FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

REDISEÑO DE LA RED DE COMUNICACIONES PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GONZALO PIZARRO

AUTOR

DARÍO XAVIER LONDOÑO JUMBO

AÑO

2017

FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

REDISEÑO DE LA RED DE COMUNICACIONES PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN GONZALO PIZARRO.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Electrónica y Redes de Información.

Profesor Guía

Mg. Ángel Gabriel Jaramillo Alcázar

Autor

Darío Xavier Londoño Jumbo

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Ángel Gabriel Jaramillo Alcázar

Magíster en Gerencia de Sistemas y Tecnologías de Información

CI: 1715891964

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

William Eduardo Villegas Chiliquinga

Máster en Redes de Comunicaciones

CI: 1715338263

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

_____

Darío Xavier Londoño Jumbo

CI: 2100543111

AGRADECIMIENTOS

A mis padres quienes han sido el pilar fundamental para seguir adelante con mis objetivos académicos.

DEDICATORIA

A Dios, a mis padres y a mi hermano

RESUMEN

El estudio de investigación se orientó a dar solución a los problemas que conectividad que existen en el Gobierno Autónomo Descentralizado del Municipio del Cantón Gonzalo Pizarro, para lo cual se desarrolló el rediseño de la red de conectividad. La investigación parte de una fundamentación teórica donde se estudió los enfoques de diseño de redes, las metodologías ciclo de vida de la red, las herramientas de análisis de red, protocolos, entre otros. La aplicación permitió evidenciar problemas de la institución mencionada en el acceso a la información y la urgencia de contar con nuevas aplicaciones que ayuden a mejorar los procesos internos y así dar una buena atención a los ciudadanos. La metodología utilizada es la PPDIOO, se presenta la fase de preparación en donde se realiza la recolección de información, análisis de requerimientos, las aplicaciones que se utilizan, cómo es la estructura de la Institución, cantidad de usuarios. En la fase de planificación, se realizó un análisis de las aplicaciones más importantes, los dispositivos que forman parte de la infraestructura de la red de conectividad, es decir estudiar la solución para la fase siguiente. La fase de diseño presenta los protocolos y configuración necesarios para satisfacer las necesidades del cliente, teniendo en cuenta que esta nueva red debe cumplir con parámetros de disponibilidad, escalabilidad, seguridad y con calidad de servicio. Por último se presenta un presupuesto referencial que asocia los dispositivos y medios necesarios para una posible implementación si la Institución lo considera pertinente. La propuesta del módulo de gestión presentada, permitirá centralizar el control y la administración de toda la arquitectura de la red de conectividad, ayudando a monitorear la red, actuar ante posibles fallas eficazmente y realizar tareas de auditoría y la correlación de eventos.

Palabras claves: Diseño de redes, conectividad, proyectos de tecnologías de la información, metodología PPDIOO, GAD Gonzalo Pizarro.

ABSTRACT

The research study was oriented to solve the connectivity problems that exist in the Decentralized Autonomous Government of the Municipality of Canton Gonzalo Pizarro, for which the redesign of the connectivity network was developed. The research starts from a theoretical foundation where studies of network design approaches, network life cycle methodologies, network analysis tools, protocols, among others. The application made it possible to highlight problems of the institution mentioned in the access to information and the urgency of having new applications that help improve the internal processes and thus give good attention to citizens. The methodology used is the PPDIOO, it presents the preparation phase in which the information is collected, the applications that are used, how the structure of the Institution, the number of users. In the planning phase, an analysis was made of the most important applications, the devices that are part of the infrastructure of the connectivity network and the analysis of the requirements, we study the solution for the next phase. The design phase presents the necessary protocols and configuration to satisfy the needs of the client, taking into account that this new network must comply with parameters of availability, scalability, security and quality of service. Finally, a reference budget is presented that associates the devices and means necessary for a possible implementation if the Institution considers it pertinent. The proposed management module will centralize the control and administration of the entire connectivity network architecture, helping to monitor the network, take action against possible failures effectively, and perform audit tasks and the correlation of events.

Keywords: Network design, connectivity, IT projects, methodology PPDIOO, GAD Gonzalo Pizarro.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El Cantón Gonzalo Pizarro como parte integrante de la división política de la provincia de Sucumbíos, aspira un estilo de gobierno con transparencia, inclusión y participación ciudadana como indicadores de su gestión. Para ello será necesario contar con una red informativa informática que permita a sus diferentes usuarios, tanto internos como externos, contar con información veraz y oportuna para que puedan tomar las decisiones necesarias en el marco de la gobernabilidad. Para ello el Gobierno Autónomo Descentralizado Municipal del Cantón Gonzalo Pizarro, debe contar con una red con aspectos de Velocidad, Seguridad, Confiabilidad, Escalabilidad y Disponibilidad que favorezcan la gestión municipal. La presente investigación cobra actualidad y pertinencia en virtud de los avances tecnológicos que dan a la conectividad un enfoque necesario para la comunicación institucional e interinstitucional, de cara a la interconexión de todos los usuarios con miras a compartir la información necesaria para disfrutar desde la modernidad, los avances en la administración de los servicios que cotidianamente impactan la vida de los habitantes de la localidad. Se pretende una evaluación tipo diagnóstico de carácter preliminar con miras a levantar toda la información de la red actual del Gobierno Autónomo Descentralizado Municipal del Cantón Gonzalo Pizarro y plantear todas aquellas mejoras que requieran y necesiten los actores y gestores para el uso adecuado y seguro de la información institucional a través de la red y si fuese necesario rediseñarla para su futura implementación.

DESARROLLO DEL PROYECTO DE TITULACIÓN

Definición del problema

En la actualidad la comunicación es un tema de interés para todas las organizaciones. Usuarios de diverso índole (internos y externos) requieren institucionalmente la información para tomar oportunamente las decisiones en un ambiente cambiante caracterizado por la incertidumbre y el riesgo. En este

sentido, la comunicación institucional en el marco de la seguridad y disponibilidad, de mano de los avances tecnológicos favorecen los niveles de información y comunicación a través de las infraestructuras de redes informáticas las cuales pueden definirse como “un conjunto interconectado de ordenadores, que ofrece a sus usuarios diversos servicios relacionados con las comunicaciones y el acceso a la información” (Adell, 1998).

Autores como Romero (2012) sostienen que “un buen diseño de la red informática es fundamental para evitar problemas de pérdidas de datos, caídas continuas de la red, problemas de lentitud en el procesamiento de la información y problemas de seguridad informática y crecimiento futuro de la red” (pág. 8).

También es importante considerar lo expuesto por Aguaiza (2016) citando a Juliá (2013) cuando expone que una red informática óptima debe considerar estas características: 1. Velocidad 2. Seguridad de la Red 3. Confiabilidad 4. Escalabilidad 5. Disponibilidad (pág. 15).

En este orden de ideas, el diseño de la red del Gobierno Autónomo Descentralizado Municipal del Cantón Gonzalo Pizarro (de ahora en adelante GADMCGP), observa algunas debilidades en el funcionamiento de las aplicaciones y acceso a los servicios externos, en un entorno seguro, lo que podría impedir la disponibilidad y comprometer la información almacenada en los servidores locales.

A continuación se detallan algunas de las observaciones que en aspectos organizacionales y tecnológicos a considerar para su mejora:

Problemas organizacionales

- Para el diseño e implementación de la red, no se han observado las buenas prácticas o un modelo de diseño de red. No existen políticas de seguridad que limiten el acceso al Internet y el uso indebido de los equipos informáticos.

- No existen políticas de seguridad, no se ha definido listas de control de acceso (*ACLs*), que permitan el ingreso a la información sólo a las áreas autorizadas.
- No hay reglas específicas que definan el uso adecuado de los recursos y equipos informáticos.
- El acceso a las redes sociales no está limitado y cualquier usuario puede acceder al Internet, poniendo en peligro la seguridad de la información e instalación de aplicaciones malintencionadas.

Alcance

La propuesta que tiene el presente proyecto, empieza desde un estudio detallado para la caracterización del modelo de negocio, los servicios internos de tecnología y conectividad que dispone el GADMCGP, y un nuevo diseño de la red de comunicaciones.
El objetivo principal de las actividades mencionadas anteriormente es lograr la actualización tecnológica de la infraestructura, para adaptarse a las nuevas tendencias, tener mayores velocidades de acceso, configuraciones de los dispositivos de núcleo, distribución y acceso, técnicas de control de acceso, seguridad de la información, calidad de servicio y por último un estimado de inversión para una posible implementación en dicha Institución en los primeros meses del año 2017.

Cabe indicar que la Institución dispone de una infraestructura de 3 pisos y posee una red de conectividad interna deteriorada, por lo tanto se hará el estudio completo a través de un diagnóstico técnico para evidenciar posibles insuficiencias, fallas o debilidades. Se presenta a continuación el alcance del proyecto:

- Estudio de la red requerida, considerando la topología, cantidad de usuarios por departamentos, dimensionamiento de equipos necesarios para los servicios o aplicaciones actuales usadas cotidianamente en la

Institución con la finalidad de hacer un diseño adecuado a las necesidades y nuevas tendencias.

- Diseño de la red interna, configurando todos los equipos en la búsqueda del mejor desempeño, y solucionando los requerimientos de la Institución.

Justificación

El nuevo diseño ofrecerá adaptarse a las nuevas tendencias con respecto a los medios de transmisión, altas velocidades de acceso hacia el Internet, respuestas rápidas ante posibles fallos en los equipos, obteniendo así calidad y eficiencia de los recursos gestionados a través de la red interna de la Institución.

Con el nuevo diseño de la red interna, se obtendrá los siguientes beneficios:

- Incrementar la disponibilidad de la informática mejorando su desempeño
- Sistema escalable, capaz de agregar o quitar dispositivos de red, servicios y actualizaciones que mejoran su rendimiento.
- Disponibilidad, una red configurada para resolver problemas ante posibles fallas, a través de la redundancia y agregación de enlaces.
- Seguridad, dispositivos de acceso que controlan la cantidad de usuarios que se conectan, y filtración de paquetes que puedan causar daños a los servicios internos,
- Calidad de servicio, dar prioridades al tráfico más importante como la voz y el video en la Institución a través de protocolos de calidad de servicio.

OBJETIVOS

Objetivo General

- Diseñar una nueva red de comunicaciones que sea escalable, segura, tolerante a fallas y con calidad de servicio, para una futura implementación en el GADMCGP.

Objetivos específicos

- Identificar los requerimientos del GADMCGP, aplicaciones, y equipos que forman parte de la infraestructura de la Red de Comunicación, y que son utilizados para el trabajo diario de los usuarios internos.
- Analizar la red de comunicación actual del GADMCGP y definir los requerimientos, definir los principales problemas que afectan el buen funcionamiento de la Red de Conectividad.
- Desarrollar el diseño lógico de la red LAN, y las configuraciones necesarias de los equipos.

1. CAPÍTULO I. MARCO TEÓRICO

1.1 Enfoques de diseño de redes

Existen varios enfoques cuando se trata del diseño de una red de datos, cada una propone fases importantes que dependiendo de cada autor, ayudan a que se establezca la conexión entre los dispositivos informáticos. Es muy importante el diseño de una red, porque será la base para adaptarse a las necesidades de las nuevas tendencias tecnológicas, tales como: incremento de

la velocidad en la transmisión de datos, seguridad de la información, protocolos de enrutamiento, estándares (Wang, 2013).

El enfoque de diseño se refiere al desarrollo de un sistema o método para una situación única. Hoy en día, el término se aplica más frecuentemente a los campos tecnológicos en referencia al diseño de páginas web, software o diseño de sistemas de información (Learn.org, 2017).

La clave del enfoque de diseño es encontrar la mejor solución para cada situación a diseñar, ya sea en el diseño industrial, la arquitectura o la tecnología. El enfoque de diseño hace hincapié en el uso de una lluvia de ideas para fomentar ideas innovadoras y el pensamiento de colaboración para trabajar a través de cada idea propuesta y llegar a la mejor solución.

Dar una solución a los requerimientos del usuario final es la preocupación más importante. Los enfoques de diseño también emplean métodos de investigación básicos, tales como el análisis y pruebas (Learn.org, 2017).

Si bien este enfoque se utiliza en muchas industrias, se aplica comúnmente en los campos de la tecnología, incluyendo los que utilizan internet, software y sistemas de información de desarrollo. Varios enfoques de metodología de diseño se han desarrollado en el sector tecnológico. Algunos enfoques de diseño de tecnología común incluyen:

El diseño *Bottom Up* es una metodología que comienza con los cimientos y trabaja hacia una solución.

1.1.1 Enfoque de diseño Top-Down

La metodología de diseño *Top Down* o por etapas de refinamiento se inicia desde la solución final y trabaja inversamente perfeccionando cada paso en el camino. El enfoque Top-Down tiene un enfoque de diseño, que comienza desde la capa superior del modelo OSI y trabajar hacia abajo. Comienza con los requerimientos de la Organización antes de mirar a las tecnologías.

1.1.1.1 Fase de análisis de requerimientos

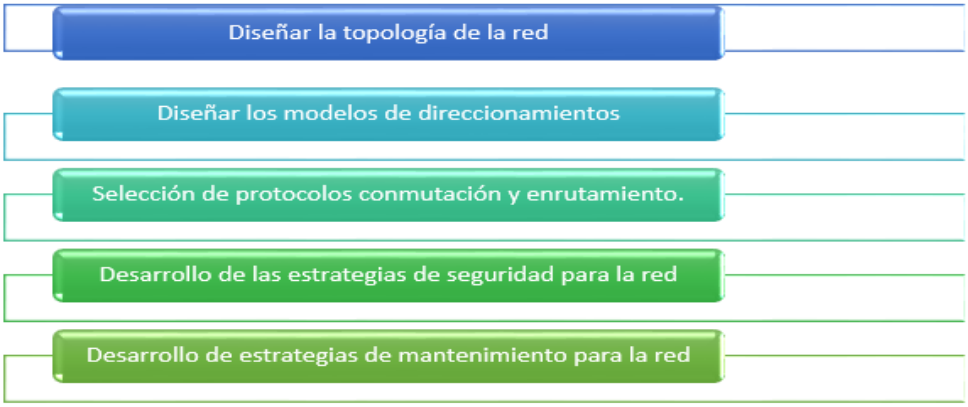

Figura 1. Fases de análisis del requerimiento
Tomado de (Learn.org, 2017).

1.1.1.2 Fase de diseño lógico de la red

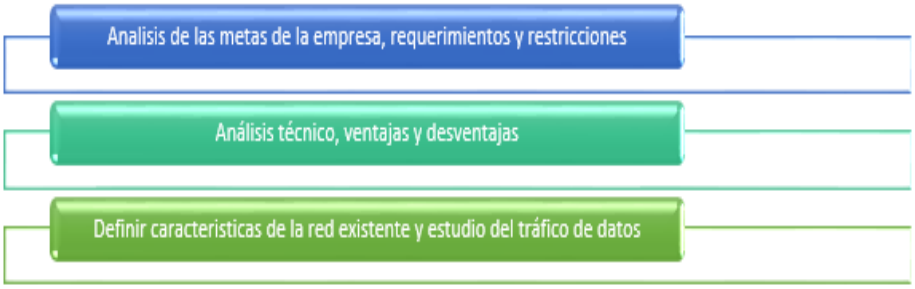

Figura 2. Fases de diseño lógico de la red (Learn.org, 2017).
Tomado de (Learn.org, 2017).

1.1.1.3 Fase de diseño de la red física

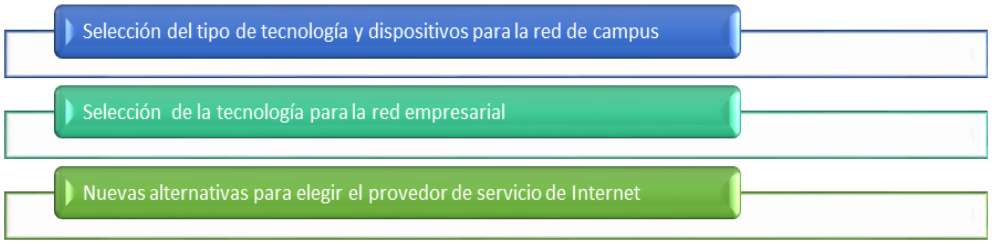

Figura 3. Fases de diseño de la red física
Tomado de (Learn.org, 2017).

1.1.1.4 Implementación, pruebas, optimización y documentación de la red

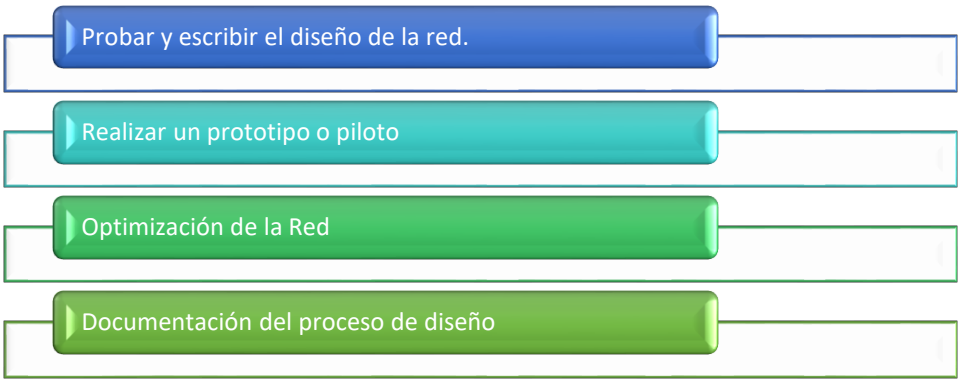

Figura 4. Implementación, pruebas, optimización y documentación de la red Tomado de (Learn.org, 2017).

1.1.2 Enfoque *Bottom Up*

El enfoque *Bottom Up* para solucionar un problema de red, comienza con los componentes físicos de la misma y se abre camino hasta las capas del modelo OSI. Si la conclusión de que todos los elementos asociados a una capa particular, están en buenas condiciones de trabajo, se inspeccionan los elementos asociados a la siguiente capa hacia arriba hasta que la causa (s) del problema que se identifica (Ranjbar, 2017).

La solución de problemas *Bottom Up,* constituye un método eficaz y eficiente para situaciones en las que el problema se sospecha que es físico. La mayoría de los problemas de red residen en los niveles inferiores, por lo que la aplicación del enfoque de abajo hacia arriba a menudo produce resultados efectivos y quizás más rápidos.

Al enfrentarse a un caso de solución de problemas complejos, el enfoque de abajo hacia arriba por lo general se ve favorecido. Esto es así porque después de cerciorarse de que los elementos asociados con una capa OSI particular, están en buenas condiciones de trabajo, puede cambiar su enfoque sobre la

capa inmediatamente superior, y así sucesivamente, hasta que identifique la capa defectuosa (Ranjbar, 2017).

La desventaja de este enfoque de abajo hacia arriba es que se le requiere para comprobar cada dispositivo, interfaz, y así sucesivamente. En otras palabras, independientemente de la naturaleza del problema, el enfoque de abajo hacia arriba comienza con una comprobación exhaustiva de todos los elementos de cada capa, empezando por la capa física, y se abre camino hacia arriba.

Una manera de evitar tener que empezar solucionando problemas de la capa inferior (capa física) es poner a prueba la salud de las capas inferiores mediante el uso de la mesa de ping o herramienta traceroute/tracert. Un ping totalmente exitoso a través de un enlace elimina la posibilidad de hardware roto (capa física) o capa de enlace de datos en cuestiones tales como encapsulados desajuste o DLCI de Frame Relay, inactivos Ping o el fracaso traceroute / tracert que indicarán la posible existencia de problemas en las capas inferiores, requiriendo una investigación al respecto.

1.2 Metodologías ciclo de vida de la red (PPDIOO)

La metodología PPDIO, se enfoca principalmente en definir las actividades mínimas necesarias, por complejidad y tecnología de la red. Se optimiza el desempeño a través de su ciclo de vida, ya que cada fase depende de la anterior y ayuda a que se ejecute la predecesora.

Independientemente de la metodología, el punto principal es el análisis de la red mediante el modelo SAFE de Cisco, que se enfoca en las buenas prácticas para implementar una red segura y permitirá mantener la integridad de la información que maneja el GADMCGP, así mismo será la base para proponer otros protocolos que ayudarán a tener una red con disponibilidad, escalabilidad y calidad de servicio.

Cisco ha formalizado el proceso de ciclos de vida para el diseño y la implementación de una red en seis fases, donde cada una de estas

corresponde a una letra: Preparación, Planificación, Diseño, Implementación, Operación y Optimización.

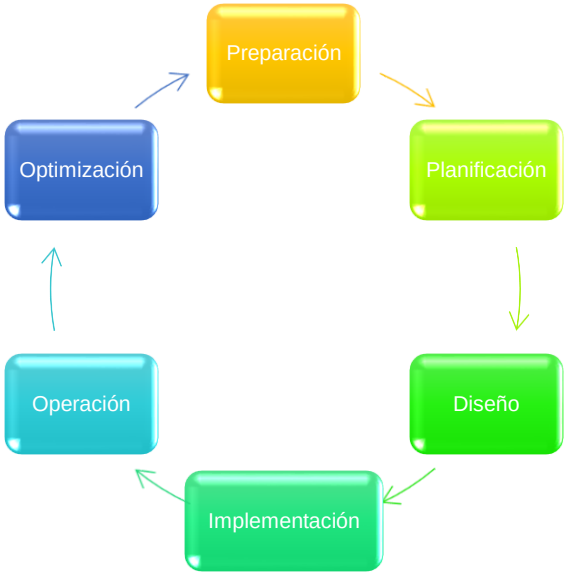

Figura 4. Proceso de ciclo de vida para el diseño y la implementación de redes.

La metodología PPDIOO o enfoque del ciclo de vida para el diseño e implementación de redes se erige para preparar, planificar, diseñar, implementar, operar y optimizar una base de datos. La PPDIOO es una metodología de Cisco que define el ciclo de vida continua de los servicios necesarios para una red (Sivasubramanian, Frahim, & Froom, 2017).

Cabe recordar que el alcance de este proyecto contiene las 3 primeras fases: Preparación, Planificación, Diseño. Cada fase cumple funciones específicas y es la base para que se pueda desarrollar la siguiente, por lo que se reseña brevemente cada una (Sivasubramanian, Frahim, & Froom, 2017):

- **Fase de preparación:**

Esta etapa implica el establecimiento de los requisitos de la organización, el desarrollo de una estrategia de red, y proponiendo una arquitectura conceptual

de alto nivel de la identificación de tecnologías que pueden apoyar mejor la arquitectura. La fase de preparación puede establecer una justificación financiera para la estrategia de la red mediante la evaluación del caso de negocio para la arquitectura propuesta.

En lo que respecta al proyecto de redes del presente trabajo, la fase de preparación permite definir las características técnicas de la Red del GADMCGP Estas características comprenden a los empleados, aplicaciones, servicios, equipos informáticos y medios de transmisión. Toda esta información se obtendrá mediante realización de entrevistas a los usuarios internos de la Institución y la documentación de la red actual.

- **Fase de Planificación:**

Involucra la identificación de los requisitos de red iniciales basados en objetivos, las instalaciones, las necesidades del usuario, y así sucesivamente. La fase de planificación implica la caracterización de los sitios y la evaluación de todas las redes existentes y la realización de un análisis de brecha para determinar si la infraestructura existente: sistema, sitios, y el medio ambiente operativo pueden apoyar la propuesta. Un plan de proyecto es útil para ayudar a gestionar las tareas, responsabilidades, hitos críticos y los recursos necesarios para implementar cambios en la red. El plan del proyecto debe alinearse con el alcance, costo y parámetros de recursos establecidos en los requisitos de negocio originales (Thomas, 2017).

El análisis se realizará en base al modelo SAFE de Cisco y la utilización de la herramienta PRTG.

- **Fase de Diseño:**

Los requisitos iniciales obtenidos en la fase de planificación conducen las actividades de los especialistas de diseño de red. La especificación de diseño de red es un bosquejo detallado integral que cumpla con los negocios actuales y los requisitos técnicos, e incorpora especificaciones para soportar la

disponibilidad, fiabilidad, seguridad, escalabilidad y rendimiento. La especificación de diseño es la base para las actividades de aplicación.

En esta fase se desarrolla el diseño de la red de conectividad del. El nuevo diseño se realizará en base al análisis realizado y los requerimientos obtenidos en la fase de planificación. Esta fase está descrita en el capítulo de desarrollo.

- **Fase de Implementación:**

La red está construida por componentes adicionales se incorporan de acuerdo con las especificaciones de diseño, con el objetivo de integrar dispositivos sin interrumpir la red existente o la creación de puntos de vulnerabilidad.

Esta fase abarca el diseño de la red de conectividad del GADMCGP. El nuevo diseño se desarrollará en base al análisis realizado y los requerimientos obtenidos en la fase de planificación. Esto permite definir las características técnicas de la Red del GADMCGP.

Estas características involucran a los empleados, aplicaciones, servicios, equipos informáticos y medios de transmisión. Toda esta información puede ser obtenida mediante realización de entrevistas a los usuarios internos de la Institución y la documentación de la red actual (Learn.org, 2017).

- **Fase de Operación:**

La operación es la prueba final de la adecuación del diseño. La fase operativa implica el mantenimiento del estado de la red a través de las operaciones del día a día, incluyendo el mantenimiento de una alta disponibilidad y reducir los gastos. El monitoreo de detección de fallos, la corrección, y el rendimiento que se producen en las operaciones diarias proporcionar los datos iniciales de la fase de optimización.

- **Fase de Optimización:**

Implica una gestión proactiva de la red, cuyo objetivo es identificar y resolver los problemas antes de que afecten a la organización. La detección de fallos

reactiva y corrección (solución de problemas) es necesaria cuando la gestión proactiva no puede predecir y mitigar los fracasos.

En el proceso PPDIOO, la fase de optimización puede llevar a un rediseño de la red si se presentan demasiados problemas de red y los errores, si el desempeño no cumple con las expectativas, o si se identifican nuevas aplicaciones para soportar los requerimientos técnicos y de organización.

Con respecto a las fases descritas, el diseño aparece como una de las seis fases PPDIOO, algunos elementos de diseño pueden estar presentes en todas las otras fases.

1.2.1 Beneficios de un enfoque de ciclo de vida

El enfoque de ciclo de vida de la red ofrece varios beneficios clave además de mantener el proceso de diseño organizado (Sivasubramanian, Frahim, & Froom, 2017). Las principales razones documentadas para la aplicación de un enfoque de ciclo de vida para el diseño del GADMCGP son los siguientes:

- Reducir el coste total de propiedad de la red
- El aumento de la disponibilidad de red
- La mejora de la agilidad del negocio
- El exceso de velocidad de acceso a aplicaciones y servicios

El coste total de propiedad de la red es especialmente importante en el clima de negocios de hoy. Menores costes asociados a los gastos de TI se están evaluando de forma agresiva por los ejecutivos de la empresa. Sin embargo, un ciclo de vida de red adecuado ayuda a las alcanzar una importante reducción de los costos de estas acciones (Wang, 2013):

- Identificar y validar los requisitos de la tecnología
- La planificación de cambios en la infraestructura y los recursos necesarios
- El desarrollo de un diseño de la red de sonido alineado con los requisitos técnicos y objetivos requeridos

- Acelerar la implementación exitosa
- La mejora de la eficiencia de la red y del personal de apoyo
- La reducción de los gastos de operación mediante la mejora de la eficiencia de los procesos y las herramientas operativas

La disponibilidad de la red ha sido siempre una de las principales prioridades de las empresas. Sin embargo, el tiempo de inactividad de la red puede resultar en una pérdida de ingresos. Ejemplos: en los que el tiempo de inactividad podría causar la pérdida de ingresos, son los cortes de la conectividad que impiden a la bolsa de valores, durante un recorte de tasas de interés sorpresa, hacer operaciones. El ciclo de vida de la red mejora la alta disponibilidad de las redes por parte de estas acciones (Sivasubramanian, Frahim, & Froom, 2017):

- La evaluación de estado de seguridad de la red y su capacidad para apoyar el diseño propuesto.
- Especificaciones al conjunto correcto de comunicados de hardware y software, y mantenerlos en funcionamiento y actual.
- La producción de un diseño de operaciones de sonido y validación de las operaciones de red.
- Puesta en escena y prueba del sistema propuesto antes del despliegue
- La mejora de las capacidades del personal.
- monitoreo de forma proactiva el sistema y la evaluación de las tendencias de la disponibilidad y alertas.
- la identificación proactiva de las brechas de seguridad y la definición de planes de remediación.

Las empresas tienen que reaccionar rápidamente a los cambios en la economía. Las empresas que lo hacen obtienen ventajas competitivas frente a otros negocios. Sin embargo, la agilidad en obtener ganancias del ciclo de vida de la red de negocios se da mediante las siguientes acciones:

- El establecimiento de requisitos de negocio y estrategias de tecnología.
- Preparando los sitios de apoyo al sistema que desea implementar.

- La integración de los requisitos técnicos y objetivos de negocio en un diseño.
- La demostración de que la red está funcionando como se especifica en la instalación, configuración, y la integración de los componentes del sistema.
- Mejorar continuamente el desempeño.

La accesibilidad a las aplicaciones y servicios de red es fundamental para un entorno productivo. Como tal, el ciclo de vida de la red acelera el acceso a las aplicaciones y servicios de red por las siguientes acciones:

- Evaluar y mejorar la preparación operativa para apoyar las tecnologías y servicios de red actuales y previstos.
- La mejora de la eficiencia de prestación de servicios y la eficacia mediante el aumento de la disponibilidad, la capacidad de los recursos y el rendimiento.
- Mejorar la disponibilidad, la fiabilidad y la estabilidad de la red y las aplicaciones que se ejecutan en él.
- Actual gestión y resolución de problemas que afectan a su sistema y mantenimiento de aplicaciones de software.

El contenido de este trabajo se centra en las fases de: preparación, planificación, y el diseño del proceso de PPDIOO tal como se aplica a la construcción de una red de campus de una empresa, por tanto, se detallan lo atinente al planeamiento de la implementación de la red.

Al documentar de forma más detallada el plan de implementación, se incrementa la probabilidad de que la aplicación sea un éxito. Aunque los pasos de implementación por lo general son complejos, requieren que el diseñador lleve a cabo la ejecución, otros miembros del personal pueden completar los pasos de implementación especificados y bien documentados sin la participación directa del diseñador (Wang, 2013).

En términos prácticos, la mayoría de los ingenieros de diseño de las grandes empresas rara vez participan en las etapas de despliegue del nuevo diseño. En su lugar, las operaciones de red o ingenieros de aplicación son a menudo las

personas que implementan un nuevo diseño basado en un plan de implementación.

Por otra parte, al aplicar un diseño, se debe considerar la posibilidad de un fallo, incluso después de una prueba de red piloto o prototipo exitoso. Es necesario un proceso de prueba bien definido, pero simple en cada paso y un procedimiento para volver a la configuración original en caso de que haya un problema. Una estrategia que ha mostrado buenos resultados en la práctica es diseñar medidas de aplicación en forma tabular y revisar esos pasos con sus pares.

De este modo, es importante conocer los componentes de la implementación, entendiendo ésta como un diseño de la red que se compone de varias fases (instalar hardware, configurar sistemas, poner en marcha en la producción, y así sucesivamente). Cada fase consta de varios pasos, y cada paso debe contener, pero ser no se limita a, la siguiente documentación:

- Descripción de la etapa.
- La referencia a los documentos de diseño.
- Directrices detalladas de implementación.
- Directrices detalladas de retrocesión en caso de fallo.
- Tiempo estimado necesario para la ejecución.
- Plan de aplicación resumen.

1.3 Proyectos de Tecnologías de la información

La gestión de proyectos es un trabajo muy complicado y exigente que implica a un propietario del proyecto, una unidad de construcción y otra unidad de supervisión confiable e implica la inclusión de toda la información en la construcción del proyecto. Desde un ángulo horizontal, que incluye la organización de proyectos, planificación, la gestión de las finanzas, recursos y el control del mismo, como otros aspectos (Wang, 2013).

Desde un ángulo vertical, que incluye la configuración del proyecto, la aprobación, el diseño de la construcción con su cierre de inspección y aceptación. Una pieza implica a menudo a varios departamentos, cubriendo varias etapas del proyecto (Wang, 2013). Por lo tanto, la gestión eficaz de los datos, la consulta de información al momento y el procesamiento exacto de la misma, son factores clave en la gestión de proyectos.

El sistema de gestión de proyectos proporciona métodos eficaces para liberar a los colaboradores del trabajo complejo y pesado, en gran medida ayudaron a los trabajadores consultar información. El diseño del sistema se rige por los principios de funcionalidad, estabilidad, integridad y facilidad de uso, lo que garantiza que éste proporcione comodidad a los usuarios, sea estable y tenga la información completa, al final contar con una página amigable al usuario con una buena capacidad de expansión.

El diseño de redes implica versatilidad y criterios de seguridad para garantizar que la información que se maneje adecuadamente y se respeten los protocolos existentes.

El diseño de redes que es común en instituciones privadas como bancos es la red LAN, a través de estos mecanismos se comparte datos y comunicación local de manera eficiente. Dentro de este proceso se usan tecnologías como la *Ethernet, Token Ring* entre otras. A este mecanismo se suma la red *WAN* la misma que se conecta con la red *LAN*. Con la red *WAN* permite conectar a la empresa a grandes distancias los mismos que son compartidos en diferentes sitios, proporcionan una comunicación eficiente y se obtiene acceso a la información de manera rápida. Esta clase de redes son muy usadas por las empresas. (Burgos, 2014)

La seguridad es un elemento esencial para las empresas es por esta razón que se emplean mecanismo de seguridad como sensores biométricos, que no son más que dispositivos que funcionan con las huellas dactilares las mismas que son leídas para dar paso a la información. A eso se suma el desarrollo de alternativas complementarias para proteger los datos. La encriptación de datos

es una tecnología muy usada y su función es cifrar los datos, para que solo sean usados por una persona que conozca la clave. (Giménez, 2014)

Las medidas de seguridad que se implementan son mecanismos de control que evitan el acceso a la información que la empresa maneja, por consiguiente el uso de redes y la incorreción de distintos modelos informáticos dependen de las necesidades y requerimientos de la empresa. Muchos de los mecanismos usados pueden ser demasiado costosos pero son esenciales para establecer márgenes de seguridad óptimos.

La seguridad en América Latina se va incrementando conforme las instituciones bancarias crecen, de acuerdo a Seguridad en América latina (2017) menciona que:

> La situación de inseguridad en bancos va en aumento y las amenazas están adaptándose, por lo que las entidades bancarias han tenido que buscar la manera de resolver los problemas y obstruir el paso a brechas donde se pueda fugar cualquier tipo de información de los clientes y así garantizar la protección de los datos (p.1).

Los bancos son propensos y vulnerables a que los accesos de red sean amenazados, por tanto la seguridad está inmersa con la implementación de políticas de seguridad y del conocimiento y análisis de todos los componentes de red. Por tanto es indispensable considerar los componentes de datos, software, Hardware, componente humano, infraestructura, interconectividad. Al conocer la vulnerabilidad existente las soluciones se pueden emplear de acuerdo a la necesidad de la empresa.

1.4 La arquitectura del sistema

El diseño de la arquitectura juega un papel crucial en la construcción del sistema de información de gestión de proyectos. En la actualidad, las corrientes principales para el desarrollo son dos modos, el C/S y B/S. El modo de C/S,

posee funciones de procesamiento lógicas, con utilidades de negocios que se completan para cada tipo de cliente, lo que reduce la carga del servidor con una velocidad de circulación relativamente rápida (Wang, 2013).

Sin embargo, las necesidades del cliente individual con respecto a la instalación de software y las necesidades de mantenimiento, pueden significar un alto costo, débil capacidad de expansión y poca flexibilidad tanto en el servidor y el cliente.

En términos de B/S, la mayoría de las funciones de procesamiento de lógica de negocio se completan a través del servidor y no hay necesidad de instalación individual de clientes. La evaluación de información se realiza a través del navegador Web, y es fácil su mantenimiento y actualización. El costo es bajo y la capacidad de expansión es buena, pero la carga del servidor es relativamente pesada.

Con el continuo desarrollo de hardware, la velocidad, el almacenamiento y la estabilidad de software se presentan problemas más evidentes. Además, en base a las características de las nuevas tendencias como la dispersión espacial de las oficinas de los usuarios, la compilación de datos para la construcción debe ser al momento, en tal caso, es más conveniente elegir B/S.

La arquitectura del sistema de información de gestión de proyectos comprende tres capas: la capa de acceso de datos, la capa de lógica de negocio y la capa de presentación de datos. La función de la capa de acceso a datos es recibir la petición de consulta a la base de datos de la capa de lógica de negocio para enviar resultados (Wang, 2013).

La capa de lógica de negocio incluye la capa de fachada de negocio y capa de reglas, la primera capa es responsable de la organización de los datos y la segunda responsable de procesar los datos. La función principal de la capa de lógica de negocio es recibir peticiones de los usuarios de la interfaz de presentación de datos, analizarlos y, mientras tanto, enviar el requerimiento a la capa de acceso a datos, consultarlos y recibirlos a partir de información

alojada en la interfaz de acceso, realizando este proceso basado en cierta lógica de negocio y enviando a la capa de presentación de datos los resultados.

La función principal de la capa de presentación de datos (también llamado interfaz de usuarios) es recibir las solicitudes enviadas por los usuarios, enviarlos a la capa de lógica de negocio y en el ínterin recibir resultados de procesamiento de datos de capa de lógica de negocio e ilustrarlos al usuario. La función prenombrada tiene tres capas que son independientes y la coordinación con una lógica sencilla y clara.

1.5 Diseño del módulo de funciones

Todo el sistema incluye nueve módulos de función. Estos son: Proyecto de gestión declarativa, tareas de proyectos, contratos de proyectos, calidad del proyecto, avance del proyecto, pagos de proyectos, supervisión de proyectos, seguridad del proyecto y configuración del sistema.

En este orden de ideas, la gestión declaración de proyecto tiene como función principal darse cuenta de la puesta en marcha del proyecto y la gestión de la extensión de la autoridad, propiedad de todos los usuarios, y la clasificación de los gastos del proyecto. En cuanto a la gestión de tareas del proyecto, la función principal es la de tramitar todas las tareas y comprobar el progreso (Wang, 2013).

Con respecto a la gestión de contratos del proyecto, su función principal es la administración de los contratos firmados por la administración de proyectos. Igualmente, la gestión de la calidad del proyecto que tiene como propósito principal la gerencia de la calidad del proyecto durante el proceso de construcción.

En cuanto a la gerencia del avance del proyecto, su centro de atención es gestionar el progreso del proyecto. La unidad de construcción se avoca a subdividir las tareas en fases y la unidad de supervisión puede calcular el progreso de acuerdo a las relaciones de trabajo.

El proyecto de gestión de pagos, es otra función medular como es percatarse de que la unidad de construcción puede llegar a la declaración de cálculo del proyecto, con el propietario del proyecto supervisar y examinar el cálculo y examinar y aprobar el pago a la unidad de construcción.

Es igualmente importante supervisar la gestión del proyecto, con la cual se realiza la gestión de los problemas de supervisión de esa unidad. El proyecto de gestión de la seguridad se encarga de tratar los asuntos de seguridad. Finalizando con el sistema de gestión global que se encarga de monitorear a los usuarios, el nivel de autoridad y la gestión de códigos.

1.6 Herramientas de análisis de red

1.6.1 Modelo de seguridad para redes empresariales SAFE.

El modelo SAFE para redes de empresas, define una arquitectura que integra toda la red de una organización, incluyendo el campus, el centro de datos, enlaces WAN, sucursales y los tele trabajadores: servidores públicos que prestan su servicio fuera de la Institución (CISCO Systems, 2000).

La arquitectura de SAFE es modular, separando las áreas funcionales llamadas módulos. En cada módulo se analiza su funcionalidad, la arquitectura lógica y física, las amenazas de seguridad y los distintos medios para combatirlas. Cada módulo es independiente, permitiendo así no afectar la seguridad a los demás módulos de la red, considerando los siguientes objetivos:

- Autenticación y autorización administradores y usuarios a recursos de la red.
- Conectividad segura para empresas que dependen del Internet para comunicarse con las sucursales o tele-trabajadores.
- Seguridad perimetral para el control de acceso a usuarios no autorizados.
- Implementación de seguridad en la red interna.

- Seguridad y atenuación de ataques basado en políticas.
- Escalabilidad.
- Análisis de vulnerabilidad y protección con sistemas de detección de intrusos para subredes en tiempo real. (CISCO Systems, 2000):

Hoy en día las empresas cada vez gestionan sus recursos y comparten su información con las sucursales a través del Internet, permitiendo el acceso remoto, acceso a usuarios móviles, por lo que se convierten en redes vulnerables a los ataques externos.

SAFE permite diseñar una red segura a través de módulos, cada uno de ellos puede incluir, sistemas de escaneo, sistemas de detección de intrusos, firewalls, autenticación de usuarios, tecnologías antivirus, encriptación de la información, VPN's. Este modelo permite a los administradores de redes, construir las soluciones por etapas, realizando configuraciones para las aplicaciones, entornos y usuarios determinados (CISCO Systems, 2000).

La arquitectura SAFE como se observa en la figura 6, presenta un enfoque modular, permitiendo afrontar la seguridad en distintos bloques y así mismo evaluar e implementar la seguridad modulo a modulo. Un diseño modular permite un eventual reemplazo de dispositivos, la implementación de nuevos servicios y funciones si el negocio lo necesita.

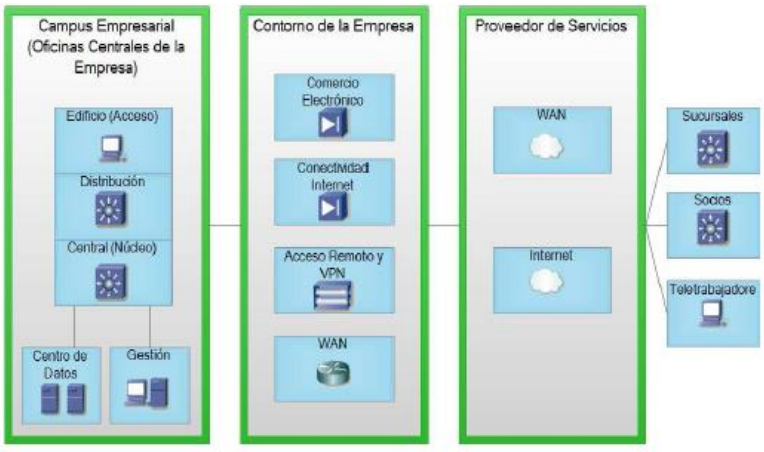

Figura 5. Modelo para administradores de redes
Tomado de (Wilkins, 2012).

El diagrama de bloques representado en la figura 6 contiene las siguientes áreas funcionales:

- Campus Empresarial.
- Perímetro Empresarial.
- Proveedor de Servicios (ISP).

A continuación, se hace un estudio detallado de cada área:

Campus Empresarial

Cada módulo contenido en este campus cumple una función específica, detallándose en el siguiente diagrama de bloques.

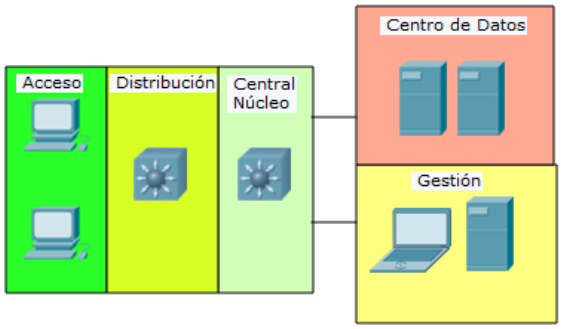

Figura 6. Diagrama de bloques campus empresarial.
Tomado de (Wilkins, 2012).

Módulo de Acceso: También llamado modulo del edificio, es el que permite el acceso a los dispositivos finales como: teléfonos IP, computadoras, impresoras de red, y todos los elementos asociados a la capa 2, el cual provee el acceso a la información a los usuarios finales autorizados. La seguridad debe ser implementada en todas las computadoras o estaciones de trabajo con antivirus que detecten cualquier amenaza de red (CISCO Systems, 2000).

Módulo de Distribución: Se divide en el módulo de distribución perimetral y el de distribución de edificios. El objetivo principal del primero es ofrecer conectividad con otros módulos contenidos en el perímetro empresarial como: Internet corporativo, comercio electrónico, acceso remoto (VPN), y WAN.

El modelo de distribución de edificios, provee servicios de capa de distribución hacia los switch de capa 2, los cuales permiten la conexión a los usuarios finales, incluye calidad de servicio, enrutamiento. Además, controla el acceso a la información a ciertos departamentos, de acuerdo a las políticas de seguridad establecidas por la compañía.

Módulo Central: Se encarga del enrutamiento de la información hacia otras redes locales y el Internet. Se comunica con el módulo de distribución de edificio y el módulo de servidores.

Módulo de Centro de datos: Este módulo de servidores proporciona servicios de las aplicaciones para los usuarios finales y estaciones de trabajo. Puede ser controlado por switches de capa 3.

Módulo de Gestión: Es el encargado de la administración, como el monitoreo de la red interna, syslogs, gestión de la configuración, actualización de software, autenticación de usuarios.

1.6.2 PRTG Network Monitor o monitoreo “Todo en Uno”

La herramienta PRTG Network Monitor es utilizada para monitorizar redes, servidores, aplicaciones, etc., permitiendo definir la configuración necesaria de los dispositivos en la propuesta del nuevo diseño. Ejemplo: la cantidad de tráfico generado por los usuarios de la red privada y el trafico real que permite el proveedor de Internet, esto será clave al momento de generar políticas de calidad de servicio.

Por tanto, el PRTG es un software de monitorización de red que puede ejecutarse en una máquina bajo ambiente Windows dentro de la red y se puede recoger estadísticas de los anfitriones designados como enrutadores, servidores, switches y otros dispositivos o aplicaciones importantes (Gilchrist, 2017).

El beneficio de software de gestión de la red es que puede detectar problemas antes de que el deterioro se convierta en faltas y alerte de estos problemas a

un administrador de red, muchas interrupciones del servicio pueden evitar costos. Por otra parte, PRTG es libre para las pequeñas empresas de seguimiento de menos de 25 dispositivos.

Muchas redes de pequeñas empresas no instalan aplicaciones de monitorización de red, ya que se consideran a veces complicadas, innecesarias o costosas. Sin embargo, el monitoreo de red puede evitar costosas pérdidas de servicio, tales como el correo de la empresa o el fracaso de la página web de comercio electrónico de la empresa. Por otra parte, el monitoreo de red ya no es caro, complejo y complicado de instalar y configurar. PRTG en particular, es fácil de instalar y operar, de ahí su popularidad en entornos SMB (Gilchrist, 2017).

Lo que hace PRTG especialmente fácil de usar es que detectará automáticamente los dispositivos de la red y auto-configurarlos. PRTG entonces sondea estos dispositivos a través de su elección de SNMP, WMI, detección de paquetes, el flujo neto, JFlow, sflow o IPFIX. PRTG de fácil uso en la interfaz web y la configuración de apuntar y hacer click con el botón que sea adecuado tanto para la resolución de problemas en tiempo real o para compartir datos con el personal no técnico a través de gráficos en línea e informes personalizados.

La forma en que funciona PRTG es mediante el uso de sensores, que son entidades de control individuales configurados para un propósito específico. Por ejemplo, hay HTTP, SMTP / POP3 (email) sensores de aplicación, así como sensores específicos de hardware para conmutadores, routers y servidores. PRTG tiene más de 200 tipos de sensores pre configurados que las estadísticas de la encuesta de las entidades supervisadas, tales como tiempos de respuesta, procesador / memoria / ancho de banda de uso.

El software de red-monitoreo es una herramienta administrativa importante cuando se trata de la operación y mantenimiento de una red, independientemente del tamaño que a menudo hay pocos síntomas o advertencias antes de una interrupción de la red. PRTG puede realizar un

seguimiento de anomalías del sistema y emitir alertas tempranas a los eventos de red potencialmente desastrosas dando así el administrador de tiempo suficiente para tomar medidas correctivas (Gilchrist, 2017).

1.7 Protocolos

1.7.1 Protocolo *EtherChannel*

El protocolo *EtherChannel* es una tecnología de agregación de enlaces puerto desarrollado por Cisco, que proporciona enlaces de alta velocidad tolerantes a fallos entre conmutadores, enrutadores y servidores. La tecnología *EtherChannel* permite múltiples enlaces Ethernet física *(Fast Ethernet o Gigabit Ethernet*) para combinar en un solo canal lógico (Thomas, 2017).
La tecnología *EtherChannel* permite la agrupación de varios enlaces Ethernet físicos (Fast Ethernet, Gigabit Ethernet, o 10 Gigabit Ethernet) para crear un enlace de Ethernet lógico para el propósito de proporcionar tolerancia a fallos y alta velocidad a los vínculos entre conmutadores, routers y servidores.

Asimismo, con EtherChannel se puede aumentar el ancho de banda entre dos dispositivos que soportan la tecnología EtherChannel, proporcionando la recuperación automática para la pérdida de un enlace mediante la redistribución de la carga a través de los enlaces restantes. La tecnología EtherChannel permite la redirección automática del tráfico de red desde el enlace fallido a los demás eslabones de EtherChannel (Thomas, 2017).

Hay dos protocolos utilizados para la negociación de EtherChannel y agregación de enlaces. Podemos configurar EtherChannel de tres maneras en Cisco Switches.

- Puerto Protocolo de agregación (PAgP) - protocolo propietario de Cisco.
- Protocolo de agregación de enlaces IEEE (LACP) - Estándar de la Industria.

- Configuración manual de EtherChannel - Sin utilizar ningún protocolo de negociaciones mencionadas anteriormente.

El Protocolo de agregado de puertos (PAgP) y el Protocolo de control de agregación de enlaces (LACP) se pueden utilizar para la negociación EtherChannel. Protocolo de agregación de puertos (PAgP) es un protocolo propietario de Cisco. Por lo tanto PAgP se puede utilizar para negociar EtherChannels sólo entre interruptores Cisco.

Protocolo de control de agregación de enlaces (LACP) es un estándar del sector definido en el estándar IEEE 802.3ad. Usando el Protocolo de control de agregación de enlaces (LACP), interruptores Cisco pueden negociar Agregación de enlaces con los interruptores de diferentes proveedores que apoyan protocolo 802.3ad.

Protocolo de agregado de puertos (*PAgP*) o protocolo de control de agregación de enlaces (*LACP*) es utilizado por un interruptor para conocer la identidad de los socios, la capacidad de los socios y las propiedades de la interfaz y capacidades. Protocolo de agregado de puertos (*PAgP*) o grupos de Enlace *Aggregation Control Protocol (LACP)* configurados de manera similar las interfaces en un único enlace lógico presentar el grupo de *Spanning Tree Protocol* (STP) como un único puerto del switch (Thomas, 2017).

1.7.2 Protocolo HSRP

Hot Standby Routing Protocol (HSRP), es un protocolo de enrutamiento que permite a los ordenadores anfitriones en Internet usar varios enrutadores que actúan como un solo enrutador virtual, manteniendo la conectividad incluso si la primera hop router falla, debido a que otros routers están en "espera activa" o listo para funcionar (Davis, 2017).

Esta herramienta es configurada en los routers de Cisco, que ejecutan el protocolo de Internet (IP) a través de Ethernet, Fiber Distributed Data Interface-(FDDI) y conforman un anillo de redes de área local (LAN). Por lo que HSRP

proporciona una copia de seguridad automática del router. El protocolo es totalmente compatible con Intercambio de paquetes de Novell (IPX), AppleTalk y *Banyan* VINES, y (en algunas configuraciones) con *Xerox Network Systems (XNS)* y *DECnet.*

Las redes virtualizadas plantean desafíos a los sistemas de gestión de la red, ya que a medida que más se convierten en componentes de hardware virtualizados, el reto es aún mayor. El HSRP fue desarrollado por Cisco y especificado en IETF *Request for Comments* (RFC) 2281, HSRP asegura que sólo un único router (llamado el enrutador activo) reenvía paquetes en nombre del enrutador virtual en un momento dado.

Un enrutador de reserva se elige para convertirse en el router activo, en caso de que falle la corriente router activo. HSRP define un mecanismo que se utiliza para determinar las redes activas y de reserva, haciendo referencia a sus direcciones IP. Una vez que estos se determinan, el fallo de un enrutador activo no causará ninguna interrupción significativa de conectividad (Davis, 2017).

1.7.3 Protocolo NBAR (Calidad de Servicio)

Existen desarrolladores que consideran que la Red de Aplicaciones de Reconocimiento de Cisco (NBAR) fue una de las mejores características de Cisco IOS 12.3. Posteriormente sigue siéndolo al observar lo que NBAR es capaz y puede hacer (Davis, 2017).

Esta afirmación se sustenta en la base de la Red de Aplicaciones de Reconocimiento (NBAR) que es una de las mejores características de la IOS. NBAR de Cisco es realmente una característica sorprendente. Para la mayoría de los routers es suficiente con ver el tráfico en la capa 3; con NBAR, los routers también pueden ver las capas 4 a 7.

Esto quiere decir que un router puede reconocer las aplicaciones, y una vez que pueda reconocer las aplicaciones, a continuación, puede tomar algunas medidas para asegurar que la aplicación se hace mayor prioridad, descartar paquetes desde dicha aplicación, o tomar alguna otra acción (Learn.org, 2017).

NBAR ha existido desde IOS 12.0, pero es reconocido por sólo un pequeño número de aplicaciones. Con IOS 12.3 mejora, *NBAR* fue capaz de reconocer más aplicaciones a causa de la disponibilidad de la función de paquetes Descripción módulo de idioma (*PDLM).*

El IOS utiliza *PDLMs* que lo habilita para identificar la aplicación al momento de mirar a través del flujo de tráfico. Cisco publica periódicamente nuevos *PDLMs* para nuevas aplicaciones, y se puede encontrar la lista de la página Web *PDLM* (CCO entrada válida es necesario) (Davis, 2017).

Aunque originalmente fue diseñado para reconocer las aplicaciones con el fin de proporcionar una calidad de servicio, NBAR tiene una larga lista de usos. La mayor parte de ellos giran en torno a controlar el tráfico por motivos de seguridad o simplemente eliminar el tráfico no deseado de un enlace de red. Cuando se trata de identificar el tráfico, el uso más popular es el de identificar los campos de un paquete HTTP, tales como la dirección URL, tipo de contenido, o el agente de usuario.

Un ejemplo clásico del uso de NBAR por motivos de seguridad fue cuando NBAR reconoció el gusano de movimiento rápido Código Rojo que primero circuló por Internet en 2001. Mientras que los firewalls tradicionales no fueron capaces de mirar dentro de la secuencia HTTP de los datos y bloquear el Código rojo del semáforo, NBAR fue capaz de hacerlo y lo hace ideal para esta situación.

En general, se puede utilizar NBAR para identificar cualquier tráfico de capa de aplicación para el que tiene una "definición". Para una lista exacta de todos los protocolos soportados, puede consultarse la documentación de Cisco IOS que se enumeran los protocolos soportados Cisco NBAR (Davis, 2017).

Sin embargo es necesario considerar algunas precauciones, hay algunas cosas que NBAR no puede hacer. No se puede utilizar en un túnel o interfaz de cifrado, y no se puede utilizar para trabajar con flujos de tráfico asimétrico,

comprender URL o el resto del tráfico en el tráfico HTTPS, el trabajo con el tráfico no CEF, o identificar el tráfico fragmentado.

Hasta ahora es común enviar a los ingenieros de redes a desplazarse físicamente a un sitio para solucionar problemas de rendimiento. Hoy en día las empresas están distribuidas geográficamente dispersas y requieren un enfoque proactivo 24x7 para medir y monitorear.

Se hace necesario considerar, que en su forma más simple NBAR es una identificación de tráfico y sistema de marcado. Lo que se hace con los paquetes marcados depende del usuario. Por ejemplo, se puede optar por dejarlos caer o elegir para darles una mayor calidad de servicio.

Finalmente, NBAR es un firewall de capa de aplicación muy potente, es el mejor de los que se haya instalado en el router Cisco. Mientras que los cortafuegos tradicionales sólo pueden reconocer el tráfico basado en IOS Capas 3 ó 4, NBAR de Cisco puede ir todo el camino a la Capa 7.

1.7.4 Protocolo SNMP

El protocolo SNMP se ha diseñado para disminuir la complejidad que existe en la información de redes, con lo cual se puede supervisar y gestionar todos los componentes de red y software.

De acuerdo a Dordoigne (2015) define al SNMP como “un protocolo elemental que asegura el transporte entre los equipos supervisados y administrados y la consola de administración o supervisión ya que utiliza una base de UDP y utiliza puertos 161 y 162 la misma que asegura las tramas de red”. (p.468)

La evolución del SNMP permite reemplazar versiones anteriores y dinamizar el entorno del SNMP, el funcionamiento es simple en los equipos se establecen servidores integrados los mismos que interactúan con los supervisores del SNMP a través de las peticiones de información o configuraciones de

actualización, es decir un acceso de lectura y escritura. El funcionamiento es menos complejo si se cuenta con los accesos correctos, cuando se trabaja en espacios comunes, por tanto se autoriza el acceso de escritura y lectura acorde a la comunidad por defecto.

Las redes que se encargan del monitoreo, lo realizan a través de dos elementos claves que son:

- NMS (*Network Management Station*, Estación de administración de la red: es el equipo encargado de la supervisión.
- Agente SNMP es el componente Software instalado en los equipos que se desean monitorizar, proporciona la información solicitada por los NMS (Valdivia, 2017 , pág. 188).

Al ser un mecanismo integral a través del SNMP se puede programar un agente mediante un mensaje cuando se supere el ancho de la banda WAN para evitar la saturación de del disco y de los servidores. Las eventualidades se pueden supervisar gráficamente a través de colores, las mismas que son identificadas con rapidez (Dordoigne, 2015).

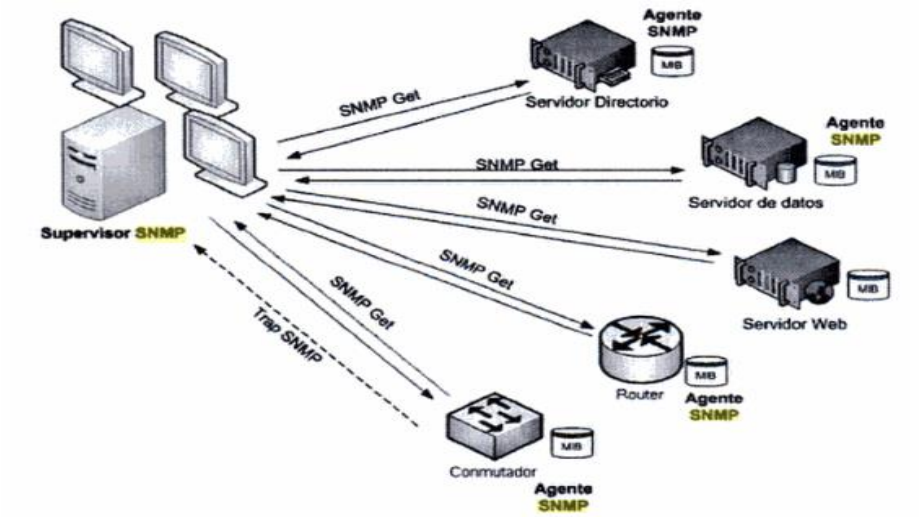

Figura 7. Comunicaciones SNMP supervisor –agentes.
Tomado de (Dordoigne, 2015).

1.7.5 Protocolo *VPN-GRE-over IPSEC*

La introducción de una contextualización de un mundo globalizado incluye herramientas complementarias que se han generado a través de dos enfoques:

- La red virtual.
- Encriptación de datos.

La red virtual que por sus siglas en ingles se denomina *Virtual Private Network* (VPN) “es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet” (Goujon, 2012, pág. 1) es una de las redes más usadas por las empresas para conectar a sus empleados desde cualquier lugar en donde se encuentren, sin embargo es importante mencionar que la facilidad que tienen estas redes incrementa el grado de vulnerabilidad en cuanto a la seguridad.

La encriptación de datos no es más que asegurar que la información está segura y cumple con todos los protocolos establecidos por la empresa por tanto se requiere tener una red virtual segura que permita el uso de información privada a quienes los requirieran. (Gerometta, 2006)

Asimismo de acuerdo al autor Márquez (2016, pág. 25) menciona que:

> Las red VPN nos permite dar un nivel de seguridad y / o confidencialidad a nuestras comunicaciones en redes públicas. Para ello la información que viaja por ella puede y suele estar encriptada y por lo tanto, inaccesible hasta su llegada al otro extremo de la VPN. Esto puede presentarnos dificultades a la hora de clasificar el tráfico, ya que no podemos ver nada del paquete original.

Es importante considerar que la VPN requiere de la utilización de protocolos para lograr así la tunelización y la encriptación. Adicionalmente se utiliza GRE para la implementación de túneles.

GRE

Es un protocolo que fue diseñado por Cisco Systems, del cual se establecen estándares RFC 1701, 1702 y 2784 que son usados como túneles, su función principal es trasladar paquetes de una red a otra diferente.

De acuerdo a Gerometta (2006) menciona que existen consideraciones especiales para el manejo del GRE:

- GRE toma un paquete ya existente, con su encabezado de capa de red, y le agrega un segundo encabezado de capa de red, lo que implica que el paquete que se envía a través del túnel es de mayor longitud por lo que puede ocurrir que esté excediendo la longitud permitida en la interfaz física. Esto provoca el descarte de ese paquete.
- Para solucionar este inconveniente se puede aplicar el comando *ip tcp adjust-mss* 1436 sobre la interfaz túnel para asegurarse de que no se supere el MTU permitido sobre el enlace.
- El enlace sobre el túnel GRE no requiere ninguna información de estado, por lo que puede ocurrir que un extremo del túnel se encuentre en estado de *DOWN* y el otro continúe presentándose como *UP*.
- Para evitar esta situación habilite keepalive en cada extremo del túnel. De este modo cada extremo enviará mensajes de keepalive sobre el túnel y si un extremo no recibe los mensajes enviados por el otro entonces pasará al estado de *DOWN* (p.1)

Todos los protocolos deben ser considerandos antes de emplear un túnel de información, es importante determinar las necesidades y requerimientos de las empresas puesto que no todas las redes pueden ser usadas. Y el objetivo es mantener la seguridad de la información.

Ipsec GRE

De acuerdo a Márquez (2016) menciona que:

> Hay que destacar que los Ipsec solo nos permite transportar IP *unicast*. Esto puede convertirse en un problema si lo que deseamos crear un túnel VPN entre dos redes IPX /SPX o si simplemente queremos que a

través de ese túnel funcione protocolos de enrutamiento que usan trafico *multicast* (p.32)

IPsec VPN

La clasificación del tráfico es compleja por tanto “cisco soporta dos modos de tráfico IPsec (VPN): Túnel y transporte. En el modo túnel todo el paquete original IP y su contenido es encapsulado en otro paquete IP. Este paquete contienen una cabecera IP nueva que encapsula a un protocolo de capa 4 ESP o AH.” (Márquez, 2016, pág. 25)

2. CAPÍTULO II. FASE DE PREPARACIÓN

En la fase de preparación comienza con la obtención de los requerimientos del GADMCGO y la descripción de todos los elementos que forman parte de la red de conectividad, como son los usuarios finales, dispositivos de red, aplicaciones, medios de transmisión que actualmente operan en la Institución. El estudio de la red del GADMCP, permitirá obtener datos exactos para el rediseño de la red de conectividad.

2.1 Requerimientos

2.1.1 Requerimientos y restricciones

El proceso para la obtención de los requerimientos se efectuó conjuntamente con la Jefatura de Talento Humano y de Tecnologías de la Información.

La recolección de dicha información permitirá obtener conclusiones en base al análisis físico y lógico de la red del GADMCGP. Cabe recordar que la entrevista se hace a un lenguaje de alto nivel, considerando que el personal interno de la Institución no tiene conocimientos técnicos.

La metodología PPDIOO aplicada en este proyecto recomienda cinco pasos para la obtención de los requerimientos. Así mismo será la base para definir los requerimientos y proponerlos en el nuevo diseño.

Los pasos para la obtención de los requerimientos se resume de la siguiente manera:

- Identificar las Aplicaciones y servicios de red.
- Definir los Requerimientos Técnicos.
- Definir los las Restricciones Técnicas.
- Definir los Requerimientos Organizacionales.
- Definir las Restricciones Organizacionales.

La definición de los requerimientos, permitirá crear un modelo de red de comunicaciones, que se adapte a todas las necesidades y problemas que los usuarios internos expongan.

2.1.2 Diseño de la entrevista

El objetivo de basarse en un diseño de entrevista es para poder documentar la información obtenida y definir los requerimientos del GADMCGP.

Las preguntas expuestas hacia el personal de la Institución permitirán identificar lo siguiente:

- Las aplicaciones y servicios de la red del GADMCGP.
- Los objetivos y restricciones organizacionales.
- Los objetivos y restricciones técnicas.

Las preguntas presentadas a continuación se basan en el libro *Designing for Cisco Internetwork Solutions*, por lo tanto la información obtenida será analizada y se definirán los requerimientos.

2.1.3 Aplicaciones y servicios

1) **¿Qué aplicaciones y servicios se consideran más importantes para la Institución?**

Las aplicaciones internas más importantes para la Institución son: GCS, SIC, SARP y SIG-AME, las cuales son utilizadas en la Intranet. Por otro lado el Sistema de Gestión Documental QUIPUX, el cual es un servicio web que ofrece la Subsecretaría de Gobierno Electrónico, así mismo permite generar y guardar toda la información del GADMCP.

2) **¿Cuál información que manejan las aplicaciones de la organización puede considerarse como de mayor importancia y riesgo?**

Todas las aplicaciones internas del GADMCP, se consideran importantes ya que hay información de los ciudadanos del Cantón Gonzalo Pizarro.

3) **¿Qué porcentaje de disponibilidad deberían presentar las aplicaciones y servicios, tanto para usuarios internos como externos?**

Se requiere una disponibilidad del 100% de todas las aplicaciones tanto internas como externas.

4) **¿Qué aplicaciones y servicios son ofrecidos actualmente?**

Actualmente no existen servicios que el GADMCGP ofrezca a usuarios externos. Para el año 2018 se tiene previsto que las aplicaciones migren a una plataforma web, para que los ciudadanos puedan consultar valores a pagar como el agua potable, alcantarillado, recolección de desechos sólidos, impuestos a pagar de predios.

Por otro lado la implementación de una VPN ha sido considerada para la administración remota de los dispositivos de red.

2.1.4 Requerimientos y restricciones Organizacionales

1) **¿Qué retos u objetivos empresariales enfrenta actualmente la Institución?**

Apertura de nuevas ventanillas de pagos en parroquias grandes como El Reventador y Amazonas. Así mismo para finales de este año existe un proyecto de la construcción de un parque que ofrecerá el servicio de Internet gratuito a la ciudadanía

2) **¿Cuáles son las consecuencias de no sobrellevar estos retos u objetivos?**

La GADMCGP debe garantizar el buen servicio a la ciudadanía, y buscar nuevas formas de atención al cliente. Se ha notificado en el año 2016 por parte de la Contraloría General de Estado, que todas las Instituciones Públicas deben mejorar los procesos internos y minimizar tiempos de respuestas hacia los ciudadanos, esto mediante la implementación de sistemas que permitan manejar la información digitalmente. Una notificación que de no ser puesta en marcha o aplicada, será motivo de sanción a la Institución.

3) **¿Cuáles son las limitaciones para la implementación de un nuevo diseño de red en la Organización?**

No existen limitaciones en proyectos que beneficien a la ciudadanía, el Plan Anual de Contratación permite gestionar los recursos de las direcciones de una manera adecuada. Se debe además dar a conocer el plan de Tecnologías de la

Información y ser aprobada por la sesión de consejo para la asignación de los recursos.

4) **¿Qué limitaciones se han identificado en el diseño actual en base a los requerimientos iniciales solicitados?**

No se ha identificado algún problema, con respecto a la recolección de la información. El acceso a algunos dispositivos de la infraestructura de red actual no es administrable, por lo que se pondrá en consideración en el capítulo de diseño para tener acceso seguro.

2.1.5 Requerimientos técnicos

1) **¿Cuáles son sus prioridades tecnológicas?**

El acceso a los servicios externos importantes como son QUIPUX, CORREO INSTITUCIONAL, PAGINA WEB, SERCOP, presenta lentitud. Por otra parte en la Intranet, cuando se guarda información en el servidor local existe retardos en la respuesta del mismo, las transacciones se demoran un poco en realizarse, lo que causa tiempos de espera por parte de la ciudadanía local.

2) **¿Qué problemas de infraestructura existen o podrían existir?**

Los dispositivos de red tienen una antigüedad considerable, no pueden ser administrados por el personal de soporte técnico del Departamento de Tecnologías de la Información. Así mismo los medios de transmisión, tienen características que sólo admiten velocidades de 100Mbit/s, y en la actualidad existen velocidades mayores a 1Gbit/s.

3) **¿Existe un plan para el desarrollo técnico del personal?**

El personal no es capacitado frecuentemente, todo el conocimiento que existe en sí es autodidacta. No hay un plan para el desarrollo para los técnicos del área de Tecnologías de la Información.

Para culminar con la fase de planificación, el principal objetivo del GADMCGP, es mejorar los procesos internos y externos para atender de manera más eficaz y eficiente a los ciudadanos que diariamente visitan la Institución. La aplicación de nuevos mecanismos para que la disponibilidad del Internet sea satisfactorio y que la velocidad del accesos a la información sea rápida. Por último la necesidad de apertura de ventanillas en parroquias alejadas, permitiendo así dar todos los servicios que beneficien a los ciudadanos del Cantón Gonzalo Pizarro.

En el capítulo de diseño se consideran todos estos puntos, para desarrollar de la mejor manera un diseño que se adapten a las necesidades del GADMCGP y nuevas tendencias tecnológicas.

2.1.6 Análisis y definición de los requerimientos

El diseño actual no ha cumplido con los requerimientos solicitados, como son:

- Los switches no tienen ninguna configuración de seguridad, por lo que cualquier persona puede llegar y conectar su computadora y tener acceso a la red interna y el Internet.

- El contrato con el proveedor de servicio de Internet, no es monitoreado a través de un seguimiento diario sobre la capacidad de ancho de banda que ofrecido, y cada vez el tráfico exigido por los usuarios es mayor superando la capacidad contratada.

- Existe una sola red para todos los usuarios, no se han implementado *VLANs* (Redes de área Local Virtuales), que permiten a cualquier

usuario acceder a las aplicaciones e información de otras direcciones, así mismo aumenta el procesamiento del router y se vuelve lento el acceso a la información de otras áreas que si necesitan.

- El tráfico al Internet no está marcado, es decir no existe prioridad de acceso a servicios web que usan a diario, como el Sistema de Gestión Documental QUIPUX. Este problema impide que la información sea almacenada de manera rápida en los servidores externos.

- No existe protocolos de redundancia que permitan tener disponibilidad interna y externa. Se tiene un solo proveedor de Internet, por lo que si el servicio se suspende, no se puede acceder al Sistema de Gestión Documental QUIPUX (SGDQ), el cual es la principal herramienta de trabajo de la Institución.

- La propuesta del nuevo diseño debe garantizar la implementación de nuevas aplicaciones y que brinde la suficiente seguridad de la información que se genera localmente.

- No existe una limitación en el acceso al Internet, por lo que cualquier usuario puede conectarse a redes sociales y consumir recursos de la red.

- No se cuenta con equipos que ayuden al control del acceso a la información, ni que distribuyan correctamente el tráfico con más prioridad o importancia.

2.2 Estudio de la red del GADMCGP

La red de conectividad del GADMCGP, fue implementada en el año 2006. Esta red fue diseñada para dar acceso a los empleados o usuarios internos a varias aplicaciones que permiten almacenar información importante de los ciudadanos y llevar a cabo procesos de cobranzas de los distintos servicios que ofrecen a

la ciudadanía del Cantón Gonzalo Pizarro, como son: agua potable, registro de la propiedad, títulos de crédito, desechos sólidos. Aplicaciones que ayudan a manejar la información financiera de la Institución y cumplir con las normas que rige el Ministerio de Finanzas.

La tabla 1 muestra el número de usuarios que laboran dentro de la Institución y que hacen uso de la red de datos para enviar y recibir información.

Tabla 1.

Cantidad de usuarios por Dirección del GADMCGP

EMPLEADOS DEL GADMCGP	
Dirección	**Cantidad**
Alcaldía	1
Concejales	7
Secretaría General	8
Dirección Administrativa	35
Dirección Financiera	15
Asesoría Jurídica	4
Dirección de Gestión de Riesgos	15
Dirección de Servicios Básicos	14
Dirección de Planificación	30
Dirección de Obras Públicas	45
Coordinación de Gestión Turística	10
Consejo Cantonal de la Niñez y Adolescencia	10
Auditoría Interna	2
TOTAL EMPLEADOS	**196**

Nota: Cabe destacar que algunas Direcciones tienen Jefaturas bajo su mando.

2.3 Estructura orgánico funcional del GADMCGP

La estructura orgánica funcional del GADMCGP, permite definir rangos y organizar las diferentes áreas que existen dentro de la Institución, para definir niveles jerárquicos y tener en cuenta en los procesos de documentación interna.

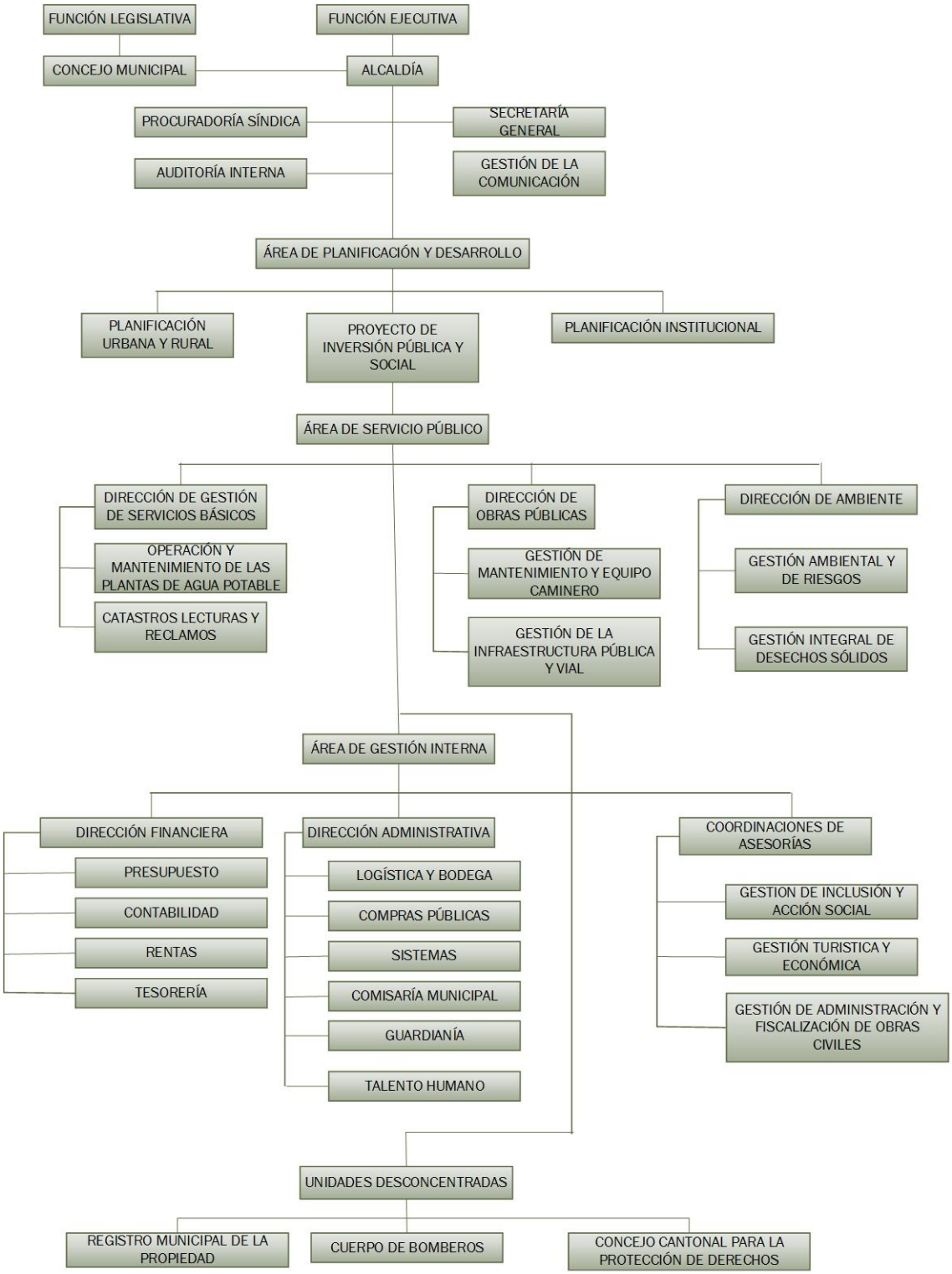

Figura 8. Estructura orgánica funcional del GADMCGP.

Tomado de (GADMCGP, 2017)

La tabla 2 muestra la infraestructura de la planta física del GADMCGP, la cual está conformada por tres pisos, distribuidos en distintas Direcciones y Departamentos:

Tabla 2.

Direcciones y Departamentos de la planta física del GADMCP

Tercer Piso	Segundo Piso	Primer Piso(Planta Baja)
Concejales	Alcaldía	Talento Humano
Catastro	Secretaría General	Registro de la Propiedad
Gestión de Riesgos	Dirección Administrativa	Dirección Financiera
Servicios Básicos	Asesoría Jurídica	Rentas
Planificación	Gestión de la Comunicación	Contabilidad
Sistemas	Contraloría Interna	Tesorería
GIAS	Compras Públicas	Gestión de Turismo

2.4 Esquema de la red física del GADMCGP

La figura 10 muestra un esquema, que permite tener una visión de cómo es la infraestructura física y cómo están interconectados los equipos.

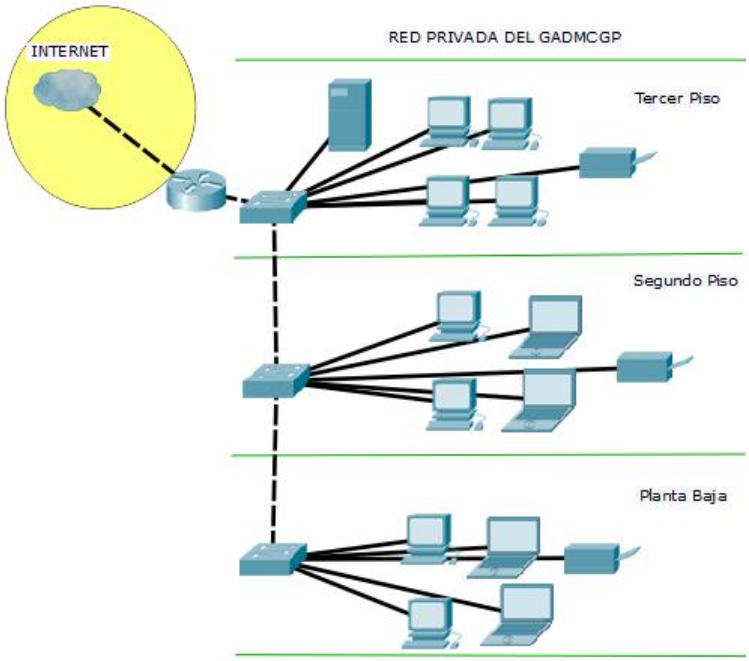

Figura 9. Infraestructura física de la red privada del GADMCGP.

2.5 Aplicaciones y servicios del GADMCGP

Actualmente se utilizan aplicaciones intranet, es decir que los usuarios sólo pueden acceder a la información si están dentro de la red privada del GADMCGP.

A continuación se detallan las aplicaciones de más uso y que se consideran muy importantes para el cumplimiento de las actividades diarias en la Institución.

- GCS.- El Sistema de Gestión de Comercialización de Servicios; automatiza los procesos del área de comercialización de servicios en los GAD's municipales y empresas públicas; maneja los procesos de administración de inventarios, determinación, facturación y recaudación de Servicios Municipales como por ejemplo: agua potable, alcantarillado y recolección de desechos sólidos.
- SIGAME.- El Sistema de Gestión Administrativa-Financiera, facilita los procesos realizados en los departamentos de Contabilidad, Presupuesto, Recursos Humanos e Inventarios; es un sistema Multi-periodo (Contable) y Multi-Institución (Municipio).
- SIC.- El Sistema Integral de Catastro, conforma el inventario de propiedades urbanas/rurales, realiza los procesos de valoración, determinación y recaudación de títulos de créditos.
- SARP.- El Sistema Automatizado de Registro de la Propiedad, realiza los procesos de administración, certificación, inscripción, revisión y recaudación de tributos relacionados con los diferentes tipos de Propiedades Municipales.

Los servicios web y aplicaciones de mayor uso:

- Correo Institucional
- Servidor Web
- Control de asistencia
- Telefonía IP
- Cámaras IP

- Internet
- Sistema de Gestión Documental QUIPUX.

El análisis de todas estas aplicaciones y servicios, se detalla en la fase de planificación.

2.6 Dispositivos de red y equipos

El GADMCGP cuenta con los siguientes elementos, que permiten dar uso a las aplicaciones locales, acceso a Internet y servicios externos:

Tabla 3.

Dispositivos de red y equipos

Descripción	Cantidad
Servidor	1
Computadora de escritorio y laptop	116
Cámara IP	20
Lector biométrico/facial	1
Switch capa 2	3
Router	1
Access Point	12
Impresoras con puerto TCP/IP	15

Nota: Descripción de cantidades de los dispositivos de red en la actualidad.

2.7 Medios de transmisión

Todo el cableado horizontal y vertical de la infraestructura de la Institución está integrado por cable UTP categoría 5E. Para el acceso inalámbrico se utiliza el estándar IEEE 802.11n y como método de autenticación el WPA2.

En la figura 11 se detallan los medios de transmisión de cada piso.

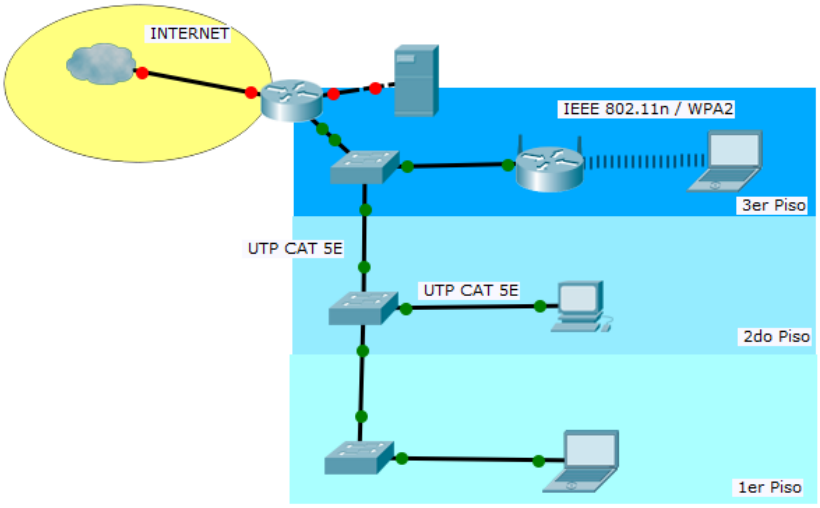

Figura 10. Medios de transmisión de la red GADMCGP.

La infraestructura física del GADMGP, consta de un switch de 48 puertos Fast Ethernet por piso, así mismo la conexión entre estos dispositivos de acceso es mediante cable UTP Categoría 5E. Todo el cableado que se distribuye desde los racks de telecomunicaciones hacia las computadoras de escritorio, también es cable UTP 5E, mientras que las laptops se conectan inalámbricamente mediante el estándar IEEE802.11 a/b/g/n.

Algunos puntos de red físicos no funcionan, por lo que algunas computadoras usan adaptadores de red inalámbricos para conectarse a los Access Point respectivos.

3. CAPÍTULO III. FASE DE PLANIFICACIÓN

El objetivo de este capítulo es analizar la situación actual y definir los requerimientos de la red de conectividad del GADMCGP.

El análisis comprende la red física, la red lógica, seguridad interna y aplicaciones. Se toma como referencia el modelo de Interconexión de Sistemas Abiertos *(OSI - Open System Interconnection*). La red física abarca la capa física y de enlace de datos, mientras que la red lógica comprende la capa de

red y de transporte. Las aplicaciones son analizadas de acuerdo al consumo de los recursos de la red interna y flujo de información.

3.1 Análisis de la red física del GADMCGP

Estudiando el modelo de seguridad para redes empresariales SAFE, se analiza que éste enfoque modular tiene dos ventajas en particular. La primera es que permite a la arquitectura afrontar la relación de seguridad entre los distintos bloques funcionales de la red. Y en Segundo lugar, permite a los diseñadores evaluar e implementar la seguridad módulo a módulo, en lugar de intentar completar la arquitectura en una sola fase.

La arquitectura actual de la red del GADMCGP, presenta un modelo jerárquico de 2 capas o núcleo colapsado, en donde la primera capa realiza las funciones de núcleo y de distribución, y la segunda capa es la de acceso.

Haciendo una comparación con la arquitectura modular de SAFE, se identifica que la capa de núcleo y distribución representan un solo equipo con respecto a la red del GADMCGP, por lo que se va a analizar el mismo equipo tanto para el Modulo Central y de Distribución de la estructura física del Edificio. La figura 12 muestra la arquitectura actual de la Institución en base al modelo SAFE.

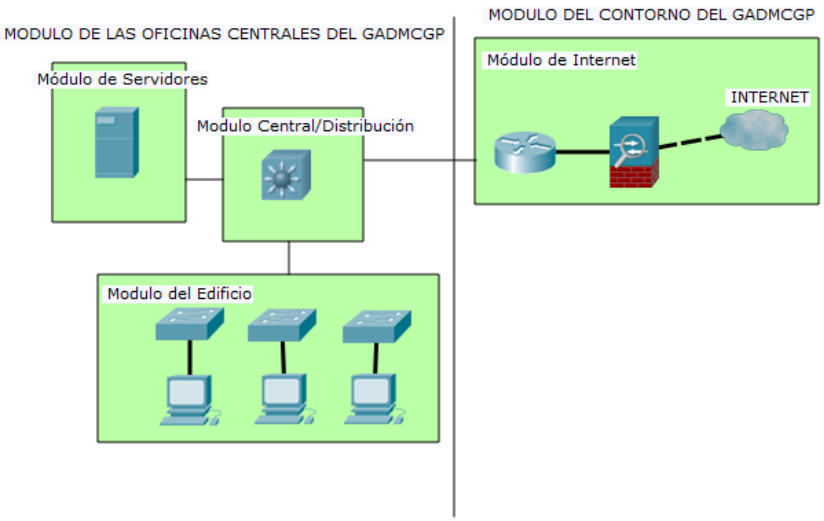

Figura 11. Arquitectura actual en base a la arquitectura modular SAFE del GADMCGP.

A continuación se estudia cada módulo, considerando dos puntos, el primero definiendo la funcionalidad, recomendaciones de implementación y las amenazas que se esperan, mientras que el segundo punto, detalla la situación actual y las características que no cumplen en base a las recomendaciones propuestas por SAFE.

3.2 Oficinas centrales de la empresa

3.2.1 Módulo Central

El módulo central de la arquitectura SAFE, es similar a cualquier arquitectura de red, cuyo objetivo es el enrutamiento y conmutación del tráfico a velocidades muy altas hacia otras redes.

Los dispositivos que constituyen éste módulo son routers y switchs encargados del envío de la información cuán rápido sea posible, y los cuales se comunican con el módulo de distribución del edificio, módulo de servidores y módulo de Internet.

El GADMCGP, tiene como módulo central un router Cisco Serie 800, el cual se encarga de la conmutación y enrutamiento rápido de los paquetes provenientes y salientes al Internet, módulo de servidores y de distribución. Esto hace a la red Interna depender de un solo dispositivo, en donde si falla el modulo central, no se pueden acceder a los servicios que se utilizan a diario por la Institución. La comunicación se la realiza mediante enlaces físicos cableados tipo UTP categoría 5e, hacia los distintos módulos.

No existen protocolos usados a nivel de capa de enlace de datos, como STP (*Spanning Tree Protocol*), el cual ayuda a solventar el problema de bucles en la red; la información regresa al dispositivo de origen.

3.2.2 Módulo de Distribución

Este módulo proporciona los servicios de capa de distribución a los switchs de la Institución, se aplica calidad de servicio, conmutación de paquetes y control de acceso.

La redundancia es el enfoque de este módulo, el cual permite tener disponibilidad y acceso a la información de manera rápida y sin retardos. El modelo de SAFE combate las amenazas como son los accesos no autorizados, los rastreadores de paquetes y ataques de falsificación IP; para combatir estas amenazas se aplican el filtrado de paquetes en capa 3 de las determinadas subredes, la implementación de una infraestructura conmutada y la configuración de puertos confiables para limitar los intentos de falsificación.

El dispositivo actual instalado en la Institución cumple además de ser módulo central, es también de distribución, siendo un punto de falla muy vulnerable. Al no existir redundancia, la red privada depende únicamente del funcionamiento del switch de capa 3, sin ofrecer disponibilidad y sobrecarga del rendimiento de dicho dispositivo. La conexión que existe hacia el modulo del edificio es mediante cable UTP categoría 5e, no existe ningún protocolo configurado que ofrezca mayores velocidades y redundancia en la red interna.

3.2.3 Módulo del Edificio

Este módulo contiene los dispositivos finales como son las estaciones de trabajo de los empleados, teléfonos IP, puntos de acceso e impresoras. El objetivo principal es el acceso de los usuarios finales a los distintos servicios locales y de Internet. Las amenazas principales son los rastreadores de paquetes, virus y troyanos, en donde SAFE la contrarresta con una infraestructura conmutada, la implementación de Vlans y la instalación de antivirus.

La Institución presenta una infraestructura conmutada, no existe una segmentación de la red y la mayoría de estaciones de trabajo no tienen

antivirus. El módulo está compuesto por tres switchs y tres routers inalámbricos, los cuales se conectan uno tras otro. Los dispositivos finales que se conectan a los switchs son estaciones de trabajo, impresoras de red, cámaras IP y lector biométrico. La conexión hacia los terminales es con cable UTP categoría 5e. La figura 13, muestra cómo se encuentran los módulos del edificio de la Institución en la actualidad, en la fase de diseño se propone el uso de puntos de acceso para mejorar la velocidad y rendimiento de los dispositivos de red.

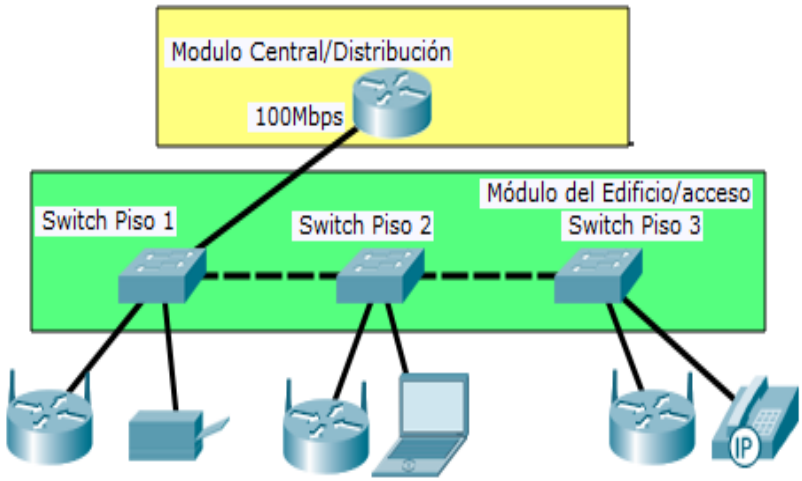

Figura 12. Módulos del edificio actual del GADMCGP.

La red privada del GADMCGP es totalmente plana, es decir no se ha configurado alguna segmentación de red, en donde se puedan aplicar políticas de control de acceso y así limitar el acceso a algunos servicios. Todos los dispositivos finales pertenecen a la VLAN 1, lo que es imposible crear reglas para una administración adecuada de los recursos de la red. Es necesario recalcar que el tráfico de VOIP que se genera sobre la red privada tiene otro direccionamiento, pero que a la vez hace el mismo uso del canal lógico, que en este caso es la VLAN1.

El antivirus que se encuentra instalado en las computadoras es el "*Eset Smart Security 9",* cuya actualización de base de datos se realiza los fines de semana automáticamente.

3.2.4 Módulo de Servidores

La función principal del módulo de servidores es ofrecer los distintos servicios de aplicaciones a los usuarios locales y estaciones de trabajo. Este módulo no debe ser accesible por usuarios remotos y solo debe dar acceso autorizado al personal asignado a de la red privada.

Las amenazas de seguridad más importantes que combate SAFE son los ataques a la capa de aplicación, redirección de puertos, control de acceso no autorizado, abusos de confianza. Todas estas amenazas son mitigadas mediante el uso de detección de intrusos basada en hosts y control de acceso. Las actualizaciones de seguridad más recientes son muy importantes en los dispositivos finales y aplicaciones. El uso de VLANs evita que otros usuarios de otra subred puedan ver información local de la Institución.

Actualmente existe un solo servidor físico que contiene las aplicaciones que se usan a diario en la Institución. La conexión del servidor hacia el modulo central es con cable tipo UTP categoría 5e de 100Mbps. El servidor forma parte de la única subred que existe, y no hay una VLAN específica para el módulo de servidores. Además que puede ser controlado remotamente desde el Internet, para la realización de respaldos de la base de datos.

3.3 Contorno de la empresa

3.3.1 Módulo de internet de la empresa

Este módulo proporciona a los usuarios de la red privada conexión a los servicios de Internet y acceso desde el Internet hacia la información interna de la Empresa.

La implementación de este módulo considera tener redundancia mediante dos routers, a través de la contratación del servicio de Internet de dos proveedores diferentes, esto ayudará en el caso de que algún enlace falle se tiene otro para salir al Internet.

En la actualidad este módulo de servidores no presenta redundancia. Se tiene un único proveedor el cual es CNT (Corporación Nacional de Telecomunicaciones), lo que impide tener disponibilidad si el servicio se suspende. No existe un Firewall que analice el tráfico a nivel de capa de aplicación, para limitar las amenazas de accesos no autorizados y denegación de servicios aplicación de políticas

Luego de analizar la situación actual de la red física del GADMCGP, se encontraron algunos hallazgos que no cumplen aspectos considerados por el modelo propuesto por SAFE:

- Implementación de control de acceso, sólo al personal autorizado de la Institución.
- Redundancia de dispositivos en el módulo Central.
- Redundancia de dispositivos en el módulo de Internet.
- Redundancia de dispositivos en el módulo de Servidores.
- Redundancia de medios de transmisión en el módulo de Distribución.

Los problemas anteriores serán analizados en la fase de planificación, en donde se presenta el nuevo diseño de la red de conectividad del GADMCGP.

3.4 Análisis de la red lógica del GADMCGP

El análisis de la Red Lógica estudia los protocolos de la capa de red y transporte, los cuales corresponden al direccionamiento, enrutamiento y configuración de los equipos. La manera en cómo se comunican y organizan los dispositivos entre sí, es la parte fundamental de este proceso. Así mismo está relacionada con las capas de red y transporte, encargadas de dirigir el tráfico adecuadamente hacia los dispositivos finales.

3.4.1 Direccionamiento

En el GADMCGP no se ha implementado una segmentación de la red, no existe un estudio de crecimiento de la red física, ya que la única red que existe es la 212.219.12.0/24, la misma que pertenece a una red pública. Todo el proceso de asignación de direcciones IP a los dispositivos finales es manual.

Tomando en cuenta que la red tiene una máscara /24, la cantidad máxima de hosts que pueden tener conectividad tanto a los servicios internos como externos son 254 direcciones IP disponibles, tomando en cuenta la dirección de red y de broadcast.

3.4.2 Enrutamiento

Este proceso permite elegir el mejor camino para que la información llegue a su destino de manera rápida. No existe un enrutamiento interno ya que en la red es un diseño de núcleo colapsado en donde existe un único dispositivo de red que cumple la función de núcleo y de distribución. Con respecto al enrutamiento externo, el router tiene una ruta STUB; ruta que por defecto es la única salida hacia el internet.

3.4.3 Configuración

La red del GADMCGP, no tiene configurado DHCP. Cualquier dispositivo que desea tener acceso a los servicios internos y externos, deberá pedir al administrador de red de la institución que se le asigne una dirección IP. El router tiene una única VLAN, y sus 4 puertos disponibles están asignados a la VLAN 1.

3.4.4 Seguridad

Con respecto a la seguridad de la red, esta se analizó con el modelo que presenta SAFE. En el capítulo de diseño se describe la configuración necesaria para todos los módulos de la arquitectura, fundamentado en las buenas prácticas que ofrece Cisco en los dispositivos de red.

3.5 Aplicaciones y servicios

En el posterior análisis de las aplicaciones internas del GADMCGP, el consumo de los recursos es muy importante para determinar cómo clasificar el tráfico que fluye dentro de la red privada, así como el tráfico saliente y entrante de

Internet. Al saber cuáles son las aplicaciones o servicios que consumen más recurso de la red, se puede aplicar políticas de calidad de servicio, el cual dará prioridad del acceso a la información más importante.

3.6 Análisis del flujo de la información externa

Para dicho análisis, se utilizó la herramienta PRTG. Este sistema de administración de redes, utiliza sensores para analizar el tráfico que fluye por un agente SNMP (dispositivo configurado para obtener información).

La instalación del PRTG fue realizada en un host en el Área de Sistemas, y se configuró en el router Cisco 800, la versión SNMPV2c, favoreciendo más seguridad al generar el nombre de la comunidad y permitir sólo lectura.

La figura 14 representa el esquema físico de la configuración, estableciendo como agente al módulo central, que es el punto de entrada de todas las peticiones de los host internos, ya sea para el acceso a las aplicaciones internas o el Internet, y por otro lado el NMS (Network Manager System), que es el software PRTG que será instalado y configurado en una computadora local.

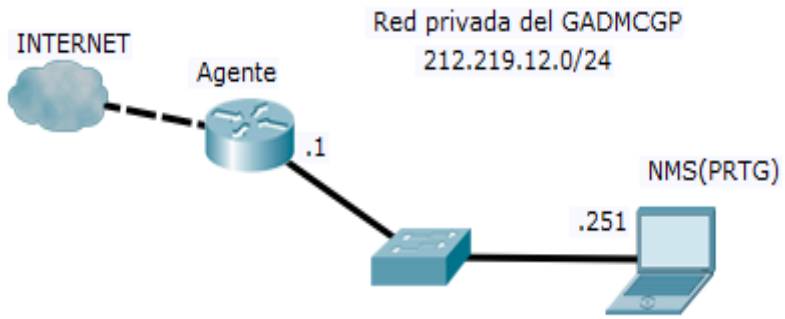

Figura 13. Modelo de conexión cliente –servidos PRTG.

Por otra parte, la figura 15 muestra la configuración del router Cisco 800 (Agente), mediante la consola de administración, en donde se crea una comunidad con un nombre especifico, el mismo que será configurado en el host

de administración, además se establece en una versión SNMPv2c en modo de lectura y la dirección IP de destino del host.

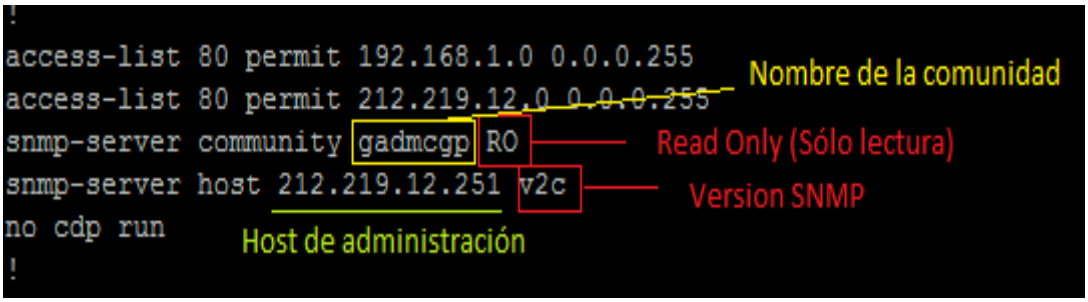

Figura 14. Configuración del agente PRTG.

Para la configuración del PRTG, se siguieron los siguientes pasos:

3.7 Configuración

Se asigna una dirección IP estática al host en donde operará el PRTG. Esta dirección IP es la misma que se configuró en el Agente.

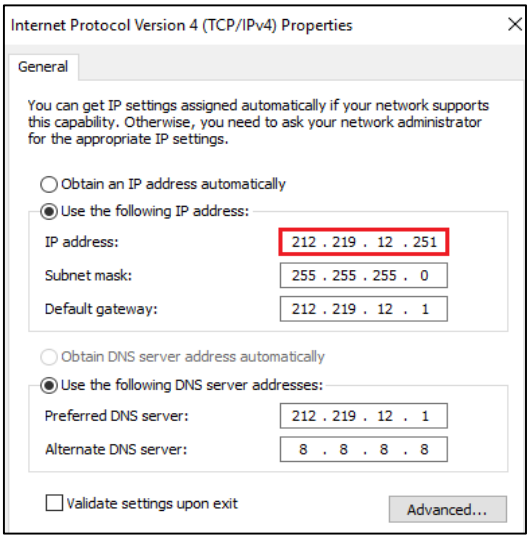

Figura 15. Configuración de dirección IP estática en el host.

Una vez instalado el PRTG, se ingresa a Herramientas Administrativas de PRTG, en web server, seleccionamos el puerto 8080 y la dirección IP que tiene asignado el host.

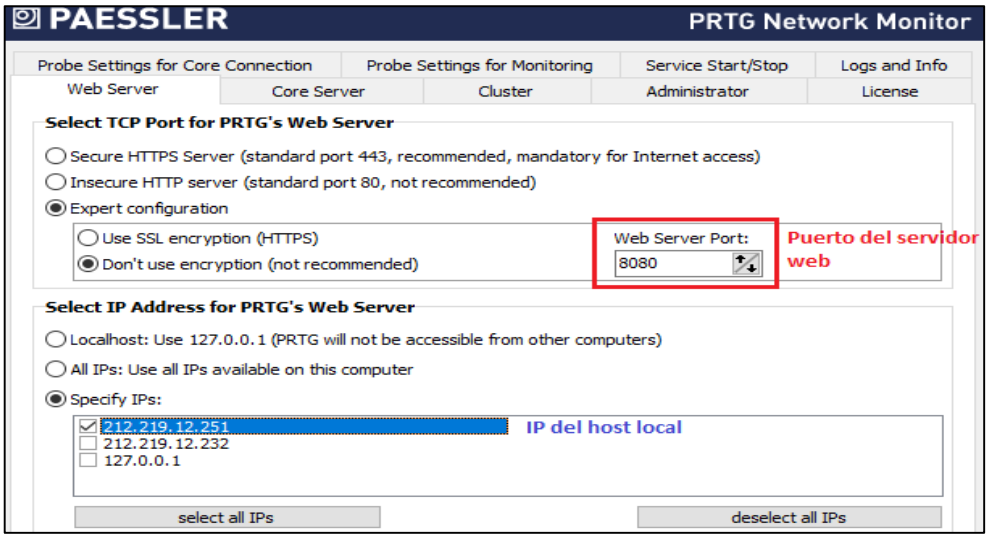

Figura 16. Configuración Web server.

Posteriormente se inician los servicios del núcleo del PRTG, permitiendo acceder al servidor web local, a través del protocolo HTTP.

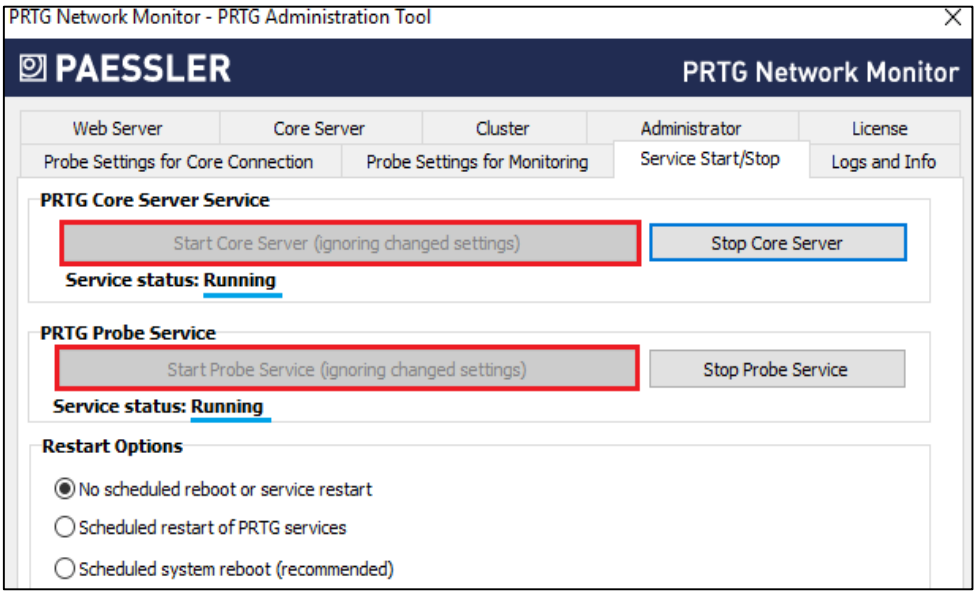

Figura 17. Inicio de servicios del NMS.

Se ejecuta la aplicación Monitoreo de Red PRTG y se agrega el dispositivo Agente, con las configuraciones necesarias para establecer la comunicación a través del protocolo SNMP.

En este mismo orden de ideas, se configura la dirección IP del Agente. Esta dirección IP es especial, porque es la interfaz por donde circulará todo el tráfico de entrada de los dispositivos finales como las estaciones de trabajo, VoIP, Video vigilancia.

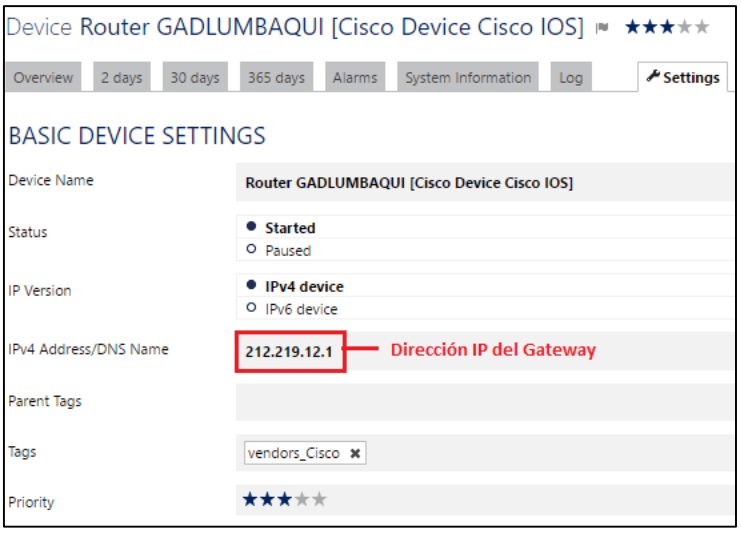

Figura 18. Configuración de IP para monitoreo.

Seguidamente se configuran las credenciales SNMP.

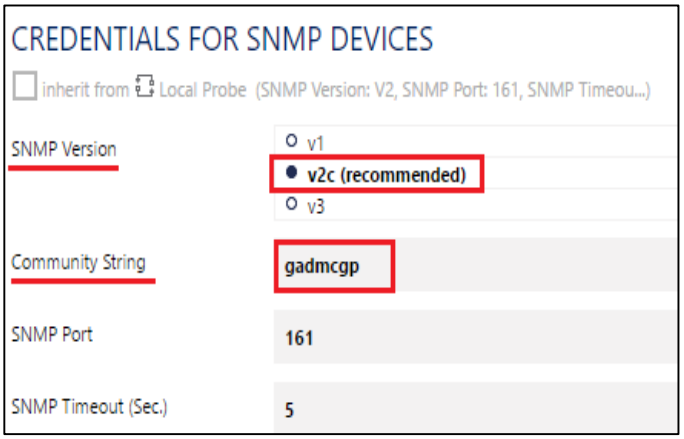

Figura 19. Configuración credenciales SNMP.

El GADMCGP, utiliza servicios externos para guardar información importante que generada en la Institución a través del Sistema de Gestión Documental *QUIPUX*, que es la herramienta principal de trabajo en donde se genera información digital como oficios, memorandos, circulares y así mismo se requiere una alta disponibilidad del Internet. Por otra parte el correo y la Página Web Institucional son de uso diario.

La Institución no ofrece servicios públicos, por lo tanto no existe medición del tráfico de entrada por usuarios remotos o del Internet.

En la tabla 4 se muestra el consumo de ancho de banda de los servicios de Internet más importantes a los que acceden los funcionarios internos del GADMCGP. Se analizó durante 30 días, no incluidos los días sábados y domingos. El tráfico generado tiene un consumo de 1.100.363.559 Kbyte (1.074.574 Mbyte). Por otra parte se crearon 4 sensores para analizar tráfico HTTP, en donde se configuraron las direcciones de los dominios de las aplicaciones de QUIPUX, CORREO INSTITUCIONAL, SERCOP, PAGINA WEB.

Tabla 4.

Consumo de datos

Servicio	**Consumo en porcentaje %**	**Consumo en GB**
QUIPUX	19,08	200,23
CORREO INSTITUCIONAL	12,88	135,12
SERCOP	2,20	23,1
PAGINA WEB	14,34	150,5
OTROS	51,50	540,44
TOTAL	100,0	1049,39

Nota: Descripción de los servicios y consumo en *Gigabytes.*

Por otra parte la figura 21, que representa el consumo en porcentaje muestra cómo el consumo de otros servicios es el más alto, esto quiere decir que hay acceso a otra información que no es de suma importancia para la Institución, por lo tanto se puede aplicar políticas de calidad de servicio, dar más prioridad

a las páginas con mayor uso para evitar retardos tanto en la carga como descarga de la información.

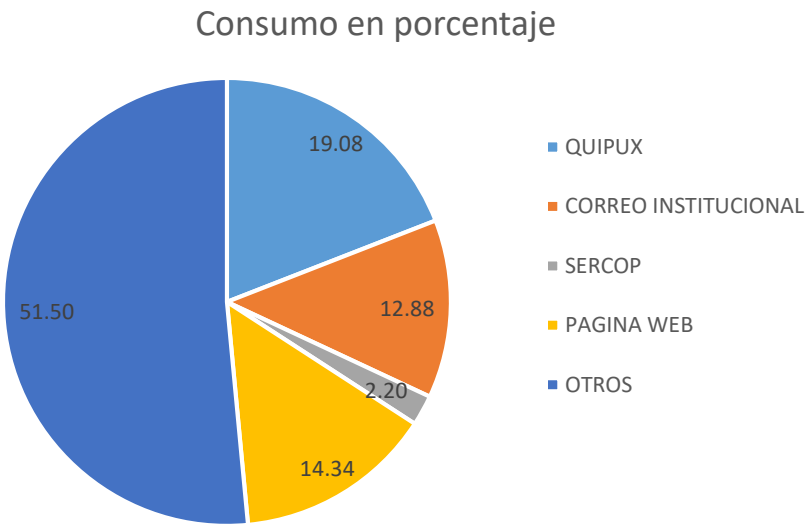

Figura 20. Consumo del canal de datos en porcentaje.

La figura 22 muestra que el consumo de otros servicios es el doble del consumo de la información que en realidad se necesita, siendo un punto muy importante de tomar en cuenta momento de crear las nuevas políticas del rediseño de la red.

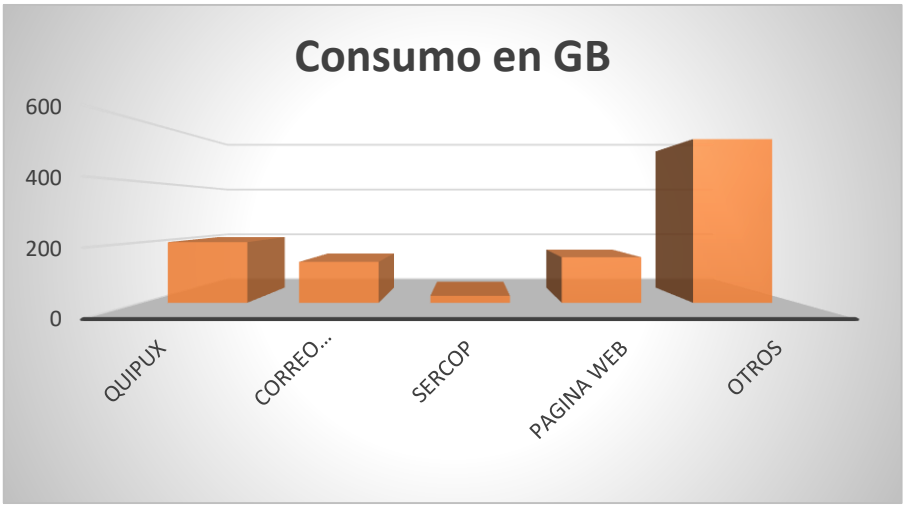

Figura 21. Consumo de recursos en GB del canal de datos.

El software PRTG, permite obtener reportes reales y con mayor detalle.

El reporte en un tiempo determinado, fue tomado en el periodo comprendido del 29/03/2017 a las 13:31:00 hasta el 10/05/2017 a las 13:31:00, cabe destacar que el análisis se hizo en el horario de la jornada laboral habitual del personal, es decir desde las 7:30am a 16:30 pm.

Esto fue posible por un tipo de sensor llamado analizador de tráfico, el cual efectuaba el análisis con un intervalo de 60s.

El dispositivo de prueba, en este caso fue el router Cisco 800, el cual es el agente que envía la información al host de destino.

El tiempo real ejecutado para el análisis del tráfico fue de 7 días, 21 horas 50 minutos con 2 segundos, esto referencia el total de horas consideradas en el mes.

El trafico promedio que se genera o soporta la red a diario es de 13622 Kbit/s= 13,3 Mbit/s.

El tráfico total generado al mes es de 1100363559Kbyte=1049,39 GBytes. Así lo detalla la figura 22:

Report for (001) FastEthernet0 Traffic

Report Time Span:	29/03/2017 13:31:00 - 10/05/2017 13:31:00					
Sensor Type:	SNMP Traffic 32bit (60 s Interval)					
Probe, Group, Device:	Local Probe > Local Probe > Router GADLUMBAQUI [Cisco Device Cisco IOS]					
Uptime Stats:	Up:	99,995 %	[7d21h50m2s]	Down:	0,005 %	[35s]
Request Stats:	Good:	99,432 %	[11376]	Failed:	0,568 %	[65]
Average (Traffic Total):	13.622 kbit/s					
Total (Traffic Total):	1.100.363.559 KByte					
Percentile	29.179 kbit/s					

Figura 22. Reporte de tráfico generado por los usuarios finales en PRTG.

El GADMCGP tiene un contrato de servicios con la Corporación Nacional de Telecomunicaciones (CNT), que especifica las siguientes condiciones: es una

línea dedicada, cuyo medio de transmisión de la última milla es fibra óptica y un ancho de banda de 10 Mbps sincrónica; la misma velocidad para descarga y carga de información. Por lo tanto la capacidad de ancho de banda de entrada supera la de salida, debiendo hacer los cambios necesarios los cuales serán expuestos en la fase de diseño.

3.8 Análisis del flujo de información interna

Las aplicaciones internas también consumen ancho de banda a nivel de la red privada. Los usuarios internos hacen uso de los servicios a diario, todo el acceso a la información es limitado y asignado a cada departamento a través de la instalación de aplicaciones estáticas; cabe indicar que no son aplicaciones web.

Tabla 5.

Aplicaciones autorizadas por departamento

DEPARTAMENTO/ APLICACIÓN	SIGAME	GCS	SIC	SARP	Cámaras	Lince Web/ Biométrico
ADMINISTRATIVO	X					
BODEGA	X					
CATASTRO Y AVALÚOS			X			
CONTABILIDAD	X					
FINANCIERO	X					
REGISTRO DE LA PROPIEDAD				X		
RENTAS	X	X				
SECRETARÍA GENERAL	X					
SERVICIOS BÁSICOS		X				
SISTEMAS	X	X	X	X	X	X
TALENTO HUMANO	X				X	X
TESORERÍA	X	X	X	X		

Nota: Muestra cómo están asignados los servicios por departamento.

Con la presentación de estos datos, se puede identificar, que la red interna necesariamente debe implementar una segmentación de la red general en subredes más pequeñas, para crear grupos más pequeños de dispositivos y servicios con los siguientes fines:

- El control del tráfico mediante la contención del tráfico de *broadcast* dentro de la subred.
- La reducción del tráfico de la red y el mejoramiento del rendimiento de esta.

La división en subredes es el proceso de segmentación de una red en varios espacios de red más pequeños o también llamado subredes. Todas las áreas del GADMCGP pertenecen a la VLAN 1.

Al existir varios servicios en la red interna, el flujo de la información puede desbordar la capacidad del canal, ya que los switch tienen puertos *Fast Ethernet*, por lo tanto la capacidad del canal es de 100 Mbps sin considerar el tráfico de control y que no afecte el *throughput*. Todo esto se toma en cuenta debido al uso de las cámaras IP, que al ser dispositivos de red, envían datos por el mismo medio de la red interna. Para solventar este problema, existen protocolos como *EtherChannel*, que pueden agrupar varios enlaces físicos y funcionar como un enlace lógico, permitiendo aumentar el ancho de banda e implementar redundancia de los medios.

4. CAPÍTULO IV. FASE DE DISEÑO

Este capítulo comprende el diseño físico y lógico de la red de conectividad del GADMCGP, basándose en un modelo de seguridad SAFE y los distintos protocolos que permitirán diseñar una red conforme a los requerimientos y análisis realizados en los capítulos anteriores.

4.1 Diseño de la red lógica

El análisis de la red física basándose en la arquitectura SAFE, muestra la necesidad de las siguientes características:

- Redundancia de dispositivos en el módulo Central.
- Redundancia de dispositivos en el módulo de Internet.

- Redundancia de dispositivos en el módulo de Servidores.
- Redundancia de medios de transmisión en el módulo de Distribución.

Se consideran estos aspectos porque el diseño de la red lógica debe mostrar las configuraciones de dichos dispositivos.

El GADMCGP, tiene una infraestructura totalmente antigua, donde existen aplicaciones que cada vez exigen recursos y disponibilidad en la red interna. Así mismo hay la propuesta de proyectos que van a exigir una red de conectividad estable para acceder a las aplicaciones de una manera eficiente y poder atender a los ciudadanos de la mejor manera.

La propuesta de este diseño lógico, comprende el direccionamiento, enrutamiento y la configuración necesaria para todos los dispositivos que formarán parte de la Infraestructura de red.

4.2 Direccionamiento

El análisis realizado a la red actual, evidencia la inexistencia de una segmentación de la red, permitiendo a todos los usuarios tener acceso al servidor local. Para dar un control de acceso se propone realizar una segmentación por departamentos y permitir el acceso limitado, evitando la vulnerabilidad de la información. Por otra parte, la necesidad de incluir dispositivos independientes con funciones específicas, ayudará a mejorar el rendimiento de los mismos y minimizar los tiempos de respuestas ante posibles fallas de la conectividad de la red.

Para realizar la segmentación de la red, se estimó conjuntamente con el jefe de Talento Humano un porcentaje de crecimiento del 30% del personal de la Institución, por lo que la información de la tabla 6 identifica y presenta las subredes incluyendo la cantidad de hosts real.

Tabla 6.

Segmentación de la red interna del GADMCGP

Departamento	Cantidad	VLAN	Red
Dirección de Obras Públicas	68	10	10.10.10.0/26
Dirección Administrativa	53	15	10.10.10.64/26
Dirección de Planificación	45	20	10.10.10.128/26
Cámaras	30	25	10.10.10.192/27
Dirección de Gestión de Riesgos	23	30	10.10.10.224/27
Dirección Financiera	23	35	10.10.11.0/27
Impresoras	23	40	10.10.11.32/27
Dirección de Servicios Básicos	21	45	10.10.11.64/27
Coordinación de Gestión Turística	15	50	10.10.11.96/28
Gestión de Inclusión y Acción Social(GIAS)	15	55	10.10.11.112/28
Secretaría General	12	60	10.10.11.128/28
Concejales	9	65	10.10.11.144/28
Servidores	8	70	10.10.11.160/28
Sistemas	8	75	10.10.11.176/28
Asesoría Jurídica	6	80	10.10.11.192/29
Auditoría Interna	3	85	10.10.11.200/29
Alcaldía	2	90	10.10.11.208/29

Nota: Identifica y presenta las subredes incluyendo la cantidad de hosts real.

Esta segmentación de VLANs permitirá realizar un control de acceso hacia las aplicaciones, y poder realizar un análisis de tráfico.

4.3 Enrutamiento

El enrutamiento permite y favorece buscar el mejor camino para que la información llegue lo más rápido a sus destinos, además existen protocolos de enrutamiento que dependiendo la necesidad de las redes son aplicadas para mejorar el rendimiento y la manera de responder ante posibles cambios.

El enrutamiento será mediante una ruta STUB o por defecto, es decir una única salida al Internet. Esta parte será expuesta en la fase configuración.

El protocolo de enrutamiento entre el modulo Central y el de Distribución, será OSPF (*OpenShorest Protocol First*). Se debe recordar que se va a implementar una VPN para el acceso remoto hacia las aplicaciones SIG-AME, GCS, SIC y SARP, por lo tanto el enrutamiento hacia la SUCURSAL será también OSPF.

4.3.1 Ventajas de OSPF

- Envía las actualizaciones cuando existe un cambio en la red, por lo tanto no consume recursos constantemente y el tiempo de convergencia es rápido.
- Permite enviar la máscara de la red, no existirá bucles de enrutamiento y los paquetes no se descartan.
- Los routers conocen la topología de la red.
- Las bases de datos de estado de enlace se pueden minimizar al diseñar la red con cuidado.

Por último la razón de elegir éste protocolo de enrutamiento dinámico para comunicar la Institución con la sucursal es, que es un estándar, es decir que la información es expuesta y abierta a todas las empresas que deseen desarrollar e implementar el estándar en sus equipos de redes; esto facilitará la adquisición de los dispositivos sin considerar marcas, sino características técnicas.

4.4 Configuración

Esta sección mostrará la configuración de todos los dispositivos que formarán parte de la red interna, teniendo en cuenta la topología física y los requerimientos analizados en conjunto con el personal del departamento de tecnología del GADMCGP.

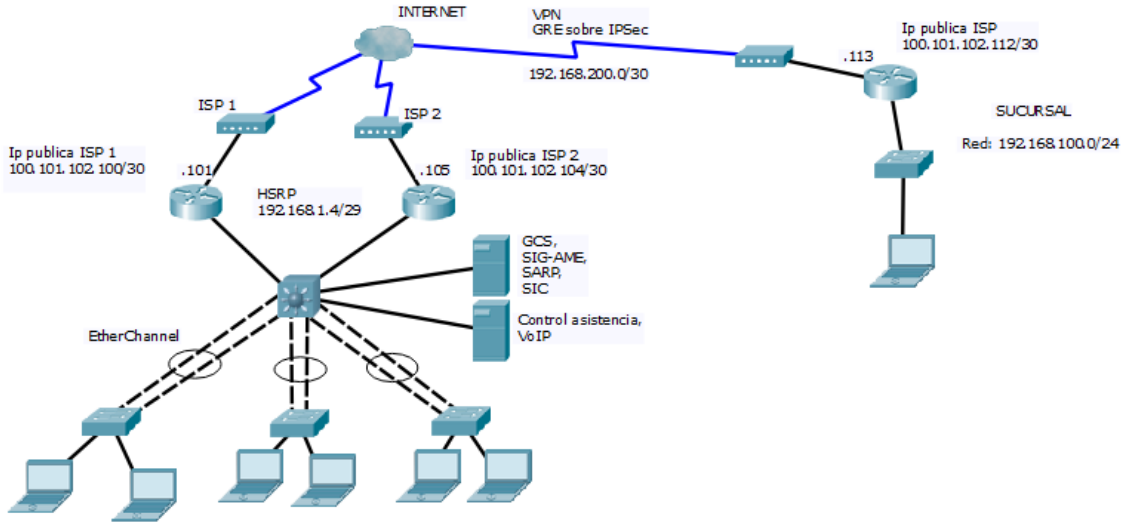

Figura 23. Topología física de la nueva red de conectividad.

SAFE es una guía para implementar la seguridad en la red de la Institución. No es un una normativa ni tampoco sirve de diseño global para proporcionar una seguridad total a todas las redes existentes. SAFE, es más bien una plantilla, pensada para que los diseñadores de redes sepan cómo diseñar e implementar una red y poder satisfacer los requisitos de seguridad de una empresa. Es la primera configuración de seguridad, donde es necesario crear claves para las líneas de acceso, tanto para la consola, auxiliar y líneas remotas (*telnet*). El acceso remoto hacia los dispositivos será mediante SSH, que es la versión encriptada de *telnet*, la misma que usa una encriptación *RSA (Riviest Shamir Aldleman).*

En este sentido, bloquear los dispositivos por número de intentos fallidos por un tiempo determinado, será importante para minimizar el riesgo de que los hackers tomen el control de la red.

Esta configuración será necesaria aplicarla en todos los dispositivos de red, lo que permitirá minimizar el riesgo de acceso no autorizado y empezar con la primera norma para el GADMCGP. (Ver Anexo 1)

4.5 Configuración de módulo de acceso

En este módulo se implementará lo siguiente:

Seguridad.- Los puertos se configuran en modo seguro, en donde máximo aceptará 5 direcciones físicas, así mismo guardará las direcciones persistentes en la configuración por defecto, para mantener la tabla MAC de los dispositivos de acceso (*Switch*), actualizada. Por otra parte, al existir una violación los puertos deben apagarse y notificar inmediatamente; este método de puerto seguro obliga al puerto que entre en modo error, en este orden de ideas, en los equipos CISCO la configuración en modo *Shutdown* viene por defecto.

Conjuntamente los puertos configurados como troncales por donde pasará el tráfico etiquetado, deben cambiarse por una VLAN diferente a la de por defecto que es el VLAN1. Así mismo serán los únicos puertos que recibirán peticiones del servidor DHCP; ningún otro puerto será un puerto de entrada para recibir direcciones IP de otro servidor DHCP.

Velocidad.- Los puertos de acceso se configurará como puertos de alta velocidad o *PortFast*, esto ayudará a que la transición del estado de bloqueo a reenvío se realice de manera inmediata. (Ver Anexo 2)

4.6 Configuración del módulo de distribución

Para mejorar la velocidad de la información al servidor, se plantea implementar E*therChannel*, la cual es una forma de agregación de enlaces usado en redes conmutadas o entre *switchs.*

Algunas de las ventajas de la agregación de enlaces son:

- Balanceo de carga entre los enlaces que conforman el *EtherChannel*.
- Se elimina la necesidad de *Spanning Tree Protocol (STP),* ya que es visto como un solo enlace lógico.
- Provee redundancia, si se da de baja un enlace físico, no causa ningún cambio en la topología y no requiere recalculación de *STP*.
- Mayores velocidades: se tiene un ancho de banda de más capacidad, por ejemplo si se tiene puertos de 1Gb, se puede agrupar 6 canales físicos a través de *EtherChannel* verlo como un solo camino lógico, con una capacidad del canal de 6Gb/s.

La configuración de VTP (*Vlan Trunking Protocol*), en modo servidor se implementa para que sea el único que envíe las actualizaciones hacia los Switch clientes, así permitirá mejorar el rendimiento y tener una mejor organización en la creación de nuevas VLANs. También cada subred hará peticiones a un servidor DHCP para obtener una dirección IP automáticamente; el servidor DHCP estará habilitado en el módulo central el cual enviará las repuestas a las solicitudes de las subredes.

La creación de listas de acceso para limitar el ingreso a las aplicaciones internas, solo dará acceso a la información a los departamentos autorizados. Es importante considerar que este conjunto de reglas que permiten el tráfico (entradas o salidas), deben seguir un orden específico. Cisco recomienda a través de la regla *Access Control Entry (ACE)*, que la última pauta sea un *deny (denegar)* de todo; pues será mejor tener todo cerrado e ir abriendo reglas.

Algunos Departamentos del GADMCGP, se han incluido en las VLAN de las Direcciones, para tener un mejor control del tráfico y acceso a las aplicaciones internas. Se creó una VLAN para los servidores y no se implementa servicio DHCP para esta VLAN por motivos de seguridad y futuro despliegue de aplicaciones web para el acceso mediante el Internet. Se crea una lista de acceso extendida, porque es más explícita, permitiendo o denegando el flujo del tráfico mediante la detección de puerto y la dirección de red del destino.

Por lo tanto se genera una lista de acceso, que permita el ingreso a las aplicaciones SIG-AME, GCS, SARP y SIC, en donde sólo los departamentos autorizados pueden ingresar o actualizar información. Estas aplicaciones se acceden a través del protocolo http y ftp, cuyo número de puerto es el 80 y 22 respectivamente. Así mismo el VLAN de Sistemas tendrá total acceso a todos los servicios internos.

Además se crea una segunda lista de acceso, a la que sólo tendrá entrada del video de las cámaras, la VLAN de Sistemas. Cabe destacar que la red es escalable, las listas de acceso se pueden editar según las necesidades o medidas preventivas que sugiera el personal de soporte técnico de la Unidad correspondiente. A continuación se muestra la configuración del dispositivo del módulo de distribución; esto corresponde a los requerimientos de redundancia de medios, seguridad, escalabilidad, mayores velocidades de acceso y menores tiempos de respuestas.

La conexión con el modulo central será a través de 2 enlaces, que estarán en la misma red. Cada interfaz del dispositivo del módulo de distribución representa una red diferente, y para poder dar solución al requerimiento de la Institución referente a una alta disponibilidad del acceso a Internet, se implementa HSRP, que consiste en la creación de un router virtual, el cual ordena a un router determinado a ser el activo y al siguiente router a ser el pasivo o estado *standby*. Todo esto a la espera de que suceda un error a nivel software o hardware para asumir la función de router activo. La configuración que se realiza en el módulo de distribución será para crear la VLAN 110 y que todo el tráfico que entre desde el modulo central sea por la VLAN propuesta, esto se realiza porque la implementación de HSRP requiere que los 2 router formen parte de la misma red, que en este caso es la 192.168.1.0 con máscara 255.255.255.248. (Ver Anexo 3)

4.7 Configuración del módulo central

Cada dispositivo que forma parte de los módulos correspondientes cumplen una función especial, el diseño que se propone no sigue los pasos exactos de algún estándar, más bien estudia los protocolos necesarios para aplicarlos en la red de conectividad y satisfacer las necesidades del cliente. También la red expuesta ofrecerá escalabilidad, debido a que existen proyectos a futuro a ser implementados por parte de la Institución, como en el caso del acceso web para que los clientes puedan ver su estado de cuenta o saldos pendientes, el acceso gratis al Internet en el centro de la ciudad, en donde se está construyendo un parque recreativo.

Éste módulo central o limite empresarial, debe dar prioridad al tráfico más importante. Analizando los requerimientos del GADMCGP, el acceso a las aplicaciones como el QUIPUX, SERCOP, CORREO son muy necesarias para el desarrollo de las actividades diarias de los empleados internos. Así mismo la limitación del acceso a las redes sociales, ya que en la fase de planificación se observa que la mayoría de peticiones hacia el internet son el acceso a redes sociales como *FACEBOOK* y de video como *YOUTUBE*. El objetivo de este diseño no es bloquear el acceso a las redes sociales, sino más bien clasificar el tráfico desde lo más importante hasta lo que en realidad no es necesario.

En este orden de ideas, Calidad de Servicio (*QoS*) sólo funciona cuando hay congestión, esto con el fin de minimizar la pérdida de paquetes, *Jitter* y Latencia alta. La congestión aparece cuando el tráfico supera al ancho de banda máximo que permite el dispositivo. Cabe indicar que el retardo es inevitable ya que no se puede controlar por donde viajan los datos y se desconoce cuáles son los medios que utiliza el proveedor de servicio de Internet, por lo tanto el tiempo de respuesta de las peticiones serán variables. Existen algunos algoritmos de encolamiento que se asocian con los modelos de QoS, para éste caso se aplicará el modelo de *DiffSer* (Servicios diferenciados) MQC (*Modular QoS CLI*), quien realiza la clasificación del tráfico a través de *class-map*, luego se agrega el *class-map* a un *policy-map*, en

donde definimos ancho de banda o prioridad, y finalmente aplicamos a una interfaz o subinterfaz mediante el comando *service-policy.*

Por ello, los comandos *bandwidth* y *priority* ofrecen garantías de ancho de banda a los paquetes que coinciden con aquellos criterios para la clase de tráfico, sin embargo cuentan con diferencias funcionales, en donde será necesario elegir la mejor opción. Para el caso requerido se han creado 2 clases: la clase REDES-SOCIALES, en donde se marca el tráfico que contenga en el texto de petición HTTP palabras claves, por ejemplo "*youtube*", por otra parte, la clase SERV-INTERNET, hace referencia a las aplicaciones externas muy importantes y que exigen un ancho de banda siempre disponible para cargar y descargar información, en este caso se marca el trafico http mediante la url, por ejemplo www.gestiondocumental.gob.ec. A continuación se crea la política para relacionar las clases y asignar un ancho de banda o prioridad específico; para la primera clase se configura una prioridad del 5%, en este caso el ancho de banda que ofrece el proveedor al GADMCGP es de 10Mbps, por lo tanto la clase tendrá un ancho de banda de 0,5 Mbps, se aplica el comando *priority* porque durante condiciones de no congestión, esta clase de prioridad no puede utilizar ningún ancho de banda en exceso, así se mantiene el canal libre para otros servicios y para la segunda clase se configura un ancho de banda del 60%, correspondiendo a 6 Mbps y se aplica el comando *bandwidth* porque en congestión permite exceder la velocidad asignada.

Por otra parte, el modulo central será servidor *DHCP*, dando *IPs* automáticamente a los host correspondientes de cada VLAN creadas en el módulo de distribución.

La propuesta de este diseño lógico, ofrece disponibilidad del Internet a través de la configuración de HSRP. No se puede aplicar este protocolo con 2 dispositivos en el módulo central si se tiene un solo proveedor de servicio, si el problema es a nivel de hardware se soluciona inmediatamente pero si el servicio se suspende será innecesario tener redundancia de equipos y de otro proveedor.

Finalmente, para satisfacer una necesidad considerada importante en la Institución, como lo es la apertura de una ventanilla única en la parroquia de EL Reventador, se propone la implementación de una Red Privada Virtual (VPN), la que permitirá tener acceso a los servicios internos del GADMCGP para que los ciudadanos puedan realizar sus pagos correspondientes. Es necesario indicar que la información que viaja a través de los medios debe cumplir con los requisitos de seguridad, como confidencialidad, integridad y autenticación. Una VPN es usada para crear un túnel privado sobre una red pública y permite que esta información viaje segura a través de la encriptación de los datos y la autenticación para protegerlos del acceso no autorizado.

Para ello, IPsec (Internet Protocol Security), es un protocolo que define como una VPN debe ser configurada de una manera segura usando el protocolo de Internet, lo cual ofrece seguridad entre el camino de un par de *gateways*, un par de host o *gateway* a host.

La configuración de modulo central incluye:

- Servicio DHCP
- Protocolo HSRP, redundancia de equipos para ofrecer disponibilidad.
- Seguridad de líneas de acceso y control.
- Conexión a Internet.
- SSH versión 2.
- Red Privada Virtual; GRE sobre IPsec.
- Calidad de servicio.
- Protocolo de enrutamiento OSPF. (Ver Anexo 4)

La configuración del acceso remoto desde la sucursal, contiene lo siguiente:

- Servicio DHCP
- Seguridad de líneas de acceso y control.
- Conexión a Internet.
- SSH versión 2.
- Red Privada Virtual; GRE sobre IPsec.

- Calidad de servicio.
- Protocolo de enrutamiento OSPF. (Ver Anexo 5)

4.8 Diseño de la red física

Respecto al análisis de la red física realizada, el módulo de las oficinas ventrales de la empresa con la arquitectura modular de SAFE. El diseño actual presenta algunas características que no se cumplen y que se consideran necesarias para que la red sea administrable.

La propuesta de la red física, incluye las características de los dispositivos que formarán parte de la nueva red de conectividad del GADMCGP. Cabe destacar que esta arquitectura empresarial satisface todos los requerimientos de la Institución y que propone la solución para futuros proyectos.

4.8.1 Dispositivos de las oficinas centrales de la empresa

El módulo de las oficinas centrales de la empresa en la red actual del GADMCGP, no presentan garantías de seguridad, disponibilidad, escalabilidad y calidad de servicio. La propuesta del diseño de red física es totalmente nueva, no se toma en cuenta ningún dispositivo de la red actual, por la antigüedad y por la carencia de características y protocolos que se requieren para satisfacer las necesidades de la Institución.

Debido a que la administración centralizada es un requisito esencial para tener conocimiento de todo lo que sucede en la red de conectividad y además que es una recomendación de SAFE, se agregará el módulo de gestión.

4.8.2 Módulo central

Router

Este dispositivo debe soportar los siguientes protocolos y características mínimas:

- Protocolos: *IPv4, IPv6, Open Shortest Path First (OSPF).IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, Hot Standby Router Protocol, MPLS, 802.1 ag, 802.3ah, Simple Network Manager Protocol (SNMP), L2 y L3 VPN, Secure Shell (SHH) Protocol.*
- Encapsulación: Ethernet, 802.1q, Multilink Point-to-Point Protocol (MLPPP), Frame Relay, High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, EIA-530).
- Administración de tráfico: *QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Policy-Based Routing (PBR), Network-Based Advanced Routing (NBAR).*
- Interfaces: 10/100/1000 Gigabit Ethernet puerto WAN/LAN

4.8.3 Módulo de distribución

Switch de capa de 3

- *Ethernet IEEE 802.3*
- *OSPFv2, OSPFv3*
- *10 GigaEthernet: IEEE 802.3ae*
- *IEEE 802.1D Spanning Tree Protocol*
- *IEEE 802.3ad / Link Aggregation Control Protocol (LACP)*
- *IEEE 802.1p CoS Prioritization*
- *IEEE802.1Q VLAN*
- *IEEE 802.1X User Authentication*
- *Secure Shell (SHH) Protocol*

4.8.4 Módulo de acceso

Switch de capa 2

- *Automatic QoS(AutoQoS)*

- *Auto-negotiation*
- *48 GigaEthernet: IEEE 802.3ae*
- *Dynamic Trunking Protocol (DTP)*
- *IEEE 802.3ad / Link Aggregation Control Protocol (LACP)*
- *Automatic media-dependent interface crossover (MDIX)*
- *Multicast VLAN Registration*
- *Vlan Trunking Protocol.*
- *Trivial File Transfer (TFTP)*
- *Network Timing Protocol (NTP)*
- *DHCP Snooping*
- *Dynamic ARP Inspection (DAI)*
- *IP source guard*
- *Port-based ACLs*
- *Secure Shell (SHH) Protocol*
- *Simple Network Management Protocol Version (SNMP).*
- *Port Security*
- *MAC Address Notification*
- *Bridge Protocol Data Unit (BPDU) Guard.*

4.8.5 Módulo de Gestión

El modulo será un valor agregado al nuevo diseño de la red de conectividad del GADMCGP, ya que es una recomendación de SAEF y además facilita la gestión segura de los dispositivos de la arquitectura de red. Para minimizar el gasto, formará parte del módulo de servidores, por lo tanto forma parte de la VLAN Servidores.

La agregación de los servidores permitirá realizar una gestión centralizada de la red, Por otra parte brinda mayor seguridad los servidores que contienen las aplicaciones y servicios.

Los servidores a implementarse son:

- Servidor de Gestión, *Simple Network Manager Protocol* (SNMP): ayudará a supervisar o monitorear el funcionamiento de la red, detección de errores, análisis de tráfico de las interfaces, esto permitirá realizar una gestión de cambios en los routers o switch, para la generación de nuevas políticas.

- Servidor NTP: permitirá mantener sincronizada la hora de todos los dispositivos de la red privada. Todo esto con el fin de relacionar los eventos basándose en la secuencia real de la hora de ocurrencia de un evento, así se podrá solucionar los problemas de manera más eficaz.

- Servidor de registro de logs: almacenará y clasificará los registros de los eventos ocurridos de todos los dispositivos de red. Este servidor estará configurado para recibir un nivel 0 hasta el nivel 4.

  Nivel 0: Emergencia, es decir el sistema está inusable.

  Nivel 1: Alerta, se necesita una acción inmediata.

  Nivel 2: Crítico, condición crítica.

  Nivel 3: Error, condición de error.

  Nivel 4: Peligro, condición de peligro.

  El módulo de gestión quedaría como lo muestra la figura 25:

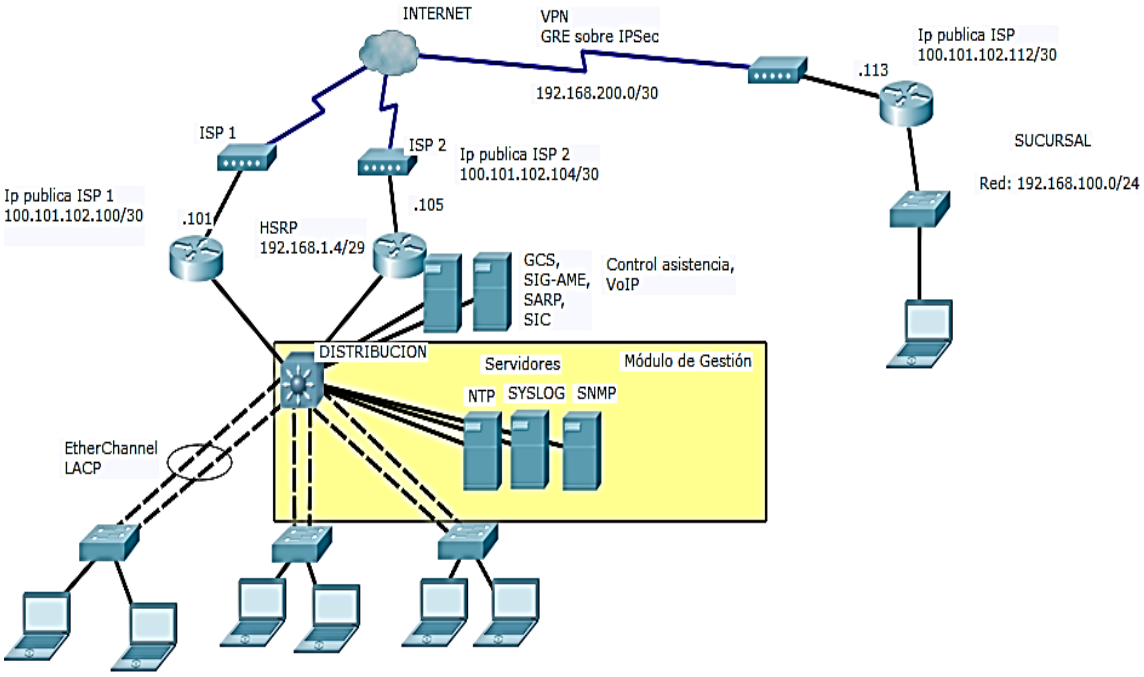

Figura 24. Módulo de gestión de la nueva red.

4.9 Presupuesto referencial para la implementación de la nueva red de conectividad del GADMCGP

El estudio del presupuesto referencial para la implementación de la nueva red de conectividad, incluye los equipos que forman parte de un modelo de diseño jerárquico de 3 capas. El estudio para el presupuesto sólo incluye dispositivos de red y los medios para interconectarlos. Además los precios de referencias son analizados con empresas locales dedicadas a las actividades de diseño de redes de datos e incluyen la configuración de los mismos.

Los equipos propuestos a continuación cumplen con las características necesarias para satisfacer los requerimientos de la Institución.

Tabla 7.

Descripción del presupuesto por módulos

Dispositivo	Descripción	Cantidad	Precio	Total
Modulo central y sucursal	Cisco CISCO2901/K9 2901 Security Bundle with License	3	$ 1.885,00	$ 5.655,00
Módulo de distribución	Cisco Catalyst 4500-X - Switch - 10 ports - Rack-mountable (WS-C4500X-F-16SFP+)	1	$ 8.944,00	$ 8.944,00
Módulo de acceso	Cisco WS-C2960S-48TS-S 2960 48 10/100/1000 Port Gigabit Switch	3	$ 1.430,00	$ 4.290,00
Punto de red	Punto certificado de red; cumplimiento del estándar TIA-942. El punto incluye cable UTP Cat 6, Canaletas, Cajetín y Patch hembras, etiquetado.	90	$ 180,00	$ 16.200,00
			Subtotal	$ 35.089,00
			IVA 12%	$ 4.210,68
			TOTAL	$ 39.299,68

Nota: Establece el total de recursos financieros que serán indispensables en la ejecución de cada módulo

5. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se realizó el análisis de la red de conectividad del GADMCGP y se determinó que los dispositivos y medios de transmisión no son aptos para soportar nuevas aplicaciones y futuros proyectos que exigirán disponibilidad, seguridad, escalabilidad y calidad de servicio.

El protocolo *EtherChannel*, permite agrupar varios canales físicos y verlo como un solo enlace lógico, esto permite un alto grado de disponibilidad de los *switchs* de acceso hacia el módulo de distribución, además el ancho de banda del canal tendrá más capacidad.

Se revisó el tráfico generado de entrada y salida del módulo central el cual presenta un cuello de botella, es decir la capacidad del ancho de banda que ofrece el ISP es menor al tráfico que exige la red de privada del GADMCGP.

Se realizó un diseño de red que ofrece calidad de servicio, dando prioridad a las aplicaciones muy importantes que la Institución usa a diario, como es el Sistema de Gestión Documental y se da un acceso limitado a páginas que consumen recursos como redes sociales y de video *streaming*, mejorando así la velocidad de acceso.

Calidad de Servicio es útil en situaciones de congestión, debido a que permite dar prioridad al tráfico sensible a retardos como la *VoIP*, video-llamadas, pero a la vez se necesita tener acceso a los dispositivos de red para realizar un monitoreo mediante protocolos como *SNMP*, con la finalidad de clasificar el tráfico y aplicar políticas que mejoran el acceso a las aplicaciones del Internet.

La implementación de la VPN es una solución para solventar la necesidad de una ventanilla única en la Parroquia de El Reventador, por lo tanto se cumple con los requerimientos de la Institución y mejora de manera eficiente el acceso a la información y pago inmediato de servicios públicos a la ciudadanía.

El diseño de la red WAN (*Wide Area Network*), entre la Institución y la Sucursal, se encarga el proveedor de Internet, el cual es el responsable de que la conexión siempre esté disponible para acceder a las aplicaciones y recursos de la red privada del GADMCGP.

La propuesta del módulo de Gestión permitirá centralizar el control y la administración de toda la arquitectura de la red de conectividad, ayudando así a monitorear la red, actuar ante posibles fallas de manera eficaz, realizar tareas de auditoría y la correlación de eventos.

Recomendaciones

Un diseño de red está expuesto a cambios constantes, por lo que es necesario tener en cuenta la escalabilidad para que la red permita agregar o quitar dispositivos, pero que a la vez no afecten el rendimiento del mismo.

No existe un estándar general para el diseño de redes LAN, cada diseñador de redes crea un modelo esencial conforme a los requerimientos del cliente, por lo tanto es necesario realizar un análisis o planificación para definir los nuevos parámetros.

Se recomienda siempre utilizar software que permita simular un ambiente de pruebas y tener la certeza de los protocolos que se van a implementar. Esto ayudará también a verificar el funcionamiento de las configuraciones, pruebas de control y cambios en la red, para así evitar posibles problemas de disponibilidad y desempeño de la red a futuro.

Se recomienda realizar un análisis del tráfico tanto de entrada como de salida, para poder aplicar políticas de calidad de servicios y así mejorar el acceso a los servicios internos y externos. Con esto se evita la pérdida de paquetes y actuar de manera eficientes cuando existe congestión en la red.

REFERENCIAS

Adell, J. (1998). *Redes y educación*. Recuperado el 5 de abril de 2017 de http://elbonia.cent.uji.es/jordi/wp-content/uploads/docs/Adell_redesyeducacion.pdf

Aguaiza, D. (2016). *"Propuesta de rediseño de la infraestructura de red de la Universidad Laica "Eloy Alfaro" de Manabí, para ofrecer un modelo de servicios con calidad de servicio (qos)* ". Quito, Ecuador: Facultad de Ingeniería - Pontificia Universidad Católica del Ecuador-Maestría en Redes de Comunicaciones.

CISCO Systems. (2000). CISCO SAFE*: Un modelo de seguridad para las redes de las empresas.* New York: Cisco System.

Davis, D. (2017). *Techrepublic.* Recuperado el 24 de abril de 2017 de http://www.techrepublic.com/blog/data-center/what-can-ciscos-network-based-application-recognition-nbar-do-for-you/

Gilchrist, A. (2017). *Virtual Hosted PBX.* Recuperado el 4 de mayo de 2017 de https://www.virtualhostedpbx.net/what-is-prtg/

Learn.org. (2017). *Learn.org.* Recuperado el 10 de mayo de 2017 de https://www.google.co.ve/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=0ahUKEwjIgsSltNLTAhXmIJoKHQGJCyQQFghuMAk&url=http%3A%2F%2Flearn.org%2Farticles%2FWhat_is_Design_Methodology.html&usg=AFQjCNGOUolDIA4tv6FOz2yQJyPqs8HEMw&sig2=YYD3SZQGbXLU

Ranjbar, A. (2017). *Cisco Press.* Recuperado el 20 de mayo de 2017 de http://www.ciscopress.com/articles/article.asp?p=102211&seqNum=3

Romero, S. (2012). *Aspectos metodológicos a tener en cuenta para el diseño de una red.* Riochacha: Uniguajira.

Sivasubramanian, B., Frahim, E., & Froom, R. (2017). *CISCO.* Recuperado el 6 de junio de 2017 de

http://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3

Thomas, J. (2017). *OmniSecu.* Recuperado el 24 de junio de 2017 de http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-etherchannel-in-cisco-switches-and-routers.php

Wang, L. (2013). *Design and Implementation of Project Management Information System Based on .Net.* New York: Springer Science+Business Media.

ANEXOS

Anexo 1

Configuración de seguridad en equipos de la red interna del GADMCGP

```
!
service password-encryption
security passwords min-length 10
!
hostname RBORDEGADMCGP
login block-for 300 attempts 5 within 60
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUUl.
username gadmcgp secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUUl.
license udi pid CISCO1941/K9 sn FTX1524TMI9
!
ip ssh version 2
ip domain-name gadmcgp.com
!
banner motd ^CProhibido el ingreso sin autorizacion, si se encuentra manipulando el dispositivo se tomaran las medidas necesarias como lo expone la Subsecretaria de Gobierno Electronico^C
!
line con 0
password 7 0822455D0A165445415F59
login
!
line aux 0
password 7 0822455D0A165445415F59
login
!
line vty 0 4
password 7 0822455D0A165445415F59
login local
transport input ssh
line vty 5 15
password 7 0822455D0A165445415F59
login local
transport input ssh
end
```

Anexo 2

Configuración de equipos del módulo de acceso

```
!
hostname SWACCESO
!
ip dhcp snooping
!
interface FastEthernet0/1
switchport mode trunk
switchport trunk native vlan 5
switchport nonegotiate
channel-group 1 mode active
spanning-tree portfast
!
interface FastEthernet0/2
switchport mode trunk
switchport trunk native vlan 5
switchport nonegotiate
channel-group 1 mode active
spanning-tree portfast
!
interface FastEthernet0/3
switchport mode access
switchport port-security
switchport port-security maximum 5
switchport port-security mac-address sticky
spanning-tree portfast
!
interface FastEthernet0/4
switchport mode access
switchport port-security
switchport port-security maximum 5
switchport port-security mac-address sticky
spanning-tree portfast
!
```

ANEXO 3

Configuración equipos del módulo de distribución.

```
!
hostname DISTRIBUCION
!
ip routing
!
interface Port-channel 1
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 2
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 3
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
!
interface FastEthernet0/2
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
!
interface FastEthernet0/3
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
channel-group 2 mode active
!
interface FastEthernet0/4
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
switchport nonegotiate
channel-group 2 mode active
!
interface FastEthernet0/5
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
channel-group 2 mode active
!
interface FastEthernet0/6
switchport trunk allowed vlan 10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
channel-group 2 mode active
!
interface GigabitEthernet0/1
switchport access vlan 110
switchport mode access
!
interface GigabitEthernet0/2
switchport access vlan 110
switchport mode access
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 0050.0fa3.3b01
ip address 10.10.10.1 255.255.255.192
ip helper-address 192.168.1.1
ip helper-address 192.168.1.2
!
interface Vlan15
mac-address 0050.0fa3.3b02
ip address 10.10.10.65 255.255.255.192
ip helper-address 192.168.1.1
!
interface Vlan20
mac-address 0050.0fa3.3b03
ip address 10.10.10.129 255.255.255.192
ip helper-address 192.168.1.1
!
interface Vlan25
mac-address 0050.0fa3.3b04
```

```
ip address 10.10.10.193 255.255.255.224
ip helper-address 192.168.1.1
ip access-group 110 out
!
interface Vlan30
mac-address 0050.0fa3.3b05
ip address 10.10.10.225 255.255.255.224
ip helper-address 192.168.1.1
!
interface Vlan35
mac-address 0050.0fa3.3b06
ip address 10.10.11.1 255.255.255.224
ip helper-address 192.168.1.1
!
interface Vlan40
mac-address 0050.0fa3.3b07
ip address 10.10.11.33 255.255.255.224
ip helper-address 192.168.1.1
!
interface Vlan45
mac-address 0050.0fa3.3b08
ip address 10.10.11.65 255.255.255.224
ip helper-address 192.168.1.1
!
interface Vlan50
mac-address 0050.0fa3.3b09
ip address 10.10.11.97 255.255.255.240
ip helper-address 192.168.1.1
!
interface Vlan55
mac-address 0050.0fa3.3b0a
ip address 10.10.11.113 255.255.255.240
ip helper-address 192.168.1.1
!
interface Vlan60
mac-address 0050.0fa3.3b0b
ip address 10.10.11.129 255.255.255.240
ip helper-address 192.168.1.1
!
interface Vlan65
mac-address 0050.0fa3.3b0c
ip address 10.10.11.145 255.255.255.240
ip helper-address 192.168.1.1
!
interface Vlan70
mac-address 0050.0fa3.3b0d
ip address 10.10.11.161 255.255.255.240
ip access-group 100 out
```

```
!
interface Vlan75
mac-address 0050.0fa3.3b0e
ip address 10.10.11.177 255.255.255.240
ip helper-address 192.168.1.1
ip helper-address 192.168.1.2
!
interface Vlan80
mac-address 0050.0fa3.3b0f
ip address 10.10.11.193 255.255.255.248
ip helper-address 192.168.1.1
!
interface Vlan85
mac-address 0050.0fa3.3b10
ip address 10.10.11.201 255.255.255.248
ip helper-address 192.168.1.1
!
interface Vlan90
mac-address 0050.0fa3.3b11
ip address 10.10.11.209 255.255.255.248
ip helper-address 192.168.1.1
!
interface Vlan110
mac-address 0050.0fa3.3b12
ip address 192.168.1.3 255.255.255.248
!
router ospf 1
log-adjacency-changes
network 10.10.10.0 0.0.0.63 area 0
network 10.10.10.64 0.0.0.63 area 0
network 10.10.10.224 0.0.0.31 area 0
network 10.10.10.128 0.0.0.63 area 0
network 10.10.10.192 0.0.0.31 area 0
network 10.10.11.0 0.0.0.31 area 0
network 10.10.11.32 0.0.0.31 area 0
network 10.10.11.64 0.0.0.31 area 0
network 10.10.11.96 0.0.0.15 area 0
network 10.10.11.112 0.0.0.15 area 0
network 10.10.11.128 0.0.0.15 area 0
network 10.10.11.144 0.0.0.15 area 0
network 10.10.11.160 0.0.0.15 area 0
network 10.10.11.176 0.0.0.15 area 0
network 10.10.11.192 0.0.0.7 area 0
network 10.10.11.200 0.0.0.7 area 0
network 10.10.11.208 0.0.0.7 area 0
network 192.168.1.0 0.0.0.7 area 0
!
router rip
```

```
!
ip classless
!
ip flow-export version 9
!
!
access-list 100 permit tcp 10.10.10.0 0.0.0.63 10.10.11.160 0.0.0.15 eq www
access-list 100 permit tcp 10.10.10.0 0.0.0.63 10.10.11.160 0.0.0.15 eq ftp
access-list 100 permit tcp 10.10.10.64 0.0.0.63 10.10.11.160 0.0.0.15 eq www
access-list 100 permit tcp 10.10.10.64 0.0.0.63 10.10.11.160 0.0.0.15 eq ftp
access-list 100 permit tcp 10.10.10.128 0.0.0.63 10.10.11.160 0.0.0.15 eq www
access-list 100 permit tcp 10.10.10.128 0.0.0.63 10.10.11.160 0.0.0.15 eq ftp
access-list 100 permit tcp 10.10.11.0 0.0.0.31 10.10.11.160 0.0.0.15 eq www
access-list 100 permit tcp 10.10.11.0 0.0.0.31 10.10.11.160 0.0.0.15 eq ftp
access-list 100 permit tcp 10.10.11.128 0.0.0.15 10.10.11.160 0.0.0.15 eq www
access-list 100 permit tcp 10.10.11.128 0.0.0.15 10.10.11.160 0.0.0.15 eq ftp
access-list 100 permit tcp 10.10.11.64 0.0.0.31 10.10.11.160 0.0.0.15 eq www
access-list 100 permit tcp 10.10.11.64 0.0.0.31 10.10.11.160 0.0.0.15 eq ftp
access-list 100 permit ip 10.10.11.160 0.0.0.31 any
access-list 100 deny ip any any
access-list 110 permit ip 10.10.11.160 0.0.0.31 any
access-list 110 deny ip any any!
```

ANEXO 4

Configuración de equipos del módulo central

```
!
service password-encryption
security passwords min-length 10
!
hostname RBORDEGADMCGP
!
login block-for 300 attempts 5 within 60
!
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUUl.
!
ip dhcp pool ObrasPublicas
network 10.10.10.0 255.255.255.192
default-router 10.10.10.1
dns-server 8.8.8.8
ip dhcp pool Administrativo
network 10.10.10.64 255.255.255.192
default-router 10.10.10.65
ip dhcp pool Planificacion
network 10.10.10.128 255.255.255.192
default-router 10.10.10.129
ip dhcp pool GestionRiesgos
network 10.10.10.224 255.255.255.224
default-router 10.10.10.225
ip dhcp pool Financiero
network 10.10.11.0 255.255.255.224
default-router 10.10.11.1
ip dhcp pool ServiciosBasicos
network 10.10.11.64 255.255.255.224
default-router 10.10.11.65
ip dhcp pool Turismo
network 10.10.11.96 255.255.255.240
default-router 10.10.11.97
ip dhcp pool GIAS
network 10.10.11.112 255.255.255.240
default-router 10.10.11.113
ip dhcp pool Secretaria
network 10.10.11.128 255.255.255.240
default-router 10.10.11.129
ip dhcp pool Concejales
network 10.10.11.144 255.255.255.240
default-router 10.10.11.145
ip dhcp pool Sistemas
network 10.10.11.176 255.255.255.240
default-router 10.10.11.177
```

```
ip dhcp pool Juridico
network 10.10.11.192 255.255.255.248
default-router 10.10.11.193
ip dhcp pool Auditoria
network 10.10.11.200 255.255.255.248
default-router 10.10.11.201
ip dhcp pool Alcaldia
network 10.10.11.208 255.255.255.248
default-router 10.10.11.209
!
username gadmcgp secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUUl.
!
license udi pid CISCO1941/K9 sn FTX1524TMI9
license boot module c1900 technology-package securityk9
!
crypto isakmp policy 102
encr aes
authentication pre-share
group 5
!
crypto isakmp key cisco address 100.101.102.113
!
crypto ipsec transform-set SUCURSAL_GADMCGP esp-aes esp-sha-hmac
!
crypto map SUCURSAL_GADMCGP_map 102 ipsec-isakmp
set peer 100.101.102.113
set transform-set SUCURSAL_GADMCGP
match address 102
!
ip ssh version 2
ip domain-name gadmcgp.com
!
spanning-tree mode pvst
!
class-map match-all SERV-INTERNET
match protocol http url www.gestiondocumental.gob.ec
match protocol http url www.compraspublicas.gob.ec
match protocol http url www.socioempleo.gob.ec
match protocol http url www.webmail.gonzalopizarro.gob.ec
match protocol http url www.gonzalopizarro.gob.ec
class-map match-all REDES-SOCIALES
match access-group 1
match protocol http mime facebook
match protocol http mime youtube
match protocol http mime twitter
match protocol http mime badoo
!
policy-map POLITICAREDES
```

```
class REDES-SOCIALES
priority percent 5
class SERV-INTERNET
bandwidth percent 60
class class-default
fair-queue
!
interface Tunnel0
ip address 192.168.200.1 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/1
tunnel destination 100.101.102.113
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.248
duplex auto
speed auto
standby 1 ip 192.168.1.4
standby 1 priority 150
standby 1 preempt
!
interface GigabitEthernet0/1
ip address 100.101.102.101 255.255.255.252
ip nat outside
service-policy output POLITICAREDES
duplex auto
speed auto
!
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 192.168.1.0 0.0.0.7 area 0
default-information originate
!
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip nat inside source list 2 interface GigabitEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
!
ip flow-export version 9
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 1 permit 10.10.10.0 0.0.0.63
access-list 1 permit 10.10.10.224 0.0.0.31
```

```
access-list 1 permit 10.10.10.128 0.0.0.63
access-list 1 permit 10.10.10.192 0.0.0.31
access-list 1 permit 10.10.11.0 0.0.0.31
access-list 1 permit 10.10.11.32 0.0.0.31
access-list 1 permit 10.10.11.64 0.0.0.31
access-list 1 permit 10.10.11.128 0.0.0.15
access-list 1 permit 10.10.11.144 0.0.0.15
access-list 1 permit 10.10.11.160 0.0.0.15
access-list 1 permit 10.10.11.176 0.0.0.15
access-list 1 permit 10.10.11.192 0.0.0.7
access-list 1 permit 10.10.11.200 0.0.0.7
access-list 2 permit 10.10.10.64 0.0.0.63
access-list 2 permit 10.10.11.96 0.0.0.31
access-list 2 permit 10.10.11.208 0.0.0.7
!
banner motd ^CProhibido el ingreso sin autorizacion, si se encuentra manipulando el
dispositivo se tomaran las medidas necesarias como lo expone la Subsecretaria de
Gobierno Electronico^C
!
line con 0
password 7 0822455D0A165445415F59
login
!
line aux 0
password 7 0822455D0A165445415F59
login
!
line vty 0 4
password 7 0822455D0A165445415F59
login local
transport input ssh
line vty 5 15
password 7 0822455D0A165445415F59
login local
transport input ssh
!
end
```

ANEXO 5

Configuración de equipos de la sucursal

```
!
hostname SUCURSAL
!
login block-for 300 attempts 5 within 60
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp pool SucursalReventador
network 192.168.100.0 255.255.255.0
default-router 192.168.100.1
dns-server 8.8.8.8
!
username gadmcgp secret 5 cisco
!
license udi pid CISCO1941/K9 sn FTX1524I948
license boot module c1900 technology-package securityk9
!
crypto isakmp policy 102
encr aes
authentication pre-share
group 5
!
crypto isakmp key cisco address 100.101.102.101
!
crypto ipsec transform-set SUCURSAL_GADMCGP esp-aes esp-sha-hmac
!
crypto map SUCURSAL_GADMCGP_map 102 ipsec-isakmp
set peer 100.101.102.101
set transform-set SUCURSAL_GADMCGP
match address 102
!
ip ssh version 2
ip domain-name gadmcgp.com
!
spanning-tree mode pvst
!
class-map match-all SUCURSAL_APLICACIONES
match protocol http url www.gestiondocumental.gob.ec
match protocol http url www.compraspublicas.gob.ec
match protocol http url www.socioempleo.gob.ec
match protocol http url www.webmail.gonzalopizarro.gob.ec
match protocol http url www.gonzalopizarro.gob.ec
class-map match-all SUCURSAL_REDESSOCIALES
match protocol http mime facebook
```

```
match protocol http mime youtube
match protocol http mime twitter
match protocol http mime badoo
!
policy-map POLITICA_SUCURSAL
class SUCURSAL_APLICACIONES
bandwidth percent 70
class SUCURSAL_REDESSOCIALES
priority percent 5
class class-default
fair-queue
!
interface Tunnel0
ip address 192.168.200.2 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/1
tunnel destination 100.101.102.101
!
interface GigabitEthernet0/0
ip address 192.168.100.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 100.101.102.109 255.255.255.252
service-policy output POLITICA_SUCURSAL
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.200.0 0.0.0.3 area 0
network 192.168.100.0 0.0.0.255 area 0
!
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
!
ip flow-export version 9
!
access-list 5 permit 192.168.100.0 0.0.0.255
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
```

```
deny tcp any any eq 22
permit tcp any any eq 22
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
password 7 0822455D0A16
login
!
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
!
```