UNIVERSIDAD TÉCNICA DEL NORTE

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

REDISEÑO DE LA RED DE DATOS Y OPTIMIZACIÓN DE LA SEGURIDAD PERIMETRAL PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE URCUQUÍ.

INFORME CIENTÍFICO IEEE

AUTOR: MORÁN VELASCO JONATHAN MARCELO

DIRECTOR: ING. FABIÁN CUZME

IBARRA, 2016

REDISEÑO DE LA RED DE DATOS Y OPTIMIZACIÓN DE LA SEGURIDAD PERIMETRAL PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN MIGUEL DE URCUQUÍ.

J.M. Morán
jonathanmarcelomoran@gmail.com

***Resumen*— El presente trabajo de titulación consiste en el rediseño de la red de datos y optimización de la seguridad perimetral en el "Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí" (GADMU), se comenzó con el levantamiento de información sobre infraestructura del edificio principal (GADMU) sobre el cableado horizontal, cableado vertical, cuarto de telecomunicaciones, áreas de trabajo, puesta a tierra con la finalidad de determinar el estado de la red. Luego se utilizó un modelo jerárquico basado en dos capas: acceso y núcleo colapsado con el cual se estructura la nueva red, cada capa con las configuraciones respectivas para solucionar problemas en aspectos de: dominios de broadcast, fallos de enlace físicos, control de tráfico entre departamentos, en éstas se determinó la utilización de los switches (CISCO WS-C2960-24-TD/ C2960-48-TD) y (WS-C3750X-24-PS). Por otra para se hizo la microsegmentación mediante VLANs y se utilizó VLSM para distribuir las direcciones IP basado en la cantidad de usuarios, con lo cual se pretende mejorar la administración de la red. Para verificar su funcionamiento se realiza las simulaciones respectivas en GNS3 con el cual se pretende validar las configuraciones realizadas demostrando su operatividad. Se realizó un análisis de riesgos y vulnerabilidades mediante la metodología MARGERIT y se determinó el equipo JUNIPER para la seguridad perimetral. Mediante la norma ISO/IEC/IEEE 29148 se determina el sistema operativo para los servidores FTP y PROXY SQUID. En el análisis referencial costo beneficio, se determinó un período de recuperación de 6 meses y 5 días aproximadamente.**

I. ANTECEDENTES

A. Problema

Se han presentado problemas de ciertos funcionarios que acceden a los archivos de departamentos que no les corresponden y revisan la información y manipulan documentos importantes; el departamento financiero es el más comprometido debido a su información la cual debería ser confidencial.

En la red de datos del GADMU, se tiene una demora en la solución de problemas, como por ejemplo en la búsqueda de un punto de red dañando; debido al escaso registro de los mismos, ocurrido por la falta de un mapeo físico; provocando así no solo insatisfacción al personal laboral en el GADMU, sino también a la ciudadanía del cantón SAN MIGUEL DE URCUQUÍ, que visita las instalaciones en busca de algún servicio y no está disponible.

Así mismo la falta de un esquema de direccionamiento IP (Protocolo de internet), ha ocasionado que los servicios y recursos de red se encuentren en un mismo rango y cualquier persona que ingrese al servicio de internet tenga acceso a recursos restringido como la impresora, scanner entre otros.

De igual manera el crecimiento de la red ha ocasionado un bajo rendimiento, debido a la infraestructura de switches en cascada que se han venido colocando para solucionar el problema de escalabilidad, esto ha causado una baja disponibilidad, desperdicio de recurso de ancho de banda, tormentas de broadcast, entre otros.

Otra problemática es la compartición de información; que realiza mediante la red, por lo cual empleados del establecimiento con un conocimiento más amplio en redes, manipulan fácilmente esta información, remplazando la IP de su equipo personal por la IP que deseen hacer daño obtenido un fácil acceso a los recursos, por estos motivos de desorganización de la red es muy fácil que personas tanto internas, como externas realicen manipulaciones indebidas.

Y por último el entretenimiento en redes sociales por parte de los funcionarios públicos en horas laborables provoca un bajo desempeño no adecuado en sus actividades laborables.

B. Justificación

La realización de este proyecto se va a realizar con la finalidad de contribuir al desarrollo social de la empresa del cantón SAN MIGUEL DE URCUQUÍ, logrando que el beneficiario directo sea el ciudadano, al recibir un servicio mejorado y eficiente por parte de las áreas que están ligadas directamente con ellos, cumpliendo así con la misión y visión de la Universidad Técnica del Norte.

El proyecto del rediseño lógico e implementación de servidores basado en software libre, ayudará al GADMU a una disminución de los tiempos en resolver problemas en caso de fallas, con la ayuda del etiquetamiento y mapeo físico; además se corregirá falencias de seguridad sobre datos almacenados, así se disminuirá las posibilidades de que ocurran daños de información, se optimizará la seguridad perimetral según la necesidades de los departamentos, evitando el uso excesivo en páginas no autorizadas por el personal establecimiento; se corregirá problema de inactividad de la red mediante un modelo jerárquico, es decir

que un daño en una parte de la red, no ocasione daño a la red completa. Se mejorará el rendimiento, eliminando los tráficos innecesarios en la red, logrando que los empleados y ciudadanía estén satisfecha por el servicio que se ofrece con la prestación de servicios eficientes.

En el proyecto mediante el uso de un diagrama de la red ayudará a solucionar lo más rápido posible, cuando surja un problema de inactividad de la red, además se realizara VLAN´S para que los datos no se crucen entre departamentos, evitando que eliminen la información importante. Además al separar las redes en 3 niveles, la red será más fácil de diseñar, implementar, mantener y escalar la red, la hace más confiable.

La implementación de un servidor PROXY SQUID ayudará a administran los accesos provenientes de internet hacia la red privada, es decir el bloqueo páginas de internet que distraen a los empleados de la institución, permite al administrador de la red mantener fuera de la red privada a los usuarios no-autorizados. El servidor FTP es un protocolo de transferencia de ficheros entre sistemas conectados a una red TCP (Protocolo de control de Transmisión) basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar ficheros desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo, con el conocimiento adquirido en la carrera se pondrá solución al problema, afrontando los obstáculos y los inconvenientes que este nos presente, además de adquirir nuevas experiencias y conocimientos que fortalecerán mis habilidades y desempeño laboral.

II. FUNDAMENTO TEÓRICO

A. Qué es una red

[1] Afirma que “Una red de telecomunicaciones es un conjunto de medios técnicos instalados, organizados, operados y administrados con la finalidad de brindar servicios de comunicaciones a distancia”.

B. Topología de red

“Una topología se define como el mapa físico o lógico de una red para intercambiar datos” [1]. Las topologías físicas se basa en la forma de cómo los equipos se encuentran conectados, entre algunos tipos se encuentran: topología tipo bus, topología estrella, topología anillo, entre otras. La topología lógica de una red es la forma en que los equipos se comunican a través del medio, los dos tipos de topología más comunes son: topología broadcast, topología por transmisión de tokens.

C. Medios de transmisión

“El medio de transmisión constituye el canal de transmisión de información entre dos o más terminales. La transmisión se la realiza por medio de una señal electromagnética que se propagan a través del canal. Para la transmisión a veces se usa un canal físico o guiado y otras veces no, es decir no guiado.” [2].

D. MODELO DE REFERENCIA OSI

La ISO (International Standards Organization) propuso un modelo de referencia adaptable a todos los sistemas informáticos, los sistemas que acojan esta arquitectura se llamaran “sistemas abiertos”, estos permiten la comunicación con otros sistemas. En la Figura 1 se muestra como los modelos de referencia OSI se divide en siete capas.

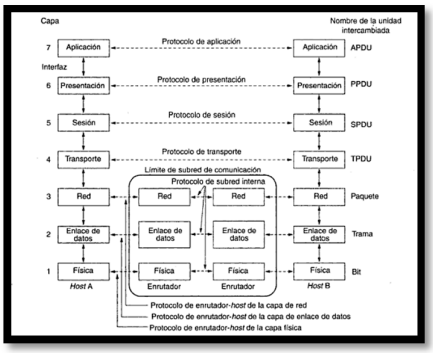

Figura 1.Modelo de Referencia OSI

Referencia: [3]

E. MODELOTCP/IP

Este modelo es el más utilizado en la actualidad, maneja la misma lógica del modelo OSI, en la Figura 2 se visualiza las capas de los dos modelo de red.

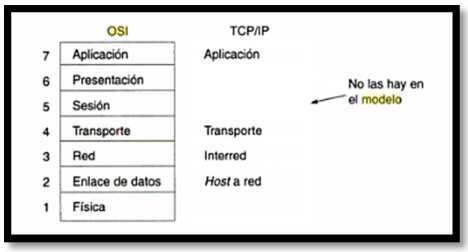

Figura 2. Modelos de referencia

Referencia: [3]

F. Fundamentos de construcción de una red LAN

Un sistema de cableado estructurado es una de las partes fundamentales de cualquier edificación, ya que soporta aplicaciones como voz, video y datos, constituyéndose en la base para la operación de todos los sistemas, al ser una de las partes vitales de la red. Es importante tener en cuenta que los sistemas de cableado estructurado tienen una vigencia aproximada de 10 años por lo que su diseño debe permitir y facilitar futuros cambios o ampliaciones en la red, teniendo en cuenta una debida planificación de crecimiento sobre la red actual.

G. Seguridad perimetral

[4],menciona que la seguridad de los datos que se cursan dentro, desde y hacia una red informática es la principal preocupación de un administrador de red, es por ello que se deben implementar métodos de seguridad para evitar ataques, intrusos e información que puedan alterar el correcto

funcionamiento de la red, para ello está la seguridad perimetral de la red.

H. Definición de la seguridad perimetral

"La seguridad perimetral basa su filosofía en la protección de todo sistema informático de una empresa desde "fuera" es decir componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático. Esto implica que cada paquete de tráfico transmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para nuestra red". [5]

I. Tipos de vulnerabilidades

Las vulnerabilidades, son también denominadas como puntos débiles que pueden afectar u ocasionar riegos en cuanto se refiere a seguridad, entre algunas vulnerabilidades se encuentran: vulnerabilidades físicas, naturales, de hardware y software, medios de almacenamiento, humanas, entre otros.

J. UTM (Unified Threat Management)

[6] Afirman que "UTM o Gestión de Amenazas Unificadas es un conjunto de características diseñadas para proporcionar la inspección de capa de aplicación, del tráfico que atraviesa una red. Al igual que en la detección y prevención de intrusiones (IDP por sus siglas en inglés), los dispositivos de seguridad que admiten características UTM descifran e inspeccionan los protocolos de capa superior para detectar tráfico malicioso o simplemente no reconocido."

III. ANÁLISIS DE LA SITUACIÓN ACTUAL

A. Levantamiento de información del cuarto de telecomunicaciones

En la Figura 3, se visualiza los cables en el suelo sin ninguna protección, junto a estos se encuentran fuentes de energía en funcionamiento, causando una degradación del rendimiento de la red.

Figura 3. Cableado estructurado en el cuarto de telecomunicaciones

Referencia: Fotografía propia

En la Figura 4, se observa dos patch panel de 48 puertos, estos distribuyen el cableado estructurado a los diferentes departamentos del GADMU, esta imagen indica como los cables se encuentran acumulados sin cumplir con la norma ANSI/TIA/EIA-569-A, que indica la forma de estructurar los cables en un cuarto de telecomunicaciones.

Figura 4. Patch panel 48 puertos ubicado en el cuarto de telecomunicaciones

Referencia: Fotografía propia

En la Figura 5, se indica el estado del rack, el cual está ubicado en el cuarto de telecomunicaciones y contiene dos patch paneles, un router cisco 881 y cables de red (Categoría 5e) acumulados en el piso, sin ninguna protección afectando la disponibilidad de la red.

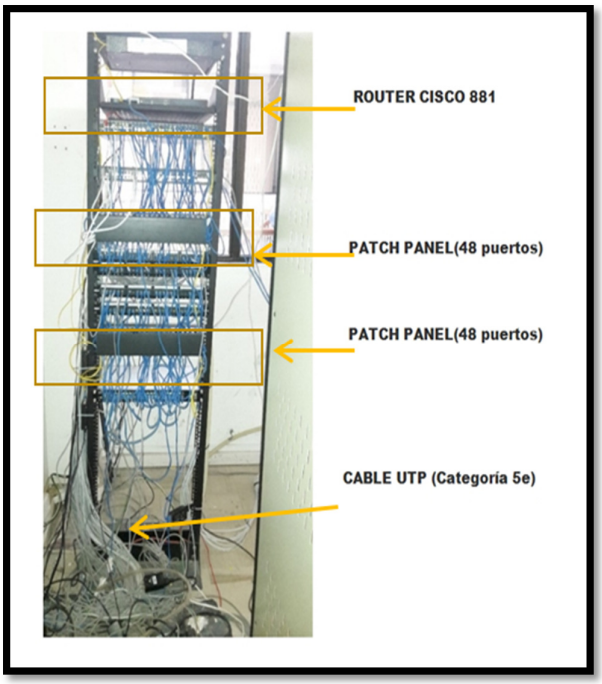

Figura 5. Rack ubicado en el cuarto de equipos vista frontal

Referencia**:** Fotografía propia

En la Figura 6, se observa los cables de red sin cubierta plástica y enredada con los cables de energía, ocasionando la inestabilidad del servicio de red en el departamento de agua potable.

Figura 6. Cableado estructurado en el departamento de agua potable

Referencia: Fotografía propia

B. Levantamiento de información para el cableado estructurado

Dentro del levantamiento de información para el cableado estructurado se consideró los siguientes elementos: subsistema horizontal, subsistema vertical, cuarto de equipos, áreas de trabajo, sistema de puesta a tierra.

1. Levantamiento de información del subsistema horizontal

El subsistema horizontal va desde el área de trabajo hasta el armario de telecomunicaciones. En el GADMU se obtuvo la siguiente información:

- La edificación no cuenta con un subsistema horizontal.
- La instalación se realizó mediante la perforación de los pisos para dar el servicio de internet a cada área de trabajo.
- El cableado estructurado en su gran mayoría se encuentra con cable UTP categoría 5e. En los departamentos recaudación, rentas y sistemas informáticos, se encuentra instalado categoría 6.
- No utiliza ductos para guiar el cable de red hacia las respectivas áreas de trabajo.
- No tiene bandejas metálicas para evitar daños en los cables de red.

2. Levantamiento de información del subsistema vertical

La función principal del armario de telecomunicaciones es concentrar las terminaciones de todo tipo de cable horizontal reconocido por el estándar. En el GADMU se obtuvo la siguiente información:

- En la edificación no cuenta con un subsistema vertical.
- El cable es atravesado hacia otros departamentos mediante hoyos taladrados en la pared.
- El subsistema vertical se instaló con cable categoría 5e.
- Los enlaces de backbone no cuentan con ningún tipo de protección a lo largo de su recorrido.
- No se utiliza escalerillas verticales para guiar el cable de red hacia el cuarto de telecomunicaciones.

3. Levantamiento de información del cuarto de telecomunicaciones

El cuarto de telecomunicaciones debe ser capaz de albergar equipos de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado, en el GADMU se obtuvo la siguiente información:

- Corporación Nacional de Telecomunicaciones provee el servicio de internet, el cual llega mediante fibra óptica al cuarto de telecomunicaciones.
- Cuenta con un rack principal que contiene dos patch panel para albergar los cables de datos, además contiene un ODF (Organizador de fibra óptica) el cual suministra el servicio de internet al router CISCO 881 y router Mikrotik routerboard 750, los cuales está conectado a dos switch cisco SG 200-50.
- Contiene un gabinete donde se alojan dos servidores HP PROLIANT E5649 no operativos, cada equipo con sus respectivos UPS (Uninterruptible power supply), estos se encuentran bajo llave y es administrado solo por el jefe de área sistemas.
- No posee seguridad para acceso al cuarto de telecomunicaciones, solo es manejado mediante una simple cerradura.
- Posee un equipo de ventilación que se encuentra dañado.
- Cuenta con dos lámparas fluorescentes, no muy adecuadas para el trabajar.
- Contiene una caja para alojar cables electricidad y se encuentra en mal estado.

4. Levantamiento de información de las áreas de trabajo

Son los espacios dónde se ubican los escritorios de los usuarios y son lugares habituales para los empleados. En el GADMU se obtuvo la siguiente información:

- En el 40% de las áreas de trabajo, los puntos de red se encuentran en mal estado. Para la instalación de puntos de red en las áreas de trabajo se ocupó la norma ANSI/EIA/TIA 568B y la etiquetación de los mismos se encuentra en la mayoría de las áreas de trabajo, excepto en los nuevos puntos de red que se instalaron recientemente.
- En los departamentos de fiscalización, financiero, obras públicas los puntos de red se encuentran sin flaceplate.

5. Levantamiento de información de la red de internet

La velocidad de transmisión es 12 [Mbps] de subida y 16 [Mbps] de bajada. CNT presta los equipos activos de red como: router cisco 881 y el routerboard 750 que enrutan datos hacia los respectivos departamentos los cuales se conectan a los switch SG 200-50 y estos distribuyen el servicio de internet a los departamentos en funcionamiento en el GADMU.

.

6. Levantamiento de información del subsistema de puesta a tierra

Cuenta con un sistema puesta a tierra centralizado por una varilla de cobre, que se encuentra ubicada enterrada en los exteriores del edificio del GADMU.

C. Equipos activos

A continuación se presentan los equipos activos que se encuentran en cada piso de las instalaciones, de los cuales algunos se encuentran en uso y otros no.

1. Primer piso

En la figura 7, se especifican los equipos existentes en el primer piso detallando: su marca, descripción y su estado.

CANTIDAD	EQUIPO ACTIVO	MARCA	DESCRIPCION	ESTADO
2	SWITCH	D-LINK DES-1024D	24 puertos 10/100 Mbps	OPERATIVO
1	ROUTER INALAMBRICO	TP-LINK	2,4 Ghz - 802.11 a/g	OPERATIVO
1	BIOMETRICO	WALDSO		OPERATIVO

Figura 7. Equipos activos en primer piso

Referencia: Elaboración propia

2. Segundo piso

En la figura 8, se especifican los equipos utilizados en el segundo piso detallando: su marca, descripción y el estado de equipo.

CANTIDAD	EQUIPO ACTIVO	MARCA	DESCRIPCION	ESTADO
1	SWITCH	D-LINK DES-1024D	24 puertos 10/100 Mbps	OPERATIVO
1	SWITCH	CISCO	SG 200-50	OPERATIVO
1	ROUTER	CISCO	CISCO 881	OPERATIVO
1	TRANCEIVER	HUMANITY	10/100 BASE –TX & 100 BASE FX CONVERTER	OPERATIVO
1	ROUTER	TRENDNET	TK-409	OPERATIVO
1	ROUTER	MIKROTIK	ROUTERBOARD 750	OPERATIVO
1	SWITCH	HP 5130	SERIES SWITCH JG934	NO OPERATIVO
3	UPS	TRIPP-LITE	APC 1500VA 120 W	NO OPERATIVO
1	UPS	SMART UPS	APC 1500VA 120 W	OPERATIVO
1	ROUTER	D-LINK	2,4 Ghz - 802.11 a/g	OPERATIVO
1	UPS	APC	BACK UPS PRO 1500	OPERATIVO

Figura 8. Equipos activos en segundo piso

Referencia: Elaboración propia

Con el levantamiento de información del segundo piso se obtuvo información sobre los servidores, en la figura 9 se explica cada equipo con su respectiva marca y su función cumple en el GAD Municipal de San Miguel de Urcuquí.

CANTIDAD	EQUIPO	SISTEMA OPERATIVO	DESCRIPCIÓN	ESTADO	FUNCIÓN
1	HP	CENTOS 5.5	PROLIANT E5649	NO OPERATIVO	PROXY
1	HP	CENTOS 6.5	PROLIANT ML170	OPERATIVO	CORREO
1	HP	CENTOS 6.5	PROLIANT ML170	OPERATIVO	WEB

Figura 9. Servidores en el cuarto de equipos

Referencia: Elaboración propia

3. Tercer piso

En la figura 10, se especifican los equipos utilizados en el tercer piso detallando: su marca, descripción y el estado de equipo.

CANTIDAD	EQUIPO ACTIVO	MARCA	DESCRIPCION	ESTADO
1	SWITCH	D-LINK DES-1024D	24 puertos 10/100 Mbps	OPERATIVO

Figura 10. Equipos activos en tercer piso

Referencia: Elaboración propia

D. Esquema de topología de red

El esquema de topología de red, se encuentra dividida en dos partes: física y lógica.

1. Topología lógica

La topología lógica del GADMU es de tipo bus Ethernet, ya que todos los dispositivos se encuentran conectados por un mismo medio.

En la figura 11, se explica características lógicas que se obtuvo de la recopilación de información.

TECNOLOGIA	VELOCIDAD DE TRANSMISION	TIPO DE CABLE	DISTANCIA MAXIMA	TOPOLOGIA
100BaseTX	100 Mbps	Par trenzado(Cat. 5e UTP)	100 M	Estrella-Full Dúplex(Switch)

Figura 11. Características lógicas

Referencia: Elaboración propia

2. Topología física

Se basa en una topología de estrella extendida, ya que todos los switch se encuentran conectados a un nodo central, en la figura 12 se visualiza la topología física del GADMU.

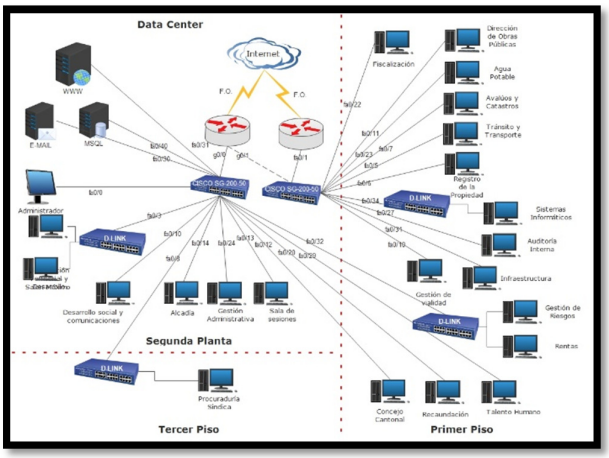

Figura 12. Topología física

Referencia: Elaboración propia

E. Planos del edificio

Dentro del levantamiento de los puntos de red existentes, se elaboró los planos arquitectónicos utilizando la herramienta AUTOCAD. Para lo cual los símbolos a utilizarse que identifican a puntos de red y cableado estructurado. Se detallan en la tabla 1.

Tabla 1. Símbolos utilizados en el cableado estructurado

SIMBOLO	SIGNIFICADO	# DE PUNTOS DE RED
△	PUNTOS DE RED	100
|	CABLEADO ESTRUCTURADO (Cat. 5e)	

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

En la figura 13, se muestra el plano del primer piso con su respectiva ubicación de los puntos de red.

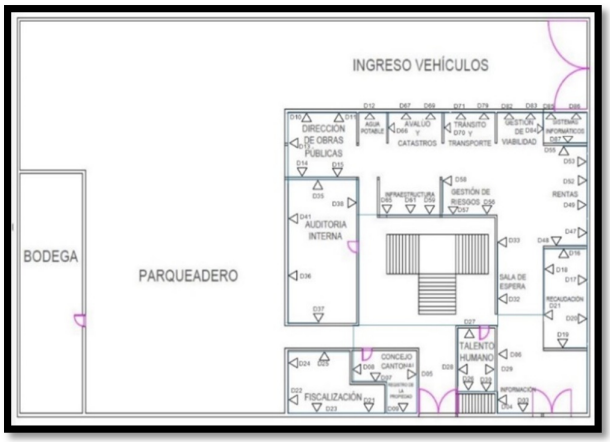

Figura 13. Planos del primer piso del edificio Principal

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

En la figura 14, se muestra el plano del segundo piso con su respectiva ubicación de los puntos de red.

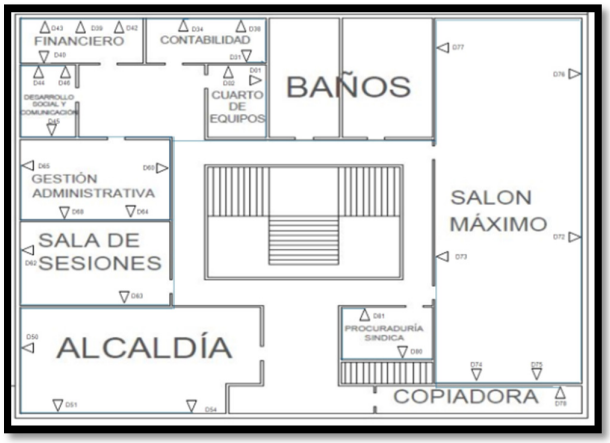

Figura 14. Planos del segundo piso edificio Principal

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

En la figura 15, se muestra el plano del tercer piso con su respectiva ubicación de los puntos de red.

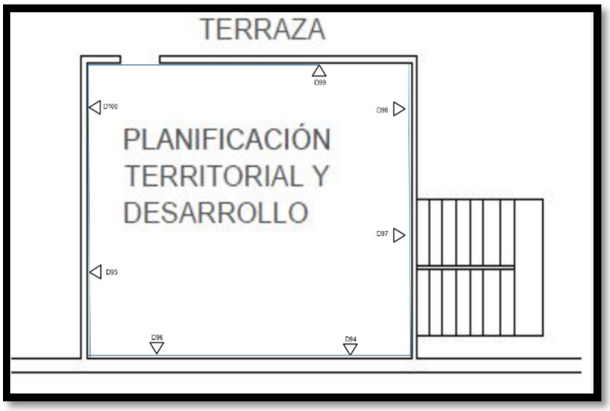

Figura 15. Planos del tercer piso del edificio Principal

Referencia: Elaboración propia con información obtenida del edificio principal del GADMU

IV. REDISEÑO LÓGICO DE LA RED DE DATOS

En este capítulo se elabora el rediseño lógico de la red de datos del GADMU, mediante aspectos importantes como: la proyección del crecimiento de la red, acceso a aplicaciones para cada punto de red, dimensionamiento de equipos de red y la nueva propuesta para las topologías lógicas y física.

Luego se realiza sus configuraciones respectivas basado en el modelo jerárquico y conjuntamente para su comprobación se utiliza la herramienta simuladora de redes GNS3 ya que cumple con funcionalidades similares a switches a elegir.

1. Diagrama de bloques

En la figura 16, se indica el proceso para realizar el rediseño de la red de datos, en el cual se indica los pasos a seguir para la elaboración del proyecto.

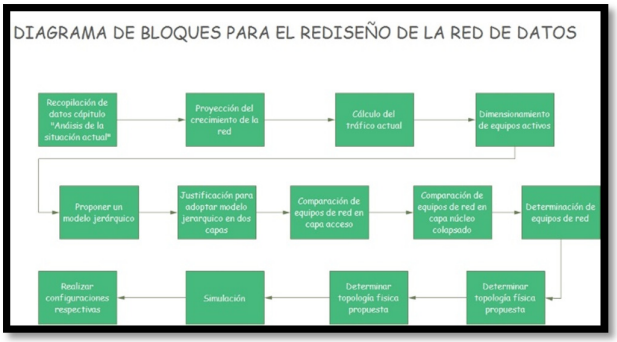

Figura 16. Diagrama de bloques a seguir

Referencia: Elaboración propia

2. Estudio de la proyección de crecimiento

Según la información brindada por el departamento de Sistemas, a través del administrador de la red el ingeniero

encargado de sistemas, en el GADMU no existe un crecimiento de personal, ya que el número de plazas de trabajo es fijo y la mayoría de trabajadores han permanecido fijos al pasar de los años.

Pero el uso de las TIC`S ha demando la instalación de puntos de red sin ninguna planificación, afectado la infraestructura del GADMU. Se estima que para el próximo año un incremento aproximado de 148 puntos de red, este crecimiento es para los equipos de red (servidores, computadoras, impresoras, scanner, entre otros).

3. Acceso de aplicaciones

En la figura 17, se visualiza las aplicaciones que se encuentran operativas en el GADMU, entre las que; la aplicación de base de datos (SQL Sever) es la más crítica de acuerdo al administrador de red.

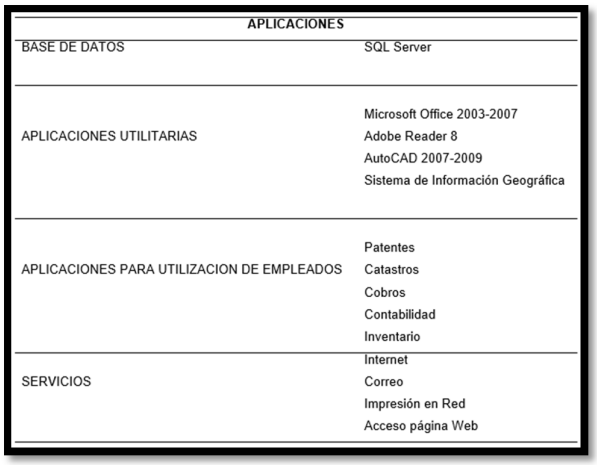

Figura 17. Aplicaciones para cada empleado

Referencia: Elaboración propia

A. Cálculo de tráfico de servicios externos e internos brindado por GAD Municipal de Urcuquí

Para el cálculo de tráfico se considera los siguientes servicios que brinda el GADMU: correo electrónico, base de datos, descarga de archivos, páginas web. En la tabla 2, se explica todos los datos obtenidos de los cálculos realizados anteriormente, para el tráfico (interno) por cada usuario.

Tabla 2. Demanda del tráfico actual

SERVICIOS INTERNOS	CAPACIDAD INDIVIDUAL (KBPS)	CAPACIDAD 125 USUARIOS (KBPS)
Correo Electrónico	0,22	22,20
Base de Datos	0,11	11,11
Descargas de información de internet	62,27	6.226,60
Acceso a páginas web	45,55	4.555,10
Total	108,15	10.815,01
Total en Mbps	0,11	10,56

Referencia: Elaboración propia

En la tabla 3, se explica todos los cálculos para realizados anteriormente, el cual indica un tráfico (externo) por cada usuario.

Tabla 3. Cálculo total de servicios internos

SERVICIOS EXTERNOS	CAPACIDAD INDIVIDUAL (KBPS)	CAPACIDAD 125 USUARIOS (KBPS)
Correo Electrónico	0,89	111,00
Acceso a páginas WEB	68,27	8.533,25
Total externo	69,15	8.644,25
Total interno	108,15	10.815,01
Total	177,30	19.459,26
Total en Mbps para cada empleado	0,17	19,00

Referencia: Elaboración propia

B. Dimensionamiento de equipos activos

El dimensionamiento de equipos activos nos determina la cantidad de equipos de red que se debe utilizar en la capa acceso, a continuación se encuentra un resumen:

Tabla 4. Requerimientos para capa acceso

REQUERIMIENTOS	VALORES
Switches de 48 puertos	4
Switches de 24 puertos	1
Switches por motivos de contingencia	1
Velocidad hacia las estaciones de trabajo	100 Mbps
Velocidad de puertos up-link hacia las capa núcleo	1 Gbps
Capacidad de conmutación	13,6 Gbps

Referencia: Elaboración propia

C. Rediseño de la red

En este ítem se explica el rediseño de la red de datos para el GAD Municipal de San Miguel de Urcuquí, el cual se divide en dos partes: física y lógica; para la parte física se plantea un modelo en dos capas (núcleo colapsado y acceso), los cuales serán esquematizados indicando la función que realiza cada capa; y para la parte lógica se plantea un esquema de creación de vlans con sus direccionamientos respectivos para cada una de ellas.

Para determinar el tipo equipo de red a utilizarse, se realiza un análisis de cálculo del tráfico actual con el cual se determina el ancho de banda que necesita cada empleado de la institución el cual es [0,17 Mbps]. Con estos cálculos se realiza un dimensionamiento para la capa acceso, con ello se determina el número de switches que se necesita cada capa acceso, en la tabla 22 requerimientos mínimos (se detalla un resumen que debe cumplir cada switch de acceso para ser utilizado). Una vez analizado todos estos parámetros se procede a elegir los equipos de red a utilizarse, realizando un cuadro en donde se comparan marcas que ofrecen los equipamientos de red.

Finalmente, se simula el diseño en el programa GNS3 con la finalidad de verificar el funcionamiento.

D. Justificación del modelo en dos capas

(Domíguez Limaico & Gordillo Pasquel, 2006) ha mención: "La estructura de interconexión de la red a diseñarse, se basa en el modelo jerárquico propuesto por CISCO Systems, por lo que los equipos que conforman la sección de "backbone" o "Core", deben tener la capacidad de conmutación (backplane) suficiente capaz de soportar los requerimientos de la red a diseñarse, además proporcionar opciones de redundancia.

En la sección de distribución, se controla y monitorea el tráfico de la red, además se implementa seguridad y autenticación de usuarios registrados; que dependiendo del tamaño de la red, se la puede integrar junto con la sección de backbone en un solo equipo".

Se acogerá el modelo en dos capas (acceso y núcleo colapsado) ya que el número de empleado que tiene el GAD Municipal de San Miguel de Urcuquí es pequeño.

Al mezclar las dos capas se elimina una capa en el modelo jerárquico, esta capa llamada núcleo colapsado se compacta en un solo equipo robusto, el cual solucionarán todos los problemas del bajo desempeño de la red mencionados en el capítulo 3; se considera que en la institución la principal desventaja es el déficit económico, por lo este modelo se adapta perfectamente a las necesidades del GADMU.

"Actualmente existen switches de gran capacidad los cuales integran interfaces Ethernet, FastEthernet, 1 Gigabit Ethernet para UTP y fibra óptica, y 10 Gigabit Ethernet para fibra óptica, los mismos que logran conmutación a gran velocidad." (Domíguez Limaico & Gordillo Pasquel, 2006).

Para el proyecto se necesitará switches Fastethernet (100 Mbps), este análisis se encuentra en este mismo capítulo en el ítem (4.3) dimensionamiento para switches de capa acceso. Y un resumen de los parámetros que se necesitan la capa acceso se indica en la tabla 22.

(Domíguez Limaico & Gordillo Pasquel, 2006), hace mención: "En la actualidad existen switches que manejan capa 2, capa 3 y hasta capa 4 (capa transporte) denominados switches multicapa. Con este tipo de equipos se puede implementar seguridades tales como restricción de direcciones MAC, direcciones IP's y puertos lógicos de capa transporte, a manera de un cortafuegos14 (firewall).

Por lo tanto en el presente diseño se utilizará en cada nodo este tipo de dispositivos."

Para el rediseño se utilizarán switches de capa 2 y capa 3.

En la figura 18, se indica una topología física propuesta en la cual se divide en dos capas (acceso y núcleo colapsado), se puede apreciar que en la capa de núcleo colapsado se encuentran dos equipos de red, un equipo principal y un secundario (redundancia), se recomienda utilizar en la institución un equipo redundante en caso de que el equipo principal falle, el otro equipo entra en funcionamiento y la red se mantenga operativa.

Además se observa que los switches de acceso se conectan hacia los switches de núcleo colapsado, mediante interfaces de uplink a 1 Gigabit por lo cual estos equipos necesitarán: 2 puertos uplink a 1 Gigabit para cada uno de estos para aplicaciones futuras.

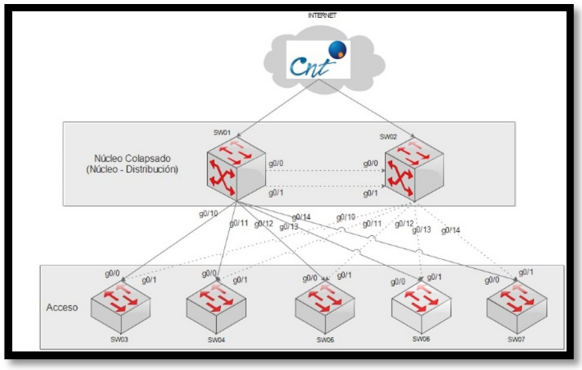

Figura 18. Propuesto para la parte física de red

Referencia: Elaboración propia

1. Configuración en capa núcleo colapsado

Para la capa núcleo colapsado se realiza la configuración para crear la VLANs, estas se agruparon según la funciones de los departamentos en el GAD Municipal de Urcuquí, conjuntamente a estas se configuró el enrutamiento entre VLANs que se utiliza para la transportación de información de dichas Vlans.

Se configura el protocolo VTP (VLAN Trunking Protocol) en modo servidor con lo cual se evitará la creación de VLAN en los switches de acceso en modo manual, evitando problemas con fallos de escritura al momento de crear una Vlans.

Es muy importante tener en cuenta aspectos de fallos (equipos), por lo cual se habilitará HSRP, su funcionamiento básico es: cuando un switch se pone en modo activo y otro en espera, si el switch activo falla el que se encuentra en espera desempeña las funciones de éste.

Se configura listas de acceso con las cuales se impedirá y aceptará principalmente la comunicación entre departamentos agrupado por Vlans mediante reglas, por ejemplo se permitirá la comunicación entre departamento financiero y departamento administrativo, estas reglas fueron escogidas por el departamento de sistemas.

Los puertos conectado hacia los switches de capa acceso, se configura en modo troncal para el transporte de muchas Vlans por un solo enlace. En la figura 19, se observa como deberá ir conectados los switches en la capa núcleo colapsado.

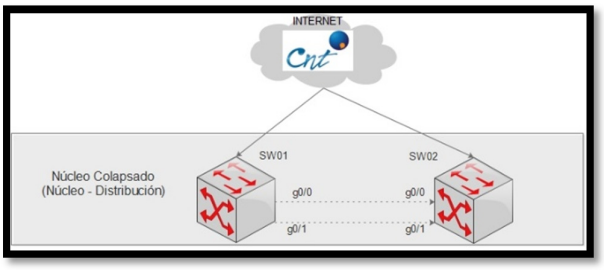

Figura 19. Modelo jerárquico - Núcleo colapsado

Referencia: Elaboración propia

2. Configuraciones de capa acceso

En la capa acceso es indispensable configurar la autenticación mediante MAC para cada computadora que existentes en el edificio principal del GAD Municipal de Urcuquí, esto evitará el acceso a los recursos (impresora, internet, base de datos, correo institucional). Se realiza la configuración de VTP (VLAN Trunking Protocol) en modo cliente para evitar configurar las Vlans en forma manual.

Los puertos conectado hacia los usuarios finales, se configurará en modo acceso para el transporte tráfico de cada usuario conectado a esa VLAN.

Se configura el protocolo rapid-spanning tree esto permite recuperar la conectividad después de una interrupción, esto proporciona una rápida convergencia si el enlace falla. En la figura 20, se observa cómo deben estructurarse los switches en capa acceso brindando conexión a todos los departamentos existentes.

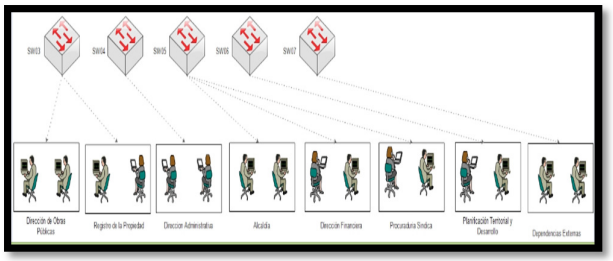

Figura 20. Modelo jerárquico - acceso

Referencia: Elaboración propia

E. Propuesta para modelo de red lógico

Para la parte lógica se realiza la microsegmentación basado en VLANs, conjuntamente se realiza el cálculo de direccionamiento IP mediante VLSM, su cálculo se basa en número de usuarios que tiene cada VLANs. A continuación se explica el procedimiento para la parte lógica.

1. Segmentación de la red

En la figura 21, se observa las VLANs con diferentes imágenes los cuales se encuentran situados en diferentes pisos; se propone la creación un total de 14 Vlans.

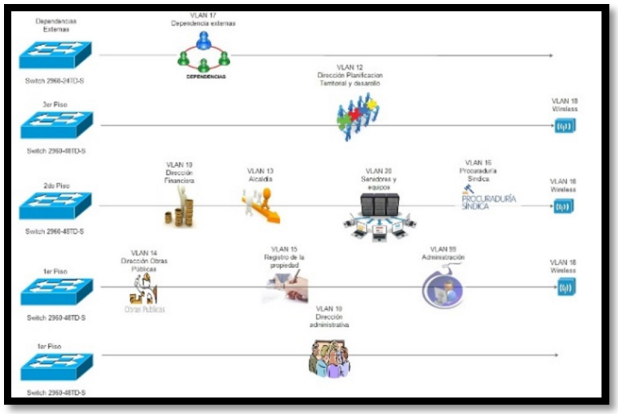

Figura 21. Distribución de VLANs

Referencia: Elaboración propia

Mediante la creación de VLANs se tiene un esquema lógico en forma ordenada, con una gran ventaja de brindar mayor control al administrador ya que se encuentran asignadas localmente, la agrupación de departamentos se basa en la tabla 5.

Tabla 5. Agrupación de los departamentos

VLAN	AGRUPACIÓN DE DEPARTAMENTOS	DEPARTAMENTOS
10	Dirección Administrativa	Talento Humano Sistemas Informáticos Bodega Contratación Pública Mantenimiento
11	Dirección Financiera	Presupuesto Contabilidad Tesorería Rentas
12	Planificación territorial y desarrollo	Regulación Urbana Avalúos y Catastros Gestión y proyectos Tránsito y Transporte
13	Alcaldía	Comunicación Secretaria General Asesoría Fiscalización Auditoria Interna Alcaldía Consejo Municipal
14	Dirección de Obras publicas	Agua Potable Infraestructura Gestión de Riesgos Gestión Ambiental
15	Registro de la Propiedad	
16	Procuraduría Sindica	Comisaria Municipal
17	Dependencias externas	Plaza del Buen Vivir Unidad de Desarrollo Social Biblioteca Mantenimiento

Referencia: Elaboración propia

En la tabla 5, se indican la VLANs complementarias que se propone crear en el GADMU para administración y monitoreo.

Tabla 6. Vlans complementarias en GADMU

VLAN	USO
18	Wireless
19	Servidores y Equipos
20	Área de sistemas
99	Administración
22	Voz
23	Video Vigilancia

Referencia: Elaboración propia

2. Direccionamiento IP

Para la asignación de direcciones IP se consideró los grupos de VLANs con mayor cantidad de usuarios y también el de menores usuarios, en nuestro caso el grupo (Dependencias externas) tiene mayor afluencia de usuarios y grupo de Procuraduría Sindica con menor afluencia de usuarios. Con los siguientes datos recolectados se describe en las siguientes subredes:

- Una subred de 24 host para ser asignado a la VLAN de dirección administrativa.
- Una subred 24 host para ser asignados a la VLAN dirección financiera.
- Una subred 24 host para ser asignados a la VLAN planificación territorial y desarrollo.
- Una subred 18 host para ser asignados a la VLAN Alcaldía.
- Una subred 18 host para ser asignados a la VLAN dirección de obras públicas.
- Una subred 11 host para ser asignados a la VLAN registro de la propiedad.
- Una subred 7 host para ser asignados a la VLAN Procuraduría Síndica.
- Una subred de 29 host para ser asignado a la VLAN de dirección Dependencias externas.
- Una subred 240 host para ser asignados a la VLAN Wireless.
- Una subred 40 host para ser asignados a la VLAN Servidores.
- Una subred 20 host para ser asignados a la VLAN Área de sistemas.
- Una subred 10 host para ser asignados a la VLAN Administración.

En la tabla 7, se especifica el direccionamiento basado en VLANs, junto con su respectiva mascara de red, puerta de enlace y ubicación, con la IP 172.16.0.0/24 se propone las siguientes redes:

Tabla 7. Direccionamiento basado en VLANs

VLAN	DEPARTAMENTO	ACRÓNIMO	# PUNTOS DE RED	MÁSCARA RED	DIRECCIÓN DE RED	1ERA IP UTILIZABLE	ÚLTIMA IP UTILIZABLE	BROADCAST	LOCALIZACIÓN
18	Wireless	WIRELESS	240	/24	172.16.0.0	172.16.0.1	172.16.0.254	172.16.0.255	P1,P2,P3
23	Voz	VOZ	150	/24	172.16.1.0	172.16.1.1	172.16.1.254	172.16.1.255	P1,P2,P3
24	Video vigilancia	VIDEOVIG	50	/26	172.16.2.0	172.16.2.1	172.16.2.62	172.16.1.63	P1,P2,P3
19	Servidores y Equipos	SRVEQU	40	/26	172.16.2.64	172.16.2.65	172.16.2.126	172.16.2.127	Cuarto de equipos
17	Dependencia externas	DEPEXT	29	/27	172.16.2.128	172.16.2.129	172.16.2.158	172.16.2.159	EXTERIORES
10	Dirección administrativa	DIRADMIN	24	/27	172.16.2.160	172.16.2.161	172.16.2.190	192.16.2.191	P1
11	Dirección Financiera	DIRFINAN	24	/27	172.16.2.192	172.16.2.193	172.16.2.222	172.16.2.223	P2
12	Planificación Territorial y desarrollo	PLANDES	24	/27	172.16.2.224	172.16.2.225	172.16.2.254	172.16.2.255	P3
20	Área de sistemas	ARSIST	20	/27	172.16.3.0	172.16.3.1	172.16.3.30	172.16.3.31	P1
13	Alcaldía	DEPALCD	18	/27	172.16.3.32	172.16.3.33	172.16.3.62	172.16.3.63	P1,P2,P3
14	Dirección Obras Públicas	DIROBPUB	18	/27	172.16.3.64	172.16.3.65	172.16.3.94	172.16.3.95	P1
15	Registro de la propiedad	REGPRO	11	/28	172.16.3.96	172.16.3.97	172.16.3.110	172.16.3.111	P1
99	Administración	ADMIN	10	/28	172.16.3.112	172.16.3.113	172.16.3.126	172.16.3.127	P1
16	Procuraduría Sindica	PROSIN	7	/28	172.16.3.128	172.16.3.129	172.16.3.142	172.16.3.143	P2

Referencia: Elaboración propia

F. Listas de control de acceso

Estas listas de control se implementan en el switch de núcleo colapsado para limitar el tráfico, estas fueron dadas por el departamento de sistemas para mejorar el tráfico entre las Vlans. Las reglas son las siguientes:

- El usuario con la IP 172.16.3.34 (Alcalde) tendrá acceso a las Vlans de: Dirección administrativa, Dirección Financiera, Planificación territorial y desarrollo, Dirección de Obras públicas, Registro de la Propiedad, Procuraduría Sindica, Dependencias externas.

- Los usuarios con la red 172.16.2.160 (Dirección administrativa) tendrá acceso a los recursos VLAN de dirección Financiera.

- Los usuarios con la red 172.16.2.192 (Dirección financiera) tendrá acceso a los recursos VLAN de Dirección Administrativa.
- El usuario con la IP 172.16.3.2 (Área de Sistemas) tendrá acceso todos los recursos de la red.

G. Elección de equipos de red

En la tabla 4 se presenta los parámetros para capa acceso son: número de puertos (48 – 24 puertos), velocidades hacia las áreas de trabajo (100 Mbps), velocidades de puertos up-link (1Gbps), capacidad de conmutación (13,6 Gbps).

Otro punto importante es la cantidad de puertos y tipos de interfaces que deben tener los equipos de conmutación para capa núcleo colapsado. Hay que considerar una capacidad de crecimiento a futuro y a la vez integrar en un solo equipo (distribución y núcleo), por lo que es recomendable una cantidad de al menos 24 puertos Gigabit Ethernet 1 [Gbps] y 4 interfaces 10 Gigabit Ethernet para fibra óptica, de las cuales 2 son utilizadas para tener conexión redundante entre nodos. Los switches de capa acceso y capa núcleo deben trabajar con los siguientes protocolos.

- IEEE 802.3x para recepción y transmisión simultáneos (full dúplex).

- IEEE 802.3u para conexión de los equipos finales mediante tarjetas 10/100 Mbps a través de cable UTP CAT6.

- IEEE 802.3ab para conexión de los equipos finales mediante tarjetas 10/100/1000 Mbps a través de cable UTP CAT6 y el estándar.

- IEEE 802.3z para la conexión de los enlaces de fibra óptica a 1 Gbps.

- IEEE 802.1q permite tener múltiples redes compartiendo el mismo espacio físico, mediante esta alternativa se generan segmentos de red lógicos en el GADMU este protocolo permite crear Vlans.

- Es necesario garantizar la redundancia de la red, que los enlaces tengan disponibilidad por lo cual se establece utilizar protocolos tales como IEEE 802.1d y 802.1w.

- Para aplicaciones futuras el switch principal debe brindar calidad de servicio y etiquetar el trafico diferenciándolo si son datos o es voz. Para lo cual se necesita tener el protocolo IEEE 802.1p, y diferenciar el tráfico generado por las Vlans.

- Tanto los switches de acceso como los de núcleo deben proveer el servicio dinámico de asignación de hosts.

- A nivel de seguridad se requiere que los puertos de los switches soporten el protocolo IEEE 802.1x para autenticación y que mediante listas de acceso se brinde permisos a los usuarios, las listas de acceso deberán ser estándares y extendidas.

- Inclusive la administración del equipo debe proveer seguridad mediante el protocolo SSH, acceso remoto con el protocolo Telnet, y que soporte el protocolo de administración SNMP en sus versiones actuales. Y los equipos de conmutación deben soportar administración tanto por interfaz gráfica como por línea de comando.

En la figura 22, se muestra la topología a realizarse en la cual cuenta con dos equipos (SWITCH WS-C3750X-24-PS) para la parte núcleo colapsado, estos se encuentran establecidos con dos enlaces redundantes. Para la parte de capa de acceso tenemos 5 switches (SWITCH CISCO CATALYST WS-C2960**)** donde están creadas diferentes VLANs estos también cuentan con enlaces redundantes, con los cual procura tener un red operativa en caso de falló de equipos o enlaces.

H. Resumen general del diseño

Para un funcionamiento del rediseño de la red es importante que el cableado estructurado se encuentre en óptimas condiciones, en el GAD Municipal de San Miguel de Urcuquí no cuenta con ninguna norma, por ende se debe consideraciones solucionar el cableado estructurado del GADMU.

Mediante cálculos realizados en este capítulo se determinó que se necesitan 4 switches de acceso de 48 puertos y un switch 24 puertos, estos deben tener velocidades hacia las áreas de trabajo de 100 Mbps y velocidades de up-link de 1 Gbps, con una capacidad de conmutación de 13,6 Gbps y para la parte de núcleo se necesita dos switches con 24 puertos FastEthernet a 1Gbps con 8 puertos up-link a 1 Gbps para conexión con equipos de capa acceso, con una capacidad de conmutación de 160 Gbps. Los equipos seleccionados para cada capa son switches Cisco Catalyst WS-C2960 y WS-C3750X-24-PS que se adaptan al rediseño propuesto Con la finalidad de verificar el funcionamiento del rediseño se utilizó el programa GNS3, en el cual se configuró todos los protocolos mencionados anteriormente.

I. Simulaciones y configuraciones

Una vez desarrollado el rediseño de la red de datos es necesario validar el modelo propuesto, se utilizará el programa GNS3 es un simulador gráfico de redes que permite diseñar fácilmente topologías de red y luego ejecutar simulaciones en él, además es un emulador de routers Cisco dando soporte a plataformas 1700, 2600, 3600, 3700 y 7200, para probar el funcionamiento del proyecto se utilizaron los routers 2961 y 7200 (como switches de capa 3).

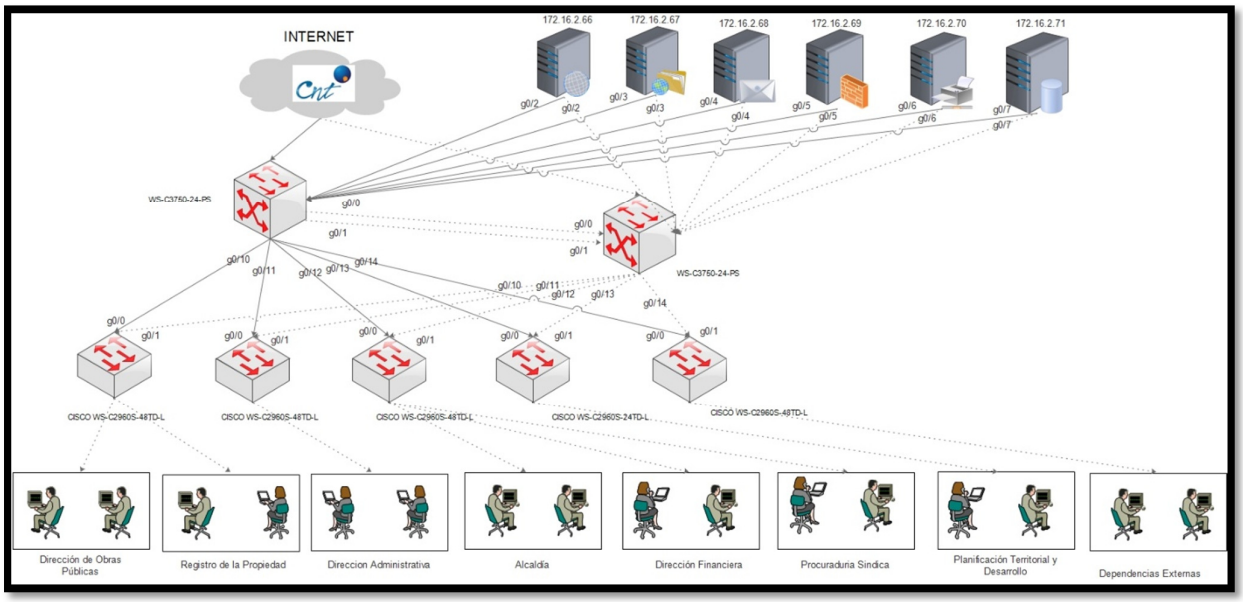

Figura 22. Distribución de VLANs

Referencia: Elaboración propia

En la figura 23, se indica la topología en funcionamiento cuenta con dos switch para núcleo colapsado con sus respectivos enlaces redundantes, además se observa las VLAN cada una estas configurada con su respectiva dirección IP y se en una máquina virtual(Ubuntu).

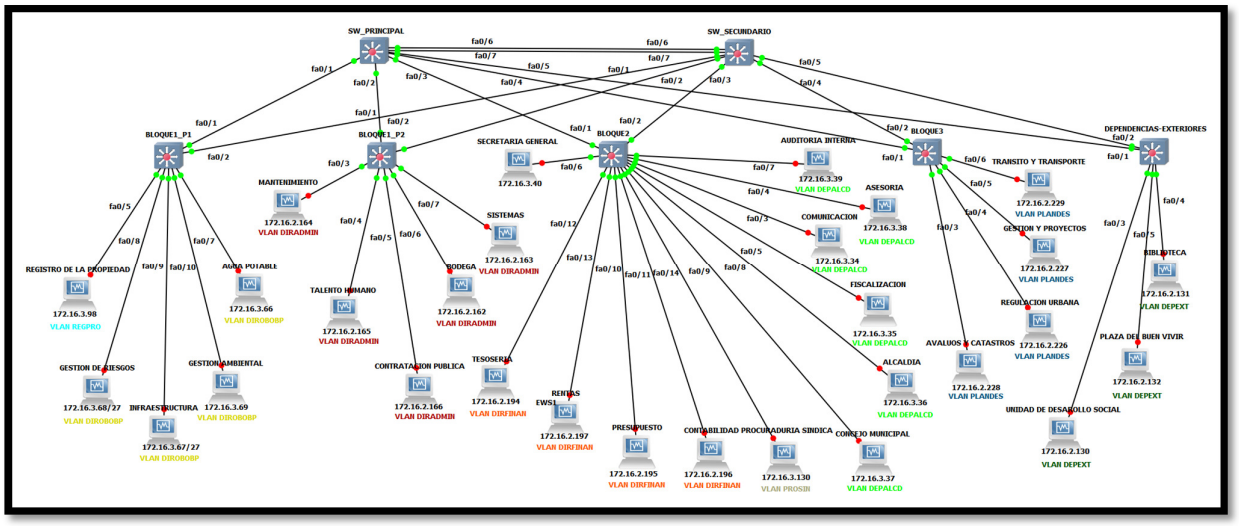

Figura 23. Distribución de VLANs en GNS3

Referencia: Elaboración propia

V. OPTIMIZACIÓN DE LA SEGURIDAD PERIMETRAL

En este capítulo se adoptará la metodología MARGERIT para determinar un análisis de riesgos, con ello se pretende distinguir las vulnerabilidades en el GAD Municipal de Urcuquí; conjuntamente se realizará una comparación entre dos propuestas con las marcas (JUNIPER y CISCO) y se escogerá un equipo para la seguridad perimetral, logrando proteger activos der red e información importante.

Luego para la elección del sistema operativo a utilizarse en los servidores (FTP y PROXY SQUID) se utiliza la norma ISO/IEC/IEEE 29148:2011.

Con la metodología MAGERIT se realizará un análisis de riesgos de la seguridad de la red de la Gobierno Autónomo Descentralizado Municipal de San Miguel de Urcuquí, dicho análisis permitirá identificar amenazas que afecten a la vulnerabilidad de la información y al final poder proponer un equipo para optimizar la seguridad perimetral.

De esta manera los administradores de la red podrán identificar fácilmente las amenazas y poder tomar decisiones más acertadas al momento de que algunas amenazas.

A. Justificación de la metodología MARGERIT

En la figura 24, se observan las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de la información son: MAGERIT, OCTAVE, CRAMM, IRAM, para determinar cuál es la metodología que genere confianza en la mitigación de riesgos se ha realizado la siguiente tabla comparativa.

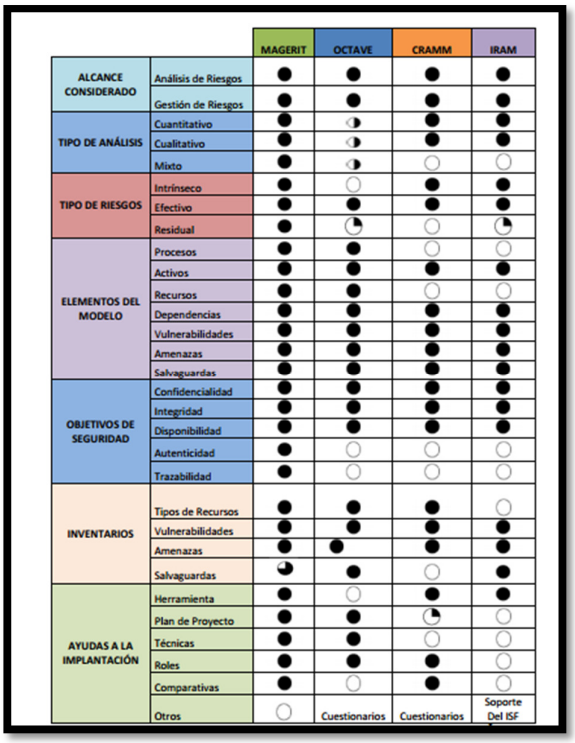

Figura 24. Comparación de metodologías

Referencia: Basado de (Álvarez, 2014)

De la tabla comparativa anteriormente desarrollada se puede concluir que MAGERIT, es una metodología completa porque tiene procesos, actividades.

Una parte fundamental dentro de la gestión de la seguridad de la información, es conocer y controlar los riesgos a los cuales está expuesta la información del GAD Municipal de Urcuquí. Precisamente MAGERIT se basa en analizar el impacto que puede tener para la institución, buscando identificar las amenazas que pueden llegar a afectar la institución y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Esta metodología es muy útil para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocar los esfuerzos en los riesgos que pueden resultar más críticos para una empresa.

B. Elaboración del análisis de riesgo en el GADMU

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento, para el proceso de análisis de riesgos se realizará los siguientes pasos como se indica en la siguiente figura.

TAREAS DELANÁLISIS DE RIESGOS
Paso 1. Caracterización de los activos
1.1 Identificación de los activos
1.2 Dependencias entre activos
1.3 Valoración de los activos
Paso 2. Caracterización de las Amenazas
2.1 Identificación de las amenazas
2.2 Valoración de las amenazas
Paso 3. Caracterización de las salvaguardas
3.1 Identificación de las salvaguardas pertinentes
3.2 Valoración de las salvaguardas.
Paso 4. Estimación del estado de riesgo
4.1 Estimación del impacto
4.2 Estimación del riesgo

Figura 25. Tabla para análisis de riesgos

Referencia: Basado en (Álvarez, 2014)

En la figura 25 se indica los pasos 4 pasos que se va a cumplir para determinar los riesgos y vulnerabilidades.

Identificación y clasificación de activos en la red

La identificación de activos es importante ya que permite plasmar con precisión el alcance del proyecto, permite valorar los activos con exactitud e identificando y valorando las amenazas a las que están expuestos dichos activos. Se realizó la respectiva recolección de información de los activos.

La descripción de toda la información recolectada ya se la ha mencionado anteriormente en el capítulo 3 “Análisis de la situación actual”, a través de las tablas 5, 7, 8.

Como resultado de las anteriores entrevistas realizadas a los administradores de la infraestructura del GAD Municipal de Urcuquí, se ha identificado el siguiente conjunto de activos de red LAN:

- **Datos/ Información**: Los datos son la parte principal que permite a una organización prestar sus servicios. La información es un activo impreciso que será almacenado en equipos. Dentro del GADMU se han identificado que es necesario proteger la información de ciudadanos almacenada en la base de datos

- **Equipos informáticos (hardware):** Son medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la institución, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Dentro de este tipo de activos de red que posee el GADMU, tenemos los siguientes: Servidores de correo, Servidor de base de datos

- **Instalaciones:** Entre los lugares donde se hospedan los sistemas de información y comunicaciones. En el GADMU cuenta con un cuarto de telecomunicaciones.

- **Personal:** En este tipo de activos aparecen las personas relacionadas con los sistemas de comunicaciones. Además este tipo de activos (Personal) no se identifican dependencias. En el área del GADMU se han podido identificar que son los Administradores de Redes.

Valorización de equipos activos

Se puede concluir que los activos con mayor valor muy alto para la organización en la dimensión de seguridad disponibilidad en forma descendente son los siguientes:

- ✓ Cuarto de telecomunicaciones
- ✓ Servidor de Base de datos
- ✓ Servidor de correo

Identificación de amenazas

Luego de la identificación de los activos se deben de identificar las amenazas que pueden afectar a cada activo, por lo que una amenaza puede desencadenar muchas más.

Valorización de amenazas

	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
Instalaciones	Cuarto de telecomunicaciones	Fuego Daños por agua Desastres naturales Desastres industriales Contaminación mecánica Contaminación electromagnética Avería de origen físico y lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Errores del administrador Errores de mantenimiento actualización de programas Perdida de equipos Alteración de secuencia Acceso no autorizado Uso no previsto Manipulación de los equipos Emanaciones electromagnéticas Manipulación de Programas	2	75%
Personal	Administradores de red	Indisponibilidad del personal Deficiencias en la organización Fugas de información Extorsión Ingeniería social	12	75 %

Figura 26. Valorización de amenazas

Referencia: Elaboración propia

	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
Equipamiento	Servidores	Fuego Daños por agua Desastres naturales Desastres industriales Contaminación mecánica Contaminación electromagnética Avería de origen físico y lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Errores del administrador Errores de mantenimiento actualización de programas Perdida de equipos Alteración de secuencia Acceso no autorizado Uso no previsto Manipulación de los equipos Divulgación de información Manipulación de programas	2	25 %
Datos	Información de ciudadanos almacenada en la base de datos	Errores del administrador Alteración accidental de la información Destrucción de información Fuga de información Suplantación de identidad del usuario Abuso de privilegios de acceso Acceso no autorizado Modificación deliberada de la información Destrucción de información Divulgación de información	12	75

Figura 27. Valorización de amenazas

Referencia: Elaboración propia

En la siguientes tablas 26, 27 se indica la frecuencia y degradación de los equipos activos.

Identificación de salvaguardas

Una vez identificado las amenazas, se identificara los mecanismos de salvaguarda implantados en aquellos activos, describiendo las dimensiones de seguridad que estos ofrecen (Disponibilidad, Integridad, Confidencialidad, Autenticidad).

	ACTIVOS	SALVAGUARDAS
Instalaciones	Cuarto de telecomunicaciones	Control de los accesos físicos Aseguramiento de la disponibilidad Alarmas Ventilación Extintores Ups
Personal	Administradores de red	Formación y concienciación. Aseguramiento de la disponibilidad.
Equipamiento	Servidores	Claves. Protección del equipo dentro de la organización. Se aplica perfiles de seguridad. Autenticación del canal. Protección de la integridad de los datos intercambiados.
Datos	Información de ciudadanos almacenada en la base de datos	Protección de la información

Figura 28. Identificación de salvaguardas

Referencia: Elaboración propia

C. Estudio de la tecnología UMT

Hoy en día las amenazas son cada más peligrosas y complejas, por ende para implementar un sistema de seguridad es necesario varios sistemas de control de diferentes servicios que se encuentra en la red, proxy, firewall, antivirus, anti-spam.

La solución es centralizar los servicios y una excelente opción es la gestión de amenazas unificada. Los fabricantes para la seguridad perimetral cada vez sacan características nuevas, los fabricantes más comunes son: Juniper Networks, Astaro, SonicWall, Watchguard, Netgear, Crossbeam entre otras, para este caso se analizará la solución CISCO y JUNIPER ya que se poseen masivas características que se adaptan al proyecto. Para la elección es necesario cumplir con estas características mínimas para la el equipo firewall (cortafuegos), estas se determinaron mediante la relación con las características de los servidores existentes en el GAD Municipal de San Miguel de Urcuquí las cuales son las siguientes:

1. Memoria RAM mínimo de 1024 MB.
2. Interfaces al menos seis con capacidad de 10/100/ 1000 Mbps.
3. Capacidad de manejo de ancho de banda por interfaces.
4. Conexiones simultáneas al menos 400.000 sesiones.
5. Capacidad de servicio para 150 usuarios.
6. Disco duro al menos de 20 GB.

7. Soporte para Vlans (802.1Q) en sus interfaces.
8. Incluya capacitación al menos a dos personas.
9. Garantía del equipo al menos dos años.
10. Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc.)
11. Soporte autenticación mediante certificados 802.1X
12. Interfaz para administración y configuración vía web, telnet y/o CLI.
13. Actualización automática de servicios de seguridad: IDS / IPS, Anti Spam, Antivirus (mínimo cada hora) y Lista de URLs.
14. Costo anual de las subscripciones a los servicios de seguridad.
15. Soporte técnico mensual.

Se elige dos equipos JUNIPER (Network SCG 550 M) y CISCO (ASA 5550), se realiza la comparación entre estos determinando las necesidades mínimas como: características básicas, FIREWALL, VPN, IDS/IPS, antivirus, entre otros. En la tabla 29, se explica las características mínimas que ofrece el equipo Juniper (Network SCG 550 M).

JUNIPER	Juniper Networks SSG 550M
Caracteristicas Requeridas	Caracteristicas Ofrecidas
CARACTERÍSTICAS GENERALES	
Memoria RAM Mínimo 1024 MB	1024 MB
Interfaces al menos 6	Ethernet de 10/100/1000 Mbps 4 puertos 10/100/1000 Mbps
Manejo de ancho de banda por interfaces	Si
Conexiones simultáneas al menos 256.000	256.000 sesiones
Servicio para al menos 200 usuarios	Ilimitado
Disco duro al menos 40 GB	80 GB
Soporte para VLAN´S en sus interfaces	Virtualización, 150 VLAN´S
Autenticación certificados X.509v3 (PKI, IKE)	VeriSing, Entrust, Microsoft, RSA Keon, Baltimore, DoD PKI
Interfaz para administración: web, telnet y/o CLI	Si
Certificación al menos ICSA Labs y/o EAL4	EAL4, EAL4+, ICSA (Firewall y VPN)
Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc)	VPN, SSH, HTTPS
Características y Servicios de Seguridad	
FIREWALL	
Rendimiento Firewall al menos de 1 Gbps	1 Gbps
Capacidad de Stateful Inspection	Si
Capacidad de Arquitectura proxy	Si
Soporte para protocolos RIP v1 y v2	RIP v1 & v2, OSPF, BGP & Multicast
Soporte para NAT transversal H.323	Si
Autenticación a nivel de usuario basada LDAP, RADIUS, Active Directory y Novell Directory	LDAP, RADIUS, RSA SecurID
Capacidad para bloquear tráfico P2P, IM	Si
VPN	
Rendimiento VPN al menos 100 Mbps	500 Mbps
Capacidad para creación de VPN al menos 15 300	300
Soporte encriptacion DES, 3DES, AES-128, AES-256	3DES, AES-256
Soporte VPN para autenticación SHA-1, MD5	SHA-1, MD-5
Soporte para encapsulamiento IPSec, SSL	L2TP, IPSec
Soporte cliente VPN sobre Windows XP, Windows Vista, Linux, Unix.	
IDS / IPS	
Rendimiento IDS / IPS al menos 500 Mbps	No especifica
ANTIVIRUS	
Rendimiento del antivirus al menos 100 Mbps	No especifica
Filtrado web	Si
Anti Spam	Si
Reportes y Logs	Si

Figura 29. Características del equipo Juniper

Referencia: Elaboración propia

En la figura 30, se indica la propuesta de Cisco (ASA 5550)

CISCO	CISCO ASA 5550
Caracteristicas Requeridas	Caracteristicas Ofrecidas
CARACTERÌSTICAS GENERALES	
Memoria RAM Mínimo 1024 MB	4096 MB
Interfaces al menos 6	8 Interfaces Ethernet 10/100/1000 Mbps 4 SPF Fiber 1 10/100 Mbps
Manejo de ancho de banda por interfaces	Si
Conexiones simultáneas al menos 256.000	650.000 sesiones
Servicio para al menos 200 usuarios	Ilimitado
Disco duro al menos 40 GB	No especifica
Soporte para Vlans en sus interfaces	250 Vlans
Autenticación certificados X.509v3 (PKI, IKE)	Certificados X.509, soporte CRL, (Certificate Revocation List)
Interfaz para administracion: web, telnet y/o CLI	Si
Certificación al menos ICSA Labs y/o EAL4	No especifica
Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc)	No especifica
Características y Servicios de Seguridad	
FIREWALL	
Throughput Firewall al menos de 1 Gbps	1,2 Gbps
Capacidad de Stateful Inspection	Si
Capacidad de Arquitectura proxy	Si
Soporte para protocolos RIP v1 y v2	RIP v1 & v2, OSPF, BGP & Multicast
Soporte para NAT transversal H.323	Si
Autenticación a nivel de usuario basada LDAP, RADIUS, Active Directory y Novell Directory	AAA
Capacidad para bloquear tráfico P2P, IM	
VPN	
Throughput VPN al menos 100 Mbps	425 Mbps
Capacidad para creación de VPN al menos 15 300	No especifica
Soporte encriptación DES, 3DES, AES-128, AES-256	3DES, AES
Soporte VPN para autenticación SHA-1, MD5	No especifica
Soporte para encapsulamiento IPSec, SSL	PPTP, IPSec, SSL
Soporte cliente VPN sobre Windows XP, Windows Vista, Linux, Unix	
Dispositivos CISCO Adicionales	CISCO IPS 4255 / CISCO ASA 5520
IDS / IPS	
Rendimiento IDS / IPS al menos 500 Mbps	500 Mbps
ANTIVIRUS	
Rendimiento del antivirus al menos 100 Mbps	450 Mbps
Filtrado web	Si
AntiSpam	Si
Reportes y Logs	Si

Figura 30. Características del equipo Cisco

Referencia: Elaboración propia

D. Propuesta para la seguridad perimetral

Con el análisis de riesgo y con la elección de equipos por la tecnología UTM se determina un equipo como Firewall (cortafuego) para el GAD Municipal de San Miguel de Urcuquí, el cual permitirá solucionar los problemas para las vulnerabilidades mediante la metodología MARGERIT analizada anteriormente.

En la figura 31, se observa un esquema propuesto para la seguridad perimetral, el cual utiliza un equipo Juniper Networks SSG 550M con un equipo firewall (cortafuego) para restringir el tráfico que ingresa y sale.

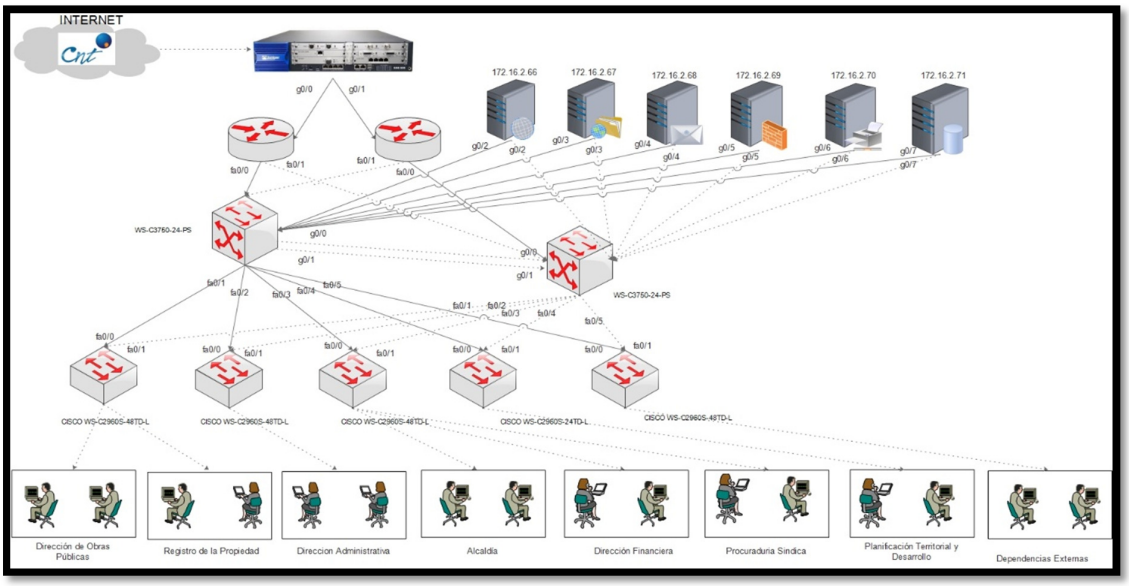

Figura 31. Características del equipo Juniper

Referencia: Elaboración propia

VI. ANÁLISIS COSTO BENEFICIO

En este capítulo se da a conocer todos los costos que se utilizaran para el rediseño de la red de datos y optimización de seguridad perimetral para una futura implementación para la red de datos.

A. Costos de los equipos y materiales necesarios

Los costos referenciales en caso de que se desee implementar, se han tomado de páginas como: mercado libre, empresas proveedoras de equipos de redes, empresas de los mismos fabricantes, entre otros.

1. Costo de equipos para el rediseño de la red interna del GAD Municipal de Urcuquí

En la tabla 8, se muestran los equipos que existen en la Institución y se reusarán para beneficio del rediseño. En la tabla 8, se observan los equipos en reusó para el sistema.

Tabla 8. Equipos de reúso para el Sistema

EQUIPO	CANT.	VALOR UNIT.	VALOR TOTAL
SERVIDOR PROLIANT E5649	1	2.730	2.730
SERVIDOR PROLIANT ML170	1	1.880	1.880
TOTAL			4.610

Fuente: Elaboración propia

En la tabla 9, se detallan los costos de los equipos que deberán ser comprados por la institución, para el rediseño de la red interna.

En la tabla 10, se detallan los costos de equipos para seguridad perimetral que deberán ser comprados por la institución si se desea la implementación.

Tabla 9. Costo de Equipos para el rediseño de la der del GAD

EQUIPO	CANT.	VALOR UNIT.	VALOR TOTAL
Switch (CISCO WS-C2960S-48TD-L)	4	2.278	9.112
Switch (CISCO WS-C2960S-24TD-L)	1	1.629	1.629
Switch (CISCO WS-C3750X-24-PS)	2	3.024	6.048
TOTAL			16.789

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración propia

2. Costo de equipos para seguridad perimetral

Tabla 10. Costo de equipos para los enlaces inalámbricos

EQUIPO	CANT.	VALOR UNIT.	VALOR TOTAL
SSG 550M	1	10.500	10.500
Anti-Virus Juniper-Kaspersky, NS-K-AVS-SSG550	1	3.150	3.150
Anti-Spam, NS-SPAM-ISG1000	1	5.000	5.000
Web Filtering, NS-WF-SSG550	1	2.300	2.300
Deep Inspection, NS-DI-SSG550	1	1.000	1.000
J-Care Support Services, SVC-COR-SSG550M	1	750	750
TOTAL			22.700

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración propia

3. Costo de material de red

En la tabla 11, se detallan los costos de materiales de red que deberán ser comprados por la institución, para la red inalámbrica interna.

Tabla 11.Costo de materiales de red

DESCRIPCIÓN	CANT.	VALOR UNIT.	VALOR TOTAL
Cable UTP Cat 6A(305m)	2 rollo	350,00	700,00
Conector RJ-45	1 caja	8,50	8,50
Canaletas plásticas 32x12	10	2,10	21,60
TOTAL			730,1

Referencia: Elaboración propia

4. Costo de material eléctrico

En la tabla 12, se detallan los costos de materiales eléctricos que deberán ser comprados por la institución.

Tabla 12.Costo de material eléctrico

DESCRIPCIÓN	CANT.	VALOR UNIT.	VALOR TOTAL
Tomas eléctricas	30	0,20	6,00
Cable eléctrico 12AWG	2 rollos 100mts c/u	40,00	80,00
TOTAL			86,00

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración propia

5. Costo de mano de obra

En la tabla 13, se detallan los costos de mano de obra que deberán ser contratados por la institución, para las instalaciones de los equipos para seguridad perimetral, parte de cableado estructurada correspondiente a rediseño de red y configuración de equipos de red.

El número de personas necesarias para el trabajo es de 2 personas.

Tabla 13.*Costo de mano de Obra*

DESCRIPCIÓN	# PERSONAS	COSTO/DÍA	#DIAS	TOTAL
Mano de obra calificada	2	40	4	$ 1000

Nota: Los valores que se presentan en la tabla, son referenciales y se los obtiene del sitio web de cada marca.

Referencia: Elaboración Propia

B. Determinación de costo total del rediseño de la red de datos y optimización de la seguridad perimetral

En la tabla 14, se observa que la sumatoria de gastos para la parte del rediseño de la red y la seguridad perimetral

Tabla 14.Costos totales del rediseño de la red y seguridad perimetral

DESCRIPCIÓN	COSTO
Costo de equipos para rediseño de la red interna	16.789,00
Costo de equipos para seguridad perimetral	22.700,00
Costo de material de red	817,71
Costo de material eléctrico	96,32
Costo mano de obra	1.000,00
SUBTOTAL	40.722,49
IVA 12%	4.886,69
TOTAL	45.609,18

Referencia: Elaboración Propia

C. Determinación del beneficio

En el GAD Municipal de San Miguel de Urcuquí actualmente trabajan 125 empleados, distribuidos entre el edificio principal y las dependencias externas. El pago mensual que desembolsa la institución es de 156.748,75 dólares, se muestra una tabla con los valores detallados de salarios de cada empleado.

Para determinar el salario promedio de cada trabajador, se aplica la ecuación 1.

$$Valor\ a\ pagar\ mensualmente\ a\ cada\ empleado = \frac{Sueldo\ desembolsado\ mensualmente}{Número\ total\ de\ empleados}$$

Ecuación 1. *Cálculo del sueldo promedio*
Referencia: Elaboración Propia

$$Valor\ a\ pagar\ mensualmente\ a\ cada\ empleado = \frac{156.748{,}75\ dólares}{125\ empleados}$$

$$Valor\ a\ pagar\ mensualmente\ a\ cada\ empleado = \$\ 1.253{,}99$$

En la tabla 15, se detalla el valor a pagar de cada empleado de forma: mensual, diaria, por hora y por minuto, para objeto de cálculo.

Tabla 15. Valores monetario que recibe cada empleado

DESCRIPCIÓN	VALOR
Valor a pagar mensualmente a cada empleado	1.253,99 dólares
Valor a pagar diariamente a cada empleado	41,79 dólares
Valor a pagar por hora para cada empleado	5,22 dólares
Valor a pagar por minuto para cada empleado	0,08 ctvs.

Referencia: Elaboración Propia

Los empleados de dicha institución, trabajan 8 horas diarias establecidas por la ley. Sin embargo; debido a problemas en la red actual no se trabaja de manera continua, lo cual provoca distracciones de los funcionarios y genera pérdidas a la institución. Se realizó una encuesta a 25 personas escogidos alzar, para determinar un promedio de tiempo en la que la red no está disponible, obteniendo como resultados un promedio del 5%. Mediante la ecuación 2, se determina el tiempo (horas) sin servicio en el GAD Municipal de San Miguel de Urcuquí.

$$5\%\_en\_horas = (8\ horas)x\ 0{,}05 = 0{,}4\ horas$$

Ecuación 2. *Determinación del tiempo sin servicio por horas*
Referencia: Elaboración Propia

Conjuntamente con la ecuación anterior se determina el cálculo de pérdida del servicio en minutos, especificado en la ecuación 3.

$$5\%\_en\_minutos = 0{,}4\ x\ (60\ minutos) = 24 minutos$$

***Ecuación 3**. Determinación del tiempo sin servicio por minutos*
Referencia: Elaboración Propia

Con estos valores podemos concluir que el 5% de indisponibilidad del servicio de red corresponde a 24 minutos al día, en la ecuación 4, se multiplica este tiempo por el valor promedio que gana cada trabajador por minuto, arrojando un valor de 2,08 dólares.

$$Beneficio\ por\ cada\ empleado = \ 24\ minutos\ x\ 0{,}08\ ctvs = 2{,}08\ dólares$$

***Ecuación 4**. Beneficio total por día*
Referencia: Elaboración Propia

En la ecuación 5, se determina el beneficio total diario, que el GADMU ahorraría si la red estuviera en buen estado.

$$Beneficio_{total_{diario}} = \ 2{,}08\ dólares\ x\ 125\ empleados = 261{,}25\ dólares$$

***Ecuación 5**. Beneficio total*
Referencia: Elaboración Propia

En la tabla 16, se describe el beneficio por diario, semanal, mensual y anual.

Tabla 16. Resumen del cálculo de beneficio

DESCRIPCIÓN	BENEFICIO
Valor del beneficio total por día	261,25 dólares
Valor del beneficio total por semana	1.828,75 dólares
Valor del beneficio total por mes	7.837,43 dólares
Valor del beneficio total por año	94.050,00 dólares

Referencia: Elaboración Propia

D. Cálculo costo/beneficio

Luego del análisis de los gastos y beneficios que genera el proyecto, aplicamos la ecuación 6, para determinar el beneficio/costo, para lo cual se usa los siguientes parámetros:

- Si B/C es mayor que 1 se acepta el proyecto.
- Si B/C es igual a 1 el proyecto es indiferente.
- Si B/C es menor que 1 se rechaza el proyecto.

$$\frac{B}{C} = \frac{\Sigma\ \text{Beneficios}}{\Sigma\ \text{Costos}}$$

***Ecuación 6.** Cálculo del Beneficio/Costo*
Referencia: [4]

$$\frac{B}{C} = \frac{94.050{,}00}{45.609{,}18} = \mathbf{2.06}$$

Al aplicar la ecuación el valor es de 2,06; por lo que se determina que el proyecto es aceptable.

E. Periodo de devengación del proyecto

La tabla 17, se aplica para determinar en qué mes se recupera la inversión, sin embargo para tener un período de tiempo más exacto se aplica la ecuación.

***Tabla 17.** Periodo de devengación*

MES	BENEFICIO / MES	BENEFICIO ACUMULADOS
		- 45.609
1	7.837,44	7.837
2	7.837,44	15.675
3	7.837,44	23.512
4	7.837,44	31.350
5	7.837,44	39.187
6	7.837,44	47.025

Nota: El valor de 45,609 es el costo total especificado en la tabla 46 y el valor de 7.837,44 es el cálculo del beneficio por mes especificado en la tabla 48
Referencia: Elaboración propia

$$\text{Período \_devengación} = 6\ meses + \left(\frac{Costo\ total - \ \Sigma\ de\ 6\ meses}{Beneficio\ Mensual}\right)$$

Ecuación 7. Período de recuperación de la inversión

Fuente: [5]

$$\text{Período \_devengación} = 6\ meses + \left(\frac{45.609 - 47.025}{7.837{,}44}\right)$$

$$\text{Período \_devengación} = 6\ meses + (0{,}18\ x\ 30 dìas)$$

$$\text{Período \_devengación} = 6\ meses + 5\ dìas$$

Estos cálculos nos muestran que se tendrá un período de devengación de la inversión de 6 meses y 5 días.

VI. CONCLUSIONES

- Mediante la utilización de libros, artículos y tesis afines al tema, se estableció criterios esenciales para la elaboración de la fundamentación teórica de los componentes involucrado en la investigación.

- Como resultado del levantamiento de información de la situación actual de la red, se determinó que el estado físico de la red y éste no cumple con ninguna norma de cableado estructurado; ocasionando inconformidad para los empleados, y esto va en concordancia con el estado lógico de la red; la misma que no se encuentra configurada adecuadamente ya que los equipos no son administrables y se encuentran difundiendo dominios de broadcast ocasionando la saturación del éstos, afectando el rendimiento de la red.

- Mediante el cálculo del tráfico interno y externo que se genera cada usuario, y conjuntamente con el análisis del dimensionamiento de equipos activos se determinó los equipos de red a utilizarse y se escogió la marca Cisco porque brinda una solución adaptable al proyecto y con la ventaja en los ahorro monetarios para GAD Municipal de San Miguel de Urcuquí, además estos equipos son excelentes para en ámbitos de

producción, y ofrece una gama amplia de productos con precios accesible para la empresa, con beneficio en los siguientes aspectos confiabilidad, escalabilidad y fiabilidad.

- Para el rediseño de la red de datos del GADMU se implementa un modelo jerárquico basado en capas que mejorará características de disponibilidad, escalabilidad y flexibilidad; de esta manera se puede optimizará el rendimiento de la de red, a nivel de enlaces físicos y equipamiento activo, asegurando la continuidad del servicio.

- El servidor FTP permite mejorar el acceso a los archivos de los empleados, y con el servidor PROXY SQUID se limitará el acceso a páginas de entretenimiento no autorizadas por el GADMU, ayudando a mejorar el desempeño de los empleados y reduciendo el tráfico innecesario en la red.

- Para seleccionar los requerimientos del software que tendrá los servidores FTP y Proxy SQUID, se propuso un análisis con la norma IEEE-STD-830-1998 pero en el desarrollo se concluyó que esta no está vigente, por ende se utilizó la norma ISO/IEC/IEEE 29148; la misma que brinda una solución para elección adecuada del sistema operativo eligiendo características esenciales como robustez, estabilidad, con la que se determinó que Centos 6.3 (32 bits) modo texto, es la opción más factible para la implementación de los servidores.

- Para simular la red se propuso GNS3 se usó la versión 1.3.0, debido a que cumplen características similares a los equipos elegidos con los switches 2960 y 3560.

- Mediante el análisis de la tecnología UTM, se determinó que la mejor opción para la implementación de la seguridad perimetral es Juniper, ya que en comparación con otras marcas, tiene un precio económico al alcance de la empresa; mejorando la protección de la información personal, prevención de intrusos, control de acceso del usuario, seguridad, administración e ingreso a las aplicaciones de forma seguras.

- El proyecto es rentable según los cálculos del costo/beneficio, recuperando así la inversión en un periodo de 6 meses y 5 días

VII. RECOMENDACIONES

- Se recomienda que el personal a cargo de la red de datos del GADMU, continuamente se encuentre el en proceso de capacitación y aprendizaje, lo cual ayudaría a solucionar problemas de forma rápida.

- Se debe llevar una bitácora donde conste todos los eventos que se presentan en la red y los incidentes con las acciones que se realizaron para de esta manera si el personal cambia, el nuevo responsable de red, pueda entender el estado de actual de la misma y sea más sencilla su administración.
- Se propone implementar políticas de seguridad en la institución que permita establecer niveles de seguridad, orientadas a la parte de la organización, tecnológica y de usuarios, de manera que regule y controle el uso y acceso a la red.

- Se aconseja restringir el acceso mediante el uso de biométricos e incluir cámaras para registrar lo eventos maliciosos que puede ocurrir en este.

- Se sugiere cambiar las contraseñas periódicamente, estas deben contener letras mayúscula, minúsculas, números y caracteres especiales para mayor seguridad.

- Es indispensable tener un backup de las configuraciones realizadas en los equipos, ya que en caso de la una configuración mal realizada se puede restaurar el sistema sin afectarlo.

- Se recomienda la utilización de herramienta de monitoreo, para determinar los incidentes o eventos que suscitan en la red.

- Se debe tomar en cuenta que ningún equipo brinda seguridad completa, por lo cual se debe adquirir equipos de seguridad adicionales para tener más confiabilidad en el sistema.

VIII. REFERENCIAS

[1] W. Stalling, FUNDAMENTOS DE SEGURIDAD EN REDES, APLICACIONES Y ESTÁNARES, España: Pearson, 2011.

[2] J. NOGUERA y A. VÁSQUEZ, Diseño eimplementación de un circuito cerrado de televisión con cámaras IP inalámbricas y monitoreo remoto, notificaciones de eventualidades mediante el uso de un servidor para la grabación de video bajo la plataforma Linux usando zonemider para el labora, Quito, 2011.

[3] A. Tanenbaum, Redes de computadoras, México: Pearson, 2011.

[4] D. Aulema, «Estudio y diseño de un sistema de seguridad perimetral utilizando tecnologia UTM,» 14 Junio 2011. [En línea]. Available: http://bibdigital.epn.edu.ec/bitstream/15000/618/1/CD-1580%282008-06-30-03-34-00%29.pdf.

[5] S. Villalba, «Diseño de un esquema de seguridad para la intranet y extranet del CONESUP,» 2013. [En línea]. Available: http://biblioteca.epn.edu.ec/cgi-bin/koha/opac-detail.pl?biblionumber=8165&shelfbrowse_itemnumber=8533.

[6] V. G. B. &. Q. Cameron, Fundamentos de sistemas operativos, Editex, 2011.

Nació en Ibarra el 1 de Enero de 1990, sus estudios secundarios lo realizo en el Unidad Experimental “Teodoro Gómez de la Toree “donde obtuvo el título de Bachiller Técnico en Físico Matemático. En 2008 ingresó a la Universidad Técnica del Norte donde realiza sus estudios en la Facultad de Ingeniería en Ciencias Aplicadas. Actualmente es Egresado de la carrera de ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte.