UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Proyecto Técnico previo a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:

IMPLEMENTACIÓN DE UN SERVIDOR RADIUS EN WINDOWS SERVER PARA CENTRALIZAR LA ADMINISTRACIÓN DE NUEVOS ACCESS POINTS EN LAS OFICINAS REMOTAS DE GALPONES Y HUERTOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL GUAYAS

AUTORES:

YUREMA NATHALIE TOBAR ESPINOZA
GERARDO ANTONIO MORA CEDEÑO

DIRECTOR:

ING. HUILCAPI SUBÍA DARÍO FERNANDO

Guayaquil, noviembre de 2016

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Nosotros, Yurema Nathalie Tobar Espinoza y Gerardo Antonio Mora Cedeño, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además, declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad los autores.

.....	.....
Yurema Nathalie Tobar Espinoza	Gerardo Antonio Mora Cedeño
CC 0919569301	CC 0919542175

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Yurema Nathalie Tobar Espinoza, con documento de identificación N° 0919569301 y Gerardo Antonio Mora Cedeño, con documento de identificación N° 0919542175 manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de grado intitulado: "IMPLEMENTACIÓN DE UN SERVIDOR RADIUS EN WINDOWS SERVER PARA CENTRALIZAR LA ADMINISTRACIÓN DE NUEVOS ACCESS POINTS EN LAS OFICINAS REMOTAS DE GALPONES Y HUERTOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL GUAYAS", mismo que ha sido desarrollado para optar por el título de: Ingeniero de Sistemas en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....	.....
Yurema Nathalie Tobar Espinoza	Gerardo Antonio Mora Cedeño
CC 0919569301	CC 0919542175

CERTFICADO DE DIRECCIÓN DE TRABAJO

Honorable Consejo Académico de la Universidad Politécnica Salesiana Sede de Guayaquil

De mi consideración:

Por medio de la presente, informo que los estudiantes Yurema Nathalie Tobar Espinoza y Gerardo Antonio Mora Cedeño han desarrollado su proyecto técnico de acuerdo a lo aprobado en la Resolución N° 143-005-2016-03-03, con el tema: "IMPLEMENTACIÓN DE UN SERVIDOR RADIUS EN WINDOWS SERVER PARA CENTRALIZAR LA ADMINISTRACIÓN DE NUEVOS ACCESS POINTS EN LAS OFICINAS REMOTAS DE GALPONES Y HUERTOS DEL GOBIERNO AUTONOMO DESCENTRALIZADO DEL GUAYAS", cumpliendo de esta manera los objetivos respectivos.

En virtud de lo antes expuesto considero que el presente proyecto se encuentra habilitado para que los estudiantes se presenten al acto de la defensa respectiva.

Guayaquil, octubre del 2016

Ing. Darío Huilcapi Subía
Director Asignado

AGRADECIMIENTO

Agradezco a Dios por todo lo que me ha dado y por lo que no también, por darme unos padres ejemplares, unos abuelos incondicionales, hermanos maravillosos, mi pequeño sobrino, amigos inolvidables, y maestros que han sido parte de mi formación Universitaria.

Agradezco de manera muy especial a nuestro Director de Proyecto Técnico al Ing. Darío Huilcapi por su colaboración en distintas fases de este crecimiento profesional.

Y agradezco al Gobierno Provincial del Guayas y a los miembros de la Dirección Provincial de Tecnología de la Información y Comunicación – TICs, por facilitarnos la información, los equipos, las instalaciones y la confianza para realizar el proyecto técnico para nuestra graduación, en especial a ese amigo y compañero de vida que siempre estuvo apoyándome en cada etapa de mi vida.

Yurema Tobar Espinoza

AGRADECIMIENTO

Papito Dios, desde que nací has puesto en mi vida seres maravillosos:

Mis padres, compartiendo su tiempo conmigo, enseñándome nuevas cosas, a ser perseverante, inculcando principios y valores que servirán toda mi vida.

Mi hermano, aliado, confidente, compañero de aprendizaje y travesuras.

Mi querida esposa, compañera fiel en mis largas horas de estudio, motivación constante y apoyo incondicional.

Al Ing. Darío Huilcapi por aceptarnos para realizar el proyecto técnico bajo su dirección, su buena predisposición y su capacidad para guiar nuestras ideas han sido clave para alcanzar este objetivo.

Al Gobierno Provincial del Guayas y a los colaboradores de la Dirección Provincial de Tecnología de la Información y Comunicación – TICs: directores, jefes departamentales, personal técnico y administrativo, su experiencia y profesionalismo han sido fundamental para mi desarrollo personal y profesional.

Docentes, familiares y amigos siempre atentos y oportunos para brindar su ayuda.

A mi compañera de tesis, por su buena predisposición y ayuda para la consecución de este proyecto.

Dios les pague a todos.

Gerardo Mora Cedeño

DEDICATORIA

Dedico este trabajo, en primer lugar, a Dios por darme las fuerzas, la paciencia y el conocimiento para superar cualquier obstáculo que se me interpuso para lograr mi meta.

A mis padres y a mis abuelos, por todo el amor que me fue entregado, por su apoyo incondicional para cada meta que me he trazado, por ser mis pilares fundamentales para cualquier decisión que vaya a tomar durante mi existencia.

A mis hermanos, por inspirarme que cada día sea mejor y demostrarle que cualquier obstáculo puede ser superado si estamos con Dios, a mi pequeño sobrino que llegó a llenar nuestras vidas de mucho amor y esperanza.

También a mis amigos por siempre escucharme y compartir momentos inolvidables. Y a esa persona especial que ha estado durante toda mi etapa universitaria y me ha apoyado e inspirado a crecer cada vez más como ser humano y profesional, usted sabe quién es.

Yurema Tobar Espinoza

DEDICATORIA

Al constructor del pensamiento, al arquitecto y dueño de mi vida. Contigo todo es posible.

A ti querido Padre Celestial.

Gerardo Mora Cedeño

RESUMEN

El Gobierno Autónomo Descentralizado Provincial del Guayas se encuentra en constante modernización de su infraestructura tecnológica, buscando proveer a sus funcionarios de alta conectividad que facilite acceso a los servicios informáticos.

El principal enfoque de este proyecto técnico fue identificar, analizar y proponer la implementación de un servidor RADIUS para centralizar la administración de los Access Point. Implementar medidas de seguridad y centralizar la administración mediante la utilización de tecnologías de información y comunicaciones de las diferentes oficinas y sucursales de una organización es fundamental en el manejo y optimización de recursos de la empresa. Esta implementación supone un cambio mínimo en la infraestructura física de la red, reduce costos, facilita la escalabilidad y brinda la oportunidad de acceso inalámbrico a la información y a las aplicaciones institucionales en todo momento y desde cualquier sitio de la Prefectura, ayudando así a incrementar la productividad.

Para el desarrollo del proyecto se recopila información de la situación actual y mediante entrevistas se identifica los requerimientos técnicos para conocer lo que se espera de la solución. Se implementará en un Windows Server el rol NPS para establecer a dicho servidor como un servidor RADIUS que interactúe tanto con la WLC como con el active directory.

Se puede mencionar que la controladora permite realizar el monitoreo, configuración, administración y control de los access point, por lo que se puede concluir que la metodología utilizada y los equipos seleccionados permitieron el cumplimiento de los objetivos.

ABSTRACT

The Autonomous and Decentralized Provincial Government from Guayas is always in constant modernization of the technological infrastructure, looking for ways to provide high connectivity to its employees which will improve their access to technological services.

The main focus of this technical project was identified, analyze and propose the implementation of a RADIUS server to centralize the management of every single access point. Implement security measures and centralize the management through the use of Communication and Information Technologies from the different offices and branches of an organization; is fundamental for the company's resources management and optimization. This implementation means a small change for the network's physical structure, reduce costs, make it easier the scalability and give the opportunity of wireless access to the information and company apps in every single moment and from every single place of the Prefectura, helping to increase the scalability.

For the developing of the project, is needed to gather the information of the current situation and through interviews identify the technical requirements to know what is expected of the solution. It is going to be implement on a Windows Server, role NPS to stablish that server as a RADIUS server which interact in WLC as well as in Active Directory.

Furthermore the controller will allow to monitor, configure, manage and control all the access points, concluding that the used methodology and the selected equipment allows the achieving of the objectives.

Índice General

Índice de Figuras

Índice de Tabla

1. Introducción.

El Gobierno Provincial del Guayas es una persona jurídica de derecho público que goza de autonomía política, administrativa y financiera. Está conformado por un prefecto, viceprefecto y el consejo provincial.

Según la misión institucional, el Gobierno Provincial del Guayas es:

> *Una institución provincial que fomenta, promueve y brinda, en el marco de la equidad, responsabilidad social y ambiental, obras y servicios que mejoran la calidad de vida de los guayasenses por medio de una gestión de procesos efectiva que permiten incrementar los niveles de progreso y desarrollo de nuestra provincia y sus habitantes.(Art.1 , 2015).*

Cuenta con una oficina matriz ubicada en las calles illingworth 108 y malecón (Esq.) y varias oficinas remotas cada una con su propia red local. Las redes locales están interconectadas entre sí a través de servicios de terceros mediante el uso de VPNs.

Son muchas las actividades que se llevan a cabo en los diferentes sitios del Gobierno Provincial del Guayas, que dependen de los servicios informáticos. La dirección provincial de tecnología de la información y comunicación – TICs, es la encargada de proveer de los medios de comunicación, así como de toda la infraestructura necesaria para mantener disponibles estos servicios.

El establecimiento de un gobierno electrónico forma parte del compromiso de la prefectura del Guayas con el país, para ello se planifican continuamente proyectos que contribuyan a que los servicios informáticos sean accesibles desde cualquier parte y a través de cualquier dispositivo.

En los últimos años ha existido un gran avance en lo que a tecnología inalámbrica se refiere, soportando cualquier tipo de servicio y haciendo posible que los usuarios tengan acceso móvil a la red de datos de la organización desde cualquier punto dentro de un área de cobertura.

Factores económicos y de infraestructura física limitan el crecimiento de la red cableada, por lo que el uso de tecnologías inalámbricas es una buena opción para el crecimiento de la red. Teniendo en cuenta que ha existido un sorprendente crecimiento de los equipos móviles como smartphone, laptops, tarjetas inalámbricas, entre otros.

2. Problema

El edificio principal donde funciona el Gobierno Provincial del Guayas, se ha ido adaptando para proveer a los funcionarios la conectividad requerida que permita el acceso a los diferentes servicios informáticos, sin embargo, los puntos de acceso no son suficientes para cubrir con la demanda de todos los usuarios que no sólo requieren conectividad para sus computadores sino también para dispositivos móviles.

Existen algunos servicios críticos de los que dependen las labores cotidianas, entre los que se pueden mencionar, por ejemplo, los sistemas SGP y SGP+, los cuales están disponibles para sus funcionarios por medio de la Intranet. Cada uno de estos sistemas cuenta con sus respectivos módulos personalizados para las diferentes áreas que tiene la Prefectura del Guayas.

Además del edificio matriz, la prefectura cuenta con otros sitios remotos:

- Galpones: Av. Pedro Menéndez Gilbert y Av. Plaza Dañín

- Huertos: Av. Pedro Menéndez Gilbert Mz. 7 Solar 2 frente a la puerta de Emergencia de Solca.
- CTP: Calle Alfredo Valenzuela (La 8va) y Venezuela, esquina del parque Puerto Lisa.
- Equinoterapia: Km 10 ½ vía a Samborondón, junto al hipódromo Miguel Salem.
- Medio Ambiente: Pichincha entre Elizalde e Illingworth, 4to piso.
- Bancopark: Luque 111 y Pichincha, piso 14.

En las oficinas remotas de galpones y huertos, operan diversos departamentos pertenecientes a la dirección provincial administrativa, así, por ejemplo:

- El Sistema de Gestión Pública (SGP), es utilizado por los departamentos de bodega de suministros, bodega de bienes y muebles y transporte.
- El Sistema de Gestión Pública Plus (SGP+), es utilizado por talleres y bodega general.

El departamento de talleres realiza órdenes de trabajo, solicitudes de pedidos a bodega sobre repuestos y accesorios para los vehículos.

La dirección TICs, ha implementado el uso de VLANs para gestionar más adecuadamente los diferentes segmentos de red definidos para los perfiles de acceso a la red. Así por ejemplo un dispositivo que no sea del Gobierno Provincial del Guayas se considera como un dispositivo invitado y sólo tiene acceso a Internet, más no a la red local. De igual forma, se mantiene a los servidores y bases de datos en VLANs independientes a las de las estaciones de trabajo. También se utiliza las VLANs para separar el tráfico de datos, del tráfico de voz y del tráfico de video.

En las oficinas remotas de galpones y huertos, falta acceso a algunos servicios que ofrece la red del Gobierno Provincial del Guayas tales como internet, intranet, debido a que no existen suficientes puntos de red ni puntos de acceso inalámbrico.

En la oficina matriz se cuenta con una controladora inalámbrica de marca cisco y con algunos access points de la misma marca, distribuidos en diferentes áreas para dar acceso inalámbrico a los usuarios.

La red inalámbrica existente sólo funciona para invitados y permite acceso a internet; sin embargo, también es necesario proveer de acceso a servicios de la red local e intranet en galpones y huertos.

2.1 Antecedentes

El problema radica en que no existe asignación de VLANs dinámicas en la red inalámbrica del Gobierno Provincial del Guayas. La red inalámbrica sólo funciona con la VLAN de invitados en la que solamente se tiene acceso a internet. Sin embargo, es necesario proveer de acceso a laptops de funcionarios para que puedan acceder a los sistemas y servicios de la red local e intranet.

Actualmente el Gobierno Provincial del Guayas cuenta con una oficina central, y varias oficinas remotas. Cada una, con su propia red local. Las redes locales están interconectadas entre sí a través de servicios de terceros mediante el uso de VPNs.

En cada oficina, cuentan con implementación de VLANs para separar el tráfico de red y manejar niveles de seguridad. Así por ejemplo, un dispositivo que no sea del Gobierno Provincial del Guayas se considera como un dispositivo invitado y sólo tiene acceso a internet, más no a la red local. De igual forma, se mantiene a los servidores y bases de datos

en VLANs independientes a las de las estaciones de trabajo. También se utiliza las VLANs para separar el tráfico de datos, del tráfico de voz y del tráfico de video.

En la oficina matriz se cuenta con una WLC de marca cisco y con algunos APs de la misma marca, distribuidos en diferentes áreas para dar acceso inalámbrico a la red de invitados, que está en la VLAN 66.

2.2 Importancia y alcances

Los beneficiarios del proyecto serían los empleados del Gobierno Provincial del Guayas, quienes podrán utilizar los diversos sistemas y servicios informáticos de manera segura a través de una red inalámbrica desde cualquier oficina.

El Gobierno Provincial del Guayas es una institución provincial que fomenta, promueve y brinda, en el marco de la equidad, responsabilidad social y ambiental, obras y servicios que mejoran la calidad de vida de los guayasenses por medio de una gestión de procesos efectiva que permiten incrementar los niveles de progreso y desarrollo de nuestra provincia y sus habitantes, además que presta servicios sociales y de infraestructura básica en calidad y cantidad adecuada y promueve la modernización de la gestión vial.

2.3 Delimitación

Los usuarios que se beneficiarían con el proyecto son todos los empleados de las oficinas remotas de huertos y galpones del Gobierno Provincial del Guayas, debido a que los usuarios de las oficinas remotas no cuentan con una red inalámbrica estable, y esto ocasiona inconvenientes para realizar sus actividades laborales, no todos tienen acceso a internet y adicional a esto no pueden acceder a los servicios que la institución cuenta, por lo que

necesita la utilización de VPN y tarjetas inalámbricas por el incremento de los dispositivos móviles como portátil, celular, tablet entre otros.

Adicionalmente, y aunque el acceso inalámbrico brinda movilidad y la oportunidad de acceder desde cualquier sitio de la prefectura, hay que tomar en cuenta la seguridad de dichos accesos, así como la gestión administrativa sobre los diferentes puntos inalámbricos de forma centralizada.

3. Objetivo General y Específico

3.1 Objetivo General

Implementar asignación dinámica de VLANs en la red inalámbrica mediante la instalación de un servidor RADIUS, usando un Servidor Windows, una WLC y un active directory.

3.2 Objetivos Especificos

- Implementar un servicio de autenticación.
- Optimizar los servicios del WLC y servidores de usuarios.
- Proveer cobertura de una red inalámbrica en huertos y galpones.

4. Revisión de la literatura o fundamentos teóricos o estado del Arte

La información obtenida ha sido en base de libros virtuales, sitios web oficiales, artículos o revistas virtuales, las cuales forman parte de la investigación y permiten plasmar un resumen de los temas más importantes para ejecutar y entender el proyecto técnico a realizar.

La red informática puede ser cableada o inalámbrica (sin la necesidad de la conexión por cable) y hacen posible que múltiples sucursales o instituciones combinen de forma

colaborativa sus recursos para resolver los problemas entre computadora o equipos o dispositivos informáticos.

Lehembre (2006) lo define así:

> *La tecnología WIFI (Wireless Fidelity), es una de las tecnologías líder en la comunicación inalámbrica y el soporte para Wi-FI se está incorporando en cada vez más aparatos: portátiles, PDAs o teléfonos móviles. De todas formas, hay un aspecto que en demasiadas ocasiones pasa desapercibido la seguridad.* (Guillaume Lehembre, 2006)

4.1.Redes Inalámbricas

Las redes inalámbricas (Wireless) son usadas en informática para designar la conexión de nodos sin necesidad de una conexión física, ésta se da por medio de ondas electromagnéticas. La transmisión y recepción se realizan a través de puertos y actualmente las redes inalámbricas son una de las tecnologías más prometedoras. Una de sus principales ventajas son los costos, ya que se elimina todo el cable ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

De acuerdo a Laurent-Maknavicius (2007*):*

> *En la cobertura de pequeñas o grandes son cada vez más populares, ya que prometer la esperada convergencia de servicios de voz y de datos al tiempo que proporciona movilidad a los usuarios. El primer gran éxito de las redes inalámbricas se vuelve a Wi- Fi (IEEE 802.11), que se abrió un canal de implementación rápida y sencilla de un local, red. Otras tecnologías inalámbricas como Bluetooth, WiMAX y WiMobile*

> *también muestran un futuro muy prometedor debido a la alta demanda de los usuarios en términos de movilidad y flexibilidad para acceder a todos sus servicios desde cualquier lugar. Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros. Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las paredes para pasar cables ni de instalar portacables o conectores. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.* (Laurent-Maknavicius, 2007*)*

Las redes inalámbricas permiten que los usuarios puedan mantenerse conectados cuando se desplazan dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad", adicional a esto no tendrían que invertir mucho para la implementación de esta alternativa.

4.2.Estándares de la IEEE 802

IEEE (Institute of Electrical and Electronics Engineers o en español Instituto de Ingenieros Eléctricos y Electrónicos), es una organización sin fines de lucro que se encarga de realizar normas y estándares en beneficio de las redes ya sean cableadas o inalámbricas, esto significa que una persona con un computador portátil puede conectarse inalámbricamente a una red, independiente de la marca o modelo del equipo y del país en que se encuentre.

Los estándares IEEE son normas internacionales que definen la forma de trabajar y desarrollar la tecnología que va evolucionando, en caso de que no existieran estas normas, cada fabricante de los equipos tecnológicos crearían sus propias normas y sería un caos por la incompatibilidad que existiría entre los diversos equipos.

*"Es por eso que IEEE se encargó de desarrollar normas en la cual aseguren el buen funcionamiento de los equipos, la interoperabilidad, la compatibilidad y la seguridad de dichos equipos tecnológicos. Adicional a esto las normas es una parte fundamental para comparar los productos de la competencia**.**" (IEEE STANDARS ASSOCIATION, 2016)*

"Muchas de las normas para la comunicación inalámbrica se están desarrollando día tras día y el precio de sus equipos es cada vez más atractiva. Esta voluntad contribuir al éxito de estas tecnologías. En esta sección, se introduce las normas que son la base de muchas redes inalámbricas." (Laurent-Maknavicius, 2007).

Tabla 1 Estándares IEEE 802

Estándar	Descripción
802.11a	Esta norma es una versión de la especificación IEEE 802.11, define una capa física, que se añadió un mayor rendimiento en enviar datos a 54 Mbps mediante el uso de la banda de 5 GHz para la transmisión. IEEE 802.11a especifica 8 canales de funcionamiento en esta banda de frecuencias. Se necesitaría muchos Access Point en este estándar para tener un área específica cubierta, especialmente si es grande.
802.11b	Este estándar utiliza la frecuencia de radio de señalización (2,4 GHz) que el original 802.11 estándar con 13 canales en Francia. Este estándar permite una gama de 300 m en un entorno al aire libre.
802.11e	Esta norma define un conjunto de mejoras de calidad de servicio para inalámbrica aplicaciones LAN a través de modificaciones en el control de acceso al medio (MAC) capa. Esta mejora permite la mejor calidad de transmisión de voz y aplicaciones de vídeo.
802.11f	Este estándar (también conocido como el Protocolo Punto Inter - Access) es una recomendación que describe una extensión opcional IEEE 802.11, que proporciona comunicaciones inalámbricas de acceso de punto entre múltiples proveedores sistemas. Este protocolo permite a los usuarios cambiar su punto de acceso cuando traspaso se produce.
802.11g	Se trata de un conjunto de estándares para redes de área local inalámbrica ordenador (WLAN) comunicaciones que operan en la 5 GHz y 2,4 GHz espectro público alzacuello.
802.11i	Esta, es una enmienda a la seguridad especificando estándar IEEE 802.11 mecanismos para redes inalámbricas. IEEE 802.11i hace uso de la Estándar de Encriptación Avanzado (AES) de cifrado de bloque, mientras que WEP y WPA utiliza el cifrado de flujo RC4. Propone diferentes tipos de cifrado protocolos para la transmisión.

Estándar	Descripción
802.11k	Se trata de una enmienda a la norma IEEE 802.11-2007 de recursos de radio administración. Se define y expone la información de radio y cadenas de facilitar la gestión y mantenimiento de una red LAN inalámbrica móvil. En una red conforme a 802.11k, si el punto de acceso (AP) tiene la más fuerte señal se carga a su plena capacidad, un dispositivo inalámbrico está conectado a una de los puntos de acceso infrautilizadas. A pesar de que la señal puede ser más débil, el general el rendimiento es mayor debido a un uso más eficiente se hace de la red recursos.
802.11n	Se trata de una enmienda propuesta que mejora la anterior 802.11 normas mediante la adición de MIMO y muchas otras características nuevas. Mejora significativamente la red incremento en el rendimiento de los datos en bruto máximo (PHY) tasa de 54 Mbit / s a un máximo de 600 Mbit / s.
802.15.1	Esto cubre la tecnología Bluetooth.
802.15.3	802.15.3a IEEE es un intento de proporcionar una mayor velocidad UWB (Ultra –Wide Banda) de capa física mejora modificación de IEEE 802.15.3 para las aplicaciones que impliquen formación de imágenes y multimedia.
802.15.4	Esta es la base para ZigBee, WirelessHART y especificación MiWi, que más intentos de redes ofrecen una completa. Ofrece una baja velocidad de datos con un precio bajo.
802.16a	Esto especifica el despliegue mundial de banda ancha Wireless Metropolitan Redes de área. Ofrece una capacidad de punto a multipunto en el 2-11 GHz banda. El estándar se extiende para incluir OFDM y OFDMA.
802.16d	Este es el estándar de revisión del 802.16 y 802.16a.
802.16e	Esta norma agrega la capacidad de movilidad de IEEE 802.16d añadiendo funciones avanzadas para el MAC y PHY capas.
802.20	Este estándar (también conocido como Mobile Broadband Wireless Access (MBWA)) permite que se instalen en todo el mundo de productos asequibles, ubicuo y siempre activo y redes interoperables de múltiples proveedores de banda ancha móvil de acceso inalámbrico que satisfacer las necesidades de los mercados de usuarios finales comerciales y residenciales.
802.21	Este estándar (también conocido como Medios Independientes de traspaso (MIH)) es del desarrollo de normas para permitir el traspaso y la interoperabilidad entre tipos de redes heterogéneas incluyendo tanto 802 y no 802 redes.
802.22	Este estándar (también conocido como Área Regionales Redes Inalámbricas (WRAN)) tiene como objetivo desarrollar un estándar para un PHY / MAC / aire basado en radio cognitiva interfaz para el uso de dispositivos exentos de licencia sobre una base de no interferencia en una espectro que está atribuida al servicio de radiodifusión de televisión.

Fuente: Laurent-Maknavicius, 2007

En la tabla 2 se puede visualizar la evolución de las versiones de los protocolos de la red inalámbrica 802.11.

Tabla 2 Cuadro comparativo entre los principales estándares IEEE 802.11 redes inalámbricas

Protocolo	Fecha de lanzamiento	Frecuencia	Tipo de Tasa de Datos	Velocidad de Datos	Alcance en interiores
Inicial	1997	2.4 – 2.5 GHz	1 Mbit/s	2 Mbit/s	?
802.11a	1999	5GHz	25 Mbit/s	54 Mbit/s	~30 metros (~100 pies)
802.11b	1999	2.4 – 2.5 GHz	6.5 Mbit/s	11 Mbit/s	~30 metros (~100 pies)
802.11g	2003	2.4 – 2.5 GHz	25 Mbit/s	54 Mbit/s	~30 metros (~100 pies)
802.11n	2008	Banda de 2,4 GHz o 2,5 GHz	200 Mbit/s	540 Mbit/s	~50 metros (~160 pies)

Fuente: (IEEE, 2012)

En las normas se publican documentos que establecen las especificaciones y procedimientos diseñados para maximizar la fiabilidad de los materiales, productos, métodos, servicios y / o la gente usa todos los días. Las normas tratan una variedad de temas, incluyendo diversos protocolos para ayudar a maximizar la funcionalidad del producto y la compatibilidad, interoperabilidad y el apoyo a la seguridad del consumidor y la salud pública.

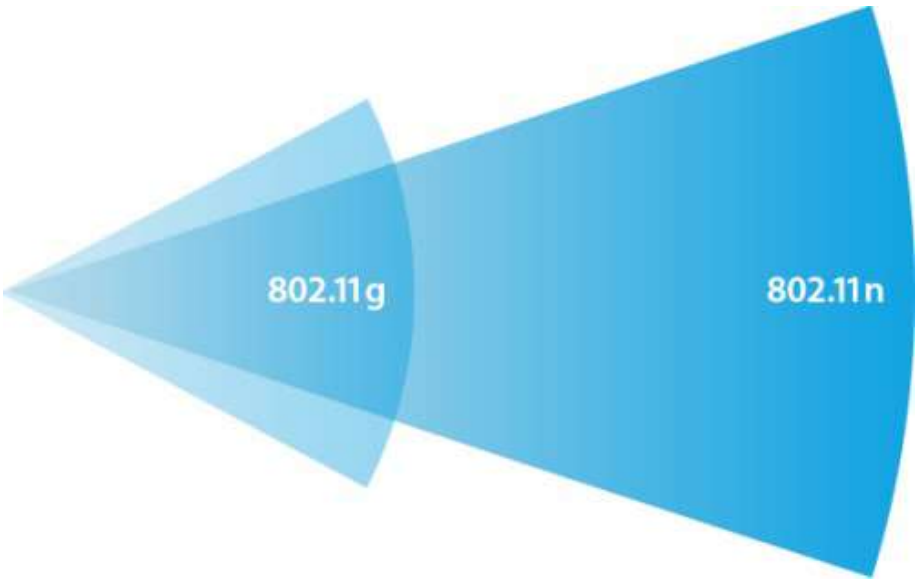

Figura 1 Alcance de estándar 802.11g y 802.11n

Fuente: (Rojas, 2013)

4.3.Modos de Operaciones

Existen 2 modos de operaciones que son las siguientes:

- Modo de Infraestructura (Red Centralizada): El modo infraestructura, también conocido como punto de acceso, debido a que utilizan muchos AP para tener una mayor cobertura en la zona de transmisión, el objetivo de este módulo es centralizar la información que se quiere transmitir, es decir si el ordenador A quiere pasar un paquete de datos al ordenador B, primero deberá llegar al Access Point para que esta se encargue de transmitir al destino deseado.
- Modo Ad-Hoc (Red Descentralizada): Este es el modo más económico para crear una red inalámbrica, debido a que no necesitan de un nodo maestro ni de un Access Point, los equipos deben contar con tarjeta inalámbrica y que todos los equipos estén en la

zona de cobertura para que pueda transmitir la información directamente desde el emisor al receptor.

El IEEE 802.11 puede funcionar en dos modos: infraestructura y ad -hoc. En el modo ad-hoc, dos estaciones WLAN pueden comunicarse directamente entre sí siempre que estén en el mismo espectro de gama sin la intervención del punto de acceso. Cada estación de WLAN puede ser considerado como un acceso punto y una estación de cliente al mismo tiempo. Sin embargo, en el modo de infraestructura, la red inalámbrica es controlada por el punto de acceso que está equipado con dos redes de interfaz.

4.4.Red de Internet Móvil

Enrutamiento IP se diseñó sin apoyo a los nodos móviles y se ha definido para nodos fijos. La movilidad IP ha sido posible gracias a la evolución de las redes inalámbricas, así como la evolución de la miniaturización de los portátiles y móviles terminales. La movilidad IP introduce nuevas características en la red para asegurar la continuidad del enrutamiento para nodos móviles que se desplazan. Estas características están abordando, ubicación gestión, transporte alternativo y la entrega de nodo del móvil: (Laurent-Maknavicius, 2007)

- ***Direccionamiento:*** *en una red IP, apoyo a los nodos móviles requiere dos IP direcciones: una dirección fija del nodo móvil, que se relaciona a la red doméstica que sirve como una identificación del nodo móvil, y una dirección temporal que es relacionados con la red visitada. Los cambios de dirección temporal como el nodo móvil se mueven de una red temporal a otro. La dirección temporal se produce cada vez por una red visitada.*

- ***Gestión de la Ubicación:*** *una correspondencia se mantiene en la red entre la dirección fija y la dirección temporal del nodo móvil. Esta correspondencia se lleva a cabo por una nueva entidad en la red, un agente de movilidad. El nodo móvil debe enviar de forma segura su nueva dirección temporal para el agente de movilidad para mantener la correspondencia entre la dirección temporal y la permanente dirección del nodo móvil y por lo tanto pueden localizarlo en orden para enviar su tráfico a su ubicación actual.*
- ***Cambio de Ruta:*** *cuando el nodo móvil tiene una sesión activa durante su viaje, que es la responsabilidad de la red para encaminar el tráfico a su nuevo destino sin interrumpir la sesión.*
- ***Handover:*** *el traspaso es el proceso de cambiar el punto de unión a la red. Contiene la fase de descubrimiento de la nueva red visitada y apego a esta nueva red. La entrega es difícil cuando hay una sesión en curso porque todo el problema es cambiar el punto de unión sin interrumpir la sesión. (Laurent-Maknavicius, 2007)*

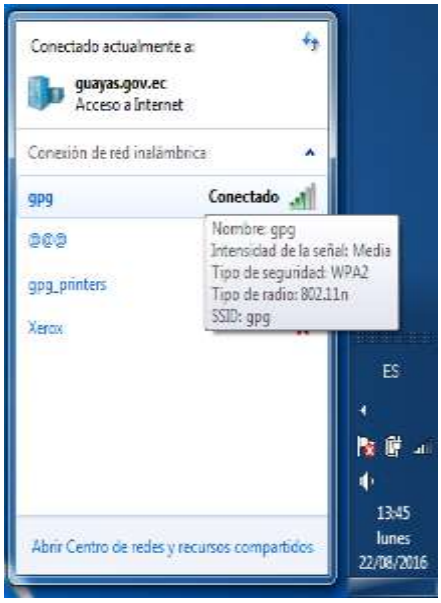

Figura 2 Red wifi móvil
Fuente: Gobierno Provincial del Guayas – Windows 7

4.5.Vulnerabilidad de las redes

La vulnerabilidad de la red afecta principalmente a los usuarios que estén conectados en ella. Actualmente mucha gente ha sido hackeada, es decir que han alterado, borrado, ingresado o eliminado información, teniendo en cuenta que los datos que viajan por internet pueden ser capturados por diversos programas con el objetivo de obtener la información que se desea transmitir.

En las redes, tanto cableadas como inalámbricas, pueden sufrir algunas amenazas en su seguridad informática e incluso daños en los equipos informáticos ocasionados por programas malignos o intrusos.

- **Virus:** Es un programa que puede infectar a otros programas modificándolos de tal manera que cause daño en el archivo.
- **Caballo de troya o troyanos:** A simple vista es un programa útil pero una vez instalado o ejecutado en el computador hace el daño, y normalmente no es detectado porque se cree que la procedencia del programa es segura. Pueden ocasionar daños serios robando, eliminando o modificando archivos del sistema, también permite crear una puerta trasera donde ingresa una tercera persona con mala intención y puede tener acceso a todo. Este programa no se autoreplica ni se reproduce infectando a otros archivos.
- **Gusanos:** Se autoreplican y se reproducen infectando varios archivos, ocasionando la perdida de información.

- **Spyware:** Es un programa que puede instalarse en distintos equipos sin que el usuario se dé cuenta, es decir que en un programa que se descarga el usuario viene oculto el programa de spyware, este último recopila en secreto la información del usuario, y generalmente se transmite por correos.
- **Worm:** Es el virus más inteligente, porque se propaga a través del internet de una manera discreta y el usuario no puede visualizar el problema hasta que el equipo presenta alguna anormalidad, puede capturar direcciones de correo electrónico, usar servicio de SMPT y sistema de envió de mail, cuya única finalidad es consumir la memoria del sistema y copiarse a sí mismo.
- Existen otros programas, como el capturador de teclas que se instalan en el ordenador y tienen la opción de almacenar lo que se ingresa a través del teclado donde el usuario puede acceder al fichero manualmente o enviarlo directamente a un correo, entre otros.

La seguridad de la red es un complemento siempre y cuando se maneje una seguridad de información, es decir indicar a los usuarios acerca de los diversos ataques y vulnerabilidades que existen en la actualidad para obtener, eliminar o modificar los datos existentes ya sea en los ordenadores o el sistema informático que maneje alguna institución, empresa u organización.

Es importante reconocer los tipos de amenazas y vulnerabilidades, para así poder proteger los datos e información que viajan en la red, asignando prioridad a cada uno y poder tomar las acciones necesarias para minimizar el riesgo que estas puedan ocasionar.

4.6. La importancia de la seguridad en las redes inalámbricas

Los problemas de seguridad de una red WLAN son su principal desventaja, debido que radian información y el acceso de los recursos informáticos de una manera ininterrumpida, teniendo en cuenta que, en una red inalámbrica, esta, se anuncia a cualquiera que este circulando dentro de su área de cobertura.

La diferencia entre una red cableada con WLAN, es que en la red cableada las personas que desean tener conexión deberán ubicar un acceso físico a la red interna de una determinada institución, en cambio en la red inalámbrica, esta red notifica a todos los que estén dentro de su alcance donde podrán acceder a toda la información en caso de no tener ningún tipo de seguridad, es decir que para algún intruso le bastará estar cerca del alcance de la red inalámbrica para cometer un acto delictivo que le permita obtener, manipular y eliminar información de la institución.

Para que un intruso puede ingresar en la red inalámbrica tiene que ser a través de un nodo, y el peligro principal es que puede escuchar la transmisión, para minimizar los riesgos lo importante es: cambiar las claves por defecto cuando se instalan los puntos de accesos (AP's), control de acceso seguro con autenticación bidireccional, control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red, configurar el protocolo de seguridad WEP donde la seguridad del cifrado de paquetes que se transmiten es fundamental en las redes inalámbricas, la codificación puede ser más o menos segura dependiendo del tamaño de la clave creada y su nivel, la más recomendable es de 128 bits, crear varias claves WEB, donde pueda variar para los AP y los usuarios, entre otros.

La inseguridad es el talón de Aquiles, que se puede presentar si una red inalámbrica no está bien estructurada con su respectivo protocolo de seguridad.

Entre los tipos de seguridad más utilizados en las redes inalámbricas, están los cifrados (WEP, WPA), basados en controles de acceso mediante claves de red, lamentablemente varios estudios han comprobado que este tipo de seguridad tiene ciertas falencias en su implementación.

La seguridad en la era digital se puede definir como la búsqueda de la protección de los activos digitales y la protección de los sistemas de tratamiento de dichos activos contra cualquier acto que no es deseado o percibida como abuso por parte de los respectivos propietarios. Tales actos no deseados son típicamente posibles debido a las vulnerabilidades presentes en la IS's (Ingeniería del Software). La explotación de vulnerabilidades crea amenazas y por lo tanto representan un riesgo desde el punto de vista del propietario. Por el contrario, en la metodología de la seguridad de la percepción de los riesgos a los activos por el dueño conduce a la aplicación de un conjunto de medidas a adoptar dentro de la IS.

La seguridad de la red se está convirtiendo en uno de los principales retos para el desarrollo de nuevas tecnologías y servicios en las redes de telecomunicaciones. Los hackers están en constante evolución hacia nuevas técnicas de ataque y las nuevas tecnologías de destino a una velocidad muy alta, con lo que la tarea de la defensa es una misión difícil.

Se debe tener en cuenta que la seguridad es parte fundamental para que el usuario se sienta seguro, ofreciendo al usuario conectividad, rendimiento, seguridad y alta disponibilidad cuando quiera usar aplicaciones, dispositivos, consultas, eliminación, ingreso o modificación de datos.

De acuerdo a (Ali Ismail Awad, 2013).

> *"Muchos esfuerzos se han hecho por la comunidad de investigación para desarrollar defensas de seguridad destinadas a derrotar a los ataques. El ciclo es casi siempre el mismo: cada vez que se descubre una nueva técnica de ataque o vulnerabilidad por un investigador, una prueba de aplicación concepto está construido como una propiedad desarrollo, una evaluación de las capacidades de esta técnica de hecho, y el desarrollo de técnicas efectivas de defensa propuesto.*
>
> *Como resultado de esta metodología de investigación, aunque muchos investigadores contribuyen su red de código de ataques, hay una falta de implementaciones aceptados para los ataques que permitirían a las soluciones de referencia en su contra. Por lo tanto, es deseable tener un marco común que permita el desarrollo de las implementaciones de los ataques de red y sus defensas. Este marco debería permitir combinar la ejecución de todos los ataques a cabo, de forma similar a como hacen los hackers, y también permiten probarlos en múltiples tecnologías, protocolos y escenarios." (Ali Ismail Awad, 2013).*

Existen dos tipos de seguridad con respecto a la amenaza, una de ellas es la seguridad lógica que consiste en las políticas y mecanismos que permitan garantizar la autenticación, confidencialidad, disponibilidad y la integridad de la información y recursos del sistema como se lo determine en la institución, empresa u organización. Y la seguridad física consiste en las amenazas a la estructura física de los equipos que pueden ser ocasionados por incendios, inundaciones, robos, entre otros.

4.7.Seguridad WI-FI (Wireless Fidelity)

En una red Wi-Fi para lograr una comunicación segura, es necesario contar con una infraestructura adecuada y con los métodos necesarios para protegerlos, es por ello que existen 4 elementos principales para construir una red segura.

A su vez Laurent-Maknavicius (2007) clasifica los elementos principales de la infraestructura de la siguiente manera:

- **Infraestructura de Autenticación. -** El estándar IEEE 802.1x recomienda el uso del servidor RADIUS (Remote Authentication Dial-In User Server). La autenticación puede llevarse a cabo por un servidor situado en el dominio. Esta arquitectura establece un círculo de confianza, a través del cual una autenticación el mensaje es apoyado por varios servidores unidos entre sí por asociaciones de seguridad.
- **Seguridad de Radio. -** El objetivo de la seguridad de radio es asegurar la confidencialidad, integridad y la firma de paquetes. Estos servicios son entregados por protocolos como WEP (Wired Equivalent Privacy), TKIP (Temporal Key Integrity Protocol) o CCMP (Counter mode with CBC MAC Protocol) , estandarizado por el Comité IEEE 802. Los protocolos utilizan claves derivadas de una llave maestra, después de que el proceso de autenticación.
- **El filtrado de paquetes. -** La fiabilidad de esta operación se basa en el paquete firma utilizando claves derivadas del proceso de autenticación. El uso de este mecanismo, los marcos que entran en el sistema de distribución son seguros (sin riesgo de suplantación de identidad o disfraz). sistemas de filtrado (punto de acceso o portal) gestionar los privilegios de IP paquetes (destrucción de los paquetes ilícitos) y hacer posible la entrega y de la cuenta servicios para QoS (Calidad de Servicio).

- **El acceso a servicios remotos (Roaming). -** El acceso a los servicios a distancia puede ser diseñada genéricamente bajo el servicio de VPN (Virtual Private Network). Por ejemplo, aplicación de inter- dominios seguros se puede lograr utilizando IPsec o SSL protocolos.

Dicha información es esencial dado que permite la autentificación de clientes y equipos de red, el hardware y el software que son necesarios para lograr seguridad en la interfaz de radio, los elementos de red que son necesarios para el paquete filtrado y detección de ataques. Y los equipos necesarios para gestionar a distancia el acceso cuando los usuarios se están moviendo.

4.8.Mecanismos de Seguridad WLAN

Un punto de acceso abierto se utiliza si se quiere atrapar a las personas que buscan puntos de acceso abierto. Otra opción sería configurar el protocolo WEP para detectar cuando se realiza un ataque (encontrar el secreto compartido utilizado para proteger las comunicaciones de datos inalámbricas) y para acceder al sistema Esto se considera una actividad maliciosa.

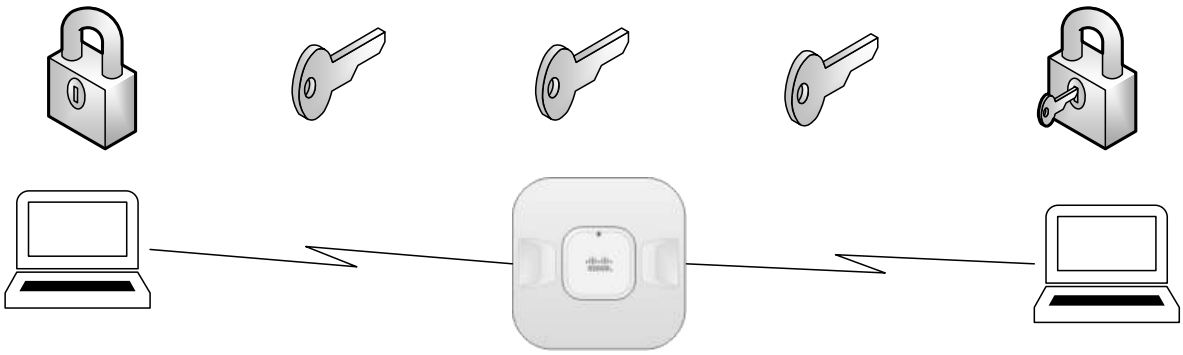

Figura 3 Mecanismo de seguridad WLAN

Elaborado por: Autores

En la figura 3, el usuario revisa en el equipo final si existe una red inalámbrica disponible, en este caso la red existente es "gpg". Para conectarse a esta red, el funcionario debe ingresar un usuario y contraseña para autenticarse con el access point que se encuentre más del equipo final.

4.8.1. Protocolo WEP (Wired Equivalent Privacy)

WEP, fue el primer protocolo de encriptación introducido por la primera versión del estándar 802.11 en el 1999, basado en el algoritmo RC4 implementado en la capa segunda capa física (MAC) del modelo OSI para cifrar los datos. Además, el WEP es usado como encriptación de información mediante claves para asegurar la confidencialidad e integridad de los datos que estén dentro de una red inalámbrica.

El protocolo WEP maneja una clave que no se puede cambiar nunca, por lo que existe una desventaja para la red, ocasionando inseguridad en ella, es decir el usuario que tenga la clave podrá ingresar libremente a la red, por lo que no se considera el mejor protocolo de seguridad.

"WEP se define como un protocolo facultativo, y las estaciones WLAN y el acceso puntos no están obligados a utilizarlo. Los mecanismos definidos en WEP también son opcionales: una estación puede utilizar el mecanismo de autenticación, por ejemplo, pero no el cifrado algoritmo, y viceversa." (Laurent-Maknavicius, 2007).

4.8.2. Protocolo WPA (Wi-Fi Protected Access)

WPA, fue el segundo protocolo de encriptación introducido por el estándar 802.11i en el 2003, fue creado debido a la notable debilidad que tuvo el protocolo WEP, por lo que utiliza un vector de inicialización de 48bits y una clave de cifrado de 128bits. Este protocolo

almacena las credenciales y contraseñas de los usuarios de la red; y es considerado que uno de los protocolos de mayor seguridad. El WPA en su primera construcción fue realizada para que el modo de infraestructura sea la única que admita este protocolo de seguridad, es decir que las redes de punto a punto no están permitidas para usar este protocolo.

El funcionamiento de WPA se basa en la implementación de un servidor de autenticación (en general un servidor RADIUS) que identifica a los usuarios en una red y establece sus privilegios de acceso. No obstante, redes pequeñas pueden usar una versión más simple de WPA, llamada WPA-PSK, al implementar la misma clave de cifrado en todos los dispositivos, con lo cual ya no se necesita el servidor RADIUS. (Kiosko.net, 2014)

4.8.3. Protocolo WPA 2

Este protocolo es una versión del WPA, en base de las vulnerabilidades que se vieron afectas por el protocolo anterior, fue creada en el 2004 en base del nuevo protocolo 802.11i, para que sea soportada por los equipos portátiles como PDA, tarjeta de red, laptop. Adicional a esto asegura que tanto el modo ad-hoc y modo de infraestructura pueda utilizar este protocolo.

"El 802.11i se ratificó el 24 de junio de 2004 para abordar el problema de la seguridad en redes inalámbricas. Se basa en el algoritmo de cifrado TKIP, como el WPE, pero también admite el AES (Estándar de cifrado avanzado) que es mucho más seguro." (Kiosko.net, 2014)

Figura 4 Niveles de seguridad de red inalámbrica

Fuente: (Colomés, 2013)

4.9.Protocolo de Autenticación EAP

EAP, es un protocolo general de autenticación usado para controlar el acceso a la red cableada o la más usada la red inalámbrica, los estándares WPA y WPA2 han adoptado el mecanismo de los 5 tipos de EAP; el EAP no requiere conectividad IP, solo ofrece soporte en el camino para la transmisión o retransmisión confiable de protocolos de autenticación.

(Microsoft, 2005) indica que: *"El Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol) es una extensión del Protocolo punto a punto (PPP) que admite métodos de autenticación arbitrarios que utilizan intercambios de credenciales e información de longitudes arbitrarias. EAP se ha desarrollado como respuesta a la creciente demanda de métodos de autenticación que utilizan dispositivos de seguridad, como las tarjetas inteligentes, tarjetas de identificación y calculadoras de cifrado. EAP proporciona una arquitectura estándar para aceptar métodos de autenticación adicionales junto con PPP."*

4.10. Redes Virtuales

LAN es una red área local que conecta varios ordenadores en un área pequeña fácil de determinar, como una habitación o un edificio. El entorno de una red área local lo componen el ISP que es el proveedor de servicios de internet; el router cuya función principal es encaminar o enviar los paquetes de datos de una red a otra, eligiendo cual es la mejor ruta para enviar el paquete, en la que se puede configurar los puertos fastethernet y seriales, enrutamiento estático y protocolos de enrutamiento dinámico; el switch es un dispositivo lógico, que interconectan más de 2 segmentos de red. En este se configuran las interfaces de fastethernet, asignaciones de puertos, enlaces troncales y VLANs.

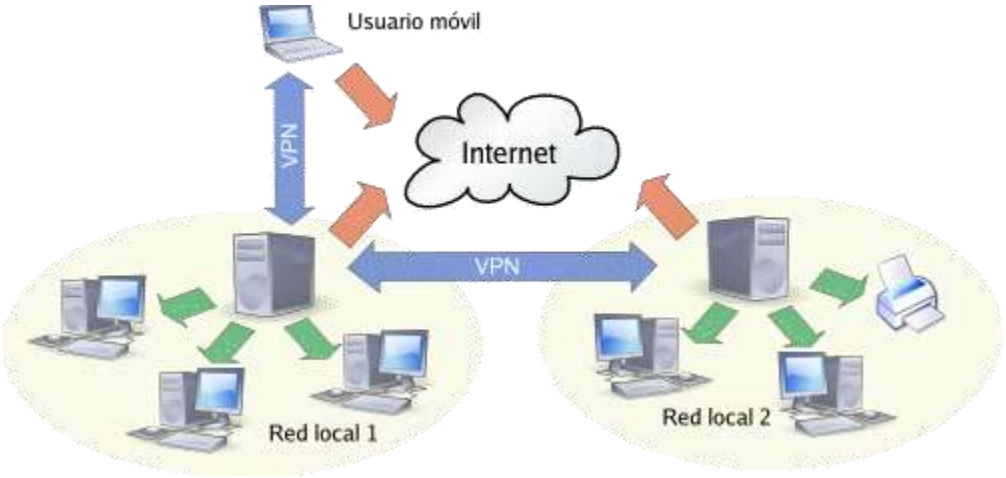

Figura 5 Redes virtuales

Fuente: (Ramirez, 2016)

4.10.1. VLAN (Virtual Local Area Network)

Es un método para crear redes lógicas independientes dentro de una misma red física, al crear una VLAN se pueden asignar los puertos en cada switch, para que estos puertos sean solo visibles con su misma VLAN en todos los switches que están continuamente conectados.

La VLAN funciona en el nivel 2 del modelo OSI, en los switch viene por defecto configurada la VLAN 1 y no se puede borrar, las VLANs ayudan a la disminución del tráfico en la red, separando los recursos que puede usar los puertos que están vinculados en la VLAN.

Como señala Ernesto Ariganello (2010):

> *Las VLAN (Virtual LAN) proveen seguridad, segmentación, flexibilidad, permiten agrupar usuarios de un mismo dominio de broadcast con independencia de su ubicación física en la red. Usando la tecnología VLAN se pueden agrupar lógicamente puertos del switch y los usuarios conectados a ellos en grupos de trabajo con interés común. Una VLAN por definición es un dominio de difusión creado de forma lógica.*(Ernesto Ariganello, 2010).

Las VLAN, fueron creadas para dividir varias redes locales, con el objetivo de economizar, es decir, si se tiene una empresa grande que cuenta con una gran cantidad de empleados y por cada usuario hay que cruzar cables y asignar un puerto en el switch, y todos los usuarios tendrán el mismo ancho de banda, esto puede ocasionar que no se aproveche eficientemente los recursos de la empresa. Una buena opción es agrupar equipos en una VLAN para administrar, evitar las colisiones de tráfico y establecer niveles de servicio.

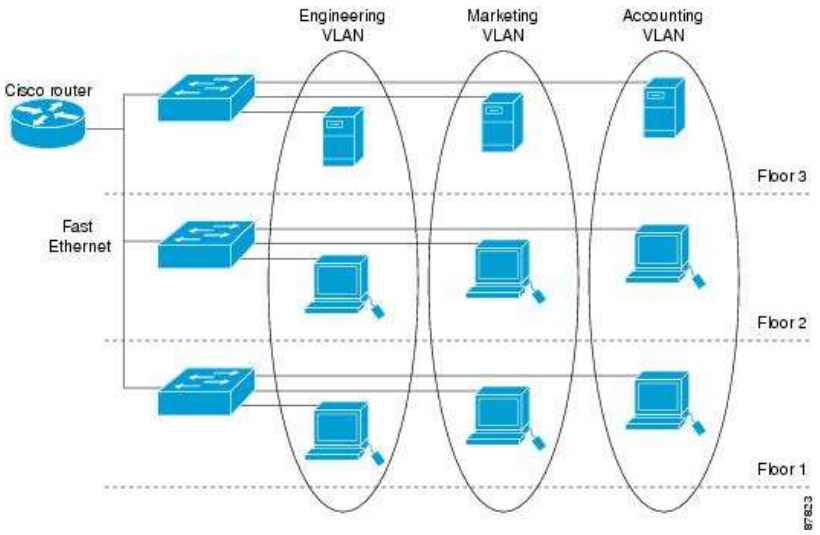

Figura 6 Virtual LAN network

Fuente: (CISCO, 2012)

4.10.2. Tipos de VLAN

Las VLAN Estáticas son puertos en un Switch que se asignan a una VLAN, consisten en que el administrador es el encargado de agregar los puertos manualmente y este tipo de VLAN no es necesario la negociación por parte del switch. Las VLAN estáticas son seguras, fáciles de configurar y controlar. Mantienen sus configuraciones de VLAN asignadas hasta que el administrador haga algún cambio y este tipo de VLAN funciona bien en las redes que se encuentran controlados y administrados.

Las VLAN dinámicas son las que definen por las direcciones MAC, en este tipo de VLAN es más flexible dado que no depende de la ubicación del equipo y pueden determinar automáticamente las VLAN, es más usado cuando no existe la necesidad de tener control y suele pasar cuando la empresa es pequeña. La asignación de puertos se realiza mediante el VMPS (VLAN Management Policy Server o Servidor de Gestión de Directivas de la VLAN).

Ariganello (2010) menciona que: *"Las VLAN dinámicas son muy utilizadas y se basan en la MAC del dispositivo que se conecte a un puerto determinado, son utilizadas por ejemplo en el caso de utilizar IEEE 802. IX para proporcionar seguridad. Las VLAN dinámicas utilizan algún software de gestión como Cisco Works para su funcionalidad."*

Entre ambos tipos de VLAN, se recomienda usar VLAN estática cuando se quiere tener la administración y el control de la red, y evitar el desperdicio de ancho de banda, para poder asignarle a un grupo determinado, es decir se puede crear una VLAN para los gerentes de la empresa y conceder permisos privilegiado para tener una gran velocidad de transmisión y descarga de datos, y en otra VLAN se puede dar a los empleados un acceso limitado y más controlado para que no exista el desperdicio de ancho de banda no utilizado, y a la vez también ayuda a prevenir las colisiones de tráfico. Pero también se puede usar los 2 tipos de VLAN si la empresa llega a crecer y en una VLAN estática se cree otras VLAN dinámicas, y es muy usado en las empresas grandes donde se maneja un control para prevenir y poder identificar de inmediato las colisiones o cuerpo de botella.

4.10.3. Tipos de Operaciones

Modo Acceso: Es cuando un puerto es solo de acceso y que a dicha interfaz se conectará un host, donde tendrá acceso directo a la VLAN sin conocer a que VLAN pertenecen.

"La operación de modo de una sola VLAN también se refiere como modo de acceso. Un puerto que está operando en este modo se asocia con una única VLAN. El tráfico entrante no tiene ningún tipo de identificación de VLAN. Cuando las tramas sin etiquetar entran en

el puerto, se añade la identificación de VLAN de la VLAN que está configurado para el puerto a las tramas entrantes." (Jon Tate, 2016)

Modo troncal: Este modo, permite transmitir punto a punto varias VLAN que estén en modo acceso con un mayor control del broadcast, es decir, que toda las VLAN viajan por la infraestructura siempre y cuando puedan recibir esa trama.

"La operación múltiple modo VLAN también se conoce como modo de tronco. Un puerto que está operando en este modo puede recibir tramas que tienen etiquetas VLAN. El puerto también está configurado con VLAN a la que se permite el puerto para enviar y recibir tramas." (Jon Tate, 2016)

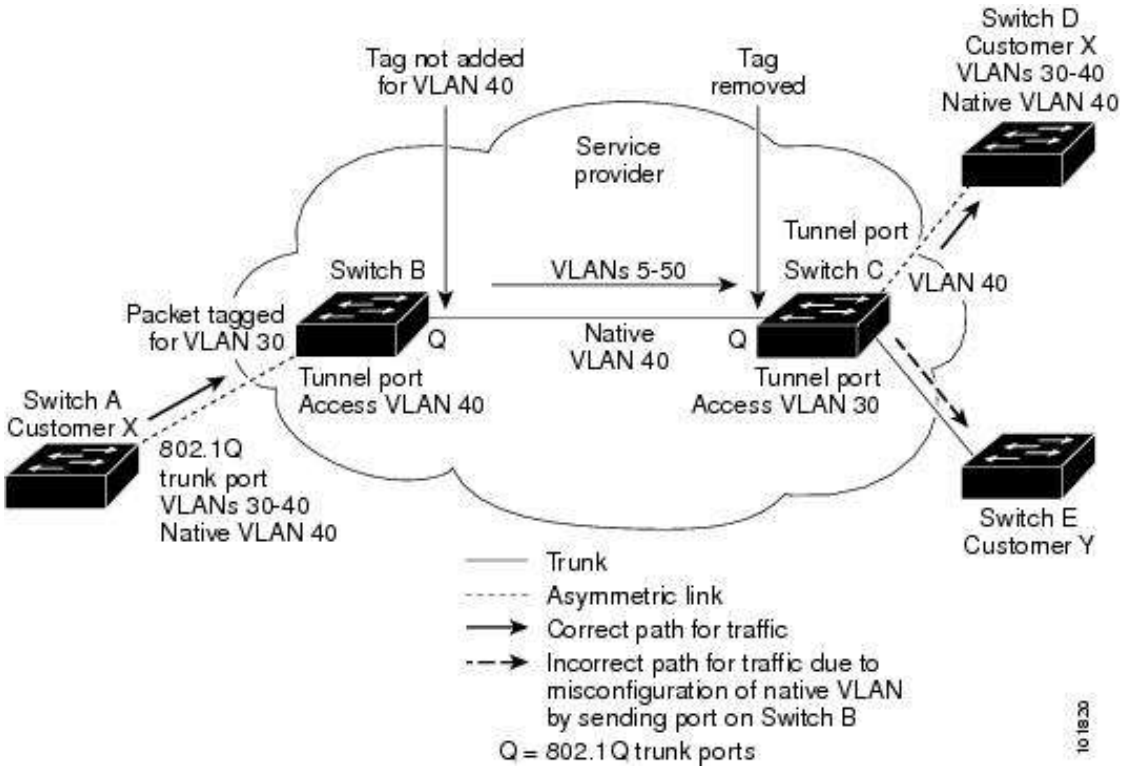

Figura 7 Tipos de VLAN

Fuente: (CISCO, Tunneling and Native VLANs, 2016)

4.11. Autenticación

Es el proceso mediante el cual una red de datos permite a un usuario acceder a los recursos.

La definición de la EAP (Extensible Protocolo de autenticación) que se describe en esta sección ayuda en la elección del método de autenticación. La necesidad de implementar medidas de seguridad desde un solo dispositivo llevó a la definición de autenticación centralizada en ciertas piezas de equipo, tales como servidores RADIUS LDAP, etc.

Los protocolos AAA surgieron por estas razones y con la posibilidad de extender la autenticación de InterDomai, es decir, para permitir a los abonados autenticar con éxito un dominio administrativo diferente de su propio dominio de suscripción. Esta sección se centra principalmente en la descripción de diversos protocolos y métodos para la autenticación para controlar el acceso a una red.

De acuerdo a (Laurent-Maknavicius, 2007):

> *"Con el fin de diversificar los métodos de autenticación, la IETF ha estandarizado un protocolo de autenticación EAP genérica llamada de [RFC3748]. Este protocolo es genérico, en que es independiente del método de autenticación. Su papel se limita al transporte de datos de autenticación entre un cliente y un servidor. El contenido de estos intercambios no se interpreta por el EAP capa de software, pero por el método de EAP seleccionado. Como tal, que aporta la ventaja de que un EAP Método detectado pronto como vulnerable se puede cambiar fácilmente a otro más método robusto, manteniendo el mismo protocolo EAP. Esto hace que la seguridad equipo más flexible y capaz de evolucionar a bajo costo."* (Laurent-Maknavicius, 2007)

4.12. Sistema de Autenticación

Es usado para acceder a la red de forma segura, donde se verifica que la persona que quiere ingresar al sistema o acceder a la información, sea quien tenga la autorización por medio de usuario y contraseña de manera confiable trabajando junto con el servidor, donde se encuentran almacenados en la base de datos o en algún active directory.

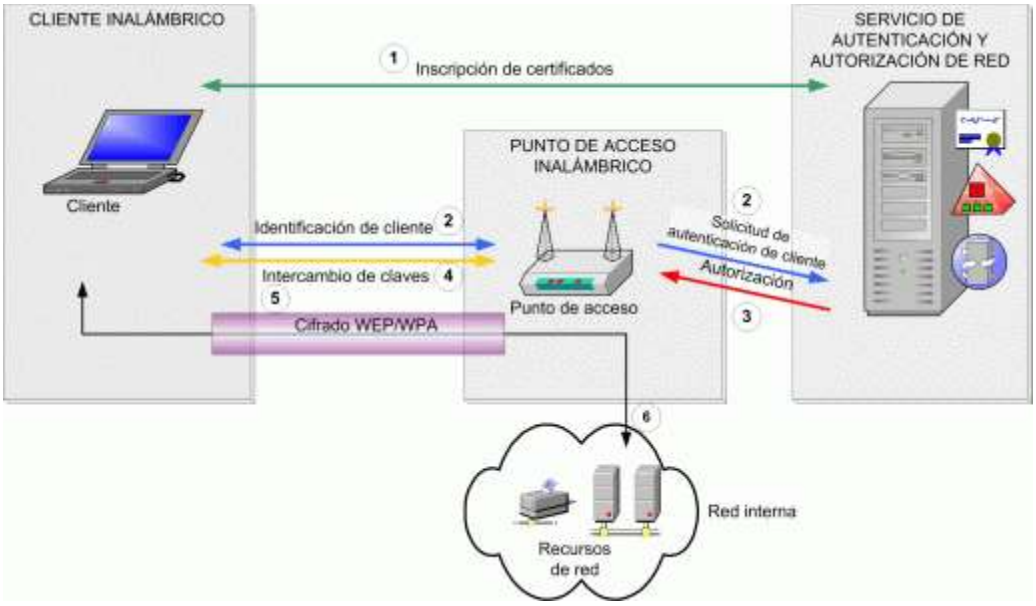

Figura 8 Sistema de autenticación

Fuente: (Microsoft T. , Technet Microsoft, 2014)

En la figura 8 se cuenta con un cliente inalámbrico y este equipo se utiliza para acceder a la información, siendo el encargado de inscribir los certificados en el servidor de autenticación y así mismo conectarse a un punto de acceso inalámbrico con un cifrado adecuado para proteger los datos que viajan en el medio; el AP es el encargado de acceder al servicio de red, donde se comunica de manera directa con el servidor de autenticaciones para saber si cuenta con el permiso para acceder a lo solicitado y tomar la decisiones para la autorización.

el servidor de autenticación, es quien se encarga de verificar los datos que el AP envía y confirma si son válidos para su respectiva autorización, teniendo en cuenta que el componente principal para el servicio de autenticación es el servidor RADIUS.

4.13. RADIUS

RADIUS (Remote Authentication Dial-In User Server) es un protocolo extensamente utilizado para el control de acceso a los servicios de red. El establecimiento de las conexiones para autenticar, autorizar y contabilizar se realiza a través de los puertos UDP 1812 y 1813.

Generalmente cuando se buscan sistemas basados en la autenticación, como mejor alternativa se piensa en RADIUS. Por los años 90 las redes tuvieron un notable crecimiento dificultando el control de acceso, adicional a esto cada fabricante de dial-up hacia uno de sus propios sistemas de control de acceso.

En 1991 Merit lanzó un RFI (Request For Information) a las principales empresas de red. Livingston Enterprises fue una de las primeras empresas en responder y promover RADIUS.

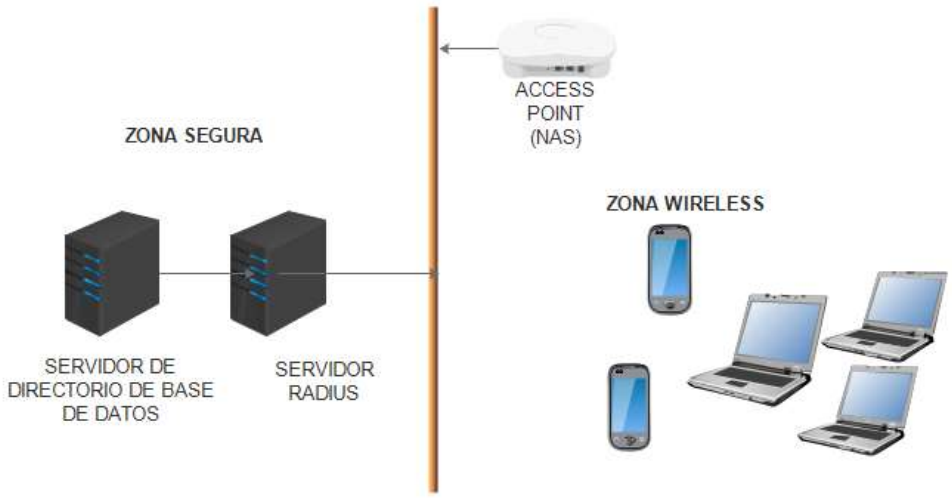

Figura 9 Comunicación con el servidor RADIUS

Elaborado por: Autores

"La comunicación entre un servidor de acceso de red (NAS) y el servidor RADIUS se basa en el protocolo de datagrama de usuario (UPD). Generalmente, el protocolo RADIUS se considera un servicio sin conexión. Los problemas relacionados con la disponibilidad de los servidores, la retransmisión y los tiempos de espera son tratados por los dispositivos activados por RADIUS en lugar del protocolo de transmisión." (Cisco Systems Inc, 2015)

RADIUS es un protocolo para controlar el acceso a los servicios de red. Es conocido como 3A o AAA (Autenticación, Autorización y Administración), y es ampliamente utilizado en redes extensas cuando se quiere proporcionar servicios de acceso centralizado. Las empresas que ofrecen el acceso a internet a grandes redes corporativas, y no solo para el acceso, sino también para los diversos servicios propios del internet como mail y VoIP, utilizan servidores AAA.

RADIUS también es usado en el NAS para avisar cuando se inicia y finaliza la sesión del usuario, el total del paquete transmitido durante la sesión, el volumen de datos transferidos durante la sesión y la razón para la terminación de la sesión.

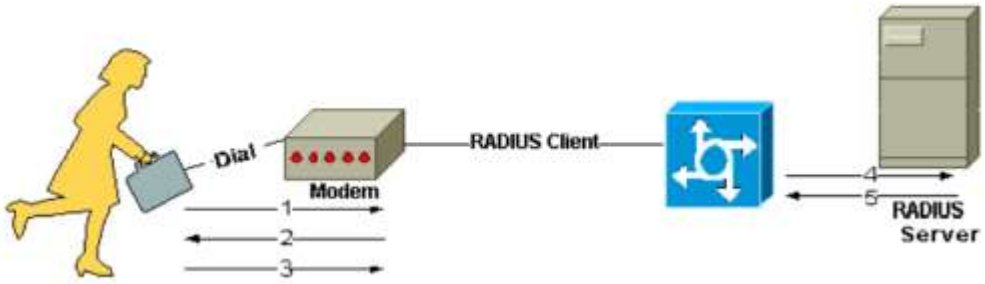

Figura 10 Interacción entre usuarios y servidor RADIUS

Fuente: (Cisco Systems Inc, 2015)

La figura 10 (Cisco Systems Inc, 2015), muestra los pasos para la autenticación del usuario.

1. El usuario inicia la autenticación con el Protocolo Point to Point (PPP) al Servidor del acceso a la red (NAS).
2. El Servidor de Acceso a la red (NAS) pedirá que ingrese el nombre de usuario y la contraseña.
3. Contestaciones del usuario.
4. El cliente RADIUS envía el nombre de usuario y la contraseña encriptada al servidor de RADIUS.
5. El servidor RADIUS responde con Aceptar, Rechazar o Impugnar.
6. El cliente RADIUS actúa dependiendo de los servicios y de los parámetros de servicios agrupados con Aceptar o Rechazar.

4.14. SERVIDOR RADIUS

Consiste en el programa que se instala como servicio en el sistema operativo del equipo que realiza la función de servidor y estará a cargo de la administración de las cuentas de acceso.

Procesa la autenticación comparando con sus registros, luego de esto envía un mensaje permitiendo o negando el acceso. El cliente debe tener un perfil del cliente RADIUS con la dirección IP y la clave de autorización.

Las empresas pequeñas no necesitan de tener un servidor RADIUS, porque no creen contar con una gran cantidad de usuarios para administrarlo y controlarlo, en cambio en las empresas grandes o con aspiración de ampliarse, deberán dar la autenticación y autorización para cada uno de los usuarios, lo que permitirá tener mayor seguridad con la información que se maneje en la empresa. Debido que cuando se realiza la conexión con un punto de acceso WIFI, el empleado enviara su usuario y contraseña; esta información se transferirá al servidor RADIUS, el mismo que verificara si la información recibida es igual a la que esta almacenada, utilizando el esquema de autenticación EAP (Extensible Authentication Protocol). En caso de que el usuario y contraseña sea correcto, el servidor RADIUS autorizara el acceso al equipo y a los recursos que han sido establecidos en el perfil que se está conectando.

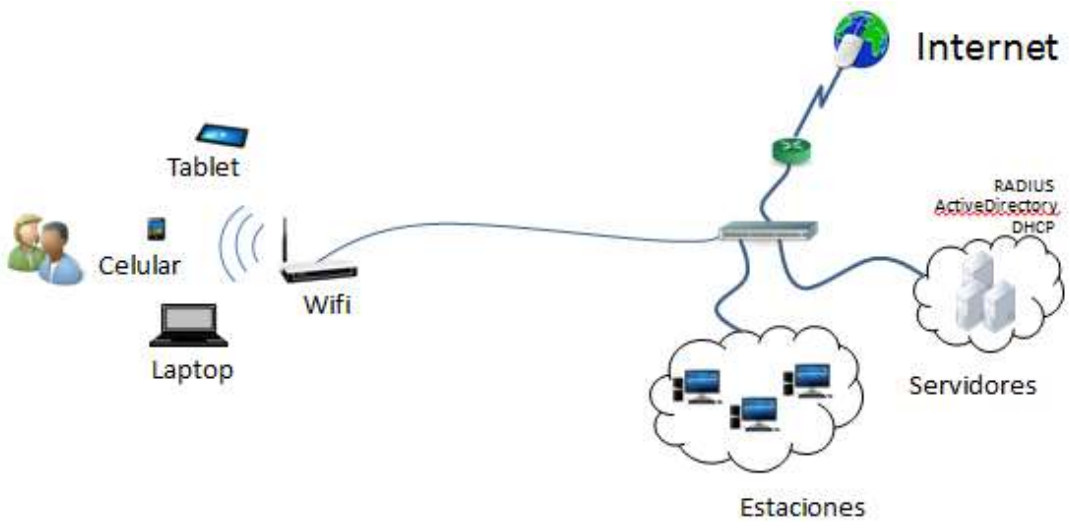

Figura 11 Como funciona RADIUS

Elaborado por: Autores

1. El empleado a través de un ordenador portátil, celular, tablet o computadora con tarjeta inalámbrica solicita acceso a la red WiFi (punto de acceso - AP) mediante un usuario y contraseña, proporcionado por la dirección provincial de tecnología de la información y comunicación – TICs.
2. El punto de acceso (AP), enviará las credenciales al servidor RADIUS para que sean autenticadas. En caso de no ser válidas, no se concederá la autorización para acceder a la red y se informará al cliente (usuario o contraseña incorrecta)
3. Si las credenciales del usuario son correctas, el servidor RADIUS autorizará al cliente al acceso a la red, comunicándoselo al punto de acceso (AP).
4. El punto de acceso (AP), a través del protocolo DHCP (Dynamic Host Configuration Protocol), enviará la dirección IP, máscara, puerta de enlace y DNS al cliente para que éste pueda acceder a la red WiFi.

4.15. CLIENTE RADIUS

También conocido como NAS (Network Access Server), es un equipo de comunicación, comúnmente un access point, un RAS o un switch, el mismo que se convierte en una puerta de ingreso a la red al cual de conecta físicamente un usuario por medio de wireless, cable o ADSL. Es el encargado de cursar las solicitudes de acceso a los servidores, y dependiendo de la respuesta del servidor permitirá o denegará el acceso al usuario.

El cliente requerirá:

- Nombre del servidor Radius o su dirección IP.
- Puerto de autenticación y autorización.
- Puerto de contabilidad.
- La clave de autorización, la misma que debe codificar la negociación con el servidor.

4.16. Windows Server 2008

Windows Server 2008, es un sistema operativo que se utiliza en los servidores, ofrece un mayor control, flexibilidad y protección a las unidades organizativas.

En los servidores se cuenta con un active directory con su respectiva ampliación de la gestión de identidad y la directiva de grupo, brindando una administración efectiva de las políticas de seguridad en toda la red.

"Está diseñado para ofrecer a las organizaciones la plataforma más productiva para virtualización de cargas de trabajo, creación de aplicaciones eficaces y protección de redes. Ofrece una plataforma segura y de fácil administración, para el desarrollo y alojamiento confiable de aplicaciones y servicios web." (Microsoft TechNet, 2007)

Windows Server 2008 incluye el "administrador del servidor" y "server core." (Server, 2009)

Server Core. - Es una nueva opción de instalación mínima de Windows Server 2008 que admite la instalación de ciertas funciones de servidor.

Administrador del Servidor. - Es una característica especial del Windows Server 2008 donde el objetivo es interactuar con una interfaz agradable para ayudar a los administradores de tecnología de la información (TI) a adaptar los servidores.

4.17. Directorio Activo o Active Directory

El active directory es un servicio de directorio de una red de Windows, donde se almacenan todos los usuarios, dispositivos, y máquinas que están conectados a la red de una manera organizada y permite agrupar por prioridades dependiendo el cargo que desempeñe cada uno de los usuarios, y así se obtiene información centralizada, controlada y eficiente para ayudar a monitorear y localizar la información almacenada. Puede instalarse en cualquier versión del Windows Server, teniendo en cuenta las ventajas y desventajas que tenga cada una de ellas y así el administrador de red puede tomar una decisión.

Con relación al Active Directory, Angie Londoña (2013) indica que:

> *Al instalar un Directorio Activo en un sistema Windows Server en la red, convertimos a dichos equipos en Servidores de Dominio o en los controladores de dominio (Domain Controllers), los demás equipos de la red se convierten en los servidores miembros del Directorio Activo para así recibir toda la información almacenada accesible siempre y cuando se autentique correctamente en los controladores de dominio.*

Dentro del active directory, se crean las cuentas para cada uno de los usuarios que laboran en la empresa, el nombre constará de dos partes, una de ellas es el nombre completo para poder identificar con facilidad los usuarios que se vayan creando, y la otra parte es el usuario que se usará para autenticarse. Así mismo la contraseña para cada uno de los usuarios dependerá de las políticas de seguridad.

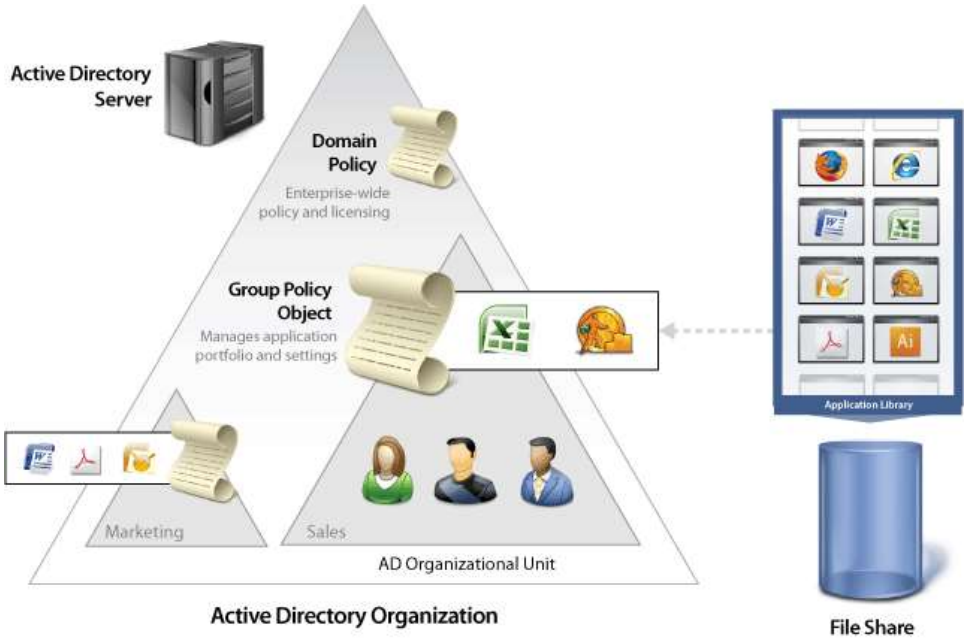

Figura 12 Implementación active directory

Fuente: (ITCONSULTANTS, 2012)

4.17.1. Unidades Organizativas

La unidad organizativa es un tipo de objeto de directorio incluido en los dominios, donde están registrados los usuarios, grupos, equipos y otras unidades organizativas, teniendo en cuenta que la UO no puede contener objetos de otros dominios, con el fin de organizar ciertos objetos en el directorio dentro de la unidad administrable; y el active directory define permisos y derechos de usuarios o grupos específicos.

Se puede decir que la unidad organizativa es como tener separada las direcciones que la empresa tenga, por ejemplo, si una empresa tiene 5 direcciones (financiero, tics, prensa, obras públicas y contratación) cada una de ellas será una unidad organizativa que tendrá su respectivos usuarios, equipos y así mismo los permisos que deberán tener para cumplir sus funciones laborables.

Las unidades organizativas pueden contener otras unidades organizativas y contar con una jerarquía dentro de un dominio, con el objetivo de reducir los dominios que requiere una red.

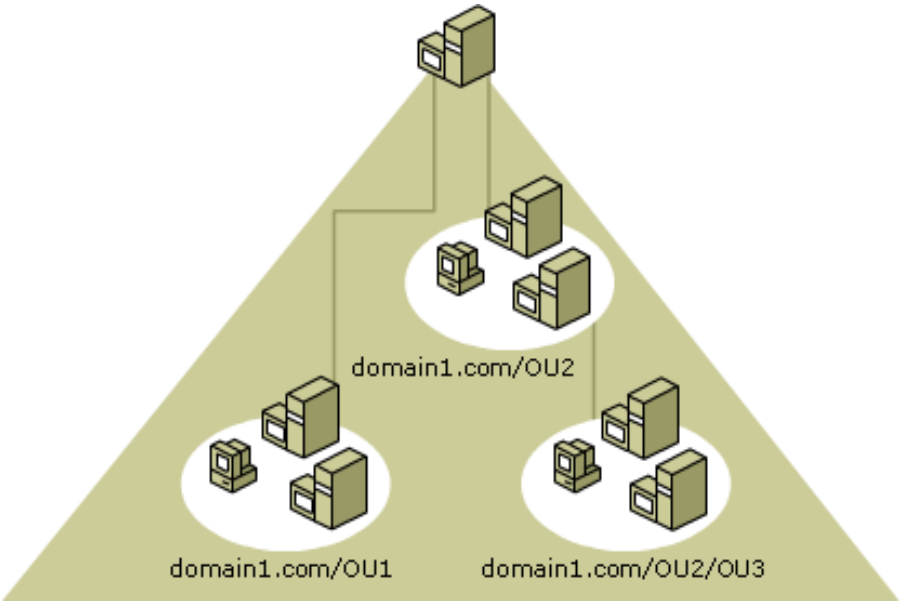

Figura 13 Unidades organizativas

Fuente: (Microsoft, Msdn Microsoft, 2005)

"Puede utilizar unidades organizativas para crear un modelo administrativo que se puede cambiar a cualquier tamaño. Un usuario puede tener autoridad administrativa para todas las unidades organizativas de un dominio o solo para una de ellas. El administrador de una unidad organizativa no necesita tener autoridad administrativa sobre cualquier otra unidad organizativa del dominio." (Microsoft, Msdn Microsoft, 2005).

4.17.2. Directivas de Grupo

Las directivas de grupos o GPO (Group Policy Object), controlan las cuentas de los usuarios y equipos, que permiten y limitan el acceso, de tal forma que el personal de la empresa no haga mal uso de los mismos.

Las directivas de grupo se clasifican con el objetivo de organizar cada nivel dentro del dominio, las configuraciones quedarán de la siguiente manera:

- **Directivas Generales:** Son aplicados para todos los miembros del bosque y dominio.
- **Directivas Personales:** Son aplicados a usuarios y equipos específicos.
- **Directivas Grupales:** Son aplicados a los grupos o unidades organizativas dentro del bosque.

Los contenedores GPO cuentan con 4 objetos que son:

- **Dominios. -** Son aplicados a todos los usuarios y equipos de un dominio.
- **Unidades Organizativas. -** Son aplicados solo a los usuarios y equipos que estén en la misma unidad organizativa.
- **Sitios. -** Son aplicados para todos los usuarios y equipos de un sitio, sin importar del dominio del mismo bosque al que pertenezcan.
- **Equipos Locales. -** Son aplicada0 solo en los equipos que no están en un dominio.

"Directiva de grupo es una infraestructura que le permite implementar configuraciones específicas para usuarios y equipos. La configuración de Directiva de grupo se encuentra en los objetos de directiva de grupo (GPO), que están vinculados a los siguientes contenedores del servicio de directorio Active Directory: sitios, dominios o unidades organizativas (OU). Los ajustes de GPO se evaluaron a continuación por los objetivos

afectados, utilizando la naturaleza jerárquica de Active Directory. En consecuencia, la directiva de grupo es una de las principales razones para implementar Active Directory, ya que le permite administrar los objetos de usuario y equipo." (Microsoft, Technet Microsoft - Group Policy GPO, 2016)

4.18. Estudio de Canal

El estándar IEEE 802.11, definió los 3 rangos de frecuencia disponibles para los dispositivos: 2.4 GHz, 3.6 GHz y 5GHz; es más común el uso de la frecuencia 2.4 GHz, pero con la tecnología MIMO ha permitido que se pueda usar la frecuencia de 5GHz y la de 2.4GHz debido a la compatibilidad que existen en los diferentes equipos. Adicional a esto, los access point ofrecen 11 canales.

Los estándares del access point son utilizados en diferentes frecuencias.

Tabla 3 Estándar del AP con su respectiva bands

Estándar	Características
IEEE 802.11b	Es uno de los principales estándares populares que se utiliza y funciona en la banda de 2.4 GHz.
IEEE 802.11g	Es el tercer estándar, el cual evoluciono del estándar 802.11b y funciona en la banda 2.4GHz.
IEEE 802.11n	Es un nuevo estándar, gracias a la tecnología MIMO que permite utilizar varios canales a la vez y funciona en la banda 2.4GHz y 5GHz.

Fuente: (Voinea, 2011)

La frecuencia de 2.4 GHz cuenta con 14 canales que se encuentran separados por 5 MHz. Teniendo en cuenta que dependiendo a la ubicación geográfico se tendrá el número de canales disponibles para transmitir las ondas. Cada canal usa 22MHz de ancho de banda para operar, lo que produce un solapamiento de varios canales contiguos.

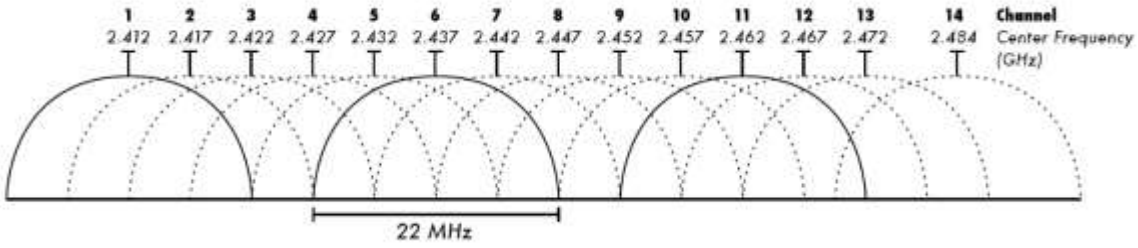

Figura 14 Canales de frecuencias

Fuente: (Alvarez, 2009)

En la figura 14 se puede apreciar que el canal 1, 6 y 11 no se superponen entre ellos, pero el canal 1 se superponen los canales 2, 3, 4 y 5; lo mismo ocurre con el canal 6 que se superponen los canales 7, 8, 9 y 10; y el canal 11 se superponen los canales 12, 13 y 14.

Debido al uso que se suele dar en un solo canal, se sugiere realizar un análisis de la disponibilidad que existe a través de alguna aplicación móvil y verificar que canal esta menos usado y cambiar el canal de la red Wi-Fi y así mejorar la red cambiando el canal existente por otro que tenga menos uso y que no se interpongan entre ellos.

4.19. Access Point

Figura 15 Access point

Fuente: (CISCO, Productos CISCO, 2016)

Un punto de acceso inalámbrico (access point) es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica, controlando el tráfico en el medio inalámbrico. Normalmente un access point también puede conectarse a una red cableada, y puede transmitir entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos access point pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar 'roaming'.

Los access point son los encargados de crear la red, están siempre a la espera de nuevos clientes para dar servicios. Dicho equipo recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada. Adicional a esto, puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de varios metros. Este o su antena son normalmente colocados en alto, pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

Los estándares del Access Point son utilizados en diferentes frecuencias.

Tabla 4 Estándar del AP con su respectiva banda

Estándar	Características
IEEE 802.11b	Es uno de los principales estándares populares que se utiliza y funciona en la banda de 2.4 GHz.
IEEE 802.11g	Es el tercer estándar, el cual evoluciono del estándar 802.11b y funciona en la banda 2.4GHz.
IEEE 802.11n	Es un nuevo estándar, gracias a la tecnología MIMO que permite utilizar varios canales a la vez y funciona en la banda 2.4GHz y 5GHz.

Elaborado por: Autores

"Este dispositivo es el punto de acceso inalámbrico a la red PC's (LAN) cableada. Es decir, es la interfaz necesaria entre una red cableada y una red inalámbrica. Considerando que son los encargados de crear una red, y están siempre pendientes de ver quiénes son los que se conectan con ellos para darle los servicios, teniendo en cuenta que dicho dispositivo es el que recibe la información, la almacena y luego hace la transmisión una vez que el usuario se haya registrado en el grupo que pertenece." (Wikipedia, 2014)

En el Access Point existen 3 tipos de acceso:

- **Modo Root:** Es donde se conecta a un backbone alámbrico a su vez muchos usuarios acceden a él al mismo tiempo.
- **Modo Repeater:** Es usado cuando se necesita extender la señal a otras zonas.
- **Modo Brigde:** Es un puente que se realiza entre los dispositivos inalámbricos de acceso, lo que permite una conexión directa entre ambos dispositivos, evitando el cableado y reduciendo costos.

4.20. Ubicación correcta de un AP

Antes de montar y desplegar un access point, se debe realizar una inspección de la zona donde está la necesidad de una conexión inalámbrica, haciendo uso de aplicaciones donde se pueda medir la cobertura de la otra access point para que no esté superponiendo entre varios canales y elegir la mejor ubicación para instalar el punto de acceso.

Es importante tener en cuenta la potencia del access point a instalar y los obstáculos que pueden existir, debido que son importantes para determinar cuánto es la distancia prudente para que no exista una reducción o pérdida de señal.

Uno de los obstáculos más comunes que existen en una red inalámbrica son las paredes, debido al material de construcción que utilizan, por lo que dificulta atravesar varias paredes que en ocasiones anulan la señal por completo.

La primera consideración es ubicar el access point en un punto céntrico del área al que se quiere dar cobertura, es decir, en el caso que se tenga una oficina cuadrada no se debe poner en una esquina porque produce pérdida de señal y disminución del área de cobertura. Por esto se recomienda colocar el access point en el centro para que todas las esquinas tengan cobertura y puedan acceder al equipo.

4.21. Equipos AP

El access point indistintos de los modelos o marca, permiten la conexión de dispositivos inalámbricos como smartphone, tarjetas inalámbricas, tablet y notebook a la red inalámbrica e inclusive hasta otros access point para ampliar las redes, cuenta con una tecnología de

comunicación capaz de traspasar muros y obstáculos, aunque la señal pierde fuerza a medida que uno se aleja del radio de cobertura.

El radio de alcance puede ser desde 30 metros hasta más de 100 metros, teniendo en cuenta que depende de la potencia del equipo, la construcción de la zona donde se va a instalar, cuantas personas promedio podría conectarse y los diferentes obstáculos que existan.

El Access Point 1600

El access point utiliza el protocolo CAPWAP como control estándar y de aprovisionamiento de otros puntos inalámbricos, para contar una mayor comunicación entre el controlador y los demás AP's en la red.

"La serie Aironet 1600 ofrece un gran rendimiento a un precio atractivo para los clientes mientras que proporciona funcionalidad avanzada como CleanAir expreso * para una mejor cobertura a través de la inteligencia del espectro y ClientLink 2.0 para redes de nivel de entrada que tienen una base de clientes mixtos. Además de estas características, la serie Aironet 1600 incluye la tecnología basada en 802.11n 3x3 múltiple entrada múltiple salida (MIMO) con dos flujos espaciales, por lo que es ideal para pequeñas y medianas empresas." (CISCO, Cisco Aironet 1600, 2014)

4.22. Comparación entre diferentes marcas de Access Point

Tabla 5 Tabla de comparación de marcas de access point

Descripción	**CISCO Access Point 1600**	**Huawei AP6510DN-AGN Access Point**
Estándar Wi-fi	802.11 a/b/g/n	802.11 a/b/g/n
Ideales para	Empresas en crecimiento o medianas.	Empresas medianas
Tipo de instalación	Interior de oficinas y bodega pequeña	-

Perfil de rendimiento de aplicaciones	Desempeño de de clase empresarial Voz/video/multimedia	Mayor rendimiento y alta densidad dirigida a las aplicaciones.
Número de Radios	Doble (2,4 GHz y 5,0 GHz)	Doble (2,4 GHz y 5,0 GHz)
Máxima velocidad de transmisión de datos	300 Mbps	600 Mbit/s
Diseño de radio MIMO: transmisiones espaciales	3 x 3:2	2 x 2
Número de clientes/Número de clientes ClientLink	128/32	≤ 256
Opción de punto de acceso autónomo	Si	-
ClientLink 2.0	Si	-
CleanAir	CleanAir Express, utiliza tecnología silicon	-
VideoStream	Si	-
Detección de puntos de acceso dudoso	Si	-
Alimentación	802.3af, adaptador de CA	PoE: –48 VCC (en cumplimiento con la norma 802.3at del IEEE)
Intervalo de temperaturas	1600i: de 0 a 40 °C 1600e: de -20 a 50 °C	-40 °C a +60 °C
Antenas	1600i: interna 1600e: externa	Antena de polarización doble o antena común externa
Precio	$ 695,00	$ 1.108,5171

Fuente: (Cisco, 2016) ,(Technologies, 2012)

Se debe utilizar equipos cisco, debido a que cuenta con la fiabilidad, seguridad avanzada, escalabilidad y garantía del producto; además que son fáciles de configurar y de usar para la red con un precio de inversión para el Gobierno Provincial del Guayas.

4.23. Comparación entre CISCO Access Point

Tabla 6 Tabla de comparación de access point cisco

Descripción	Access Point 1600	Access Point 2600
Estándar Wi-fi	802.11 a/b/g/n	802.11 a/b/g/n
Ideales para	Empresas en crecimiento o medianas.	Empresas en crecimiento, medianas o grandes.
Tipo de instalación	Interior de oficinas y bodega pequeña	Interior de oficinas y bodega mediana.
Perfil de rendimiento de aplicaciones	Desempeño de de clase empresarial Voz/video/multimedia	Optimizado para cualquier dispositivo/BYOD Escalabilidad de clientes Mitigación de interferencias de RF
Preparada para el futuro	-	-
Zonas concurridas	-	Si
Número de Radios	Doble (2,4 GHz y 5,0 GHz)	Doble (2,4 GHz y 5,0 GHz)
Máxima velocidad de transmisión de datos	300 Mbps	450 Mbps
Diseño de radio MIMO: transmisiones espaciales	3 x 3:2	3 x 4:3
Número de clientes/Número de clientes ClientLink	128/32	200/128
Opción de punto de acceso autónomo	Si	Si
ClientLink 2.0	Si	Si
CleanAir	CleanAir Express, utiliza tecnología silicon	Si
VideoStream	Si	Si
Detección de puntos de acceso dudoso	Si	Si
Alimentación	802.3af, adaptador de CA	802.3af, adaptador de CA
Intervalo de temperaturas	1600i: de 0 a 40 °C 1600e: de -20 a 50 °C	2600i: 0 a 40 °C 2600e: -20 a 55 °C
Antenas	1600i: interna 1600e: externa	2600i: interna 2600e: externa
Precio	$ 695,00	$ 712,00

Fuente: (Cisco, 2016)

Entre los modelos disponibles de la marca cisco, se elige el access point 1600 porque es adecuado para las oficinas remotas (galpones y huertos) del Gobierno Provincial del Guayas, donde no se cuenta con muchos usuarios por lo cual es considerada una institución mediana.

Cisco CleanAir

Es una tecnología desarrollada para el rendimiento del estándar 802.11ac y la fiabilidad de soportar las aplicaciones, dando una mayor automatización con el rendimiento de una red WLAN lo que promueve que exista una solución más efectiva y la reducción del tiempo inactivo.

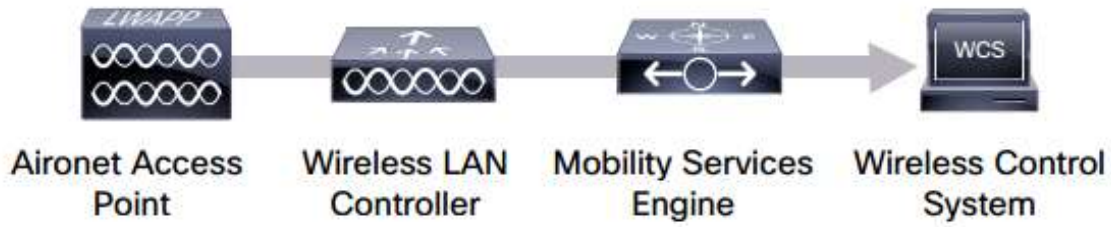

Figura 16 Componentes del cleanair

Fuente: (Cisco, 2014)

"La tecnología Cisco CleanAir Express está habilitada en el diseño de silicio avanzada de la Segunda del Cisco Generación de nivel de entrada los puntos de acceso, tales como la basado en 802.11n Cisco Aironet 1600 Series y la Cisco Aironet 1700. 802.11ac basados Con Aire Limpio Expresar el Aironet 1600 y 1700 puntos de acceso tienen la capacidad de detectar de manera efectiva la interferencia de RF, identificar la fuente, localizarlo en un mapa, y luego hacer automática ajustes para optimizar la cobertura inalámbrica. Con Clean La tecnología Air Express, las organizaciones tienen una capacidad de análisis de espectro para apoyar su inalámbrico redes al tiempo que simplifica las operaciones en curso." (Cisco, 2014)

4.24. Controladora de Wireless (WLC)

La controladora de wireless ofrece los siguientes beneficios para las pequeñas o grandes empresas, considerando la importancia que se ha tenido con las redes inalámbricas de gran escala.

- Reducción de costos de operación general.
- Simplicidad en la gestión de redes.
- Control centralizado.
- Flexibilidad en la configuración de las políticas.

Estos beneficios permiten mejorar la operatividad y reducir el costo total de implementación, y al contar con una sola red facilita la escalabilidad y flexibilidad en la rede alámbrica o inalámbrica.

El WLC ofrece gran disponibilidad entre el access point y el cliente que desee autenticarse, evitando así que el usuario tenga algún tipo de demora o inconveniente para autenticarse en el equipo y a su vez este equipo hace consulta sobre las VLANs a la que pertenece y el respectivo permiso que cuenta, este equipo se maneja por el SSID (Service Set Identifier – Nombre de la red inalámbrica). Los usuarios invitados tendrán un acceso limitado a la red e Internet.

Esto proporciona un mejor control sobre el tráfico de invitado y mayor seguridad de la red. Los usuarios invitados generalmente se autentican mediante la web.

"Los controladores inalámbricos de Cisco reducen los gastos operativos mediante la simplificación de despliegue de red, operaciones y gestión. Configurar la directiva inalámbrica, la administración o la configuración de seguridad en cualquier momento a

través del aprovisionamiento y gestión centralizada. Responder al crecimiento de la organización con el modelo de licencia escala -como- que - crece Cisco, disponible con todos los controladores inalámbricos de Cisco." (CISCO, Cisco - Wireless LAN Controller, s.f.)

5. Marco metodológico

5.1 Fuentes de Información

Las fuentes de información son donde se encuentran los datos requeridos que posteriormente se pueden convertir en información útil para el investigador. Los datos son todos aquellos fundamentos o antecedentes que se requieren para llegar al conocimiento exacto de un objeto de estudio. Estos datos que se deben recopilar de las fuentes, tendrán que ser suficientes para poder sustentar y defender un trabajo. (Eyssautier, 2002)

5.1.1 Fuentes primarias

Se refieren a aquellos portadores originales de la información que no han retransmitido o grabado en cualquier medio o documento la información de interés. Esta información de fuentes primarias la tiene la población misma. Para extraer los datos de esta fuente se utilizan los método de encuesta, de entrevista, experimental o por observación. (Eyssautier, 2002)

La recopilación de información necesaria para la elaboración del presente proyecto, se realizará mediante entrevistas a los usuarios de las diferentes direcciones del Gobierno Provincial del Guayas ubicados en galpones y huertos, y al personal a cargo del departamento de redes.

5.1.2 Fuentes Secundarias

Se refieren a todos aquellos portadores de datos e información que han sido previamente transmitidos o grabados en cualquier documento y utilizan el medio que sea esta información se encuentra a disposición de todo investigador que la necesite. (Eyssautier, 2002)

Se consultará a las áreas responsables en el Gobierno Provincial del Guayas y sitios web de proveedores de tecnología para obtener información primera respecto al proyecto en desarrollo.

Se hará uso de la información disponible en manuales de procedimiento y en las normativas vigentes en el área de redes.

5.2 Técnica de Investigación

Investigación Cualitativa

La investigación cualitativa se enfoca a comprender y profundizar los fenómenos, explorándolos desde la perspectiva de los participantes en un ambiente natural y en relación con el contexto. (Roberto Hernández Sampieri, 2010)

Este tipo de investigación no usa una medición numérica para descubrir o interpretar resultados, más bien usa el lenguaje verbal, donde puede obtener respuestas como si se estuviera dialogando con cualquier persona, tomando la forma de una entrevista, narración, video, entre otros, con el fin de obtener la descripción a partir de las observaciones.

Tabla 7 Descripción de la investigación cualitativa

	Características	Proceso	Bondades
Cualitativa	Explora los fenómenos en profundidad, se conduce básicamente en ambientes naturales, los significados se extraen de los datos y no se fundamenta en la estadística	Inductivo, Recurrente, Analiza múltiples realidades subjetivas y no tiene secuencia lineal.	Profundidad de significados, Amplitud, Riqueza interpretativa y contextualizada el fenómeno

Fuente: (Roberto Hernández Sampieri, 2010)

Se hará uso de la investigación cualitativa para comprender la perspectiva de los usuarios, recolectar información sobre el diseño de red inalámbrica, conocer sus experiencias y la forma en que perciben su realidad. (Roberto Hernández Sampieri, 2010)

Adicionalmente, la investigación cualitativa permite familiarizarse con el tema y conocer con mayor profundidad la realidad, características de conexión, nivel tecnológico, total aproximado de usuarios. Considerando que la investigación cualitativa se enfoca más en la parte teórica donde se realiza por medio de encuestas o diálogos abiertos para obtener una interpretación propia y determinar cuál sería la mejor solución ante cualquier anomalía que refleje en los resultados obtenidos de la técnica usada. Por ejemplo, si Pedro entrevista a Juan se conocerá su opinión y permite sacar conclusiones propias, luego Pedro entrevista a Diana y obtendrá otro resultado, y así sucesivamente; por lo que se tendrá que analizar cada una de las entrevistas que se realizó y sacar una conclusión general.

5.3 Fases de la Investigación Cualitativa

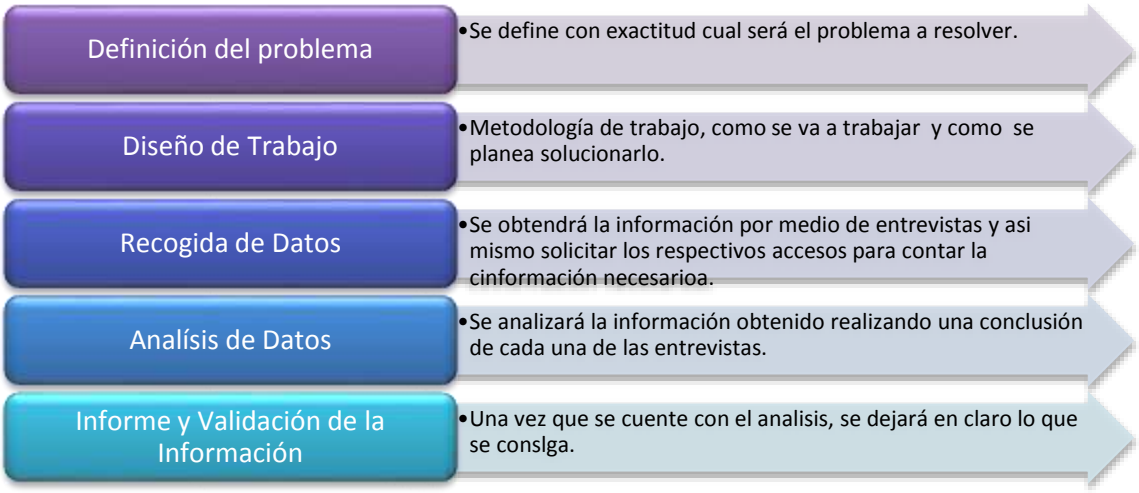

Figura 17 Fases de la investigación cualitativa

Elaborado por: Autores

5.4 Método de Investigación

Este método tiene el fin de ofrecer mejoras y cambio en los problemas identificado y es la ruta que se sigue en las ciencias para alcanzar un fin propuesto y la metodología el cuerpo de conocimiento que describe y analiza los métodos para el desarrollo de una investigación. Ambos se han particularizado y son objeto de un tratamiento especial de acuerdo con cada particular.

5.5 Técnicas de Recolección de Información

Como técnica de recolección de información se elige la entrevista. Esta se realizará mediante conversación formal con el personal del Gobierno Provincial del Guayas.

5.5.1 ¿Qué es una entrevista?

La entrevista se entiende como una conversación de tipo verbal entre dos o más personas (interrogador e interrogado) para la obtención de un propósito expreso.

Nahoum (1985) define la entrevista como: "Un intercambio verbal que nos ayuda a reunir datos durante el encuentro de carácter privado y cordial, donde una persona se dirige a otra y cuenta su historia, da su versión de los hechos y responde a preguntas relacionadas con un problema específico"

La entrevista es una de las técnicas más utilizadas en el método cualitativo, donde se asume una postura de conversación entre el entrevistador y el sujeto a investigar o quien ofrece la información deseada.

5.5.2 Entrevista Trabajo

Este es un tipo de entrevista también denominada entrevista estructurada, la cual tiene la finalidad de facilitar la información, es decir que el entrevistador se traslada al área de trabajo y es ahí donde obtiene toda la información que desee, utilizando las preguntas que ya tiene lista para no perder tiempo.

Se utilizará una entrevista no estructurada, debido a que no es necesario seguir un guion, es decir es más flexible porque según las respuestas que se tengan, se pueden sacar más preguntas para tener el panorama más claro y especifico.

5.5.3 Puntos que deben considerarse en una entrevista

Las preguntas serán distintas dependiendo del informante seleccionado, debido a que no todos los informantes tienen el mismo conocimiento sobre el tema a investigar

Gisela Díaz y Rafaela Andrés Ortiz (2015) aportan como puntos importantes a tener en cuenta los siguientes:

- Preguntas en las que es importante determinar los hechos (se pregunta directamente por la información deseada)
- Determinación de las creencias (que es lo que la gente cree que son los hechos)
- Determinación de sentimientos (identificar las reacciones emocionales)
- Descubrimiento de normas reacción (estas se dividen en dos partes, su criterio ético o lo que debe hacerse y su criterio practico o lo que es posible hacer)
- Contenido dirigido a la pregunta presente o pasada (la forma en que se haya comportado con respecto a una situación)
- Contenido dirigido a las razones consientes para las creencias, sentimientos, normas de comportamiento (que razones tiene el interrogado para sostener sus creencias, sentimientos, normas de conducta o comportamientos, es asegurar una respuesta total a la pregunta ¿Por qué?)

En base a los puntos antes mencionado, se determinó los puntos importantes a considerar en la presente entrevista.

- Determinar el problema que existe con la red.
- Determinar las oficinas remotas que tienen problemas y cuantos usuarios tiene cada una.

- Determinar los motivos que no permitieron implementar la solución.
- Determinar qué tipo de solución prefieren y por qué.
- Cuáles son los objetivos de contar con una red inalámbrica.
- Determinar con quien se hablará para llegar a un acuerdo sobre las normas de confidencialidad y seguridad para establecer que información puede ser publicada en la documentación.

5.5.4 Objetivos de la Entrevista

Al realizar la entrevista se debe lograr un buen clima donde exista confianza y respeto para lograr una excelente comunicación, comenzando con una presentación profesional explicando la razón de la entrevista y tomando el registro de lo que se comente en ella.

- Obtener la información sobre la red existente.
- Obtener información sobre las personas entrevistadas sobre el uso que le dan a la red.
- Identificar las principales diferencias entre la red implementada con la red propuesta.
- Obtener la información sobre los problemas que existen al no contar con una red inalámbrica.
- Obtener información si desean contar con una red inalámbrica la cual puedan acceder a ella, siempre y cuando cuenten con un dispositivo o una tarjeta inalámbrica.

5.5.5 Entrevista a Informantes Clave

Se realizarán entrevistas a los involucrados en el presente proyecto, se definirá el alcance, levantamiento de los requerimientos técnicos, y la puesta en práctica de recomendaciones técnicas y de profesionales en el área de estudio. Entre los principales involucrados están:

- Ing. Patricio Ordoñez Bustamante, director provincial de tecnologías de la información y comunicación – TICS, es el encargado de autorizar la ejecución del proyecto y a su vez comunicar a las áreas involucradas para que brinden la información solicitada, para tal efecto se debe cumplir con un acuerdo de confidencialidad y seguridad con la información que se almacena en los servidores de la institución.
- Sr. José Martin Barreiro, personal del departamento de redes, es el encargado de indicar las políticas y dar acceso al sistema para la implementación del servidor RADIUS.
- Ing. Pablo Tapia Bastidas, jefe del departamento de soporte técnico, conoce los incidentes suscitados en las diferentes oficinas remotas y tiene el conocimiento de los equipos y materiales que han adquirido para la ejecución del proyecto.
- Sr. Wilson Apolo, Ing. Daniel Vera, Ing. Luis Regalado y el Ing. Giovanni Podestá, son los técnicos asignados para acompañar en los recorridos en las oficinas remotas de galpones y huertos e identificar las zonas de cobertura.

La entrevista se realizará en el lugar de trabajo de cada uno de los entrevistados para no interferir mayormente con sus actividades diarias

Tabla 8 Entrevista de informantes claves

Entrevista	Asistentes	Objeto
1	Director Provincial de TICs	Planteamiento de objetivos que se pretende conseguir tras la ejecución del proyecto. Concretar horarios de visita. Funciones y Limitaciones en la línea de trabajo.
2	Jefe Departamento de Redes	Configuración e infraestructura de la red. Seguridad WLAN. Señal WIFI en algunas zonas del GPG
3	Jefe de Soporte Técnico	Conocer las actividades que se han venido desempeñando, equipos y materiales.
4	Usuarios Galpones y Huertos	Conocer punto de vista del usuario

Elaborado por: Autores

5.6 Instrumentos

Guía

Se utilizará una guía, debido a que no es una estructura de preguntas, más bien se trata de tener una lista de los temas a tratar de manera específica y de ahí tener opción de agregar temas a la lista.

Herramientas

Se utilizará una grabadora, siempre y cuando el entrevistado lo permita, sino se tendrá que usar una libreta o cuaderno para anotar lo que vaya indicando el entrevistado y así sacar conclusiones propias.

6. Análisis y Diseño De La Red

6.1 Análisis de la Situación Actual

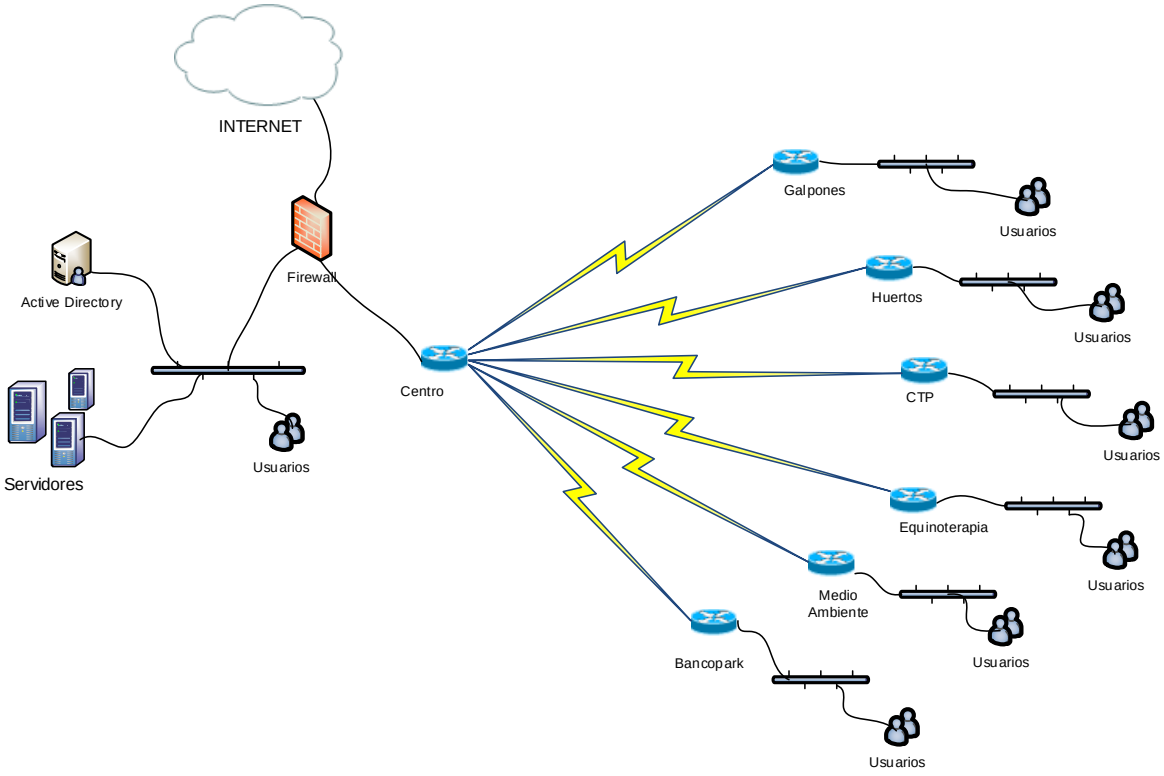

Figura 18 Diagrama actual de la red

Elaborado por: Autores

En años anteriores, el Gobierno Provincial del Guayas realizó inversiones para la renovación de su infraestructura tecnológica. Su tecnología de comunicación se basa en equipos de la marca cisco.

La figura 18 muestra la infraestructura actual de comunicación de las oficinas remotas (galpones, huertos, ctp, equinoterapia, medio ambiente y bancopark), donde existe una

topología estrella de conexión, en la que todos los routers de los sitios remotos dirigen sus comunicaciones hacia y desde la matriz, que está ubicada en el edificio principal del Gobierno Provincial del Guayas.

En la red actual se puede indicar que las oficinas remotas del Gobierno Provincial del Guayas como centro tecnológico popular – CTP, equinoterapia, medio ambiente, bancopark y el edificio principal cuentan con la instalación de los access point.

Existe un active directory que maneja el registro de cada uno de los usuarios, con las políticas de contraseña que la entidad maneja y los servidores que almacenan las diversas plataformas informáticas con las que cuenta la institución.

Las funciones de los siguientes componentes que forman la red actual son:

- Servidores con los que cuenta la entidad pública: ofrecen diferentes servicios según la necesidad que existe dentro de una red de computadoras, por ejemplo se cuenta con servidores físicos y virtuales, los cuales son correo, DNS, VoIP, antivirus, sistema de gestión pública (SGP), sistema de gestión documental (SGD), sistema inteligente de gestión públicas (SIGPU), entre otros.
- Active directory: Almacena la información de equipos y usuarios, para identificar a que área o dirección pertenece y tener un mayor control. Se hace uso de las restricciones que se puede realizar a través del active directory de las políticas de unidad organizativas, políticas de pantalla, vista clásica del panel, quitar elementos de la pantalla al panel de control, no podrá agregar impresoras, usuario solo permitido en una sola máquina para autenticarse y varias opciones más. Con el active directory se maneja las políticas de uso de equipos y servicios de red, acceso a panel de control, cambios de configuración, rutas de carpetas de red, permisos de internet, ancho de

banda, uso de pendrives, autenticación de sistemas de terceros como correo, sistema de gestión pública (SGP), sistema de gestión documental (SGD), sistema inteligente de gestión públicas (SIGPU) y entre otros.

- Firewall: Se encarga de proteger a los equipos individuales, servidores o equipos conectados a la red, teniendo el acceso para evitar el robo de información confidencial, alteración de la información o en algunos casos la eliminación de los mismos e incluso ataques de denegación de los servicios a la red. Cada subred cuenta con su firewall, el mismo que tiene asignada algunas reglas como administración de los accesos de los usuarios a los servicios, registrar todos los intentos de entrada y salida de una red que serán almacenados en logs, filtro de direcciones, filtro de protocolos, controlar el número de conexiones que se están produciendo desde un mismo punto, controlar las aplicaciones que puedan acceder a internet y la detección de puertos que están en escucha y no deberían estarlo; por lo tanto si la información que viaja hacia el firewall cumple con las reglas establecidas podrá acceder a la misma.
- La funcionalidad del segmento de la red: Es dirigir todo el tráfico que envíe el usuario desde la oficina remota a la que pertenezca (galpones, huertos, ctp, equinoterapia, medio ambiente y bancopark) hacia la sede centro, dado que ahí residen todos los servicios que presta la institución.
- Centro: Es la matriz principal del Gobierno Provincial del Guayas, donde se encuentran todos los equipos y servicios que realizan la verificación de la autenticación con los datos que ingrese desde cualquier oficina remota, en este caso es la central de las demás instalaciones de la institución donde se comunican de

manera directa a través del VPN usando un usuario y contraseña indicado hacia el centro.

- En galpones, huertos, ctp, equinoterapia, medio ambiente y bancopark se encuentran los usuarios que hacen uso del VPN para conectarse a la matriz y así poder acceder a los servicios que la institución posee. Por seguridad del almacenamiento, no todos poseen usuario y contraseña VPN .
- Usuarios: Una vez identificadas las necesidades que tiene el funcionario del Gobierno Provincial del Guayas, se deberán presentar los formularios de acceso a internet, acceso a la red, acceso a la red inalámbrica, creación de correo, instalación de software, perfil de usuario y redes sociales los mismo que están disponible en el portal interno de la institución. Para el uso de las plataformas informáticas que existen en la entidad, el director del área requirente deberá realizar un oficio al director provincial TICs.

6.2 Requerimientos de la solución

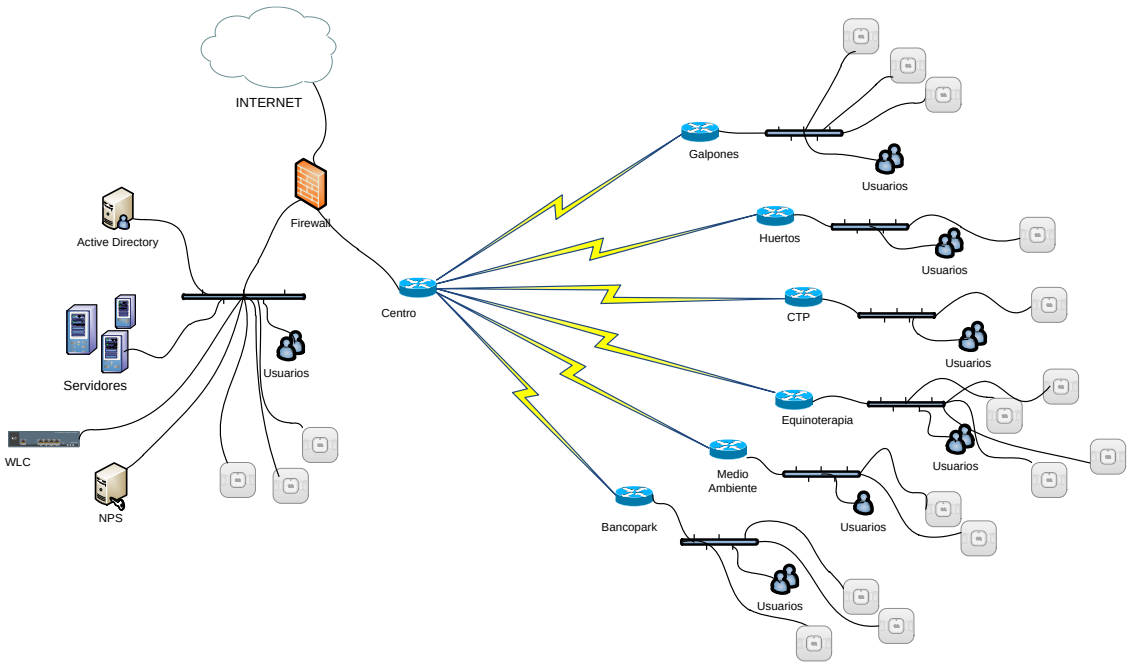

Figura 19 Diagrama propuesto de la red

Elaborado por: Autores

El Gobierno Provincial del Guayas cuenta con un edificio principal y oficinas remotas, las cuales son galpones, huertos, ctp, equinoterapia, medio ambiente y banco park. En el presente proyecto se proveerá de tecnología inalámbrica con autenticación a todas las instalaciones de la Prefectura del Guayas, se deberá instalar los access point (AP) en cada una de las oficinas remotas y edificio principal; y su vez se crearán políticas de red, en conjunto con el jefe de infraestructura tecnológica para tener un bien en común.

Una de las principales ventajas que brindan las redes inalámbricas es permitir una gran movilidad, el poder desplazarse de un lugar a otro y poder conectarse a la red. Se realizan estos trabajos por las varias reuniones que se realizan en esta área, de las que se han contabilizado. Esto genera gran movilización de personas entre departamentos (muchos de ellos utilizando portátiles). Teniendo en cuenta que la ubicación de los access point se considera a través de la cantidad de usuarios críticos y que no tenga electricidad magnética (EM) que ocasionaría perdida de señal.

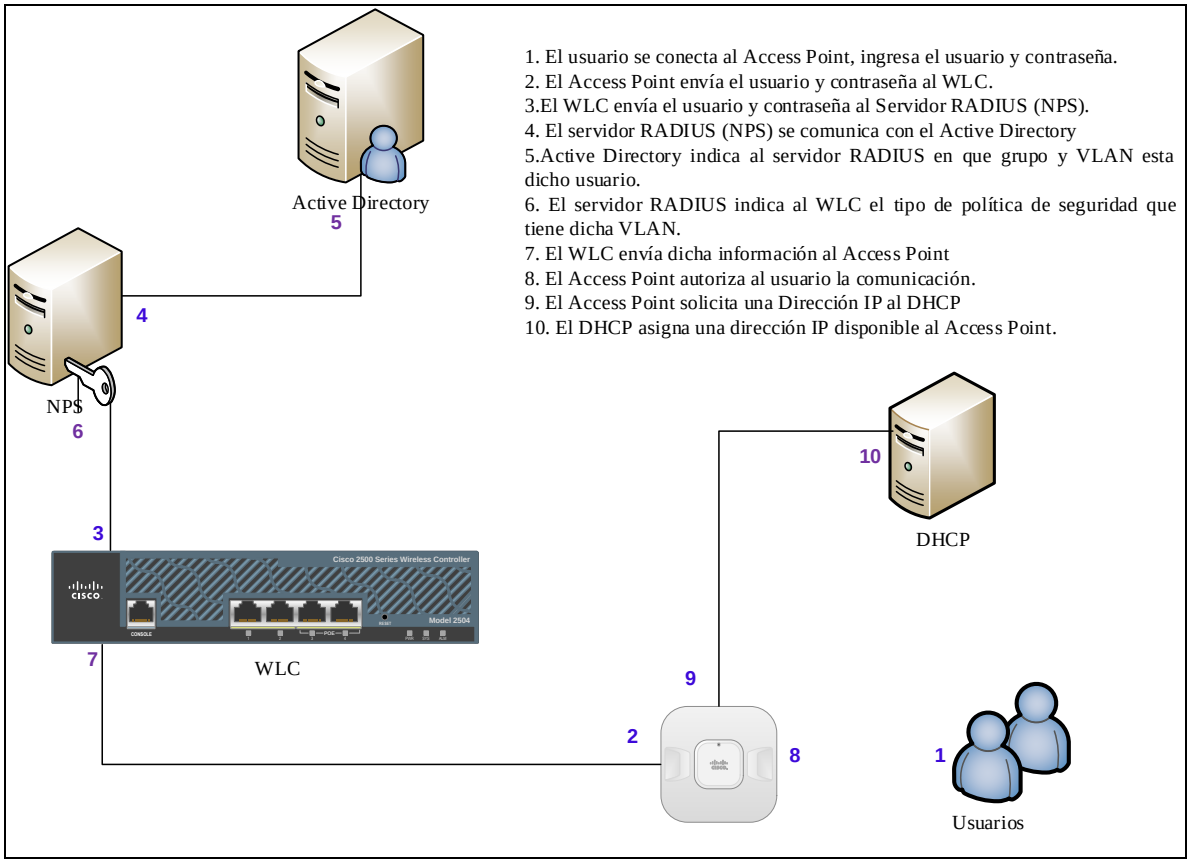

Figura 20 Funcionamiento de la propuesta

Elaborado por: Autores

Las funciones de los siguientes componentes que se añadieron que forman la red propuesta son:

- **Servidor RADIUS (NPS). -** Recibe del Wireless LAN Controllers el usuario y la contraseña, recordando que el Servidor RADIUS es conocido como las 3A o AAA (Autenticación, Autorización y Administración), donde se comunica con el Active Directory para revisar en que grupo y en que VLAN está el usuario y contraseña ingresado considerando que estos datos pasan de manera encriptado, a su vez el NPS indicará que tipo de política de VLAN tendrá el usuario que quiera autenticarse.
- **Access Point. -** Los equipos access point tienen un sitio web donde se llenan todos los parámetros para la configuración en cada uno de los equipos con el usuario y contraseña de la red, y en caso de cambiar la contraseña se deberá cambiar en cada uno de los equipos. Para automatizar este, se ha procedido a proponer como solución el uso del Wireless LAN Controllers para su respectiva configuración, una vez que establezca la conexión con el WLC, el DHCP le asignara la dirección IP para conectar a la red interna y al internet.
- **Wireless LAN Controllers.-** Este equipo se encarga de gestionar la configuración global de todos los access point que estén conectados, teniendo en cuenta que todos los equipos de marca cisco poseen el cisco discovery protocol (CDP). El Wireless LAN Controllers recibe el usuario y contraseña del access point y así mismo cuando el servidor RADIUS (NPS) envíe la confirmación de que VLAN y que políticas debe tener usuario ingresado, por tanto, el WLC se encargará de permitir la conexión.

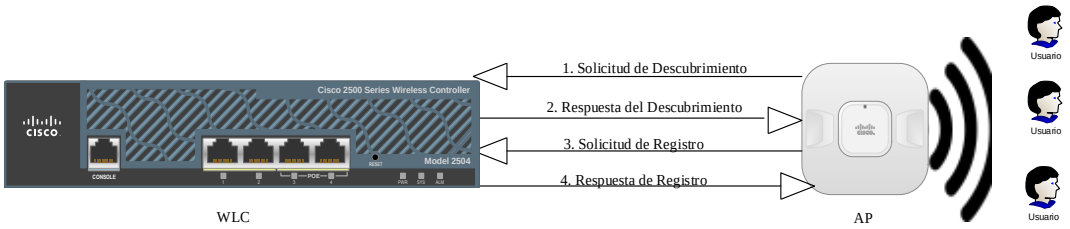

Figura 21 Funcionamiento del WLC con el AP

Elaborado por: Autores

Después del análisis se determina que la solución propuesta consiste en la instalación de:

- Galpones – 3 Access Point
- Huertos – 1 Access Point

Considerando que los access point que se detallan a continuación ya fueron instalados por el Gobierno Provincial del Guayas.

- CTP – 1 Access Point
- Equinoterapia – 4 Access Point
- Banco Park – 3 Access Point
- Medio Ambiente – 2 Access Point
- Planta Baja Edificio Principal – 1 Access Point
- Mezzanine Edificio Principal – 2 Access Point
- 1er piso Edificio Principal – 4 Access Point
- 2do piso Edificio Principal – 3 Access Point
- 3er piso Edificio Principal – 3 Access Point

- 4to piso Edificio Principal – 3 Access Point
- 5to piso Edificio Principal – 3 Access Point

Los access point que se instalaron por parte de los autores y del Gobierno Provincial del Guayas serán administrados de forma centralizada por el Wireless LAN Controller (WLC) en el edificio matriz, junto con el software de administración Wireless Control System (WCS).

Al existir disponibilidad de conexión inalámbrica en estas oficinas remotas, será posible realizar reuniones más productivas y seguras para la institución. La actual infraestructura de comunicación del Gobierno Provincial del Guayas es marca cisco, y a fin de garantizar la compatibilidad, los equipos que formen parte de la solución inalámbrica también serán de la marca cisco.

6.3 Ubicación de Access Point

Haciendo uso de la herramienta free NetSpot, se cargó el plano del primer piso del edificio central y por medio de los access point instalados se realizó el estudio de campo con el fin de determinar la cobertura actual de la señal wireless. Los 4 access point de este piso serán administrados de forma centralizada por el Wireless LAN Controller desde el departamento de redes. La infraestructura de comunicaciones actual del Gobierno Provincial del Guayas es marca cisco, y a fin de continuar con el 100% compatibilidad, los equipos requeridos para la red seguirán siendo de esta misma marca.

PLANTA BAJA EDIFICIO CENTRAL

En la figura 22 se aprecia que existe un solo access point en la planta baja, debido a la ubicación de servicios institucionales, la señal inalámbrica llega con una intensidad de (-80dBm), lo mismo sucede en el área de ventanillas de financiero y en recepción de Prefectura (-80dBm).

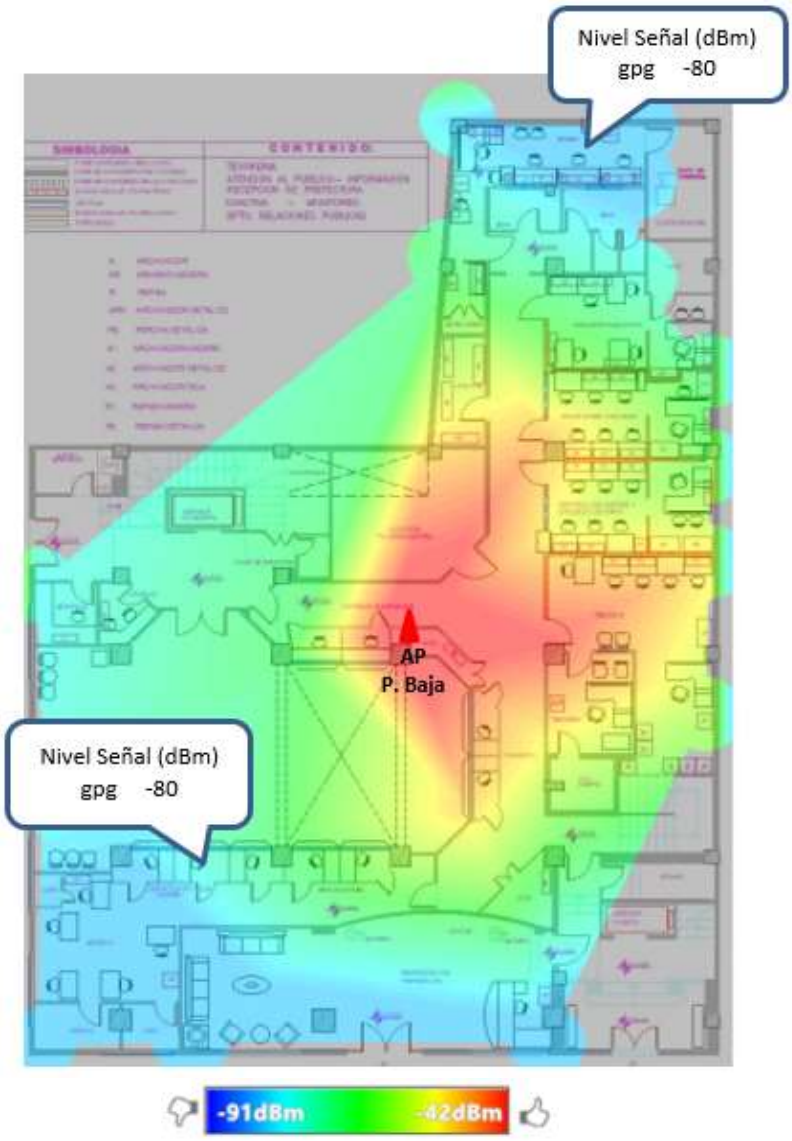

Figura 22 Intensidad de señal de los access point de la planta baja edif. central

Fuente: Herramienta NetSpot

MEZZANINE EDIFICIO CENTRAL

La figura 23 se puede notar que existe una baja intensidad de señal (-83dBm) en el departamento de presupuesto, al igual que en archivo de contabilidad con (-86dBm).

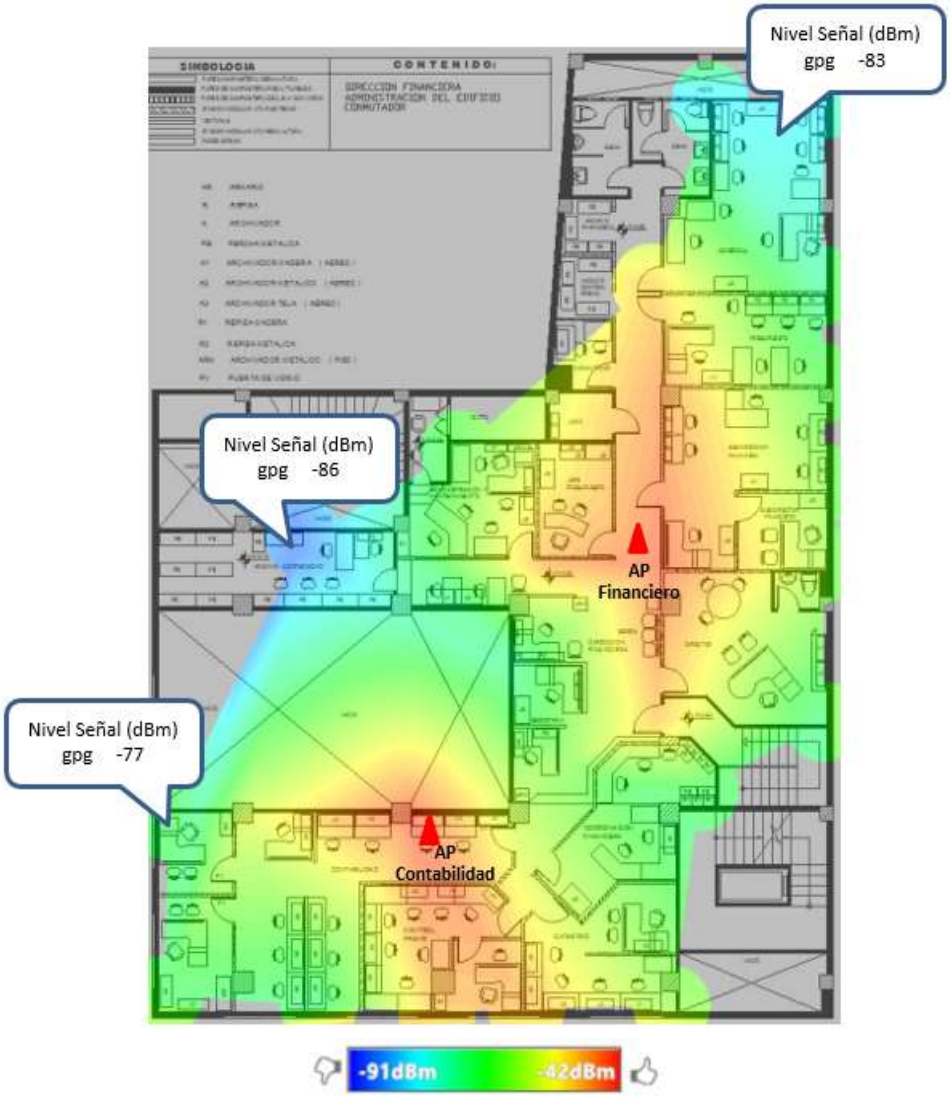

Figura 23 Intensidad de señal de los access point del mezzanine edif. central

Fuente: Herramienta NetSpot

PRIMER PISO EDIFICIO CENTRAL

La figura 24 muestra el resultado de la revisión, donde se presentan los 4 access point, se indica también la fuerza de la señal recibida, donde el color rojo es una buena señal y el color azul es una señal mala. Puede notarse que en el departamento de desarrollo y secretaría de TICs la intensidad de señal (-87dBm) es muy baja lo que genera caídas y cortes en la conexión.

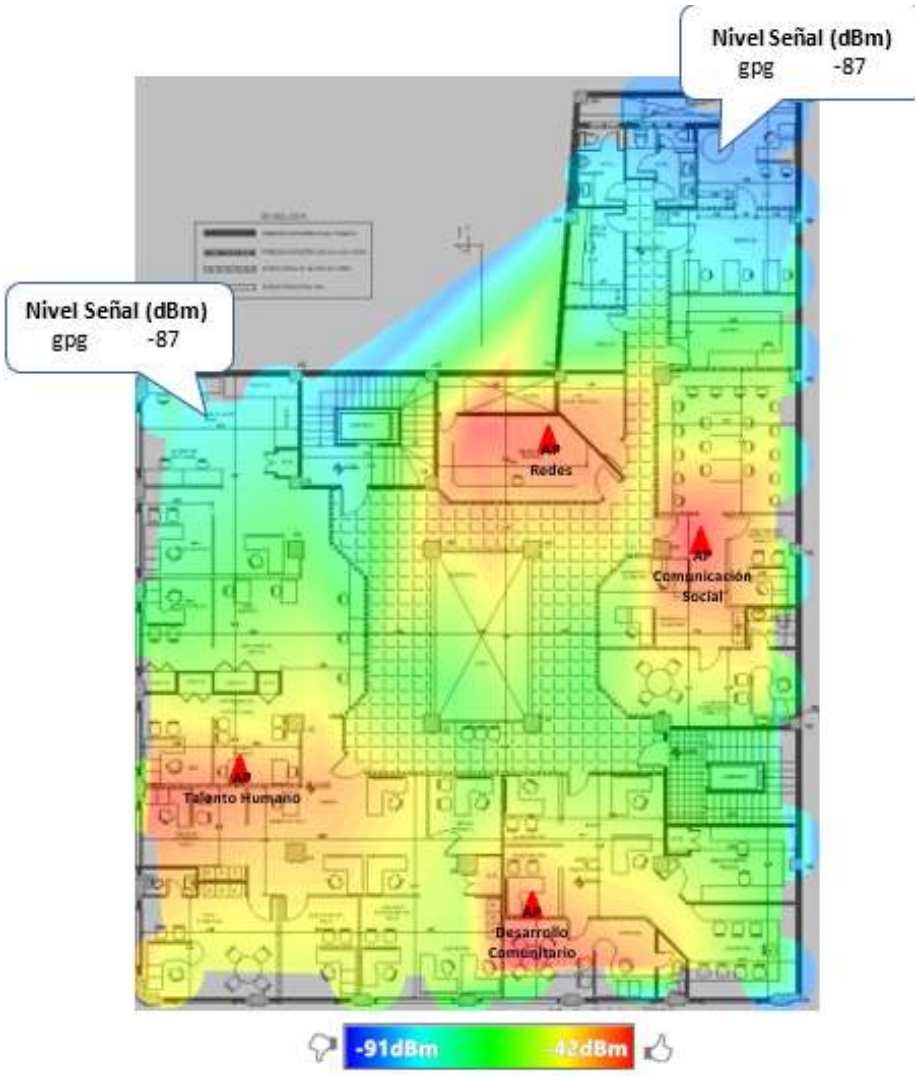

Figura 24 Intensidad de señal de los access point del 1er piso edif. central

Fuente: Herramienta NetSpot

SEGUNDO PISO EDIFICIO CENTRAL

En el segundo piso, existe un access point en cada departamento, la figura 25 muestra que existe cobertura en todo el piso, con una buena intensidad de señal en los puntos más alejados.

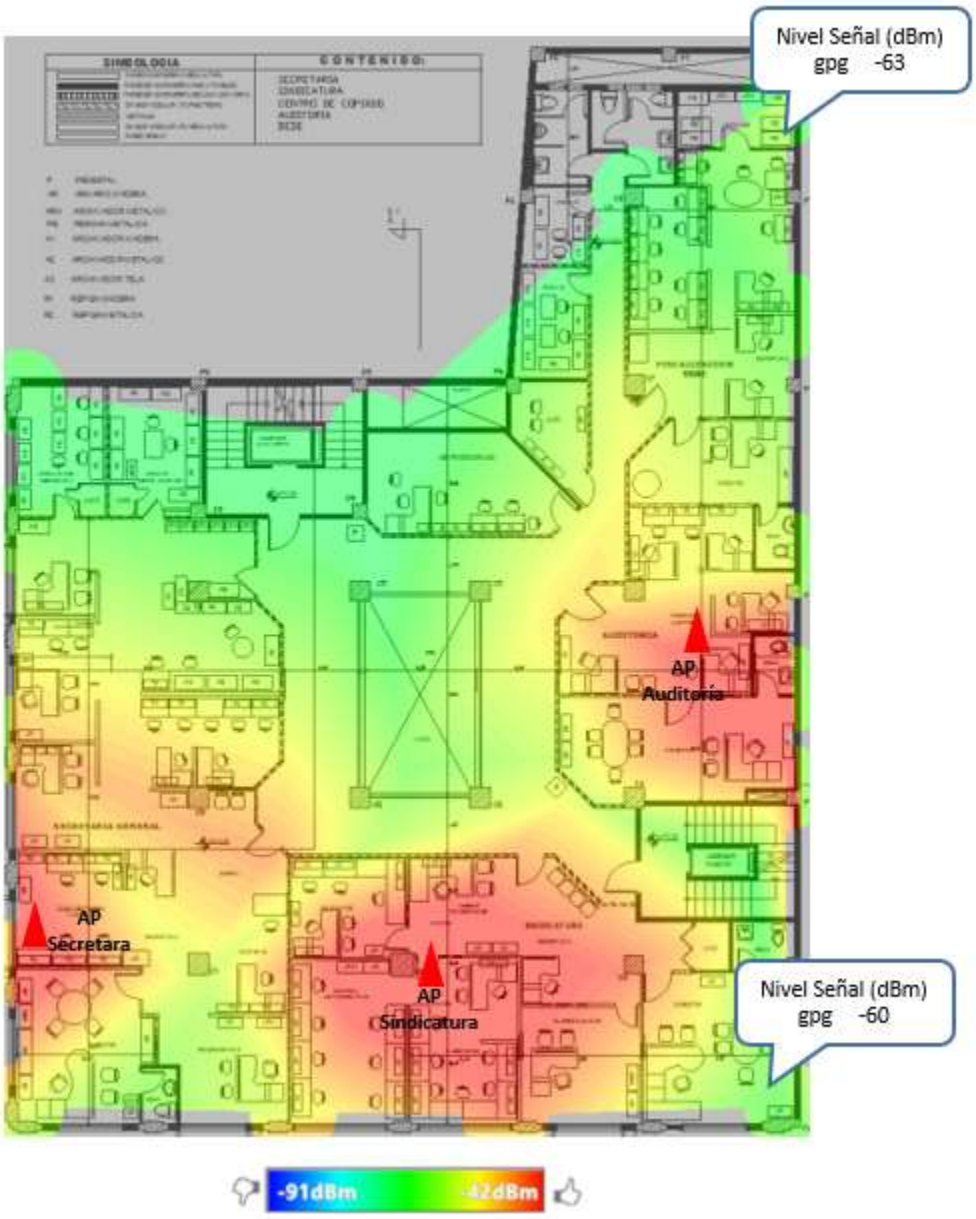

Figura 25 Intensidad de señal de los access point del 2do piso edif. central

Fuente: Herramienta NetSpot

TERCER PISO EDIFICIO CENTRAL

Los 3 access point instalados en el tercer piso brindan cobertura en todo el piso, con una buena intensidad de señal en los puntos intermedios, tal como se muestra en la figura 26.

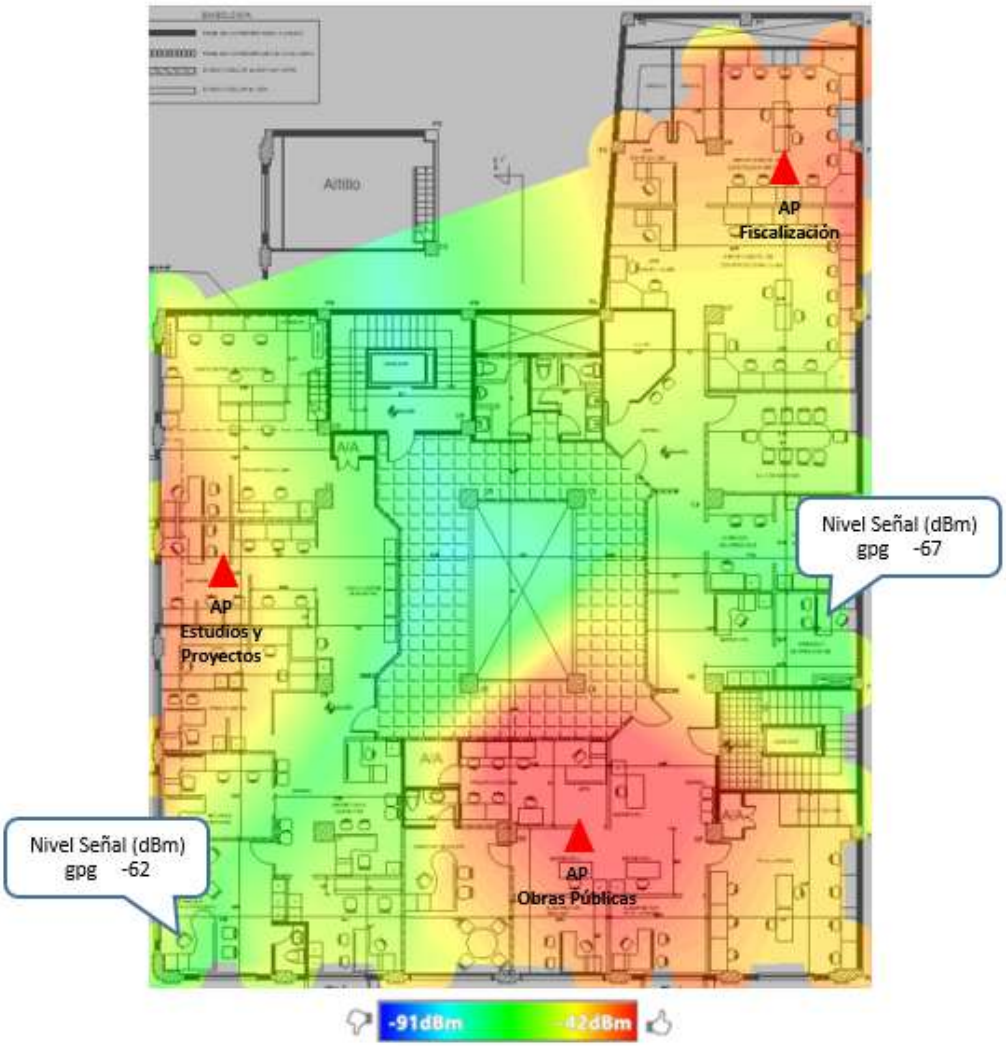

Figura 26 Intensidad de señal de los access point del 3er piso edif. central

Fuente: Herramienta NetSpot

CUARTO PISO EDIFICIO CENTRAL

La figura 27 muestra una regular intensidad de señal (-72dBm) en la dirección de equidad social, y una baja intensidad de señal en las cercanías del access point de viceprefectura.

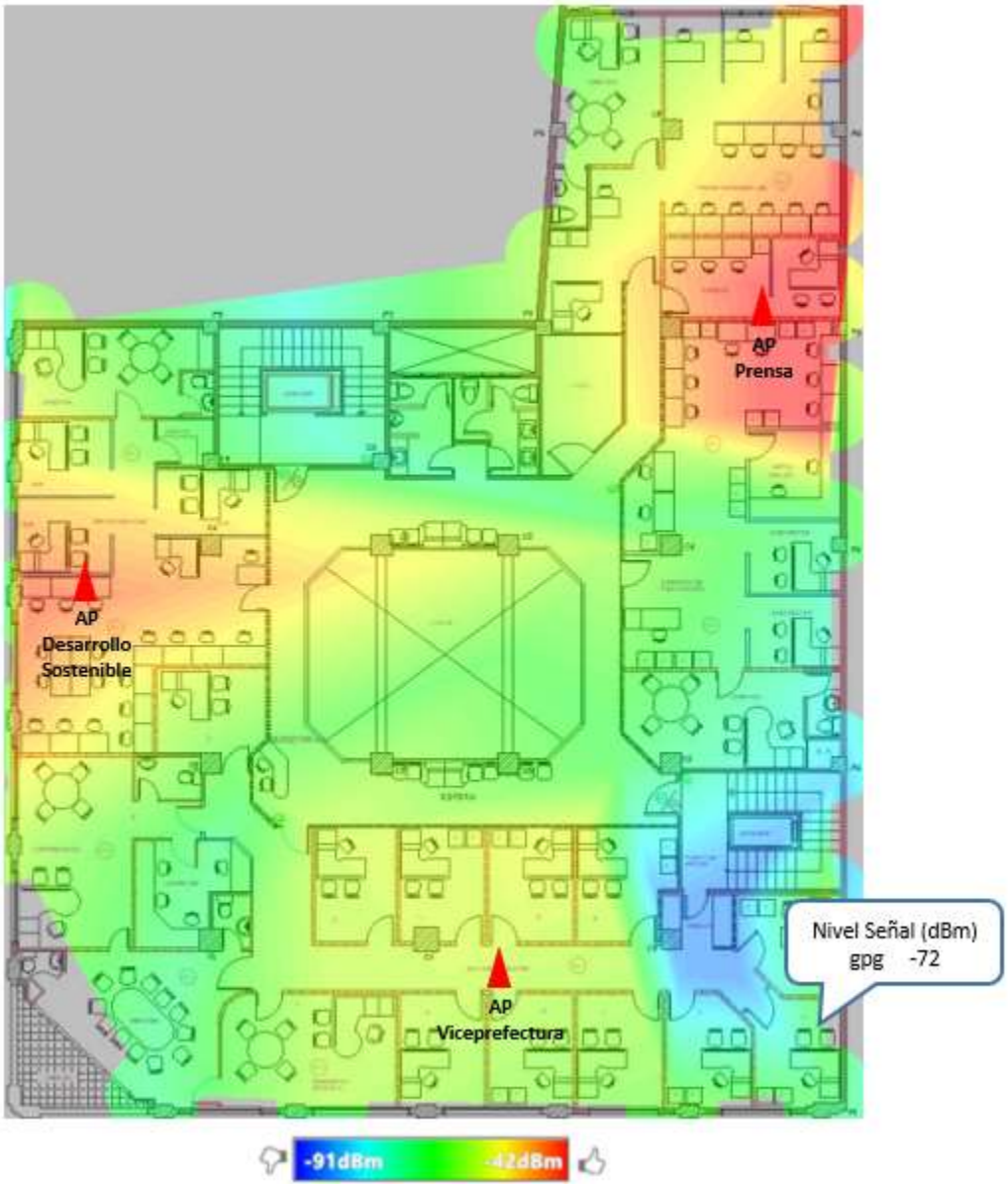

Figura 27 Intensidad de señal de los access point del 4to piso edif. central

Fuente: Herramienta NetSpot

QUINTO PISO EDIFICIO CENTRAL

La figura 28 muestra que en las oficinas de asesoría de viceprefectura la intensidad de señal (-76dBm) lo que ocasiona desconexiones de la red inalámbrica.

Figura 28 Intensidad de señal de los access point del 5to piso edif. central

Fuente: Herramienta NetSpot

EDIFICIO BANCOPARK PISO 14

El departamento de mediación tiene una baja cobertura inalámbrica (-87dBm), existen intermitencia en las conexiones, y lentitud en la navegación. Las oficinas de riego, drenaje y dragas tienen una cobertura de (-76dBm) como se muestra en la figura 29.

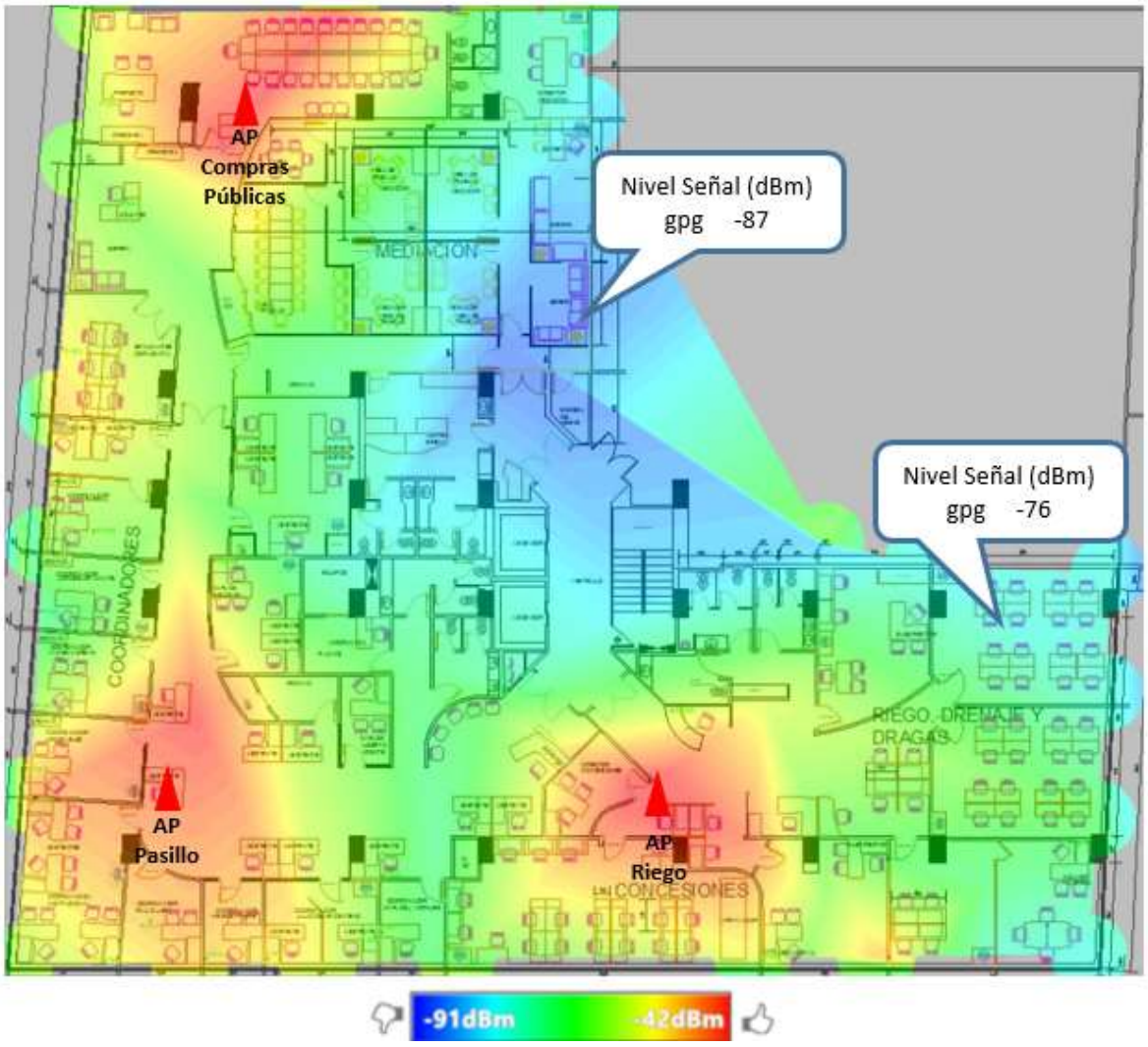

Figura 29 Intensidad de señal de los access point del piso 14 edif. bancopark

Fuente: Herramienta NetSpot

CENTRO TECNOLÓGICO POPULAR

En la figura 30 se puede apreciar que existe un access point para todo el CTP el mismo que se encuentra en el vestíbulo, la intensidad de las señal en los laboratorios 1 y 4 es baja (-84dBm y -82dBm) respectivamente. La baja cobertura no afectada en las operaciones porque en estos laboratorios si existe una red cableada.

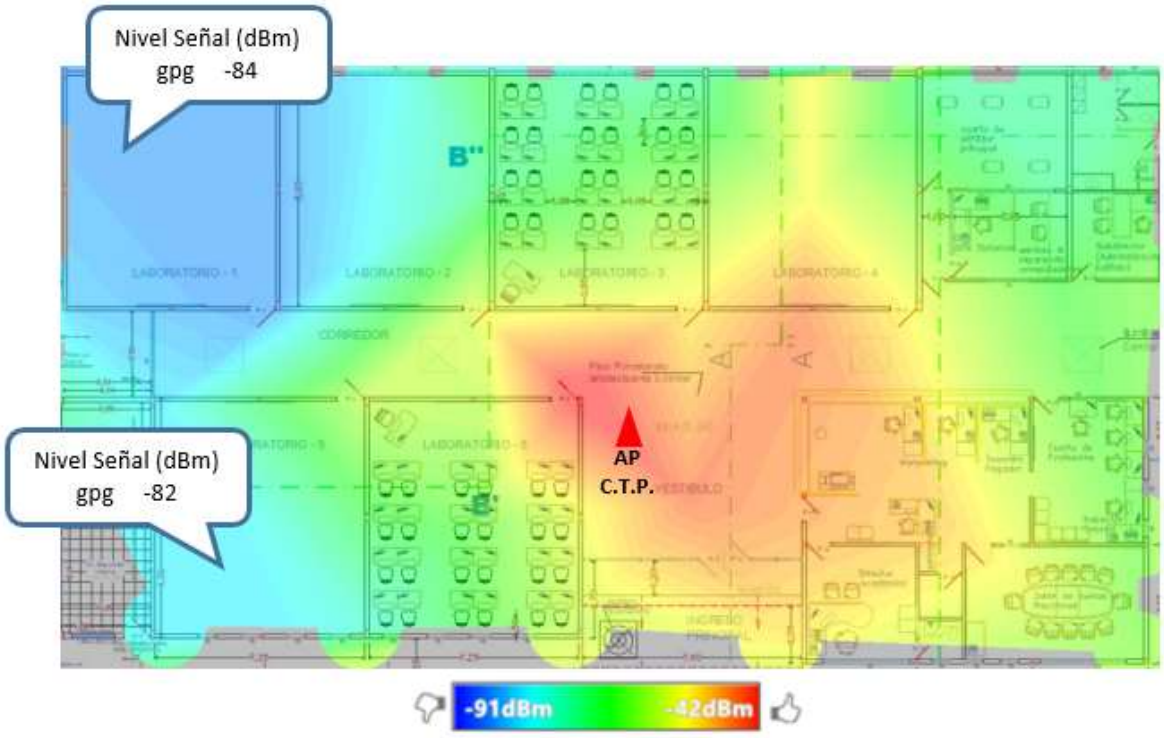

Figura 30 Intensidad de señal de los access point del CTP

Fuente: Herramienta NetSpot

MEDIO AMBIENTE EDIFICIO TOUS

Existen 2 access point que dan cobertura a medio ambiente, se puede notar en la figura 31 que existe una buena intensidad de señal en estas oficinas.

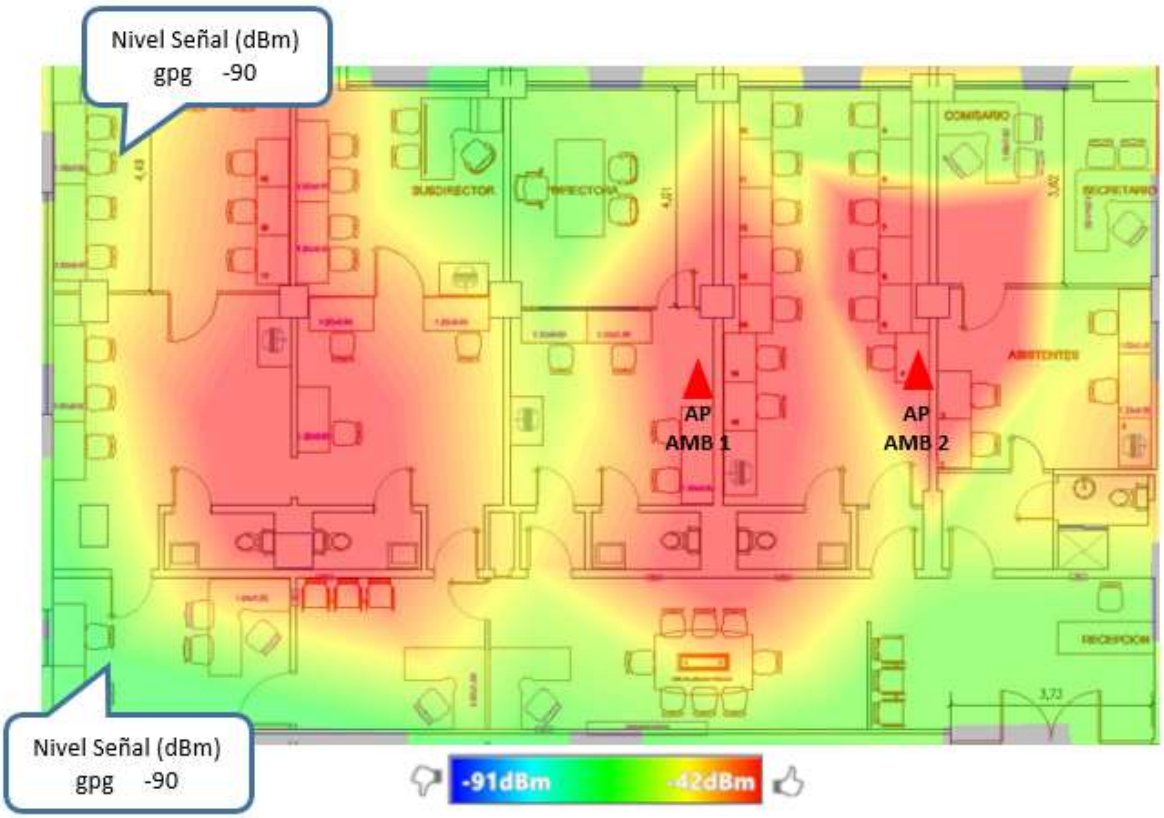

Figura 31 Intensidad de señal de los access point de medio ambiente

Fuente: Herramienta NetSpot

CENTRO INTEGRAL EQUINOTERAPIA

Como se aprecia en la figura 32, existe cobertura en las oficinas administrativas de equinoterapia, sin embargo, la intensidad de la señal en las oficinas prefabricadas donde se brindan terapias la intensidad de la señal es de (-74dBm)

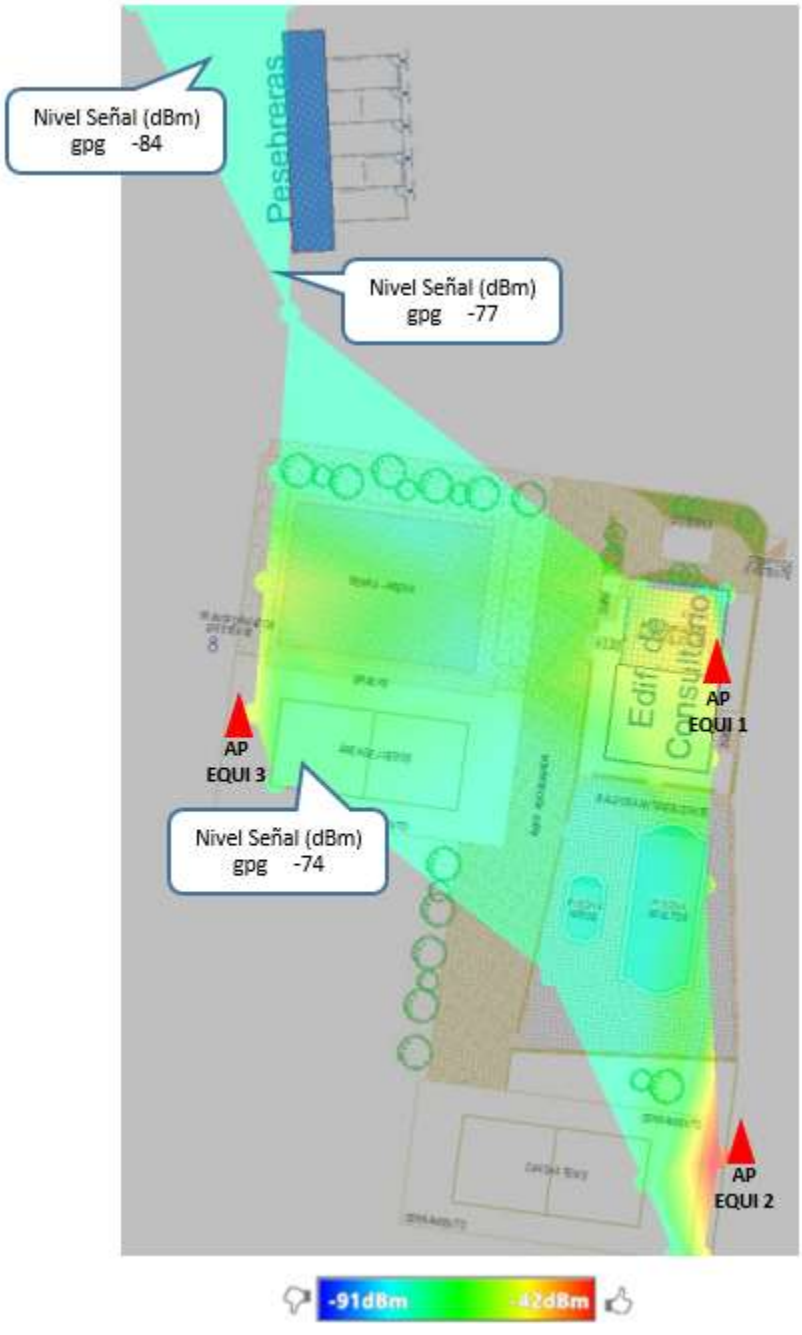

Figura 32 Intensidad de señal de los access point de equinoterapia

Fuente: Herramienta NetSpot

7. Configuración del Wireless LAN Controllers

Se debe conectar el Wireless LAN Controllers – WLC con el cable de consola a la computadora portátil de trabajo que se ha usado.

Se debe cancelar la instalación automática del controlador para que se pueda configurar con los parámetros establecidos en conjunto con el jefe de infraestructura tecnológica (Redes).

a) Se asigna el nombre del sistema '**cntapcen1**', el mismo que tiene como máximo 32 caracteres ASCCI para ingresar el nombre de la controladora.
b) Se introdujo el usuario y contraseña administrativa del equipo, el cual por seguridad debe ser ingresado y no dejarlo por default.
c) No se activó la interfaz para obtener una dirección IP por medio del servidor DHCP, por lo tanto, se ingresó una dirección estática con su respectiva máscara de red.
d) Se desactivó el link de agregación (LAG - Link Aggregation), debido a que no se cuenta con más de dos WLC.
e) Se registró la dirección IP, máscara de red y la VLAN. Considerando que la VLAN es opcional dado que puede ser válido o sin etiqueta.
f) Se ingresó la dirección IP para la interfaz virtual del controlador. Esta interfaz virtual ayudará en la gestión de la movilidad, la retransmisión de DHCP y la seguridad a través de un sitio web para la autenticación.
g) Se ingresó el nombre de los dos grupos de movilidad, en uno de ellos se encuentra los AP del auditorio y la sala de reuniones y el otro grupo se encuentran los demás AP.
h) Se ingresó el nombre de la red SSID 'GPG', es decir el nombre de los AP que los usuarios podrán ver desde los dispositivos inalámbricos.

i) Se introduce un “NO”, para que el usuario solicite una dirección IP al servidor DHCP.

j) Se configura el servidor RADIUS, se ingresó la dirección IP, máscara de red, puerto de comunicación y la clave del servidor.

k) Se introduce el código del país donde se instalará el controlador, el cual es Ecuador ECU.

l) Se habilitó los estándares de las redes inalámbricas como la 802.11b, 802.11a, 802.11g y 802.11n.

m) Se habilitó el servidor externo Network Time Protocol (NTP) ingresando la dirección IP.

n) Se guarda todo lo configurado y se reinicia el equipo para iniciar sesión.

Como se observa en la figura 33, se muestra el detalle general de la controladora, el cual indica el nombre que se asignó al equipo, la dirección IP del grupo multicast, el nombre del dominio de movilidad, el nombre del grupo RF, se indica el tipo de autenticación a través de la web es PAP y se habilita la configuración del IPv6.

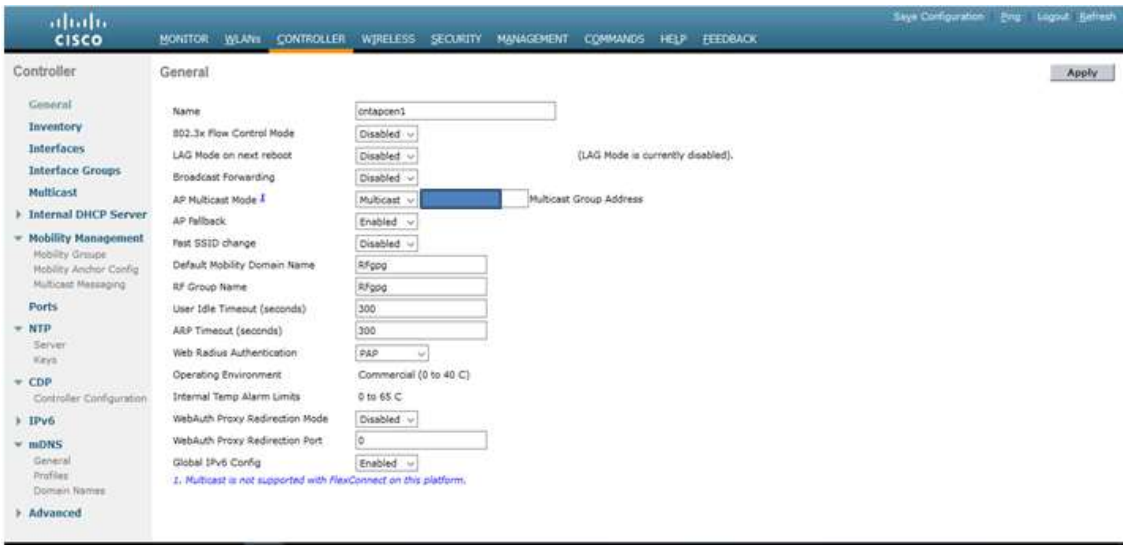

Figura 33 Interfaz general de la controladora

Fuente: WLC CISCO

En la figura 34, se muestran los miembros del grupo de movilidad estáticas, donde se indica la dirección MAC, dirección de red, nombre del grupo, la dirección IP multicast, clave única y el estado del miembro.

Figura 34 Interfaz de los grupos móviles

Fuente: WLC CISCO

En la figura 35, se muestra la configuración que se hizo en la controladora considerando que el Cisco Discovery Protocol – CDP, viene habilitado por default en la mayoría de las interfaces, lo que permite poder cambiar la versión en la que trabaja el protocolo, esto permite detectar automáticamente a todos los dispositivos marca cisco vecinos que estén conectados directamente.

Figura 35 Interfaz de la configuración del Cisco Discovery Protocol – CDP

Fuente: WLC CISCO

En la figura 36, se muestra que no se habilitó el proxy DHCP, se escoge la opción 32 del DHCP el cual permite a un Agente Relay del protocolo de configuración dinámica de host (DHCP) incluir la información sobre sí mismo al remitir los paquetes DHCP originados por el cliente a un servidor DHCP y se determinó que el tiempo de espera de DHCP es de 120 segundos.

Figura 36 Interfaz del parámetro de DHCP

Fuente: WLC CISCO

En la figura 37, se puede visualizar que se activó el modo controlador maestro, esta opción se utiliza para agregar más access point en la misma subred, porque permite verificar la configuración del AP y asignar controladores primario, secundario y terciario.

Figura 37 Interfaz de la habilitación del controlador maestro de los AP's

Fuente: WLC CISCO

8. Configuración del Servidor RADIUS

Se procedió a configurar los siguientes puntos y se podrá visualizar en las figuras, que rol o que la actividad se realizó, una vez creada la máquina virtual en Windows Server 2008 dentro del aplicativo VMWARE Player.

a) Se configura la controladora del servidor de dominio, agregando el rol de Active Directory Domain Services (Ver figura 38), el cual se procede con la instalación del Active Directory Domain Services Installation Wizard, se creó un nuevo dominio para el árbol y se asigna una contraseña de administrador (Ver figura 39).

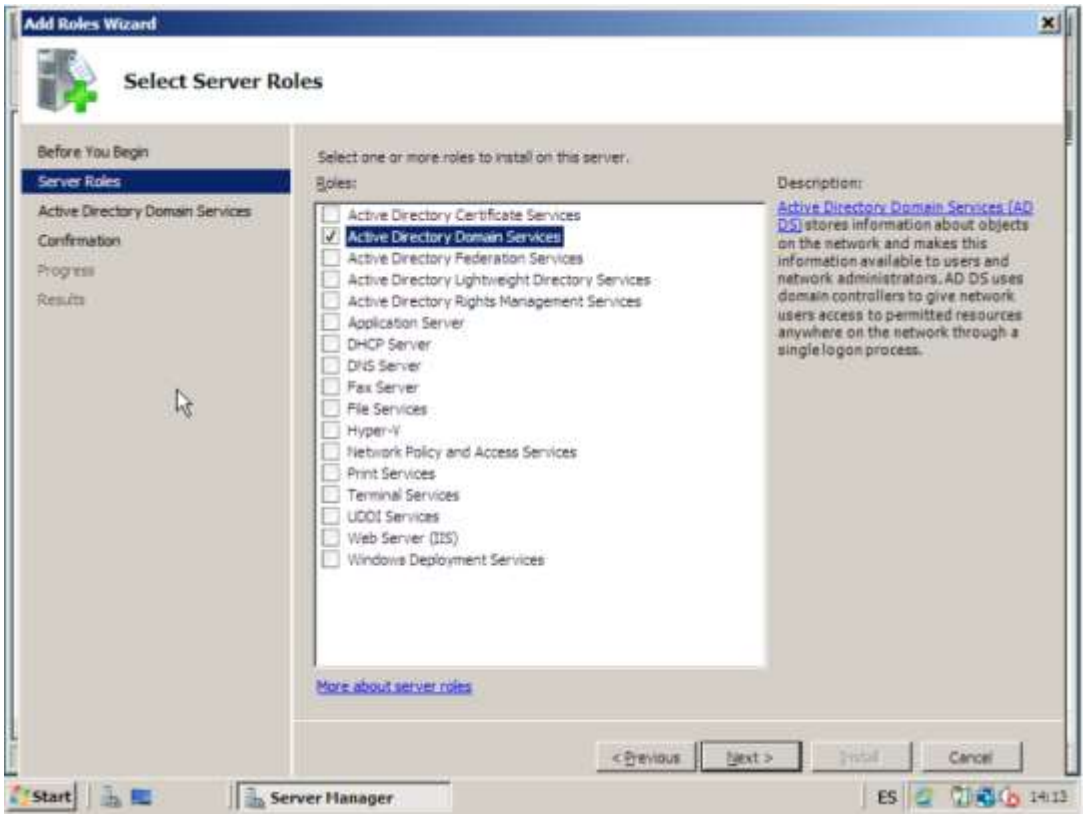

Figura 38 Interfaz de la Activación del Active Directory Domain Services

Fuente: Windows Server 2008

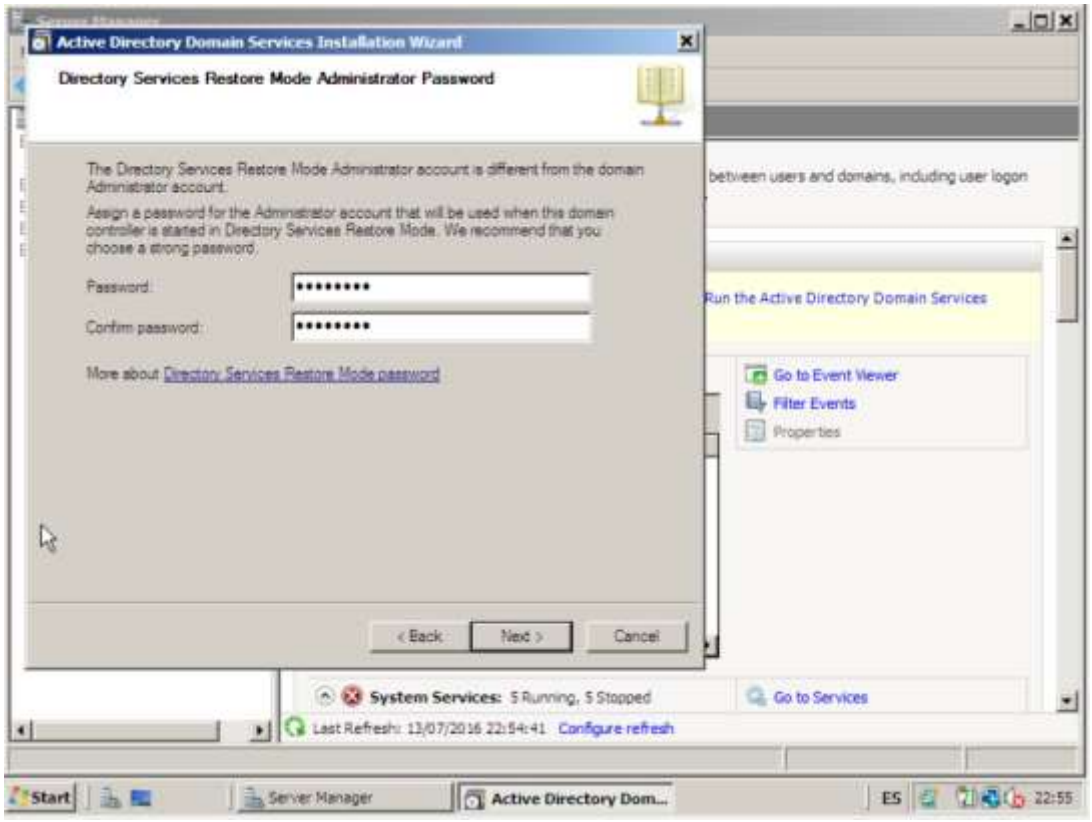

Figura 39 Interfaz del ingreso de la clave administradora

Fuente: Windows Server 2008

b) Se instala y configura los servicios DHCP, añadiendo el rol DHCP Server (Ver figura 40), luego la respectiva configuración del servidor DHCP que deberá proveer direcciones IP al cliente (Ver figura 41), se indicó que no se necesita el Windows Internet Naming Service – WINS para esta red, se habilita el DHCPv6 modo estático para este servidor, se configura el IPv6 DNS, se autorizó el certificado del dominio administrador del servidor DHCP en el Active Directory y se finaliza la instalación.

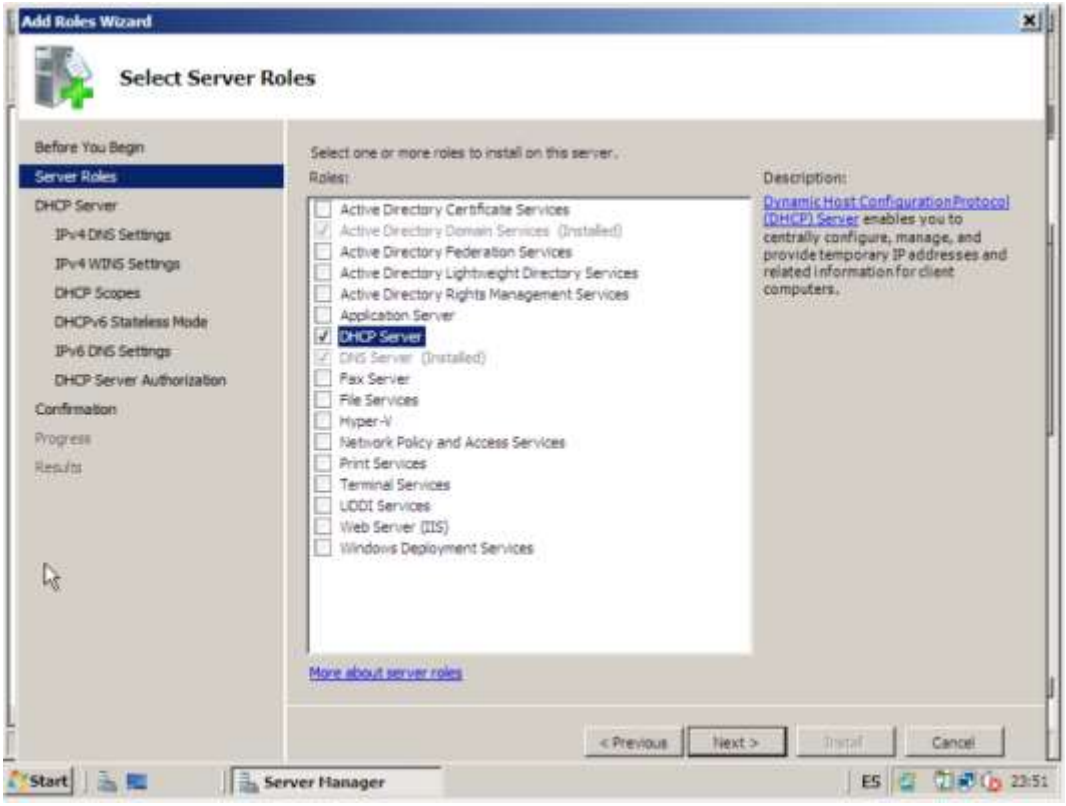

Figura 40 Agregando el rol de DHCP SERVER

Fuente: Windows Server 2008

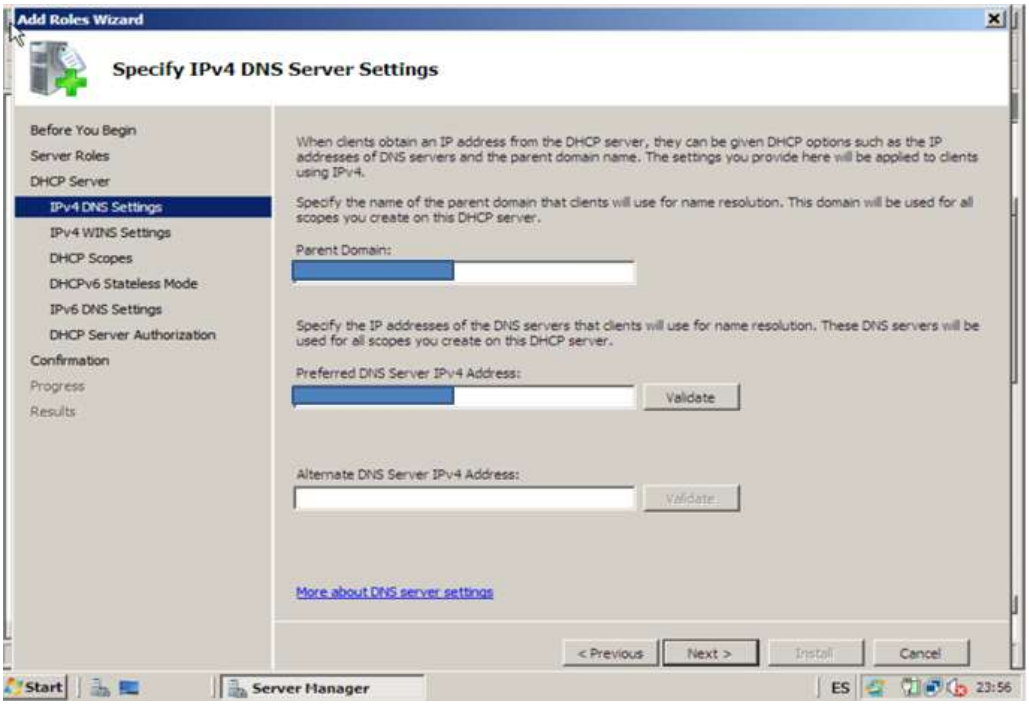

Figura 41 Interfaz de la asignación de la IP del DHCP Server

Fuente: Windows Server 2008

c) Se instala y configura en el servidor los certificados de autenticación del servidor, teniendo en cuenta que el certificado del servidor debe ser emitido por la entidad de certificación publica que sea de confianza para el equipo cliente, debe existir dentro de la carpeta de certificación raíz de confianza del almacén de certificados de equipo cliente; dando inicio agregando el rol de Active Directory Certificate Services (Ver figura 42), se selecciona el certificado de autorización que es usado para emitir y gestionar certificados, donde se especificó que el tipo de certificado que se tiene que usar es Enterprise dado que el CA utiliza los datos del Active Directory, se seleccionó el Root CA porque va hacer la primera y la única autoridad de certificación en una infraestructura de clave pública (Ver figura 43), se crea una clave privada, se configura la criptografía del Certificado de Autorización, por default se deja el nombre del certificado, se indica el periodo de validez del certificado, por default se deja la ubicación de la base de datos donde se almacenara el CA y se finaliza con la instalación del certificado de autorización.

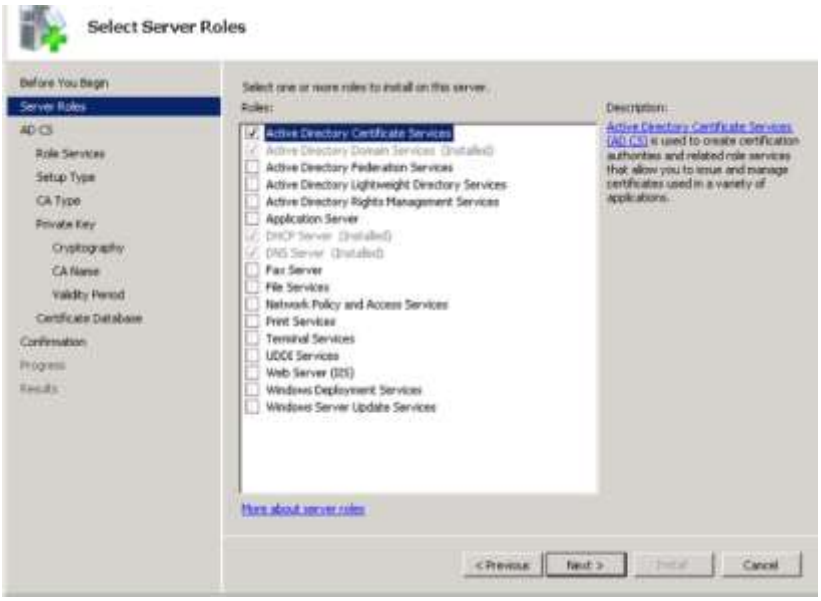

Figura 42 Agregar el Active Directory Certificate Services

Fuente: Windows Server 2008

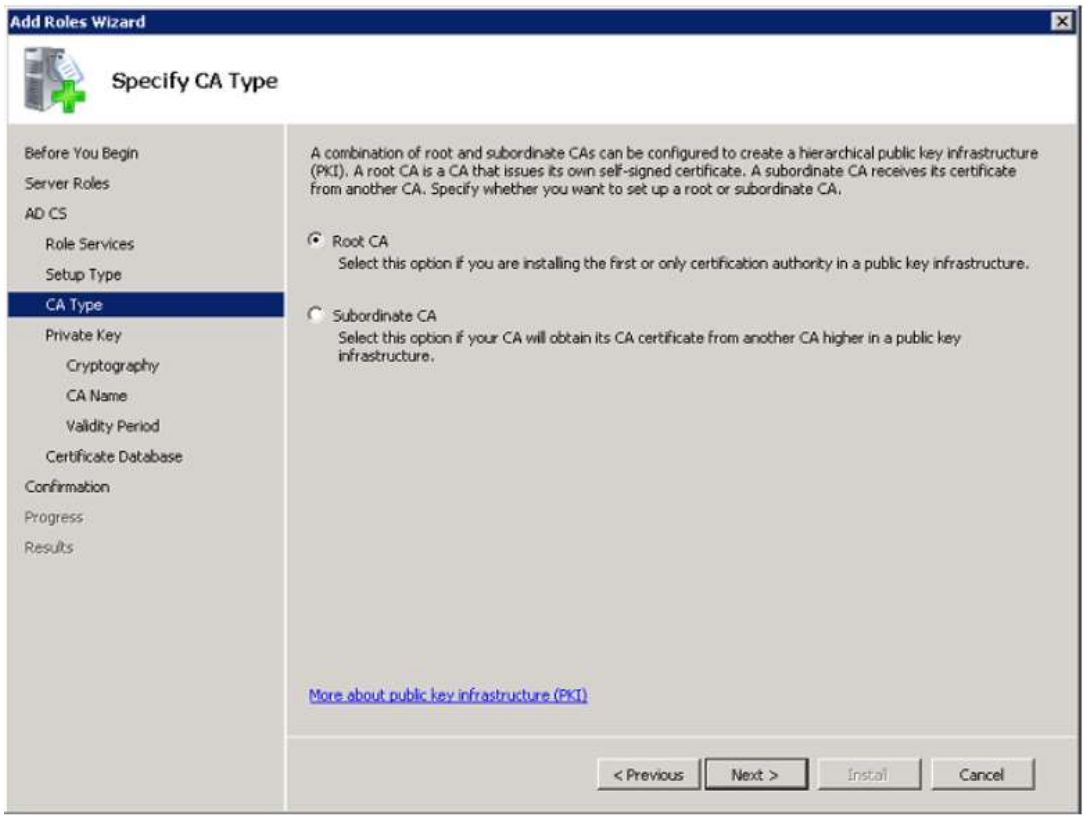

Figura 43 Única Autoridad de certificación

Fuente: Windows Server 2008

d) Conectar e ingresar a los usuarios al dominio y se agrega certificado en la cuenta del equipo local, estos pasos se deben realizar en cada uno de los equipos.

e) Instalar el Network Policy Server (NPS) que es usado en el servidor RADIUS para autenticar a los clientes Wireless con la autenticación PEAP, se agrega el rol Network Policy and Access Services (Ver figura 44), se agrega el Network Policy Server y el Routing and Remote Access Services y se instala.

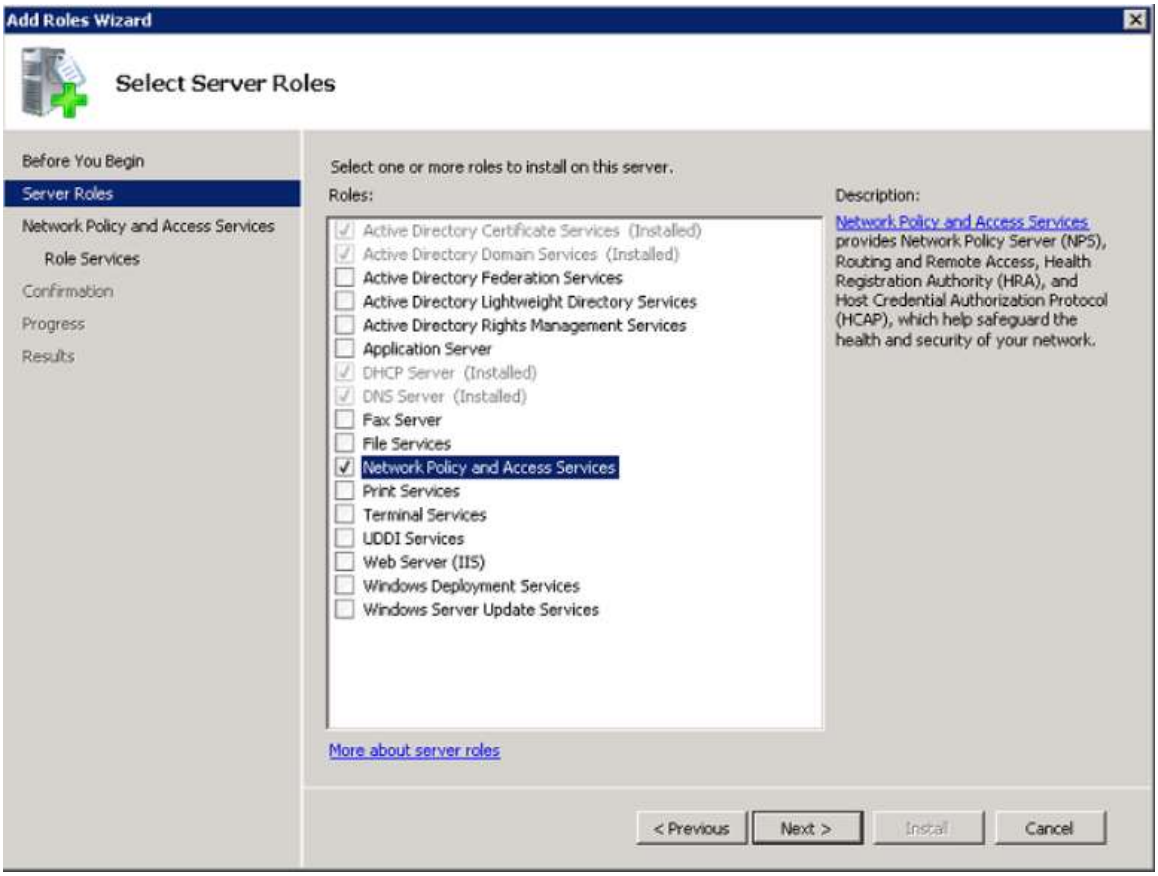

Figura 44 Interfaz agregando el rol NPS

Fuente: Windows Server 2008

f) Se agregan los certificados en la cuenta de la computadora local, en los certificados de la computadora local que se encuentra en Microsoft Management Console (MMC), dentro de la carpeta Personal se encuentra la carpeta certificado, en la cual se crea el certificado Domain Controller. (Ver figura 45 y 46)

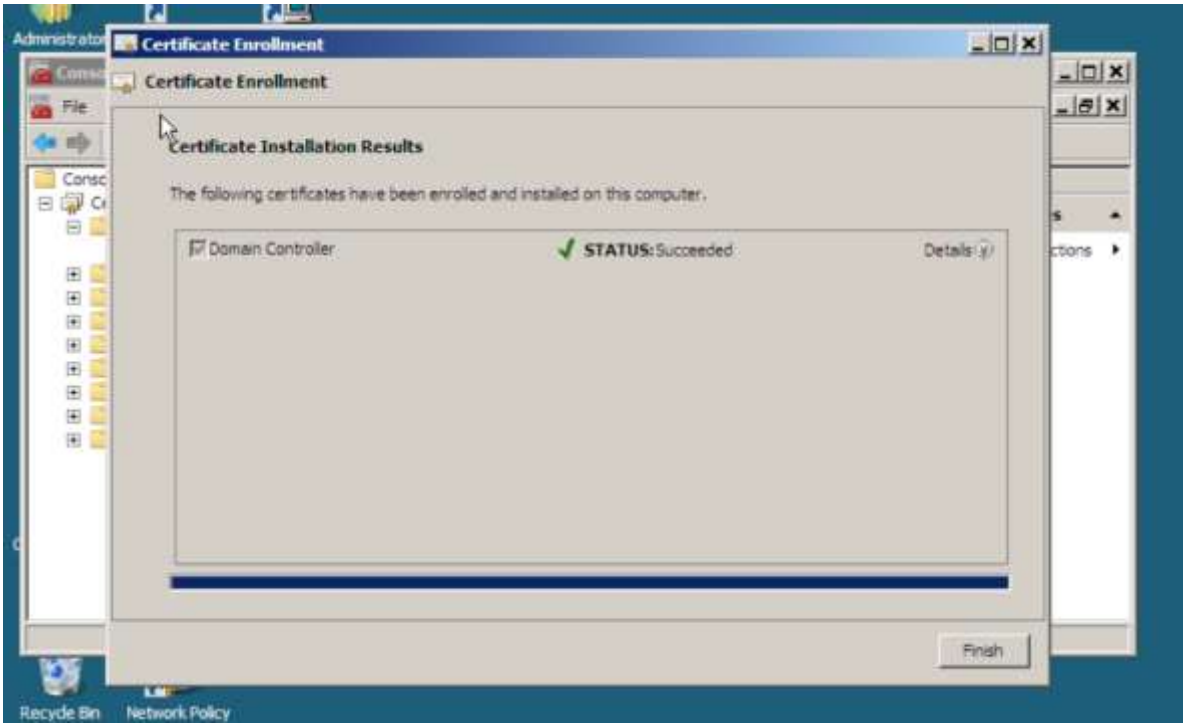

Figura 45 Interfaz de la instalación del Domain Controller

Fuente: Windows Server 2008

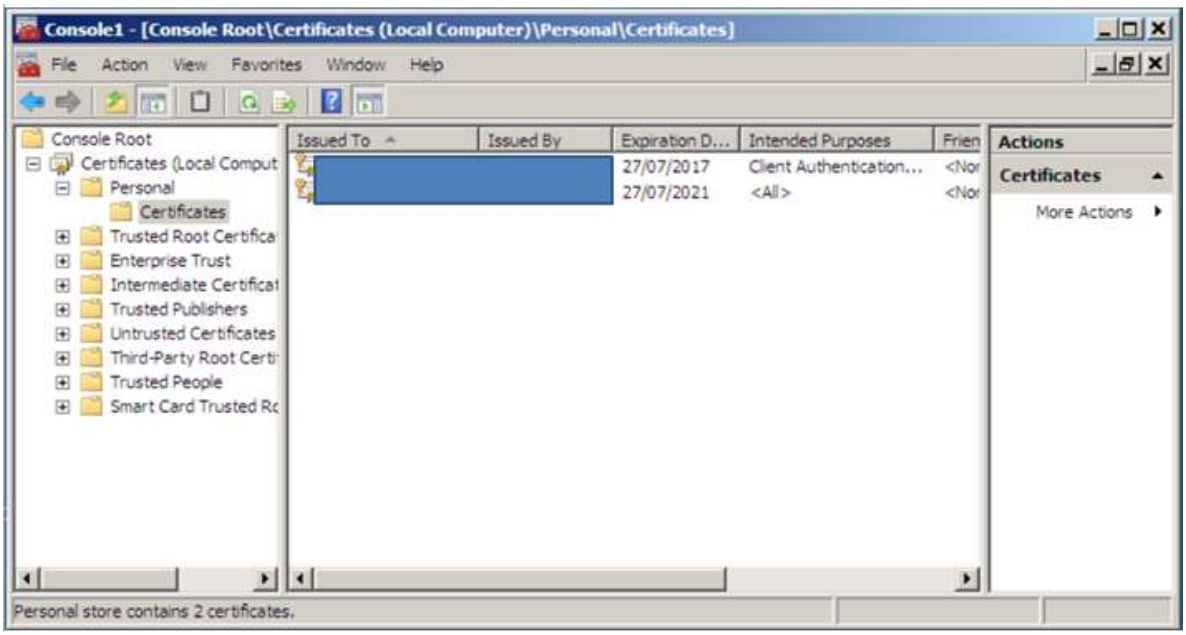

Figura 46 Interfaz del certificado agregado / Fuente: Windows Server 2008

Fuente: Windows Server 2008

g) Se registra el NPS en el Active Directory (Ver figura 47), se añade la Wireless LAN Controller como cliente en el NPS (Ver figura 48, 49 y 50), políticas de red Wireless para los usuarios (Ver figura 51), se agregan las políticas de red (Ver figura 52) y se configura el método de autenticación agregando el Microsoft Protected EAP (PEAP).

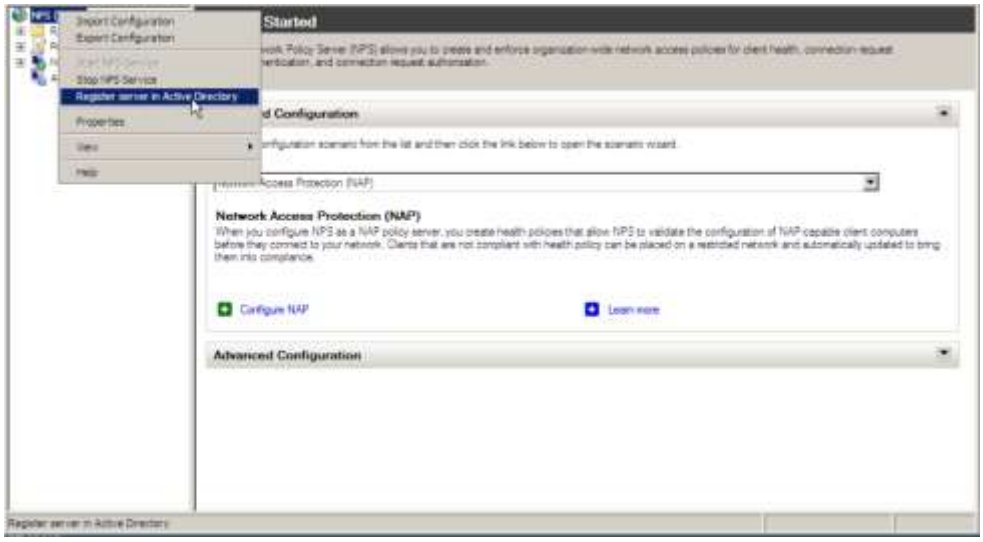

Figura 47 Registro del Active Directory en el NPS

Fuente: Windows Server 2008

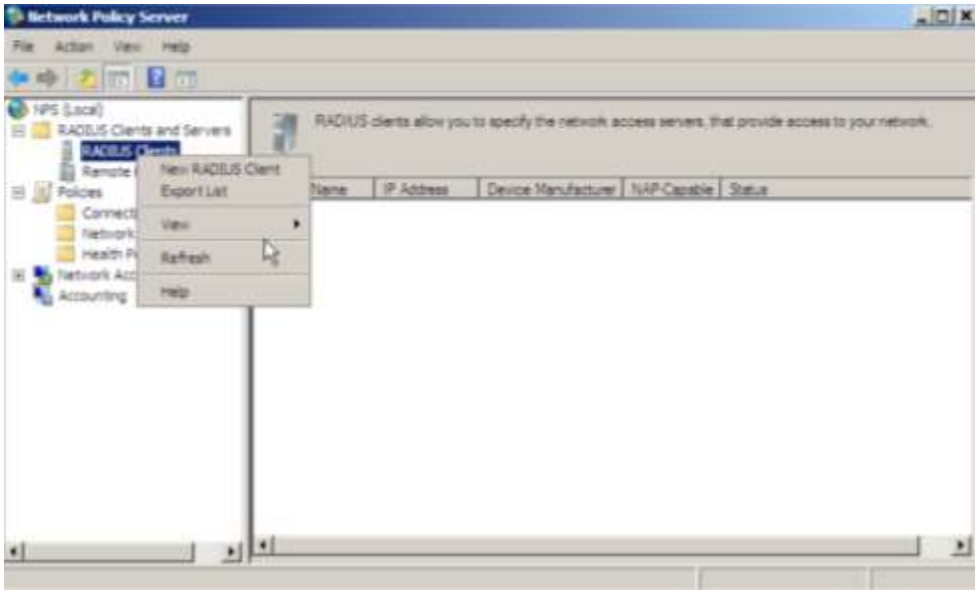

Figura 48 Interfaz para registrar la controladora al NPS / Fuente: Windows Server 2008

Fuente: Windows Server 2008

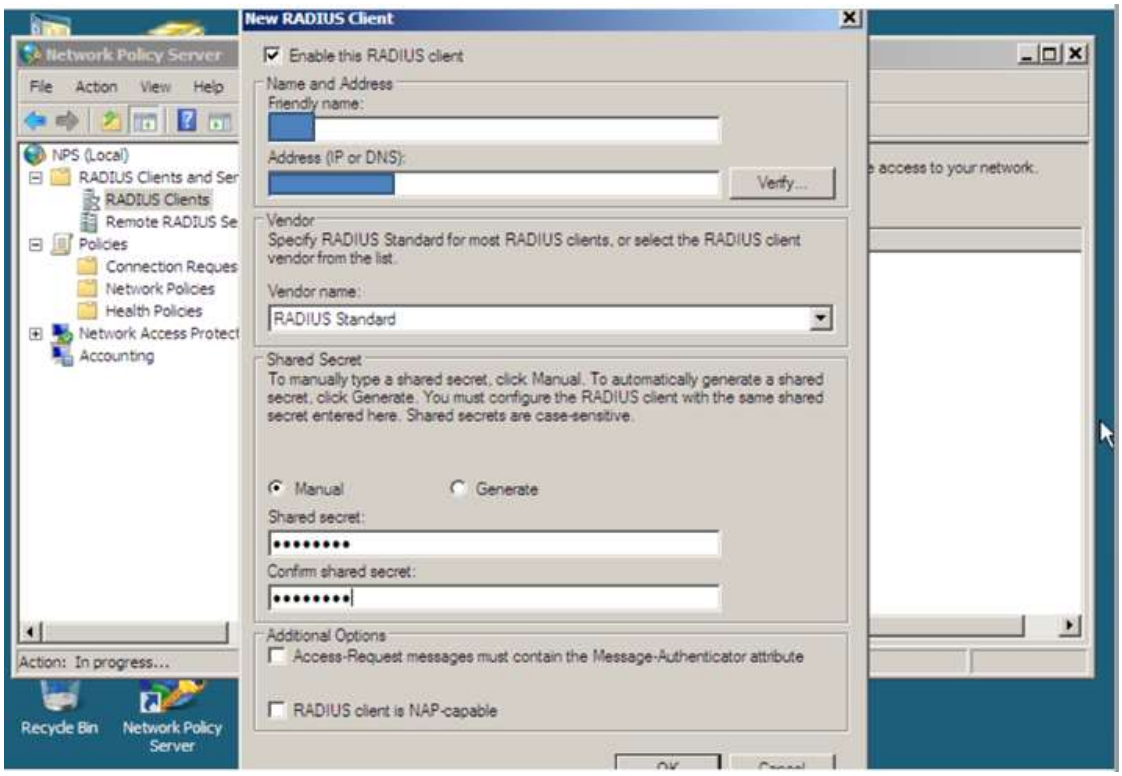

Figura 49 Registro de los clientes RADIUS

Fuente: Windows Server 2008

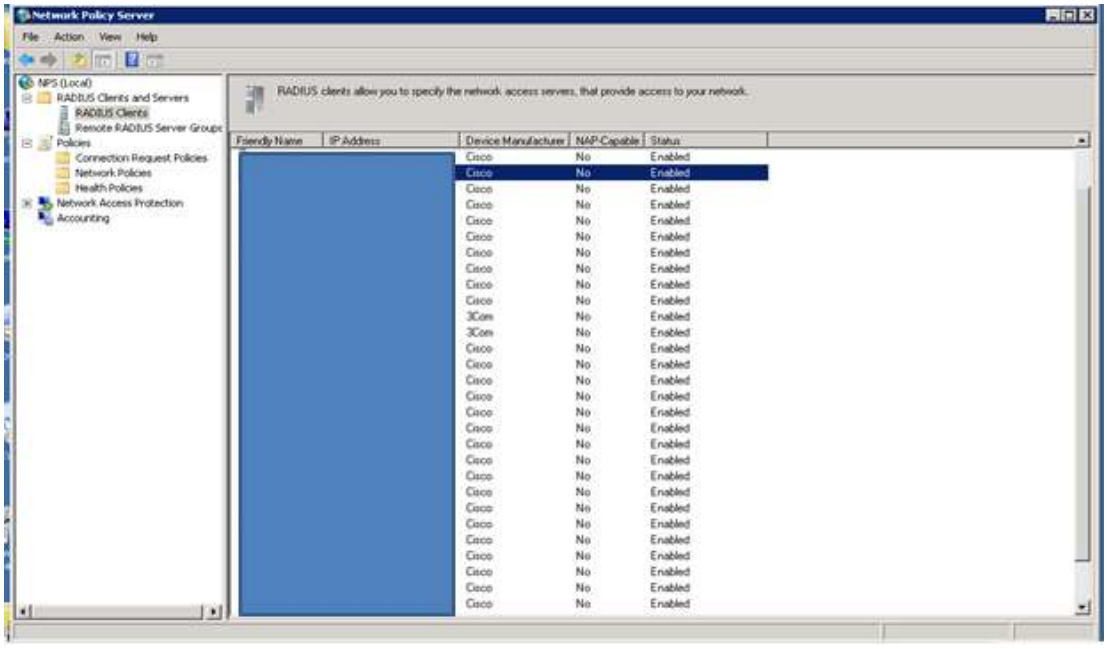

Figura 50 Clientes del RADIUS

Fuente: Windows Server 2008

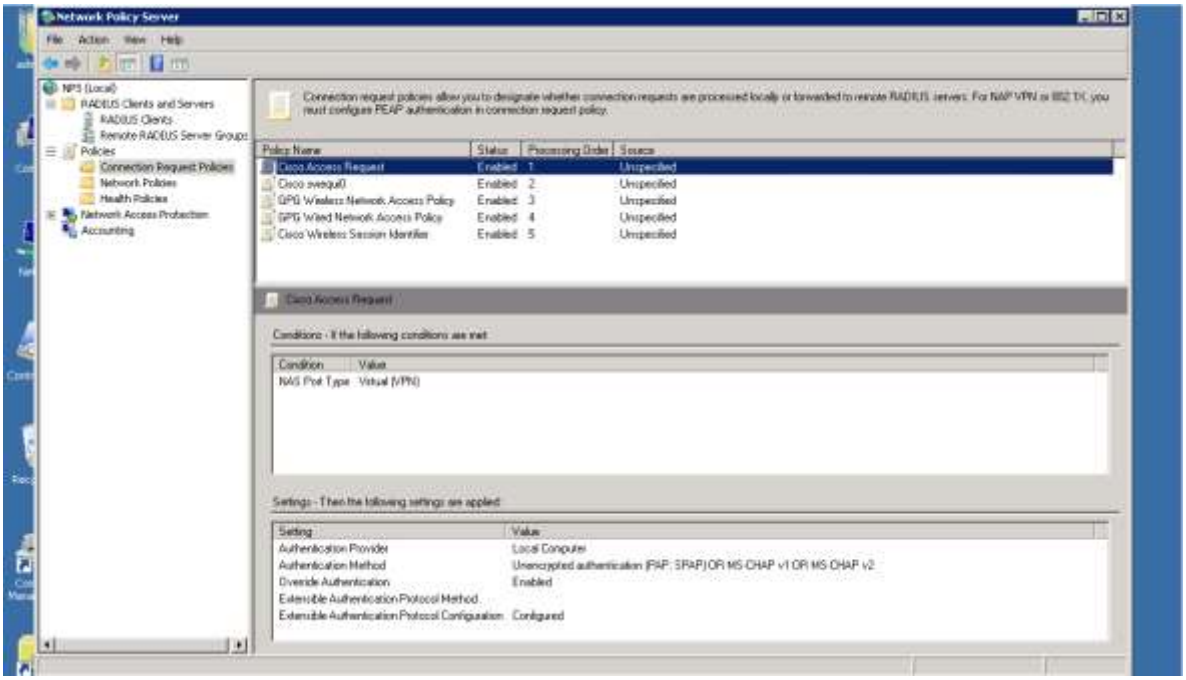

Figura 51 Políticas de conexión

Fuente: Windows Server 2008

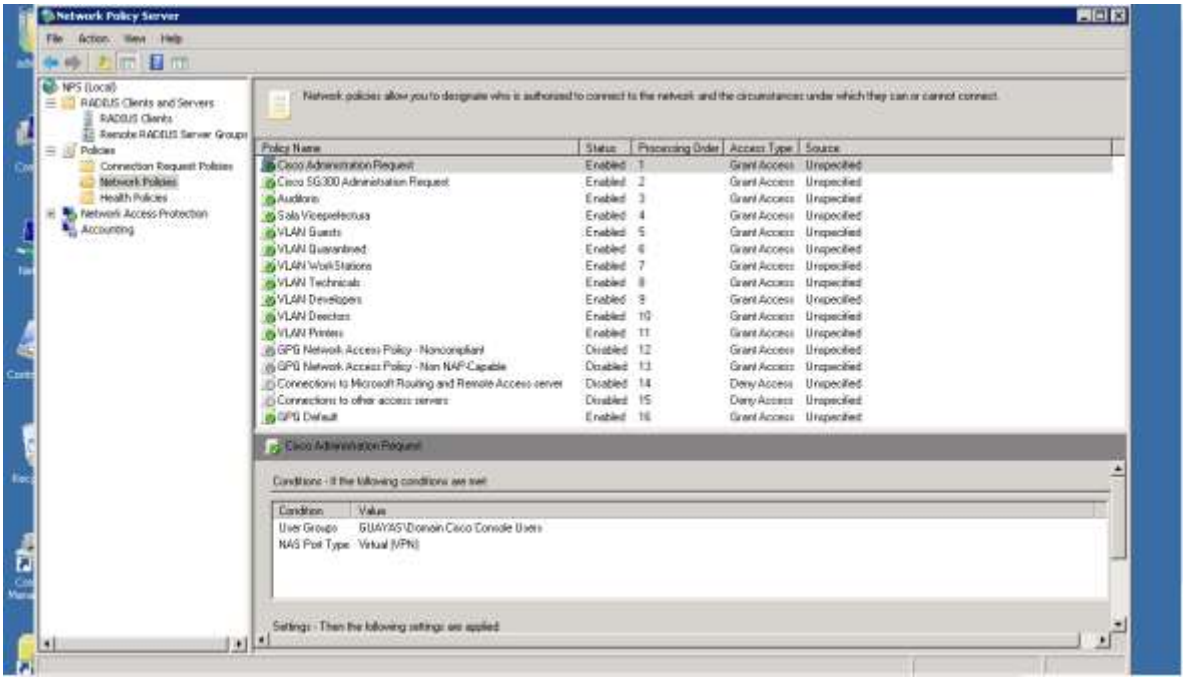

Figura 52 Interfaz de la política de red agregada

Fuente: Windows Server 2008

En la figura 53, se puede visualizar que en la aplicación de VMWARE vSphere Cliente se agregó una máquina virtual con el nombre que cumple con los parámetros que tiene el departamento de redes para identificar las funciones que cumple cada una de máquinas virtuales registrada en el aplicativo antes mencionado, por esta razón se ha trabajado en conjunto con el jefe de infraestructura tecnológica (Departamento de Redes), de modo que se culmina demostrando que dicha máquina virtual queda instalada y operativa en la institución.

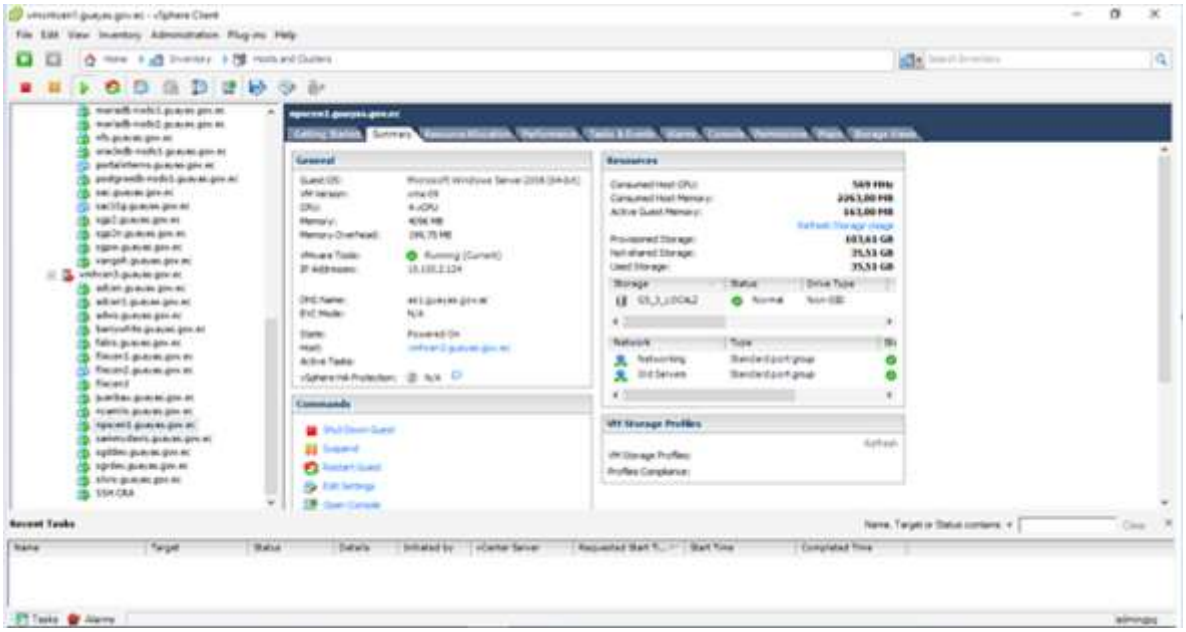

Figura 53 Registro de la Máquina Virtual Creada

Fuente: VMWARE vSphere

En la figura 54 se puede visualizar el detalle general de la máquina virtual donde se instala el Servidor RADIUS.

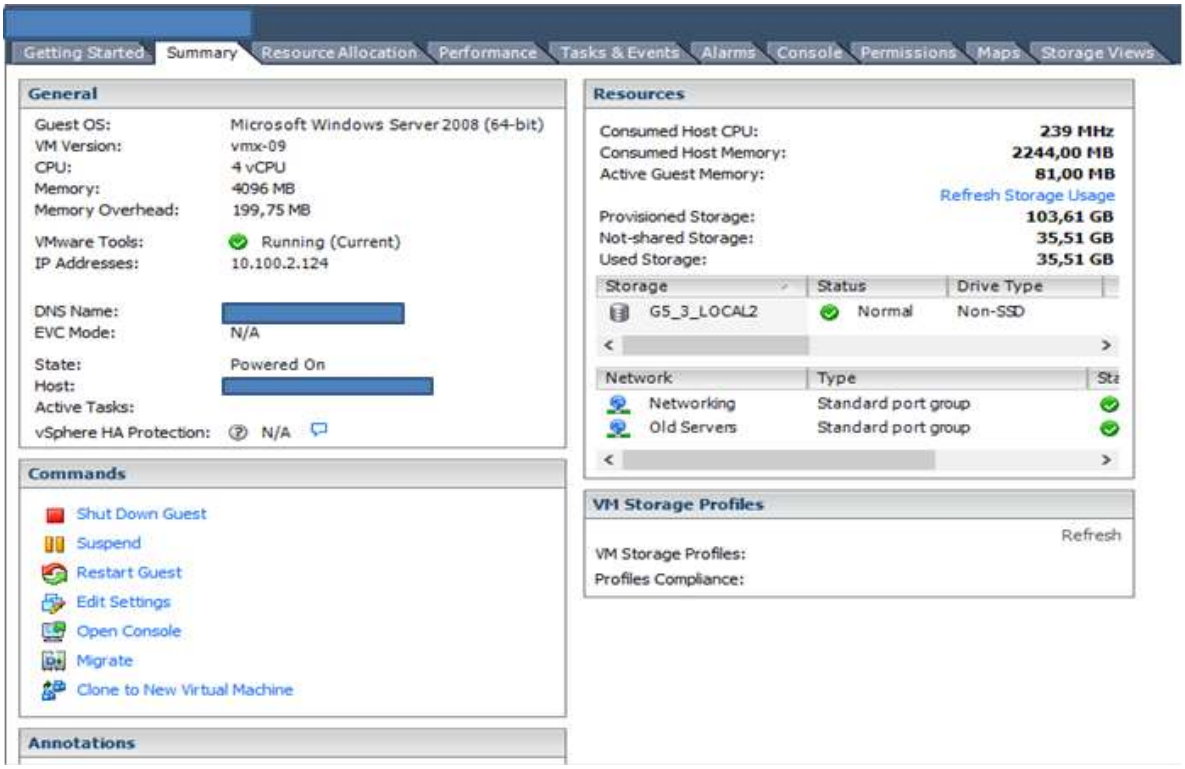

Figura 54 Detalle Windows Server 2008 de 64 bits

Fuente: VMWARE vSphere

9. Pruebas

Se realizó pruebas verificando que los usuarios de las oficinas remotas puedan conectarse al access point y se utilizó el software denominado kerio control, el mismo que facilitó el monitoreo de las oficinas remotas del Gobierno Provincial del Guayas.

Edificio Principal

Se realizó la prueba con el usuario yurema.tobar el mismo que se pudo conectar desde la computadora de escritorio al Access Point con el SSID 'gpg', en la figura 55 se puede observar la intensidad de la señal, el tipo de seguridad y tipo de radio del Access Point conectado y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al Internet. (Ver figura 56 y 57).

Figura 55 Conexión a la red inalámbrica

Fuente: Gobierno Provincial del Guayas – Windows 7

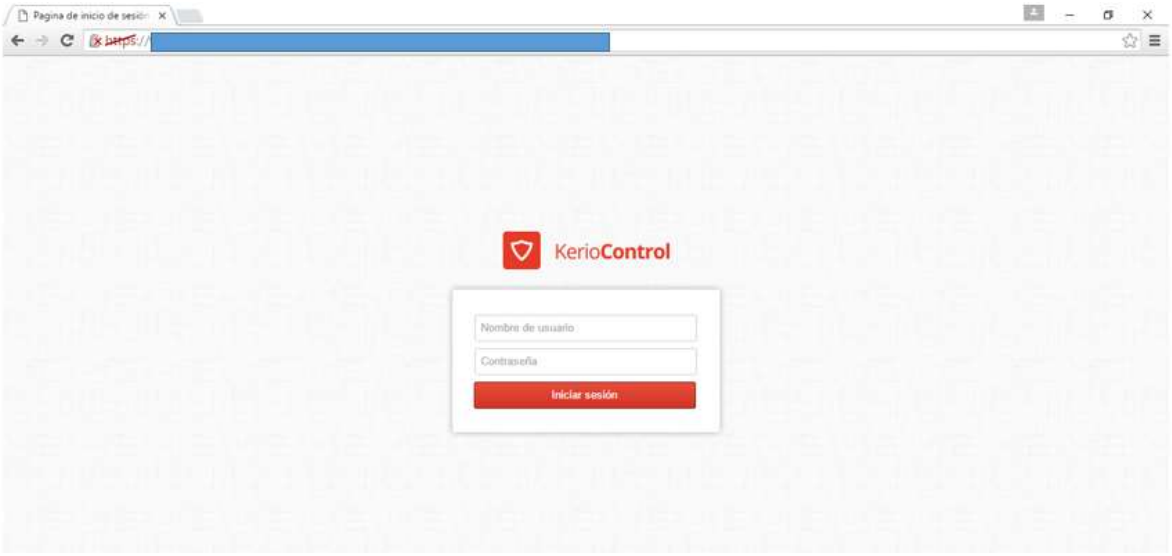

Figura 56 Página de autenticación del usuario del edificio principal

Fuente: Gobierno Provincial del Guayas – Software KerioControl

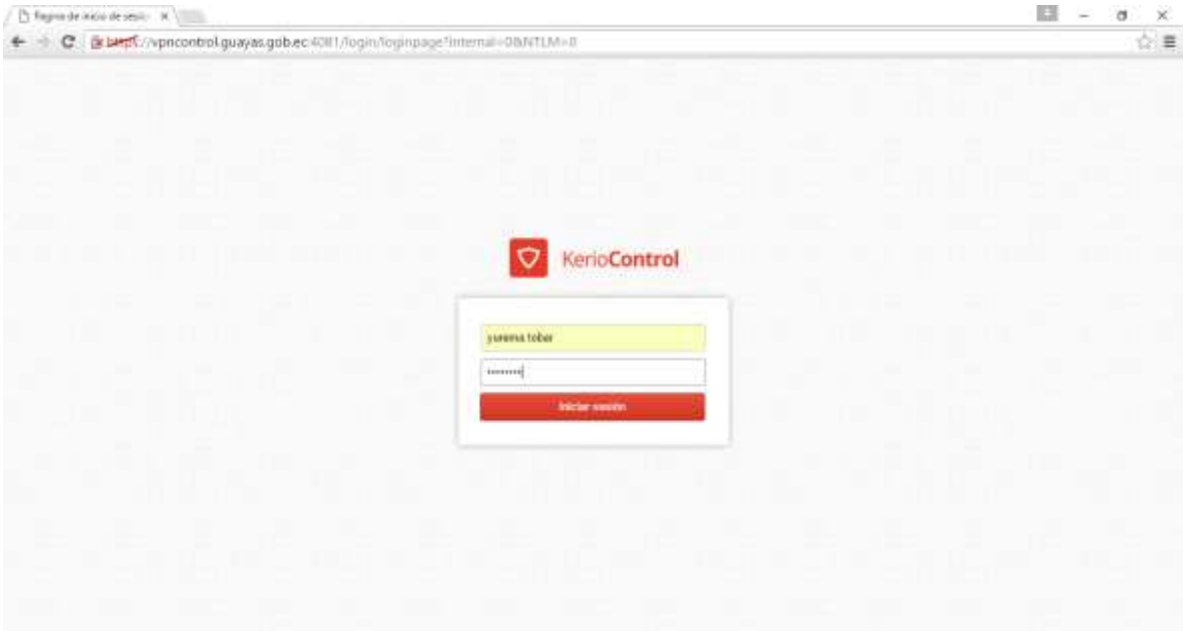

Figura 57 Ingresando datos del usuario del edificio principal

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En el Kerio Control Centro se puede visualizar cuantos equipos se han inicializado la sesión con la cuenta de yurema.tobar (Ver figura 58) y las estadísticas del usuario (Ver figura 59).

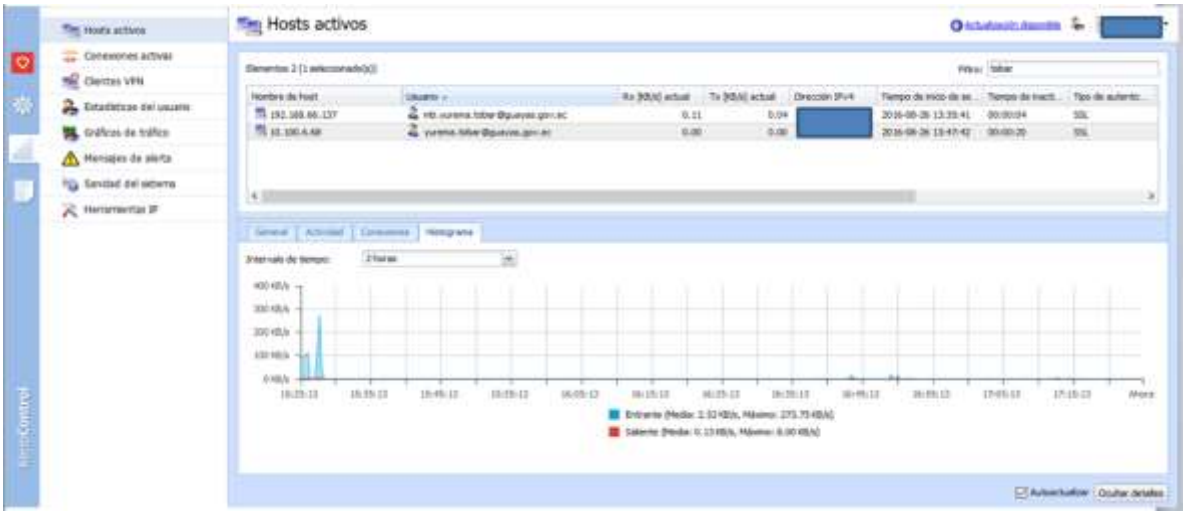

Figura 58 Host Activos del usuario del edificio principal

Fuente: Gobierno Provincial del Guayas – Software KerioControl

Figura 59 Estadísticas del usuario del edificio principal

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En la máquina virtual donde se encuentra el active directory se puede constatar que el usuario yurema.tobar si existe, a qué dirección pertenece el funcionario y cuál es la cuenta que tiene el usuario. (Ver figura 60 y 61).

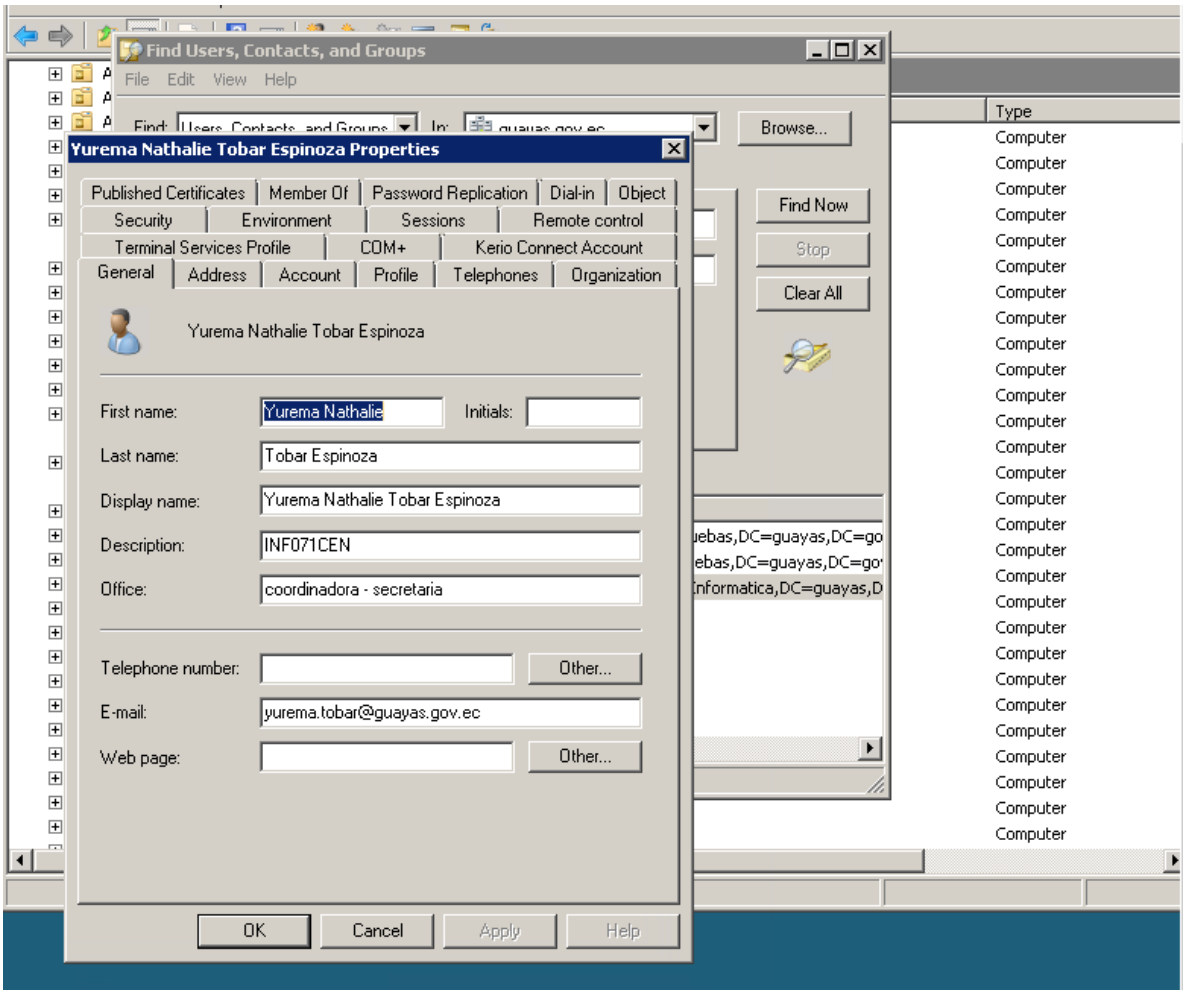

Figura 60 Detalle general del usuario del edificio principal creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

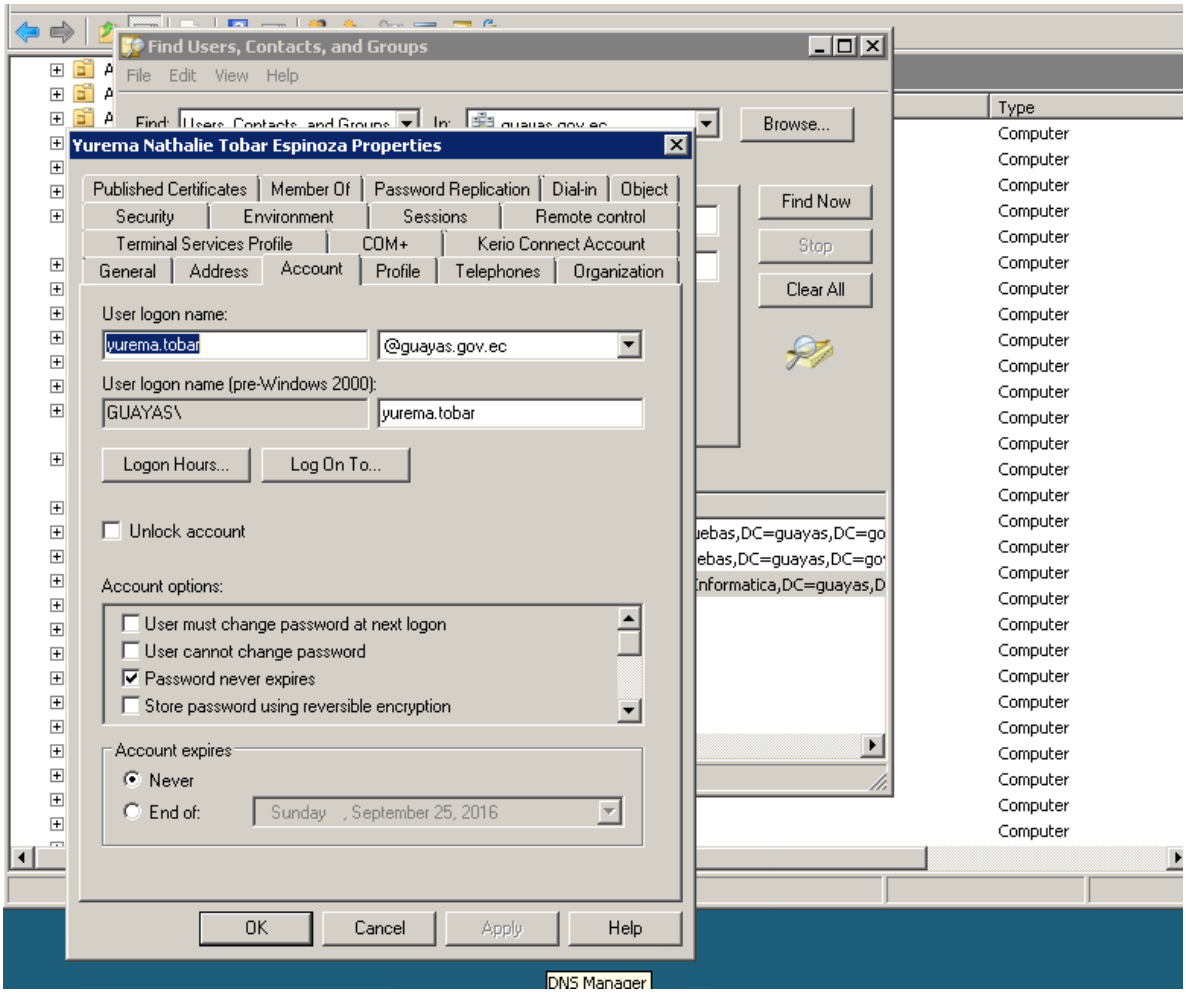

Figura 61 Cuenta del usuario del edificio principal creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

Medio Ambiente

Se realizó la prueba con el usuario rodney.caamano el mismo que se pudo conectar desde la computadora de escritorio al access point con el SSID ‘gpg’ y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al internet. (Ver figura 62 y 63).

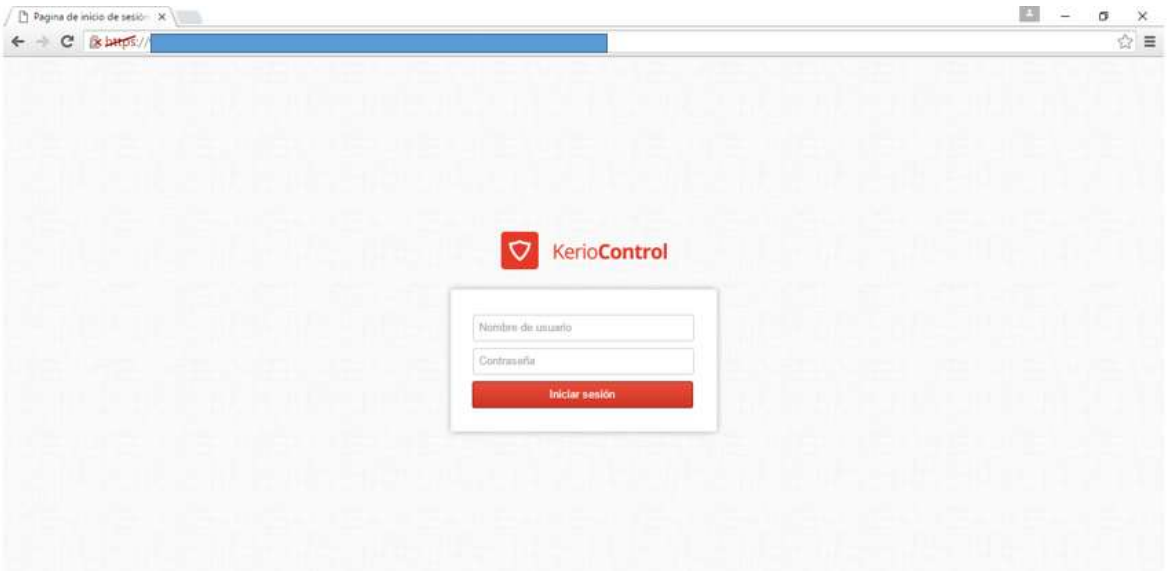

Figura 62 Página de autenticación

Fuente: Gobierno Provincial del Guayas – Software KerioControl

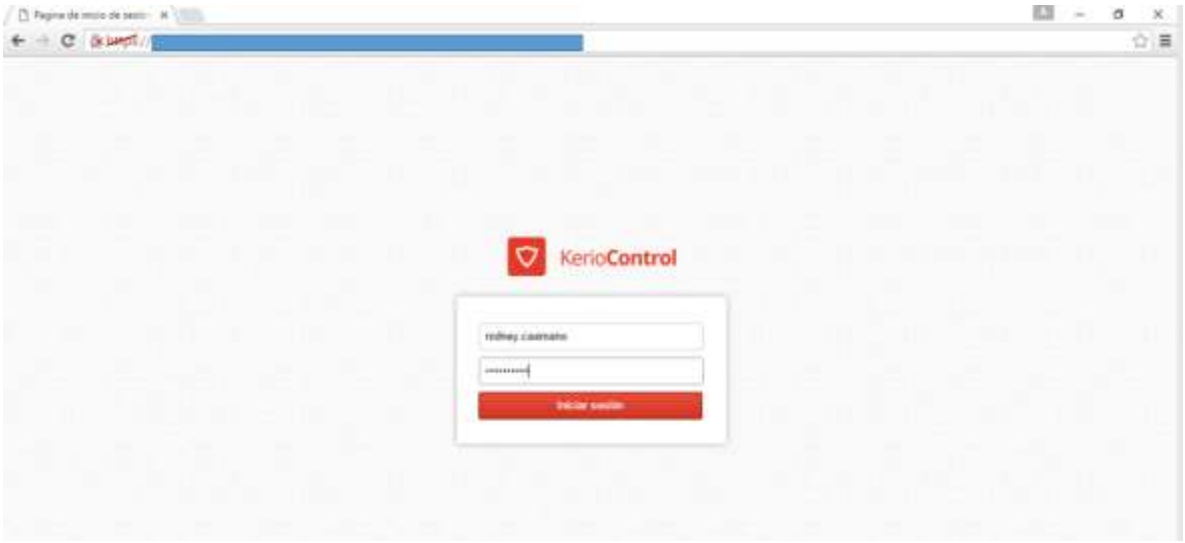

Figura 63 Ingresando datos del usuario de medio ambiente

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En el Kerio Control Centro se puede visualizar cuantos equipos han inicializado la sesión con la cuenta de rodney.caamano (Ver figura 64) y las estadísticas del usuario (Ver figura 65).

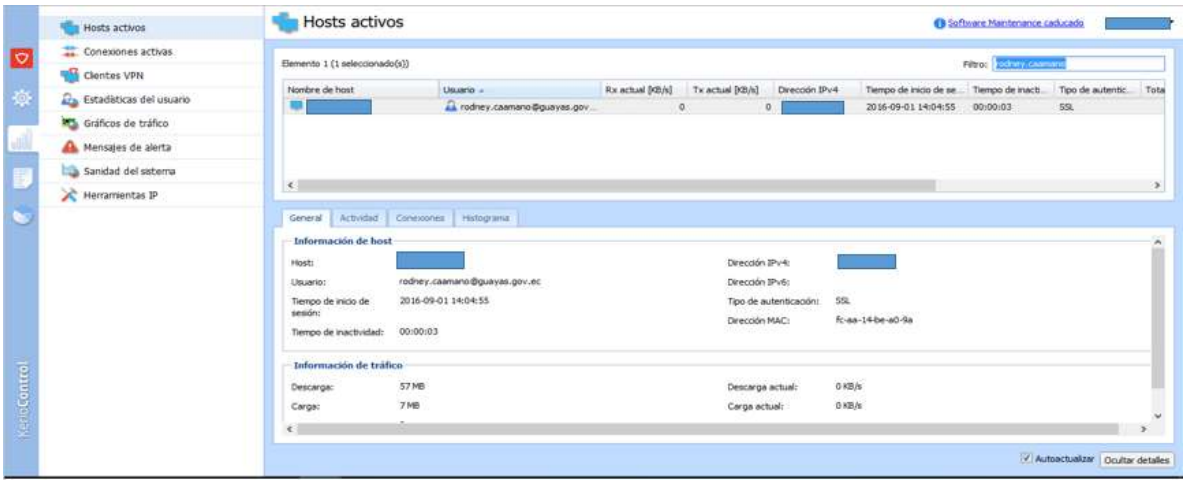

Figura 64 Host activos del usuario de medio ambiente

Fuente: Gobierno Provincial del Guayas – Software KerioControl

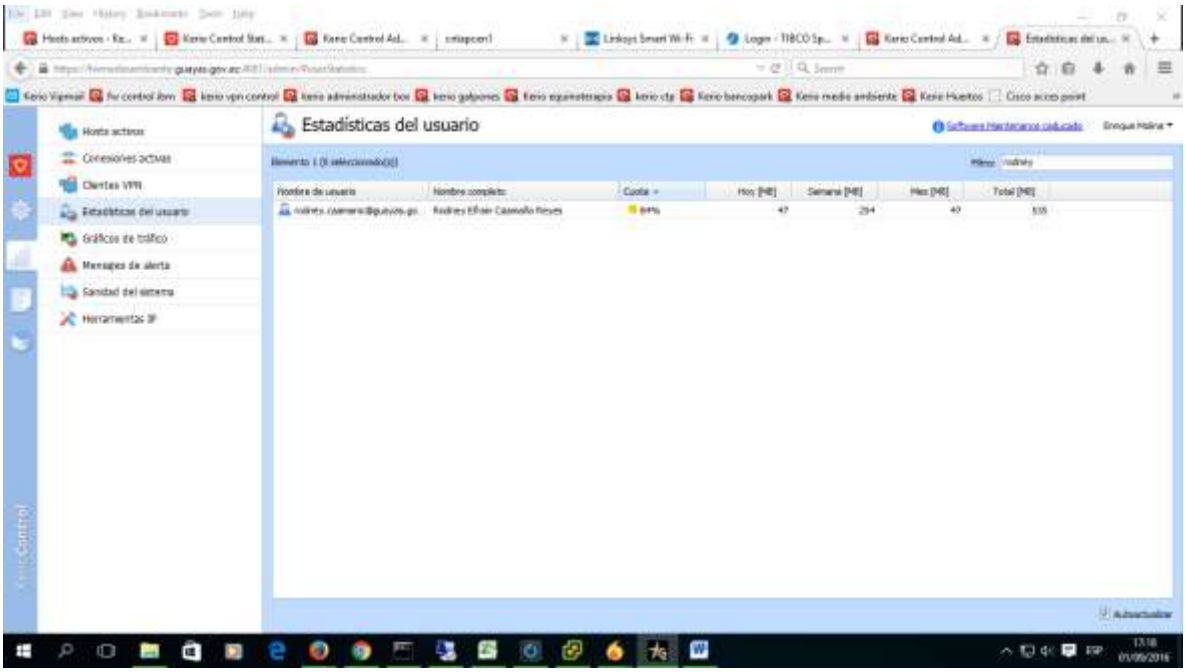

Figura 65 Estadísticas del usuario de medio ambiente

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En la máquina virtual donde se encuentra el active directory se puede constatar que el usuario rodney.caamano si existe, a qué dirección u oficina pertenece el funcionario. (Ver figura 66).

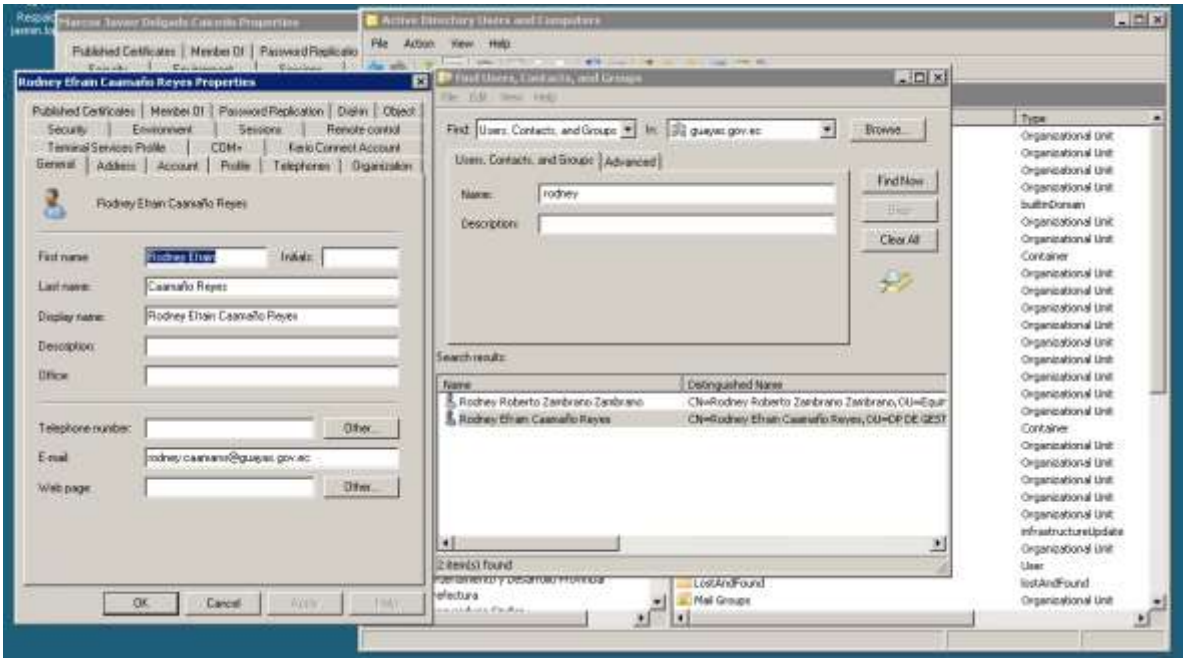

Figura 66 Cuenta del usuario de medio ambiente creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

Galpones

Se realizó la prueba con el usuario giovanni.podesta el mismo que se pudo conectar desde la computadora de escritorio al access point con el SSID ‘gpg’ y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al internet. (Ver figura 67 y 68).

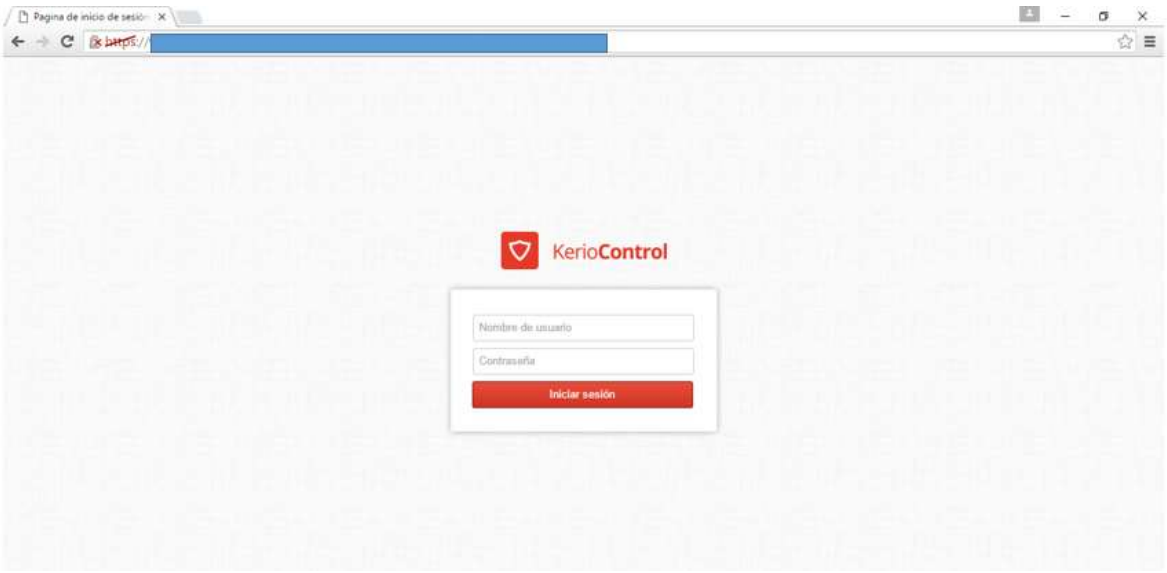

Figura 67 Página de autenticación

Fuente: Gobierno Provincial del Guayas – Software KerioControl

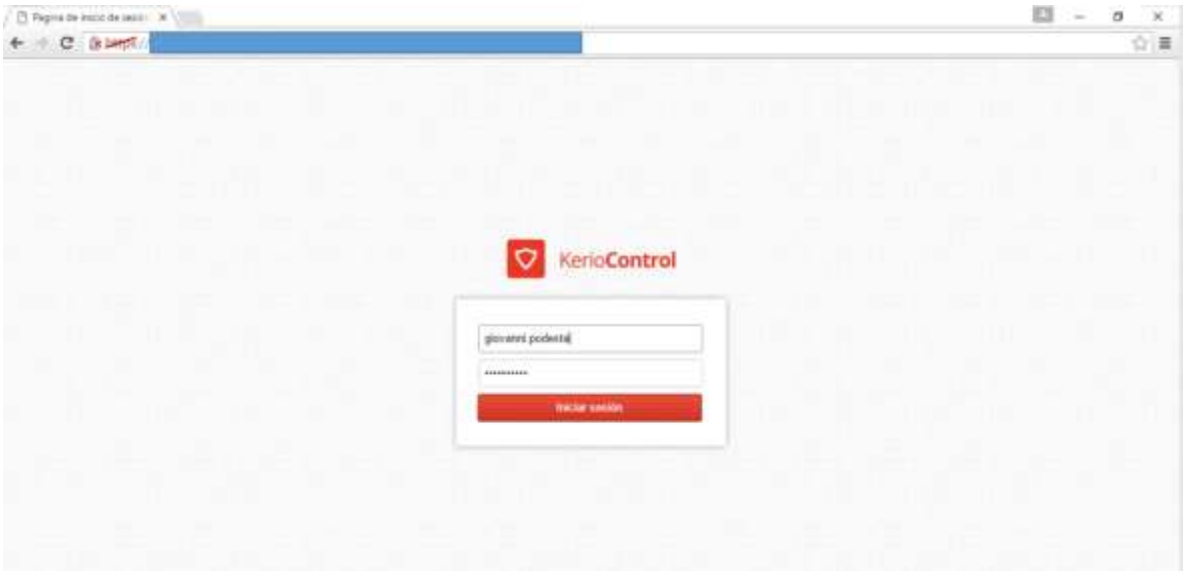

Figura 68 Ingresando datos del usuario de galpones

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En el Kerio Control galpones se puede visualizar cuantos equipos se han inicializado la sesión con la cuenta de giovanni.podesta (Ver figura 69) y las estadísticas del usuario (Ver figura 70).

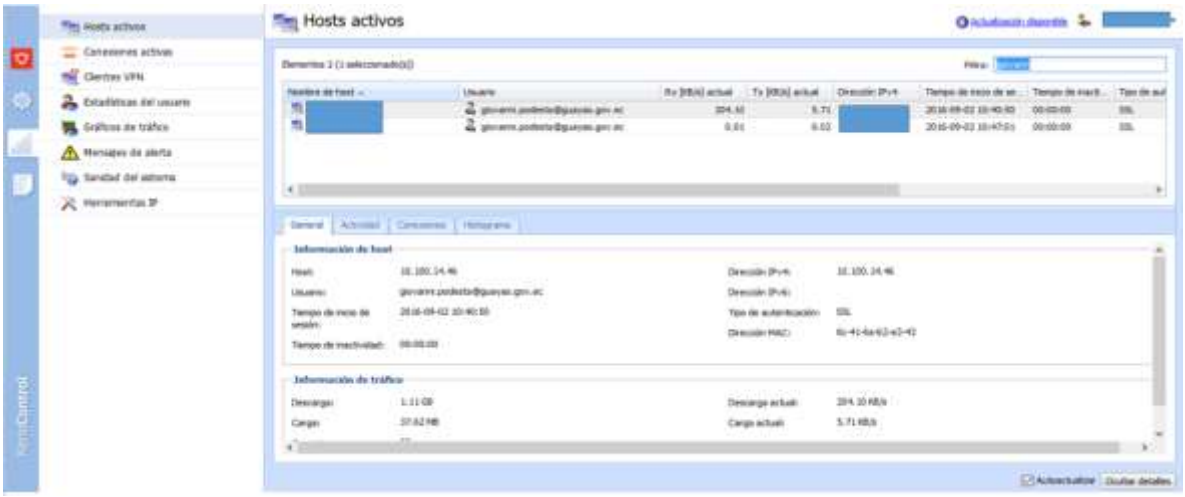

Figura 69 Host activo con el usuario de galpones

Fuente: Gobierno Provincial del Guayas – Software KerioControl

Figura 70 Estadísticas del usuario de galpones

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En la máquina virtual donde se encuentra el active directory se puede constatar que el usuario giovanni.podesta si existe, a qué dirección u oficina pertenece el funcionario y cuál es la cuenta que tiene el usuario. (Ver figura 71 y 72).

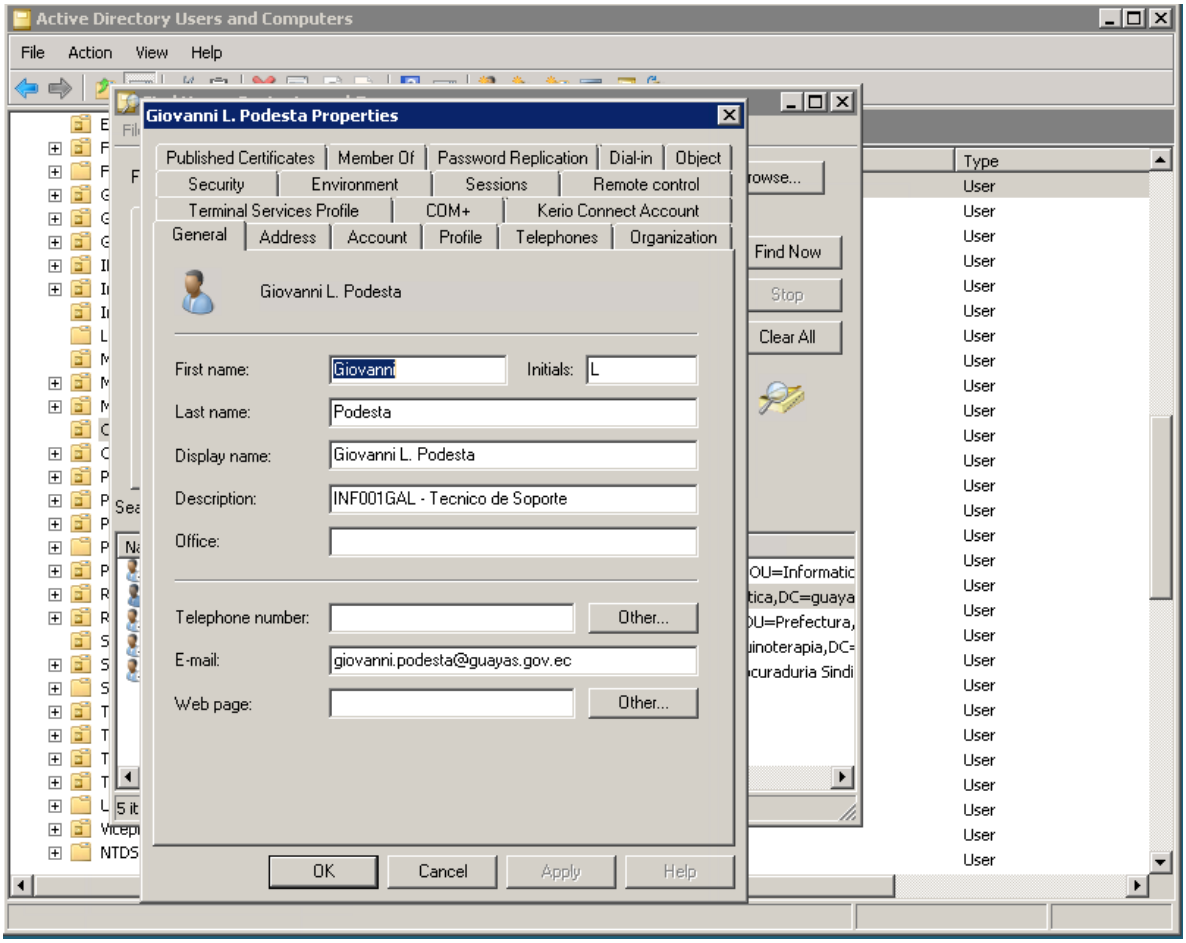

Figura 71 Detalle General del usuario de Galpones creado en el Active Directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

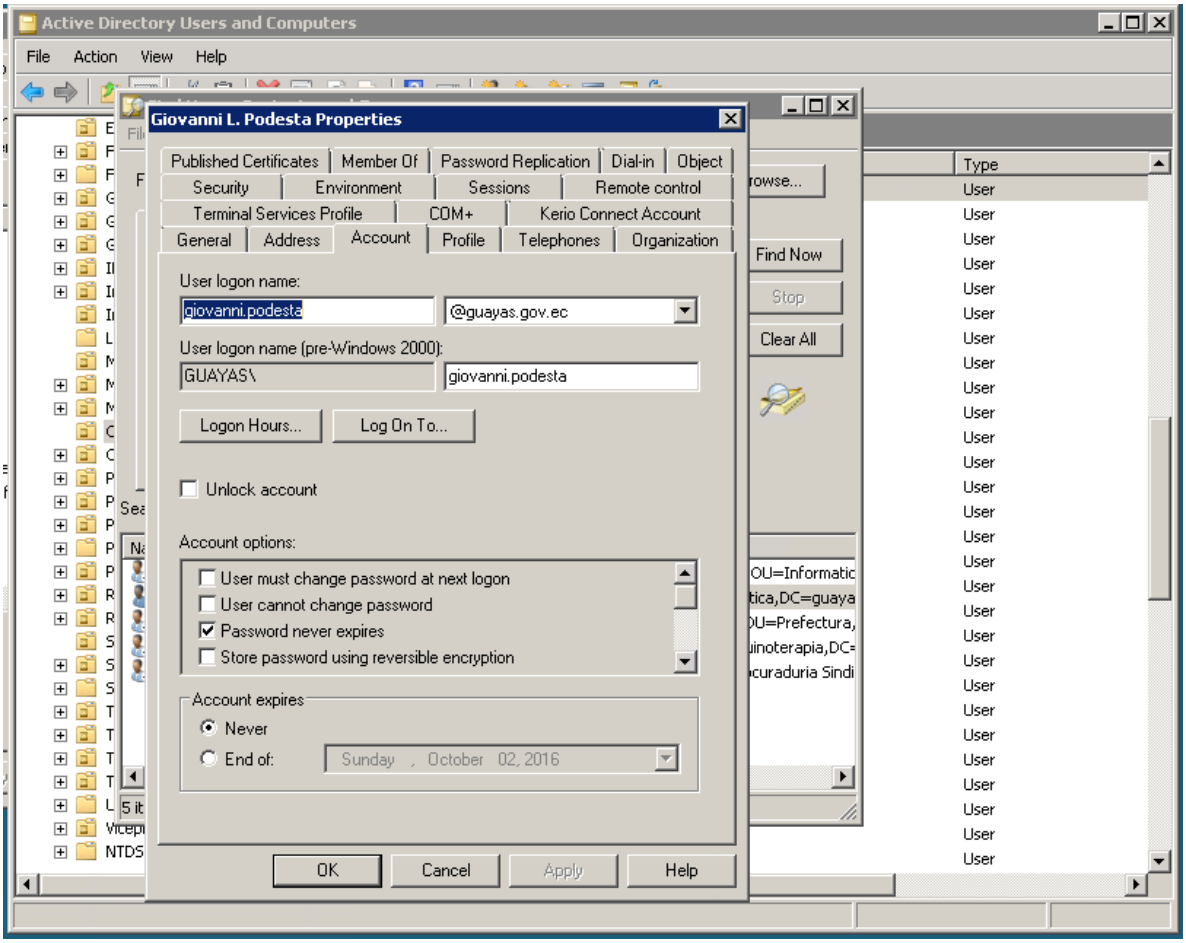

Figura 72 Cuenta del usuario de Galpones creado en el Active Directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

CTP

Se realizó la prueba con el usuario leonardo.chang el mismo que se pudo conectar desde la computadora de escritorio al access point con el SSID ‘gpg’ y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al internet. (Ver figura 73 y 74).

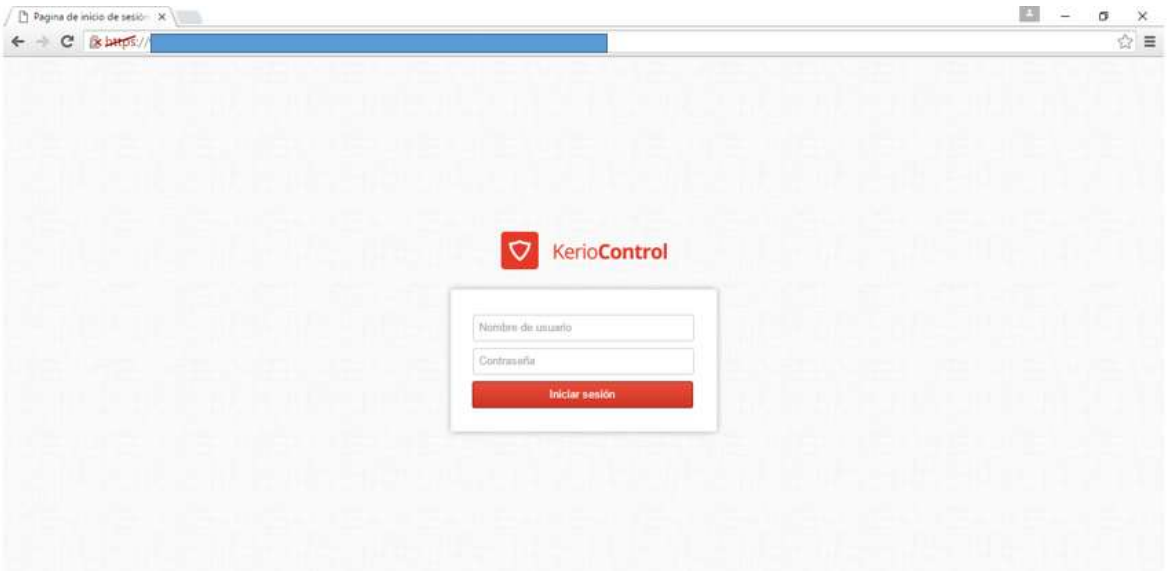

Figura 73 Página de autenticación

Fuente: Gobierno Provincial del Guayas – Software KerioControl

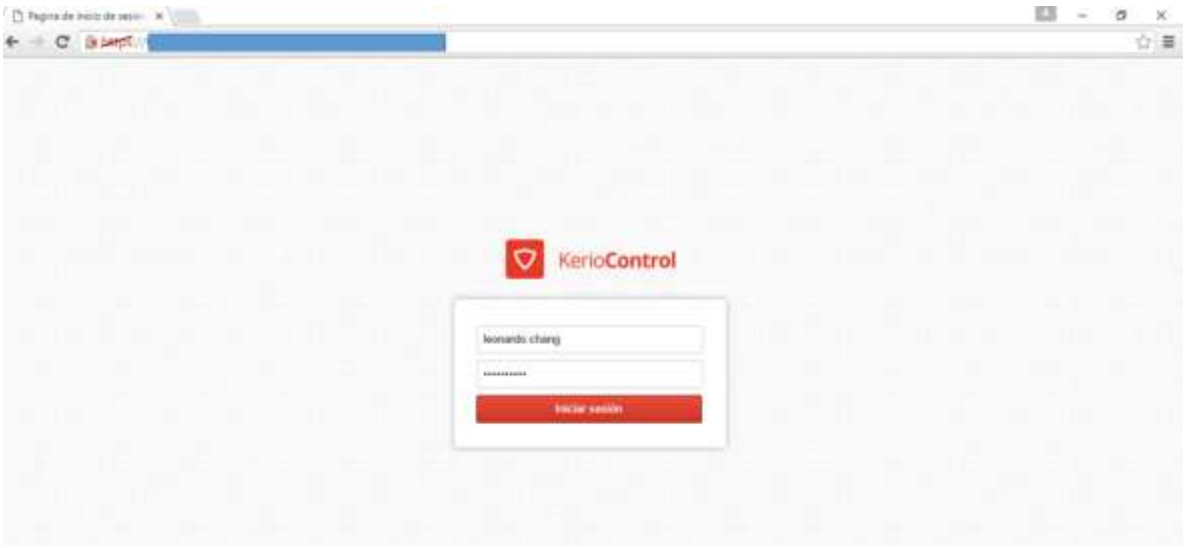

Figura 74 Ingresar datos del usuario de CTP

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En el Kerio Control CTP se puede visualizar cuantos equipos han inicializado la sesión con la cuenta de leonardo.chang (Ver figura 75) y las estadísticas del usuario (Ver figura 76).

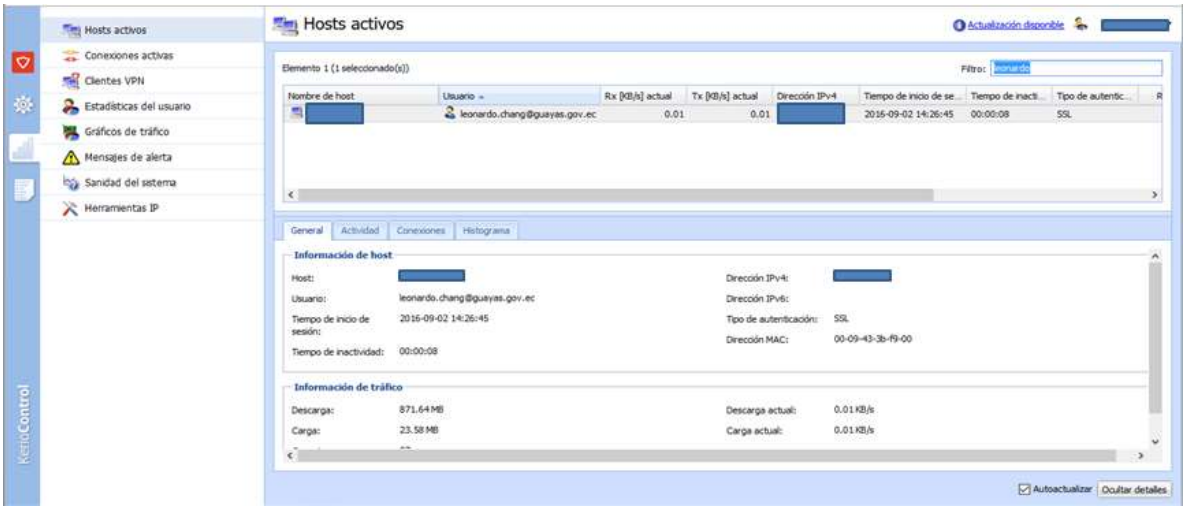

Figura 75 Host activos del usuario CTP

Fuente: Gobierno Provincial del Guayas – Software KerioControl

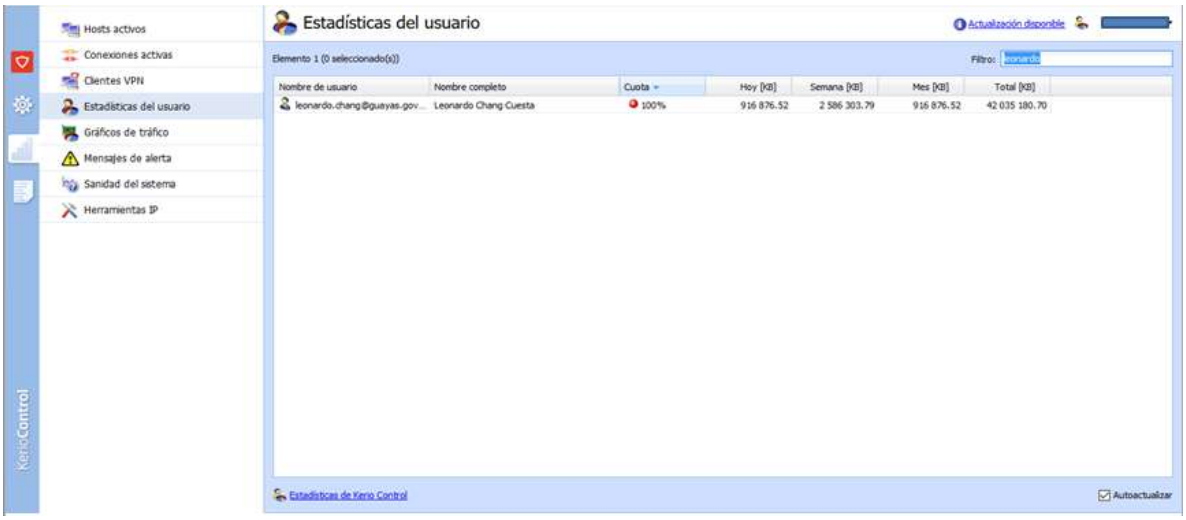

Figura 76 Estadísticas del usuario de CTP

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En la máquina virtual donde se encuentra el active directory se puede constatar que el usuario de leonardo.chang si existe, a que dirección u oficina pertenece el funcionario y cuál es la cuenta que tiene el usuario. (Ver figura 77 y 78).

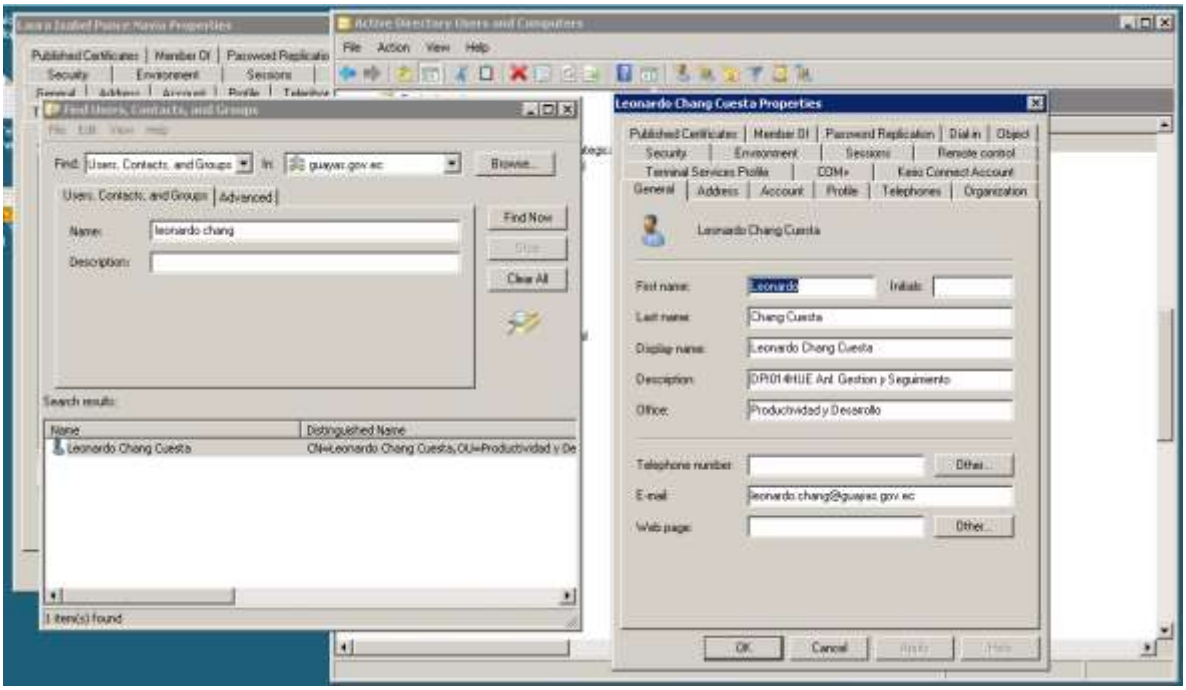

Figura 77 Detalle general del usuario de CTP creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

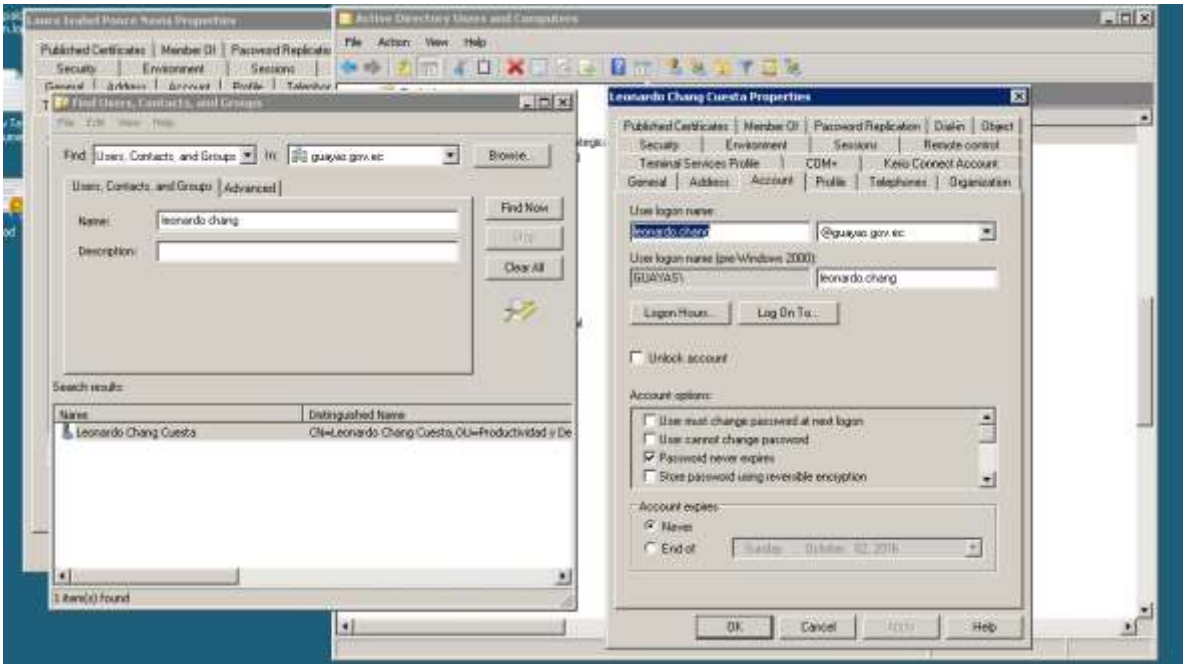

Figura 78 Cuenta del usuario del CTP creado en el Active Directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

BancoPark

Se realizó la prueba con el usuario janeth.maldonado el mismo que se pudo conectar desde la computadora de escritorio al access point con el SSID ‘gpg’ y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al internet. (Ver figura 79 y 80).

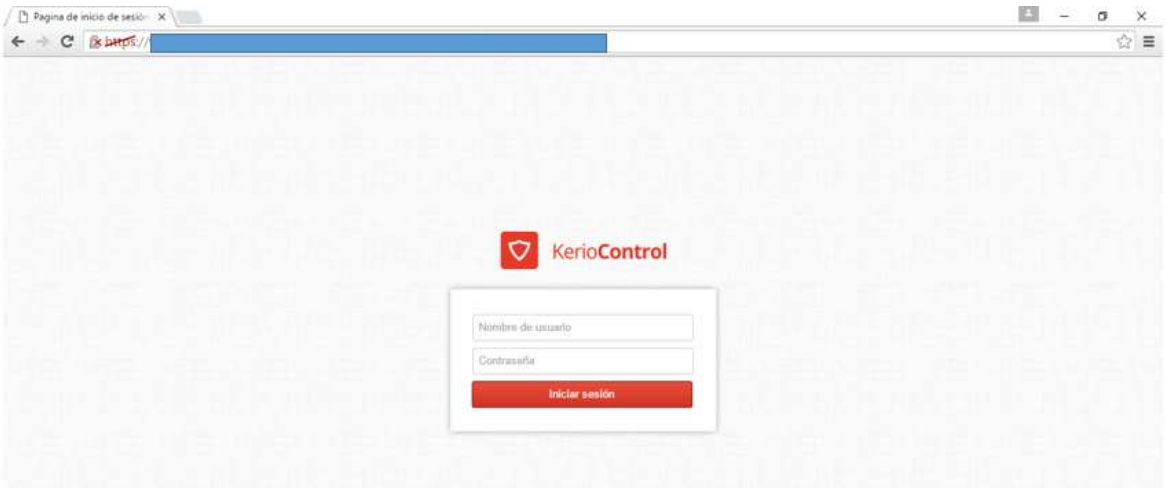

Figura 79 Página de autenticación

Fuente: Gobierno Provincial del Guayas – Software KerioControl

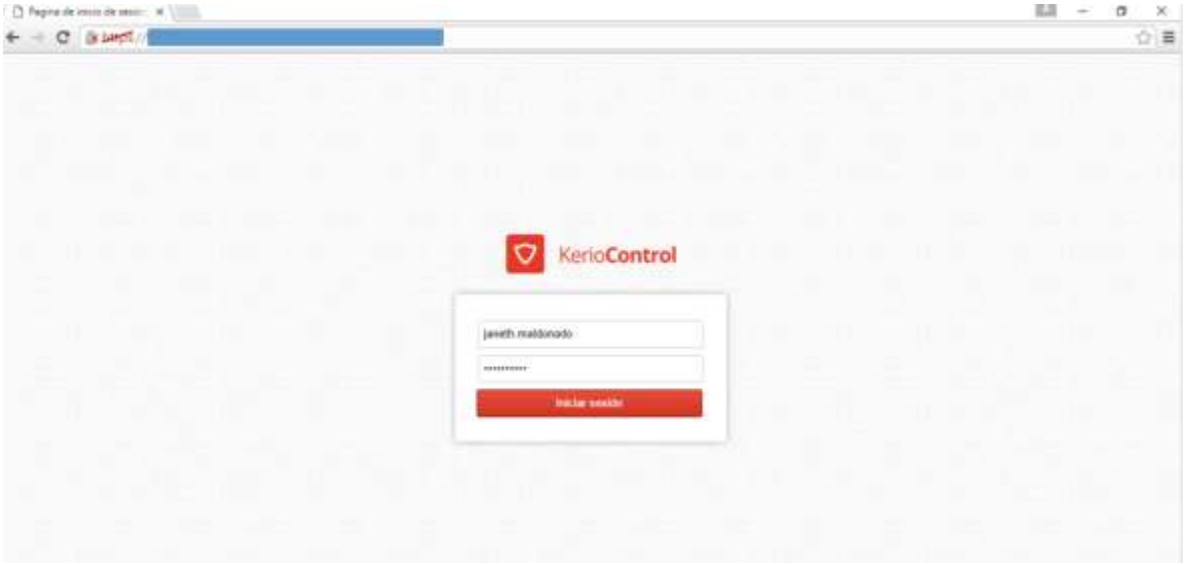

Figura 80 Ingresar datos del usuario de bancopark

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En el Kerio Control bancopark se puede visualizar cuantos equipos han inicializado la sesión con la cuenta de janeth.maldonado (Ver figura 81) y las estadísticas del usuario (Ver figura 82).

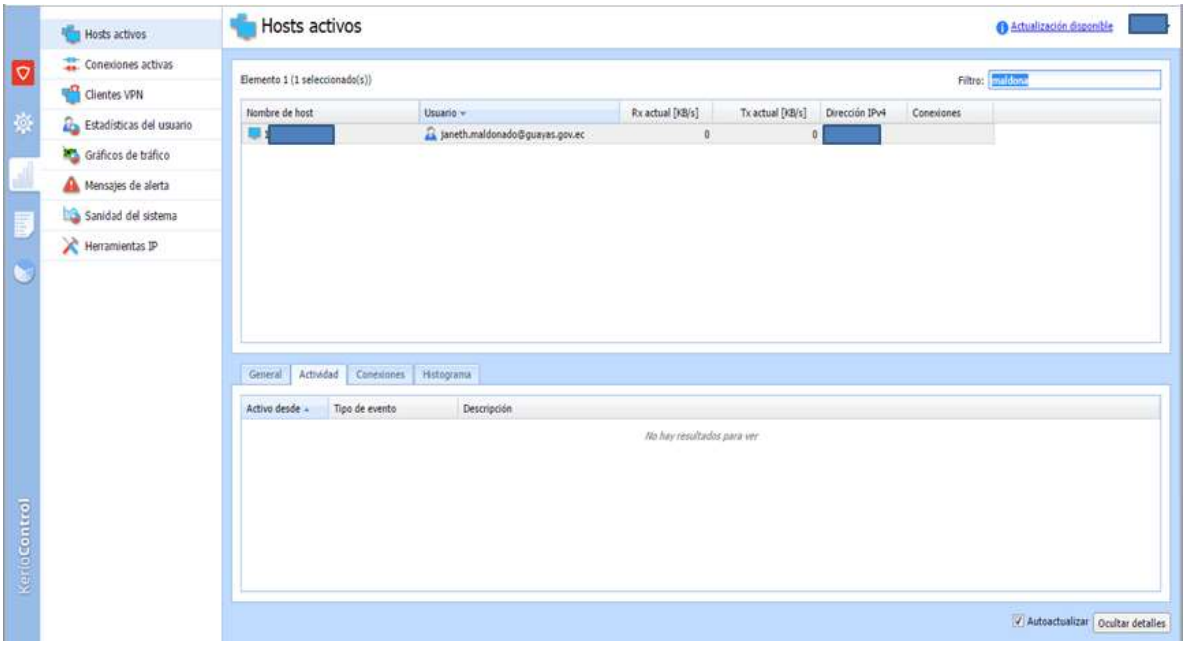

Figura 81 Host activo del usuario de bancopark

Fuente: Gobierno Provincial del Guayas – Software KerioControl

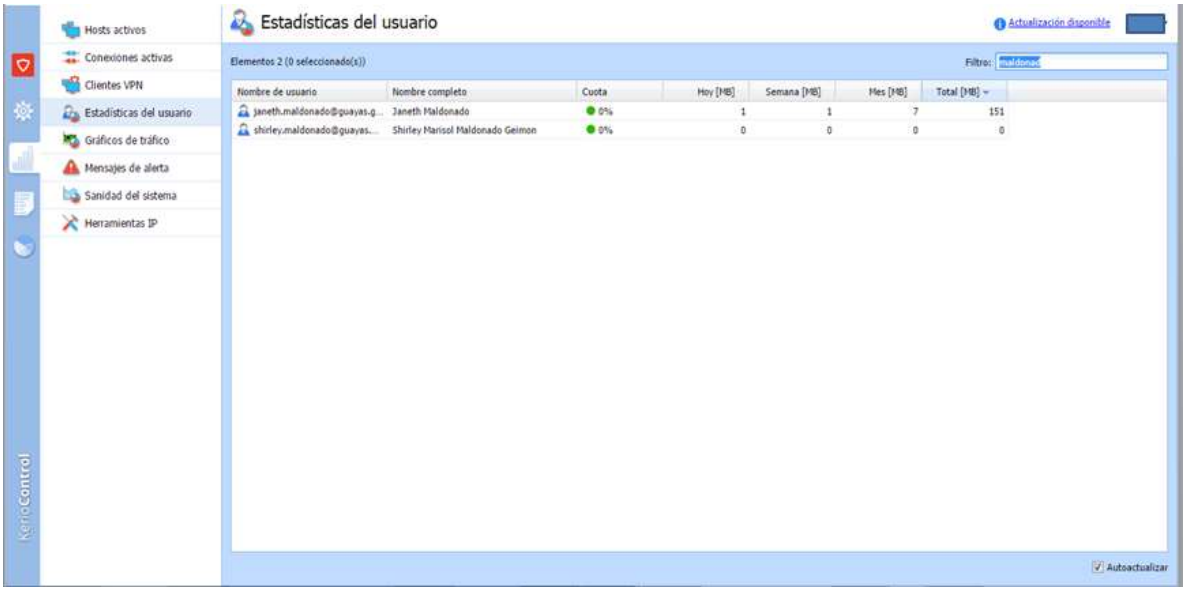

Figura 82 Estadísticas del usuario de bancopark

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En la máquina virtual donde se encuentra el active directory se puede constatar que el usuario de janeth.maldonado si existe, a que dirección u oficina pertenece el funcionario y cuál es la cuenta que tiene el usuario. (Ver figura 83 y 84).

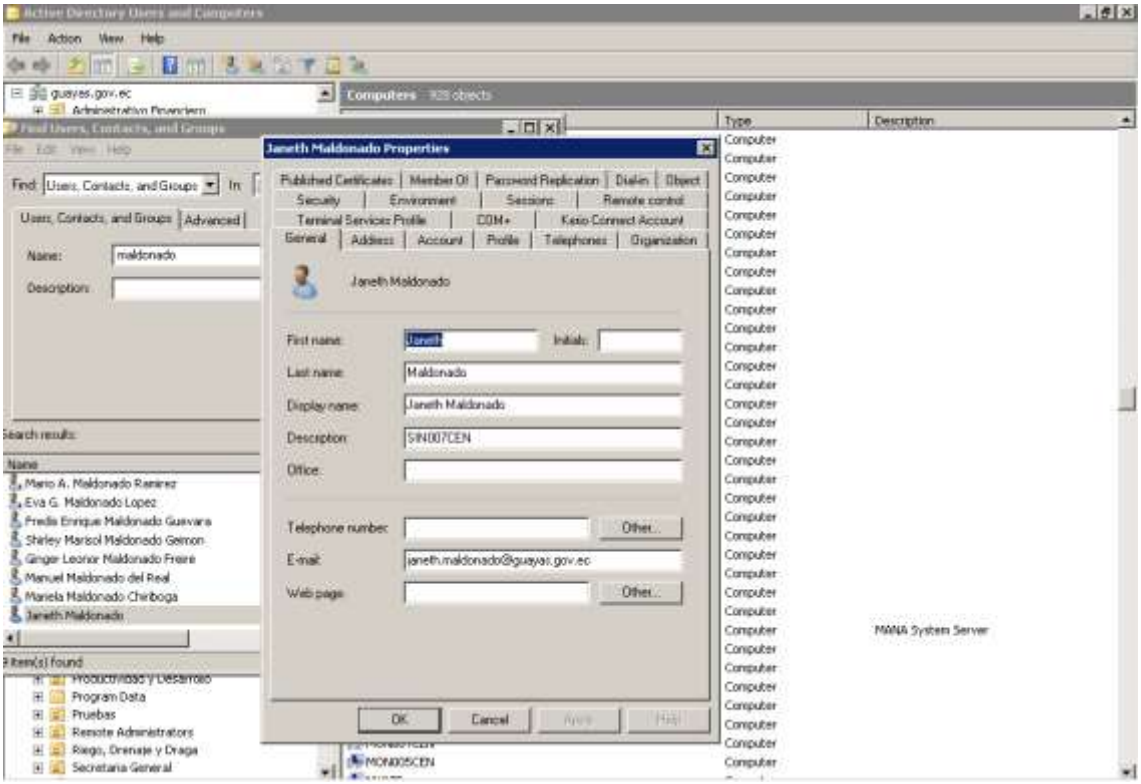

Figura 83 Detalle General del usuario de bancopark creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

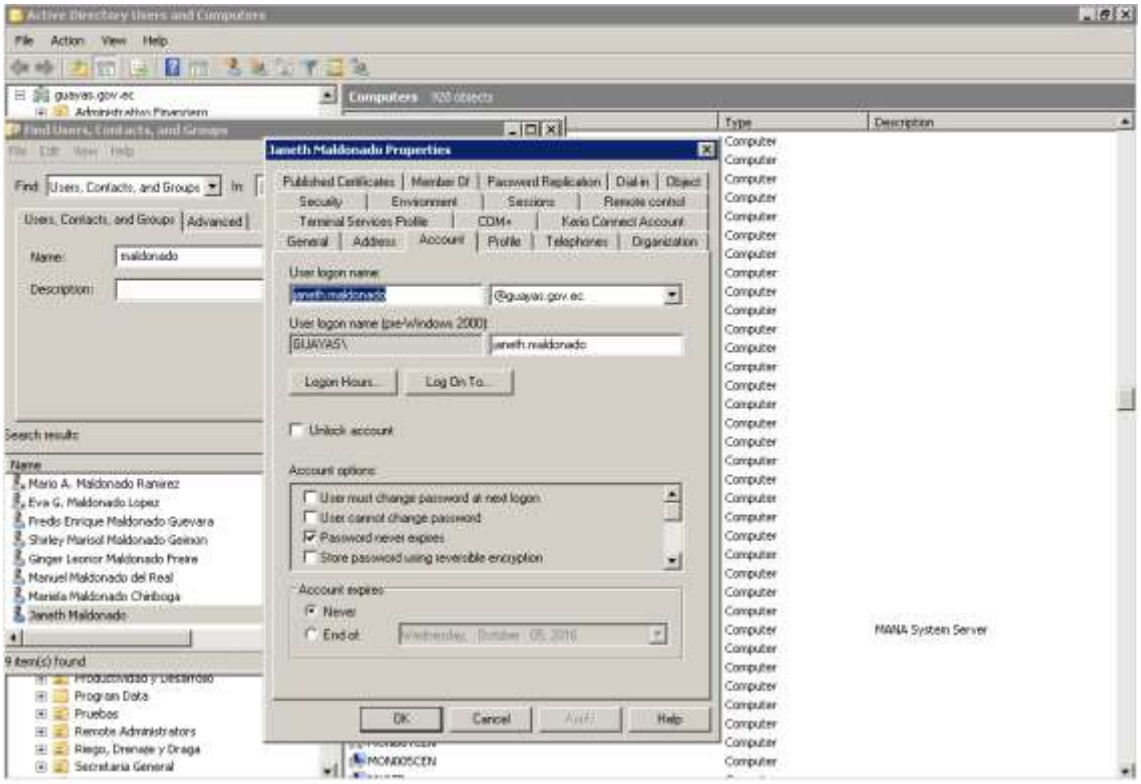

Figura 84 Cuenta del usuario de BancoPark creado en el Active Directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

Huerto

Se realizó la prueba con el usuario washington.wiesner el mismo que se pudo conectar desde la computadora de escritorio al access point con el SSID ‘gpg’ y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al internet. (Ver figura 85 y 86).

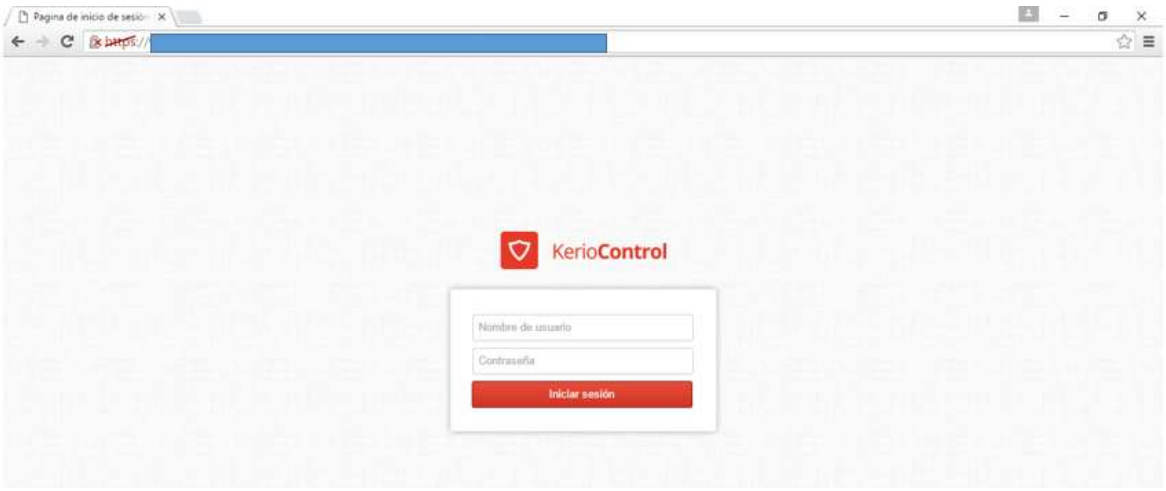

Figura 85 Página de autenticación

Fuente: Gobierno Provincial del Guayas – Software KerioControl

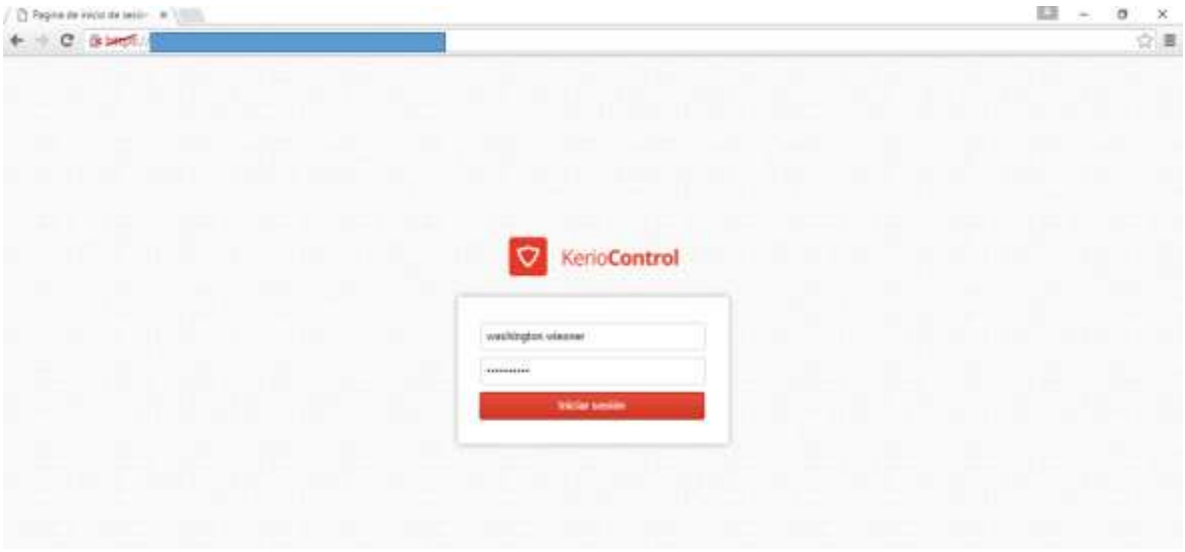

Figura 86 Ingresar datos del usuario

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En el Kerio Control galpones que es el mismo de huertos por falta de licencias se puede visualizar cuantos equipos han inicializado la sesión con la cuenta de washington.wiesner (Ver figura 87) y las estadísticas del usuario (Ver figura 88).

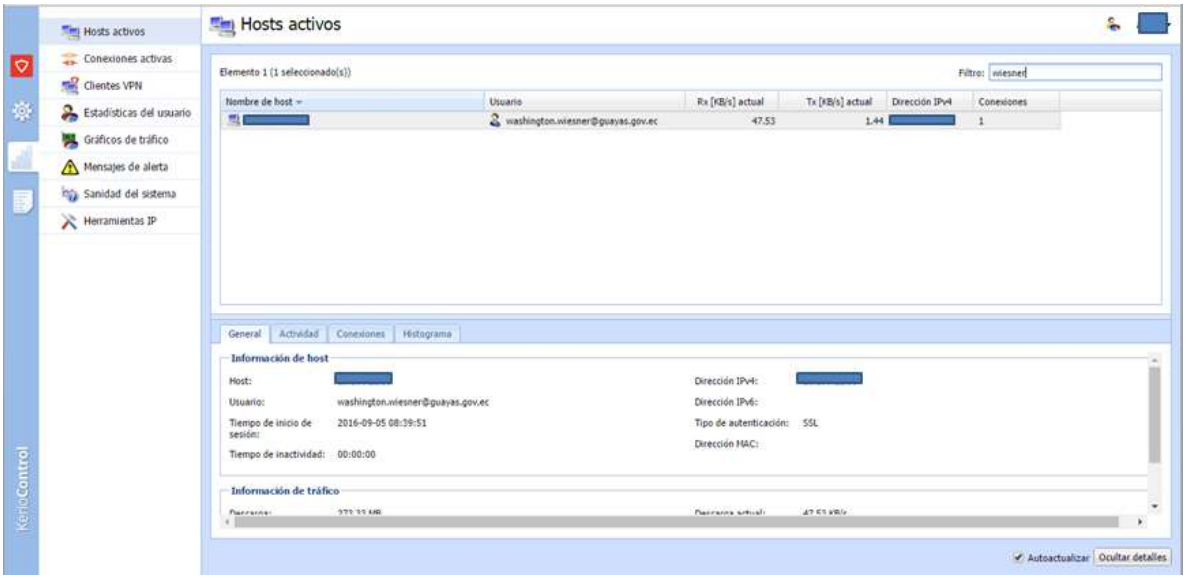

Figura 87 Host activos del usuario de huertos

Fuente: Gobierno Provincial del Guayas – Software KerioControl

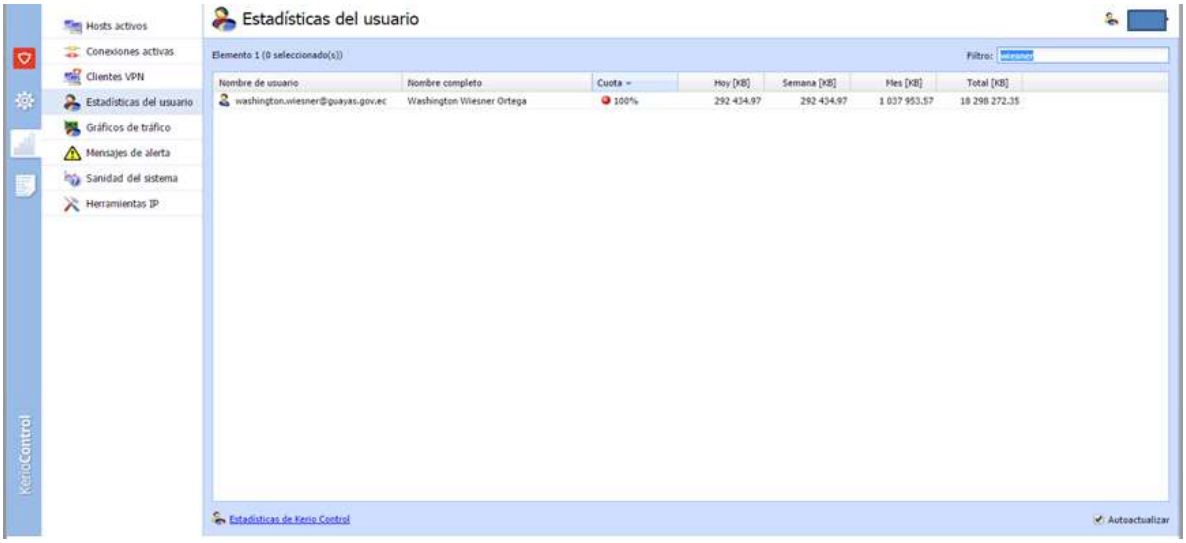

Figura 88 Estadísticas del usuario de huertos

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En la máquina virtual donde se encuentra el active directory se puede constatar que el usuario de washington.wiesner si existe, a que dirección u oficina pertenece el funcionario y cuál es la cuenta que tiene el usuario. (Ver figura 89 y 90).

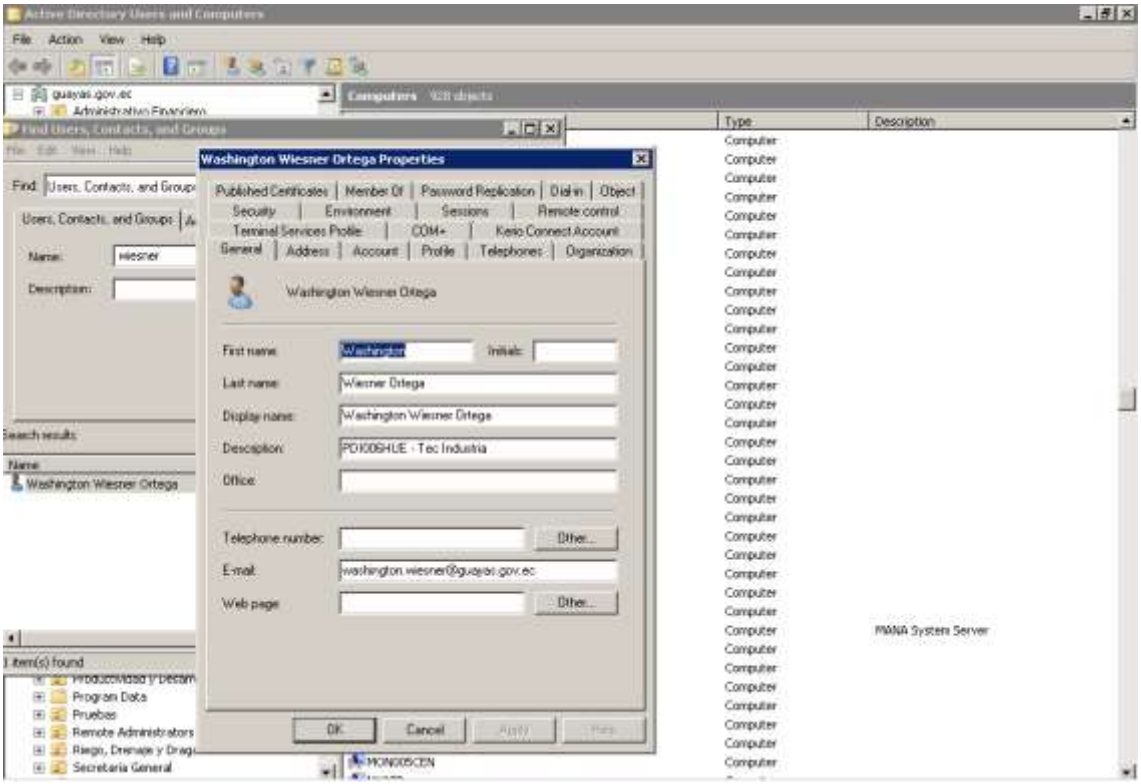

Figura 89 Detalle general del usuario de huertos creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

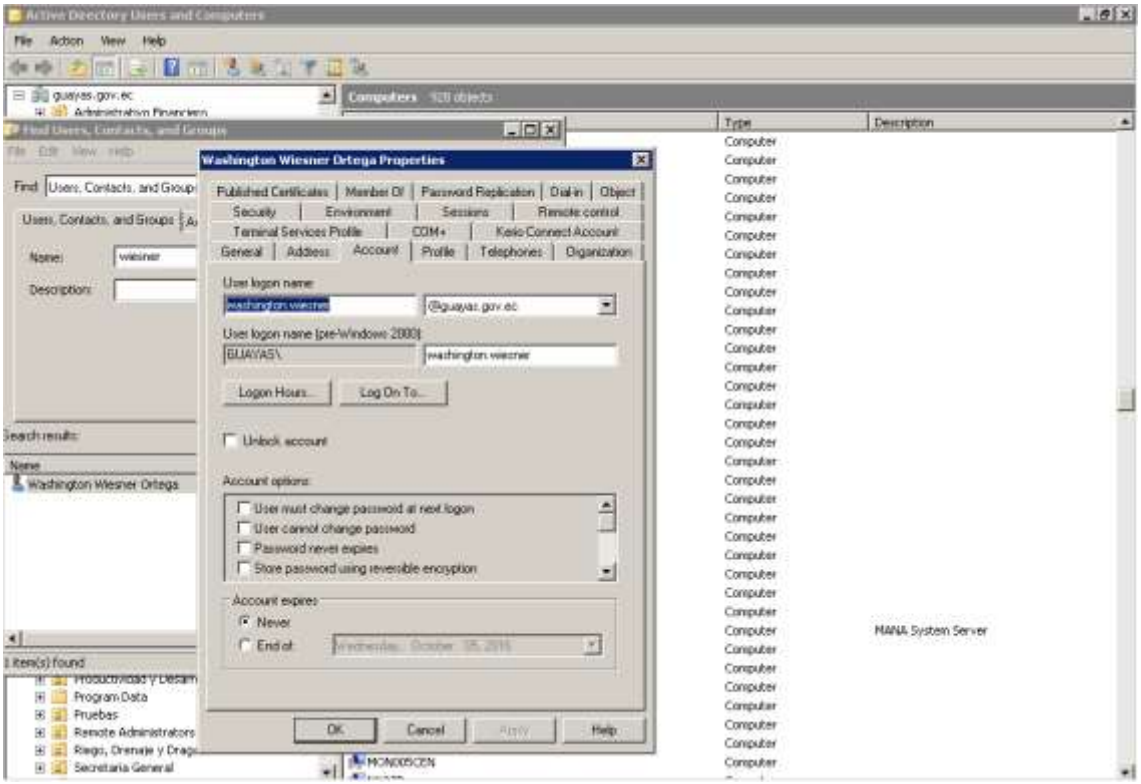

Figura 90 Cuenta del usuario de huertos creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

Equinoterapia

Se realizó la prueba con el usuario mb.wilson.apolo el mismo que se pudo conectar desde la computadora de escritorio al access point con el SSID ‘gpg’ y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al internet. (Ver figura 91 y 92).

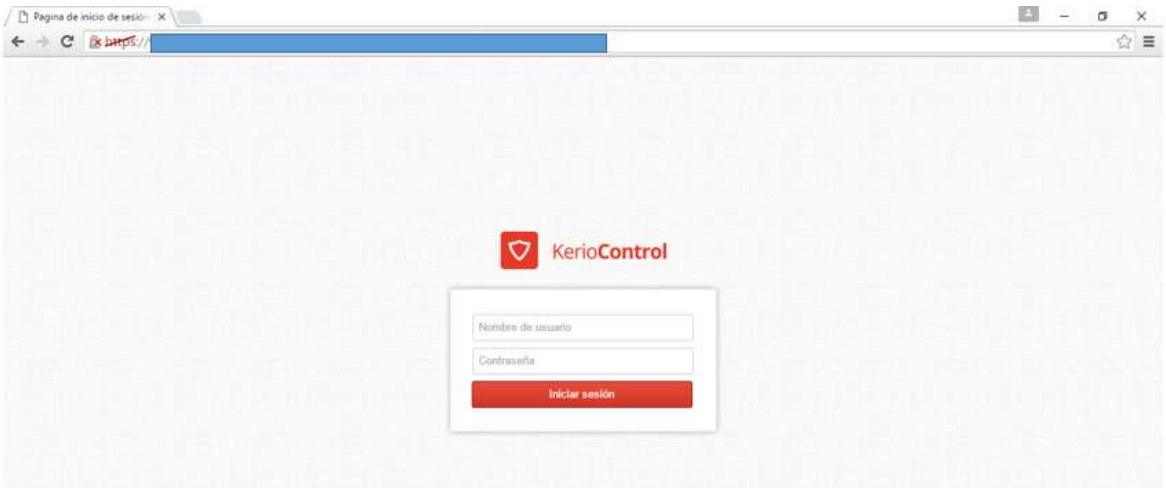

Figura 91 Página de autenticación

Fuente: Gobierno Provincial del Guayas – Software KerioControl

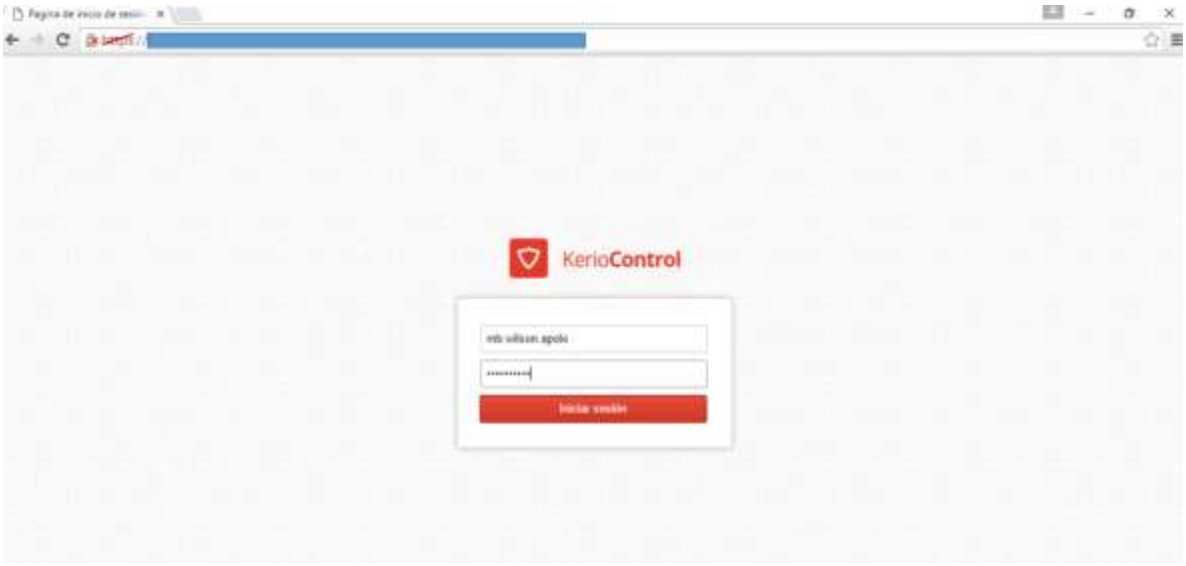

Figura 92 Ingresar datos del usuario de equinoterapia

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En el Kerio Control equinoterapia se puede visualizar cuantos equipos han inicializado la sesión con la cuenta de mb.wilson.apolo (Ver figura 93) y las estadísticas del usuario (Ver figura 94).

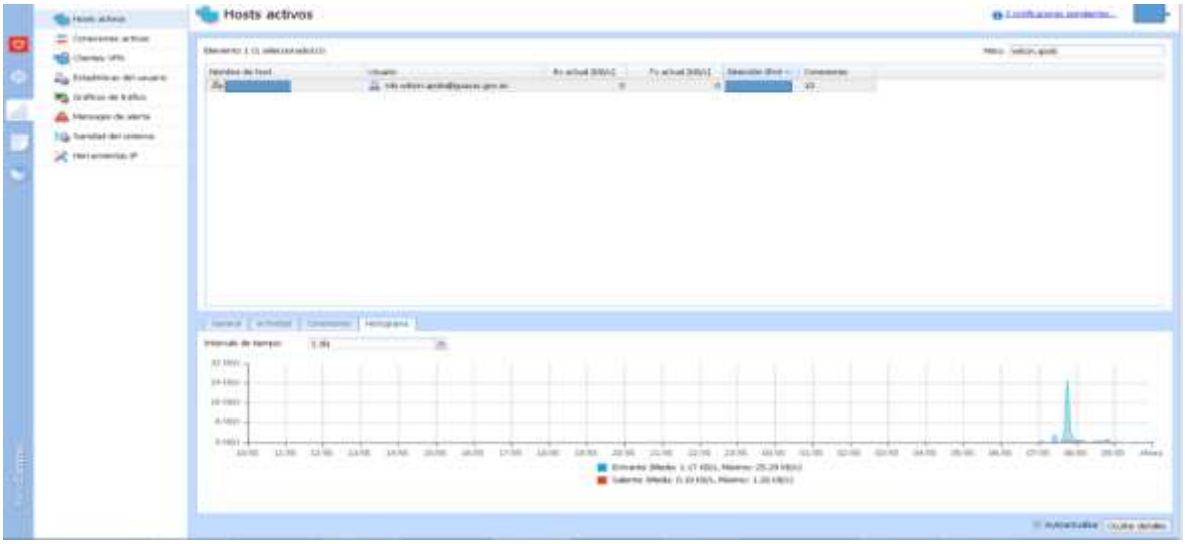

Figura 93 Host activos del usuario de equinoterapia

Fuente: Gobierno Provincial del Guayas – Software KerioControl

Figura 94 Estadísticas del usuario de equinoterapia

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En la máquina virtual donde se encuentra el active directory se puede constatar que el usuario de mb.wilson.apolo si existe, a que dirección u oficina pertenece el funcionario y cuál es la cuenta que tiene el usuario. (Ver figura 95 y 96).

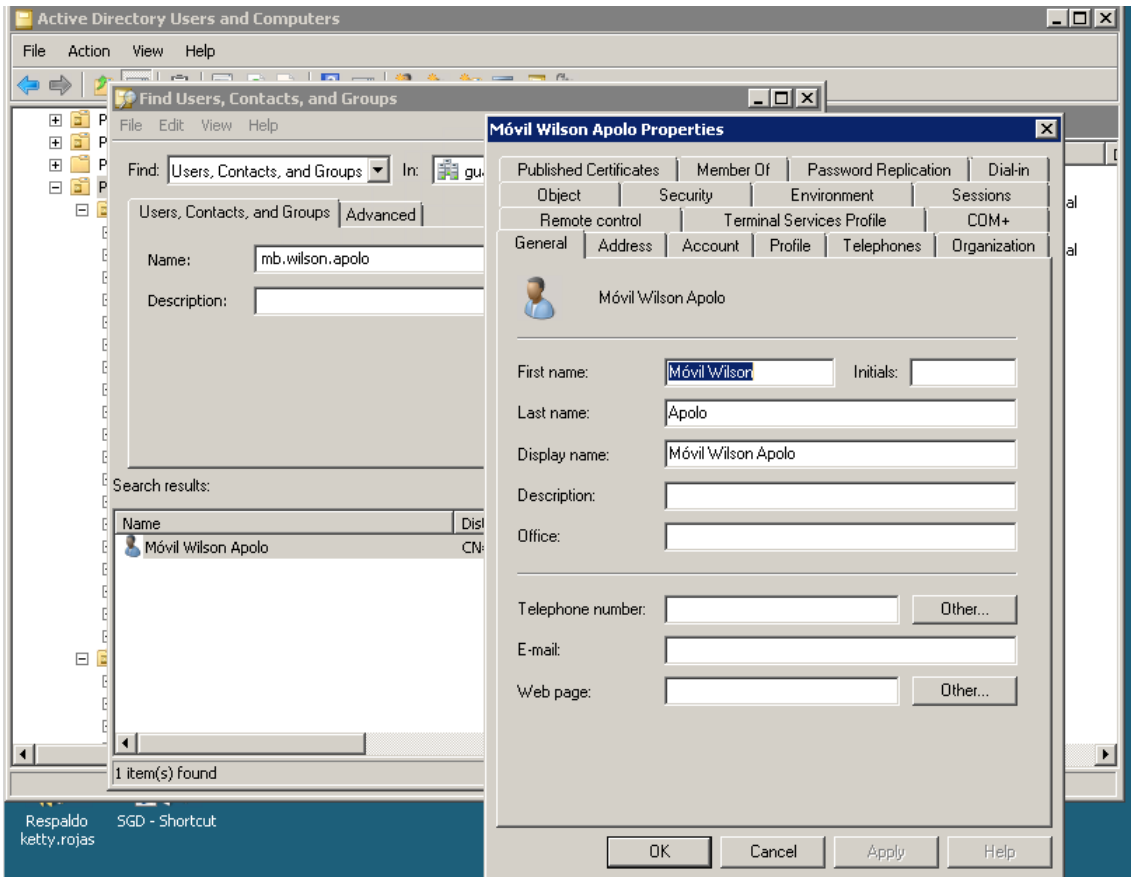

Figura 95 Detalle General del usuario de Equinoterapia creado en el Active Directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

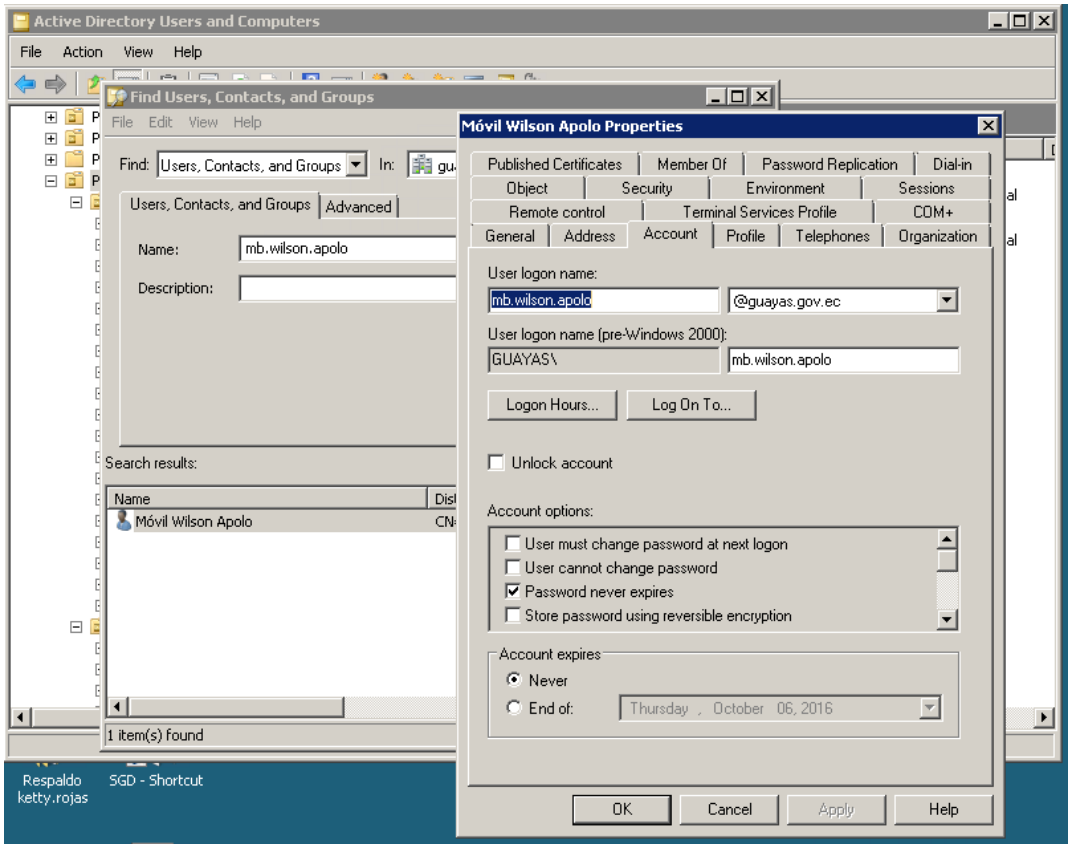

Figura 96 Cuenta del usuario de Equinoterapia creado en el Active Directory

Fuente: Gobierno Provincial del Guayas – Windows Server 208

Se realizó la prueba con el usuario visitante.gpg el mismo que se pudo conectar desde la computadora de escritorio al access point con el SSID ‘gpg’ y automáticamente carga la página de autenticación el cual se registra los datos del usuario que se quiere autenticar para acceder al internet. (Ver figura 96 y 97).

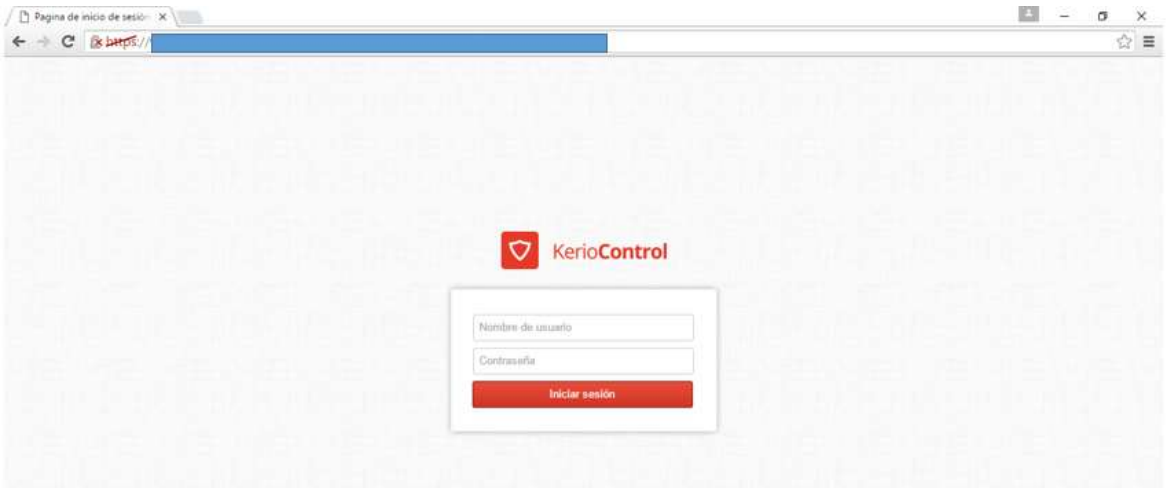

Figura 97 Página de autenticación

Fuente: Gobierno Provincial del Guayas – Software KerioControl

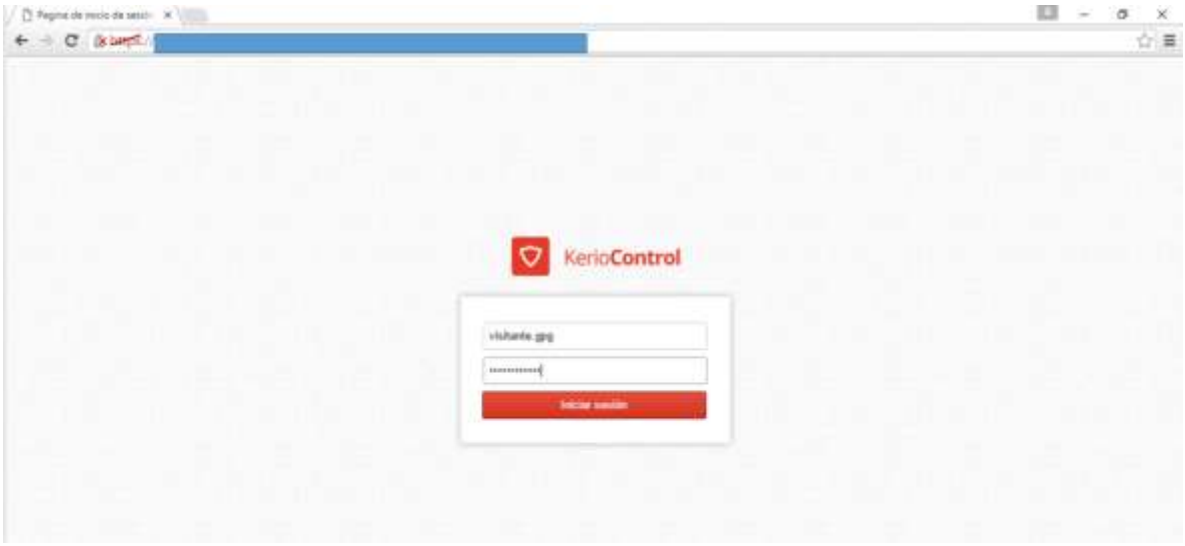

Figura 98 Ingresar datos del usuario de equinoterapia

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En el Kerio Control equinoterapia se puede visualizar cuantos equipos han inicializado la sesión con la cuenta de mb.wilson.apolo (Ver figura 99) y las estadísticas del usuario (Ver figura 100).

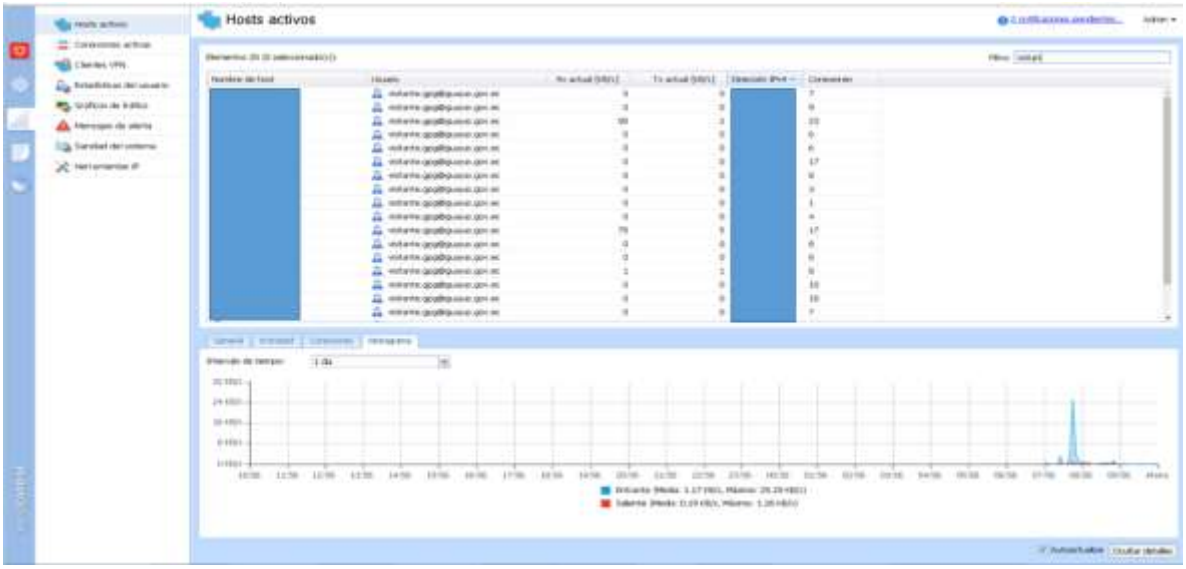

Figura 99 Host activos del usuario visitante

Fuente: Gobierno Provincial del Guayas – Software KerioControl

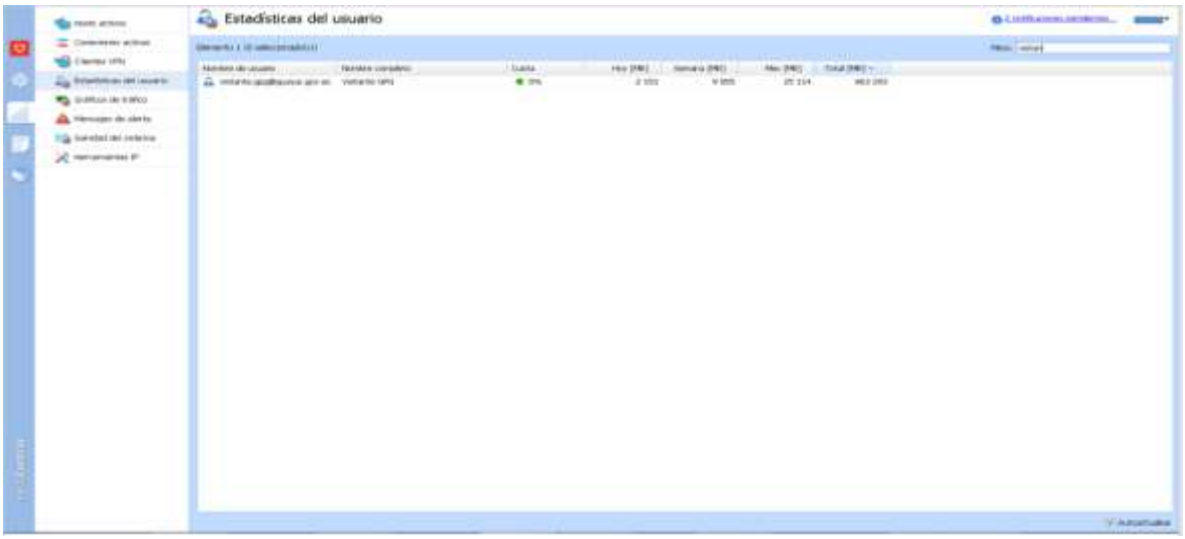

Figura 100 Estadísticas del usuario visitante

Fuente: Gobierno Provincial del Guayas – Software KerioControl

En la máquina virtual donde se encuentra el active directory se puede constatar que el usuario de visitante.gpg si existe, a que dirección u oficina pertenece el funcionario y cuál es la cuenta que tiene el usuario. (Ver figura 101 y 102).

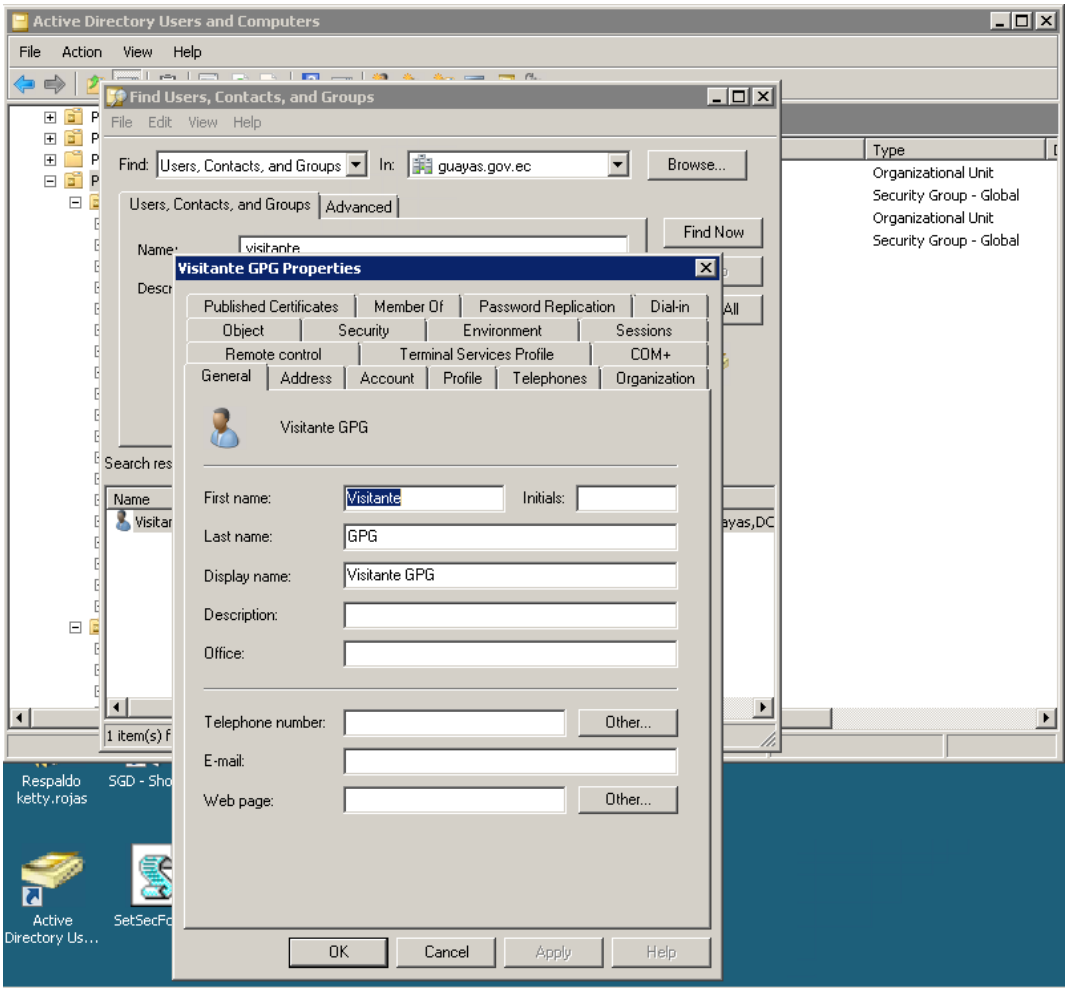

Figura 101 Detalle general del usuario de equinoterapia creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

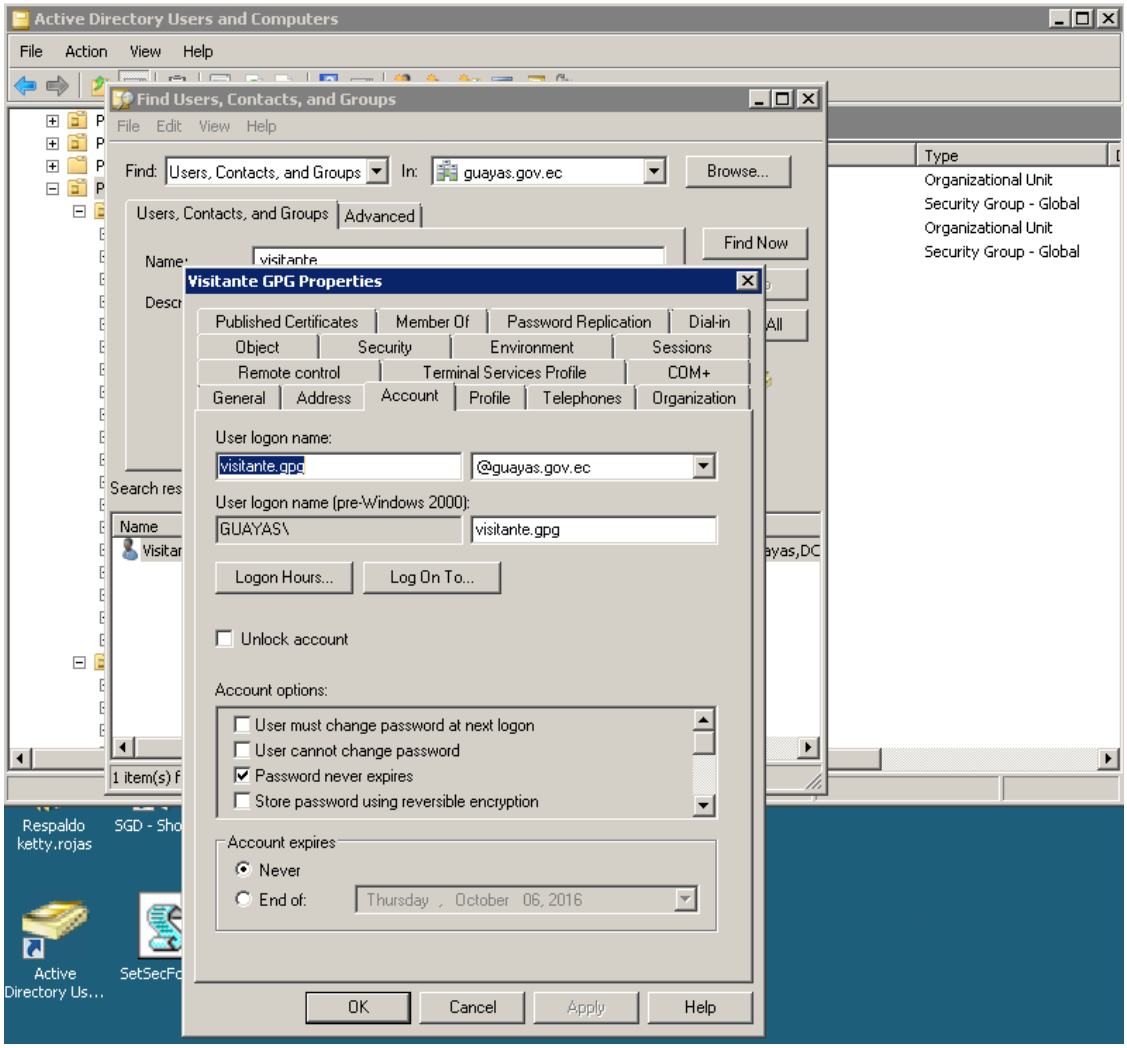

Figura 102 Cuenta del usuario de equinoterapia creado en el active directory

Fuente: Gobierno Provincial del Guayas – Windows Server 2008

10. Resultados

En base a las pruebas antes realizadas se pudo evaluar que los objetivos y las expectativas del proyecto de implementación de un servidor RADIUS en windows server para centralizar la administración de nuevos Access Points en las oficinas remotas de galpones y huertos del Gobierno Autónomo Descentralizado del Guayas se cumplieron.

La conexión inalámbrica entre access point y las computadoras de escritorio con tarjeta inalámbrica, computadoras portátiles, móviles u otros, se estableció con éxito y los funcionarios lograron autenticarse con su usuario y contraseña, lo que se validó con el servidor RADIUS; mismo que permite la autenticación, autorización y administración, donde se comunica con el active directory para revisar en que grupo y en que VLAN está el usuario y contraseña ingresado considerando que estos datos se transmiten encriptados, a su vez el NPS indicará que tipo de política de VLAN tendrá el usuario que se ha autenticado.

Se utilizó el Kerio Control que es un programa que utiliza el departamento de infraestructura tecnológica para administrar y controlar cada una de las oficinas remotas del Gobierno Provincial del Guayas, a su vez este programa administra y supervisa el consumo de ancho de banda y las páginas web que no están permitidas acceder en horario de labores.

El uso de la controladora WLC permitió optimizar el tiempo de configuración de los access point, debido que al estar todos conectados al WLC, se configuran automáticamente con el Cisco Discovery Protocol.

11. Conclusiones

La red inalámbrica es una solución en diversas organizaciones públicas y privadas, satisfaciendo las necesidades de los usuarios. Este tipo de redes brindan confiabilidad y flexibilidad, así como redundancia en los access point que permiten alta disponibilidad.

Se determinó que la implementación de un servidor RADIUS incidió positivamente en la asignación dinámica de VLAN's a través de la red inalámbrica. La construcción del diseño propuesto fue acorde a las necesidades institucionales de brindar cobertura los sitios remotos garantizando autenticación y control en el acceso inalámbrico a los recursos de red.

Se emplearon un total de 33 access point de la marca Cisco de series Aironet 1600 los que son administrados por la controladora, esto permite la gestión oportuna y precisa de la red inalámbrica.

La revisión de los manuales con las políticas de seguridad, facilitó la configuración del servidor y permitió establecer nuevos roles y políticas para los usuarios

La implementación del presente proyecto técnico resultó más económico para el Gobierno Provincial del Guayas que realizar todo un cableado para datos, más aún cuando algunos edificios son alquilados.

Las pruebas realizadas comprueban el correcto funcionamiento del servidor y la aplicación de las políticas de acuerdo al rol de los usuarios. Además, el adiestramiento realizado al personal durante la implementación comprueba el cumplimiento de los requerimientos.

12. Recomendaciones

Se recomienda realizar actualizaciones periódicas, para asegurar un correcto rendimiento de los equipos, además realizar mantenimientos periódicos al servidor RADIUS y el Active Directory, así como revisar el estado físico del equipo de cómputo donde residen estos servidores.

Es indispensable que el Gobierno Provincial del Guayas explote más la tecnología inalámbrica a fin de potencializar otros servicios como VoIP, reubicar el access point de comunicación social 10 metros hacia el norte, para dar cobertura al área de secretaria y desarrollo de TIC's; así mismo trasladar el access point del centro tecnológico popular sobre las ventanillas de atención al público lo que permitirá brindar cobertura a la sala de sesiones de juntas. Actualmente este equipo se encuentra en el vestíbulo donde no existen oficinas; se debe revisar la potencia de transmisión del access point del pasillo de viceprefectura en el edificio principal, debido a que la intensidad de la señal en las cercanías es débil y existe pérdida de paquetes.

Instalar nuevos access point en el edifico principal (1 en talento humano y 1 en asesoría de prefectura), en el edificio tous (1 en medio ambiente), en el edificio bancopark piso 14 (1 en mediación). Estos nuevos access point deben ser configurados y administrados al igual que el resto mediante la controladora.

Debido a la cantidad de usuarios que se encuentran en las oficinas, se recomienda utilizar un ancho de banda igual o superior a los 2 Mbps y manejar un plan de contingencia en caso de que la red inalámbrica presente fallas, este plan deberá incluir equipos access point de backup.

Designar un administrador del sistema de control de red inalámbrica (WLC y WCS), de tal forma que exista constante monitoreo de lo que sucede en la red inalámbrica y pueda brindar solución oportuna ante la presencia de fallos y contar con manuales de configuración y administración para todos los dispositivos de la infraestructura inalámbrica: switches, access point, controladores de access point, servidores de autenticación, servidores active directory, administrador y monitor de la red inalámbrica WCS.

13. Referencias Bibliografía

Cisco Systems Inc. (18 de Octubre de 2015). *¿Cómo el RADIUS trabaja?* Recuperado el 15 de Julio de 2016, de http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.pdf

Ali Ismail Awad, A. E. (2013). *Advances in Security of Information and Communication Networks.* Cairo, Egipto: Springer.

Alvarez. (10 de Septiembre de 2009). *Alvarez*. Recuperado el Junio de 2016, de http://blog.alvarezp.org/2009/07/10/el-mito-de-los-11-canales-de-80211bg/

Angie Londoña, N. L. (11 de Diciembre de 2013). *Slideshare.* Recuperado el Junio de 2016, de http://es.slideshare.net/Rasta-Aliria/manual-de-instalacin-de-active-directory-en-windows-server-2008-r2

Charles, N. (1990). *El proceso de la entrevista.* Mexico: Kapelusk.

CISCO. (19 de Enero de 2012). *CISCO*. Recuperado el 22 de Agosto de 2016, de CISCO: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2940/software/release/12-1_19_ea1/configuration/guide/2940scg_1/swvlan.html

CISCO. (24 de Octubre de 2014). *Cisco Aironet 1600*. Recuperado el Junio de 2016, de http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1600-series/data_sheet_c78-715702.html

Cisco. (2014). Cisco CleanAir Technology. *Cisco CleanAir Technology*, 4.

Cisco. (08 de Agosto de 2016). *Cisco Product.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1600-series/data_sheet_c78-715702.html

Cisco. (08 de Agosto de 2016). *Cisco Product.* Obtenido de Cisco Product: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1600-series/data_sheet_c78-715702.html

CISCO. (2016). *Productos CISCO.* Recuperado el Junio de 2016, de http://www.cisco.com/c/en/us/products/wireless/aironet-1600-series/index.html#

CISCO. (09 de Agosto de 2016). *Tunneling and Native VLANs.* Obtenido de http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swtunnel.html

CISCO. (s.f.). *Cisco - Wireless LAN Controller*. Recuperado el 2016, de http://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html?referring_site=smartnavRD

Colomés, P. (03 de Septiembre de 2013). *Slideshare.* Recuperado el 22 de Agosto de 2016, de http://es.slideshare.net/pcolomes/cracking-wep-97

EUROPA.EU. (12 de MAYO de 2006). *LIBRO VERDE SOBRE LAS CONVERGENCIAS.* Recuperado el 25 de JUNIO de 2015, de http://europa.eu/legislation_summaries/information_society/internet/l24165_es.htm

Eyssautier, d. l. (2002). *Metodología de la Investigación.*

Gobierno Provincial del Guayas. (30 de Enero de 2015). Art.1 . *Resolución No.DTH-GPG-001-005*. Guayaquil, Guayas, Ecuador.

IEEE. (10 de Diciembre de 2012). *IEEE*. Obtenido de http://standards.ieee.org/about/get/802/802.11.html

ITCONSULTANTS. (2012). *Windows Server Active Directory.* Recuperado el 22 de Agosto de 2016, de Windows Server Active Directory: http://www.itcopr.com/index.php/soluciones/beneficios-de-windows-2012/implementacion-de-active-directory/

JAIN, R. (10 de ABRIL de 2010). *www.cse.wustl.edu.* Recuperado el 25 de JUNIO de 2015, de http://www.cse.wustl.edu/~jain/cis788-97/ftp/h_7vlan.pdf

Jon Tate, P. B. (Enero de 2016). *Book Google.* Recuperado el Junio de 2016, de https://books.google.com.ec/books?id=m-1jCwAAQBAJ&pg=PA73&dq=virtual+local+area+network&hl=es-419&sa=X&redir_esc=y#v=onepage&q&f=true

Kioskea. (8 de Junio de 2014). Redes Inalámbricas. *Kioskea Enciclopedia*, http://es.ccm.net/contents/818-redes-inalambricas.

Laurent-Maknavicius, H. C. (2007). *Wireless and Mobile Network Security.* Francia: Hermes Science/Lavoisier.

Microsoft. (Enero de 2005). *Msdn Microsoft.* Recuperado el Junio de 2016, de https://msdn.microsoft.com/es-es/library/cc758565(v=ws.10).aspx

Microsoft. (1 de Enero de 2005). *Protocolo de autenticación extensible(EAP).* Recuperado el 16 de Julio de 2016, de https://msdn.microsoft.com/es-es/library/cc782159(v=ws.10).aspx

Microsoft. (2 de Marzo de 2016). *Technet Microsoft - Group Policy GPO.* Recuperado el Junio de 2016, de https://technet.microsoft.com/en-us/windowsserver/bb310732.aspx

Microsoft, T. (11 de Octubre de 2004). *Technet Microsoft.* Recuperado el Junio de 2016, de https://technet.microsoft.com/es-es/library/dd458733.aspx

Microsoft, T. (23 de Julio de 2014). *Technet Microsoft.* Recuperado el Junio de 2016, de Windows Server 2008 R2 and Windows Server 2008: https://technet.microsoft.com/en-us/library/dd349801(v=ws.10).aspx

NIGEL, W. (18 de MARZO de 2014). *WIFI NIGEL*. Recuperado el 25 de JUNIO de 2015, de http://wifinigel.blogspot.com/2014/03/microsoft-nps-as-radius-server-for-wifi_18.html

Ramirez, M. T. (07 de Julio de 2016). *Rincon del Vago.* Recuperado el 22 de Agosto de 2016, de http://html.rincondelvago.com/redes-privadas-virtuales_1.html

Roberto Hernández Sampieri. (2010). *Metodología de laInvestigación.* Mc Graw Hill.

Rodríguez Gómez, D., & Valldeoriola Roquet, J. (s.f.). *Metodología de la Investigación.* Universitat Oberta de Catalunya. Recuperado el 15 de 06 de 2016, de http://zanadoria.com/syllabi/m1019/mat_cast-nodef/PID_00148556-1.pdf

Rojas, E. (18 de Febrero de 2013). *MuyComputerPro*. Recuperado el 22 de Agosto de 2016, de MuyComputerPro: http://www.muycomputerpro.com/2013/02/18/elementos-red-wlan-estandar-802-11n

Server, S. W. (2009). *Search Windows Server 2009.* Obtenido de http://searchwindowsserver.techtarget.com/tutorial/Windows-Server-2008-Learning-Guide

Technologies, H. (2012). *Huawei Productos.* Obtenido de http://e.huawei.com/en/products/enterprise-networking/wlan/outdoor-access-points/ap6510dn-agn-ap6610dn-agn

Voinea, J. G. (2011). *Redes de Comunicaciones. Administración y Gestión.* El Parador - Almeria: Plaza Romera 9.

Wikipedia. (2 de Noviembre de 2014). *Punto de Acceso Inalámbrico.* Recuperado el Junio de 2016, de https://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico

14. Anexos

1. Guía de Preguntas Para entrevista

DIRECTOR PROVINCIAL TICS

1) De acuerdo a su criterio ¿Cuál es el problema que existe actualmente?
2) ¿Qué causas conllevan a que ocurra este problema?
3) ¿Lo han resuelto? Y de ser afirmativo ¿Cómo lo resuelven ahora?
4) ¿Qué espera que se mejore?
5) ¿Dónde están ubicadas las oficinas remotas que necesitan tener conexión?
6) Qué tipos de servicios desean brindar a través de la red inalámbrica
7) ¿Cuál será el beneficio para los usuarios finales?
8) ¿Quiénes serán los beneficiados con esta solución?
9) ¿Considera que si se implementa un servidor RADIUS en Windows server para centralizar la administración de nuevos Access Points en las oficinas remotas de galpones y huertos solucione este problema?
10) ¿Con qué marcas de equipos de conmutación trabajan en los centros de cómputo?, se debe considerar para la tomar de decisión sobre la compatibilidad entre los Access Point y los Switches.

JEFE DEL DEPARTAMENTO DE REDES

1) De acuerdo a su criterio ¿Cuál es el problema que existe actualmente?
2) ¿Existe un diagrama de la red de la institución? Y de ser afirmativa, ¿Puede ser facilitada?
3) ¿Cuentan con alguna solución inalámbrica?
4) ¿Existe un manual con las políticas de seguridad que maneja la institución?

 NO (Pasar a la 7ma. pregunta.)

 SI (Pasar a la siguiente pregunta.)

5) ¿Puede ser publicado en el presente trabajo de titulación?

 NO (Pasar a la siguiente pregunta.)

 SI (Se publicara.)

6) ¿Puede ser facilitado a quienes están elaborando el proyecto de solución?

 NO  SI

7) ¿Se puede acceder a la información de configuración para conocer la situación actual y proponer políticas de mejoras?

JEFE DEL DEPARTAMENTO TÉCNICO

1) De acuerdo a su criterio ¿Cuál es el problema que existe actualmente?
2) ¿Cuántos usuarios existen en las oficinas remotas? y ¿Cuenta con algunas áreas dentro de la ellas y cuantas son?
3) En caso de que exista algunas áreas, indicar ¿cuantos usuarios son por cada una de ellas?
4) ¿Qué tipo de dispositivos utilizan los usuarios y que sistema operativo tienen instalado?
5) ¿Cuál es el área de cobertura que desean alcanzar?
6) ¿Cuántos equipos inalámbricos serian? para medir la cantidad de transmisión de datos.
7) ¿Con cuántos Access Point se cuenta para el proyecto?

USUARIOS FINALES GALPONES Y HUERTOS

1) ¿Cuáles son sus principales responsabilidades?
2) ¿Cómo determina el éxito en lo que hace?
3) ¿Qué tipo de aplicaciones utiliza?
4) ¿Qué problemas interfieren con su éxito?
5) ¿Qué problemas tiene con la red actualmente?
6) ¿Cómo lo resuelve hasta ahora?
7) ¿Cuáles son sus expectativas con respecto a la conexión inalámbrica?
8) ¿Tiene usted alguna necesidad especial con respecto a la conexión?

2. Conclusión

DIRECTOR PROVINCIAL TICS

Durante la entrevista, el Ing. Patricio Ordoñez Bustamante indica que el problema es la falta de puntos de red en las oficinas remotas, dado que no hubo una planificación adecuada para el crecimiento de la institución; cuando un dispositivo externo no pertenece a la Institución solo podrá contar con el servicio de Internet y no a la red Interna, debido a que no se cuenta con lo suficiente equipos Access Point y un servidor AAA para la autenticación de usuarios, no pueden acceder a los diversos servicios que el Gobierno Provincial del Guayas ofrece a los empleados de la Institución, un tiempo los empleados tuvieron que solicitar usuario y contraseña VPN y la Dirección Provincial de Tecnología de la Información y Comunicación – TICs es la encargada de aprobar dicha solicitud, en las oficinas remotas de Galpones y Huertos ubicadas en la Av. Pedro Menéndez Gilbert y Av. Plaza Dañin, falta acceso a algunos servicios que ofrece la red del Gobierno Provincial del Guayas tales como internet, intranet, debido a que no existen suficientes equipos Access Point y un servidor AAA para la autenticación de usuarios, lo cual no permite satisfacer las solicitudes de acceso realizadas por funcionarios que tienen equipos portátiles personales en el 2016. En la oficina matriz se cuenta con una Controladora Inalámbrica de marca Cisco y con algunos Access Points también de marca Cisco distribuidos en diferentes áreas para dar acceso inalámbrico a la red de invitados. La red inalámbrica existente sólo funciona para invitados y permite acceso a Internet; sin embargo, también es necesario proveer de acceso a servicios de la red local e Intranet en Galpones y Huertos.

Al implementar un servidor RADIUS en Windows Server para centralizar la administración de nuevos Access Point en las oficinas remotas, solucionara el problema dado que se puede ofrecer a los funcionarios de Galpones y Huertos el acceso a la red interna y al internet aumentando los equipos de Access Point (AP).

Todos los equipos que se utilizaron en los centros de cómputo, tanto del Edificio principal como en las oficinas remotas, son de la marca CISCO.

JEFE DEL DEPARTAMENTO DE REDES

La red inalámbrica existente solo sirve para usuarios invitados permitiendo acceso a Internet, pero no a los servicios disponibles en la red Interna, se cuenta con un diagrama de red de la zona donde será implementado la solución, será entregado para la respectiva visualización; en la actualidad se cuenta con una red inalámbrica pero solo tienen acceso al Internet, y se quiere brindar a todos los usuarios el acceso al internet y a la red interna, si son necesarias para cumplir con las funciones laborables, es por eso que cada usuario está asignada a un grupo y ese grupo a su respectiva VLAN con sus políticas asignadas.

Se cuenta con un manual de políticas de seguridad que por seguridad no puede ser publicado, pero será facilitado en las instalaciones del Gobierno Provincial del Guayas, podrán visualizar las configuraciones que actualmente posee la institución y alguna sugerencia dada, será analizada y si eso beneficia a la entidad pública será implementado.

JEFE DEL DEPARTAMENTO TÉCNICO

En entrevista con el Ing. Pablo Tapia Bastidas indica que existe falta de acceso a los servicios de la intranet a través de medios inalámbricos. Existen alrededor de 165 usuarios en Galpones y Huertos, de estos usuarios alrededor del 50 % requieren conectarse a la red de forma inalámbrica tanto con el computador como con Smartphone.

La solución inalámbrica debe cubrir a todas las oficinas remotas de Galpones y Huertos.

De lo antes descrito se puede concluir que para la solución inalámbrica se debe gestionar de manera centralizada la autenticación en el acceso inalámbrico, de igual manera que existirá alrededor de 150 conexiones inalámbricas.

USUARIOS FINALES GALPONES Y HUERTOS

Después de haber entrevistado a los informantes clave señores Wilson Apolo, Ing. Daniel Vera, Ing. Luis Regalado e Ing. Giovanni Podestá, se puede concluir que existe gran lentitud en la conexión inalámbrica, descargar un archivo de la web es muy lento y si se trasladan de una oficina a otra se pierde la conexión.

En muchos casos reportan que se conectan a la red wifi y no navegan, y en el peor de los casos no logran conectarse a la red inalámbrica y aparece mensaje “Obteniendo dirección IP”, que seguramente se debe a que no hay direcciones IP`s disponibles para la conexión.

Algunos usuarios requieren acceder a la intranet vía wireless desde sus portátiles, pero los servicios no están disponibles.

Se considera que deben existir políticas de calidad de servicio a fin de mejorar el tráfico de los diversos servicios a los que acceden los usuarios.

2. **Fotos de la Ubicación de los AP**

PLANTA BAJA EDIFICIO CENTRAL

Figura 103 Ubicación del AP en Pasillo de Tesorería

Fuente: Gobierno Provincial del Guayas

MEZZANINE EDIFICIO CENTRAL

Figura 104 Ubicación del AP en Contabilidad

Figura 105 Ubicación del AP en Pasillo Dirección Financiera

Fuente: Gobierno Provincial del Guayas

PRIMER PISO EDIFICIO CENTRAL

Figura 106 Ubicación del AP de Comunicación Social

Figura 107 Ubicación del AP en Desarrollo Comunitario

Fuente: Gobierno Provincial del Guayas

Figura 108 Ubicación del AP en Talento Humano

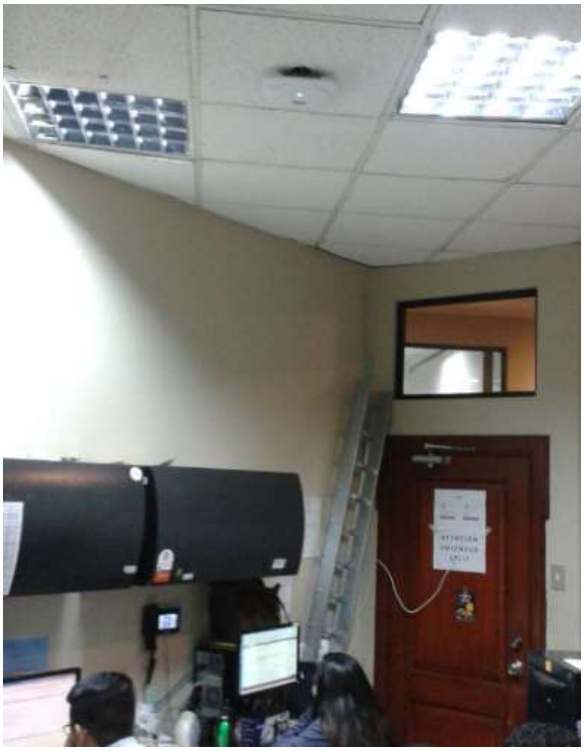

Figura 109 Ubicación del AP en Redes

Fuente: Gobierno Provincial del Guayas

SEGUNDO PISO EDIFICIO CENTRAL

Figura 110 Ubicación del AP en Auditoría

Figura 111 Ubicación del AP en Procuraduría Síndica

Fuente: Gobierno Provincial del Guayas

Figura 112 Ubicación del AP en Secretaría General

TERCER PISO EDIFICIO CENTRAL

Figura 113 Ubicación del AP en Fiscalización

Fuente: Gobierno Provincial del Guayas

Figura 114 Ubicación del AP en Obras Públicas

Figura 115 Ubicación del AP en Estudios y Proyectos

Fuente: Gobierno Provincial del Guayas

CUARTO PISO EDIFICIO CENTRAL

Figura 116 Ubicación del AP en Prensa Prefectura

Figura 117 Ubicación del AP en Pasillo de Asesores

Fuente: Gobierno Provincial del Guayas

Figura 118 Ubicación del AP en Desarrollo Sostenible

QUINTO PISO EDIFICIO PRINCIPAL

Figura 119 Ubicación del AP en Auditorio

Fuente: Gobierno Provincial del Guayas

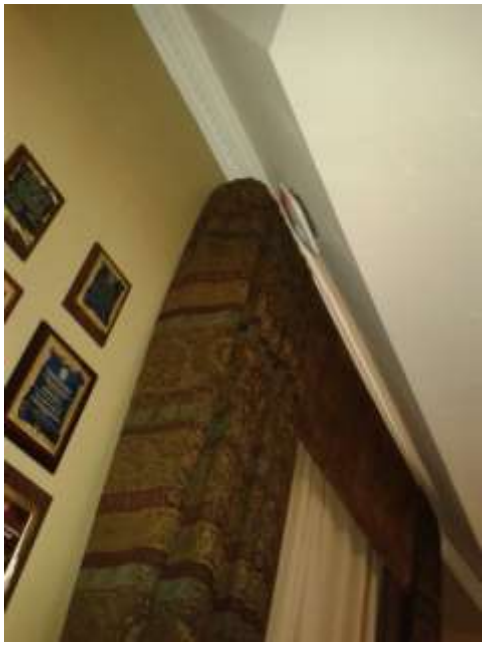

Figura 120 Ubicación del AP en Oficina del Prefecto

Figura 121 Ubicación del AP en Sala de Reuniones

Fuente: Gobierno Provincial del Guayas

PISO 14 EDIFICIO BANCO PARK

Figura 122 Ubicación del AP en Riego, Drenaje y Dragas

Figura 123 Ubicación del AP en Riego, Drenaje y Dragas

Fuente: Gobierno Provincial del Guayas

Figura 124 Ubicación del AP en Coordinación Compras Públicas

MEDIO AMBIENTE

Figura 125 Ubicación del AP en Gestión Ambiental

Fuente: Gobierno Provincial del Guayas

CENTRO TECNOLOGICO POPULAR – CTP

Figura 126 Ubicación del AP en CTP

EQUINOTERAPIA

Figura 127 Ubicación del AP en Dirección de Equinoterapia

Fuente: Gobierno Provincial del Guayas

Figura 128 Ubicación del AP en Estimulación Temprana

Figura 129 Ubicación del AP en Terapia de Lenguaje

Fuente: Gobierno Provincial del Guayas