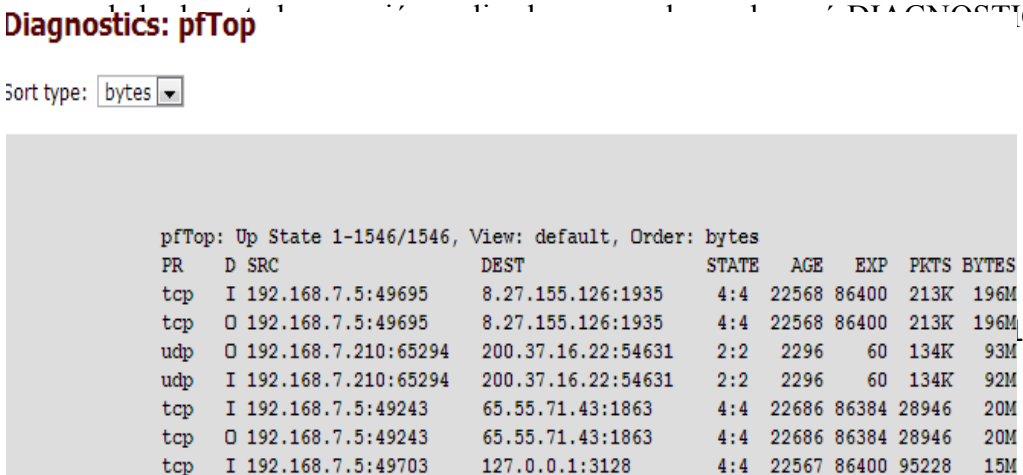


Figura 5.14 – Monitoreo del tráfico con pftop.
Elaboración propia Fuente: Instalación y configuración de pfsense

Se puede monitorear las direcciones de red que han sido asignadas de forma automática y su estado, para ello se hace clic en STATUS ␣ DHCP LEASES:

Status: DHCP leases

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.7.3	00:50:ba:39:c5:56 *D-link*	LC_Raul2Nic	n/a	n/a	online	static
192.168.7.4	00:19:d1:9d:18:1b *Intel*	AA_Server	n/a	n/a	online	static
192.168.7.5	00:1c:c0:b1:d6:eb *Intel Corporate*	LC_Raul	n/a	n/a	online	static
192.168.7.6	00:1c:c0:39:cf:f7 *Intel Corporate*	LC_Carlos	n/a	n/a	online	static
192.168.7.8	00:16:35:af:fa:c0 *Hewlett-Packard Company*	SERVER	n/a	n/a	online	static
192.168.7.10	00:06:f4:06:b7:a0 *Prime Electronics & Satellitics*	AP_PYSOC	n/a	n/a	online	static
192.168.7.11	00:1d:09:b2:2b:03 *Dell*	Gerente	n/a	n/a	online	static
192.168.7.12	00:1c:c0:37:bc:76 *Intel Corporate*	Secretaria Gerente	n/a	n/a	online	static
192.168.7.13	00:1c:c0:a5:bc:be *Intel Corporate*	SD_SecretariaCable	n/a	n/a	online	static
192.168.7.15	00:1c:c0:a3:d3:a6 *Intel Corporate*	PYSC_ElenaCable	n/a	n/a	online	static
192.168.7.18	00:1c:c0:b0:0a:f1 *Intel Corporate*	SD_Jefe	n/a	n/a	online	static
192.168.7.19	00:1c:c0:7a:38:de *Intel Corporate*	PYSC_Jefe	n/a	n/a	online	static

Status: DHCP leases

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.8.130	00:90:4c:14:43:29	android_5242bcd5d7f42a32	2012/12/07 14:42:21	2012/12/07 15:12:21	offline	active
192.168.8.167	e4:d5:3d:2d:97:fe	eventoscrizz-PC	2012/12/07 14:35:21	2012/12/07 15:05:21	online	active
192.168.8.197	8c:a9:82:b7:f0:50	USER-PC	2012/12/07 14:34:02	2012/12/07 15:04:02	online	active
192.168.8.163	0c:ee:e6:d8:4a:6b	Dhavid-PC	2012/12/07 14:33:15	2012/12/07 15:03:15	online	active
192.168.8.104	00:1e:4c:a4:bf:6e	dennis	2012/12/07	2012/12/07	online	active

Figura 5.16 – Estado de las direcciones IP de la red inalámbrica.
Elaboración propia Fuente: Instalación y configuración de pfsense

El monitoreo a la red inalámbrica también es importante, se puede visualizar los usuarios activos y el tiempo que llevan, para ello se hace clic en STATUS

␣CAPTIVE PORTAL:

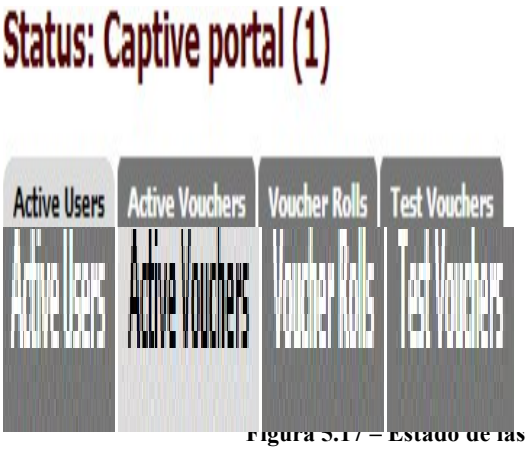


Figura 5.17 – Estado de las conexiones inalámbricas.
Elaboración propia Fuente: Instalación y configuración de pfsense

Debido a que los códigos para ingresar a la red inalámbrica tienen un tiempo de vida es necesario monitorearlos para volver a generar nuevos códigos. Para saber el estado de cada código hacemos clic en el menú STATUS ␣ CAPTIVE

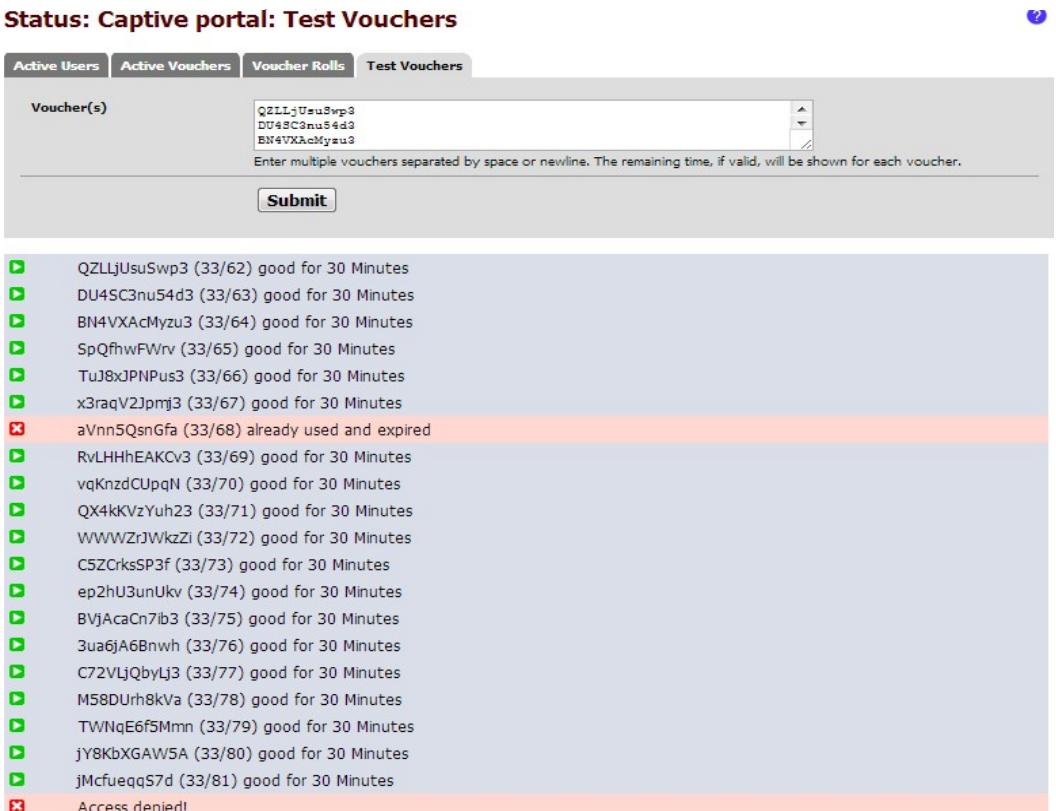


Figura 5.18 – Estado de los códigos (vouchers) para la red inalámbrica.
Elaboración propia Fuente: Instalación y configuración de pfsense

Así como existen herramientas para monitoreo en línea, también se tiene un sistema de registro (SYSTEM LOGS) para realizar análisis de lo que sucede en la red, este sistema permite monitorear el funcionamiento de toda la red según lo que se va configurando, se ingresa por el menú STATUS ⎵ SYSTEM LOGS:

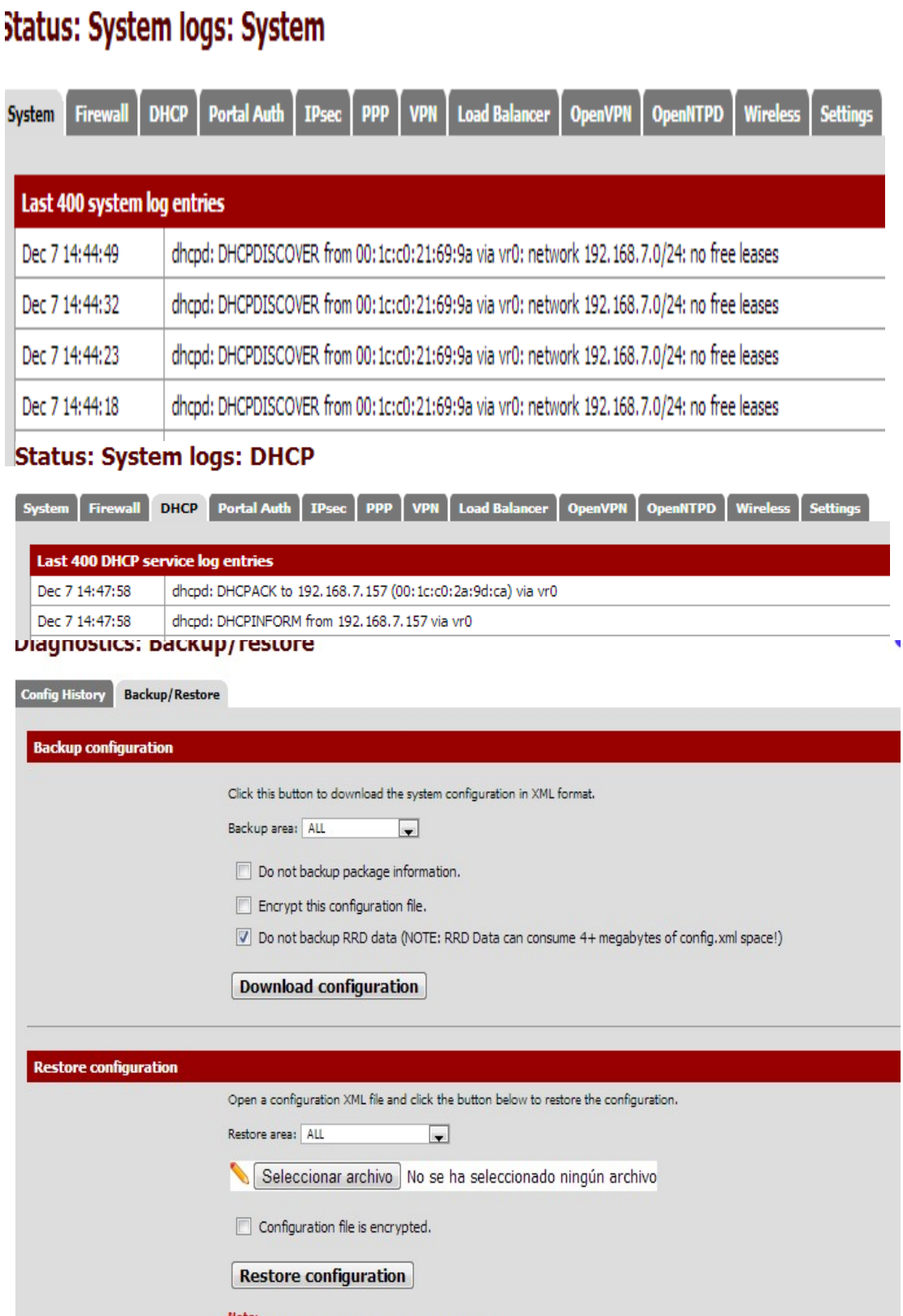


Figura 5.21 – Utilidad para generar y/o restaurar copias de seguridad.
Elaboración propia Fuente: Instalación y configuración de pfsense

5.6. DESCRIPCIÓN DEL SISTEMA DE SEGURIDAD

Desde la concepción del uso del aire como medio de transmisión en las redes inalámbricas, la mayor tarea de investigación y desarrollo ha sido ofrecer un nivel de seguridad adecuado para esta nueva tecnología. Ningún tipo de red es 100% segura, incluso las redes con cables sufren distintos tipos de vulnerabilidades. Las redes inalámbricas son aún más vulnerables que las redes con cables, debido a que la propagación de la señal es en todas las direcciones y es fácil el acceso a la misma.

La seguridad de las redes debe cumplir con tres objetivos primordiales:

- Confidencialidad

  Es el término utilizado para describir los datos que se encuentran protegidos ante la intercepción de cualquier parte no autorizada.
- Integridad

  Significa que los datos no han sido modificados desde el emisor hasta el receptor.
- Autenticación

  Es la base en cuestiones de seguridad, pues parte de la fiabilidad de los datos es conocer con certeza el origen.

Con el diseño del sistema de la red inalámbrica que se está proponiendo, el sistema de seguridad será manejado a través del servidor y por el portal cautivo,

adicional a eso se configurara los puntos de accesos inalámbricos (Access Point) para brindar una mayor protección y seguridad a la red de la Institución

5.6.1. POLÍTICAS DE SEGURIDAD

Aparte de las medidas que se hayan tomado en el diseño del HotSpot debemos aplicar ciertas normas y políticas de seguridad basadas en el estándar ISO 27001 para la seguridad de la información y mejores prácticas descritas en ISO/IEC 27002, para la Dirección de Titulación de Tierras y Catastro Rural.

- **Acuerdos de confidencialidad**

  [ISO/IEC 27001:2005 A.6.1.5]

Todos los funcionarios de la Dirección de Titulación de Tierras y Catastro Rural deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Acceso a Internet

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no, con las actividades propias de la Dirección de Titulación de Tierras y Catastro Rural, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio.
- El intercambio no autorizado de información de propiedad de la Dirección de Titulación de Tierras y Catastro Rural de sus usuarios y/o de sus funcionarios, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, información y/o productos que de alguna forma atenten contra la integridad,

disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Jefe respectivo o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b) La institución debe realizar un monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación.
c) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, responsable, y sin afectar la productividad ni la protección de la información de la Dirección de Titulación de Tierras y Catastro Rural.

Correo electrónico

Los funcionarios autorizados a quienes la Dirección de Titulación de Tierras y Catastro Rural les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera responsable y sin afectar la productividad.
b) Los mensajes y la información contenida en los buzones de correo son propiedad de la institución y cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
c) El tamaño de los buzones de correo es determinado por la institución de acuerdo con las necesidades de cada usuario y previa autorización del Jefe de la dependencia correspondiente
d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por la institución.
e) No está permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico que atenten contra la productividad o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos, y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Utilizar la dirección de correo electrónico de la institución como punto de contacto en comunidades interactivas de contacto social, tales como Facebook y/o myspace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva.

f) El envío de información debe ser realizado exclusivamente desde la cuenta de correo que la institución proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

g) Toda información de la institución generada con los diferentes programas y sistemas computacionales (Ej. Office, AutoCAD, SSET, Catastro virtual, etc.), que requiera ser enviada fuera de la entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por la institución. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por la institución a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la institución es responsabilidad del área de informática, y por tanto son los únicos autorizados para realizar esta labor.
b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios pueden ser realizados únicamente por el área de informática.
c) El área de informática debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
d) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la

infraestructura tecnológica de la institución, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de informática.

e) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la institución; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidas por el área de informática.

- **Control de acceso físico**

  [ISO /IEC 27001:2005A.9.1]

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones

- **Protección y ubicación de los equipos**

  [ISO/IEC 27001:2005A.9.2]

Los equipos que hacen parte de la infraestructura tecnológica de la institución tales como computadoras, equipos de uso personal y sus periféricos, servidores, puntos de acceso, centros de cableado, UPS, así como estaciones de trabajo y dispositivos de almacenamiento que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

- **Protección contra software malicioso**

  [ISO /IEC27001:2005 A.10.4]

La Dirección de Titulación de Tierras y Catastro Rural establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Así mismo, la Dirección de Titulación de Tierras y Catastro Rural define los siguientes lineamientos:

a) No está permitido:

• La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por la institución.

• Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

- **Copias de respaldo**

  [ISO/IEC 27001:2005 A.10.5]

La Dirección de Titulación de Tierras y Catastro Rural debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el área de informática. y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

- **Gestión de medios removibles**

  [ISO/IEC 27001:2005 A.10.7]

El uso de medios de almacenamiento removibles (como por ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, etc) sobre la infraestructura para el procesamiento de la información de la institución, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera. Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la institución que éste contiene.

- **Intercambio de información**

  [ISO/IEC 27001:2005 A.10.8]

Todo funcionario de la institución es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

- **Gestión de contraseñas de usuario**

  [ISO/IEC 27001:2005 A.11.2.3]

Todos los recursos de información críticos de la institución tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones. Todo funcionario que requiera tener acceso a los sistemas de información de la institución debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la institución. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

CONCLUSIONES

Conclusión al Objetivo General:

- ✓ Se llegó a la conclusión que sería factible la implementación de un HotSpot en la Dirección de Titulación de Tierras y Catastro Rural, el cual contribuirá a mejorar el sistema de comunicación mediante el uso de las redes inalámbricas, las cuales permitirán brindar acceso a la información de manera oportuna y segura. El diseño garantiza la conectividad de red y el acceso del personal a internet y a los servicios que la institución requiera permitiendo el beneficio de los trabajadores y sobre todo de los usuarios.

Conclusiones a los objetivos específicos:

- ✓ Se realizó un análisis de la tecnología adecuada para la implementación de un HotSpot en la Dirección de Titulación de Tierras y Catastro Rural llegando a la conclusión que el estándar 802.11G es el adecuado por tener mayores beneficios, así como modularidad, escalabilidad, rendimiento y calidad de servicio.
- ✓ La Dirección de Titulación de Tierras y Catastro Rural cuenta con una infraestructura muy antigua por lo que se realizó un análisis exhaustivo de la misma, concluyendo con la ubicación estratégica de las estaciones (Access Point) considerando principalmente la cobertura de la señal.
- ✓ Tomando en cuenta la información económica del área de presupuesto de la Dirección de Titulación de Tierras y Catastro Rural se llegó a la conclusión de que los costos de la implementación sean de acuerdo al presupuesto fijado para dicha entidad, considerando las necesidades del entorno y capacidades adquisitivas.

Así mismo se plantea el uso de un portal cautivo para la administración de la red inalámbrica de la Dirección de Titulación de Tierras y Catastro Rural es una opción con grandes beneficios, ya que permitirá el ingreso a la red únicamente a usuarios registrados en el sistema, evitando el acceso de personas ajenas a la institución. El monitoreo de uso de red es importante, ya que podremos ver el estado de las conexiones y consumo del ancho de banda, permitiendo además asignar de manera personalizada a cada usuario un determinado límite de velocidad de navegación, pudiendo de esta manera evitar lentitud de navegación dentro de la red inalámbrica.

Debemos tomar en cuenta que las conexiones que quedan abiertas en los puntos de acceso a las redes inalámbricas producen congestionamiento del servicio, esta herramienta da un tiempo de caducidad a cada conexión, evitando estos contratiempos y optimizando la calidad del servicio.

Luego de haber analizado las necesidades del personal de la institución, la seguridad a la misma es de gran importancia, por lo que las medidas para la prevención ante ataques, infecciones por virus y de más otros problemas a la red deben de hacerse de manera inmediata. Una red de estas características debe tener estándares de seguridad que garantice a los usuarios de la misma manera tener sus equipos libres de este tipo de infecciones o ataques.

RECOMENDACIONES

Recomendación al Objetivo General:

- ✓ Se recomienda la capacitación del personal en el uso de las redes inalámbricas como en el acceso a internet implantando políticas de seguridad.

Recomendaciones a los Objetivos Específicos:

- ✓ Se recomienda el uso del estándar 802.11g ya que es totalmente compatible con los productos desarrollados en la versión anterior 802.11b y que puede soportar equipos antiguos y modernos.
- ✓ Se recomienda reestructurar los ambientes de la institución para mejor ubicación y rendimientos de los equipos inalámbricos.
- ✓ Se recomienda invertir económicamente en la mejora de equipos informáticos.

Se recomienda concientizar a los usuarios la importancia de mantener sus claves seguras como normas básicas, evitando anotaciones como recordatorio o que no deban facilitárselas a otras personas ya que afectaría a la seguridad de la información.

Así mismo se recomienda que el área de instalación de los equipos (servidores) debe poseer una apropiada instalación eléctrica así como también elementos de respaldo como sistemas de alimentación ininterrumpida (UPS).

Para el uso del portal cautivo se recomienda activar JavaScript en los navegadores ya que algunos lo traen desactivado por defecto, para el correcto funcionamiento de las páginas web.

Se recomienda cumplir y hacer cumplir las políticas de seguridad establecidas por la organización para garantizar la seguridad de la red.

BIBLIOGRAFÍA

[1] **PABLO GIL / JORGE POMARES / FRANCISCO CANDELAS**
2010 "Redes y Transmisión de Datos"

[2] **JOSE M. HUIDOBRO MOYA**
2008 "Redes de área local: Administración y Sistemas Informáticos" 2da Edición Madrid España

[3] **IEEE**
2009 IEEE 802.11 Standard Wireless

[4] **MINISTERIO DE TRANSPORTES Y COMUNICACIONES - PNAF**
http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_115.pdf

[5] **Cisco Networking Academy**
2008 Wireless LAN Fundamentos_v1.02.
San Jose, CA: Cisco Press.

[6] **FOROUZAN, BEHROUZ A**.
2008 "Transmisión De Datos Y Redes De Comunicaciones."
España: McGraw-Hill.

[7] **Cisco Networking Academy**
2010 CCNA 3 Exploration 4.0, LAN Switching and Wireless.
San Jose, CA: Cisco Systems.

[8] **PHILIPPE ATELIN, JOSÉ DORDOIGNE**
2006 "Redes Informáticas: Conceptos Fundamentales: Normas, Arquitectura, Modelos OSI TCP/IP Ethernet Wifi.

[9] **ING. VICENTE ALAPON MIGUEL**
2007 "Seguridad en redes Inalámbricas"
Universidad de Valencia

[10] **ING. JEAN POLO CEQUEDA OLAGO**
2013 **"**Diseño e Implementación de un Sistema de Seguridad Perimetral para una Empresa usando la herramienta Pfsense"
colombia

[11] **DIRECCIÓN REGIONAL DE AGRICULTURA JUNÍN**
2013 http://agrojunin.gob.pe/

[12] **PETT**
http://www.minag.gob.pe/portal/marco-legal/normas-legales66/directiva-de-organo/70-titulacion-agraria-en-el-peru/414-el-pett

[13] **ENRIQUE DE MIGUEL PONCE, ENRIQUE MOLINA TORTOSA, VICENTE MOMPO MAICAS**
2006 "Redes Inalámbricas IEEE 802.11"

[14] **REID NEIL y SEIDE RON.**
2005 "Manual de Redes Inalámbricas 802.11 (Wi-Fi)" 2da Edición
México: McGraw-Hill

[15] **Cisco Networking Academy**
2009 CCNA 1 Exploration 4.0, aspectos básicos de redes.
San Jose, CA: Cisco Systems.

[16] **Cisco Networking Academy**
2009 CCNA 2 Exploration4.0, Routing Protocols and concepts.
San Jose, CA: Cisco Systems.

[17] Cisco Networking Academy

2010 CCNA 4 Exploration 4.0, Accessing the WAN.
San Jose, CA: Cisco Systems.

GLOSARIO

AD-HOC: Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.

AP: Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable. También se utiliza para ampliar el alcance de una red inalámbrica.

CRC: (Control de redundancia cíclica) Es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida.

CSMA/CD: Sensor de portadora de accesos múltiples con detección de

colisiones. Método de transmisión de datos en donde todas las estaciones pueden mandar datos con una señal eléctrica sumada (portadora). En caso de que existan transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.

DHCP: Protocolo para la configuración automática de los parámetros de red de los equipos. La información se almacena en un servidor DHCP al que los equipos, al encenderse, solicitan los parámetros de configuración.

EAP: Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.

ESSID: El ESSID es el nombre identificador de una red inalámbrica, es estrictamente el nombre para identificar un punto de acceso inalámbrico. Permite que una red inalámbrica para poder diferenciarse claramente de otro.

FIRMWARE: Programación en Firme, es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

IEEE: Instituto independiente que desarrolla estándares de redes. Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas.
Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN.

IP: Protocolo utilizado para enviar datos a través de una red.

ISP: Internet Service Provider. Proveedor de Servicio Internet. Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.

LAN: La Red de Área Local (LAN) es una pequeña red de datos que cubre un área limitada, tal como un edificio o grupo de edificios. La mayoría de las LAN conectan

estaciones de trabajo o computadoras personales. Esto permite a muchos usuarios compartir dispositivos, tales como impresoras de rayo láser así como datos. La LAN también permite comunicación fácil, facilitando el correo electrónico (e-mail) o respaldando sesiones de conversación (Chat).

MAC: Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.

MIC: Es un procedimiento de modulación utilizado para transformar una señal analógica en una secuencia de bits.

MULTICAST: Multidifusión es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

NIC: Una tarjeta de red permite la comunicación entre diferentes aparatos conectados entre sí y también permite compartir recursos entre dos o más equipos (discos duros, CD-ROM, impresoras, etc). A las tarjetas de red también se les llama adaptador de red.

PCI: Interconexión de Componentes Periféricos, consiste en un bus de ordenad estándar para conectar dispositivos periféricos directamente a su placa base. Estos dispositivos pueden ser circuitos integrados ajustados en ésta o tarjetas de expansión que se ajustan en conectores.

PCIMCIA: Tarjeta estandarizada de expansión, del tamaño de una tarjeta de crédito, utilizada en ordenadores personales. En telecomunicaciones, uno de sus principales usos es la transmisión de mensajes, datos y faxes a través de computadoras portátiles y teléfonos móviles.

PDA: Ordenador de pequeño tamaño cuya principal función era, en principio, mantener una agenda electrónica. No obstante, cada vez más se va confundiendo con los ordenadores de mano y de palma.

PSK: La modulación por desplazamiento de fase es una forma de modulación angular

que consiste en hacer variar la fase de la portadora entre un número de valores discretos.

RADIUS: Protocolo que utiliza un servidor de autenticación para controlar acceso a redes.

RF: El término radiofrecuencia, también denominado espectro de radiofrecuencia, se aplica a la porción menos energética del espectro electromagnético, situada entre unos 3 Hz y unos 300 GHz.

ROAMING: Nombre dado a la acción de moverse del área de cobertura de un Punto de Acceso a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.

SSID: Conjunto alfanumérico de hasta 32 caracteres que identifica el nombre de una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.

TKIP: Protocolo de cifrado inalámbrico que cambia periódicamente la clave cifrado, haciendo más difícil su decodificación.

VPN: La Red Privada Virtual, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

WEP: Es un protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro. Para permitir la comunicación entre los equipos y el enrutador se utiliza una clave compartida (similar a una contraseña). WEP ofrece un nivel básico (pero satisfactorio) de seguridad para la transferencia de datos a través de redes inalámbricas.

WIFI: Es una de las tecnologías de comunicación inalámbrica (sin cables – wireless) más extendidas. También se conoce como WLAN o como IEEE 802.11.

WLAN: Utilizando tecnología de radio frecuencia (RF), las WLAN transmiten y reciben datos de forma inalámbrica en una cierta área. Esto permite a los usuarios en una zona pequeña transmitir datos y compartir recursos, tales como impresoras, sin conectar físicamente cada computadora con cables o alambres.

WPA: Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. Asegura la transferencia de datos de forma inalámbrica mediante la utilización de una clave similar a WEP. La robustez añadida de WPA es que la clave cambia de forma dinámica. La clave, en continuo cambio, dificulta que un pirata informático pueda conocer la clave y obtener acceso a la red.

ANEXOS

Anexo 01

Recursos Humanos			
	Hora	Costo/Hora	Total
1 técnico	40	S/. 10.00	**S/. 400.00**
Hardware			
		Precio x unidad	Total
1 ROUTER D-link DI-624 108Mbps		S/. 76.16	S/. 76.16
3 ACCESS POINT DWL - 2100AP		S/. 76.16	S/. 228.48
3 2.4GHz 12dBi ANTENA OMNIDIRECCIONAL para exteriores TL-ANT2412D		S/.200.00	S/. 600.00

10 D-Link DWA-525 Adaptador PCI Wireless N 150		S/. 40.00	S/.400.00
1 D-Link DGE-528T TARJETA RED PCI Gigabit Ethernet 10/100/1000 Mbps		S/. 50.00	S/. 50.00
2 PATCH CORD 30m		S/. 11.00	S/. 11.00
3 CAJAS PARA EXTERIORES		S/. 52.00	S/.156.00
		TOTAL	**S/.1921.64**
Software			
WINDOWS XP/WINDOWS 7			S/. 392.00
Licencia de uso de frecuencia electromagnética Ministerio de Transportes y Comunicaciones			Gratuita
Gastos Varios			
Transporte			S/. 20.00
Copias			S/. 10.00
Imprevistos			S/. 40.00
Alimentación			S/. 40.00
TOTAL			**110.00**
Valor calculado para una persona:			**S/.2423.64**

El costo estimado de los equipos para una futura implementación:

Anexo 02

Equipos que se utilizaran para una futura implementación:

ROUTER D-link DI – 624/108Mbps El router D-Link cuenta con una velocidad de transmisión de datos de 54 Mbps y Trabajando bajo los estándares 802.11b y con el 802.11g, es compatible con cualquier producto de otros fabricantes, y a su vez posee firewall con un alto nivel de seguridad.	

ACCESS POINT D-link DWL - 2100AP El Dlink DWL-2100AP es un punto de acceso, que responde al estándar 802.11g, operando con un ancho de banda 108Mbps, y que gracias al nuevo Chip de Atheros puede alcanzar unas tasas de transferencia quince veces superior -15x* - que una red inalámbrica tradicional de 11Mbps, interopera en forma transparente con cualquier producto Dlink o con cualquier producto de otros fabricantes, bajo el estándar 802.11b y con el estándar 802.11g. En conjunto con las altas tasas de transferencia, un muy buen nivel de seguridad, hacen del DWL-2100AP la solución ideal para la nueva tecnología, además de proteger las inversiones wireless ya hechas. El punto de acceso DWL-2100AP incorpora mecanismos adicionales de seguridad, tales como Wi-Fi™ Protected Access (WPA), WEP y 802.1x, que en conjunto con un servidor Radius proporcionan un mayor nivel de seguridad.	
D-Link DGE-528T TARJETA RED PCI Gigabit Ethernet 10/100/1000 Mbps La tarjeta de red PCI es la opción propuesta por D-Link para habilitar estaciones de trabajo a Gigabit y que proporciona al usuario hasta 2000Mbit de trasmisión de datos en Full / Dúplex. La DGE-528T es una solución alternativa y económica a la conexión de fibra, proporcionando velocidad Gigabit y seguridad.	
D-Link DWA-525 ADAPTADOR PCI Wireless N 150 El Adaptador PCI Wireless N 150 permite la creación de redes inalámbricas de alto rendimiento en ordenadores de escritorio. Una vez conectadas, este adaptador puede utilizar Internet de alta velocidad y al mismo tiempo compartir documentos, música y fotos en tu red.	

2.4GHz 12dBi ANTENA OMNIDIRECCIONAL para exteriores TL-ANT2412D La antena ominidireccional para exteriores emite una poderosa señal amplificada en un radio de 360 grados, entregando una señal fuerte multidirección de un punto de acceso o un puente.. Es más efectivo cuando se coloca en la parte superior de los edificios.	
Patch Cord 110 IDC Los Patch Cables 110 IDC se pueden usar en cualquier sistema que considere bloques del tipo 110 IDC para la terminación de cables. También se puede administrar con este producto la conexión entre sí de equipos de PABX con cables telefónicos convencionales.	
DAP – 3220 Wireless 108 G Exterior Access Point El DAP-3220 está diseñado para manejar una amplia variedad de ambientes al aire libre. Tiene una caja impermeable die-cast, un calefactor integrado y un sensor de temperatura. Soporta 802.3af Power over Ethernet (PoE), se puede colocar en lugares al aire libre donde las tomas de corriente no son fácilmente accesibles.