UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE INGENIERÍA

CARRERA INGENIERÍA ELECTRÓNICA

PROYECTO DE GRADO

DISEÑO DE UN SISTEMA DE GESTIÓN REMOTO PARA OPTIMIZAR EL ACCESO AL SERVICIO DE INTERNET EN LA COOPERATIVA DE AHORRO Y CRÉDITO "UNIÓN SANTIAGO DE MACHACA"

AUTOR: LUIS ALBERTO BLANCO SALCEDO

TUTOR: ING. CESAR LOZANO MANTILLA

La Paz – Bolivia

2020

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERIA

LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

DEDICATORIA

El presente proyecto de grado lo dedico principalmente a Dios por guiar mi camino a este momento.

A mi hermana Graciela y a mis padres quienes siempre me brindaron su apoyo en los buenos y malos momentos y por ser un ejemplo de superación.

A todas aquellas personas que siempre me acompañaron a lo largo de mi carrera universitaria brindándome sus consejos y apoyo.

A la Universidad Mayor de San Andrés por darme la oportunidad de ser parte de esa gran familia.

AGRADECIMIENTOS

Agradezco a Dios, por haberme permitido culminar una de mis principales metas y acompañarme todos los días de mi vida. También debo decir que este esfuerzo lo atribuyo a mi hermana y a mis padres por brindarme su apoyo incondicional.

Asimismo, un sincero agradecimiento al Ing. Cesar Lozano Mantilla por el asesoramiento y enseñanza, al Ing. Marcelo Gutierrez Guachalla y Ing. Ramiro Puch Terán por los consejos y la paciencia que me brindaron a la hora de revisar el presente proyecto de grado.

RESUMEN

El presente proyecto, tiene como propósito diseñar un sistema de gestión remoto para optimizar el acceso al servicio de internet en la cooperativa de ahorro y crédito “Unión Santiago de Machaca”. Dentro el principal problema detectado se tiene que la Cooperativa al ser una entidad financiera necesita un Certificado de Adecuación para lo cual requiere actualizar las tecnologías desarrolladas y mejorar así la seguridad informática por su adecuación con el sector financiero, dicho análisis, se diagnostica la situación actual de la cooperativa para poder hallar las falencias y vulnerabilidades dentro de la misma, se clasificara las mejores soluciones considerando las características principales de los equipos y precios para luego diseñar un diagrama global de red WAN, LAN para el sistema de gestión remoto, y de esta manera configurar los equipos con políticas de protección perimetral de red para fortalecer la comunicación remota entre ambas sucursales. Lo anterior favoreció para la formulación de conclusiones, las cuales pretenden ayudar a minimizar los riesgos de conexión considerando que el flujo de información viaje de forma segura y optima evitando así gastos futuros en su mantenimiento.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

CAPITULO I

MARCO REFERENCIAL

1.1. Introducción

El desarrollo del Presente Estudio determinará el diseño de una red remota para optimizar el servicio de comunicación y el intercambio de información mediante el acceso al servicio de internet en la Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca" mejorando el servicio de comunicación entre los funcionarios de la cooperativa tanto el departamento de gerencia, administrativo y el departamento operativo que ayudaran a minimizar los riesgos de conexión e interferencia que amenazan la prestación del servicio.

El propósito que persigue la investigación va en respuesta a la necesidad de un cambio tecnológico donde se evitará gastos futuros en mantenimientos y nuevos diseños de red con cableado estructurado posteriormente, es por ello que la presente propuesta permitirá disminuir los costos e incrementará la agilidad de intercambio de comunicación y correspondencia manteniendo la confidencialidad que amerita una institución de esta naturaleza mediante el acceso al servicio de internet.

Debido a las características y sus necesidades de la cooperativa, no es factible actualmente ofrecer el servicio por medio de conexiones cableadas entre la agencia central y las sucursales; a esto se une la baja capacidad de internet inalámbrica contratada con el proveedor de servicios.

El problema de estudio fue identificado a través de un diagnostico donde se pudo verificar que el servicio de la red es asimétrico, lo cual dificulta el intercambio de información documentada entre las agencias con la que maneja la cooperativa, causando pérdidas de tiempo y gastos económicos extras por tanto se precisa un servicio de internet en base a una red inalámbrica simétrica para los servicios que brinda la institución como tal.

De tal manera a continuación se describen desde los antecedentes, el problema trazado y los objetivos trazados para el desarrollo investigativo.

1.2. Antecedentes

La Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca" (USAMA Ltda.) fue constituida mediante Resolución de Consejo N° 04655 de 6 de junio de 1994, se encuentra inscrita en el Registro Nacional de Cooperativas con el registro N° 5033 de 29 de mayo de 1998.

Su oficina central se encuentra ubicada en la Zona 16 de Julio, Avenida Juan Pablo II, N° 2887 de la ciudad del El Alto, asimismo, cuenta con un punto de atención ubicado en la calle Isaac Tamayo N° 662, zona el Rosario de la ciudad de La Paz.

La Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca" (USAMA Ltda.) dispone de un servicio de internet con un tendido de red cableado (para mejorar la velocidad) en cada agencia, datos recabados al visitar el centro de datos de esta institución, estas redes cuentan con 5 Mbps de velocidad de descarga y 1.2 Mbps de carga.

El servicio de red asimétrico no es adecuado para instituciones que trabajan con intercambio de información constante y confidencial como maneja la cooperativa, es deficiente tanto por las interrupciones del servicio como por la velocidad.

1.3. Situación actual

La Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca", tiene planificada la actualización del Plan Estratégico para el periodo 2018 – 2020, para lo cual se efectuó un seminario taller en la segunda semana del mes de diciembre de 2017 con la participación de los miembros del Directorio, Gerencia General, Jefaturas y Encargados de Área de la Cooperativa.

1.4. Planteamiento del problema

Dentro el principal problema detectado se tiene que la Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca" (USAMA Ltda.), actualmente cuenta con un servicio de afiliación, ahorro y crédito en todas sus agencias centralizadas en servidores ubicados en dependencias de la oficina central bajo resguardo de un oficial de recursos tecnológicos.

Por tanto, a las características de velocidad del sistema y conforme a los recursos tecnológicos con los que se cuenta van enmarcándose en riesgos de tecnología por su adecuación con el sector financiero.

Otra de las necesidades detectadas por parte de La Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca" (USAMA Ltda.) es la obtención del Certificado de Adecuación para lo cual se requiere actualizar las tecnologías desarrolladas en el ámbito de la intermediación financiera y de valores establecidos por las normas de la ASFI, problema que aqueja y preocupa a la institución actualmente.

Posterior al diagnóstico se detectan también problemas específicos o secundarios:

- Interrupción en la Transmisión de los datos que puede ocasionar el apagado de los servidores.
- Medidas de cableado pueden abarcar disoluciones de cada uno de los datos, así los envíos y recepción de datos establecidos por los usuarios.
- Pérdida de tiempo en la carga de información al sistema y en la recuperación de información.

1.4.1. Formulación del problema

¿Cómo mejorar el acceso al servicio de Internet mediante la gestión remota de recursos en la Cooperativa de Ahorro y Crédito "Unión Santiago De Machaca"?

1.5. Objetivos

1.5.1. Objetivo general

- Diseñar un sistema de gestión remoto para optimizar el acceso al servicio de internet en la Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca".

1.5.2. Objetivos específicos

- Diagnosticar la situación actual respecto al servicio de internet de la Cooperativa de Ahorro y Crédito "Unión Santiago De Machaca".

- Realizar un análisis de riesgo en tecnología para su adecuación en el sector financiero en la Cooperativa de Ahorro y Crédito “Unión Santiago De Machaca”.
- Clasificar las mejores soluciones para fortalecer la comunicación remota entre cada uno de las agencias y oficina central de la Cooperativa.
- Diseñar un diagrama global de todas las redes WAN, LAN y MAN para el Sistema de Gestión Remota.
- Configurar adecuadamente todas las herramientas necesarias para que la Cooperativa tenga políticas de protección perimetral de red.
- Configurar los accesos remotos entre la agencia y la principal de la Cooperativa a fin de que puedan aprovechar el ancho de banda y la seguridad en el flujo de la información.

1.6. Justificación

La importancia del presente trabajo de investigación; radica en el hecho de determinar la factibilidad en los dispositivos de un sistema de gestión de Redes y Telecomunicaciones. Estos equipos traen simplicidad a las redes con puntos de acceso de red inalámbrica, switches y dispositivos de seguridad gestionados de forma centralizada, un sistema de gestión remoto ofrece a los administradores de red visibilidad y control, sin el costo y la complejidad de las arquitecturas de redes tradicionales.

Además la administración de los puntos de acceso a través de un sistema de gestión remoto permite que las aplicaciones y los servicios sean administrados de una manera más minuciosa, siendo capaz de denegar servicios por cada módulo de cada aplicación, administrar el ancho de banda por usuario y por aplicación y el filtrado de todo tipo de contenido en todo momento, denegar el acceso a los usuarios aunque hayan estado registrados antes, y adicional a estas características, el tipo de tecnología permite detectar problemas de conexión, desde un error en la autenticación hasta saber si el cable de conexión a internet está dañado.

De igual forma, este tipo de redes cuenta con un sistema de filtrado de contenidos para distribuir y priorizar el uso del servicio para los funcionarios; permitirá que cualquier

miembro de la cooperativa de ahorro y crédito “Unión Santiago De Machaca” pueda navegar por Internet a velocidad de transmisión desde 54 Mbps hasta un máximo de 600Mbps, además de trabajar en dos bandas de frecuencias: 2,4GHz y 5.8GHz.

1.7. Alcances y limitaciones

1.7.1. Alcances

1.7.1.1. Alcance temático

La presente investigación esta aplicada a la Ingeniería Electrónica, de acuerdo al análisis para la implementación de un sistema de gestión remoto que mejorará el servicio de internet en base a los recursos de comunicación que cuenta la cooperativa de ahorro y crédito “Unión Santiago de Machaca”.

1.7.1.2. Alcance espacial

La presente propuesta de investigación se llevará a cabo en la cooperativa de ahorro y crédito “Unión Santiago de Machaca” ubicada en la ciudad de La Paz y sucursales de la misma.

1.7.1.3. Alcance temporal

En cuanto a la delimitación temporal se debe detallar que los datos obtenidos son a partir del 2017 hasta la fecha del trabajo practico de la presente investigación es decir 2019.

1.7.2. Limites

Dentro de los límites se tiene los diseños de red y estándares de redes inalámbricas que proporcionaran un adecuado diseño de red inalámbrica y utilización de la mejor tecnología y equipos, basados en estándares internacionales que permiten un mejor funcionamiento en la red de telecomunicaciones de la mencionada entidad pública.

1.8. Metodología

1.8.1. Métodos de investigación

Los métodos pueden ser conjuntos de tal manera que las aproximaciones cuantitativa y cualitativa conserven sus estructuras y procedimientos originales. Alternativamente, estos métodos pueden ser adaptados, alterados o sintetizados para efectuar la investigación y lidiar con los costos de estudio [RODRÍGUEZ, F. 1994].

Investigación no experimental:

Es aquella que se realiza sin manipular deliberadamente variables. Se basa fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para analizarlos con posterioridad.

De tal manera el presente proyecto trabajara desde ambos métodos análisis del problema y medición del alcance respecto a la propuesta, sin ejecución plena del sistema.

1.8.2. Enfoque de Investigación

Dentro los lineamientos principales del enfoque investigativo ira dirigido baja las normativas APA.

1.8.3. Unidad de análisis

- Acceso de las redes y encriptación de la información
- Conexiones de Internet

1.8.4. Selección de la muestra

La Oficina Central de la Cooperativa de Ahorro y Crédito “Unión Santiago de Machaca” tiene una pequeña red de área local que conecta todas las maquinas al sistema contable, impresora en red y Servidores. Además, la Cooperativa cuenta con un punto de atención ubicado en la ciudad de La Paz, la misma que cuenta con el servicio de Internet, una red LAN, la oficina envía los respaldos diariamente de actualización de sus sistemas a la oficina central.

Dentro de la estructura de la organización se cuenta que todos los equipos se encuentran conectados a la red de área local respectiva. Sin embargo, al no contar con herramientas de control, todos se conectan a todo.

1.8.5. Técnica de recolección de datos primarios y secundarios

1.8.5.1. Fuentes primarias

Tomando como fuentes primarias: la información obtenida de como los cajeros y funcionarios de la oficina sucursal es que pudimos realizar un estudio acertado de los requerimientos y necesidades a nivel de infraestructura y validar el acceso remoto desde la sucursal a la central de los usuarios y servicios que ofrece la Cooperativa.

1.8.5.2. Fuentes secundarias

Las fuentes secundarías, estarán constituidas por la información bibliográfica y la teoría referente al tema. [RODRÍGUEZ, F. 1994].

1.8.6. Técnicas de recolección de datos primarios

1.8.6.1. Análisis documental

El análisis documental es el registro de información obtenida, en fichas bibliográficas, que son papeles o cartulinas de tamaño rectangular donde se anotan datos breves y de gran interés sobre un tema y que se pueden ordenar o archivar con otras similares con el fin de tenerlas disponibles para consultarlas. Aunque hoy en día este tipo de archivos también se puede llevar de una manera informática. [CHUMACERO, J. 2004].

Para la utilización de esta técnica se procederá a la identificación de fuentes de información documental de orden bibliográfico, poniendo mayor relevancia a la documentación institucional de la Cooperativa de Ahorro y Crédito “Unión Santiago de Machaca” clasificando la información dependiendo de su importancia en fuentes Primarias y Secundarias, dependiendo de su dosificación e interpretación a la que se pretenda llegar.

CAPITULO II
2. MARCO TEÓRICO

2.1. Redes inalámbricas

Las redes inalámbricas (en inglés wireless network) son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas. En un principio las redes inalámbricas se desarrollaron en base a radioenlaces, y posteriormente desde el año 1996 aparecieron las primeras redes propietarias portátiles, estando el desarrollo actual normado para que la tecnología pueda ser utilizada independientemente de cuál es el fabricante de los equipos. Las normas han surgido en base a estándares regulados por la IEEE (Institute of Electrical and Electronics Engineers), una entidad sin fines de lucro, que reúne a más de 360.000 miembros de 175 países (base de datos de IEEE). Las empresas telefónicas celulares por su parte también han ingresado al mercado de redes de datos, pero su enfoque hasta ahora ha sido como adicional a su servicio principal que es la comunicación de voz. Es probable que las redes de telefonía celular se dediquen cada vez más a los datos mejorando el ancho de banda disponible para ello, para telefonía existe una dificultad el ancho de banda, es muy costoso; En redes de computadoras inalámbricas se usan las frecuencias libres estandarizadas conocidas como bandas ISM 2.4 GHZ. Ha habido varios intentos de desarrollo de redes inalámbricas con diferentes tecnologías, como ser la tecnología de Infrarrojo, Bluetooth.

- Tecnología infrarroja, que se ha utilizado exitosamente para comunicación de dispositivos entre sí, como calculadoras portátiles o bien la comunicación de una computadora (PC) con otros equipos tal como una impresora, una agenda electrónica (Palm o PDA), y no tanto para acceder a redes. Su alcance es limitado debido a que las ondas infrarrojas no pueden atravesar objetos opacos.
- Tecnología Bluetooth, creada para comunicar una PC con un teléfono celular o bien con micrófonos, mouse u otros, pero es también de corto alcance, es de bajo consumo de energía, por tal razón es muy requerida.

Figura 2.1. Redes Inalámbricas

Fuente: Fernández, P. 2008

Si bien, Wi-Fi se creó para acceder a redes LAN en forma inalámbrica, hoy se utiliza mayormente para acceder a internet. Recientemente han surgido los llamados "Hot-Spots"

- Un hotspot («punto caliente») es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet.

Usualmente, los hotspots están en zonas de alta demanda de tráfico, y que por tanto el dimensionamiento de su cobertura está condicionado a cubrir esta demanda por parte de un punto de acceso o varios, y de este modo proporcionar servicios de red a través de un proveedor de servicios de Internet inalámbrico (WISP o redes públicas inalámbricas, establecidas en determinados lugares para conectarse a internet, basadas en Wi-Fi, que corresponde al estándar IEEE 802.11.

Dichos lugares son en general zonas de uso público como aeropuertos, restaurantes y cafeterías, universidades, etc., en donde es posible acceder a internet en forma inalámbrica. Hay lugares en que el acceso es compartido gratuitamente, y sólo es necesario acceder a la red inalámbrica para tener acceso a Internet (Free Hot-Spot).

También hay espacios en que se debe realizar un pago por el acceso. Pero indudablemente una importante aplicación del denominado Wi-Fi es en el hogar, en las empresas, centros de esparcimiento, donde puede establecerse fácilmente una red inalámbrica de bajo costo;

mediante la cual se puede compartir la impresora o el acceso a internet desde cualquier ubicación de su casa o departamento y sin tener que romper murallas o desplegar cables. Esta tecnología permite conectarse a una distancia de 100 metros o más. Ya que todas estas tecnologías están disponibles para el usuario final, debemos advertir que para un mundo convulsionado como el actual, se deben tener precauciones de seguridad para prevenirnos de un uso malintencionado. Así como una persona tiene acceso a una red en particular en forma inalámbrica, cualquiera que esté en las cercanías también lo tiene.

Si no se implementan medidas de seguridad adecuadas, al desplegar redes inalámbricas como en cualquier red, es factible que se vulnere la privacidad de la información. De nada sirve que una empresa tenga cortafuegos y adopte medidas de seguridad extremas para su red cableada, si alguno de sus empleados instala un acceso inalámbrico en su puesto de trabajo sin protección adecuada. Al instalar una red inalámbrica, preocúpese de activar las protecciones de acceso que la tecnología también le ofrece. En la actualidad existen muchas maneras de implementar redes inalámbricas y distintos estándares existen organizaciones internacionales que ya formalizaron estándares para el uso de redes inalámbricas la IEEE (INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS), UIT (UNIÓN INTERNACIONAL DE TELECOMUNICACIONES) y la IETF (INTERNET ENGINEERING TASK FORCE) y que dicta normas llamadas RFC que son las normas que rigen el tráfico de internet (red de redes), por recomendación de la UIT en la actualidad para redes inalámbricas de corto alcance y de largo alcance todas están normalizadas.[1]

- RFC, es una sigla en inglés (Request For Comments) que significa solicitud de comentarios y consiste en un documento que puede ser escrito por cualquier persona y que contiene una propuesta para una nueva tecnología, información acerca del uso de tecnologías y/o recursos existentes, propuestas para mejoras de tecnologías, proyectos experimentales y demás. Las RFC conforman básicamente la documentación de protocolos y tecnologías de Internet, siendo incluso muchas de ellas estándares. La metodología que se utiliza con las RFC es asignarle a cada una un número único que la identifique y que es el consecutivo de la última RFC publicada. Una RFC ya publicada jamás puede modificarse, no existen varias

[1] Profesor Carlos Alcocer. 2008 apuntes del curso de telemática (PUCP). Lima: Pontificia Universidad Católica del Perú.

versiones de una RFC. Lo que se hace, en cambio, es escribir una nueva RFC que deje obsoleta o complemente una RFC anterior.

- IUT, La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

2.2. Ventajas y desventajas de las redes

2.2.1. Ventajas

Ventajas que ofrece una red inalámbrica son las siguientes:

- Estar basada en estándares y contar con certificación Wi-Fi.
- Instalación simple.
- Robusta y confiable.
- Escalabilidad.
- Facilidad de uso.
- Servidor Web para una administración más fácil.
- Seguridad.
- Una aplicación que detecte localidades.
- Costo de propiedad reducido.
- Fácil configuración para el usuario.

Sobre estas ventajas se puede comentar lo siguiente:

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

que su red inalámbrica trabaje sin interrupciones con su sistema existente de LAN tradicional.

- **Instalación simple.** La solución inalámbrica debe ser del tipo plug and play; tomando solamente unos minutos para su instalación. Al conectarla, los usuarios empezarán a gozar de inmediato de los servicios en red. Para obtener una instalación aún más fácil, su solución deberá soportar el protocolo denominado Dynamic Host Configuration Protocol (DHCP), el cual asignará automáticamente direcciones IP a los clientes inalámbricos. En lugar de instalar un servidor DHCP en algún aparato independiente para obtener esta capacidad de ahorro de tiempo, los usuarios deben seleccionar hubs inalámbricos que ofrezcan servidores DHCP incorporados.
- **Robusta y confiable.** Considera soluciones inalámbricas robustas que tienen alcances de por lo menos 100 metros. Estos sistemas les ofrecerán a los empleados de una compañía una considerable movilidad dentro sus instalaciones. Un usuario puede optar por un sistema superior que automáticamente detecte el ambiente, para seleccionar la mejor señal de frecuencia de radio disponible y obtener máximos niveles de comunicaciones entre el punto de acceso y las PC cards. Para garantizar una conectividad a las velocidades más rápidas posibles incluyendo largo alcance o ambientes ruidosos, el usuario debe asegurarse que su nuevo sistema pueda hacer cambios dinámicos de velocidades, basándose en las diferentes intensidades de señal y distancias del punto de acceso. Además, el usuario debe seleccionar PC cards inalámbricas para computadoras portátiles que ofrezcan antenas retractables para prevenir rupturas durante la movilización de los aparatos.

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

- **Facilidad de uso**. Si un usuario planea conectar múltiples puntos de acceso inalámbricos a una red existente de cables, debe considerar una solución que ofrezca

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

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

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

- **Una aplicación que detecte localidades.** Una solución de redes inalámbricas deberá incluir una aplicación para la detección de instalaciones. Esta aplicación podrá ayudar al usuario a determinar la posición óptima de los hubs inalámbricos y el número de hubs que necesita para soportar a sus usuarios. Además, ayudará a implementar una solución inalámbrica en forma efectiva y eficiente.
- **Costo de propiedad reducido**. Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida pueden ser significativamente inferiores, ya que en ambientes dinámicos se requieren acciones y movimientos

frecuentes, lo cual abarata los costos debido a que no hay instalaciones físicas [Castro, Edgar. 2003].

- **Facilidad de configuración para el usuario.** La persona que se va a conectar a la red sólo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red está abierta no es necesario configurar nada, pues la tarjeta detecta la red automáticamente [Del Razo, Minerva, 2004].

2.2.2. Desventajas

Los inconvenientes o desventajas que tienen las redes de este tipo se derivan fundamentalmente de encontrarnos en un periodo transitorio de introducción, donde faltan estándares que permitan trasmisiones más rápidas, por otro lado hay dudas de que algunos sistemas pueden llegar a afectar a la salud de los usuarios, también no está clara la obtención de licencias para las que utilizan el espectro radioeléctrico y son muy pocas las que presentan compatibilidad con los estándares de las redes fijas, sin embargo, se ha estado trabajando en ello, logrando hasta el momento un gran avance que ha permitido la implementación cada vez más de este tipo de comunicación.

Algunas otras desventajas que se derivan por la implementación de redes inalámbricas son las que se mencionan a continuación.

- **Interferencias.** Se pueden ocasionar por teléfonos inalámbricos que operen a la misma frecuencia, también puede ser por redes inalámbricas cercanas o incluso por otros equipos conectados inalámbricamente a la misma red.
- **Velocidad.** Las redes cableadas alcanzan la velocidad de 100 Mbps, mientras que las redes inalámbricas alcanzan cuando mucho 54 Mbps.
- **Seguridad.** En una red cableada es necesario tener acceso al medio que transmite la información mientras que en la red inalámbrica el medio de transmisión es el aire [Del Razo, 2004].

2.3. Clasificación de redes inalámbricas

Las redes inalámbricas se pueden clasificar teniendo en cuenta como parámetro principal su rango de cobertura, en Wireless Personal Area Network, Wireless Local Area Network,

Wireless Metropolitan Area Network,Wireless Wide Area Network, según su topología Existen 2 las básicas que pueden implementarse en el protocolo 802.11b: Redes sin infraestructura o Ad-hoc (IBSS) y Redes con Infraestructura (BSS).

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

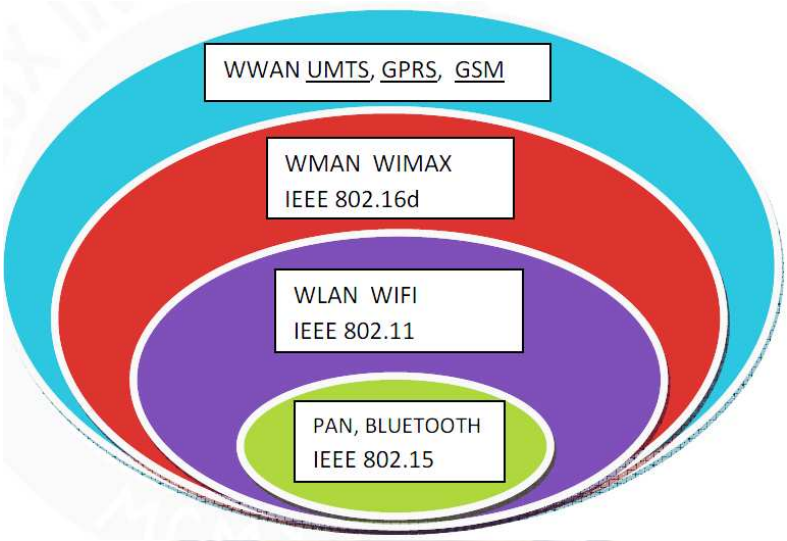


Figura 2.2. Clasificación de las tecnologías inalámbricas

Fuente: Fernández, P. 2008

Figura 2.3. Aplicaciones de las Redes inalámbricas

Fuente: Fernández, P. 2008

2.3.1. Redes inalámbricas de área personal (WPAN)

Incluye redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Este tipo de red se usa generalmente para conectar dispositivos periféricos (por ejemplo, impresoras, teléfonos móviles y electrodomésticos) o un asistente personal digital (PDA) a un ordenador sin conexión por cables. También se pueden conectar de forma inalámbrica dos ordenadores cercanos [Fernández, P. 2008].

Se usan varios tipos de tecnología para las WPAN:

- La tecnología principal WPAN es Bluetooth, lanzado por Ericsson en 1994.
- Ofrece una velocidad máxima de 1 Mbps con un alcance máximo de unos treinta metros.
- La tecnología Bluetooth, también conocida como IEEE 802.15, tiene la ventaja de tener un bajo consumo de energía, algo que resulta ideal para usarla en periféricos de pequeño tamaño.[2]

[2] Profesor Fernández Pilco. 2008 apuntes del curso de Sistemas de Comunicación (PUCP). Lima: Pontificia Universidad Católica del Perú.

Figura 2.4. Red WPAN

Fuente: Fernández, P. 2008

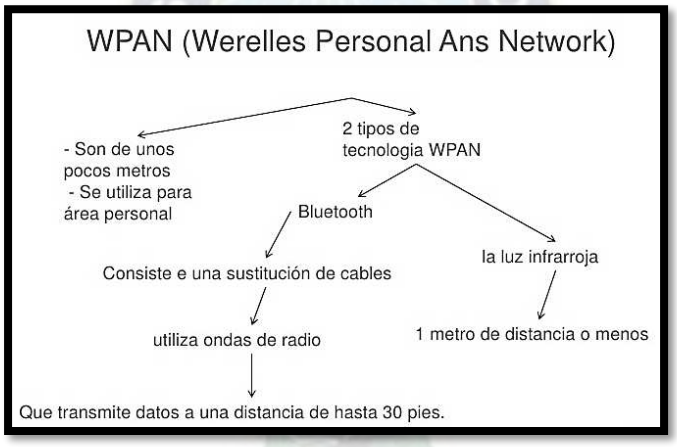


Figura 2.5. Características WPAN

Fuente: Fernández, P. 2008

2.3.2. Redes inalámbricas de área local (WLAN)

Del inglés Wireless Local Area Network es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en

tiempo real la norma más usada en este tipo de redes es la 802.11g, promovida por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), y que la asociación WiFi está ayudando a consolidar. En segundo lugar, aunque menos utilizado, se sitúa HomeRF.

Una red de área local o WLAN (Wireless LAN) utiliza ondas electromagnéticas (radio e infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, ..).[3]

Figura 2.6. Red WLAN

Fuente: Fernández, P. 2008

Las redes locales inalámbricas más que una sustitución de las LANs convencionales son una extensión de las mismas, ya que permite el intercambio de información entre los distintos medios en una forma transparente al usuario.

En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas. Enlazando los diferentes equipos o terminales móviles asociados a la red.

Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado.

[3] Profesor Carlos Alcocer. 2008 apuntes del curso de telemática (PUCP). Lima: Pontificia Universidad Católica del Perú.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps, 100 Mbps. y se espera que alcancen velocidades de hasta 1 Gbps de manera regular.

Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de hasta 300 Mbps (802.11 n).[4] Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.[5]

2.3.3. Redes inalámbricas de área metropolitana (WMAN)

También se conocen como bucle local inalámbrico (WLL, Wireless Local Loop). Las WMAN se basan en el estándar IEEE 802.16.d Los bucles locales inalámbricos ofrecen una alternativa de comunicación entre varios edificios de oficinas de una ciudad o en un campus universitario, algo muy útil para compañías. La mejor red inalámbrica de área metropolitana es WiMAX, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros.[6]

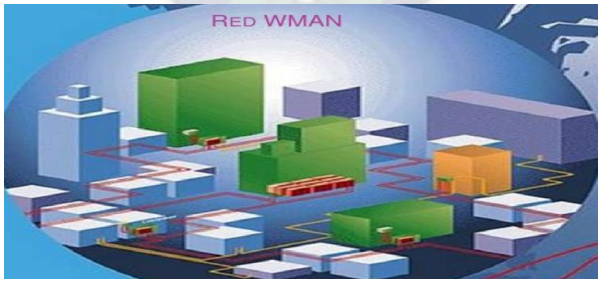


Figura 2.7. Red WMAN

Fuente: Fernández, P. 2008

[4] Cisco Networking Academy 2008 Wireless LAN Fundamentos_v1.02. San Jose, CA: Cisco Press.
[5] Cisco Networking Academy 2010 CCNA 3 Exploration 4.0, LAN Switching and Wireless. San Jose, CA: Cisco Systems.
[6] Profesor Fernández Pilco. 2008 apuntes del curso de Sistemas de Comunicación (PUCP). Lima: Pontificia Universidad Católica del Perú.

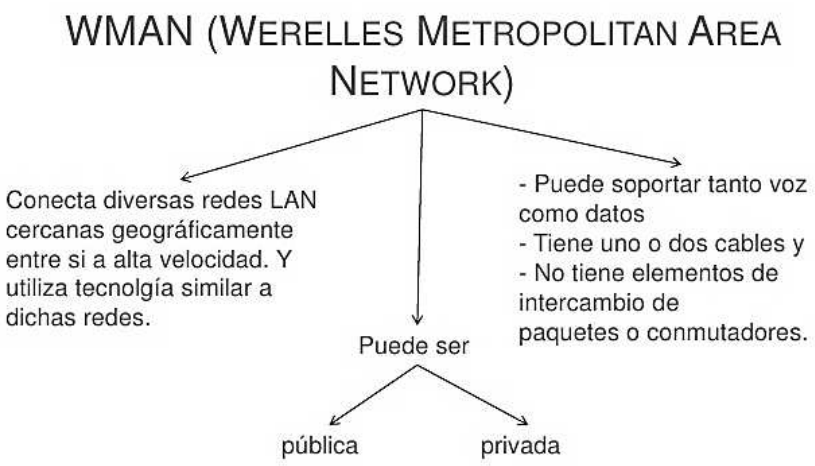


Figura 2.8. Características WMAN

Fuente: Fernández, P. 2008

2.3.4. Redes inalámbricas de área extensa (WWAN)

Tienen el alcance más amplio de todas las redes inalámbricas. Por esta razón, todos los teléfonos móviles están conectados a una red inalámbrica de área extensa. Las tecnologías principales son:

- GSM (Global System for Mobile Communication)
- GPRS (General Packet Radio Service)
- UMTS (Universal Mobile Telecommunication System).

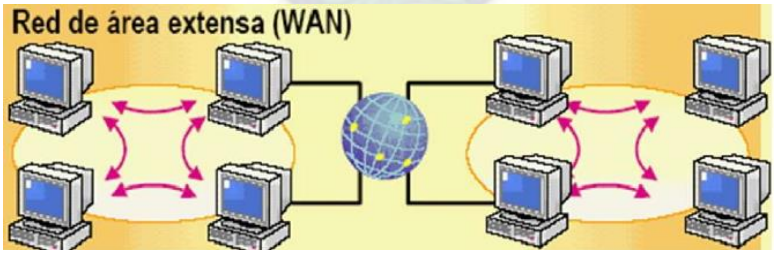


Figura 2.9. Red WWAN

Fuente: Fernández, P. 2008

2.4. Clasificación según topología de redes inalámbricas

Existen 2 topologías básicas que pueden implementarse en el protocolo 802.11b: Redes sin infraestructura o Ad-hoc (IBSS) y Redes con Infraestructura (BSS).

2.4.1. Redes ad-hoc sin infraestructura (IBSS, Independent Basic Service Set)

El estándar IEEE 802.11 describe los protocolos y las técnicas de transmisión correspondientes a los dos modos principales de construir y utilizar una LAN inalámbrica RF. Una parte del estándar contempla la comunicación en redes "ad-hoc" simples. Estas redes están compuestas por varias estaciones de trabajo con un alcance de transmisión limitado interconectadas entre sí. No obstante, estas topologías no necesitan ningún sistema de control ni de transmisión central. Una LAN inalámbrica se puede instalar, por ejemplo, en una sala de conferencias para conectar sistemas portátiles que se usarán en una reunión.

Ventajas:

- Comunicación punto a punto sin punto de acceso
- Instalación rápida y costes mínimos
- Configuración simple

Desventajas:

- Alcance limitado - Número de usuarios limitado
- No integración en estructuras LAN existentes

2.4.2. Redes con infraestructura (BSS, Basic Service Set)

La segunda aplicación en importancia de las que se describen en el estándar IEEE 802.11 utiliza "puntos de acceso". Los puntos de acceso son componentes de red que controlan y gestionan toda la comunicación que se produce dentro de una célula LAN inalámbrica, entre células LAN inalámbricas y, finalmente, entre células LAN inalámbricas y otras tecnologías LAN. Los puntos de acceso garantizan un empleo óptimo del tiempo de transmisión disponible en la red inalámbrica.

Ventajas:

- Las estaciones que no pueden "verse" entre sí, pero mantiene una comunicación más directa.
- Simple integración en estructuras de cable ya existentes

Desventajas:

- Coste más elevado del equipo
- Instalación y configuración más complejas

La instalación básica, compuesta por un solo punto de acceso y los sistemas inalámbricos conectados, se denomina "Basic Service Set" (Equipo Básico de Servicio, BSS). Los equipos que pertenecen al mismo BSS se identifican entre sí por medio de un identificador de equipo de servicio (SSID, "Service Set ID") o nombre de red.

2.5. Protocolo de enrutamiento

Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la selección de las mejores rutas del protocolo de enrutamiento. El propósito de los protocolos de enrutamiento dinámico son la selección de las mejores rutas de intercambio de información de enrutamiento. El propósito de un protocolo de enrutamiento incluye:

- Descubrimiento de redes remotas,
- Mantenimiento de información de enrutamiento actualizada,
- Selección de la mejor ruta hacia las redes de destino
- Capacidad de encontrar una mejor nueva ruta si la ruta actual deja de estar disponible.

2.6. Estandarización y normalización de la tecnología WLAN

La arquitectura de las redes WLAN cumplen con los estándares genéricos aplicables al mundo de las LAN cableadas (IEEE 802.3 o estándares equivalentes) pero necesitan una normativa específica adicional que defina el uso y acceso de los recursos radioeléctricos. Estas normativas definen de forma detallada los protocolos de la capa física (PHY), la capa de Control de Acceso al Medio (MAC) y Control del Enlace de Datos.

El primer estándar de WLAN lo generó el organismo IEEE en 1997 y se denomina IEEE 802.11. Desde entonces varios organismos internacionales han desarrollado una amplia actividad en la estandarización de normativa de WLAN y han generado un abanico de nuevos estándares. En USA el grueso de la actividad lo mantiene el organismo IEEE con los

estándares 802.11 y sus variantes (b, g, a, e, h, etc) y en Europa el organismo es el ETSI con sus actividades en HiperLAN-BRAN. [7]

El protocolo IEEE 802.11 es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles inferiores de la arquitectura OSI (capas físicas y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

En general, los protocolos de la rama 802.X definen la tecnología de redes de área local.[8] La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación, todas las cuales utilizan los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11 legacy".[7]

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

Tabla 2.1. Estándares de IEEE802.11**.**

Fuente: Ponce, E. 2008.

2.6.1. IEEE 802.11a

[7] (Modelo de Cobertura para Redes Inalámbricas de Interiores)

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

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

2.6.2. IEEE 802.11b

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

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

2.6.3. IEEE 802.11g

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

[9] Forouzan, Behrouz A. 2008 Transmisión De Datos Y Redes De Comunicaciones. España: McGraw-Hill.

[9] Sector de normalización de las telecomunicaciones de la UIT-T

Los equipos que trabajan bajo el estándar 802.11g. llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

2.7. Capas según la organización de estándares

2.7.1. Estándares

El significado primario original de estándar (del inglés standard) era bandera; color; pancarta; especialmente nacional u otra enseña. El significado primario moderno que le siguió fue "lo que es establecido por la autoridad, la costumbre o el consentimiento general". En este sentido se utiliza como sinónimo de norma. Existe una serie de instituciones, que a nivel internacional, se encargan de definir los estándares, y las corporaciones se adjuntan a ellas para certificar sus productos. Entre las instituciones de estandarización que podemos mencionar se encuentran listadas a continuación.

2.7.2. La ISO

Iso, La Organización Internacional para la Normalización o Estandarización, es una organización internacional no gubernamental, compuesta por representantes de los cuerpos de estandarización nacionales, que produce estándares mundiales industriales y comerciales. ISO coopera estrechamente con la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC), que es responsable de la estandarización de equipos eléctricos. Para realizar esta ingente labor ISO se organiza en cerca de 200 comités técnicos denominados TC (Technical Committee) que se numeran en orden ascendente según su fecha de creación. El que nos interesa a nosotros es el TC97 que trata de ordenadores y proceso de la información. Cada comité tiene subcomités (SCs) que a su vez se dividen en grupos de trabajo o WGs (Working Groups). El proceso de creación de un estándar ISO es como sigue. Uno de sus miembros (una organización nacional de estándares) propone la creación de un estándar internacional en un área concreta. Entonces ISO constituye un grupo de trabajo que

produce un primer documento denominado borrador del comité o CD (Committee Draft). El CD se distribuye a todos los miembros de ISO, que disponen de un plazo de seis meses para exponer críticas. El documento, modificado de acuerdo con las críticas recibidas, se somete entonces a votación y si se aprueba por mayoría se convierte en un estándar internacional borrador o DIS (Draft International Standard) que se difunde para recibir comentarios, se modifica y se vota nuevamente. En base a los resultados de esta votación se prepara, aprueba y publica el texto final del estándar internacional o IS (International Standard). En áreas muy polémicas un CD o un DIS han de superar varias versiones antes de conseguir un número de votos suficiente, y el proceso entero puede llevar años.[10]

2.7.3. La ITU-T ITU

La International Telecommunication Union o Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas Administraciones y Empresas Operadoras. Está compuesta por tres sectores:

- UIT-T: Sector de Normalización de las Telecomunicaciones (antes CCITT).
- UIT-R: Sector de Normalización de las Radiocomunicaciones (antes CCIR).
- UIT-D: Sector de Desarrollo de las Telecomunicaciones.

La sede la UIT se encuentra en Ginebra (Suiza). De los tres sectores sólo nos interesa el conocido como ITU-T que se dedica a la estandarización de las telecomunicaciones.

Los miembros de la ITU-T son de cinco clases:

- Representantes de los países.
- Operadores privados reconocidos (por Ej. British Telecom, Global One, AT&T).
- Organizaciones regionales de telecomunicaciones (p. Ej. el ETSI).
- Empresas que comercializan productos relativos a telecomunicaciones y organizaciones científicas.
- Otras organizaciones interesadas (bancos, líneas aéreas, etc.)

[10] Sector de normalización de las telecomunicaciones de la UIT-T

Entre los miembros hay unos 200 representantes de países, unos cien operadores privados y varios cientos de miembros de las otras clases.

La ITU-T para desarrollarse organiza en Grupos de Estudio, que pueden estar formados por hasta 400 personas. Los Grupos de Estudio se dividen en Equipos de Trabajo (Working Parties), que a su vez se dividen en Equipos de Expertos (Expert Teams). [11]

Las tareas de la ITU-T comprenden la realización de recomendaciones sobre interfaces de teléfono, telégrafo y comunicaciones de datos. A menudo estas recomendaciones se convierten en estándares reconocidos internacionalmente, por ejemplo, la norma ITU-T V.24 (también conocida como EIA RS-232) especifica la posición y el significado de las señales en el conocido conector de 25 contactos utilizado en muchas comunicaciones asíncronas.

En general, la normativa generada por la UIT está contenida en un amplio conjunto de documentos denominados Recomendaciones, agrupados por Series. Cada serie está compuesta por las Recomendaciones correspondientes a un mismo tema, por ejemplo, Tarificación, Mantenimiento, etc. Aunque en las Recomendaciones nunca se "ordena", solo se "recomienda", su contenido, a nivel de relaciones internacionales, es considerado como mandatorio por las Administraciones y Empresas Operadoras.

2.7.4. Recomendación UIT-T X.1641

La Recomendación UIT-T X.1641 proporciona directrices genéricas para la seguridad de los datos de clientes de servicios en la nube (CSC) en la computación en la nube. Se analiza el ciclo de vida de la seguridad de los datos del CSC y se proponen requisitos de seguridad para cada fase del ciclo de vida de los datos. La Recomendación también proporciona directrices acerca del momento en que debe utilizarse cada uno de los controles para lograr una práctica óptima en materia de seguridad.[12]

[11] Sector de normalización de las telecomunicaciones de la UIT-T

[12] Sector de normalización de las telecomunicaciones de la UIT-T

2.7.5. Capa física de IEEE 802.11

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos.

IEEE 802.11 define tres posibles opciones para la elección de la capa física:

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

En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación, por un lado, y prestaciones y fiabilidad, por otro. No obstante, es previsible que, al cabo de un cierto tiempo, alguna de las opciones acabe obteniendo una clara preponderancia en el mercado. Entretanto, los usuarios se verán obligados a examinar de forma pormenorizada la capa física de cada producto hasta que sea el mercado el que actúe como árbitro final.[13]

2.7.6. Capa de enlace (MAC) de IEEE 802.11

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

- Ad-hoc: redes peer-to-peer.

  Varios equipos forman una red de intercambio de información sin necesidad de elementos auxiliares. Este tipo de redes se utilizan en grupos de trabajo, reuniones, conferencias.
- Basadas en infraestructura:

[13] Forouzan, Behrouz A. 2008 Transmisión De Datos Y Redes De Comunicaciones. España: McGraw-Hill.

La red inalámbrica se crea como una extensión a la red existente basada en cable. Los elementos inalámbricos se conectan a la red cableada por medio de un punto de acceso o un PC Bridge, siendo estos los que controlan el tráfico entre las estaciones inalámbricas y las transmisiones entre la red inalámbrica y la red cableada.

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

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

La capa de enlace de datos del estándar 802.11 se compone de dos subcapas: la capa de control de enlace lógico (o LLC) y la capa de control de acceso al medio (o MAC) en la siguiente figura se muestra las subcapas de la capa de enlace de datos para el estándar IEEE 802.11.

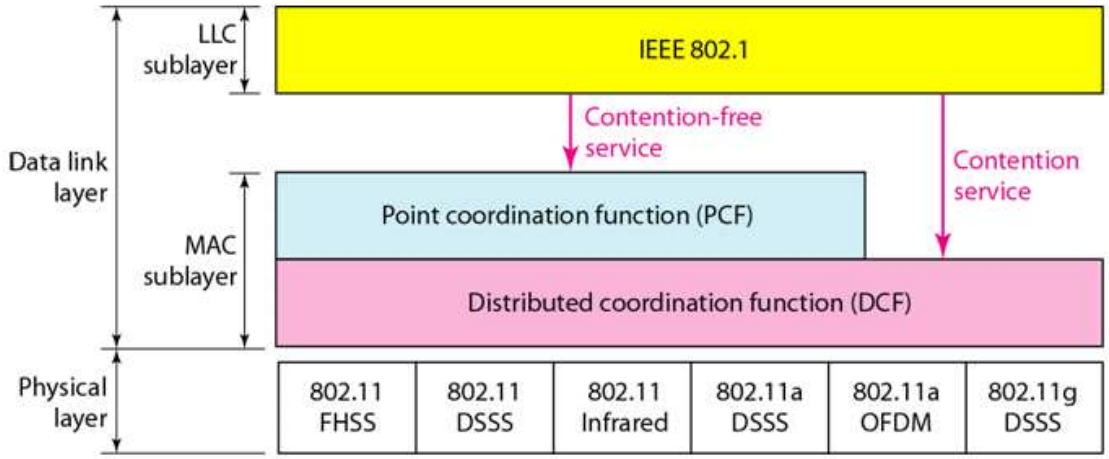


Figura 2.10. Muestra de las subcapas de la capa de enlace de datos

Fuente: Forouzan, A. 2008

2.8. Elementos de enrutamiento

Descubrir puntos de acceso: Descubrir nuevos puntos de acceso en una topología que puede cambiar permanentemente y establecer recorridos dinámicos en base a cada descubrimiento.

Descubrimiento de frontera: Encontrar los limites o bordes de una red, generalmente los sitios donde un punto de acceso o ruteador (Router) se conecta a la red cableada.

Cálculo de rutas: Descubrir el mejor camino basado en diferentes métricas y opiniones de enrutamiento como calidad de la conexión, número de saltos, o ancho de banda del medio.

Manejo de la red troncal: Se encarga de administrar conexiones a redes externas, como por ejemplo enlaces a Internet o acceder a una red de servidores local.

2.9. Sistema de seguridad en las redes

Los usuarios de servicios de telecomunicaciones demandan, cada día más beneficios y flexibilidad. Por tal motivo, en los últimos cinco años ha existido un desarrollo acelerado de la tecnología inalámbrica, en el campo de las redes de área local. Así, nace la tecnología WiFi que define las normas de comunicación para la tecnología en cuestión; uno de los aspectos de mayor importancia que no fue atacado con el debido cuidado fue la seguridad en esta tecnología, que inicialmente incorporó protocolos existentes de seguridad de redes alambradas denominadas:

WEP (Wired Equivalent Privacy), y que, al sufrir anomalías en su implementación, por tratarse de un tipo de encriptación del tipo estático, se llegó a determinar que para cierta cantidad de información encriptada era posible derivar la llave de encriptación. En consecuencia, por esta falta de seguridad, se crearon comités encargados en desarrollar un nuevo estándar orientado a la seguridad de las redes WiFi (802.11i).

De esta manera, se definieron nuevos conceptos de seguridad para redes WiFi que prometen asegurar la confidencialidad de los datos.

Muchas empresas lideran en el desarrollo tecnológico que da empuje para la utilización de nuevas técnicas de privacidad y autentificación de los usuarios.

Hoy en día es fácil conseguir acceso a redes inalámbricas mal configuradas, y nada garantizadas, aunque conviene recordar que una red inalámbrica correctamente administrada no es más que uno de los muchos puntos de seguridad que se deben mantener adecuadamente en cualquier institución.

Es recomendable la aplicación UIT-T X.1641, donde se proporcionan directrices para la seguridad de los datos de clientes de servicios en la nube (CSC) en la computación en la nube, en los casos en que el proveedor de servicios en la nube (CSP) es responsable de velar para que el tratamiento de datos se realice con la seguridad adecuada. No siempre es el caso, pues para algunos servicios en la nube, la seguridad de los datos es responsabilidad de los propios CSC.

En otros casos, puede existir una responsabilidad compartida. En algunos casos, por ejemplo, el CSP puede ser responsable de la limitación del acceso a los datos, mientras que el CSC es responsable de decidir qué usuarios del servicio en la nube (CSU) pueden acceder a ellos, y el comportamiento de cada guion o aplicación con los cuales el CSU procesa los datos.

En UIT-T X.1641 se identifican controles de seguridad para los datos de CSC que pueden utilizarse en diferentes fases del ciclo de vida completo de los datos. Estos controles de seguridad pueden diferir cuando cambia el nivel de seguridad de los datos del CSC.

2.9.1. Tecnologías de seguridad

Se ha presentado varias tecnologías de seguridad al mercado por diferentes empresas, con características particulares y específicos, podemos citar los más representativos:

- SSID (uso por default)
- MAC filtering
- VPN
- Captive Portal
- WEP (Wired equivalent privacy)
- WPA

2.9.1.1. SSID (Service Set IDentifier)

El SSID es el mecanismo para identificar redes inalámbricas, es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. A menudo

al SSID se le conoce como nombre de la red. Uno de los métodos más básicos de proteger una red inalámbrica es desactivar el broadcast del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo, no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación, además existe software con el cual es posible identificar el SSID.

2.9.1.2. Filtrado de MAC

El filtrado por direcciones MAC permite hacer una lista de equipos que tienen acceso al AP, o bien denegar ciertas direcciones MAC, la dirección MAC es única en cada tarjeta de red ya sea Ethernet, modem, WiFi sin embargo la principal desventaja radica en que la dirección MAC de la tarjeta puede ser intercambiable (clonada), lo que permite una obtención de una entrada válida en el AP.

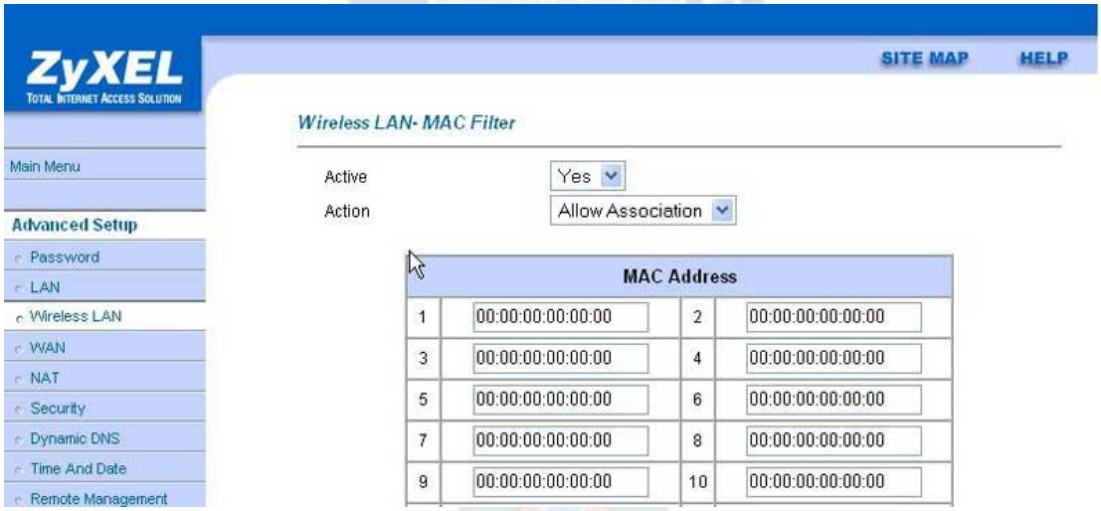


Figura 2.11. Filtrado por MAC

Fuente: CRESPO, A. s.f.

2.9.1.3. VPN (Red Privada Virtual)

Algunos AP permiten la configuración de VPN en el equipo, permitiendo que el usuario que se conecte tenga que autentificarse para poder salir del AP, además de ofrecer una encriptación de los datos en el tránsito de datos, haciendo más difícil el husmeo de tráfico por un tercero.

La desventaja que presenta es que no todos los APs tienen este servicio. La autenticación en la mayoría de los casos no es centralizada y cuando la es, se tiene acceso a una parte de la red que puede ser utilizada para otro tipo de ataques. Se requiere un software adicional, no todos los equipos lo soportan.

Existe una gran diversidad de VPN, como: IPSec, L2TP, PPTP, entre otras, y pueden ser atacados por DOS o ataques de diccionario.

2.9.1.4. Captive Portal

Estos permiten dar acceso a un portal donde se autentifica el cliente, dando el acceso a este equipo por un tiempo determinado o bajo ciertas condiciones. Este esquema de seguridad no es muy utilizado debido a que debe de estar en el AP para un mejor funcionamiento.

No todos los AP tienen soporte, los OpenAP o soluciones fuentes abiertas (opensource) ofrecen estas cualidades. Puede ser atacado por DOS o ataques de diccionario. El problema aún sigue ya que el control de acceso al AP no existe.

2.9.1.5. WEP (Wired Equivalent Privacy)

La característica principal de las redes inalámbricas es que utilizan el aire para transmitir la información. Esta particularidad le otorga enormes beneficios sobre las redes tradicionales por cables, pero también es el principal riesgo de seguridad que presenta: si la información se transmite por el aire, cualquier persona, con el receptor adecuado, puede acceder a la información.

Desde las primeras fases del desarrollo del protocolo 802.11 por parte del IEEE, se tuvo en cuenta este problema, y en el estándar se incluyó un protocolo de seguridad de uso opcional, el WEP (Wired Equivalent Privacy). Como su nombre indica, se pretendía que otorgase a las redes inalámbricas una seguridad equiparable a las redes por cable, pero esto no fue así.

Este protocolo se basa en el algoritmo de encriptación simétrico RC4 de RSA Security, con claves secretas compartidas de 40 y 104 bits y un vector de inicialización de 24 bits, que deben ser introducidos en todos los dispositivos que participan en una misma red inalámbrica.

Diversos estudios declararon que el protocolo WEP presenta graves problemas de seguridad, siendo el más importante de ellos el ataque que consiste en el análisis de paquetes de información encriptados con el mismo vector de inicialización y la misma clave. Esta coincidencia ocurrirá tarde o temprano si no se renueva la clave de encriptación debido a lo reducido de la longitud del vector de inicialización (24 bits). Esto se puede evitar cambiando manualmente la clave WEP de la red inalámbrica.

Sin embargo, esta tarea consistiría en modificar la configuración de todos los equipos de una red, lo que puede convertirse en un trabajo bastante pesado.

Se encuentran disponibles diversos programas de libre distribución que realizan este ataque, con lo que basta con recoger cierta cantidad de tráfico de la red para obtener, gracias a estos programas, la clave WEP de una red inalámbrica.

La solución a este problema se encuentra en el estándar 802.11i, en fase borrador; para no esperar a la publicación oficial del mismo, la WECA lanzó el protocolo WPA como sustituto de las deficiencias del protocolo WEP.

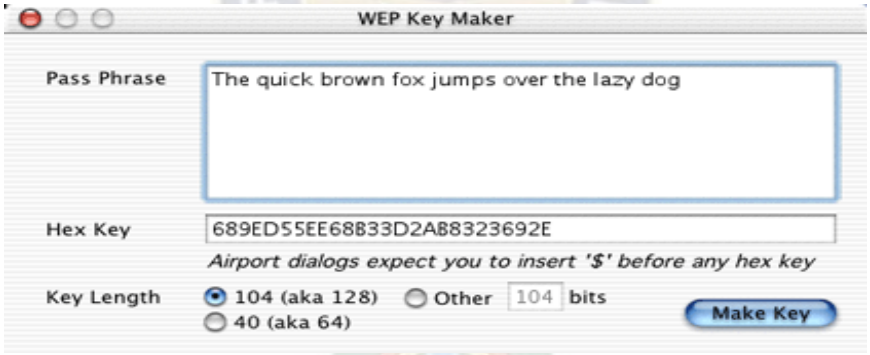


Figura 2.12. Protocolo de seguridad WEP

Fuente: ATPM. Wireless Network Encription. 2012

2.9.1.6. WPA (Wi-Fi Protected Access)

En la actualidad, los nuevos mecanismos para la encriptación de redes WiFi apuntan a la utilización de una variante del protocolo WEP denominado WEP Enhancement, que incorpora la utilización de un protocolo de integridad de llave temporal (Temporal Key Integrity Protocol, TKIP) el cual evita la derivación de la llave de encriptación del protocolo WEP. El protocolo TKIP es parte del nuevo estándar 802.11i.

La WECA (*Wireless Ethernet Compatibility Alliance)* desarrolló el protocolo Wi-Fi Protected Access con los objetivos de encontrar un sustituto del protocolo WEP ante la revelación de su debilidad ante ataques pasivos y por la conveniencia de autentificar a los usuarios en lugar de los dispositivos, tal como hace el protocolo WEP, hasta la aparición definitiva del protocolo 802.11i.

La WECA declara que los dispositivos que implementan WPA serán compatibles con el futuro 802.11i, con el fin de evitar el temor de los usuarios de tener que renovar su equipamiento para adaptar el nuevo estándar. WPA es una parte del borrador del 802.11i, tomando la autentificación mediante el protocolo 802.1x y la encriptación TKIP. Otros avances del 802.11i, como la asociación segura, no son posibles mediante el protocolo WPA.

El protocolo de encriptación TKIP, Temporal Key Integrity Protocol, es una modificación del WEP, del que se duplica la longitud del vector de inicialización (de 24 a 48 bits) para evitar la repetición de un mismo valor, y un método de renovación automática de la clave de encriptación entre los dispositivos inalámbricos.

Además del protocolo TKIP, se desarrolló, en el estándar 802.11i un sistema de control de la integridad de los mensajes denominado MIC (Messages Integrity Control) que permite prevenir ataques que interceptan los datos y los retransmiten al receptor (Bit-Flip attack). El sistema MIC es posible de implementarse en ambos sentidos de la comunicación.

Hoy en día, uno de los mecanismos más robustos disponibles para la autentificación es el protocolo EAP (Extensible Authentication Protocol), que permite habilitar en forma individual por usuario, por llave para cada sesión (EAPTLS).

Finalmente, a diferencia del protocolo WEP que utiliza el algoritmo de encriptación RC4, el protocolo WEP Enhancement ha adoptado la utilización del algoritmo de encriptación AES (Advanced Encryption Standard).

El conjunto de estas nuevas formas de autentificar a los usuarios de las redes WiFi se denomina WPA (WiFi Protected Acces).

2.9.1.7. WPA y servidores RADIUS.

Para obtener las mayores prestaciones del protocolo WPA, se requiere el uso de un servidor de autentificación externo como el RADIUS. Estas dos herramientas juntas, proporcionan una administración y un control de acceso centralizado de toda la red inalámbrica. Con esto, la necesidad de soluciones adicionales como VPN puede ser eliminada, al menos, en lo referente al enlace inalámbrico. Un cliente inalámbrico debe ser autentificado antes de tener acceso a los recursos de la red.

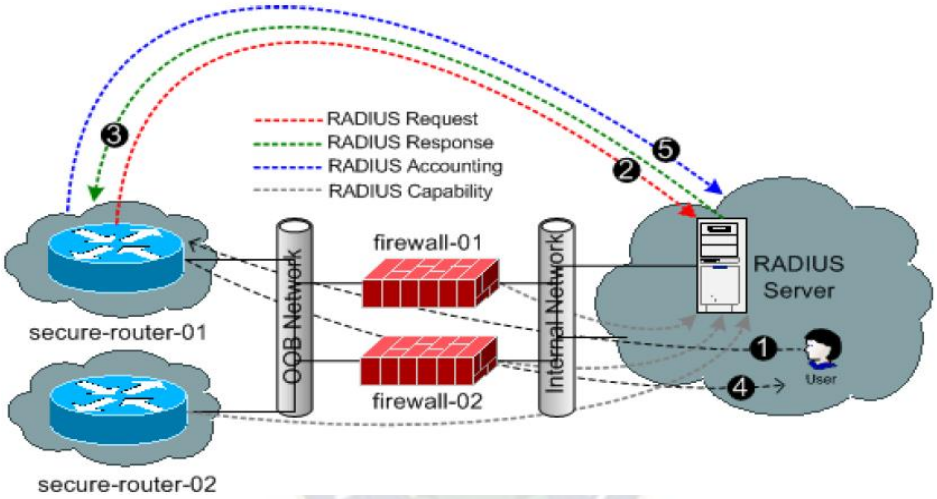


Figura 2.13. Esquema de servidor RADIUS

Fuente: Ponce, E. 2008

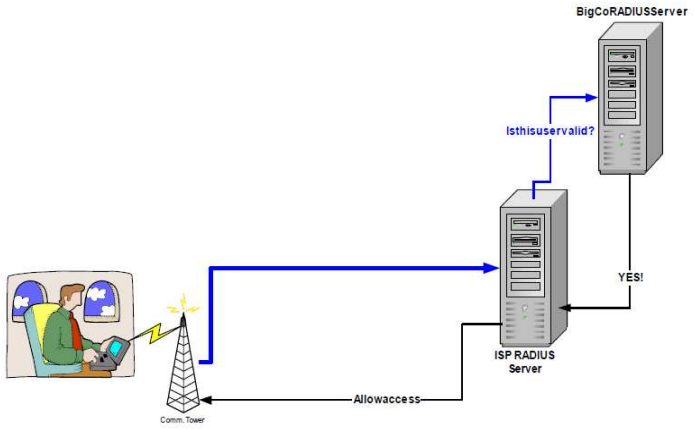


Figura 2.14. Proceso Autenticación Radius

Fuente: Microsoft Corporation, 2001

Sin embargo, en redes pequeñas o domésticas no se dispone de un servicio como el RADIUS mostrado en la Figura 2.14, por lo que el protocolo WPA permite operar en un modo más sencillo llamado PSK (PreShared Key), muy parecido al protocolo WEP, en el que se debe introducir una misma clave en todos los dispositivos de la red inalámbrica. Esta clave se emplea para autentificar al equipo en el momento del acceso a la red posteriormente, entra en funcionamiento el protocolo TKIP.

El estándar **802.11i ratificado** en junio del 2004, resuelve las debilidades del WPA. Este es dividido en 3 categorías principales:

- **Temporary Key Integrity Protocol (TKIP)**, es el término de la solución que resuelve los problemas del WEP. TKIP puede ser usado por el equipo con soporte 802.11, este provee la integridad y la confidencialidad requerida.
- **Counter Mode with CBC-MAC Protocol (CCMP) [RFC2610],** es un algoritmo criptográfico, utiliza AES [FIPS 197] como algoritmo principal, desde ahí podemos decir que es mayor el consumo de la CPU con respecto a RC4, este requiere un nuevo hardware, así como driver con soporte a CCMP.
- **802.1X Port-Based Network Access Control**, *e*ste usa tanto TKIP como CCMP, 802.1X para la autentificación.

Adicionalmente hay otro método de encriptación opcional llamado "Wireless Robust Authentication Protocol" (WRAP) que puede ser usado con CCMP.

2.10. Tecnología de la red en la nube

Con la terminología (del inglés cloud computing) conocida también como servicios o informática en la nube, término más usado en la actualidad, que describe la tecnología de nube o aplicaciones y programas que se ejecutan en la nube.

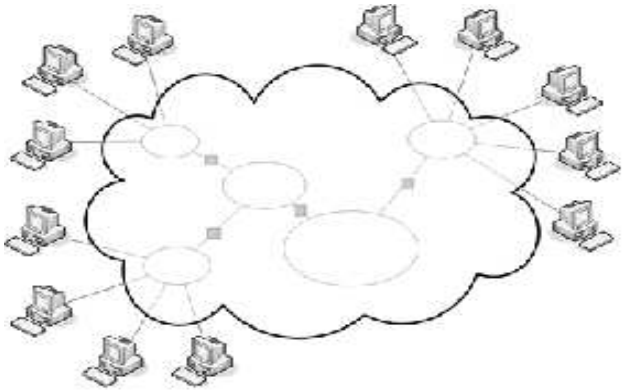


Figura 2.15. Esquema de la tecnología de nube

Fuente: Vea Baró Andreu, 2014

2.10.1. Tecnología de nube

Esta tecnología que ofrece servicios de computación mediante el internet, prácticamente es una arquitectura informática y se la define como tecnología de la nube. Se trata de una nueva tendencia de software, en la cual todos los servicios prestados al ordenador se hacen directamente desde Internet, por lo tanto, ya no se tendrá que instalar una enorme cantidad de archivos en el ordenador, ya que el programa que se desea utilizar, se ejecutará directamente desde el servidor del proveedor de software, aligerando los discos duros.

El inconveniente de esta tecnología, es que necesariamente se debe tener una conexión a internet para acceder a ella. Podemos decir entonces, que es una tecnología orientada al uso de equipos pequeños y portátiles (que utilizan servicios online), con la cual se simplifica la instalación de software y se optimiza el uso del espacio del disco duro, al no tener que llenarlo con enormes cantidades de archivos complementarios.

Figura 2.16. Aplicaciones de nube

Fuente: Padilla, M. 2014

2.10.2. Cómo funciona

Para su funcionamiento, se debe instalar una pequeña aplicación en la PC: Un cliente del software que se desea utilizar. Cada vez se ejecuta este cliente, se conectará mediante la conexión a Internet con el servidor que contiene el software que se está utilizando, convirtiéndose en una especie de programa cliente-servidor, donde se envía información al server para que este ejecute la tarea.

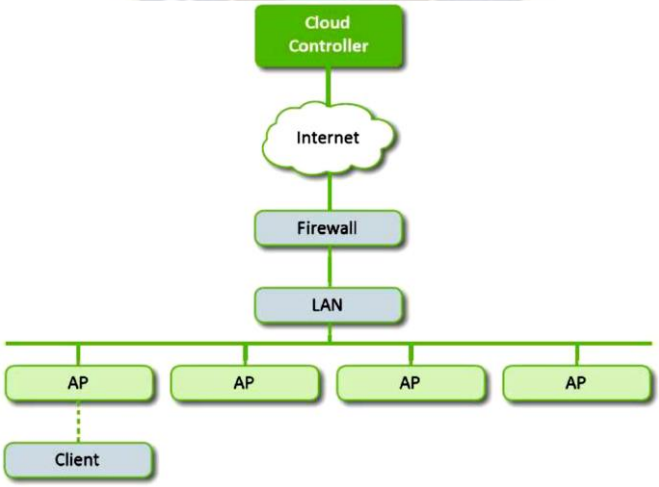


Figura 2.17. Modo de operar de la nube

Fuente: Meraki. 2010

El funcionamiento es similar a las máquinas terminales de una red. Con la ventaja del usuario final es que gana un gran espacio en los discos y en la movilidad de información.

Se debe hacer notar que todo el trabajo se realizará en un ordenador central, que por demás dejará registrados los archivos y de presentar problemas, no se tiene la oportunidad de trabajar hasta que dicho inconveniente sea solventado.

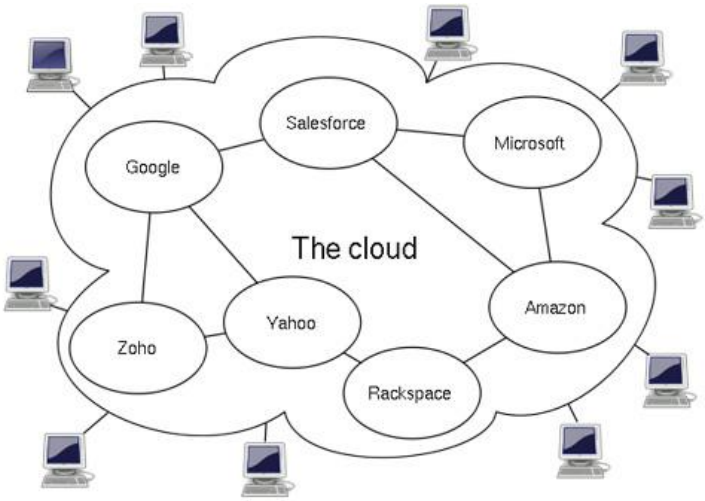


Figura 2.18. Esquema de tecnología de nube

Fuente: Padilla, M. 2014

2.10.3. Tipos de nube

Existen básicamente tres tipos de aplicaciones de nube:

- Nubes públicas, de uso global.
- Nubes privadas, las cuales son orientadas a soluciones corporativas.
- Nubes híbridas, las cuales son una mezcla de las nubes anteriores.

2.10.3.1. Nube pública

Es un servicio en donde los clientes usan la red, el almacenamiento y la memoria de forma compartida. El usuario hace todo el trabajo de despliegue por medio de un portal, por lo cual debe poseer amplias habilidades técnicas. Ej. Nube pública Azure y Amazon.

Ventajas:

No hay contratos de permanencia**,** permite autonomía en la administración de los recursos, permite realizar hibridación de servicios y ahorro en Costos (Solo cuando el Cliente es de nivel experto).

Desventajas

- El Cliente pierde para sus procesos internos la probabilidad de cumplir políticas de privacidad y confidencialidad.
- La inseguridad aumenta, no hay destrucción inmediata de Datos cuando se retira el servicio, por lo cual la información puede quedar en la nube muchos años o incluso expuesta.
- El cliente se afecta cuando malos vecinos abusan del servicio porque se comparte el Hardware.
- Es muy costoso si el Cliente no es experto, porque debe contratar el soporte por separado.

Figura 2.19. Nube Pública

Fuente: Londoño, M. 2012

2.10.3.2. Nube privada

Es un servicio exclusivo para una sola empresa u organización, en donde el hardware es totalmente dedicado. El rendimiento es mayor y es la mejor opción cuando la prioridad es la seguridad. Su despliegue generalmente se realiza en un proveedor de servicios o dentro de las oficinas del cliente, pero se recomienda por temas de velocidad de red en un datacenter externo. No es obligatorio que el cliente sea un experto en tecnologías porque generalmente el proveedor ofrece el soporte.

- **Ventajas:**

  La seguridad es mayor, y esto permite al Cliente cumplir políticas de privacidad y confidencialidad para sus procesos internos, el rendimiento es superior porque el

hardware no se comparte con otros clientes y generalmente el proveedor ayuda con la gestión.

- **Desventajas**:

  Su principal desventaja es que los costos pueden llegar a ser mayores, pero consolida el costo de la gestión tecnológica a su vez que permite el cumplimiento de normativas.

Figura 2.20. Nube Privada

Fuente: Londoño, M. 2012

2.10.3.3. Nube hibrida

Es la fusión de dos o más tipos de nubes con el fin de intercambiar datos o extender las funcionalidades de alguna de ellas.

- **Ventajas:**

  Permite realizar planes de continuidad de negocios y desplegar servicios en múltiples localizaciones geográficas.

- **Desventajas**

  Lo desventajoso es que requiere obligatoriamente una Red de alta velocidad, por lo cual se recomienda realizarla entre Datacenters.

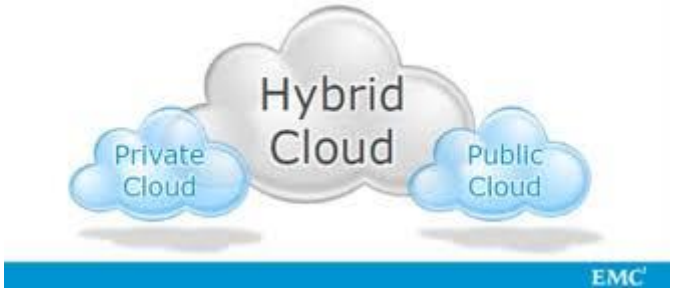


Figura 2.21. Nube Hibrida

Fuente: Londoño, M. 2012

2.10.4. Tecnología de nube en la actualidad

Actualmente, los softwares que trabajan con tecnología de nube se hacen cada vez más populares. Entre los principales programas de este tipo, tenemos el Antivirus Panda Cloud, aplicaciones ofimáticas online y programas de almacenamiento de archivos, como Flicker[14].

La tendencia a usar esta tecnología va en aumento y es posible que en el futuro los desarrolladores de software creen sólo este tipo de programas.

2.11. Almacenamiento en red en la nube

El NAS (Almacenamiento conectado en red) en la nube es un subconjunto de almacenamiento en la nube, (cloud storage) también denominado almacenamiento como servicio (Storage as a Service (SaaS)). La mayoría de la gente, cuando piensa en NAS, piensa en un dispositivo de almacenamiento en su oficina o centro de datos y se accede al mismo a través de Internet utilizando un módulo de software instalado en el propio host, se está tomando la funcionalidad del dispositivo NAS y trasladándola a la nube. Y se accede al mismo igual que si se tratara de un dispositivo local.

En pocas palabras, en eso consiste el NAS en la nube. Es un espectro en el servidor, que hace pensar al usuario que está accediendo a un dispositivo local cuando en realidad accede al mismo a través de Internet o de una conexión dedicada a larga distancia.

[14] Es un sitio web que permite almacenar, ordenar, buscar, vender y compartir fotografías o videos en línea, a través de Internet.

2.11.1. Ventajas del NAS en la nube

Con un dispositivo NAS clásico, no se sale de ese emplazamiento en concreto. De modo que, si el emplazamiento sufre algún problema, los servicios dejarán de estar disponibles. Por lo tanto, si se tienen requisitos de servicio de archivos críticos, y si se está de viaje y se necesita acceder a los mismos pero el router de la oficina no funciona, mala suerte. Pero si se traslada el dispositivo a la nube, éste está disponible virtual y permanentemente. La ventaja principal es que se puede acceder a la información en cualquier momento, sin las restricciones asociadas a la ubicación física de los datos.

2.11.2. Inconvenientes que tiene el almacenamiento en red en la nube

El principal inconveniente del NAS en la nube es que su velocidad depende de la conexión de acceso a la red. Por lo tanto, si se utiliza una conexión analógica para intentar acceder a los datos, el acceso será muy lento. Por ello, no resulta idóneo para archivos grandes o grandes grupos de datos. Sólo se debe utilizar para pequeños subconjuntos de datos o para aplicaciones especializadas, como el backup, ya que el tiempo de latencia (latency) se puede convertir en una dificultad seria.

CAPÍTULO III

3. INGENIERÍA DEL PROYECTO

3.1. Introducción

La Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca Ltda., es una entidad financiera que brinda sus servicios con responsabilidad y que desde su creación apoya el crecimiento tanto institucional como de sus socios, mediante personas y equipos eficientes, tecnología adecuada e innovador, comprometiéndose con el desarrollo de toda la institución con el paso de los años.

En esta etapa se encuentra en forma detallada toda la información requerida para comprender el problema, a la vez se puede definir estrategias poniendo atención en las restricciones bajo las cuales se debe desarrollar el sistema de acuerdo a los objetivos planteados en el proyecto.

Se requiere diseñar un sistema de gestión remoto para optimizar el acceso al servicio de internet de manera más segura y que facilite la comunicación y el intercambio de información en la Cooperativa de Ahorro y Crédito "Unión Santiago de Machaca".

3.1.1. Parámetros de diseño

El sistema debe cumplir los siguientes parámetros para un diseño jerárquico y eficiente:

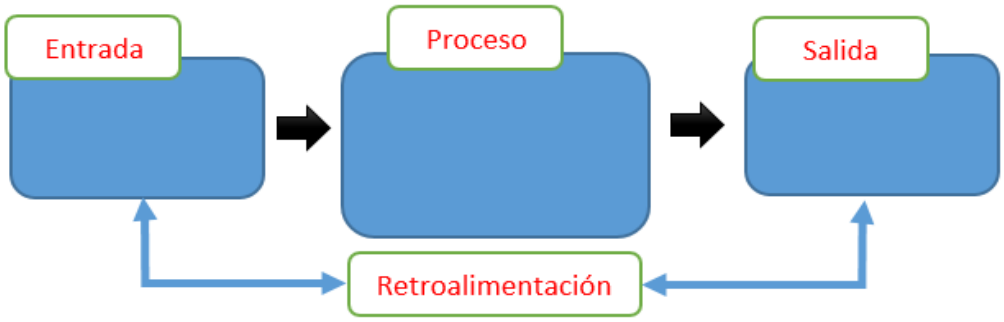


Figura 3.1 Esquema General de Sistema Entrada – Proceso - Salida

Fuente: Análisis y Desarrollo de Sistemas de Información, 2011

Por lo que la muestra de Entrada – Proceso – Salida del sistema el cual está en marcha es la siguiente:

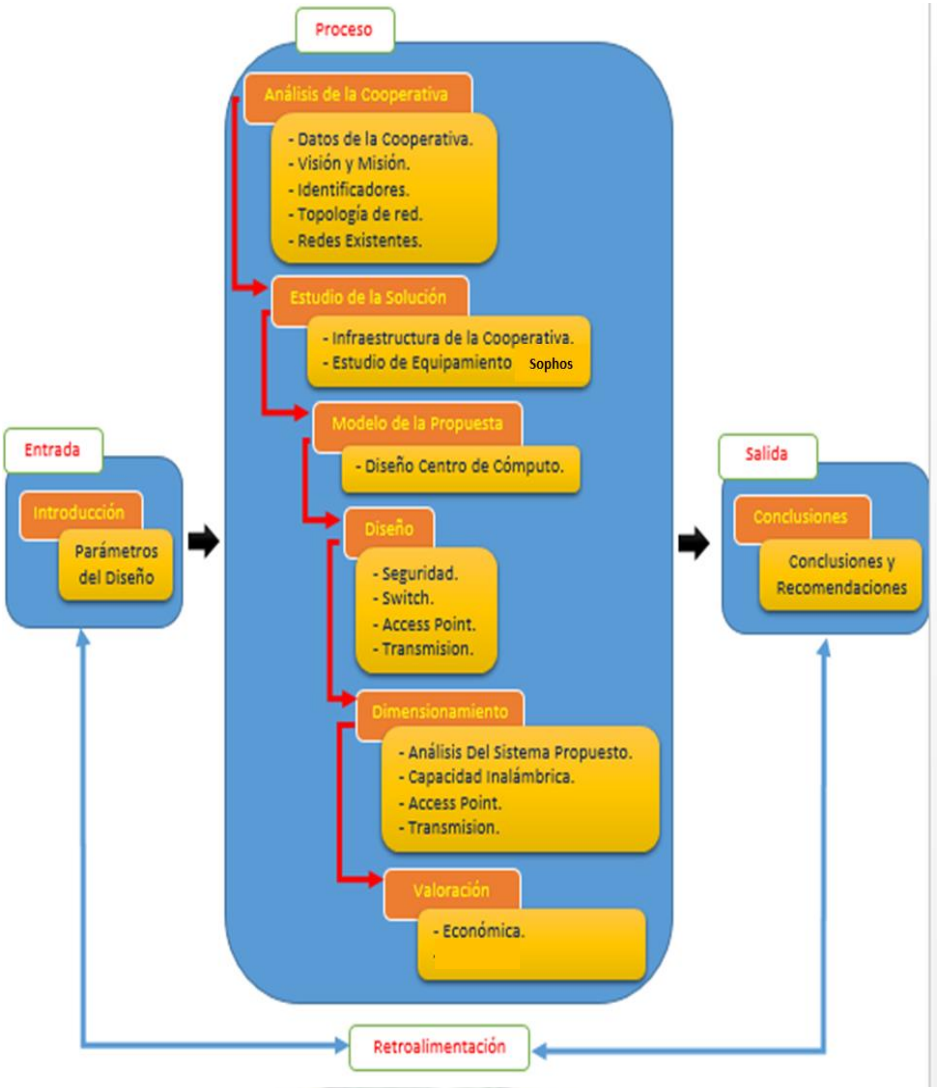


Figura 3.2 Diagrama Entrada – Proceso – Salida en la Cooperativa

Fuente: Propia

Los beneficios que presenta el sistema son:

- **Escalabilidad**

  La escalabilidad indica que el sistema puede crecer y adaptarse a nuevos usuarios sin perder la calidad de su servicio ni interrumpir funciones.

- **Disponibilidad**

  La disponibilidad es el porcentaje de tiempo que la red está operativa, consideramos en una semana 168 horas (7*24), teniendo así una disponibilidad de 100% con características integrales y siempre actualizadas.

- **Facilidad de gestión**

  El sistema será de fácil empleo y a la vez practico se necesita poco tiempo para su funcionamiento para que los usuarios puedan acceder a la red de manera fácil y hacer uso de ella en todo momento.

- **Adaptabilidad**

  El diseño es flexible, lo cual determina que puede ser adaptable para pequeñas empresas, sucursales o grandes empresas ya que puede ser adaptado con nuevas tecnologías y sistemas de la información.

El diseño del sistema se basa en parámetros que facilitan encaminar a una mejora en el acceso a la red de la cooperativa. Los servicios están dados de acuerdo a las capas que se desean cubrir en la red, es decir, seguridad mediante firewall, conectividad de la red mediante el router del ISP, switches de capa 2 para la red LAN y finalmente los Access Points para la Wireless.

3.2. Análisis de la Cooperativa

3.2.1. Datos de la Cooperativa

Rubro de la Empresa: Cooperativa de Ahorro y Crédito
Razón Social: Cooperativa de Ahorro y Crédito “Unión Santiago de Machaca S.R.L.”
Fecha de Creación: 6 de junio de 1994
Dirección: Zona 16 de Julio, Avenida Juan Pablo II, N° 2887 de la ciudad del El Alto (AGENCIA CENTRAL).

Calle Isaac Tamayo, Nro: 662, Zona el Rosario, ciudad de La Paz (SUCURSAL).

Contacto: 2846771 - 2451970

Figura 3.3 Logotipo de la Cooperativa

Fuente: USAMA LTDA.

3.2.2. Visión y Misión

- **Visión**:

  Ser una de las entidades líder en el sector de Cooperativas reguladas en el departamento de La Paz, con un crecimiento sostenible en el tiempo y brindando beneficios a los grupos de interés.″

- **Misión:**

  "Brindar servicios financieros con atención de calidad y calidez, optimizando tiempos y costos en la prestación de los mismos, promoviendo el desarrollo del vivir bien, facilitando, de esta manera, el acceso a dichos servicios sin discriminación, orientados al crecimiento de la Cooperativa, los socios, los empleados y la comunidad, aplicando una sólida tradición de prudencia.″

Figura 3.4 Valores de la Cooperativa

Fuente: USAMA LTDA.

3.2.3. Identificación de los departamentos y número de usuarios de la Cooperativa de Ahorro y Crédito Unión Santiago de Machaca LTDA.

La empresa cuenta con un edificio matriz de 2 plantas, cada piso tiene sus áreas de trabajo ya definidas por la empresa, cada sección o área está dividida por su importancia y servicio que ofrece para los socios en las dos plantas.

PISO	SECCIÓN DE LA COOPERATIVA	CANTIDAD
PLANTA BAJA	INFORMACIÓN	1
	CAJAS	2
	CRÉDITO	5
	ASISTENTE OPERATIVO	1
	ASISTENTE DE CARTERA	1
	INVERSIONES	1

Tabla 3.1. Características de la Cooperativa en la Ciudad de El Alto, Planta Baja

Fuente: USAMA LTDA.

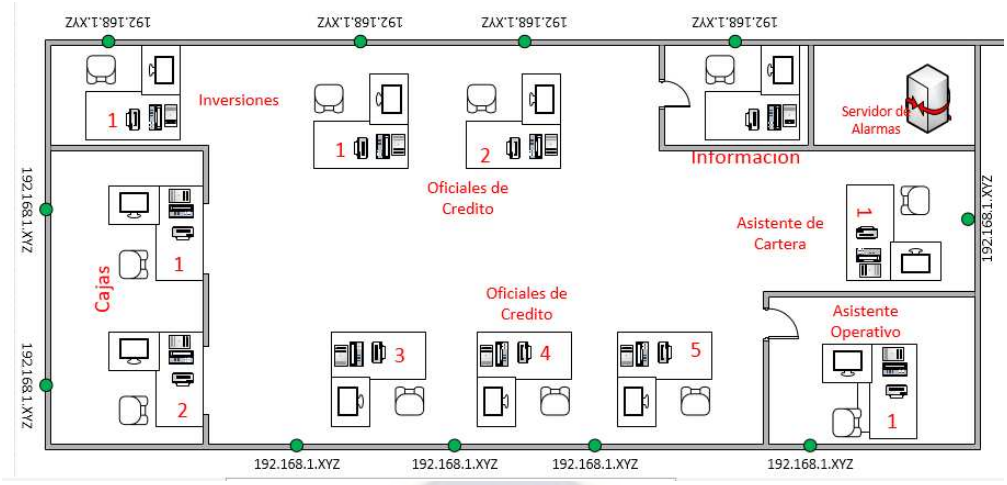


Figura 3.5 Distribución de áreas planta baja en El Alto

Fuente: USAMA LTDA

PISO	SECCIÓN DE LA COOPERATIVA	CANTIDAD
PLANTA ALTA	GERENCIA GENERAL	1
	SECRETARIA	1
	TALENTO HUMANO	1
	PRESIDENCIA	1
	AUDITORIA INTERNA	1
	CRÉDITO Y COBRANZAS	2
	CONTABILIDAD	1
	SISTEMAS	2
	RIESGOS	1
	SALA DE REUNIONES	1

Tabla 3.2. Características de la Cooperativa en la Ciudad de El Alto, Planta Alta

Fuente: USAMA LTDA

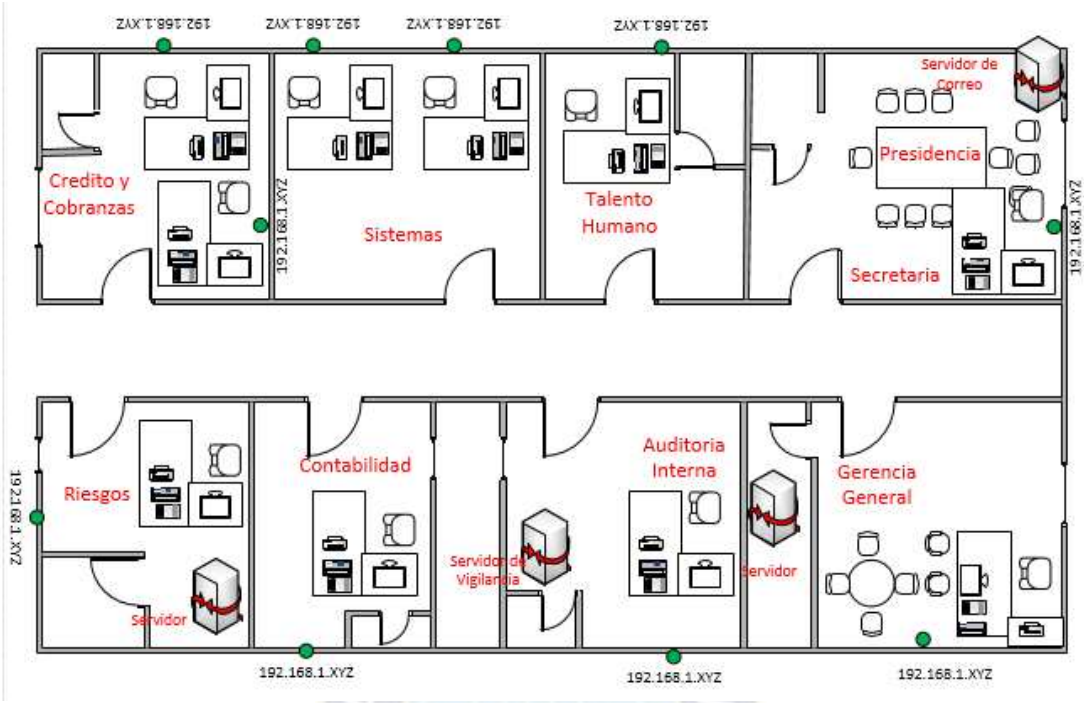


Figura 3.6 Distribución de áreas planta Alta, El Alto

Fuente: USAMA LTDA.

La empresa cuenta con una sucursal, ubicada en la Calle Isaac Tamayo, Nro: 662, Zona el Rosario, ciudad de La Paz. Cuenta con áreas de trabajo ya definidas por la empresa, a continuación, se detalla las características de la misma.

PISO	SECCIÓN DE LA COOPERATIVA	CANTIDAD
INSTALACIONES SUCURSAL	INFORMACIÓN	1
	CAJAS	2
	ASISTENTE OPERATIVO	1
	CRÉDITO Y COBRANZAS	5

Tabla 3.3. Características de la Cooperativa en la Ciudad de La Paz

Fuente: USAMA LTDA.

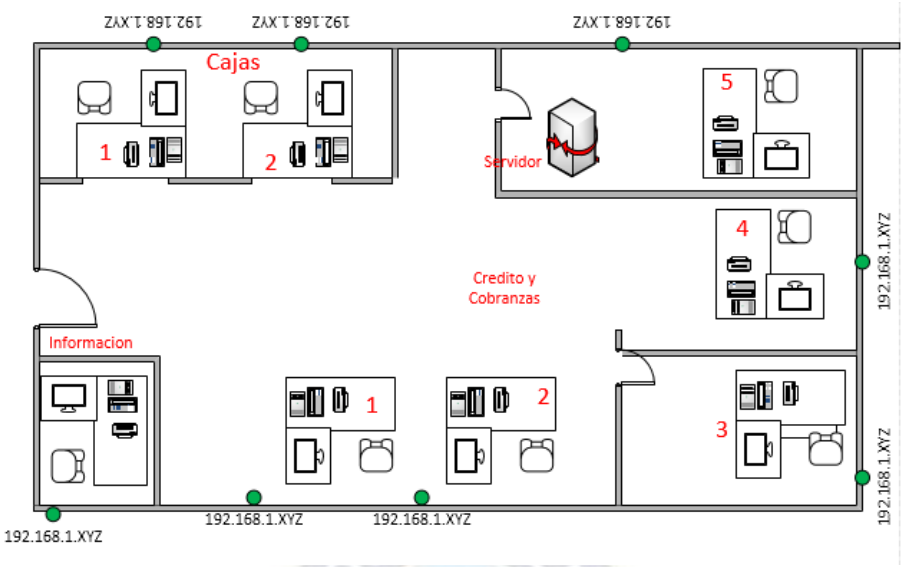


Figura 3.7 Distribución de áreas sucursal La Paz

Fuente: USAMA LTDA.

3.2.4. Topología de la red actual

La red de la cooperativa tiene una topología estrella, esto dice que todos los dispositivos de red (cámaras, servidores, impresoras, teléfonos, computadores, etc.…) están conectados a un switch, esta conmuta y transmite la información entre los dispositivos que quieren comunicarse, no existe una jerarquización en donde en lo alto estén los servidores.

En la Figura 3.8. se observa la distribución actual de la red de datos interna de la Cooperativa en cada una de sus sucursales, así como también los equipos activos que conectan los dispositivos de red.

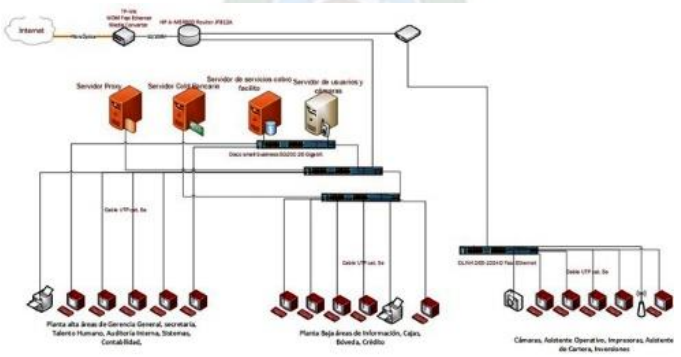


Figura 3.8 Arquitectura de Red de la Cooperativa USAMA LTDA.

Fuente: USAMA LTDA.

3.2.5. Caracterización de los Equipos Existentes de Red

3.2.5.1. Elementos de la LAN

La red de la Cooperativa de Ahorro y Crédito Unión Santiago de Machaca Ltda., tiene como principal función el brindar servicios financieros a la comunidad, para esto, dentro de la LAN utiliza el compartimiento de recursos, telefonía, Internet, etc. En este punto se evalúa las características y capacidad de los equipos existentes en la LAN.

Para la conexión de los equipos de red estos servicios se utiliza un cableado UTP cat. 5e y los equipos de red que se utilizan son:

- **Servidores**

  Los servidores existentes dentro de LAN son los definidos en la Figura 3.9:

NOMBRE DEL SERVIDOR	SISTEMA OPERATIVO	FABRICANTE	PROCESADOR	IMAGEN
Servidor Cold Bancario y Réplica	Centos 6.4	HP	Intel® Xeon® E5-2407 (126 GB de RAM)	
Servidor de servicios cobro facilito	Server 2013 Base de datos SQL Server 2005	HP	CPU: Core i3 4 GB de RAM	
Servidor Proxy	Centos		CPU: Core i3 4GB de RAM	
Servidor cámaras y usuarios	Windows 7 profesional	HP	CPU: Core i5 4GB RAM	

Figura 3.9 Características de los servidores que se encuentran en el cuarto de comunicaciones

Fuente: USAMA LTDA.

a) Servidores de aplicaciones.

Los servidores de aplicaciones funcionan como intermediarios que alojan aplicaciones web (programas que se ejecutan en un navegador web), que permite a las empresas gestionar y difundir toda la información necesaria con un punto único de entrada a los usuarios internos y externos. Teniendo como base un servidor de aplicación.

b) Servidores de bases de datos.

Este servidor mantiene y comparte la base de datos que son recopilaciones de datos organizados con propiedades predefinidas que pueden mostrarse en tablas, a través de la red.

c) Servidores de correo.

Este servidor de correo es una aplicación de red de computadoras ubicada en un servidor de Internet, que presta el servicio correo electrónico (correo-e o e-mail). De forma predeterminada, al protocolo estándar para la transferencia de correos entre servidores mediante el Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol, SMTP).

3.2.5.2. Equipos de conectividad

Switch Encore 08 puertos Fast Ethernet 10/100 Mbps

- Standard: IEEE802.3 para 10BASE-T
- Interface: Ocho puertos RJ-45 100Base-TX
- Uplink: Auto MDI/MDI-X (Auto Crossover)
- Velocidad de Red: 10/100Mbps & auto detección de modo Full/Half duplex
- Memoria: 768 Kbyte
- Conexión de Cable: Cable UTP categoría 5 RJ-45
- Indicadores LED: Sistema, Alimentación, Link/Actividad
- Alimentación: Adaptador externo
- Tabla de direcciones MAC: 1K Entradas de direcciones MAC

Figura 3.10 Switch Encore 08 puertos FE 10/100 Mbps

Fuente: Web Encore, 2013

Switch D-LINK 24 puertos Fast Ethernet 10/100 Mbps

- Anchura: 28 cm
- Profundidad: 18 cm
- Altura: 4.4 cm
- Peso: 1.9 kg
- Cantidad de puertos: 24 x Ethernet 10Base-T, Ethernet 100Base-TX
- V. transferencia de datos: 100 Mbps
- P. de interconexión de datos: Ethernet, Fast Ethernet
- Tecnología de conectividad: Cableado
- Modo comunicación: Semidúplex, dúplex pleno
- Protocolo de conmutación: Ethernet
- Expansión / Conectividad: Interfaces 24 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- Consumo eléctrico: 10 vatios
- Temperatura mínima de funcionamiento: 0 °C
- Temperatura máxima de funcionamiento: 40 °C
- Ámbito de humedad de funcionamiento: 5 - 90%

Figura 3.11 Switch D-LINK 24 puertos

Fuente: Web D-Link, 2013

Switch D-LINK 8 puertos Fast Ethernet 10/100 Mbps

- Puertos: 8 (10/100Base-TX)
- Estándares: IEEE 802.3 10Base-T Ethernet Repeater

- Conectores: RJ-45
- Transferencia: 10/100 Mbps Full Duplex, autodetect
- Método de acceso: CSMA/CD
- Método de transmisión: Store-and-forward
- Topología: Estrella
- Filtering Address Table: 8 K por dispositivo
- Fuente de poder: Externa
- Consumo 8 Watts Máximo Modelo Rev. C2 y 12 Watts Máximo Modelo Rev. D1

Figura 3.12 Switch D-LINK 8 puertos

Fuente: Web D-LINK, 2013

Router ZXHN H168N

- Puertos: 4 (10/100Base-TX)
- Estándares: 802.11b/g/n Wifi (2.4GHz)
- Conectores: RJ-45
- WAN: VDSL2/ADSL2+
- Método de acceso: CSMA/CD
- IPv4/IPv6 dual stack & DS-Lite
- Dimensiones (Largo x Ancho x Altura): 146mm x 54mm x 126xx
- Consumo: <10 Watts
- Peso: 190g

3.3. Soluciones del Mercado

A continuación, se muestran las posibles alternativas propuestas, considerando los parámetros de diseño requeridos en cada empresa.

Hoy en día toda empresa por más pequeña que sea su composición requiere de una red, pero en la mayoría se lo ha considerado a una red como un conjunto de tuberías y cables, a pensar que todo lo que se debe tener en cuenta es el tamaño de los tubos o las velocidades y la alimentación de las conexiones, con lo cual el resto no reviste de importancia. Dado que los usuarios dependen de una red para acceder a la información que se requiere para realizar un determinado trabajo y para transportar voz o video con confiabilidad, la red debe brindar un transporte inteligente y flexible. Incluso con la gran cantidad de ancho de banda disponible para los enlaces troncales de LAN donde existe la importancia de una buena administración de la red, para su aprovechamiento de todas sus ventajas.

En el intercambio de información en una red convencional, mal administrado existen aplicaciones sensibles que se ven afectados por fluctuaciones improvistas, causando demoras en el vio y en los peores casos la perdida de paquetes.

La funcionalidad de la red debe ser proporcionar un transporte eficiente y tolerante a fallas que pueda diferenciar el tráfico de aplicaciones para tomar decisiones inteligentes sobre el uso compartido de cargas cuando la red está temporalmente congestionada, independientemente de que el acceso a la red de un usuario sea por cable o inalámbrico.

La capacidad del servidor de una red debe ser proporcional a la cantidad de información intercambiada, y a los congestionamientos que se presenta en determinados momentos, considerando la importancia de una red y las falencias que genera una red convencional con una mala administración, y como respuesta a esta falencia el Firewall o Cortafuego permitirá una administración efectiva de redes.

3.3.1. Sophos Firewall serie SG

3.3.1.1. Alcance - Definición

Los dispositivos de la serie SG de Sophos están diseñados para proporcionar el equilibrio óptimo entre rendimiento y protección – para diversos entornos TI. Independientemente de

si necesita una solución para una pequeña oficina remota, quiere proteger su escuela, o si es una organización global que requiere una alta disponibilidad y características de nivel empresarial, los dispositivos de la serie SG son la elección perfecta.

3.3.1.2. Infraestructura que administra y gestiona

Estos potentes dispositivos de firewall ofrecen el rendimiento de un 1U con un factor de forma y precio de un dispositivo de sobremesa. Si necesita proteger un pequeño negocio u oficinas sucursales y trabaja con un presupuesto reducido, estos modelos son la opción ideal. También están disponibles con LAN inalámbrica 802.11ac integrada para proporcionar a sus trabajadores móviles una cobertura y conectividad óptimas. Construido sobre la última arquitectura de Intel, el software hace un uso óptimo de la tecnología multinúcleo para proporcionar un excelente rendimiento para todos sus procesos clave. Estos modelos vienen equipados con 8 puertos Gigabit Ethernet, además de 1 puerto SFP, para utilizarse, por ejemplo, con el módem DSL opcional o conectividad con fibra utilizando un transceptor SFP. La plataforma de expansión ofrece la opción de añadir conectividad adicional como el módulo 3G/4G. También está disponible un segundo módulo de radio Wi-Fi para el SG 135w. La segunda fuente de alimentación opcional garantiza la continuidad empresarial para estos modelos. Como con todos los firewalls SG, se pueden agrupar hasta 10 dispositivos en clúster para una mayor escalabilidad (debe ser el mismo modelo y número de revisión para HA).

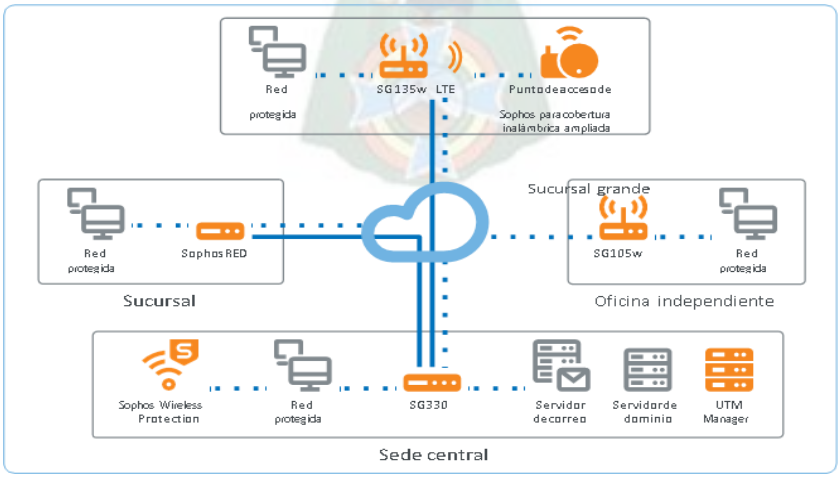


Figura 3.13 Infraestructura de Sophos Firewall

Fuente: Sophos Firewall Serie SG, s.f.

- **Productos Sophos Firewall**

Entre los principales productos que cuenta la serie SG de Firewall Sophos se encuentran los siguientes:

Modelo	Revisión n. º	Factor de forma	Especificaciones técnicas			Rendimiento			
			Puertos/ranuras (Máx. puertos)	Modelo w 802.11	Componentes intercambiable	Firewall (Mbps)	VPN (Mbps)	IPS (Mbps)	AV-proxy
SG 105(w)	3	escritorio	4	a/b/g/n/ac	aliment. ext. opc.	2.500	325	350	380
SG 115(w)	3	escritorio	4	a/b/g/n/ac	aliment. ext. opc.	2.700	425	500	500
SG 125(w)	3	escritorio	9/1 (9)	a/b/g/n/ac	aliment. ext. opc., 3G/4G	3.100	500	750	650
SG 135(w)	3	escritorio	9/1 (9)	a/b/g/n/ac	aliment. ext. opc., 3G/4G, Wi-Fi*	6.000	1.000	1.500	1.400
SG 210	3	1U	8/1 (16)	n/d	aliment. ext. opc.	12.000	1.000	2.000	500
SG 230	2	1U	8/1 (16)	n/d	aliment. ext. opc.	14.500	2.000	3.000	800
SG 310	2	1U	12/1 (20)	n/d	aliment. ext. opc.	19.000	3.000	5.000	1.200
SG 330	2	1U	12/1 (20)	n/d	aliment. ext. opc.	22.000	4.000	6.000	1.500
SG 430	2	1U	10/2 (26)	n/d	aliment. ext. opc.	28.000	4.000	7.000	2.000
SG 450	2	1U	10/2 (26)	n/d	aliment. int. opc.	30.000	5.000	8.000	2.500
SG 550	2	2U	8/4 (32)	n/d	Potencia, SSD,	45.000	8.000	12.000	3.500
SG 650	2	2U	8/6 (48)	n/d	Potencia, SSD,	65.000	10.000	16.000	5.000

Tabla 3.4. Características Técnicas del Firewall Sophos serie SG

Fuente: Propia

- **Características y capacidades**
  - Solución que gestiona todo el ciclo de vida de las redes fijas e inalámbricas.
  - Gestión convergente para facilitar la supervisión, la resolución de problemas y la generación de informes.
  - Un aspecto y una sensación similar para una mejor experiencia del usuario y gestión del flujo de trabajo.
  - Orientada a servicios, ofrecer visibilidad y soporte sobre el funcionamiento de diferentes soluciones de voz, video y los accesos de redes mientras estos son administrados.
  - Servicio centrado en administrar y resolver cuestiones vinculadas a servicios.
  - Administración unificada a través de las diferentes arquitecturas.

- Experiencia de operación optimizada, mediante una interfaz intuitiva y simplificada.
- Permite optimizar los tiempos y costos de esta área crítica de la red y alinear el flujo de trabajo de los operadores bajo las mejores prácticas de la industria, ofreciendo una administración completamente innovadora.
- Integración con las mejores prácticas.
- Soporte desde el día uno, permite descubrir y hacer un inventario de los nuevos dispositivos que se conectan a la red desde la primera vez que lo hacen.
- Interacciones inteligentes, permite una interacción personalizada para la resolución de problemas.
- Asistencia basada en contextos: permite un acceso en tiempo real a una, lo cual reduce y hasta elimina la necesidad de escalar un inconveniente.
- Administración automática de casos en el TAC: de esta forma se simplifica el proceso de seguimiento y resolución de un posible inconveniente, ya que todas las características del problema son incluidas en la solicitud inicial de soporte.
- Soporta el acceso remoto entre dos oficinas o más permitiendo que la información de una LAN a otra vaya encriptada.
- Se instala la conexión por un túnel VPN, en cada equipo haciendo transparente y única cada conexión remota, IPSEC.

3.3.1.3. Licenciamiento

- Permite monitorear y administrar los equipos para la red, cada licencia controla el número de dispositivos que puede administrar, las características y funciones.
- La arquitectura del Sophos permite habilitar cada módulo (Servicio) por licencia activando los servicios necesarios.
- Cada licencia por módulo tiene una duración de un año, dos años según corresponda.
- En la Figura 3.14 se muestra una vista de los reportes que genera de forma diaria, semanal, mensual o cuando se requiera del Sophos firewall:

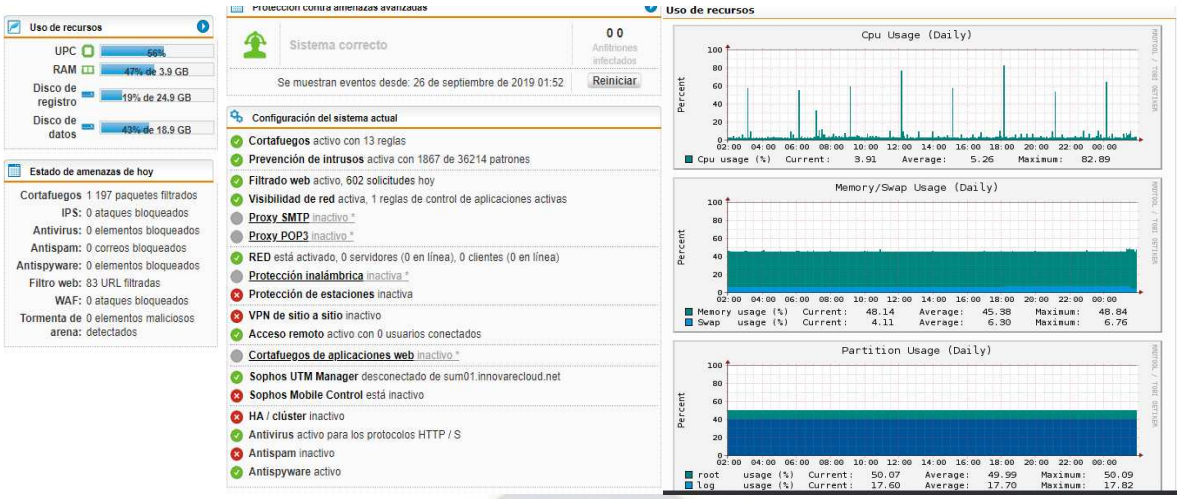


Figura 3.14 Sophos Firewall, Vía web

Fuente: Sophos Firewall, s.f.

3.3.2. Equipamiento Meraki, Cloud Management

3.3.2.1. Alcance-Definición

La solución de administración en la Nube Meraki de Cisco, se gestiona de forma centralizada y fácil desde la nube, la arquitectura de nube de Meraki tiene características que permite a los clientes en todo el mundo resolver los problemas de negocio y reducir los costos de operación, sin el costo y la complejidad de los aparatos de control o software de gestión de superposición.

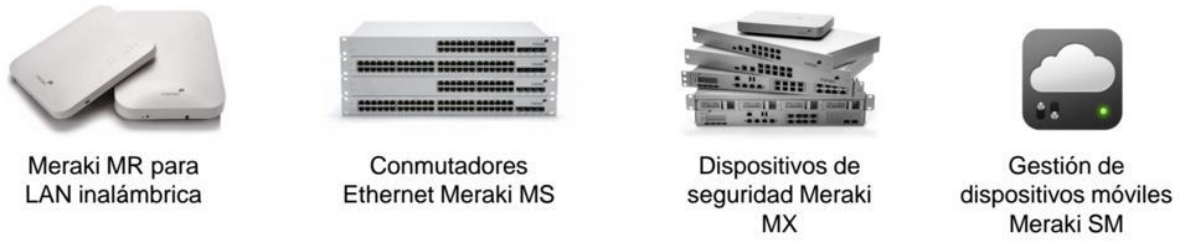


Figura 3.15 Arquitectura de Meraki

Fuente: Meraki, s.f.

3.3.2.2. Infraestructura que administra y gestiona:

La infraestructura de Meraki gestiona desde la nube “Wireless LAN”, “Security Appliance”, “Switches”, “Mobility Management”.

- **Productos Meraki, Cloud Managment:**

  - **LAN inalámbrica**, El Cisco Meraki MR26 establece el nuevo estándar en telefonía móvil, diseñada específicamente para las implementaciones de alta densidad y de próxima generación [IHS, s.f.], que es punto de acceso inalámbrico gestionado en la nube.
  - El uso de mayor ancho de banda de canal, las tecnologías de transmisión más eficientes, y los canales con menos gente a los 5 GHz ayudan al MR26 alcanzar velocidades de hasta 2,5 Gbps, mientras que también proporciona a los administradores completa visibilidad y control.
  - **Security appliance**, Las soluciones de Meraki en cuanto a seguridad están clasificadas en gama baja, media y alta que, dentro de cada clasificación proporciona diferentes equipos de acuerdo a la necesidad. Meraki permite levantar remotamente a los dispositivos de seguridad en cuestión de minutos a través del aprovisionamiento de la nube, además, sincronizar la configuración de seguridad a través de miles de sitios utilizando plantillas.

  - **Switch, cloud Meraki** cuenta con equipos switching de capa 2 y 3, de diferentes velocidades, combinan las ventajas de la gestión centralizada basada en la nube con una plataforma de acceso de gran alcance, confiable, apoyando la más sencilla de las implementaciones empresariales más exigentes.

    Con la gestión de la nube, miles de puertos de conmutación se pueden configurar y monitorizar al instante, a través de Internet. Ofrecen una completa solución de seguridad y gestión unificada de amenazas, diseñado para hacer que las redes distribuidas actúen de forma rápida y son altamente seguros y fáciles de manejar. Son gestionadas en su totalidad a través de la consola basada en web de Cisco Meraki, que proporciona controles intuitivos y auto aprovisionamiento para las implementaciones de sucursales remotas sin TI en el sitio.

- **Mobility management**, estas soluciones están dirigidas a unificar la gestión y el control de miles de dispositivos móviles y de escritorio puede ser manejado a través del portal de Meraki que está basado en un navegador seguro. Permite manejar iniciativas de movilidad en la empresa por la perfección de incorporación de nuevos dispositivos y la automatización de la aplicación de políticas de seguridad.

- **Características y capacidades**
  - Cuenta con altos estándares de seguridad y niveles de soporte.
  - Administración centralizada desde la Cloud, comprende que los servicios de seguridad, privacidad y la fiabilidad están siendo alojados en la nube de Meraki.
  - Brinda un porcentaje del 99,99% de Confiabilidad de SLA.
  - Proporciona dos factores de autenticación (usuario/password y un key o código adicional que se envía al correo).
  - Arquitectura redundante en alta disponibilidad.
  - Meraki cuenta con el certificado SSAE16 II otorgado bajo auditorías en Data Center.
  - Gestionan toda su red desde un único panel de control.
  - Los usuarios controlan, aplicaciones y dispositivos.
  - Escala de sitios pequeños a implementaciones empresariales.
  - La LAN inalámbrica añade capacidad inalámbrica en cuestión de minutos con el aprovisionamiento totalmente automático.
  - Permiten a los clientes resolver problemas de negocio y reducir los costos de operación.

3.3.2.3. Licenciamiento y Soporte

- En la arquitectura Cloud Meraki, todos los equipos tienen sus respectivos licenciamientos, esto permite que todo sea administrable desde la nube.
- Se debe considerar que en el licenciamiento de Meraki está incluido el soporte, instalación, configuración y capacitación.

La arquitectura de Sophos ofrece una visibilidad sin precedentes sobre los usuarios de mayor riesgo, apps desconocidas, amenazas avanzadas, cargas sospechosas y mucho más. También se beneficiará de la generación de informes detallados integrada, incluida sin costes adicionales, y la opción de añadir Sophos iView para la generación de informes centralizada en múltiples firewalls.

3.3.3. Comparación de Sophos Firewall y Cloud Management Meraki

Para el presente análisis se consideran los parámetros de un diseño jerárquico, es decir, equipos que permitan tener tolerancia a fallas, escalabilidad, QoS y seguridad, además de los parámetros que proporcionan las NTICS: movilidad, portabilidad y aprovisionamiento del servicio.

3.3.3.1. Análisis Comparativo entre las dos soluciones presentadas del Firewall

	Cisco Meraki	Sophos SG
Cortafuegos de red		
IPV6	SI	SI
Modelado de tráfico y colas prioritarias	SI	SI
Inspección de estado	SI	SI
Inspección profunda de paquetes	SI	SI
Protección contra amenazas		
Antimalware	SI	SI
Sandboxing basado en red	NO	NO
Sandboxing basado en la nube	NO	NO
Sandboxing de archivos	NO	NO
Cortafuegos	SI	SI
Sistema anti-bot	SI	SI
Capacidades Adicionales		
IPS	SI	SI
WAF	NO	SI
En informes de dispositivos	SI	SI
VPN	NO	SI
Seguridad web		
Control de la aplicación	SI	SI
Enrutamiento basado en políticas	SI	SI
Bloqueo GeoIP	SI	SI
Proxy de reenvío SSL	NO	SI
Descifrado SSL	NO	SI
Seguridad de correo electrónico		
Filtrado de spam	SI	SI
Prevención de malware	SI	SI
Filtrado de contenido	SI	SI
Protección de spam saliente	SI	SI
Opciones de implementación		
Nube	SI	NO
Hospedaje Administrado	NO	SI
Aparato de hardware	SI	SI
Dispositivo virtual	NO	SI
Soporte de dispositivo		
Windows	SI	SI

Android	SI	SI
IOS	SI	SI
Citrix	NO	SI
Servidor de Windows Terminal	SI	SI
Mac	SI	SI
Linux	NO	SI

Tabla 3.5. Análisis de resultados entre Firewall

Fuente: Propia

Las ventajas fundamentales de Sophos Firewall se manifiestan en la seguridad, las características son:

- Control de tráfico según aplicaciones: establece políticas de ancho de banda basadas en el tipo de aplicación de la capa 7 (p. ej., YouTube, Skype, P2P).
- Da prioridad a las aplicaciones críticas y reduce el tráfico recreativo.
- Filtrado de contenidos: filtros de contenidos basados en categorías de conformidad con la CIPA, configurables para clases de usuarios según la pertenencia a usuarios/grupos de Active Directory.
- Firewall de inspección de estado: establece políticas de firewall mediante una interfaz gráfica intuitiva.

3.3.3.2. Análisis entre Arquitecturas

En la Tabla 3.6 se puede observar un análisis final entre las arquitecturas de Cisco Meraki y Sophos SG Firewall, donde se consideraron los parámetros de: Software, Alcance de la Administración, Seguridad, Gestión e Infraestructura y precio.

En vista que Sophos Firewall Serie SG cumple con los requerimientos y objetivos del proyecto, se recomendó la implementación del Firewall para la Oficina Central y Sucursal respectivamente puesto que cumple con la mejor conexión segura de acceso remoto para la administración de políticas de seguridad a nivel de red.

	SOPHOS SG	MERAKI CLOUD
	ADMINISTRACIÓN DE LA RED	
SOFTWARE	Licenciado	Licenciado
ALCANCE DE LA ADMINISTRACIÓN	Servicio Integral desde cualquier lugar	Servicio Integral desde cualquier lugar
SEGURIDAD	La licencia es modular para los diferentes niveles de Seguridad	La seguridad se encuentra en la Nube propia de Cisco
GESTIÓN	Gestiona las redes Inalámbricas	Administración desde la nube
INFRAESTRUCTURA	Wireless Integrado	Wireless LAN
	Herramientas colaborativas	Seguridad solo a nivel Cloud
	Gestión Administrativa Remota	Gestión de Administración en la nube
PRECIO	400 USD Equipo + 1000 USD Soporte Anual	600 USD Equipo + 1500 USD Soporte Anual

Tabla 3.6. Análisis entre Arquitecturas

Fuente: Propia

3.4. Beneficios técnicos de Sophos Firewall Series SG

3.4.1. Soporte de Sophos Firewall SG

El soporte en el Sophos Firewall se encuentra organizado en centros de datos de nivel 1 certificados según SAS70 tipo II[15]. Estos centros de datos presentan las medidas de seguridad física y de software más moderno, así como diseños de alta fiabilidad.

3.4.1.1. Seguimiento de disponibilidad

- Acuerdo de nivel de servicio de 99,99% de tiempo de actividad (menos de una hora al año de inactividad).
- Procedimientos de escalado rápido a través de múltiples equipos de operaciones.
- Sistema independiente de alerta por interrupciones con triple redundancia.

[15] SAS 70 es un estándar internacional que provee una guía para que un auditor independiente emita una opinión de la descripción de controles de la organización a través del Reporte de Servicio del Auditor; este reporte puede ser de dos tipos:
El reporte de tipo I detalla la descripción de controles de la organización en un punto específico de tiempo.
El reporte de tipo II no sólo incluye de descripción de controles de la organización, sino que también incluye un testing detallado de los controles de la organización durante un período mínimo de seis meses.

3.4.1.2. Redundancia

- Las características de redundancia sin precedentes en un dispositivo Sophos con un segundo SSD (RAID) integrado y una segunda fuente de alimentación opcional disponible para ambos modelos.
- La redundancia como SSD duales, fuentes de alimentación y ventiladores intercambiables, le aseguran una protección en todo momento. Un total de 8 plataformas de FleXi Port, una de las cuales viene equipada con un módulo de cobre de 8 puertos por defecto

3.4.1.3. Recuperación en caso de desastre

- Existe mucha rapidez en caso de desastre en caso de reemplazo del hardware tanto a nivel local e internacional.

3.4.1.4. Seguridad de los servicios

- Detección de intrusiones automatizada 24 horas.
- Protección mediante firewalls basados en puertos e IP.
- Acceso remoto restringido por dirección IP y verificado por clave pública (RSA).
- Sistemas sin acceso por contraseña.
- Alerta automática a administradores en caso de cambios de la configuración.
- Todos los datos sensibles (p. ej., contraseñas) se almacenan en formato cifrado.

3.4.1.5. Seguridad física.

- El acceso a las instalaciones se controla mediante lectores biométricos y un sistema de tarjetas codificadas de alta seguridad.

3.4.2. Dispositivo de Seguridad

Para determinar el modelo apropiado, el dispositivo debe manejar las siguientes características:

- Gestión centralizada basada en la nube
- Administración de Redes y seguridad

- La modulación del tráfico y la gestión de aplicaciones
- Servicios de seguridad avanzada
- Velocidad óptima para mejor rendimiento aproximadamente 500 Mbps; Clientes máximos recomendados 200
- Cortafuegos de estado, Autoconfiguración de sitio a sitio VPN, Cliente VPN (IPSec)
- Integración de Active Directory, políticas basadas en la identidad
- La modulación del tráfico y la gestión de aplicaciones
- Visibilidad y calidad de servicio con priorización de aplicaciones

Servicios de seguridad avanzada

- Filtrado de contenido
- Confiabilidad en búsqueda de información
- Prevención de intrusiones (IPS)
- Antivirus y filtrado antiphishing
- Licencia de seguridad avanzada

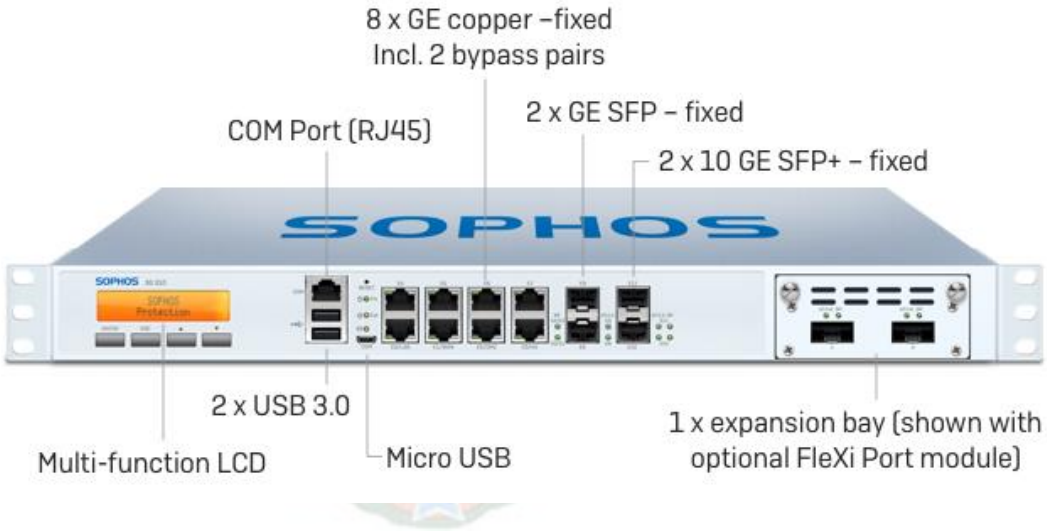


Figura 3.16 Especificaciones técnicas Dispositivo de seguridad Sophos Firewall SG 125w

Fuente: Sophos, s.f.

RENDIMIENTO	
FIREWALL	3100 MBPS
VPN	500 MBPS
IPS	750 MBPS
AV (PROXY)	650 MBPS
CONECTIVIDAD	
PUERTOS ETHERNET	8 x GE cobre 1 x SFP*
OPCIÓN WI-FI	802.11ac, 3x3 MIMO, 3 antenas externas, una única radio de 2,4 o 5 GHz
MÓDULOS	
RANURAS DE EXPANSIÓN	1
MÓDULOS OPCIONALES	Módulo 3G/4G Módem DSL SPF Transceptores SFP
REDUNDANCIA	
COMPONENTES INTERCAMBIABLES	2.ª fuente de alimentación opcional

Tabla 3.7. Características técnicas de Sophos Firewall SG 125w

Fuente: SOPHOS. Modelos de escritorio SG, s.f.

3.4.3. Switch

Para determinar el modelo apropiado, el dispositivo debe manejar las siguientes características:

- Requerimientos de Hardware: Puertos Gigabit y SFP
- Gestión centralizada basada en la nube
- Capa 2 y 3

MS 220-48

- Puertos Gigabit Ethernet, 4 x SFP de 1G de enlace ascendente, no compartido, 1 Gb de enlace.

Plataforma de Hardware:

- De voz y de vídeo QoS, como se indica en su respectivo datasheet
- Soporta sistema de alimentación redundante de Cisco (RPS2300)

- PoE disponibles al mismo tiempo en todos los puertos.

Gestión de la nube:

Gestionado de forma centralizada a través de Internet, autoabastecimiento

- Visibilidad y control sobre miles de puertos, Integrado en la gestión de múltiples sitios
- Herramientas de solución de problemas en tiempo real.

Figura 3.17 MS 220-48

Fuente: Meraki Cisco, s.f.

MS 320-48

- Puertos Gigabit Ethernet, 4 x SFP de 1G de enlace ascendente, no compartida, 10 Gb de enlace

Plataforma de Hardware:

- De voz y de vídeo QoS.
- Soporta sistema de alimentación redundante de Cisco (RPS2300)
- PoE disponibles al mismo tiempo en todos los puertos

Gestión de la nube:

- Gestionado de forma centralizada a través de Internet, autoabastecimiento
- Visibilidad y control sobre miles de puertos
- Herramientas de solución de problemas en tiempo real

Capa 3:

- El enrutamiento dinámico (OSPFv2), enrutamiento estático
- DHCP Relay, servidor DHCP
- Redundancia de repuesto caliente (VRRP)

Figura 3.18 MS 320-48

Fuente: Meraki Cisco, s.f**.**

3.4.4. Access Point

Para determinar el modelo apropiado, el dispositivo debe manejar las siguientes características:

- Ambiente empresarial crítico
- Gestión centralizada basada en la nube
- Análisis de ubicación de presencia de invitados

Punto de acceso interior MR26

Trabaja con el estándar 802.11n que tiene la frecuencia de funcionamiento de 2.4 Ghz, ya que posee dos radios cada una tiene una velocidad de datos típica de 450 Mbps y una total de 900 Mbps en un radio de distancia de 200 metros.

Figura 3.19 Router MR26

Fuente: Data Sheet MR26

Operating Band	Operating Mode	Data Rate	TX Power (dBm)	RX Sensitivity
2.4 GHz	802.11b	1 Mb/s 11 Mb/s	22 22	-92 -85
2.4 GHz	802.11g	6 Mb/s 54 Mb/s	21 20	-88 -73
2.4 GHz	802.11n (HT20)	MCS0/8/16 HT20 MCS7/15/23 HT20	22 19	-90 -70
2.4 GHz	802.11n (HT40)	MCS0/8/16 HT40 MCS7/15/23 HT40	21 19	-85 -67
5 GHz	802.11a	6 Mb/s 54 Mb/s	21 19	-89 -71
5 GHz	802.11n (HT20)	MCS0/8/16 HT20 MCS7/15/23 HT20	22 18	-88 -69
5 GHz	802.11n (HT40)	MCS0/8/16 HT40 MCS7/15/23 HT40	20 17	-83 -65

Tabla 3.8. Datos Técnicos del MR26

Fuente: Datasheet MR26

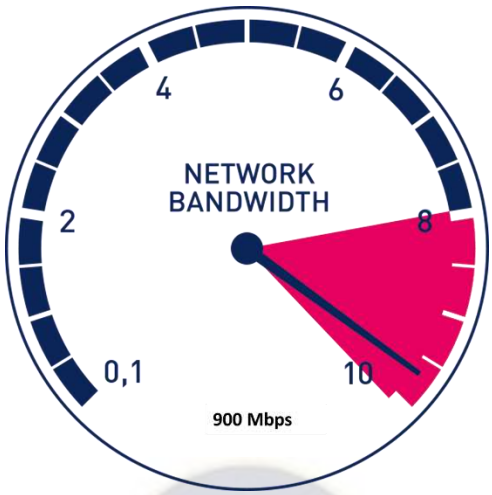


Figura 3.20 Velocidad de transmisión total de datos de los equipos

Fuente: Meraki Cisco, s.f.

3.4.5. Medio de Transmisión

El medio de trasmisión actual es el sistema de cableado 6a; presta las características técnicas para el transporte de datos, voz y video, como se observa en la Tabla 3.9.

Categoría	Estándar	Ancho de Banda	Velocidad	Distancia que Soporta	Características
Categoría 1	TIA/EIA-568-B	0,4 MHz	100 Kbps	100 Metros	Esta categoría consiste del cable básico de telecomunicaciones y energía de circuito limitado. Líneas telefónicas y módem de banda ancha.
Categoría 2	TIA/EIA-568-B	4 MHz	4 Mbit/s	100 Metros	Esta categoría de cable es capaz de transmitir datos hasta 4 **Mbit/s**. Generalmente ya dejó de ser usado.
Categoría 3	EIA/TIA-568	16 MHz	10 Mbit/s	100 Metros	El cableado de Categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps.
Categoría 4	EIA/TIA-568	20 MHz	16 Mbit/s	100 Metros	El cableado de Categoría 4 se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps.
Categoría 5 / 5e	TIA/EIA-568-B	100 MHz	1000 Mbps	100 Metros	Está diseñado para señales de alta integridad. Estos cables pueden ser blindados o sin blindar. Este tipo de cables se utiliza a menudo en redes de ordenadores como Ethernet, y también se usa para llevar muchas otras señales como servicios básicos de telefonía, token ring, y ATM.
Categoría 6	ANSI/TIA/EIA-568B-2.1	250 MHz	1 Gbps	90 Metros	Posee características y especificaciones para crosstalk y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (*Gigabit Ethernet*).
Categoría 6a	ANSI/TIA/EIA-568B-2.10	550 MHz	10 Gbit/s	100 Metros	Operan a frecuencias de hasta 550 MHz (tanto para cables no blindados como cables blindados) y proveen transferencias de hasta 10 Gbit/s. La nueva especificación mitiga los efectos de la diafonía o *crosstalk*. Soporta una distancia máxima de 100 metros. En el cable blindado la diafonía externa (crosstalk) es virtualmente cero.

Categoría 7 / 7a	ISO/IEC 11801	600-1200 MHz	10 Gbit/s	100 Metros	El Cat 7 posee especificaciones aún más estrictas para crosstalk y ruido en el sistema que Cat 6. Para lograr esto, el blindaje ha sido agregado a cada par de cable individualmente y para el cable entero.
Coaxial Grueso	IEEE 802.3 10Base5	350 GHz	10 Mb/seg	500 Metros	Este cable se conoce normalmente como "cable amarillo", fue el cable coaxial utilizado en la mayoría de las redes. Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables.
Coaxial Fino	IEEE 802.3 10Base2	350 GHz	10 Mb/seg	185 Metros	Este cable se empezó a utilizar para reducir el coste de cableado de las redes. Su limitación está en la distancia máxima que puede alcanzar un tramo de red sin regeneración de la señal. Sin embargo el cable es mucho más barato y fino que el thick y, por lo tanto, solventa algunas de las desventajas del cable grueso.

Tabla 3.9. Características técnicas del medio de transmisión

FUENTE: Lobato Javier, 2012

3.5. Dimensionamiento de la Red

Servicio	Dispositivo principal	Uso Principal	Beneficio	Desafío	Tecnología	Modelo	Tolerancia a Fallos	Estabilidad	Q&S	Seguridad
Conexión Segura a Internet	Firewall	Proporcionar acceso de entrada y salida a Internet	Conexión entre la oficina Central y Sucursal de Acceso Remoto	Seguridad	Sophos	SG 125w	✓	✓	✓	✓
Conectividad a Nivel de Red	Router	Conectividad a Nivel de Red	Conectarse con clientes, proveedores	Interconectar Subredes (enviar o encaminar paquetes de datos de una Red a otra)	Could	Proveedor	✓	✓	✓	✓
Red de Área Local Inalámbrica	Conmutadores	Conectar Servidores, Dispositivos y PCs	Conectividad LAN de alta velocidad por capas	Diseño Jerárquico	Could	MS 220-48 MS 320-48	✓	✓	✓	✓
	Medios de Transmisión	Cable	Conectividad LAN de alta velocidad	Transmisión convergente	Convergente	UTP CAT 6A	✓	✓	✓	✓
Conectividad Alámbrica Segura a la LAN	Puntos de Acceso Alámbricos Aps	Conectar dispositivos habilitados de manera inalámbrica (tales como PCs, portátiles, tablets y PDAs)	Movilidad del Cliente	Seguridad Velocidad de la Transmisión	Could	MR-26	✓	✓	✓	✓

PoE	**Power over Ethernet**	Alimentación eléctrica en una infraestructura LAN estándar	Elimina la utilización de tomas de corriente	La alimentación eléctrica se suministra a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo cable que se utiliza para la conexión de red	Convergente	proveedor	✓	✓	✓	✓

Figura 3.21 Dimensionamiento parámetros de diseño

Fuente: Propia

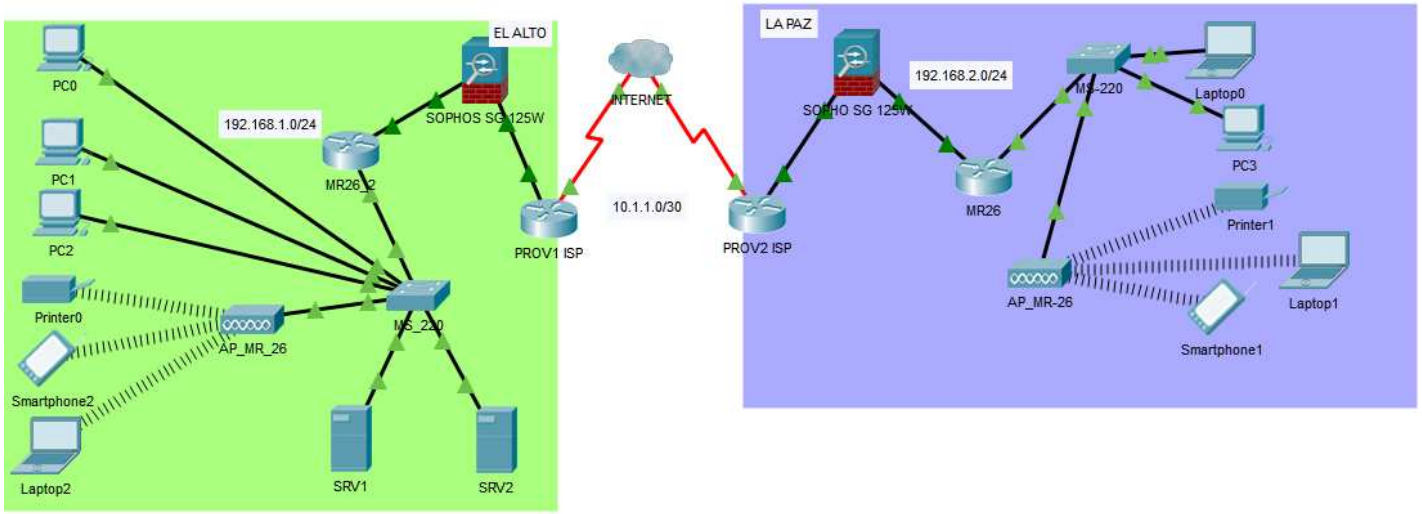


Figura 3.22 Propuesta de red de la Cooperativa USAMA LTDA.

Fuente: Propia

3.5.1. Análisis de la solución propuesta

El diseño propuesto presenta las 4 características técnicas necesarias para que esta arquitectura de red maneje eficiencia en la prestación de servicios.

- La Tolerancia a fallas se maneja en la redundancia en la capa física (dispositivos) y topología en los 3 niveles acceso, distribución-core y seguridad.
- La Escalabilidad se presenta en los 3 niveles: Nivel de acceso donde se tiene un número de puertos libres para el crecimiento en las áreas de la empresa. Nivel de Distribución, consta de 1 switch de 48 puertos y 1 dispositivo para administrar y controlar el tráfico.
- La Calidad del servicio viene ya de fábrica en los dispositivos del cluster de Meraki, donde sus puertos manejan Q&S.
- La Seguridad se manifiesta desde su diseño redundante en la capa física y que se debe aplicar a la capa de aplicación mediante la virtualización de sus discos para albergar los servicios de IT a proveer.

3.5.2. Configuración del Firewall de la Oficina Central de la Cooperativa

De acuerdo a los problemas detectados se cuenta con las siguientes configuraciones y adecuación de acuerdo a la siguiente infraestructura de red:

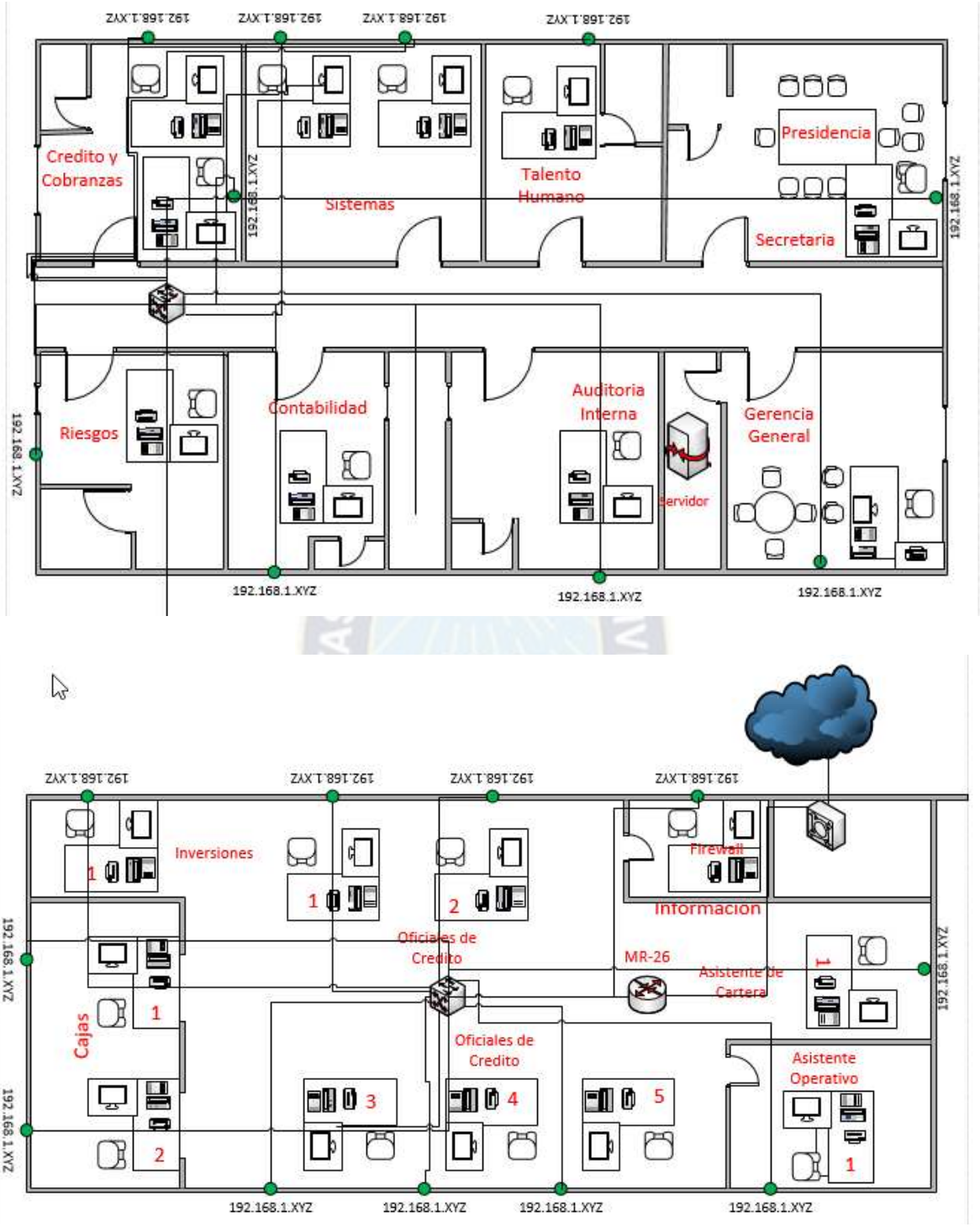


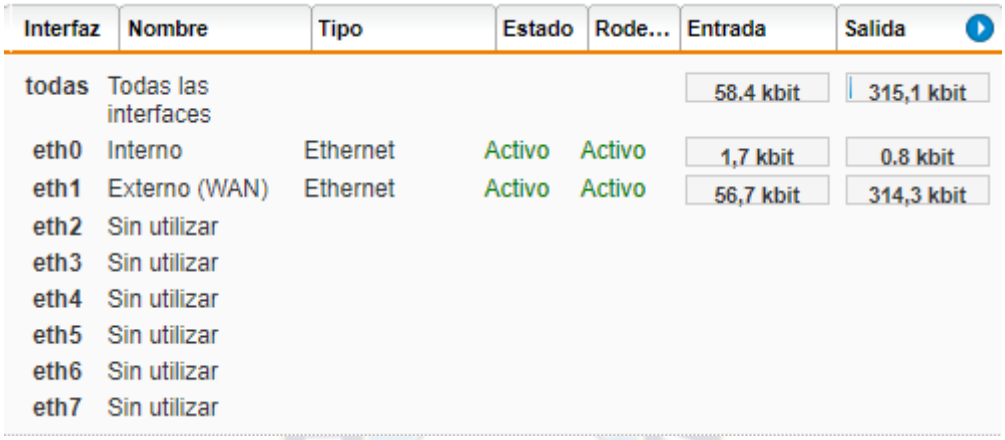
Figura 3.23 Propuesta de red de la Cooperativa USAMA LTDA Oficina Central El Alto

Fuente: Propia

3.5.3. Definición de las Interfaces

De acuerdo a políticas informáticas de la Cooperativa, las interfaces habilitadas son dos la primera WAN y LAN de acuerdo a los estándares de red conocidos.

La configuración se realizó y se puso en funcionamiento según los IP' Privados y Públicos por defecto:



Interfaz	Nombre	Tipo	Estado	Rode...	Entrada	Salida
todas	Todas las interfaces				58.4 kbit	315,1 kbit
eth0	Interno	Ethernet	Activo	Activo	1,7 kbit	0.8 kbit
eth1	Externo (WAN)	Ethernet	Activo	Activo	56,7 kbit	314,3 kbit
eth2	Sin utilizar					
eth3	Sin utilizar					
eth4	Sin utilizar					
eth5	Sin utilizar					
eth6	Sin utilizar					
eth7	Sin utilizar					

Figura 3.24 Interfaces Interna y Externa de la Oficina Central El Alto

Fuente: Propia

3.5.4. Definición de Usuarios y Red

Posterior a la detección de los usuarios, puertos y hosting hospedados en el Servidor DNS de la cooperativa se logró configurar los mismos utilizando una nomenclatura que va de acuerdo a la Unidad/Área que pertenece. Identificando también si pertenece el usuario a la oficina central o sucursal:

Figura 3.25 Definiciones de red dentro de la Oficina Central El Alto

Fuente: Propia

La creación de un usuario o denominado Nueva definición de Red está dada por el siguiente cuadro en el cual se pide el tipo de conexión de Red

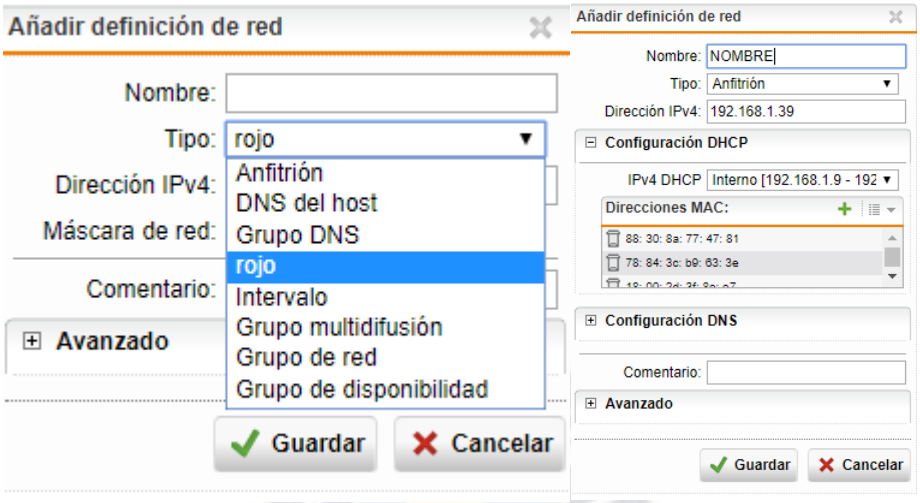


Figura 3.26 Tipo de Definiciones de red dentro de la Oficina Central El Alto

Fuente: Propia

En este caso ponemos un nombre de acuerdo a la nomenclatura descrita en párrafos anteriores, se le asigna una dirección IPV4 y también en el cuadro Dirección MAC, se colocaron el mac address de cada equipo. Este procedimiento nos puede generar un mapeo de los sitios, correo electrónicos y tareas que realizan un equipo de la red.

3.5.5. Definición de Servicios: puertos UDP/TCP

Para balancear la salida o entrada de los softwares, sistemas o página web que tiene la Cooperativa se realiza la habilitación de los puertos UDP/TCP, IP, ICMP, ICMPv6, que permitirán que las aplicaciones o servidores pasen por el Firewall:

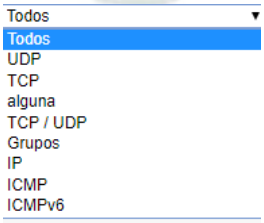


Figura 3.27 Tipo de Definiciones de puertos a habilitar de la Oficina Central El Alto

Fuente: Propia

Al tener la infraestructura de Servidores se realizó la habilitación de los puertos del Sistema Core Bancario (correspondientes) por ejemplo el puerto 80

Figura 3.28 Habilitación de puerto de postgresql y CoreBancario a habilitar de la Oficina Central El Alto

Fuente: Propia

3.5.6. Gestión de usuario para el acceso remoto entre la Agencia de La Paz y la oficina Central en el Alto

Para acceder a la infraestructura de Servidores y conexión de acceso remoto se debe utilizar usuarios personalizados, pero a la vez la habilitación del usuario VPNUSERSucursal:

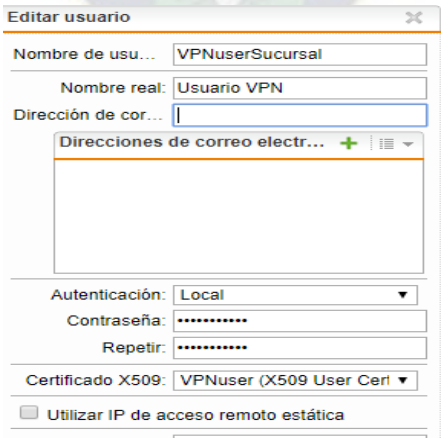


Figura 3.29 Habilitación del Usuario VPN Sucursal que permite conectar el Servidor de la Sucursal en La Paz con la Infraestructura de Servidores y Redes de la Oficina Central del Alto

Fuente: Propia

3.5.7. Cortafuegos

Posterior a ello, se instala y configura las políticas del Cortafuegos que permitirán el enlace de la red interna (LAN) con la externa (WAN)

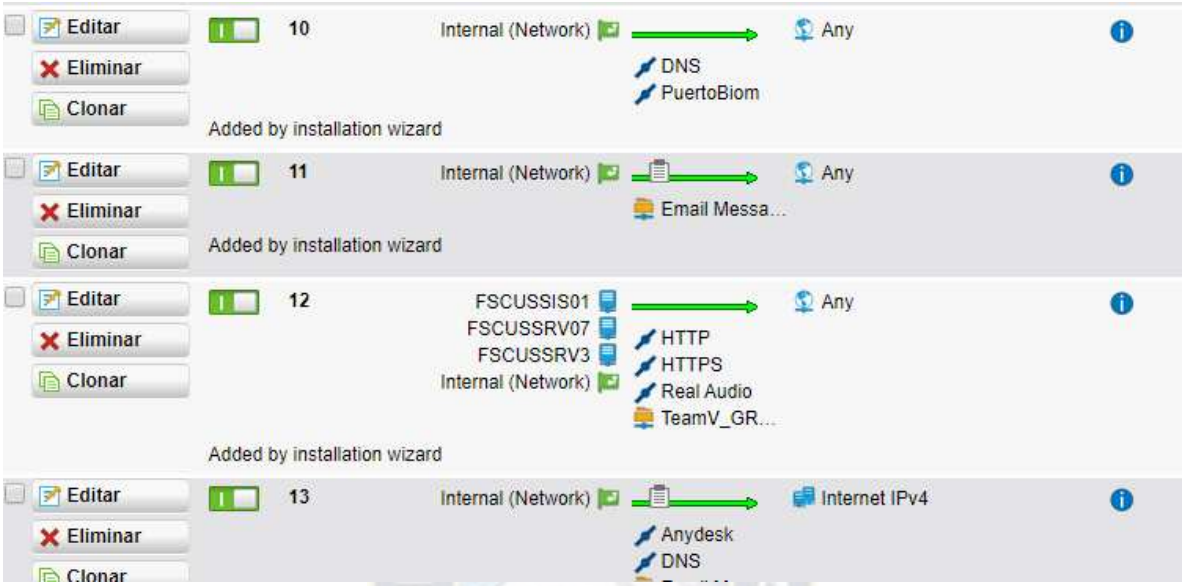


Figura 3.30 Habilitación de reglas de Cortafuego que permite dar permiso o denegar un servicio

Fuente: Propia

La administración vía consola es fácil debido a que simplemente bastará crear una nueva regla de Firewall en la Figura 3.31 se valida lo siguiente:

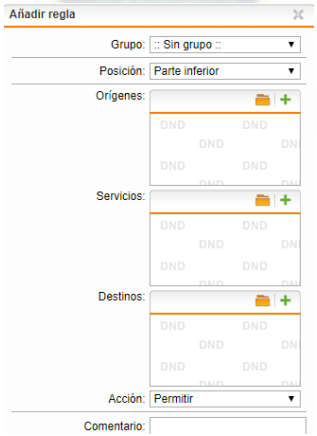


Figura 3.31 Nueva regla de Firewall

Fuente: Propia

Donde los siguientes parámetros deben ser configurados:

Grupo: Define si es Central o Sucursal

Orígenes: Son los equipos de la red de computadoras que están registrados en el AD.

Servicios: Son los servicios que se encuentran habilitados: DNS, IMAP, HTTP, SQL, ORACLE, POP3, VPN PROTOCOLS.

Destinos: Pueden ser direccionados a Servidores, equipo de computación, wan externa.

3.5.8. NAT

El enrutamiento del Servidor donde se encuentra el Core Bancario, fue configurado para que pueda ser visto únicamente por los equipos de la red (Central y Sucursal) y no así vista por el exterior (SNAT)

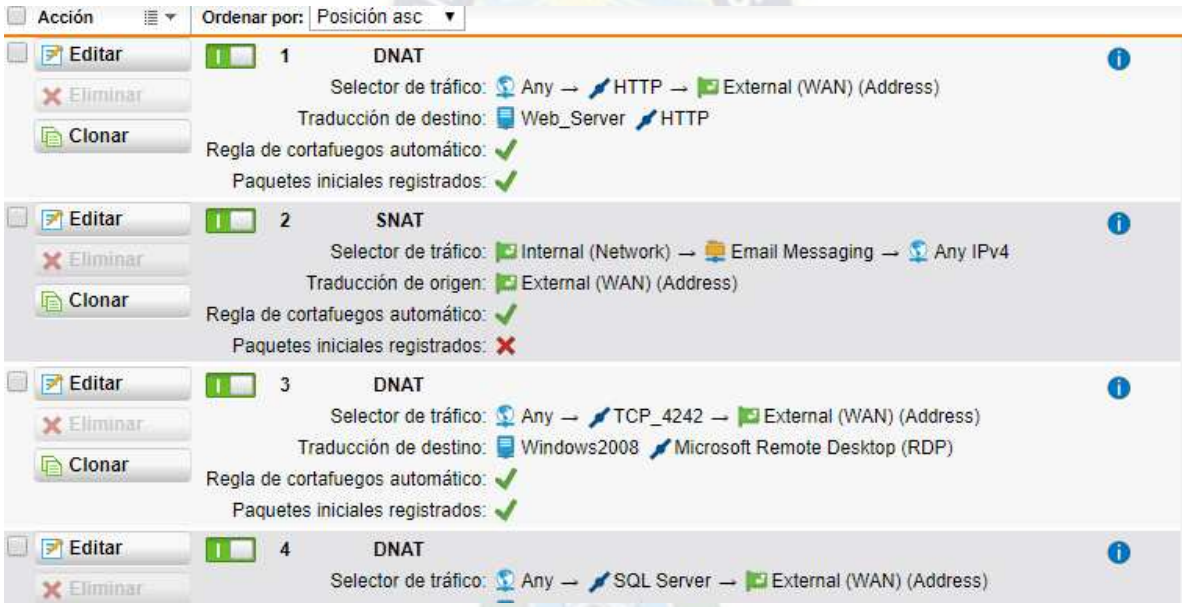


Figura 3.32 NAT

Fuente: Propia

3.5.9. Web Protection

Se creó grupos de Filtrado Web y se dividió en grupos según la jerarquía. Los grupos habilitados son:

- Gerencia
- Directivos
- Administrativos
- Cajeros

Los que se encuentran en el grupo Gerencia, son aquellos que tienen navegación sin restricciones y acceso total de los sistemas, el grupo Directivos tiene acceso nivel medio; acceso limitado; el grupo administrativo tiene acceso solo al correo; el grupo cajeros tiene acceso solo al módulo de operaciones del Core Bancario. Por otra parte, todos los grupos tienen acceso a los módulos correspondientes del Core Bancario.

3.5.10. Conexión de Acceso Remoto a la infraestructura de la Oficina Central de la Sucursal

Para la conexión de acceso remoto desde la Sucursal de la Cooperativa hacia la Oficina Central se cuenta con un software propio del Sophos Firewall con la única condición que deben estar encendidos en cada oficina los firewalls y la conexión a través del Protocolo IPSEC que nos permite encriptar la información de un punto a otro punto y también permite interactuar en la capa 3 del modelo OSI de redes.

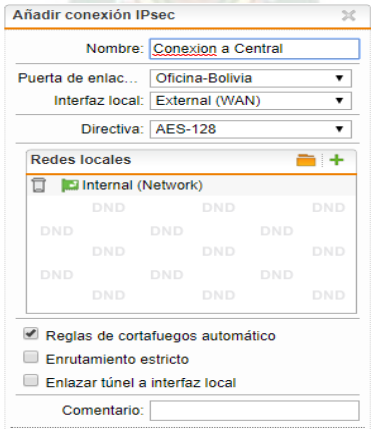


Figura 3.33 Acceso Remoto

Fuente: Propia

3.5.11. Gestión Remota entre la oficina Sucursal y la Oficina Central

Dentro de la solución implementada configuramos dos Firewall's Sophos SG 125w los mismos que tienen las mismas políticas, estas permitirán la gestión remota entre las oficinas y además la comunicación encriptada. El Sistema Bancario (Core Bancario) gracias a esta solución de red implementada se encuentra protegida al igual que los servidores correspondientes al esquema mostrado.

La gestión remota de protección puede ser accedida desde cualquier navegador y con el usuario y contraseña correspondiente al administrador puede tanto en el Firewall de la Central y Sucursal administrar las políticas remotamente.

3.5.12. Capacidad de conexión de usuarios de la red inalámbrica Meraki.

El ancho de banda está estimado en función de la capacidad de usuarios que cada MR26 y la capacidad de usuarios de los puntos de acceso MR66 posee:

Ancho de banda

$$AB = G * C$$

Ecuación 3.1. Fórmula para calcular ancho de banda en función de la capacidad de usuarios

Dónde:

AB = Ancho de banda a contratar N = Cantidad de usuarios que utilizan Internet

G = Ancho de banda a garantizar por usuario. Este valor es muy importante. Al bajar un archivo cuanto ancho de banda se quiere que consuma. Un valor en Latinoamérica puede ser quizás 256 Kbps.

C = Concurrencia de las personas (cantidad de personas que utilizan Internet simultáneamente) supongamos que el 50 % de los 360 usuarios usan el internet simultáneamente.

Calculo Usuarios MR26

N=270 (usuarios) G=256 Kbps (ancho de banda "garantizado" por usuario)

C =0.50*270=135 (Estimamos que 135 personas estarán conectadas simultáneamente a Internet).

AB = *135 * 256 Kbps* = 34560 Kbps que equivale a 34,56 Mbps

Por lo tanto, como son 2 puntos de acceso inalámbricos para interiores el total de ancho de banda necesario es de 69120 Kbps que equivale a 69.12 Mbps.

Capacidad de usuarios	Capacidad de ancho de banda
1 enrutador marca MR26 cada uno con capacidad de 200 usuarios)	34.24 Kbps
Total	34.400 Kbps

Tabla 3.10. Capacidad de Ancho de Banda

Fuente: Meraki Cisco, s.f.

3.5.13. Diagrama de la nueva infraestructura Tecnológica

Esta nueva Infraestructura tecnológica es la que genera por la usabilidad de la nueva propuesta para la cooperativa USAMA. Dos firewalls Sophos conectados

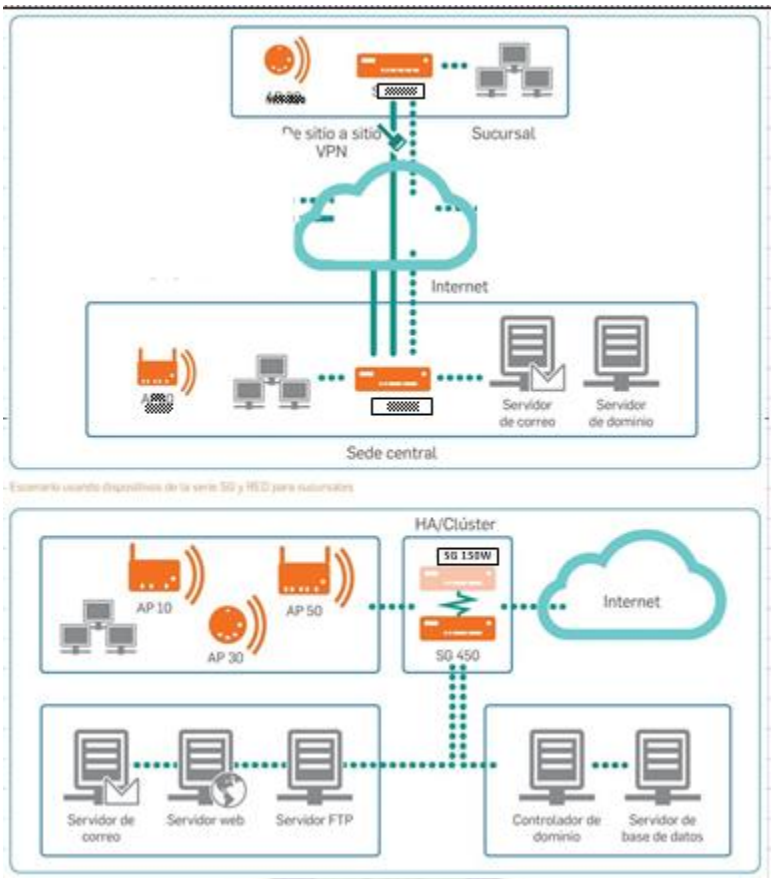


Figura 3.32 Esquema nuevo de conexión entre la Sede Central y su Sucursal

Fuente: Propia

CAPÍTULO IV

4. VALORACIÓN ECONÓMICA

Para el presente trabajo de investigación se empleará la metodología de análisis de costos. Cuando se implementa seguridad o adquisición de Infraestructura IT es necesario una fuerte inversión que se ve reflejada en la seguridad efectiva de los equipos y de la seguridad dentro de una Oficina. Es así que la Cooperativa USAMA ha decidido en el marco de resguardar la información de sus clientes en adquirir equipos de última generación para asegurar el perímetro de Servidores (oficina central) y Pc's de Escritorio (Oficina central y sucursal)

4.1. Canales de distribución:

La empresa IRET Bolivia cotizó la adquisición de los Firewall Sophos. Al igual que los router y switch de la marca Cisco. A fin de establecer el análisis de costos respectivo se cotizó los siguientes elementos:

- Sophos Firewall SG-125w (cantidad 2)
- Licencias para cada firewall (cantidad 2)
- Router Cisco Mr 26 (cantidad 2) a fin de utilizarlos en la Sucursal y Central para que pueda segmentar el uso del ancho de banda.
- Switch cisco ms 220 (cantidad 2)

4.2. Análisis de Costos

El presente subtítulo se divide en dos grupos de análisis los costos y el Beneficio final.

4.2.1. Costos Iniciales (capital)

La Cooperativa cuenta con los siguientes equipos que se encuentran inventariados en el área de administración y finanzas:

MODELO	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL $us
Equipos Pc's de Escritorio	32	800	25.600.-
Servidor Proliant ML310 Gen8	2	9.000	18.000.-
Switch y Routers (2000 – 2015)	10	50	500.-
Total			**44.100.-** (307.377 Bs)

Tabla 4.1. Costo de los equipos

Fuente: Propia

En la Cooperativa USAMA al momento de realizar el relevamiento de la información a nivel de red, se contaba con los equipos descritos en la **Tabla 4.1.** que en caso de querer montar la misma red se deberá tomar en cuenta los equipos necesarios para el funcionamiento.

4.2.2. Costos en Hardware

La Cooperativa USAMA deberá invertir en la adquisición de elementos de red para la implementación del presente proyecto.

MODELO	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL $us
Firewal Sophos SG 125 w	2	450	900.-
Switch Cisco MS-220	2	250	500.-
Router Cisco MR - 26	2	350	700.-
Total			**2.100.-** (14.637 Bs)

Tabla 4.2. Costo de implementación a nivel de Hardware

Fuente: Propia

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL $us
Licencia de Firewall Sophos	2	300	600.-
Total			**600.-** (4.182 Bs)

Tabla 4.3. Costo de implementación a nivel de Software

Fuente: Propia

4.2.3. Costos de Redes

La Cooperativa USAMA deberá gastar anualmente un monto de dinero para el óptimo funcionamiento de su red en su Oficina central y sucursal:

DESCRIPCIÓN	CANTIDAD	PRECIO ANUAL BS	PRECIO TOTAL BS
Internet de velocidad Mínimo de 8Mb	2	3.420	6840.-
Servicios eléctricos	2	1.800	3.600.-
Total en Bs			10.440.-
Total en USD			**1.498.00**

Tabla 4.4. Costo de implementación a nivel de Redes

Fuente: Propia

4.2.4. Beneficio

Es beneficioso para la Cooperativa contar con los equipos mencionados en la tabla 4.1 ya que el costo final para la implementación del presente proyecto es de USD: 4.198.- (Bs. 29.260).

CAPÍTULO V

5. CONCLUSIONES RECOMENDACIONES

5.1. Conclusiones

Como se mencionó en la introducción del presente trabajo de investigación, el estudio se desarrolló según los objetivos específicos planificados. Por lo tanto, ahora es importante extraer conclusiones sobre el diagnóstico realizado y concluir con algunas recomendaciones, para que constituyan un valor añadido para el desarrollo de la investigación realizada.

Se diagnosticó la situación actual de los problemas detectados los cuales eran: la intermitencia del servicio de red, falta de seguridad encriptada en la información entre la sucursal y la oficina central.

A través de un análisis de riesgo en tecnología realizado se explicó a la Cooperativa los riesgos tecnológicos que se tenía al no tener implementado una buena infraestructura de red correspondiente a la seguridad perimetral y acceso remoto entre las oficinas Central y Sucursal.

En el análisis técnico comparativo de las soluciones de Firewall, se determinó que las dos soluciones tienen como objetivo la gestión de la red en todo el ciclo de vida en cuanto a su administración y control; la diferencia técnica de estas soluciones radica por la forma de como gestionan la red; donde Sophos Firewall lo realiza de una forma centralizada y desde un sitio físico matriz mediante un software de control que maneja interfaces que no requieren de una capacitación especializada; a diferencia de la Solución de Cloud Meraki que gestiona la red desde la nube, mediante un software que en caso de desconexión o no acceso al Internet no se contará. En cambio, en el caso del Sophos, se puede administrar de forma remota y a través del software del mismo Firewall (Ver **manual del Usuario VPN**)

Así también bajo el cumplimiento del presente objetivo se planifico un modelo de gestión remota con el fin de detallar con exactitud el parámetro de cobertura del sistema. El cual representaba el principal problema entre la oficina central y la oficina sucursal y por ello

también el flujo de información (Core Bancario) no cumplían con normas establecidas por la ASFI, y Normas de protección a nivel de la capa 3 de transporte.

En la actualidad, el Core Bancario que es consultado por la Sucursal viaja protegido y tiene seguridad SSL porque no puede ser visto desde ningún equipo conectado desde afuera de las dos redes LAN (Central y Sucursal) de la Cooperativa.

Cuando llego el momento de decidir cuál de las soluciones tecnológicas es la mejor no solamente a nivel de costos, sino también a nivel técnico (ver cuadro comparativo de firewalls **Tabla 3.5. Análisis de resultados entre Firewall**). La principal característica del Sophos Firewall es la conexión remota y seguridad IPSEC comparado con el Firewall Cisco Meraki.

En el caso de los router's Meraki son equipos de fácil administración y permitirán el control del ancho de banda que se tiene en la oficina central y sucursal (Ver **Figura 3.22 Propuesta de red de la Cooperativa USAMA LTDA**).

En el caso de los dos firewalls (Oficina central y sucursal) se han instalado y configurado políticas de seguridad perimetral a nivel de cortafuegos, seguridad VPN, grupos de seguridad web, NAT para el manejo del Core Bancario, y además de la configuración necesaria para realizar la gestión remota de las políticas y control de seguridad perimetral.

La Arquitectura de red diseñada proporciona tolerancia a fallos, escalabilidad, calidad de servicio y seguridad, permitiendo la administración eficiente de la información para proveer los servicios de IT a los usuarios de la red.

Las soluciones implementadas responden a los estándares de red adecuados y permiten la protección y encriptación de la información.

Con los firewalls en cada oficina instalados logra levantar las observaciones que tenía la Cooperativa en temas de seguridad perimetral y de red; la información viaja encriptada y protegida bajo protocolos SSL de comunicación.

5.2. Recomendaciones

- El Departamento de sistemas debe crear políticas de uso de sus recursos tecnológicos para que el diseño propuesto de la red sea sostenible y eficiente en el aprovisionamiento de servicios de IT en cuanto al trasporte de la información por la red interna.
- Se deben crear las políticas de Administración de los Firewall Sophos instalados en la Cooperativa para tener un control de todas las políticas de seguridad implementadas y mejorar aquellas que se realizaron en beneficio de la Cooperativa.
- El Acceso remoto solo debe ser entre el túnel VPN (Protocolo IPSEC) y en caso muy extremo el uso de cliente VPN, para conectarse remotamente desde el exterior.
- Al incorporar políticas en los Firewall Sophos, dónde se estipulan accesos y restricciones de los usuarios hacia los servicios que les otorga la compañía, se deben mantener y tener constantemente actualizados las políticas de seguridad implementadas.
- Haciendo uso de los equipos Switch Meraki (QoS), se podrá controlar el ancho de banda dando prioridad a los usuarios que lo requieran más y a las aplicaciones y servicios. De esta manera también se mejora en la optimización de los empleados a sus actividades laborales, asegurando que las horas laborales sean aprovechadas para el desarrollo de la Cooperativa.
- Se recomienda manejar un programa continuo de capacitación de nuevas tecnologías en gestión y aprovisionamiento de red de los Firewall Sophos para contar con toda la experticia en el manejo de los mismos.

BIBLIOGRAFÍA

- [CHAMORRO, L. 2004] Chamorro Pietrosemoli, Lilian. **Ingeniera en Electrónica y Telecomunicaciones.** 2004.

- [CISCO INC. 2007-2008] Cisco Inc. (2007-2008). **CISCO Systems INC.**

- [CHUMACERO, J. 2004] Chumacero Zurita, Juan José. **Técnicas básicas para investigar en educación y ciencias sociales**. 2004. Pg. 62.

- [FERNANDEZ, P. 2008] Fernández, Pilco. A**puntes del curso de Sistemas de Comunicación (PUCP).** Lima: Pontificia Universidad Católica del Perú].

- [FOROUZAN, A. 2008] Forouzan, Behrouz A. 2008. **Transmisión De Datos Y Redes De Comunicaciones**. España: McGraw-Hill.

- [GEROMETTA, O. 2015] Gerometa, Oscar. **Guía de Preparación para el Examen de Certificación CCNA R&S 200-120.** 2015].

- [GÓMEZ, A. 2012] Gómez A. **Propuesta de Plan de Proyecto para el diseño e implementación de una red inalámbrica para el edificio principal de TI [Tesis para optar el grado de bachiller en Ingeniería de Sistemas]**. Costa Rica. Editorial: Científico – Técnica. 2012.

- [HERRERO, A. 2014] Herrero Perezrul, Adrian. **Sistemas operativos.** 2014.

- [LONDOÑO, M. 2012.] Londoño, Maria. **Un Archivador en la Nube**. Madrid: Fundación: Confemetal. 2012.

- [MERAKI. 2010] Meraki**. Nube Controladora Meraki**. 2010.

- [MERAKI, s.f.] Meraki, s.f. **Introduction to Cloud Networking.**

- [PADILLA, M. 2014] Padilla, Martín. **La Nube en Educación**. 2014.

- [PASQUEL, R. 2008] Pasquel R. **Análisis y diseño de la red de datos para la implementación del sistema de pensiones del IESS vía Web del Instituto Ecuatoriano de Seguridad Social [Tesis para optar el grado de bachiller en Ingeniería de Sistemas].** Ecuador. Editorial Científica – Técnica. 2008.

- [PEREIRA, S. 2008] Pereira S. **Diseño e implementación de una red de datos basado en una arquitectura de interconexión entre los campus Guaritos [Tesis para optar el grado de bachiller en Ingeniería de Sistemas].** Venezuela. Editorial – Científica. 2008.

- [PÉREZ, J. 2016] Pérez, Julian Porto. **Definición de sistema Homogéneo**. 2016.

- [PONCE, E. 2008] Ponce, Enrique. 2008. **Redes inalámbricas: IEEE 802.11.**

- [QUINTANA, P. 2007] Quintana P. **Diseño e implementación de una red piloto de telefonía IP en la Red Académica Peruana (RAP) usando software libre [Tesis para optar el grado de bachiller en Ingeniería de Sistemas].** Perú. Editorial – Científica. 2007.

- [RODRÍGUEZ, F. 1994] Rodríguez, Francisco. **Introducción a la metodología de las investigaciones sociales**. Ed. "Política". Cuba. 1994. Pág. 31.

- [VANEGAS, J. 2012] Vanegas Avendaño, Joe. **Tipos de Redes Alámbricas e Inalámbricas** (Universidad de las Fuerzas Armadas ESPE. Carrera de Telemática., 2012).

- [VELÁSQUEZ, M. 2005] Velásquez M. **Diseño e implementación de una red de cómputo para la empresa PETRO-TECH [Tesis para optar el grado de bachiller en Ingeniería de Sistemas]**. Piura. Editorial – Científica. 2005.

PAGINAS WEB

- [ADSI, s.f.] Adsi Análisis y Desarrollo de Sistemas de Información (s.f.). **Arquitecturas Tecnológicas.** Recuperado el 14 de agosto de 2018, de: http://the-peers.blogspot.com/2012/03/arquitectura-clienteservidor-definicion.html

  [ATPM. 2012] Atpm. 2012. **Wireless Network Encription.** Recuperado el 11 de marzo del 2018, de: http://www.atpm.com/8.04/wifi.shtml

- [BLAZQUEZ, s.f.] Blazquez. **Esquema Cliente Servidor en una Unidad de Información y Documentación.** Recuperado el 26 de septiembre de 2018, de: http://mblazquez.es/blog_ccdoc-automatizacion/esquemas/esquema-automatizacion-02.jpg

- [CARDENAS, P. 2006] Cardenas, Paolo Hernán. **Redes de nueva generación** Recuperado el 23 de septiembre de 2018, de: http://dspace.ups.edu.ec/bitstream/123456789/211/2/Capitulo%201.pdf

- [CASTRO, E. 2003] Castro, Edgar. 2003. **Redes inalámbricas**. Recuperado el 18 de agosto de 2018, de: http://boards5.melodysoft.

- [CCM, s.f.] CCM (s.f.). **Diferencias entre los protocolos TCP y UDP**. Recuperado el 02 de Julio de 2018, de: https://es.ccm.net/faq/1559-cual-es-la-diferencia-entre-los-protocolos-tcp-y-udp

- [CCM, 2017] CCM. 2017. **Protocolo IP.** Recuperado el 25 de octubre de 2018, de: http://es.ccm.net/contents/274-protocolo-ip

- [CIO-Latino.com, 2007] CIO-Latino.com. 2007**. ¿Qué es Storage?** Recuperado el 05 de enero de 2018, de: http://www.consultor-it.com/articulo/44001/que-es-storage CIO-Latino.com

- [CISCO, s.f.] Cisco (s.f**.**) **Access Points**. Recuperado el 15 de junio de 2018, de: http://www.cisco.com/c/en/us/products/wireless/access-points/index.html#~featured

- [CISCO, s.f.] Cisco (s.f**.**) **Cisco 2500 Series Wireless Controller Data Sheet**. Recuperado el 20 de octubre de 2018, de: http://www.cisco.com/c/en/us/products/collateral/wireless/2500-series-wireless-controllers/data_sheet_c78-645111.html

- [CISCO, s.f.] Cisco (s.f**.**) **Cisco Aironet 1130 AG Access Point.** Recuperado el 28 de mayo de 2018, de: http://www.cisco.com/c/en/us/products/wireless/aironet-1130-ag-access-point/index.html

- [CISCO, s.f.] Cisco (s.f**.**) **Cisco Aironet 2700 Series Access Points.** Recuperado el 1 de octubre de 2018, de: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2700-series-access-point/datasheet-c78-730593.pdf

- [CISCO, s.f.] Cisco (s.f). **Cisco Prime Infrastructure**. Recuperado el 15 de Junio del 2018, de: https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html

- [CO. CASTLE, 2008] CO. CASTLE. 2008. **The Experts In Building Solutions.** Recuperado el 14 de marzo de 2018, de: http://www.castleol.com/datacenter.html

- [CRESPO, A. s.f.] Crespo, Adrián. **Todo lo que necesitas saber sobre filtrado de mac de un router.** Recuperado el 14 de marzo de 2018, de: https://www.redeszone.net/2018/05/05/filtrado-mac-router/#disqus_thread

- [DEL RAZO, M. 2004] Del Razo, Minerva. 2004. **Redes inalámbricas en Boletín Tress.** Recuperado el 14 de enero de 2018, de: http://www.tress.com.mx/boletin/junio2004/redes.html

- [ESPINOZA, D. s.f.] Espinoza Rodriguez, Diana Valeria (s.f.). **Administración de red.** Recuperado el 16 de marzo de 2018, de http://mantepreventivo.blogspot.com/2011/02/administracion-de-red.html

- [FUNDACION UNIVERSITARIA, s.f.] Fundacion Universitaria (s.f.). **Redes Multiservicios.** Recuperado el 23 de febrero de 2018, de: http://redesmultiservicios.weebly.com/

- [GONZÁLEZ, O. 2006] Gonzáles, Oscar. 2006. **UIT/BDT Seminario regional sobre Costes y Tarifas para los países miembros del Grupo TAL.** Recuperado el 22 de febrero de 2018, de: https://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/rio_de_janeiro-06/gonzalez-1-sp.pdf

- [IHS, s.f.] IHS (s.f.). Las Redes de la Próxima Generación Comienzan a Transformar las Comunicaciones. Recuperado el 12 de octubre de 2018, de: http://www.ihs.com/news/uit-es-ngn-telecom-9-07.html

- [ITU, s.f.] ITU (s.f.). **ITU-T's Definition of NGN.** Recuperado el 12 de octubre de 2014, de: http://www.itu.int/en/ITU-T/gsi/ngn/Pages/definition.aspx

- [MARTÍN, E. 2014.] Martín, Eduardo. 2014. ¿**Qué es 'cloud computing'? Definición y concepto para neófitos.** Recuperado el 23 de abril de 2018, de:

http://www.ticbeat.com/cloud/que-es-cloud-computing-definicion-concepto-para-neofitos/

- [MERAKI CISCO, s.f.] Meraki Cisco (s.f.). **Cloud Managed Wireless.** Recuperado el 24 de mayo de 2018, de: https://Meraki.cisco.com/products/wireless

- [MERAKI CISCO, s.f.] Meraki Cisco (s.f.). **MX Cloud Managed Security Appliance Series.** Recuperado el 29 de mayo de 2016, de: https://meraki.cisco.com/lib/pdf/meraki_datasheet_mx.pdf

- [OSORES, M. 2013] Osores, Melisa. 2013. **Retos del networking en América Latina: El futuro de las redes.** Recuperado el 4 de abril de 2018, de http://searchdatacenter.techtarget.com/es/cronica/Retos-del-networking-en-America-Latina-El-futuro-de-las-redes

- [RIOS, R. & FERMIN, J. 2009] Ríos, Rene & Fermín, José. 2009. **ANÁLISIS DE TRÁFICO DE UNA RED LOCAL UNIVERSITARIA.** Recuperado el 26 de mayo de 2018, de: http://publicaciones.urbe.edu/index.php/telematique/article/viewFile/869/2145

- [SILVERFENIX BLOG. 2010] Silverfenix Blog. 2010. **Tipos de cables para redes de área local (LAN)**. Recuperado el 12 de mayo de 2018, de: https://silverfenix7.wordpress.com/2010/03/22/tipos-de-cables-para-redes-de-area-local-lan/

- [SLIDESHARE, 2014] Slideshare. 2014. **La Convergencia Tecnológica.** Recuperado el 12 de Mayo de 2018, de: http://es.slideshare.net/BMGtecno/la-convergencia-tecnolgica

- [SOPHOS, s.f.] **SOPHOS (s.f.).** Recuperado el 15 de agosto del 2019, de: https://www.sophos.com/es-es/products/unified-threat-management/tech-specs.aspx

- [SOPHOS, s.f.] SOPHOS (s.f.)**. Modelos de escritorio SG**. Recuperado el 16 de agosto del 2019, de: https://www.sophos.com/es-es/products/unified-threat-management/tech-specs.aspx#DesktopModels

- [THE SIEMON COMPANY, s.f.] The Siemon Company (s.f.). **High Speed Interconnects.** Recuperado el 27 de enero de 2018, de: http://www.siemon.com/

- [UOC UNIVERSIDAT OBERTA DE CATALUNYA, s.f.] UOC Universidat Oberta de Catalunya (s.f.). **Infraestructura tecnológica**. Recuperado el 9 de febrero de 2018, de: http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

- [UPS, s.f.] UPS (s.f.). **Comparación de la evolución de las redes tradicionales a redes NGN.** Recuperado el 3 de marzo de 2018, de: dspace.ups.edu.ec/bitstream/123456789/170/3/Capítulo%202.pdf

- [VMWARE. 2014] VMware. 2014. **Virtualice su infraestructura.** Recuperado el 7 de abril de 2018, de: https://pro-it.es/virtualice-su-infraestructura/

- [WIRESHARK, s.f.] Wireshark (s.f.). **Learn Wireshark.** Recuperado el 12 de Mayo de 2018, de: https://www.wireshark.org/#learnWS

GLOSARIO DE TÉRMINOS

AES. - Estándar de Encriptación, que utilizan centenares de millones de personas en el mundo en aplicaciones como las operaciones bancarias por internet, las comunicaciones inalámbricas.

Cisco Meraki. - Construye redes inteligentes administradas a través de la nube que simplifican considerablemente las redes empresariales. Tanto para una empresa o para cubrir un campus con redes inalámbricas, las redes Meraki simplemente funcionan.

Firewall (cortafuegos). - Es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

Múltiple entrada, múltiple salida (Mimo). - Es una tecnología de radio comunicaciones que se refiere a enlaces de radio con múltiples antenas en el lado del transmisor y del receptor.

Red de Área Local (LAN). - Una red de comunicaciones de datos que enlaza computadoras que permite la comunicación en un área de 200 metros.

Red de Área Metropolitana. - Es una red de comunicaciones que cubre una porción grande de una ciudad o de un campo grande.

Red privada virtual (VPN), de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

WAN (Red de Área Amplia). - Es una red que conecta dos o más redes de área local (LAN) en ciudades múltiples vía líneas de teléfono.

WPA2 (Acceso protegido para red inalámbrica). - Protocolo de encriptación más robusto que el protocolo de equivalencia con red cableada (WEP). Básicamente, la diferencia entre un protocolo y otro es que WPA2-PSK soporta una clave de hasta 63 caracteres alfanuméricos.

ANEXOS

ANEXO A

ESPECIFICACIONES TÉCNICAS DEL MODELO MR-26

ESPECIFICACIONES TECNICAS	
Radios	Una radio 802.11b/g/n de 2,4 GHz, una radio 802.11a/n de 5 GHz y una radio dedicada para WIPS de doble banda y análisis del espectro
	Funcionamiento simultáneo de las tres radio
	Rendimiento máximo de 900 Mbit/s
Capacidades de 802.11n	Varias entradas 3 x 3, varias salidas (MIMO) con tres transmisiones espaciales
	Canales de 20 y 40 MHz, Agregación de paquetes.
Potencia	Alimentación por Ethernet: 37-57 V (compatible con 802.3af).
	Consumo de energía: 13,7 W máx.
	El inyector de alimentación por Ethernet y el adaptador de CC se venden por separado.
Montaje	Todo el equipo de montaje estándar incluido, montaje en escritorio y pared
Seguridad física	Tornillo de seguridad incluido, Bahía de cables contra las manipulaciones, Placa de montaje oculta.
Medio ambiente	Temperatura de funcionamiento: 0 °C a 40 °C (32 °F a 104 °F) Humedad: 5 a 95% sin condensación
Interfaces	1 PoE 802.3af 100/1000Base-T Ethernet (RJ45) con 48 V CC 802.3af
	1 conector de alimentación de CC (5 mm x 2,1 mm, positivo al centro)
Seguridad	Firewall con política integrada (Identity Policy Manager) Políticas de dispositivos móviles
	Air Marshal: WIPS en tiempo real (sistema de prevención de

	intrusiones inalámbricas) con alarmas
	WEP, WPA, WPA2-PSK, WPA2 empresarial con 802.1X
	Cifrado TKIP protocolo de encriptación provisional introducida con WPA para reemplazar el cifrado WEP y AES protocolo de cifrado avanzado más seguro e introducida con WPA2, que sustituyó al estándar WPA provisional. Se trata de un cifrado estándar muy seguro,
Calidad de servicio	Calidad de servicio inalámbrico (Wi-Fi Multimedia. WMM/802.11e) ,Función avanzada de ahorro de energía (U-APSD) , Punto de código de servicios diferenciados (DSCP) (802.1p) Firewall y Modelado del tráfico de aplicaciones de capa 7.
Movilidad	Compatibilidad con credenciales PMK y OKC para roaming rápido de capa 2 802.11r y 802.11k Roaming de capa 3
Indicadores LED	1 conectividad Ethernet 1 estado de actualización de potencia/arranque y/firmware
Garantía	Garantía de hardware de por vida con repuesto avanzado incluido

Fuente: Datasheet MR26

ANEXO B

MANUAL DE USO DEL FIREWALL

1. Introducción

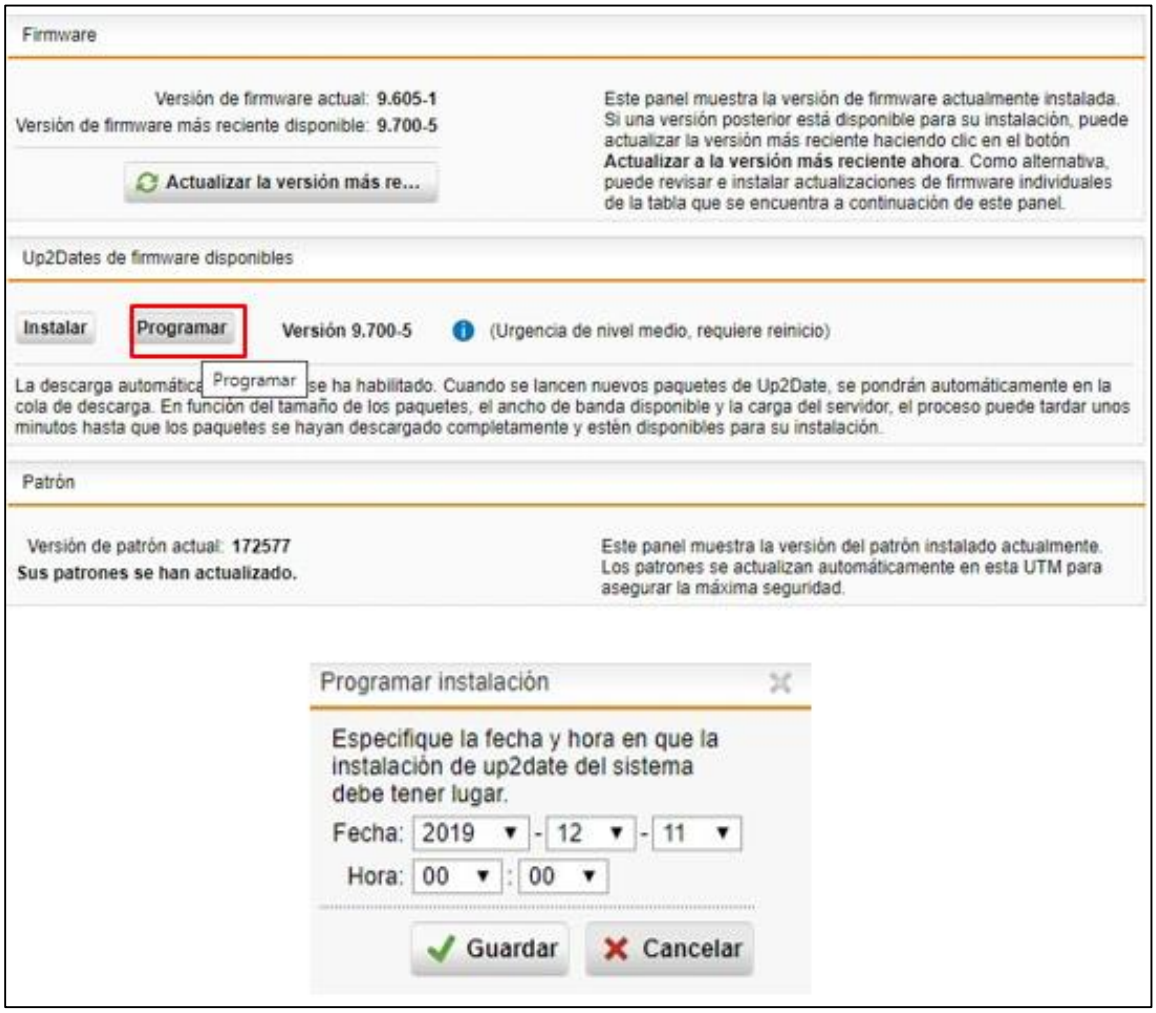
Los dispositivos de la serie SG de Sophos están diseñados para proporcionar el equilibrio optimo entre rendimiento y protección, para diversos entornos TI. Independientemente de si necesita una solución para una pequeña oficina remota, o proteger una escuela, o si es una organización global que requiere una alta disponibilidad y características de nivel empresarial, el firewall que usa la Cooperativa USAMA es el modelo SG-125w.

2. Acceso al Firewall

El acceso al sistema es mediante un navegador web, en donde se debe ingresar una dirección, en caso de estar dentro de la cooperativa se usa https://192.168.1.4:4444 y remotamente se puede ingresar a través de una dirección establecida por el administrador de redes o el encargado de sistemas. Cada vez que se logra ingresar se observa las actualizaciones, licencias y estado del Firewall.

Fuente: Propia

Nótese que en “Información de versión” se tiene una actualización disponible, la cual, debe ser programada en un horario fuera de oficina para que la velocidad de flujo de datos entre ambas agencias no se vea afectada.



Fuente: Propia

3. Gestión de usuarios

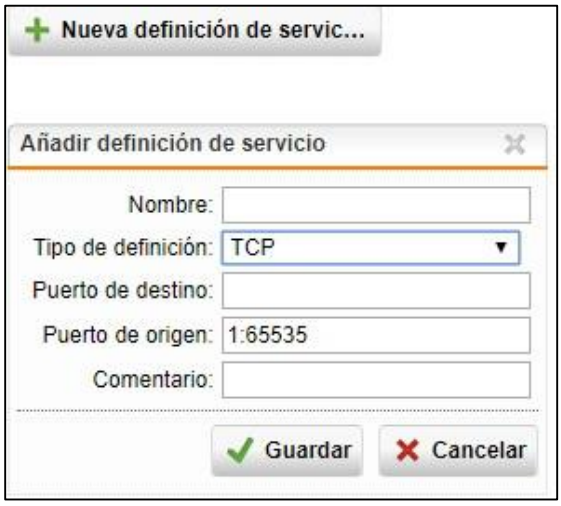
La gestión de usuarios o el acceso de los usuarios a la red de Cooperativa USAMA se encuentra establecido por la asignación de ip y su respectiva mac address. Para habilitarlo en la red se deben seguir tres pasos:

- En el equipo que desea habilitar, buscar el mac address
- Ingresar a Definiciones y usuario > Definiones de Red, y llenar los siguientes parámetros: Nombre, IP y la dirección MAC del equipo que quiere habilitar.

Fuente: Propia

4. Definición de Servicio:

Se refiere a la habilitación de protocolos o puertos UDP/TCP, los mismos permitirán agregar un servicio el cual puede ser UDP, TCP, TCP/UDP, ICMP, IP, ESP, AH. Para poder configurar se debe acceder a Definiciones y Usuarios > Definiciones de Servicio > Nueva Definición.



Fuente: Propia

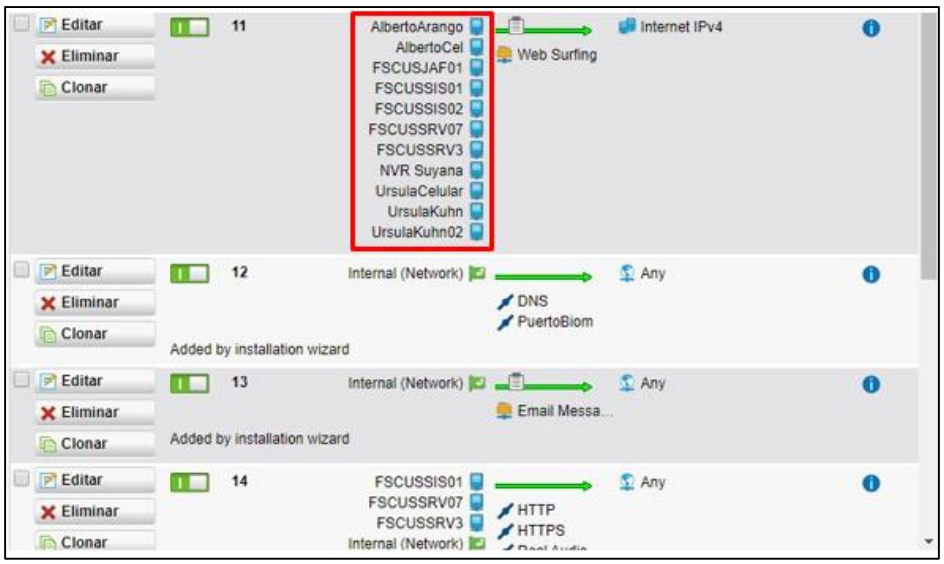
5. Interfaces y enrutamiento

Físicamente el Firewall tiene puertos de comunicación establecidos: WAN, LAN, DMZ, y para poder habilitarlos se deberá ir a Interfaces y Enrutamiento > Interfaces para poder así habilitar dichas interfaces.

Fuente: Propia

6. Reglas de cortafuego y enrutamiento NAT

En Network Protection / cortafuego existen ya implementadas varias reglas para permitir o denegar los servicios, entre los cuales, la principal regla es el acceso full a internet, misma que se encuentra reservada solamente para personal jerárquico de la Coopertativa USAMA (directores, Jefe Administrativo Financiero y otros funcionarios con previa autorización por correo electrónico).



Fuente: Propia

Como se observa, se deben agregar los equipos que tendrán permitido el ingreso a full internet sin ninguna restricción.

El enrutamiento NAT, es aquel que permitirá el acceso de los Servidores de Información, los cuales se requieren para el manejo exterior, por ejemplo, las reglas del Sistema de Coordinacion "SICO" que fueron configuradas de la siguiente manera.

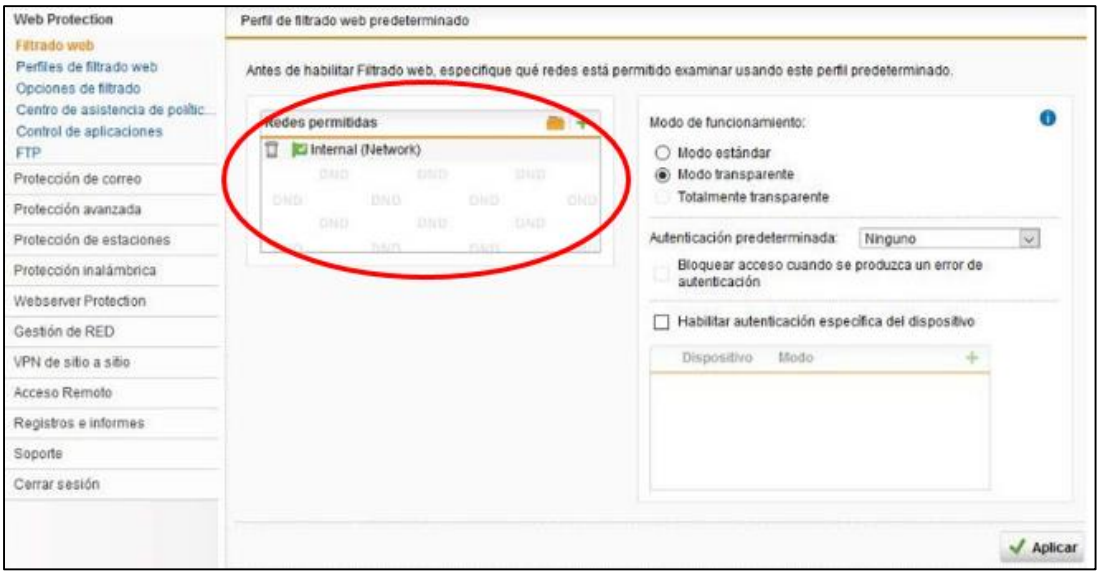
Fuente: Propia

Para poder configurar se debe ingresar a Network Protection / NAT, y completar de acuerdo a las políticas que se desee.

Fuente: Propia

7. WEB PROTECTION

Filtrado Web:



Fuente: Propia

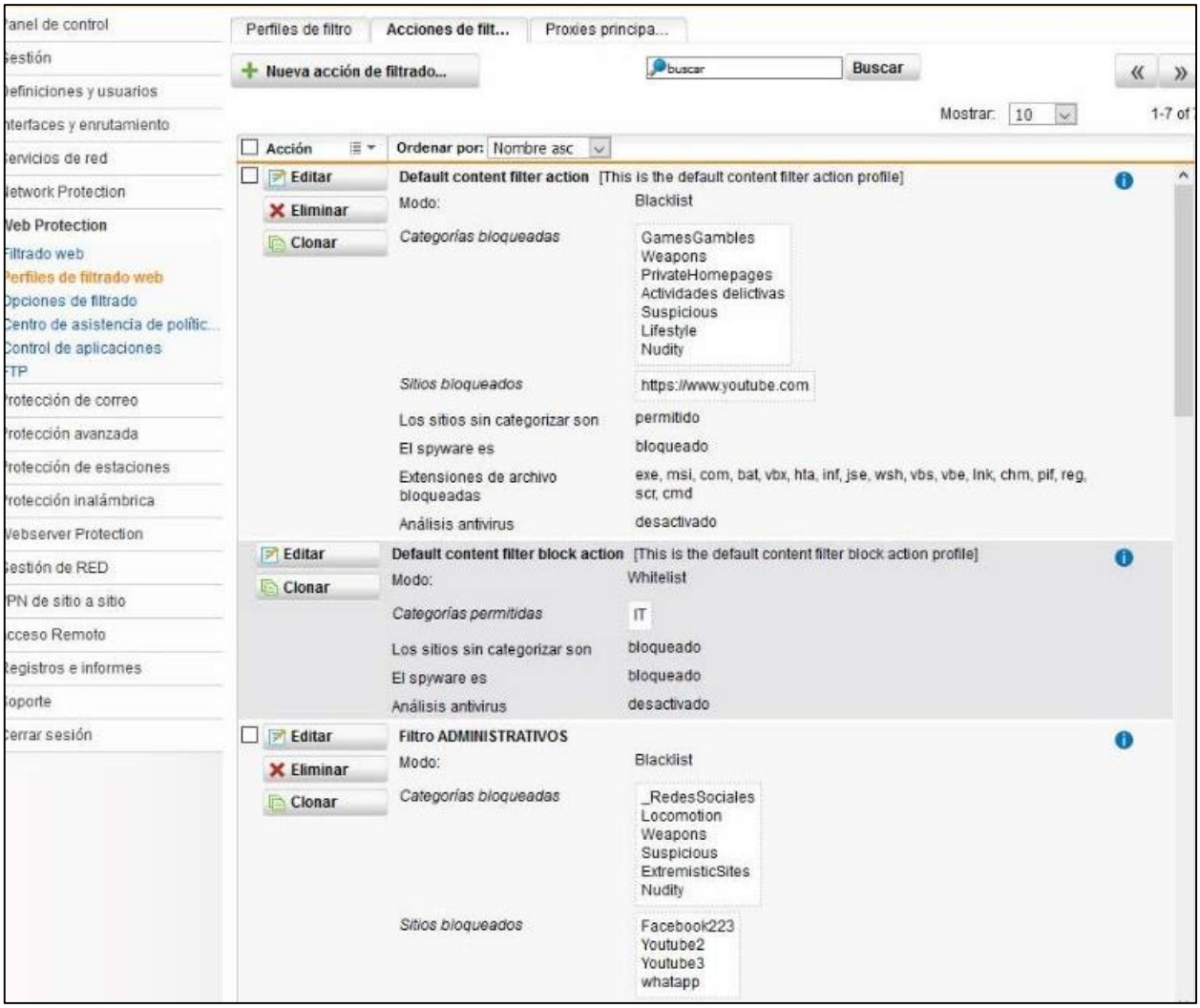
HTTPS: En este apartado se debe añadir todo tipo de formatos que se desee filtrar, se sugiere filtrar direcciones web.

Fuente: Propia

Directivas: Se establecen las directivas para cada grupo de usuarios, así como los filtros para cada usuario o red, se debe determinar que políticas de acceso se aplican a cada grupo.

Fuente: Propia

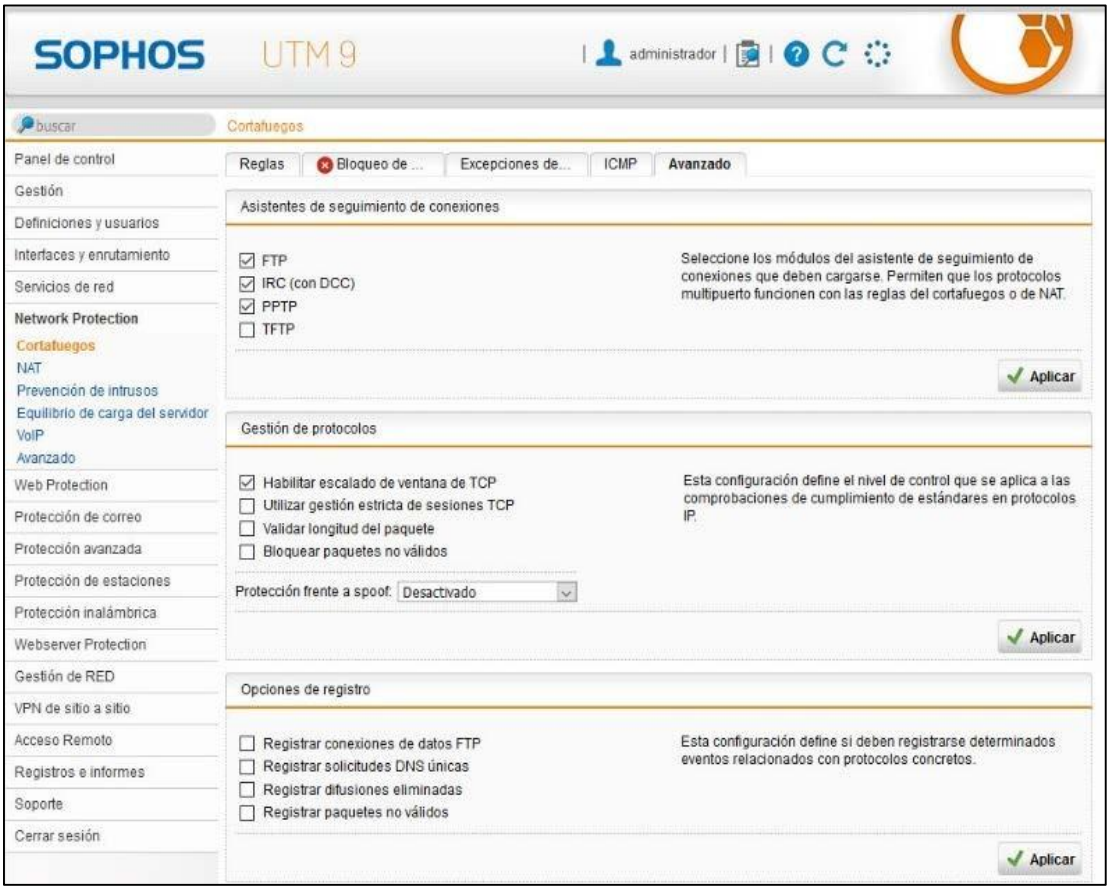
Perfiles de filtrado web: Dentro de cada perfil se puede añadir en una lista negra todas las paginas a filtrarse.



Fuente: Propia

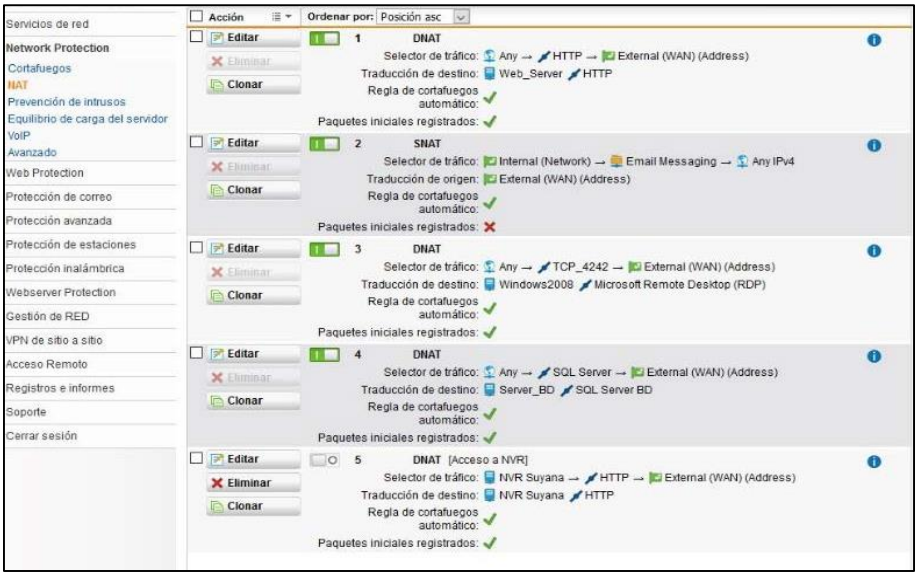
8. Network Protection

Cortafuegos. - Permite la asignación de protocolos, permitiendo o denegando accesos dependiendo del servicio a ser habilitado en la LAN, WAN, por ejemplo, el nateo del sistema SICO.



Fuente: Propia

Nateo del Sistema. - En esta opción se determina, que el servidor del SICO deberá salir por el firewall habilitando el servicio NAT del firewall. En el cual se incluye el acceso a la base de datos para la sincronización desde los equipos móviles.



Fuente: Propia

El firewall permite obtener reporte del uso de servicios y aplicaciones para realizar un seguimiento y monitoreo de las actividades realizadas por los usuarios de la cooperativa al conectarse a Internet.

Fuente: Propia

Los reportes que se generan siempre están de acuerdo a la forma de la configuración de la distribución de los mismos, forma que se quiere que se reporten y periodicidad con la q se requieren. Los reportes están configurados para generarse diariamente, semanalmente y mensualmente, dichos reportes son importantes porque puede ser un importante recurso a la hora de detectar ataques externos e internos dentro de la red.