UNIVERSIDAD DE SONORA
DIVISIÓN DE INGENIERÍA

POSGRADO EN INGENIERÍA INDUSTRIAL
MAESTRÍA EN INGENIERÍA EN SISTEMAS Y TECNOLOGÍA

DISEÑO E IMPLEMENTACIÓN DE UNA RED DE TELECOMUNICACIONES INTELIGENTE: CASO PROCURADURÍA GENERAL DE JUSTICIA DEL ESTADO

T E S I S

PRESENTADA POR

JOSÉ ISMAEL CAMARENA VIDALES

Desarrollada para cumplir con uno de los
requerimientos parciales para obtener
el grado de Maestro en Ingeniería

DIRECTOR DE TESIS
DR. GUZMÁN GERARDO ALFONSO SÁNCHEZ SCHMITZ

CODIRECTOR
DR. ALONSO PÉREZ SOLTERO

HERMOSILLO, SONORA, MÉXICO. SEPTIEMBRE 2017

"El saber de mis hijos hará mi grandeza"

Hermosillo, Sonora a 17 de agosto de 2017

JOSE ISMAEL CAMARENA VIDALES

Con fundamento en el artículo 66, fracción III, del Reglamento de Estudios de Posgrado vigente, otorgamos a usted nuestra aprobación de la fase escrita del examen de grado, como requisito parcial para la obtención del Grado de Maestro en Ingeniería.

Por tal motivo este jurado extiende su autorización para que se proceda a la impresión final del documento de tesis: **DISEÑO E IMPLEMENTACIÓN DE UNA RED DE TELECOMUNICACIONES INTELIGENTE: CASO PROCURADURÍA GENERAL DE JUSTICIA DEL ESTADO** y posteriormente efectuar la fase oral del examen de grado.

ATENTAMENTE

Dr. Gerardo Sánchez Schmitz
Director de Tesis y Presidente del Jurado

Dr. Alonso Pérez Soltero
Codirector y Vocal del Jurado

Dr. René Francisco Navarro Hernández
Secretario del Jurado

Dr. Mario Barceló Valenzuela
Vocal del Jurado

MSI. Francisco Javier Rosas Ibarra
Vocal Externo del Jurado

RESUMEN

Dado el apoyo y facilidad que brindan las telecomunicaciones a las organizaciones para el desarrollo de sus actividades y que gracias a ellas pueden tener presencia en diferentes sitios distribuidos geográficamente, en la actualidad, las organizaciones son más dependientes de las redes de telecomunicaciones, refiriéndose a las interconexiones entre las oficinas de la misma organización asi como para la conexión al mismo servicio de Internet. Por lo anterior las redes de telecomunicaciones y su administración se han vuelto más complejas, por lo que se tienen que desarrollar mecanismos automatizados para el monitoreo, control y administración de las mismas. Actualmente existe una arquitectura automatizada administrada por software, la cual facilitan la administración y a su vez optimiza la conectividad, dichas arquitectura es conocida como SDN (Software Defined Networking) y tiene como objetivo transformar una red “pasiva” en una “proactiva”.

El presente proyecto se desarrolló en la Procuraduría General de Justicia del Estado de Sonora (PGJE), específicamente en la Dirección de Sistemas. La mencionada Dirección apoya en el desarrollo y mantenimiento de los Sistemas Informáticos con los cuales la organización desarrolla sus actividades, así mismo tiene la función de interconectar las Unidades Administrativas (UA) con el edificio central de la PGJE, para que las UA puedan acceder a los sistemas y servicios hospedados dentro del edificio principal.

Derivado a que la organización está en la implementación del Nuevo Sistema de Justicia Penal, el cual cambió el esquema de red de telecomunicaciones de distribuido a centralizado, se hizo vital la interconexión entre la UA y el edificio central de la PGJE y dado a que no todas las UA cuentan con una conexión o bien las que sí tienen son demasiado lentas que no soportan la utilización de los sistemas de información requeridos para el desarrollo de sus actividades. También la infraestructura de red

interna propia tanto de las UA como la de la PGJE se encuentran en un estado tecnológico obsoleto.

Una vez realizado un proceso de investigación documental, no se encontró una metodología o procedimiento el cual ayude a resolver las problemáticas particulares que se presentaron en la organización, es por esto que se hizo el planteamiento de un procedimiento con el fin hacer una evaluación de la situación actual de la organización, teniendo como objetivo realizar una implementación de SDN, que considerara, que en el caso de no contar con una factibilidad técnica o bien que la implementación de SDN no resuelva las problemáticas planteadas de la organización recomendara optimización de los recursos de infraestructura actuales, así como un análisis de requerimientos para hacer más eficiente la red de telecomunicaciones y resolver las problemáticas planteadas.

La implementación de dicho procedimiento ayudó a resolver las problemáticas de interconexión entre las UA y el edificio central, así como optimizó y mejoró las infraestructuras de red interna tanto de la UA como de edificio central de la PGJE, donde dicha infraestructura no cumplía con los requerimientos para el buen funcionamiento de los sistemas de información. También se facilitó la administración y control de la red para el personal encargado de administrarla, automatizando procesos y disminuyendo los tiempos de reacción para la realización de acciones correctivas.

ABSTRACT

Currently the organizations are more dependent of telecommunication networks, for the interconnection between offices of the same organization as well for the Internet service connection. Giving the support and ease provided by telecommunications to the business for the development of their activities, telecommunications provide the ability to have presence in different geographical distributed points is it that their demand has grown. Based on the foregoing, the telecommunication networks and their administration has become more complex, reason why is required the development of automated mechanisms for the monitoring, control and administration. Currently exists an architecture administered by software which eases the administration and at the same time automate the connectivity. This architecture is known as SDN (Software Defined Networking), having as main objective to transform a passive network to a proactive network.

The present project was developed in the Attorney General of Justice of the State of Sonora, specifically in the Systems Division, This Division supports the development and maintenance of information systems in which the organization develops its activities and it provides the required interconnection between the administrative units and the central building giving the required access to the services and systems hosted in the central building.

Due to that the organization is implementing the new accusatory system, the architecture of the telecommunication network changed from a distributed to a centralized model. Thereby the interconnection between the administrative units and the central building became vital. Having that not all the administrative units are connected and that they have a slow connection that does not allow to use the information systems required to develop their activities. Along with these, the internal network infrastructure in the central building and in the administrative units is obsolete.

Because we were not able to find a methodology or procedure to help us solve the difficulties present in the organization, we propose a procedure to evaluate the actual situation of the organization to implement a SDN architecture, in such case that organization does not have the technical viability or that the SDN implementation does not solve the difficulties exposed, recommend instead the optimization of the current organization infrastructure resources and the analysis of the requirement needed to transform in to a more efficient telecommunication network and to solve the difficulties exposed.

The implementation of the procedure help us to solve the difficulties of interconnection of the administrative units with the central building, and to optimize and improve the internal infrastructure in the administrative units and the central building of the Attorney General of Justice of the State of Sonora, having thus that the infrastructure implemented accomplish the needed requirements for the optimal performance of the information systems, facilitating also the administration and control of the telecommunication network for the employees responsible for managing it, by process automation which decreased the time to accomplish corrective actions.

DEDICATORIAS

“Si la oportunidad no llama, construye una puerta”

A mi prometida Dalia Corral, a mis padres Ismael Camarena y Luz Cristina Vidales, a Trinidad Corral y Rosa Guerrero, familiares y amigos que estuvieron a lo largo de este ciclo en mi vida.

AGRADECIMIENTOS

Primeramente, a Dios por brindarme la capacidad y fortaleza para culminar esta etapa de mi vida y darme la fuerza de siempre seguir adelante.

A mi prometida Dalia Corral, por su amor y apoyo incondicional alentándome siempre a un crecimiento personal y profesional.

A mis padres Ismael Camarena y Luz Cristina Vidales, que siempre me han apoyado y confiado en que puedo alcanzar mis objetivos.

Al Dr. Guzmán Gerardo Alfonso Sánchez Schmitz por su apoyo y consejos para la realización de este proyecto, así como la confianza y amistad brindada.

Al Dr. Mario Barceló Valenzuela por todo el apoyo brindado y aconsejarme a lo largo del proyecto de tesis.

Al Procuraduría General de Justicia del Estado de Sonora por todo el apoyo y la oportunidad del desarrollo del proyecto, en especial a la directora Lic. Rebeca Salazar Pavlovich y Lic. Jesus Ariel Gándara Toledo.

A mis compañeros y al cuerpo académico de la maestría que estuvieron siempre brindando su apoyo.

Al Consejo Nacional de Ciencia y Tecnología (CONACYT) y al Programa de Fortalecimiento de la Calidad Educativa (PFCE 2016) por su apoyo económico, el cual me facilitó en gran medida el logro de esta meta.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN

En la actualidad utilizar aplicaciones dependientes de las tecnologías de telecomunicaciones es cada vez más común, debido a ello su crecimiento es acelerado, haciendo su administración y mantenimiento más compleja (Yang y Chang, 2011). La complejidad de una red de telecomunicaciones está dada por la demanda de múltiples servicios y versatilidad. Los modelos de administración actuales son inadecuados para soportar la gran demanda de servicios. En la administración tradicional de una arquitectura de red, el objetivo es simplemente reportar y actualizar el estatus de los dispositivos conectados (Martín et al., 2012). Hay organizaciones que hacen poca supervisión sobre el ancho de banda que consumen por cada servicio y los recursos de hardware que utilizan, propiciando ineficiencia y dificultad en la detección de fallas (Casta, 2011).

El propósito de la administración de la red es gestionar eficientemente el equipamiento involucrado en la infraestructura de red, identificar problemas presentados y realizar las acciones correctivas correspondientes, utilizando de herramientas de apoyo que permitan la detección inmediata de falla, brindando así un servicio de calidad, siendo esto último el reto más importante de la administración de las redes modernas (Yang y Chang, 2011).

Por lo que, en función de una estructura de red tradicional que se ha vuelto más compleja, la capacidad de control cada vez es menor y difícil de garantizar la calidad en el servicio. El “software defined networking” (SDN) proporciona una nueva forma de resolver los problemas anteriores mediante un nuevo tipo de arquitectura presentada por “CleanSlate”, un equipo de investigación de la Universidad de Stanford (Luan et al., 2015). La aparición de SDN transforma la red “pasiva” en una “proactiva”, de modo que la red puede manejar el tráfico de forma activa y flexible (Cui et al., 2014).

Dado que SDN permite al administrador de la red gestionarla de manera más fácil y flexible, se espera superar los problemas tales como, construir una red con equipos de

conmutación de diferentes fabricantes teniendo así un lenguaje de configuración diferente, eliminar problemas provenientes de la intervención de la mano humana (Nakayama et al., 2014).

1.1 Presentación

El proyecto se realizó en la Procuraduría General de Justicia del Estado (PGJE), la cual cuenta con varias direcciones en su organigrama, específicamente se desarrollará en la Dirección General de Sistemas de Información y Política Criminal (DGSIPC) la cual está enfocada en mantener los servicios informáticos utilizados por la dependencia, el desarrollo de nuevos sistemas y la interconectividad entre las Unidades Administrativas (UA). La Dirección se divide en cuatro direcciones de área: Dirección de Sistemas de Información y Base de Datos, Dirección de Estadística y Política Criminal, Dirección Sistema de Apoyo al Ministerio Público y Dirección de Innovación Tecnológica de Sistemas Biométricos, teniendo un total de 23 empleados incluyendo al Director General.

Actualmente dentro la PGJE se está implementando el nuevo Sistema de Justicia Penal (SJP), por lo que la dirección DGSIPC está a cargo de poner en marcha un nuevo sistema de información que cumpla con los requerimientos del nuevo esquema de Justicia. El acceso al sistema y la interconectividad entre las UA se han convertido en parte fundamental para el desarrollo de las actividades de las mismas.

El sistema de información utilizado en el esquema de Justicia anterior sigue en funcionamiento hasta que se termine de implementar el nuevo esquema, lo cual se está realizando por fases en todo el Estado, con respecto al anterior sistema tiene un funcionamiento descentralizado donde cada UA cuenta con su propio servidor, la información se replica a un servidor central para su recolección y así facilite el análisis estadístico, consulta de información y respaldo de los datos. La replicación de la información presenta problemas ya que no todas las UA cuentan con un enlace al servidor central o en algunos casos el servicio es demasiado lento o intermitente. Por otro lado, el nuevo Sistema de Información que se encuentra en fase de

implementación es un esquema centralizado, por lo que se ve afectado directamente por la problemática descrita anteriormente ya que se encuentra hospedado en el servidor central.

La infraestructura de telecomunicaciones con la que cuenta la PGJE y las diferentes UA es muy heterogénea lo que hace difícil para los administradores de la red el monitoreo y su administración, ocasionando que el tiempo de ejecución de acciones correctivas al presentarse una situación anómala o de falla sean muy largos o bien que solo una persona tenga la capacidad de solucionar los eventos presentados.

1.2 Planteamiento del Problema

La Procuraduría General de Justicia del Estado está implementado el SJP mediante un Sistema de Información en el cual accedan todas las UA del Estado, por lo que es crítico contar con una conexión estable y de alta disponibilidad con el servidor central, así mismo es necesario mejorar la arquitectura de red para un monitoreo y administración eficiente que reduzca los tiempos de acciones correctivas en el caso de falla.

1.3 Objetivo General

Diseñar e implementar una arquitectura de red administrada por software, con el fin de mejorar la estabilidad y disponibilidad de la red entre las UA y el servidor central de la PGJE; así mismo permita crear procesos automatizados de monitoreo y administración del equipamiento involucrado en la infraestructura de red.

1.4 Objetivos Específicos

- Configurar el equipo seguridad perimetral de las UA para tener un funcionamiento automatizado y de alta disponibilidad con el servidor central.
- Diseñar un modelo de monitoreo del equipamiento de red, que alerté en el caso de falla y almacené los sucesos para su análisis posterior, como apoyo a la toma de decisiones.

- Optimización de los recursos de red con el fin de automatizar los procesos y operaciones de red.
- Evaluar los tiempos de ejecución de acciones correctivas y cantidad de errores presentados en un periodo determinado, con la arquitectura actual y posterior a la implementación propuesta.
- Crear una arquitectura de red de alta disponibilidad para tener tolerancia a fallos.

1.5 Hipótesis

Implementar una arquitectura de red que permita la administración y control del equipamiento red mediante software y/o la automatización de operaciones de red, así como la interconexión entre las UA y el servidor central, disminuirá la inestabilidad y desconexiones, así como los tiempos en la ejecución acciones correctivas en el caso de fallas en la red.

1.6 Alcances y Delimitaciones

El proyecto se ha enfocado en implementar una arquitectura de alta disponibilidad entre las UA y el servidor central, y se basará solo en las UA que cuenten con al menos dos enlaces de Internet o intranet y equipamiento que soporte las configuraciones necesarias de la arquitectura propuesta. La arquitectura para la administración y control de la infraestructura de red, será implementada únicamente UA que además de los enlaces de interconexiones cuenten con el equipamiento de red para realizar la propuesta.

1.7 Justificación

La utilización del nuevo Sistema de Información se ha convertido en parte fundamental para las actividades de la PGJE, por lo que, si una UA pierde la conexión al servidor central y no se puede acceder al Sistema, ocasiona deficiencia en el servicio brindado a la ciudadanía, más grave aún la incongruencia o pérdida de información.

La arquitectura de red se ha desarrollado como apoyo al servicio de red y telecomunicaciones de la PGJE, debido a que no cuenta con un esquema adecuado de monitoreo en tiempo real que este analizando el estado de la red y con la capacidad de alertar a los administradores en el caso de presentarse alguna falla, tanto en la interconexión entre las UA y el servidor central, como dentro de la misma infraestructura de la PGJE, reflejándose en largos tiempos de ejecución de acciones para la solución de los problemas presentados.

La optimización y automatización de los procesos de red, simplifica la administración y control del equipamiento de red, así mismo la solución de fallas o configuraciones adicionales.

Por lo tanto, la implementación de dicha arquitectura beneficio a realizar acciones correctivas eficientes en el caso de presentarse problemas o anomalías en la red que afectan directamente a las principales actividades de la PGJE, así mismo se almaceno las fallas y soluciones de los eventos suscitados permitiendo su análisis posterior como apoyo a la toma de decisiones. Por último, habilito un esquema de alta disponibilidad en la conectividad con el servidor central con una operatividad automatizada de corrección de errores, resultando esto en un servicio estable durante todo el día, ya que el personal a cargo del soporte de la red tiene un horario laboral que difiere del personal vespertino/nocturno, donde en el caso de presentarse falla, se interrumpe el servicio y se espera a la solución hasta el día posterior.

2 MARCO DE REFERENCIA

En este capítulo se presenta la revisión bibliográfica, la cual sustenta el desarrollo del presente proyecto. Se aborda solo conceptos avanzados relacionados con las redes de telecomunicaciones, así como de herramientas de software diseñadas para la administración y monitoreo del equipamiento de la infraestructura de red. Así mismo se presenta estudios previos relacionados con el tema de esta investigación. Se aclara que los conceptos básicos de redes, sus protocolos y propiedades no se describen ya que son temas de conocimiento general de los administradores de red.

2.1 Redes definidas por software

La aparición del SDN ha creado el potencial y la esperanza de superar las necesidades de las siguientes generaciones de redes de telecomunicaciones, dando seguridad, flexibilidad, confiabilidad y una mejor administración. Con SDN se centraliza la administración a un controlador externo al equipamiento, haciendo más sencillo la programación de todo el hardware. Las características que ofrece SDN obviamente son muy notables, como una arquitectura innovadora, rentable y programable independientemente del fabricante de tecnología. Aunque se muestran muchas características positivas del utilizar SDN, existe la preocupación por parte de los expertos acerca del tema de la seguridad, lo cual consideran que debe de tratarse de forma muy minuciosa (Akhunzada et al., 2015).

En la arquitectura tradicional cada equipo dentro de la red se podría decir que es un controlador por lo que cada decisión de enrutamiento u otro protocolo es realizado por cada equipo. Por otro lado, en la arquitectura de SDN existen varios componentes responsables en la entrega de los paquetes de extremo a extremo como se muestran en la figura 2.1., 1- Interface de red: cada dispositivo en la red cuenta con interfaces con las cuales se interconectan para comunicarse con otros dispositivos, 2- Dirección Norte (Aplicación), es la interacción entre las aplicaciones que se ejecutan dentro la infraestructura de red y el controlador de SDN, 3- Dirección Sur (Aplicación), esta zona

se utiliza normalmente en protocolo de OpenFlow, en donde se define una serie de reglas para el desvío de los datos, lo cual permite al equipamiento de enrutamiento y conmutación el entendimiento de la topología de red, así mismo las solicitudes enviadas desde los aplicación de la dirección norte; 4- el Controlador, es lógicamente un controlador centralizado responsable de: a) Interpretación de los requisitos previos de la aplicación de SDN hasta el plano de datos, b) proporciona una visión de red que puede incluir Notificación de eventos, reportes estadístico, reenvío de paquetes, entre otros (Patel, 2016).

SDN promete simplificar la implementación y la operación de la red de telecomunicaciones, a la par reducir los costos de administración de la misma, brindando servicio de red programables (Fraser et al., 2013).

Debido a su paradigma de control centralizado, SDN está siendo adoptado para las redes como, los centros de datos, redes móviles, redes de trasporte y las redes empresariales, por lo que es muy importante la resistencia a las fallas, existen dos tópicos para atacar las problemáticas mencionadas que es la restauración y protección. La restauración, cuando un switch detecta un fallo en el enlace de la conectividad, entonces un mensaje de notificación se envía al controlador para que calcule un nuevo camino al flujo de la interconexión entre los switches. En la protección, el controlador calcula varias rutas de interconexión entre los switches, instalando las entradas en cada uno de ellos con anterioridad, con el fin de que el caso de fallo el switch puede dirigir al tráfico a otra ruta previamente cargada sin tener que esperar las órdenes del controlador. Además de la perdida de enlace, otro de los problemas que tienen los administradores de red es la congestión en los enlaces, el cual es derivado de sobre saturación de datos por un mismo enlace, efecto que ocasionaría una reducción en el rendimiento de la red (Lin et al., 2016).

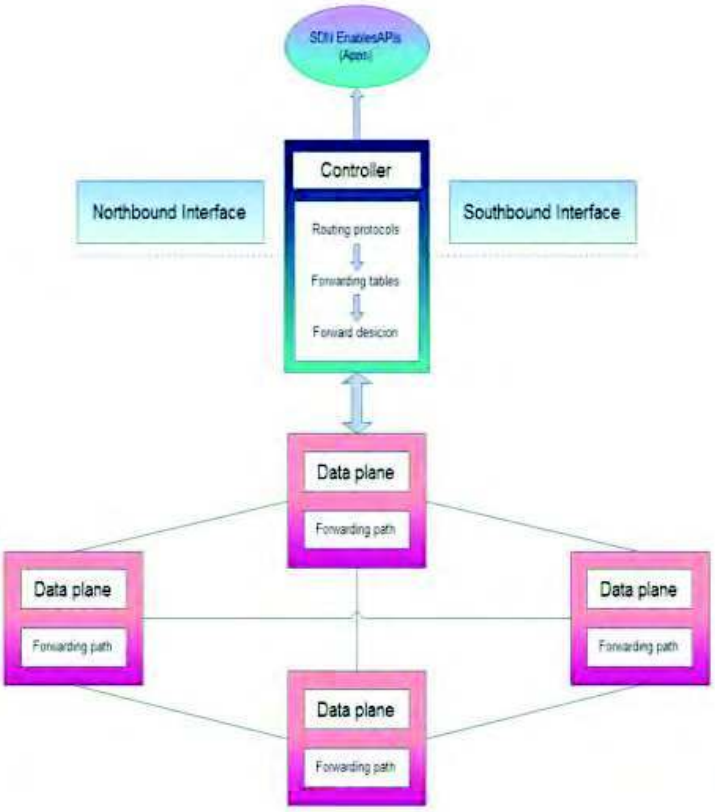


Figura 2.1 *Representación de SDN (Patel, 2016)*

2.2 Principales protocolos de monitoreo y control de SDN

Los protocolos populares para SDN son el ForCES (Forwarding and Control Elements Separation) y OpenFlow. Ambos protocolos utilizan el principio fundamental de SDN que es separar los planos de control y datos (Patel, 2016).

OpenFlow un protocolo presentado por primera vez en el año 2008, es un protocolo de comunicación para la manipulación remota el reenvió de enrutadores y conmutadores; es considerado por algunos como el sinónimo de SDN y ahora es un elemento clave dentro de las iniciativas industriales de SDN, actuando como protocolo utilizado por los controladores de SDN (Bondkovskii et al., 2016). Openflow ha ganado en los últimos años la atención de los investigadores con respecto a la red de

telecomunicaciones. La contribución de Openflow es que era una interfaz donde se programaba el reenvió de tráfico dentro de los equipos de conmutación (switch), lo que fue la inspiración para el lanzamiento de lo que hoy conocemos como SDN, ya que se presenta deficiencias en las reglas de reenvío programados en los equipos de conmutación son de forma estáticas por lo que es requerido un controlador para automatizar y hacer dinámico los ajustes den la reglas en el caso de cambios (Pontarelli et al., 2016). El protocolo Openflow tiene tres componentes: Switch OpenFlow, un canal para el OpenFlow y un controlador. Un Switch OpenFlow consiste en una o diversas tablas de flujos las cuales transitan a través del canal de flujo al controlador externo con el fin de manejar los paquetes de tráfico (Shin et al., 2016).

Uno de los servicios esenciales dentro de una red de SDN es el descubrimiento de la topología de red, la cual soporta las aplicaciones de alto nivel como es el enrutamiento y el reenvió de paquetes. Si bien no hay una norma oficial para el mecanismo de descubrimiento en una arquitectura de SDN, se podría decir que existe un estándar OFDP (OpenFlow Discovery Protocol), todos los principales controladores de SDN implementan esencialmente este mecanismo de descubrimiento (Alharbi y Portmann, 2015).

2.3 Principales plataformas de SDN de open source

El controlador central de SDN permite tener un seguimiento del rendimiento y funcionalidad de la red, así como realizar la reconfiguración si es necesario, supervisa de manera puntual el tráfico de los paquetes y los enlaces de conectividad, con el fin de restaurar si hay una pérdida de enlace, esto con el objetivo general de cualquier red, el garantizar la conectividad de un punto a otro. Uno de los protocolos más tradicionales para esto dentro del SDN es el OpenFlow, el cual funciona en la zona norte de la arquitectura entre el plano de control y el plano de datos. Por desgracia OpenFlow no implementa rápidos mecanismos de recuperación de fallos, los cuales son necesarios para una red de telecomunicaciones confiables, así mismo OpenFlow utiliza un esquema de programación de muy bajo nivel, limitando las capacidades de

control de brinda el control de SDN, por lo que los investigadores están proponiendo mecanismo de recuperación de fallos en OpenFlow (Rufaida Ahmed, 2016).

Las características principales de un controlador de SDN son:

- Multiplataforma: Fácil de aprender, buen uso y manejo de la memoria del computador, característica esencial de los lenguajes de programación, siendo lo más comunes Python, C++ y Java, teniendo ventajas y desventaja cada uno de ellos.
- Southbound API´s, permite el control sobre la red, donde el controlador utiliza estas API´s para realizar cambios necesarios en las reglas de envío de tráfico que se encuentran instaladas en los equipos del plano de datos, como lo son: switches, routers por mencionar algunos.
- Northbound API´s, son utilizadas para la comunicación del controlador con la capa de aplicación, por lo que son parte fundamental de SDN, ya que la interacción adecuada de estas, proporciona un mejor servicio.
- OpenFlow es un habilitador clave para SDN, fue la primera interfaz estandarizada de Southbound, permite la manipulación directa del plano de reenvío de tráfico.
- La programación de la red es unos de los beneficios más importantes de SDN, por la complejidad en el control y administración derivado de la gran cantidad de dispositivos conectados a la red, así como la necesidad de nuevos servicios. Por lo anterior no es factible la administración tradicional de la red que es equipo por equipo de manera individual, por lo que SDN viene a resolver estas dificultades de gestión de red.
- Eficiencia, es un término utilizado para varios parámetros: rendimiento, escalabilidad, fiabilidad y seguridad, así mismo tiene métricas como la cantidad de interfaces que puede administrar, latencia, entre otros. La parte de centralización es un reto con respeto a términos de rendimiento y fiabilidad, por lo que existen propuesta de varios controladores distribuidos con el fin de la alta disponibilidad y tolerancias a fallos.

- Asociación, se refiere a la compatibilidad con productos o soluciones de múltiples fabricantes como por ejemplo: CISCO, Linux, Intel, IBM, Juniper, entre otros (Salman et al., 2016).

2.3.1 Controladores y plataformas de SDN

Open Network Operating System (ONOS) es el primer SDN de código abierto dirigido a proveedores de servicio y a redes de telecomunicaciones de misión crítica. ONOS desde que era conocido como Network Operating System (NOS) tiene como función: administración de los recursos finitos, aislamiento y protección de los usuarios por mencionar algunas (Shin et al., 2016). Aunque con ONOS se puede resolver lo que es cuello de botella del plano de control, todavía sigue siendo problemático el decidir cuándo y cómo distribuir la carga de trabajo del plano del control, además es un factor que puede afectar e rendimiento del plano de control tales como el intercambio de comunicación entre el controlador. Por lo tanto, la mayoría de los controladores deberán exigir el sistema de seguimiento del plano de control (Kim et al., 2016).

NOX es una pieza de las redes SDN, en concreto se trata de una plataforma para el desarrollo de aplicaciones para el control de la red, donde al comienzo Openflow fue reconocido como la primera tecnología de SDN, NOX fue desarrollado en paralelo como el primer controlador de OpenFlow (Noxrepo.org, 2016).

POX es el hermano menor de NOX, el cual, en esencia, es una plataforma para el rápido desarrollo y creación de prototipos de software de control de red utilizando Python con el fin de ayudar a escribir a un controlador de OpenFlow. También es utilizado como base para ayudar a construir redes SDN (Noxrepo.org, 2016).

Opendaylight (ODL) es una plataforma modular de código abierto de SDN para las redes independientes a la escala y tamaño de las mismas. ODL permite los servicios de red a través de un entorno múltiples vendedores de hardware, proporcionando al usuario el administrar y controlar múltiples protocolos y aplicaciones (Opendaylight.org, 2016).

2.3.2 Comparativo de controladores de SDN

A continuación, se muestran en la tabla 2.1 el comparativo de algunos controladores de SDN.

	Programming Language	GUI	Documentation	Modularity	Distributed/ Centralized	Platform Support	Southbound APIs	Northbound APIs	Partner	Multithreading Support	OpenStack Support	Application Domain
ONOS	Java	Web Based	Good	High	D	Linux, MAC OS, And Windows	OF1.0, 1.3, NETCONF	REST API	ON.LAB, AT&T, Ciena, Cisco, Ericsson, Fujitsu, Huawei, Intel, Nec, NsfNtt Comunnication, Sk Telecom	Y	N	Datacenter, WAN and Transport
Open-Day-Light	Java	Web Based	Very Good	High	D	Linux, MAC OS, And Windows	OF1.0, 1.3, 1.4, NET-CONF/ YANG, OVSDB, PCEP, BGP/LS, LISP, SNMP	REST API	Linux Foundation With Memberships Covering Over 40 Companies, Such As Cisco, IBM, NEC	Y	Y	Datacenter
NOX	C++	Python + QT4	Poor	Low	C	Most Supported On Linux	OF 1.0	REST API	Nicira	NOX _MT	N	Campus
POX	Pyth on	Python + QT4	Poor	Low	C	Linux, MAC OS, And Windows	OF 1.0	REST API	Nicira	N	N	Campus
RYU	Pyth on	Yes	Fair	Fair	C	Most Supported On Linux	OF 1.0, 1.2, 1.3, 1.4, NETCONF, OF-CONFIG	REST For Southb ound	Nippo Telegraph And Telephone Corporation	Y	Y	Campus
Beacon	Java	Web Based	Fair	Fair	C	Linux, MAC OS, And Windows	OF 1.0	REST API	Stanford University	Y	N	Research
Maestro	Java	-	Poor	Fair	C	Linux, MAC OS, And Windows	OF 1.0	REST API	RICE, NSF	Y	N	Research
Floud-Light	Java	Web/ Java Based	Good	Fair	C	Linux, MAC OS, And Windows	OF 1.0 , 1.3	REST API	Big Switch Networks	Y	N	Campus
Iris	Java	Web Based	Fair	Fair	C	Linux, MAC OS, And Windows	OF 1.0, 1.3, OVSDB	REST API	ETRI	Y	N	Carrier-Grade
MUL	C	Web Based	Fair	Fair	C	Most Supported On Linux	OF 1.4, 1.3, 1.0, OVSDB, OF-CONFIG	REST API	Kaicloud	Y	Y	Datacenter
Runos	C++	Web Based	Fair	Fair	D	Most Supported On Linux	OF 1.3	REST API	ARCCN	Y	N	WAN, Telecom and Datacenter
Lib-Fluid	C++	-	Fair	Fair	-	Most Supported On Linux	OF 1.0, 1.3	-	ONF	Y	N	-

Tabla 2.1 *Comparativo de Controladores de SDN* (Salman et al., 2016)

2.4 La seguridad y SDN

La administración de la red ha pasado al siguiente nivel, pero también viene con las cuestiones de seguridad y vulnerabilidades. Un administrador de red puede controlar el equipamiento desde una consola central, sin tener que tocar cada uno de los equipos, esto también aplica para las redes inalámbricas, lo que hace más flexibles, escalables y agiles, que las redes tradicionales. La parte de seguridad de SDN puede ser divida en tres áreas: 1.- amenazas actuales como ataques de negación de servicio, ataques distribuidos de negación de servicio, troyanos, hackeo y robo de información sensibles, 2.- Vulnerabilidad en los softwares utilizados para SDN y 3.- único punto de falla por utilizar una arquitectura centralizada (Bindra y Sood, 2016).

Desde el surgimiento de SDN el tema de la seguridad de la red ha sido muy relevante. Los nuevos paradigmas de las redes traen grandes beneficios a la parte de la seguridad de la red, se mencionan tres características que diferencias las redes de SDN con las redes Tradicionales: la perspectiva de la seguridad, visión global de la red, auto-corrección de errores y el aumento en la capacidad de control y administración de la red. Sin embargo, algunos problemas de seguridad son específicos de la arquitectura de SDN y los cuales no han sido abordados, centrándolo es la parte de ataques de las comunicaciones en el plano del control, ataques contra los controladores y falta de mecanismos para asegurar la confianza entre las aplicaciones de administración específicas de SDN y el controlador, donde dichas vulnerabilidades se pueden reflejar en graves desastres dentro de la red (Wang et al., 2016).

2.4.1 Tipos de ataques comunes

Al tener una arquitectura de SDN, también conlleva tener una serie de vulnerabilidades o ataques, que ocasionen interrupción en la comunicación a continuación, se mencionan algunos de los ataques más comunes:

- (Man-in-middle attack between switch and controller) es un método clásico de ataque a la red, donde implica colocar un nodo intermedio entre la comunicación del nodo fuente con el nodo destino, lo cual es utilizado para interceptar datos y manipularlo sin ser detectado por ninguno de los dos nodos participantes en la comunicación.
- (DoS attack to saturate the flow table and flow buffer) el ataque de negación de servicio es una inundación de paquetes en la red y como en la arquitectura de red, cada vez que un paquete vaya a un destino desconocido se genera una nueva regla de flujo dentro del switch, por lo que si se comienza a genera de manera simultánea y rápidamente paquetes a múltiples destinos saturando la capacidad de almacenamiento de tablas de flujo del switch (Shu et al., 2016).

2.4.2 Ventajas y desventajas de seguridad de SDN

La utilización de SDN a comparación de las redes tradicionales, tiene amenazas aún más concentradas por el esquema centralizado, a diferencia de un esquema más distribuido o disperso como lo es el tradicional, por lo que SDN tiene ventajas y desventajas con respecto a la seguridad:

Ventajas:

- Eficiencia al monitorear tráfico anormal, debido que el controlador de SDN tiene conocimiento de todo el tráfico de la red de manera simultánea, por lo que facilita observar un comportamiento anómalo.
- Tratamiento oportuno de las vulnerabilidades, el administrador puede programar la forma de analizar y tratar dicha vulnerabilidad, a diferencia de cuando se depende del fabricante lo resuelva y actualice el software del equipamiento involucrado.

Desventajas:

- Vulnerabilidad del Controlador, ya que la mayoría de las acciones tales como, recopilación de la información de la red, la configuración del equipamiento de

red y cálculo de enrutamiento, se concentran en el controlador, por lo que, si un atacante logra conseguir la administración de un controlador de SDN, puede causar una parálisis total de los servicios de red afectando toda la red, donde el controlador tenga cobertura.

- Riesgo a causa de interfaces abiertas programables, debido a su naturaleza abierta, SDN se hace más susceptible a las amenazas de seguridad.
- Más puntos de ataque debido a que la arquitectura de SDN se divide en 3 capas y la comunicación entre ellas será necesaria y más frecuente, como se representa en la figura 2.2 (Shu et al., 2016).

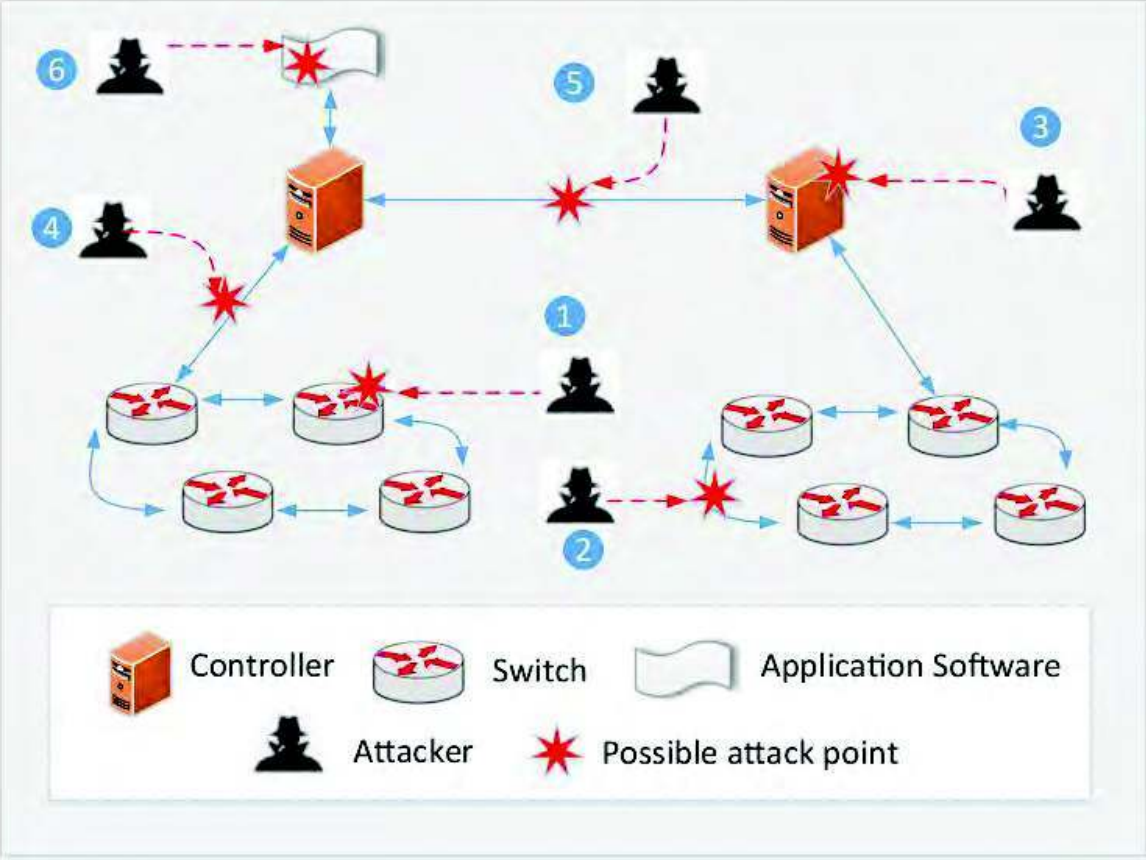


Figura 2.2 *Múltiples puntos de ataque en SDN* (Shu et al., 2016)

2.5 Virtualización y SDN

La virtualización de la red es un método que provee una ilusión de una red dedicada por encima de los recursos de hardware, la cual permite compartir los mismos recursos de hardware a múltiples usuarios sin ocasionar alguna interferencia entre ellos. La virtualización de red puede tener varias ventajas, como la flexibilidad, compartición de recursos, escalabilidad, agilidad y bajos costos económicos y de operación. Desafortunadamente este tipo de soluciones de virtualización se centran en tecnologías como VMware y Hyper-V utilizando un método de túnel fácil de implementar y sin tener que realizar cambios de configuración en la red, pero al trabajar de esta forma genera sobrecarga del túnel, por lo que se requiere un equipamiento especializado como son conmutadores virtuales o controladores (Han et al., 2016).

SDN (Software Defined Networking) y NFV (Network Function Virtualization) son paradigmas que se complementan como se muestra en la figura 2.3, donde SDN se centra en el control de los recursos de red mediante software para proveer un servicio, mientras NFV se centra en el ciclo de vida de algunos servicios de red. De hecho, SDN puede ser utilizado para el control de los servicios en una arquitectura de red tradicional, virtualizada o un combinación de ambas (Naudts et al., 2016).

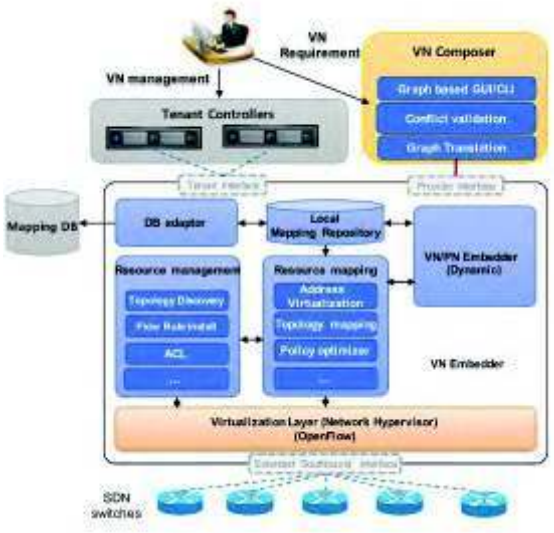


Figura 2.3 *Virtualización con SDN* (Han et al., 2016)

2.5.1 Usos y Ventajas de SDN

SDN y OpenFlow proporcionar varias ventajas al utilizar la virtualización en la red, ya que provee la abstracción en hardware de los switches. Con OpenFlow se pueden asignar los recursos físicos para cada una de las virtualizaciones a través de tablas de flujo segmentadas, por lo que ha este enfoque es llamada enfoque de red virtual segmentado. Actualmente existen varias herramientas para el enfoque anteriormente mencionado los cuales están disponibles como, FlowVisor, OpenVirtex y FlowN. Al utilizar este enfoque basado en segmentos se soluciona la parte de la sobrecarga de los túneles, así mismo, proporciona un mejor nivel de control para la parte de calidad y nivel de servicio en el tráfico de red. El principal problema que se presenta con la implementar SDN y Virtualización es que se requiere un infraestructura de red basada en OpenFlow (Han et al., 2016).

2.7 Estudios Previos

En base a la revisión de la literatura, a continuación, se presentan estudios previos relacionados con el tema de esta investigación.

2.7.1 Universidad de Guadalajara y SDN

La nueva dorsal de telecomunicaciones la Universidad de Guadalajara ha comenzado la implementación de funcionalidades con SDN, ya que los equipos cuentan con circuitos integrados programables (FPGAs, similares a las aplicaciones de los ASICs) que son lo suficientemente sofisticados para reconocer diferentes tipos de paquetes y tratarlos de forma diferente. Con la finalización de la primera etapa de implementación de SDN en la red de comunicaciones universitaria, permite el fortalecimiento e innovación de la red por medio de OpenFlow, ofreciendo al administrador de red la capacidad de controlar los flujos de tráfico de manera dinámica, desde una consola centralizada (web) sin tener que tocar los switches en lo individual, cambiar cualquier regla de los switches cuando sea necesario agregando o quitando prioridad, o hasta bloquear tipos específicos de paquetes con un nivel de control muy detallado por medio de APIs de programación, disponibles en plataformas como OpenDayLight, (Ipv6.udg.mx, 2016).

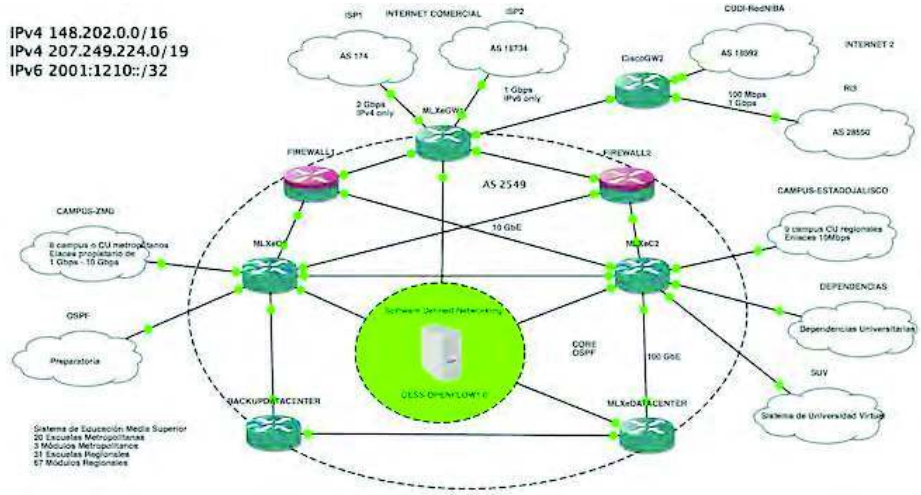


Figura 2.4 *Ruteo utilizando SDN* (Ipv6.udg.mx)

2.7.2 GEANT

GEANT está introduciendo las capacidades de SDN en su infraestructura principal para un servicio de ancho de banda bajo demanda (BoD). Este servicio utiliza el

DynPaC Framework como se muestra en la figura 2.5, el cual ofrece ingeniería de trafico dinámico y adaptable utilizando el cálculo de enrutamiento. DynPaC proporciona un uso eficiente de las capacidades de la red, así como flexibilidad en el caso de fallas en los enlaces, teniendo tiempos de recuperación de errores más rápidos, como una reducción de costos operativos y una mejora significativa en la supervisión y monitoreo de la red, recopilando la información. El administrador de servicios DynPaC actúa como un coordinador de las interacciones entre los otros módulos del Framework mencionado y supervisando los eventos para determinar cómo reaccionar, utilizando movimiento de flujos a rutas alternativas resultando en resiliencia y recuperación de fallas (Opendaylight.org, 2016).

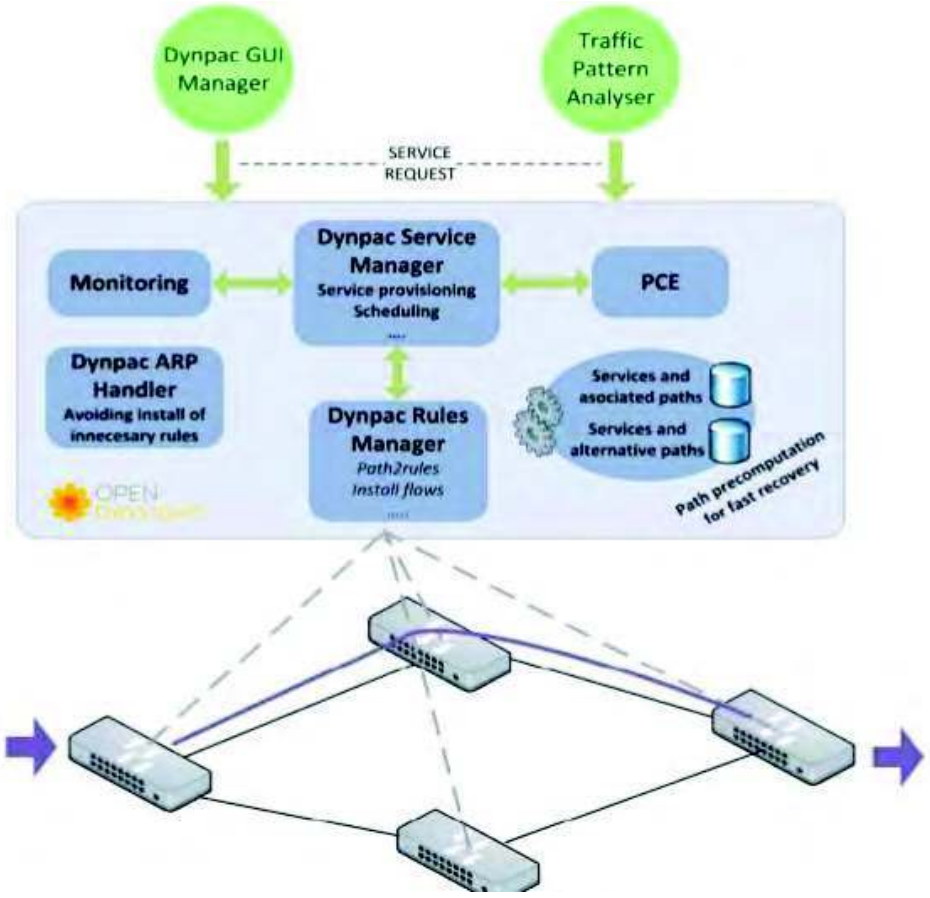


Figura 2.5 *DynPaC Framework* (Opendaylight.org, 2016)

3 PROCEDIMIENTO

En este capítulo se presenta un procedimiento creado para aprovechar de la infraestructura de red, identificar las necesidades de adecuaciones y mejoras para la optimización del flujo de información dentro de la organización, así como el mejoramiento del servicio que se brinda a los usuarios en general. Como se puede observar la figura 3.1, el procedimiento consta de 5 fases, donde se comienza con el análisis de la situación actual de la organización para conocer el equipamiento de infraestructura con el que cuenta, así como lo servicios de interconectividad que utiliza. Después se realizará las adecuaciones para la implementación de una arquitectura de SDN, en el caso de que la infraestructura de red actual de la organización no cuente con los requerimientos mínimos necesario para la implementación de SDN, se realiza la fase 3 la cual tiene como objetivo realizar las adecuaciones y reestructuraciones a la red actual, también realizar propuestas económicas y operativas de los requerimientos para cumplir la meta de la implementación de SDN, si las propuestas son aceptadas y se adquieren lo necesario se procede a realizar las actividades de la fase 2, si el caso por cuestiones técnicas y presupuestales no se cuenta con lo necesario para realizar la arquitectura de SDN, se procederá a realizar la fase 4, en la cual se optimizará los recursos y la infraestructura actual para reestructurar el esquema y funcionamiento con el fin de resolver las problemáticas planteadas. Según sea el caso, implementar la arquitectura SDN o la optimización de la infraestructura actual, se probó en un sitio de bajo impacto definido por la organización en el caso de no tener uno definido se procederá a realizar la implementación de la solución de manera general.

Figura 3.1 *Procedimiento para el aprovechamiento de la infraestructura de red*

A continuación, se explica detalladamente cada una de las fases del procedimiento, para entender cada uno de los pasos a seguir, así como el resultado de cada una de ellas.

3.1 Análisis de la situación actual

El objetivo de esta fase es analizar de manera inicial la organización de los sitios de red, así como los recursos (equipamiento de red), así mismo tener un panorama de la situación con respecto a las solicitudes que han sido generadas en un intervalo de tiempo, para tener un punto de referencia al momento de evaluar la implementación de la solución propuesta (véase en figura 3.2).

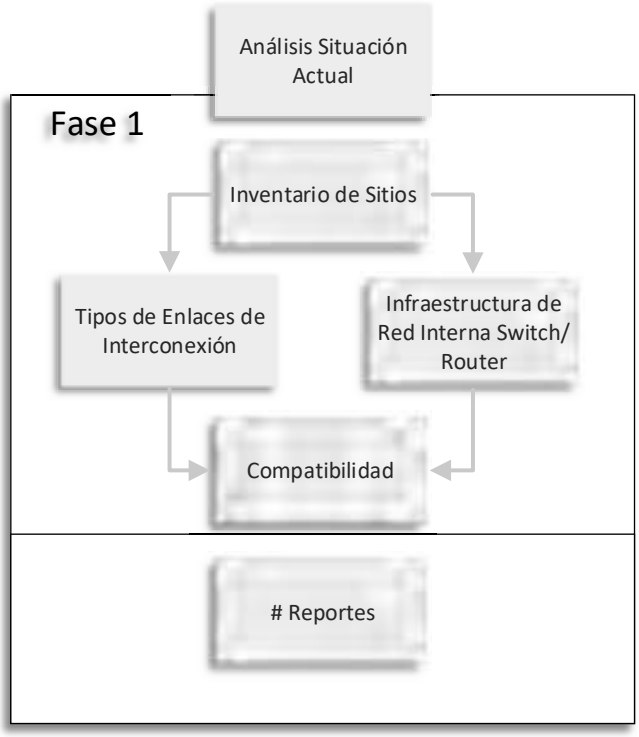


Figura 3.2 *Fase 1: Análisis de la situación actual.*

Fase 1: Análisis de la situación actual de la organización.

- Sitios de red: Definición de espacio físico (edificación/domicilio) donde se encuentra concentrado el equipamiento de red, tanto equipo de infraestructura como servidores.
- Enlaces de interconexión: Anchos de banda, proveedores, equipamiento y protocolos de ruteo, relacionados con los servicios de Internet o de red LAN de la organización, utilizados para la interconexión con uno o más sitios.

- Equipamiento de red: Equipamiento de infraestructura de telecomunicaciones y de servidores, involucrado directamente en las actividades del sitio en estudio.
- Compatibilidad: Revisión exhaustiva de cada uno de los equipos anteriormente mencionados, con el fin de verificar si cuentan con la posibilidad de utilizar el protocolo de OpenFlow, el cual es pieza importante para el desarrollo de la arquitectura de SDN.
- Solicitudes de servicios y/o correcciones: Se refiere a la cantidad de eventos registrados que implicaron alguna modificación en el equipamiento de red, lo cual puede ser capturado en un sistema especializado para HelpDesk o bien hoja de cálculo o cualquier método que utilice la organización para el registro de reportes de fallas o solicitudes de servicios, correspondientes al área de redes de telecomunicaciones.

Productos esperados al finalizar la fase:

- Base de Datos de sitios
    - Dirección/Domicilio
    - Cantidad de usuarios concurrentes
    - Cantidad de enlaces de interconexiones
    - Anchos de banda de los enlaces
    - Equipamiento de infraestructura de red asociado
- Base de Datos de Equipamiento
    - Tipo de equipo (Router/Switch/Punto de Acceso)
    - Marca
    - Modelo
    - Propósito de uso
    - Cantidad de usuarios a los que brinda servicio
    - Subnet/Vlan (Direccionamiento y propósito)

3.2 Solución y Pruebas de SDN

En esta fase se realizará el estudio a fondo sobre las diferentes plataformas disponibles para realizar una arquitectura de SDN, así mismo se trabaja a detalle por separado en las siguientes áreas que le compete al tema de SDN: Controlador, Seguridad, Virtualización y Aplicativos, lo anterior con el fin de tener el dominio del tema y la selección de herramientas que más se adecuan a las necesidades de la organización como se puede observar en la figura 3.3.

Se realizará la simulación mediante software para comprender el funcionamiento de la arquitectura y realizar los ajustes que sean necesarios para trasladarlo a un ambiente de pruebas real, antes de una implementación de producción.

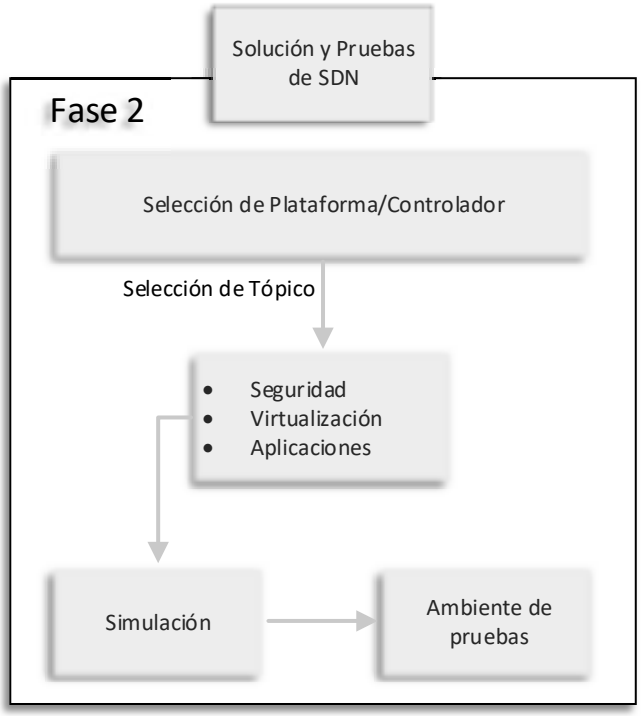


Figura 3.3 *Fase 2: Solución y Pruebas de SDN*

Fase 2: Solución y Pruebas de SDN:

- Selección de plataforma de SDN: Se refiere de elegir la plataforma de SDN a utilizar, basándose en los estudios previos y literatura, dependiendo del objetivo que se quiere alcanzar con la implementación de SDN.
- Tópico a desarrollar: Se tiene que seleccionar uno o más de los propósitos para los que se utilizará SDN.
- Simulación: Utilizar una plataforma de simulación (software) seleccionada después de la investigación literaria y probar el esquema propuesto, tratando de aproximar lo más posible el ambiente a la realidad. Se recomienda la utilización de la plataforma de simulación de redes GNS3, ya que permite crear ambientes con distintos controladores de SDN, como se muestran en las figuras 3.4,3.5 y 3.6.

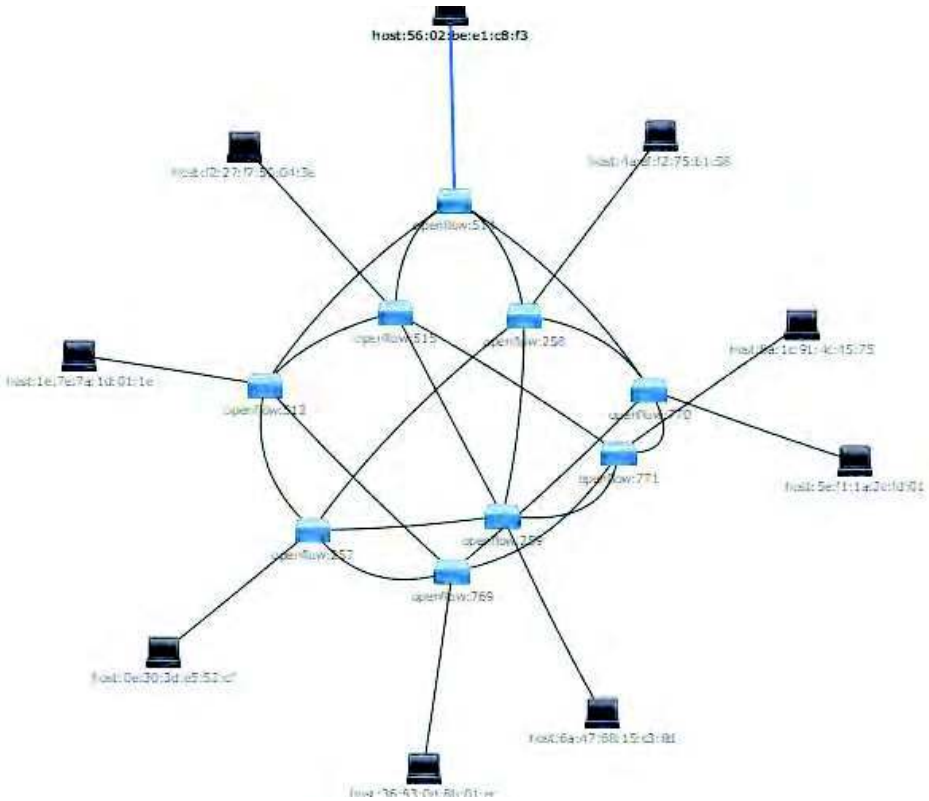


Figura 3.4 *Simulación utilizando OpenDaylight* (Gns3.com, 2017)

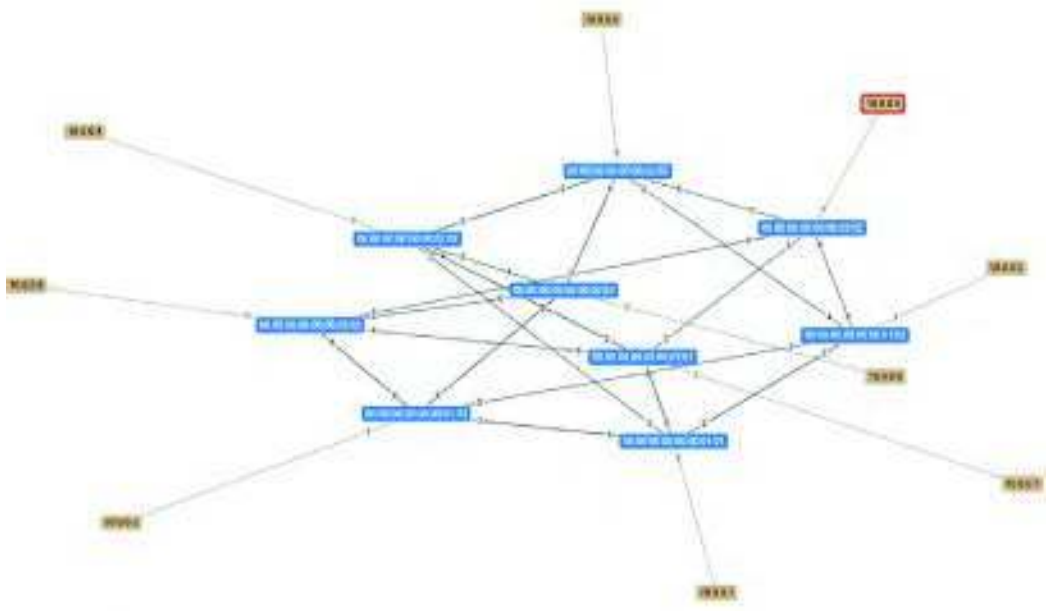


Figura 3.5 *Simulación utilizando HP VAN* (Gns3.com, 2017)

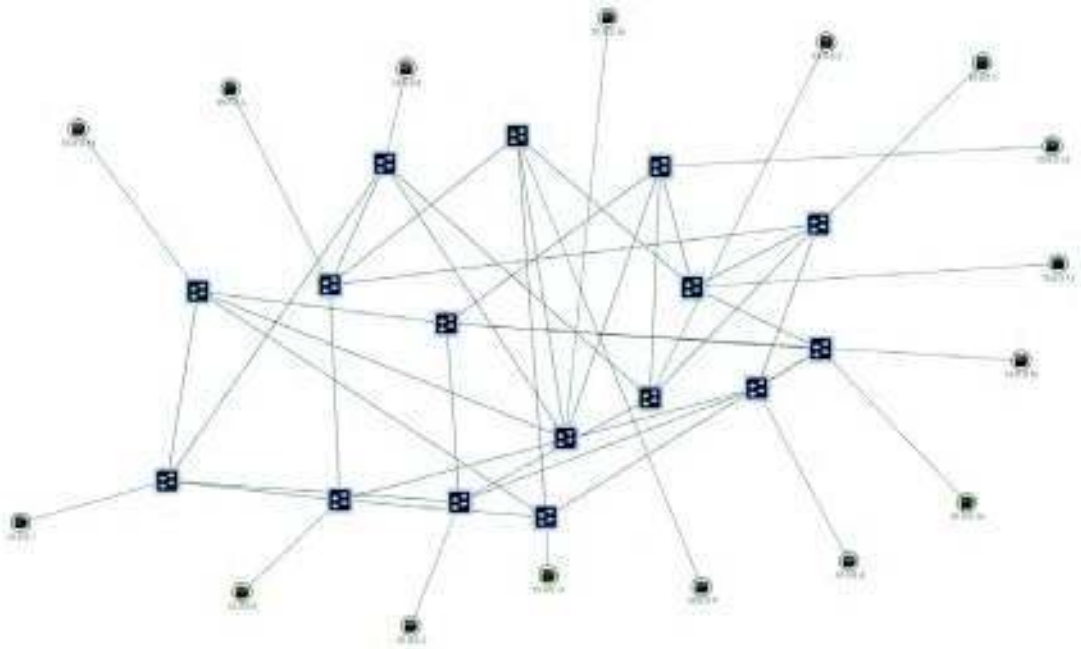


Figura 3.6 *Simulación utilizando ONOS* (Gns3.com, 2017)

- Ambiente de pruebas: Realizar pruebas de laboratorio con el equipamiento (modelos y marcas) de la organización, a partir del modelo resultante de la simulación.

Productos esperados al finalizar la fase:

- Comparativo y selección de plataforma de SDN a utilizar.
- Criterios para realizar la propuesta:
    - Selección de controlador y protocolos de conexión
    - Definición de aplicaciones para aplicar calidad de servicio
    - Definir herramientas o complementos de seguridad para fortalecer la arquitectura centralizada propuesta
- Reporte de datos generado con el software de simulación para ver el ambiente real y la nueva arquitectura (latencia/Ruteo dinámico).
- Reporte en ambiente de pruebas con infraestructura de equipo activo.

3.3 Estudio Económico y Requerimientos

Esta fase es presentar el panorama de la situación actual a la Dirección, mediante diagramas y propuestas de mejora utilizando la infraestructura existente. También se realizará una propuesta económica en el caso de requerir equipamiento o servicios nuevos para la optimización de la red lo cual sea compatible con una arquitectura SDN o HDN.

Figura 3.7 *Fase 3: Estudio Económico/Requerimientos*

Fase 3: Estudios económicos y de requerimientos técnicos para una implementación de SDN u optimizar la arquitectura existente.

- Diseños y diagramas: Análisis de la situación actual con respecto a la topología de red y el rediseño si es necesario para adecuarlo a la arquitectura de SDN.
- Definición de requerimientos: Se refiere a los cambios de topologías, equipamiento, servicios de interconexión, necesarios para la mejora y optimización de la red actual. Dependiendo el equipamiento que se requiera, como, por ejemplo: equipos de Telefonía IP, switches, puntos de acceso inalámbrico, entre otros. Se puede utilizar una compañía que se dedica evaluar equipamiento de tecnología como lo es Gartner. A continuación, se muestra la representación gráfica de la evaluación en la figura 3.8:

Figura 3.8 *Cuadrante de Gartner de Firewall tipo empresarial* (gartner.com, 2017)

- Costo económico y operativos: Se describen los aspectos monetarios y de labores extraordinarias, definidas en el punto anterior (requerimientos).
- Adquisición de equipamientos y servicios: se refiere a la adquisición de los equipos y servicios propuestos para el desarrollo de una implementación de SDN.
- Definición de prioridad de los sitios: Análisis de cada uno de los sitios con respecto a la cantidad de personas involucradas, así como las actividades que realizan con el fin de definir prioridad y niveles entre los sitios, para conocer el impacto en el caso de realizar una implementación donde no se obtengan los resultados esperados y se requiera un rediseño y ajustes.

Productos esperados al finalizar la fase:

- Rediseño de arquitectura de red (Diagramas/Ruta crítica):
  - Definición y organización de direccionamiento IP (información confidencial para la empresa)
  - Definición de requerimientos de equipamiento para cada oficina con respecto a los servicios y usuarios concurrentes (dimensionamiento del hardware/equipamiento de infraestructura que soporte la demanda de usuarios)
  - Definición de anchos de banda por oficina con respecto a la demanda de usuarios y las actividades del sitio en estudio.
- Reporte Económico de gastos generados por los cambios de arquitectura y equipamiento necesarios para optimizar los servicios (Cotizaciones/tablas comparativas/anexos).
- Definición de prioridad/impacto de cada sitio con relación de la cantidad de usuarios y la carga de trabajo.

3.4 Optimización de Infraestructura Existente

El objetivo de esta fase es realizar una propuesta de optimización de recursos y equipamiento actual. En caso de que no se tenga lo necesario para efectuar un proyecto de arquitectura de SDN, se puede realizar una reestructura tomando los problemas de más impacto, para después simular una solución que pueda ser implementada en un ambiente real.

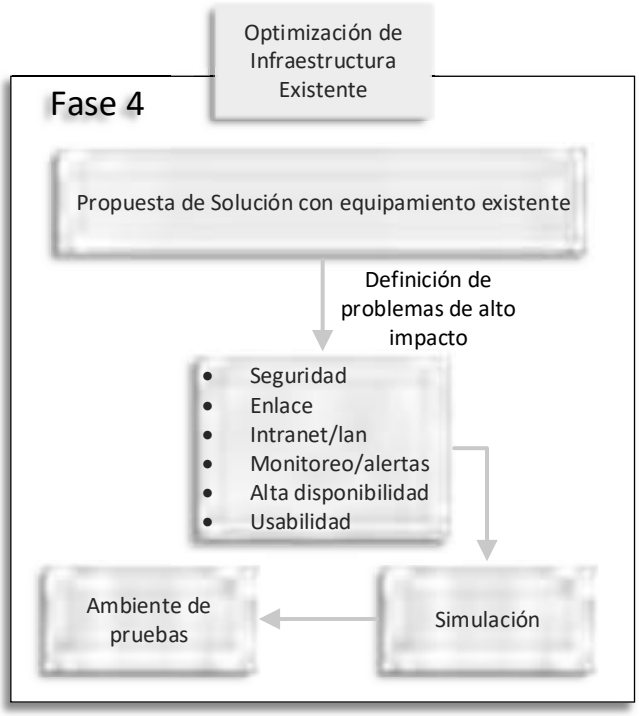


Figura 3.9 *Fase 4: Optimización de Infraestructura Existente*

Fase 4: Optimización de infraestructura existente:

- Propuesta de solución: Se refiere a la verificación a detalle del equipo existente, para investigar sus funcionalidades y recursos que sean capaces para de resolver los problemas planteados y así tener una solución integral con el objetivo de automatizar las operaciones de la red de telecomunicaciones.
- Definición de problemas de alto Impacto: Es identificar las problemáticas que se puedan clasificar en los tópicos descritos, ya que cada uno de ellos pertenece a funcionalidades específicas de un tipo de equipamiento de red.
- Simulación: Utilizar una plataforma de simulación (software) seleccionada después de la investigación literaria y probar el esquema seleccionado, tratando de aproximar lo más posible el ambiente a la realidad.
- Ambiente de pruebas: Realizar pruebas de laboratorio con el equipamiento (modelos y marcas) de la organización, a partir del modelo resultante de la simulación.

3.5 Implementación de solución y verificación de resultados

El objetivo de esta fase es poner en marcha la solución propuesta y poder verificar el funcionamiento, para realizar los ajustes en el caso de ser necesario. También tienen como objetivo validar si la solución propuesta, mejoró la problemática planteada y en qué nivel fue la mejora.

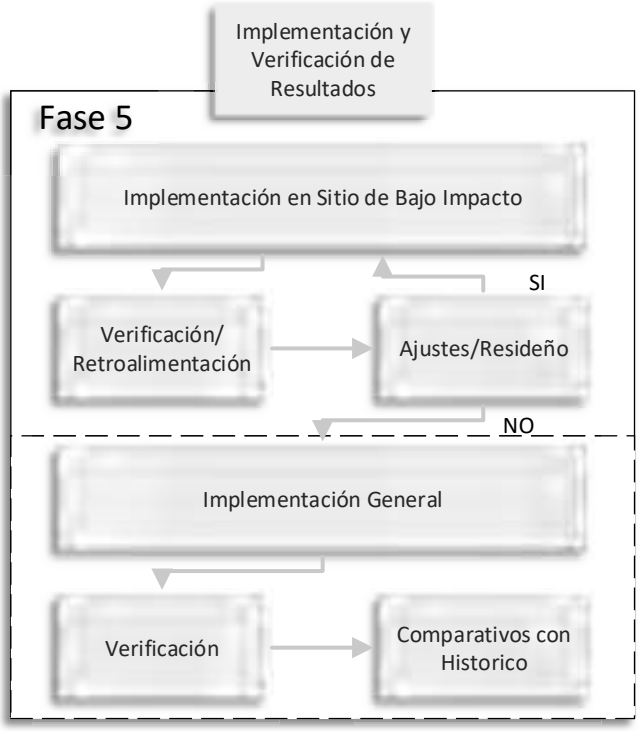


Figura 3.10 *Fase 5: Implementación y Verificación Resultados*

Fase 5: Implementación y verificación de resultados:

- Sitio de bajo impacto: Se refiere a las pruebas físicas, previas a realizarlas en un ambiente real, las cuales son ejecutadas en un sitio de bajo impacto, para tomar en cuenta todas las variables que puedan surgir y comprobar el comportamiento de nuestra propuesta.
- Verificación y retroalimentación: Comprobar si la implementación no realizo una afectación negativa o bien si se puede realizar mejoras al modelo.

- Ajuste y rediseño: Se refiere a realizar los ajustes, resultantes de la verificación y comprobarlo de nuevo dentro en el ambiente real.
- Implementación general: Implementar el modelo resultante de las pruebas en el sitio de bajo impacto.
- Verificación: Recolectar la información del modelo implementado.
- Comparativo: Realizar un comparativo de los resultados y el número de solicitudes de servicio, así como los eventos anómalos presentados con respecto al histórico previo a la implementación.

4 IMPLEMENTACIÓN

En este capítulo se presenta el desarrollo y la implementación del procedimiento propuesto en el capítulo anterior, el cual fue aplicado en la Dirección de Sistemas de la Procuraduría General de Justicia del Estado.

A continuación, se detallan las actividades que se realizaron en cada una de las fases que componen el procedimiento para el aprovechamiento de la infraestructura de red de la organización.

4.1 Análisis de la situación actual de la organización

En esta fase inicial de la implementación, se realiza un estudio a fondo de la situación actual de la organización, pero desde una perspectiva técnica y de funcionalidad de su esquema de red, con el fin de optimizar lo existente o realizar una reestructuración general de toda la infraestructura.

4.1.1 Inventario de sitios

Al realizar el estudio de los sitios se decidió trabajar en un total de 56 unidades administrativas distribuidas a lo largo de Estado de Sonora en un total de 24 municipios, ya que son las que cuentan con un equipamiento similar y se podría realizar una configuración estándar para cada una de ellas, las cuales tienen servicios y funciones diferentes dependiendo el tipo de unidad administrativa, las cuales se enlistan a continuación:

- Agencia adscrita al juzgado mixto
- Agencia adscrita al juzgado primero de lo penal
- Agencia adscrita al juzgado segundo de lo penal
- Agencia adscrita al juzgado tercero de lo penal
- Agencia especializada en delitos
- Agencia especializada en delitos de abigeatos
- Agencia especializada en delitos de querella y tránsito

- Agencia especializada en procuración de justicia para adolecentes
- Agencia Investigadora del Ministerio Público
- Agencia Investigadora del Ministerio Público especializada en delitos sexuales
- Agencia Investigadora del Ministerio Público Sector I
- Agencia Investigadora del Ministerio Público Sector II
- Agencia Mixta
- Agencia primera del Ministerio Público especializada en delitos ocasionado por el tránsito de vehículos
- Delegación regional
- Centro de atención temprana
- Centro integral de procuración de justicia

La mayoría de los tipos de unidades administrativos anteriormente mencionadas comparten una función en común, lo cual es realizar una replicar de la información capturada resultantes de las actividades propias de la unidad administrativa.

4.1.2 Tipos de enlaces de interconexión de las unidades administrativas

Los enlaces de interconexión hacen referencia a como una unidad administrativa accede al centro de operaciones de red (COR) ubicado en el edificio de la PGJE, al realizar la investigación se identificaron tipos de enlaces, proveedores y anchos de bandas, así mismo se identificó un enlace otorgado por el centro de control, comando, comunicación y cómputo (C4) el cual simula una interconexión LAN en una escala Estatal. A continuación, se describen todas las variaciones de conexión que se presentaron entre una UA y el COR:

- Tipos y anchos de banda de los enlaces
    - Simétricos de 20 Mbps, 50 Mbps y 100 Mbps
    - Asimétricos de 1 Mbps, 2 Mbps, 5 Mbps, 10 Mbps y 100 Mbps
- Proveedores
    - ISP Iusacel (Enlace TP)

- ISP Megacable (Metrocarrier)
- ISP Telmex
- C4 (gubernamental)

Los enlaces de ISP que son utilizados para realizar conexiones directas a los servidores tanto de sistemas informáticos como los de bases de datos, son realizados mediante una conexión segura de una red privada virtual VPN (virtual private network) véase en la figura 4.1, en los casos de C4 es una conexión directa, ya que los servicios prioritarios de la organización no son visibles desde el ámbito público (Internet) véase en figura 4.2.

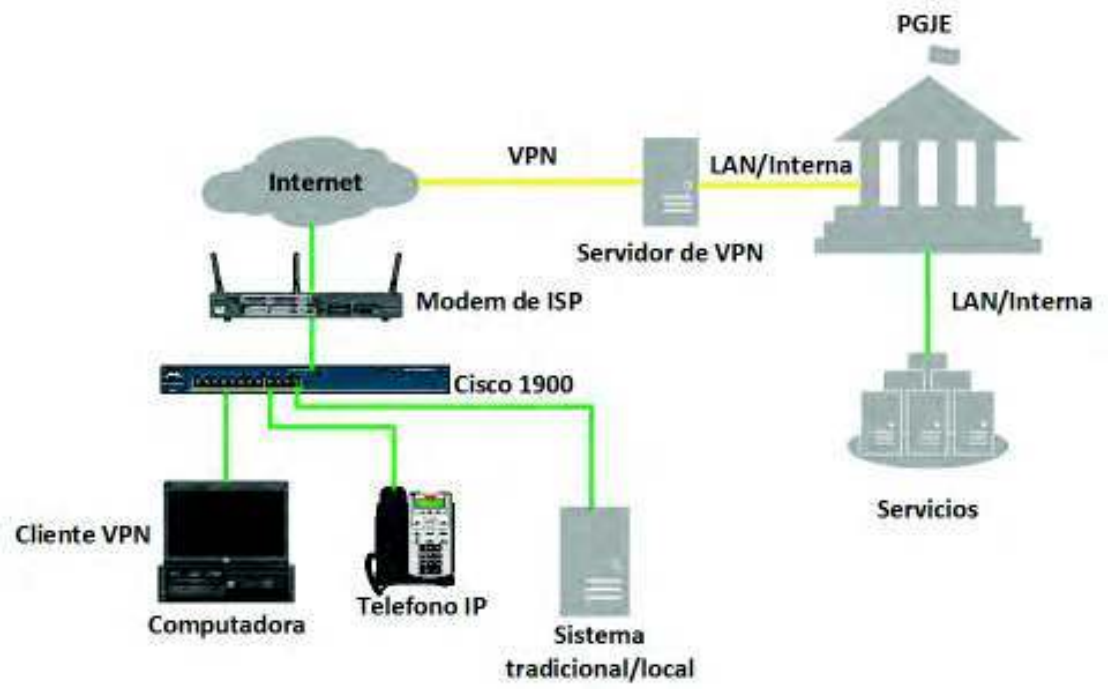


Figura 4.1 *Unidad Administrativa conectada por VPN*

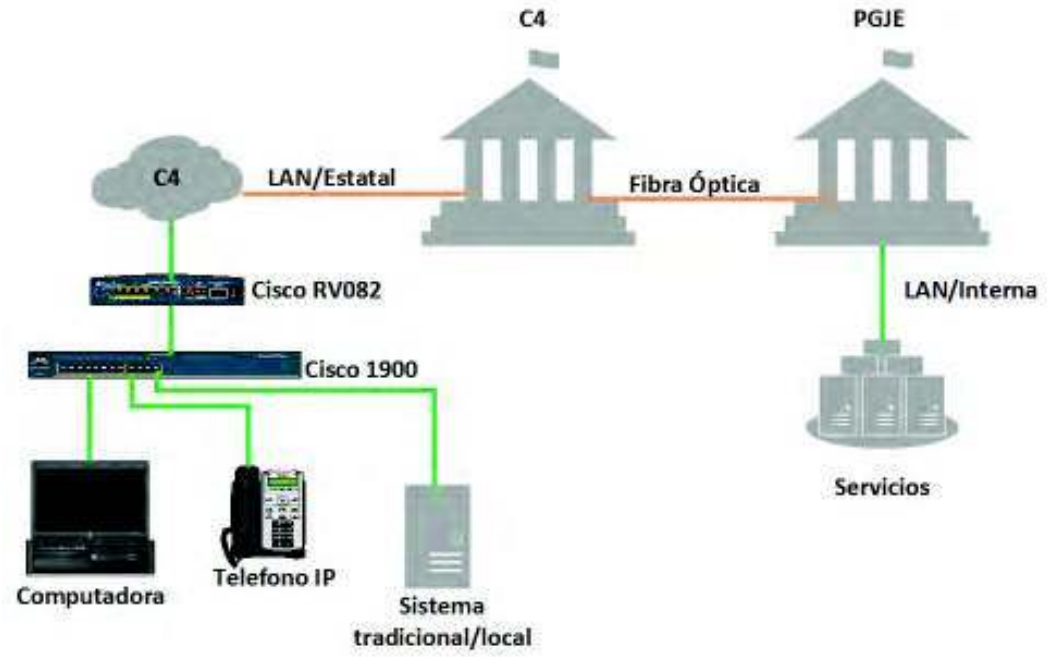


Figura 4.2 *Unidad Administrativa conectada a la PGJE mediante C4*

4.1.3 Inventario de infraestructura de red interna

Se realizó un inventario del equipamiento involucrado en la infraestructura de red, donde se dividió en el equipamiento instalado del COR ubicado en la PGJE y por cada unidad administrativa. Se encontró que en las unidades administrativas contaban con un equipo router cisco RV082 y un switch cisco catalyst 1900, este último solo está en las UA que la población de usuarios concurrentes es mayor a 7, ya que sobrepasa la capacidad de interfaces ethernet disponibles en el cisco RV082 véase a detalles y por UA en el anexo 1. Por otro lado, con respecto al equipamiento instalado dentro de la PGJE, existe una serie de equipamiento cisco, 3com, mikrotik, entre otros, los cuales en su mayoría es obsoleto. También se tiene un equipamiento de red de alto nivel de otros proyectos de las marcas: HPE y Fortinet, el cual no está en operación por falta de configuración y un proyecto para darle una funcionalidad.

4.1.4 Compatibilidad para implementación SDN

Basados en la literatura y con el propósito de utilizar una arquitectura innovadora y más automatizada, se buscó la implementación de una solución en una plataforma de

SDN tanto en el plano de control, así como en la parte de desarrollo de aplicativos específicos, por lo que, a partir del inventario del equipamiento de la infraestructura de red, se investigó en las hojas de especificaciones de cada uno para saber si contaban con la funcionalidad del protocolo de OpenFlow, por lo que el resultado fue poco favorable, ya solo 2 equipos soportan en su totalidad lo que es OpenFlow, en este caso fueron 2 switches HPE FlexNetwork 7500 series que soportan OpenFlow versión 1.3 (Hpe.com, 2016). Por lo anterior y falta de recursos en equipamiento y económicos, se decidió realizar una optimización de los recursos actuales tanto financieros como del equipamiento de la organización y así resolver los problemas ya planteados, descartando la posibilidad de desarrollar una arquitectura de SDN.

4.1.5 Solicitudes de servicios o reportes de fallas

Actualmente la organización tiene personal para la atención de usuarios con respecto a reportes de fallas o solicitudes de servicios, se identificó que, en el área de soporte técnico la cual se encarga de ver el buen funcionamiento del equipo de cómputo existente o bien la instalación de equipo nuevo según sea el caso, se cuenta con un sistema para la captura de las llamadas recibidas por parte de los usuarios (empleados de la organización) sobre solicitudes de servicios o reporte de fallas. Por otro lado, el área de redes y telecomunicaciones no cuentan con un sistema para el seguimiento de los reportes de fallas o solicitudes de servicios, por lo que se le recomendó utilizar el mismo sistema que es utilizado por el área de soporte técnico. Por otro lado, se identificó que un gran número de órdenes de servicio no son cuantificables de manera inmediata, ya que las realizan de manera formal por oficio (Anexo 01) y la respuesta o atención se hace de igual forma por oficio, por lo que solo se tiene una evidencia física no clasificada de las solicitudes o reportes para un servicio, tanto del área de redes y se soporte técnico.

4.2 Solución y pruebas de SDN

Como se mencionó después de realizar el estudio de compatibilidad donde el resultado fue negativo a la implementación de una arquitectura de SDN, las características y funcionalidades del equipamiento de red utilizados por la organización no cumplen el requerimiento mínimo que es el protocolo OpenFlow, por lo anterior se decide estudiar a fondo las funcionalidades del equipamiento actual para su optimización y así dar solución a las problemáticas presentadas. Existe equipamiento adquirido para seguridad perimetral y ruteo de la marca Fortinet, el cual para la parte de controlador inalámbrico utiliza el protocolo CAPWAP el cual propone la gestión centralizada de múltiples puntos de acceso inalámbricos (AP) (Elsadek y Mikhail, 2016) y es soportado por un controlador SDN OpenDayLight (Opendaylight.org, 2016), este último es uno de los controladores más conocidos para una solución de SDN, cuando se desea realizar una solución de código abierto y sin un costo económico.

4.3 Estudio económico, diseño y requerimientos

En esta fase de implementación una vez determinado la incompatibilidad del equipamiento para una arquitectura de SDN que resuelva las problemáticas planteadas, se desarrolla un plan secundario el cual se refiere a la optimización de los recursos para explotar las funcionalidades que apoyen a la solución de las problemáticas y así mismo a la automatización de las operaciones de red, en los tópicos de: arquitectura de alta disponibilidad, interconectividad redundantes, administración de anchos de banda y automatización de procesos de red. Por lo anterior se realizaron una serie tareas y operaciones desde técnicas a económicas, las cuales son presentadas a continuación.

4.3.1 Diagrama y reestructuración de red

Al realizar el trabajo de análisis de los sitios tanto de las UA como el COR de la PGJE, se decidió hacer una propuesta de reestructuración con el fin de solventar las problemáticas planteadas, por lo que inicialmente se hizo un diagrama de la situación actual (figura 4.3) donde se puede observar falta de redundancia de interconexión, así como de un esquema de tolerancia a fallos en el equipamiento de infraestructura.

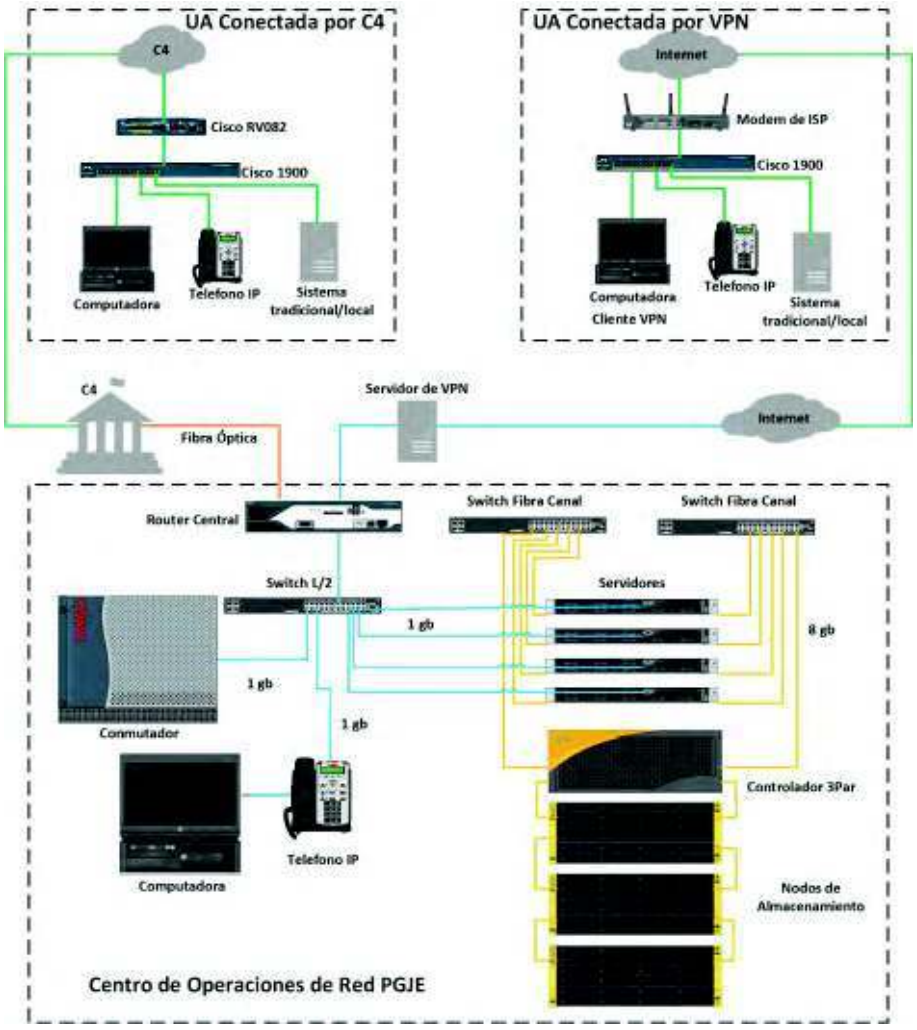


Figura 4.3 *Diagrama de red actual de la organización*

Como anteriormente se mencionó en la parte de inventario de equipo, la organización cuenta con equipamiento nuevo y que aún no está en operación como lo son los HPE Flexfabric 7503 y equipos Fortigate, así mismo se recomendó a la organización la adquisición de servicios de Internet en las diferentes UA con el fin de contar con redundancia de enlace, al tener la posibilidad de utilizar la VPN por un ISP y la conexión LAN/Estatal mediante C4, logrando un esquema de alta disponibilidad en los enlaces como se puede observar en la figura 4.4.

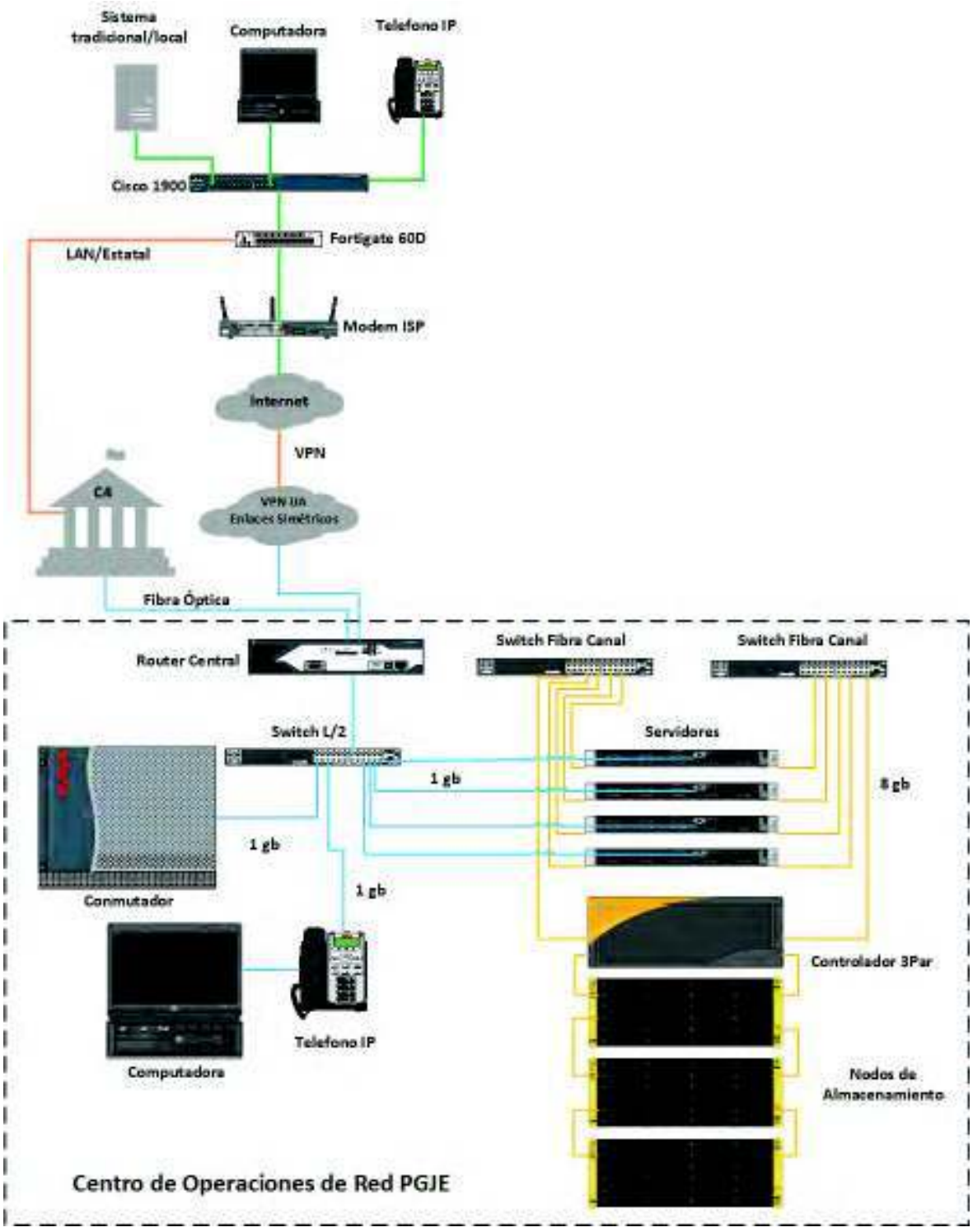


Figura 4.4 *Diagrama de red propuesto para la interconexión entre UA y COR*

4.3.2 Definición de requerimientos

Una vez realizado el diagrama propuesto para la organización, se crea un listado de requerimientos técnicos y de equipamiento para lograr dicha implementación, así mismo nuevamente se revisa el equipamiento con el que ya se cuenta para así pedir solo lo mínimo necesario, como se muestran en la tabla 4.1.

Cantidad	Equipo	Descripción
2	FG100D	Firewall central en alta disponibilidad
6	FG60D	Firewall de UA
35	FG50E	Firewall de UA
1	FG30E	Firewall de UA
6	DL360 G9	Servidores central en cluster
1	Exp 3PAR	Expansión de sistema de almacenamiento
15	FS448D	Switch para equipamiento de frontera
8	FAP221C	Punto de acceso inalámbrico para edificio central
6	Licencias	Licenciamiento de Windows Server
38	Enlace	Enlaces de Internet
4	Enlace PTP	Enlaces inalámbricos punto a punto
1	FMG400D	Consola de administración para firewall
1	FAZ400D	Servidor de recolección de información de firewall

Tabla 4.1 *Requerimientos mínimos para realizar la arquitectura propuesta*

Lo anterior es resultado de un comparativo mínimo de 3 marcas por tipo de equipamiento, utilizando varios criterios: costo, usabilidad, operatividad, funcionalidad y que cumpliera con lo necesario para el desarrollo de la arquitectura propuesta. Con respecto a los equipos de seguridad/router se eligió sobre 3 de las marcas más conocida: Palo Alto Networks, Check Point Software Technologies y Fortinet, resultado del estudio “Magic Quadrant for Enterprise Network Firewalls” publicado el 25 de mayo de 2016 (gartner.com, 2017), por cuestiones de presupuesto y facilidad de adquisición se eligió al fabricante Fortinet, aunque los 3 cumplían con los requisitos planteados de la nueva arquitectura propuesta. Por otro lado, en la parte de consola de administración, recolector de información del firewall, switches y puntos de acceso inalámbricos se optó por elegir al mismo fabricante, ya que se puede tener una solución integral y ofrece funcionalidades propietarias, para ambientes donde se usa equipamiento de la misma marca, así como una administración centralizada. El equipo

mencionado fue adquirido mediante la gestión de recursos Estatales y Federales, así como convenios con el gobierno de Estados Unidos, así mismo se realizó anexos técnicos del equipamiento como requisito para la publicación de las partidas de licitación.

Con respecto a los enlaces de Internet y con asesoría de los mismo proveedores de Internet, en este caso Telmex, Metrocarrier y Enlace TP, tomando en cuenta la cantidad de usuarios en Unidades Administrativas, se solicitaron enlaces desde 5 mb/s a 20 mb/s, con al menos una IP fija, solo en el COR de la PGJE se cuentan con al menos 2 enlaces de 100 mb/s, dedicados para realizar la interconexión con la UA, por otro lado también en el edificio mencionado se cuenta con una serie de enlaces asimétricos de 20 mb/s con el propósito de ser utilizado para la navegación de Internet de los usuarios.

4.3.3 Selección de sitio de bajo impacto

La definición de sitios fue a criterio de la organización utilizando las siguientes variables: población de usuarios, cantidad de información o casos capturados en promedio, tipo de agencia o delitos. Por lo anterior se eligió a la agencia ubicada dentro del Hospital General del Estado, ya que se solo captura casos de las personas que ingresan al hospital, por lo que fue el sitio autorizado por la organización para realizar la instalación inicial y así poder estar monitoreando para hacer los ajustes y modificaciones en la configuración en el caso de ser necesarios, así mismo, otro de los motivos de la selección del sitio mencionado, fue porque se encuentra en la misma ciudad sede donde se está trabajando de manera presencial lo que facilitaría en el caso de tener que trasladarse a la UA.

4.4 Optimización de infraestructura existente

Si nos encontramos en esta etapa, es porque no contamos con lo necesario para la realización de un proyecto de SDN. Por lo anterior se realiza la optimización del equipamiento actual y en el caso de haberlo adquirido y que no fue compatible con SDN, se quiere explotar las funcionalidades del equipamiento actual y el nuevo con el fin de automatizar los procesos de red, en este caso que resuelva y/o mejore la interconexión entre las UA´s y el COR, así como también mejorar una serie de aspectos de la red interna de cada UA y el COR.

4.4.1 Propuesta de solución con equipamiento existente

En esta etapa de la fase 4 y al no contar con lo necesario para la implementación de SDN, se realiza un estudio a fondo de los equipos descritos en el inventario de equipamiento de la organización, para ver las funcionalidades y características que se pueden explotar de los mismos, nos apoyamos en las hojas técnicas de cada uno, así como en la documentación de manuales de configuración y de esquemas propuestos por cada uno de los fabricantes. Lo anterior está asociado al equipamiento, por el lado de la organización se observan los problemas de alto impacto de los siguientes temas según sean las necesidades y problemáticas a resolver en la organización:

- Seguridad: Se refiere con respectos de políticas de acceso de firewall, las cuales protegen la red interna y equipamiento. En el caso particular de la organización bajo estudio, se aumentará la protección a los servidores internos, así como la protección de los usuarios con respecto a ataques desde Internet.
- Enlaces: En este punto se estudia los enlaces de interconexión entre oficinas, en este caso entre las UA y el COR, pero también se realiza un estudio con respecto a la necesidad de navegación de Internet de la organización. Por lo que generalizando en cualquier organización se tomaría en cuenta optimizar los anchos de banda de Internet y de enlaces de interconexión según sea el caso.
- Intranet/LAN: Se realiza un inventario de la segmentación de red interna de la organización, nos referimos al direccionamiento interno y el propósito del

mismo. Por ejemplo, creación de redes exclusivas para servidores, equipamiento de infraestructura de red (router, switch, conmutadores), equipos para video vigilancia, por mencionar algunos. También dicha segmentación nos ayudaría al momento de estar realizando las políticas de seguridad, así como facilitar la administración y control a los administradores de la red.

- Monitoreo/alertas: Se refiere a desarrollar mecanismos de monitoreo de red, los cuales pueden estar asociados a software especializado para dicho propósito o bien también a rutinas o nuevos esquemas de administración del personal quien administra la red.
- Alta disponibilidad: En esta etapa según sea el giro de la organización y las prioridades de los procesos internos de la misma, se realizan esquemas de alta disponibilidad, los cuales pueden ser en servicios, equipamiento de infraestructura y servidores; en el mejor de los casos si la organización tiene actividades criticas de alto impacto o manejo de información sensible, se puede plantear la implementación de un sitio alterno en el caso de una eventualidad que tenga grandes afectaciones del COR de la organización, tener un sitio donde se esté replicando la información y tener todo lo necesario para mantener en funcionamiento las actividades prioritarias de organización.
- Usabilidad: Este punto impacta directamente a la administración y control de la red, así mismo se tiene un impacto positivo a la percepción del usuario final, quien es el que utiliza la infraestructura de red. Aquí se refiere en crear procesos automatizados que ayuden a administrar de una forma más eficiente la red, por lo que este punto está ligado a todos los demás, así mismo como es un apoyo directo a los administradores de red, tiene como resultado disminuir el tiempo de respuesta para la resolución de problemas en la red.

Al terminar de definir cada uno de los puntos anteriores y visualizando las problemáticas y el diagrama de reestructuración de red anteriormente propuesto en la Fase 3, se tiene un ajuste y nueva propuesta de arquitectura de red como se muestra en la figura 4.5.

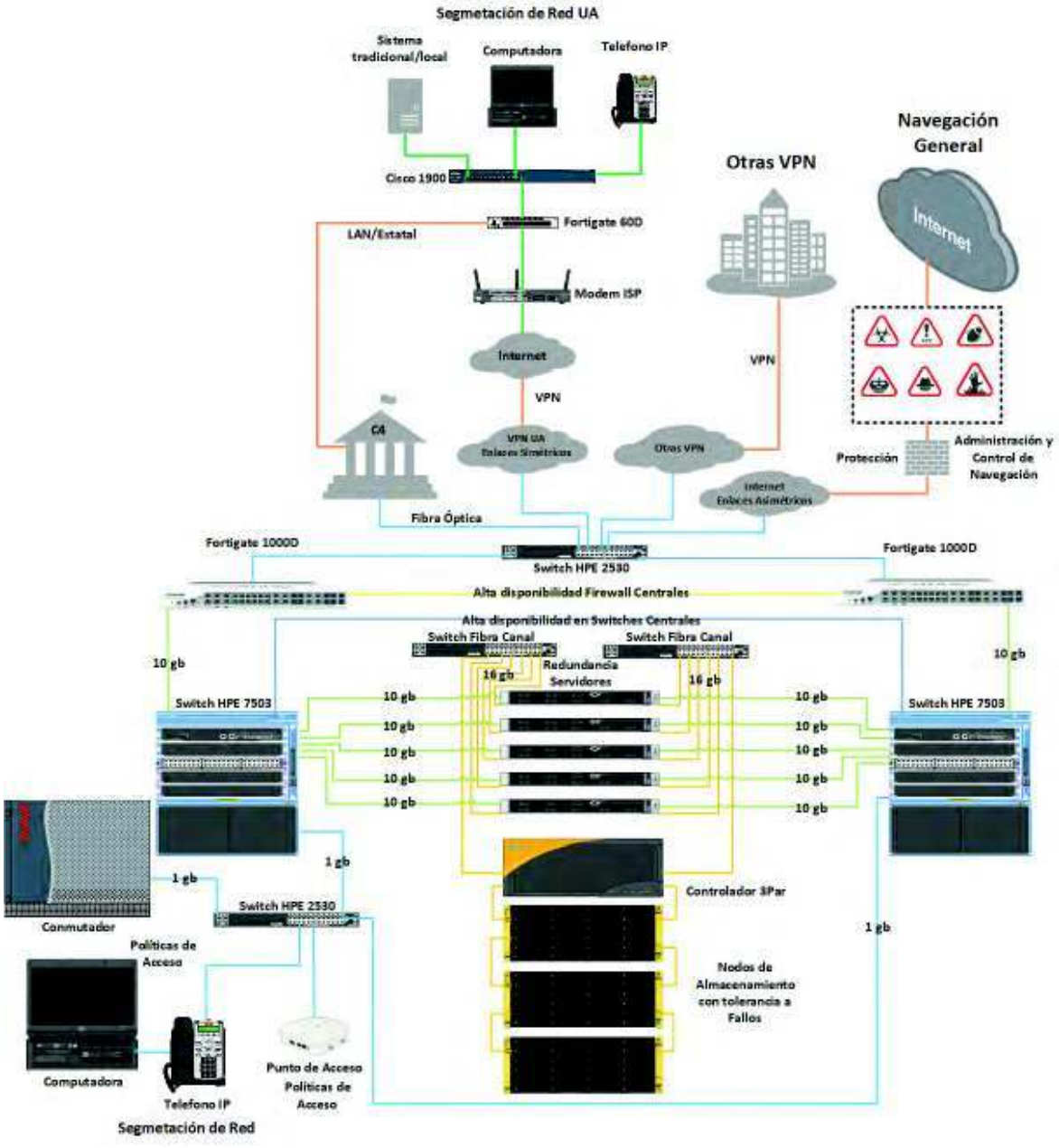


Figura 4.5 *Nueva propuesta de arquitectura de red optimizada*

4.5 Implementación de solución y verificación

En esta etapa nos encontramos con una arquitectura propuesta ya validada, según sea el caso el cual puede ser implementación de SDN o bien la optimización de la infraestructura actual, cualesquiera de las dos situaciones mencionadas comenzarán con el proceso de ajustes y modificaciones en el caso de ser requerido, así como la fase de pruebas en el sitio descrito de bajo impacto, para posteriormente realizar la instalación general en todos los sitios (Unidades Administrativas), que fueron delimitadas en el proyecto.

4.5.1 Implementación en sitio de bajo impacto

Al contar con el equipamiento y servicios solicitados para la arquitectura mencionada, se procedió realizar la instalación en el sitio piloto conocido como de bajo impacto (Hospital General del Estado). La primera fase de dicha fase fue realizar la interconexión entre la UA y el edificio de la PGJE, por lo que aprovechando la conectividad que se obtuvo con el servicio contratado de enlace de Internet, se procedió a realizar una conexión de VPN punto a punto (Site to Site) entre los equipos los equipos Fortinet adquiridos como se muestra en la figura 4.6, lo cual es muy sencillo utilizando el asistente, como se muestra en la figura 4.7.

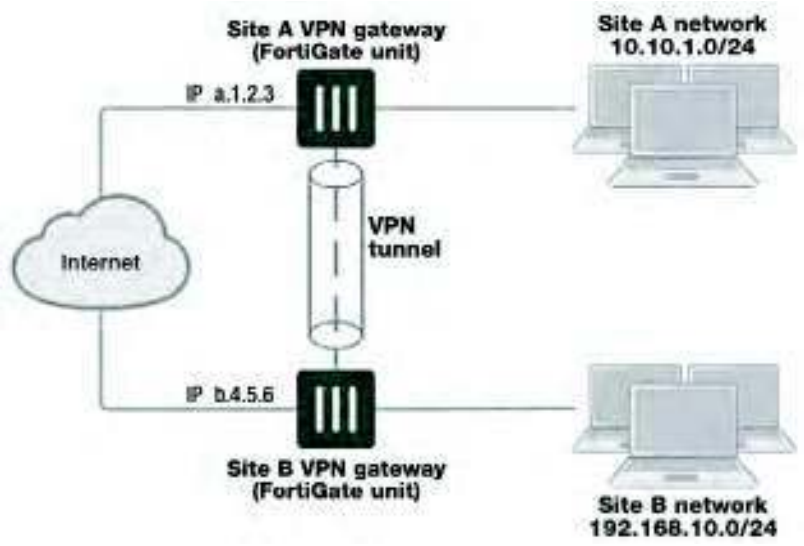


Figura 4.6 *VPN "site to site" entre equipos Fortigate*

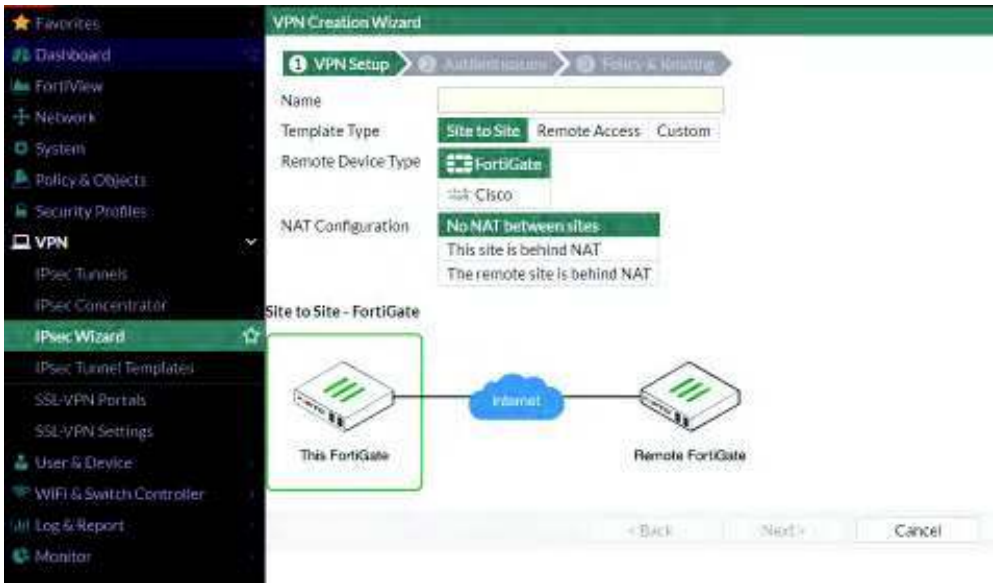


Figura 4.7 *Paso 1: creación de VPN sitio a sitio utilizando el asistente*

Como se puede observar en la figura 4.7, el primer paso para la creación del túnel de VPN consiste en otorgarle un nombre a dicho túnel, si se quiere utilizar una plantilla de configuración predeterminada por el equipo, así como el tipo de equipo con el que va a realizarle el túnel y por ultimo si va tener alguna configuración de NAT (Network Address Translation); lo anterior es para hacer una conexión trasparente entre los sitios pero al mismo tiempo realizando una conexión segura entre los mismo. En el paso 2 como se muestra en la figura 4.8, se determinar una serie de parámetros como la dirección IP del equipo remoto con el cual se va a conectar o bien esta la posibilidad de realizarlo por nombre, mediante un registro de DNS dinámico en el caso que en el sitio el proveedor de Internet no otorgue una dirección IP fija, en este caso se cuenta con un direccionamiento de IP fijo contratado, pero en la fase de monitoreo se observó que aún descrito en la contratación del servicio como IP fija, estaba cambiando y fue notificado a la brevedad con el proveedor de Internet, no se recibió una respuesta satisfactoria y por cuestiones de tiempo se decidió realizarlo con registro de nombre dinámico el cual es un servicio prestado por Fortinet por lo que no genera un costo adicional a la solución como se muestra en la figura 4.9; por último se selecciona la interface por donde está la conexión de Internet por donde se realizará la conexión de

VPN, así como si utilizaremos un clave compartida entre equipos para realizar la conexión o bien un certificado que autentifique la conexión entre los mismo.

Figura 4.8 *Paso 2 creación de VPN sitio a sitio utilizando el asistente*

Figura 4.9 *Servicio de DNS dinámico de Fortinet*

Al terminar lo anterior se puede realizar las ultimas configuraciones de la VPN, las cuales son requeridas en el paso 3 como se muestra en la figura 4.10, donde prácticamente son temas de ruteo y de políticas de firewall, para indicar cuales redes en cada uno de los sitios tendrán interacción a través del túnel de VPN. Por lo que como se puede observar en la figura mencionada, se tiene que elegir la interface de la red interna de la UA o bien de la misma Procuraduría, así como también el direccionamiento IP que estará permitido realizar intercambio de información tanto local como remoto.

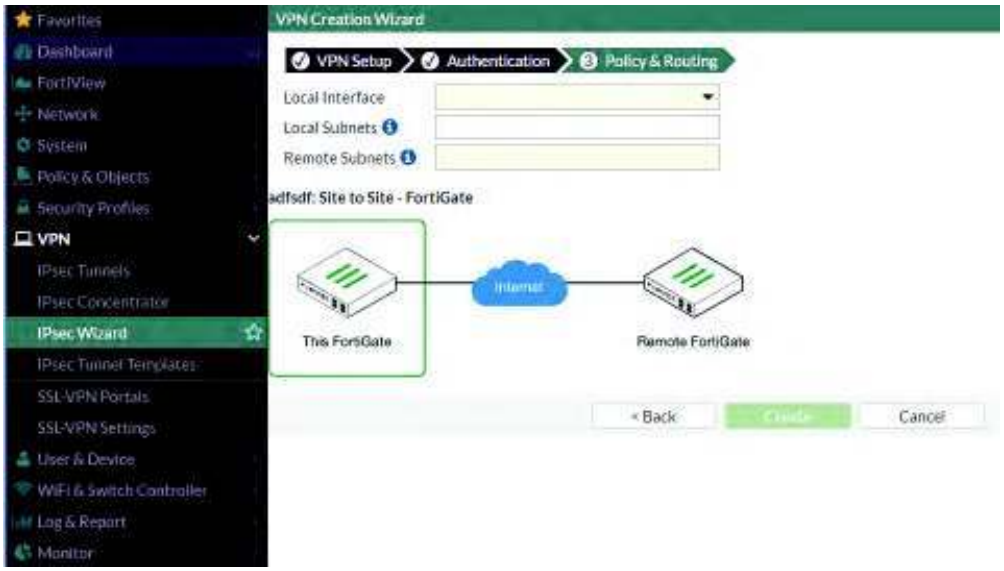


Figura 4.10 *Paso 3 creación de VPN sitio a sitio utilizando el asistente*

Una vez realizada el túnel de VPN, se realizan pruebas desde un equipo de cómputo de la UA verificando si cuentan con acceso a los sistemas correspondientes. Por otro lado, se realiza la ruta de enlace alterno por C4 utilizando ruteo estático y modificando lo que es la distancia administrativa lo cual indica cual es el enlace principal por donde se realizará la interconexión en la UA y el edificio de la Procuraduría, como se muestra en la figura 4.11.

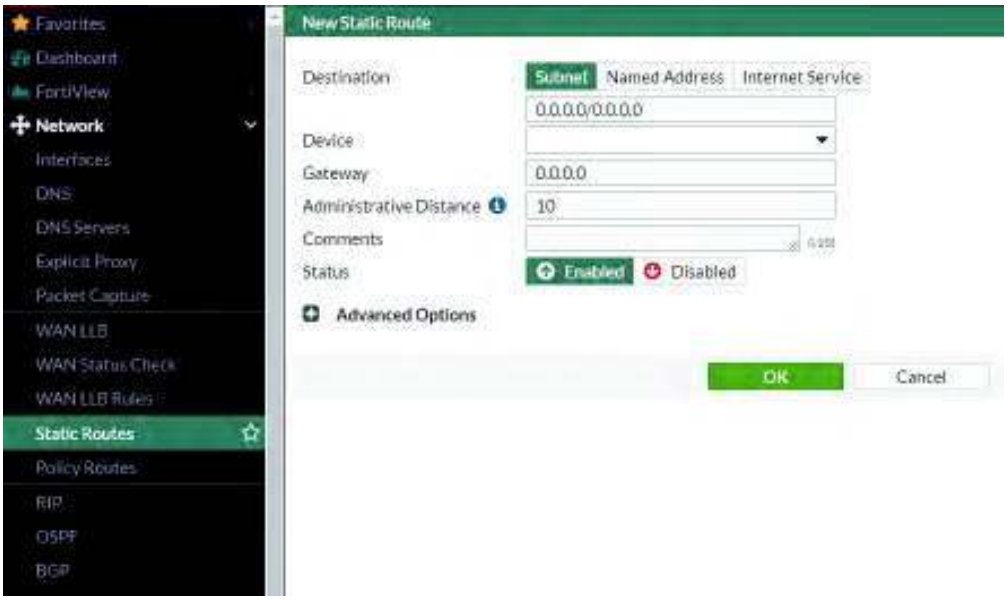


Figura 4.11 ***Configuración de ruteo definiendo distancias administrativas***

Al finalizar la parte de implementación de VPN y realizar la configuración de ruteo automatizado, se realizó una segunda un segundo túnel de VPN, ya que el Centro de Operaciones de Red ubicado en el edificio de la Procuraduría cuenta con un segundo enlace dedicado (Simétrico) y con un proveedor de Internet distinto al utilizado anteriormente en el túnel de VPN ya creado, por lo que se decidió crear un segundo túnel realizando los paso anteriormente descrito, así se aumenta la tolerancia a fallos y la alta disponibilidad en el caso de que el ISP primario falle en COR de la PGJE. Para mejorar el rendimiento de los enlaces de VPN entre las UA y el COR de la PGJE, se decidió habilitar las funciones de “Control de Aplicaciones” y el “Filtrado Web” del equipo Fortinet, ya que el mismo enlace que es utilizado para realizar la VPN es el mismo que se utiliza para el acceso a Internet, por lo que se aplicaron una serie de políticas de navegación, restringiendo una serie de categorías definidas por el mismo fabricante (Fortinet) como por ejemplo: contenido para adultos, consumo de ancho de banda, riesgo de seguridad, por mencionar algunos, dichas definiciones tanto para una aplicación, página web, virus, entre otros pueden ser consultados en la página web https://fortiguard.com como se muestra en las figuras 4.12 y 4.13.

Figura 4.12 *Barra de búsqueda de Fortiguard*

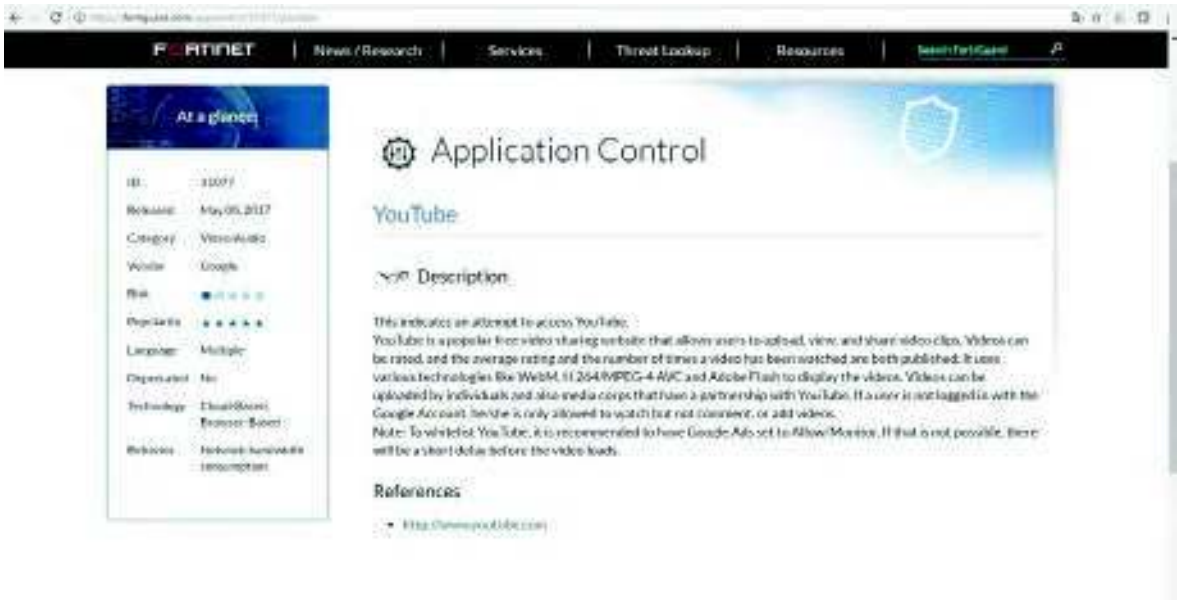


Figura 4.13 *Resultado de búsqueda en Fortiguard*

Por lo anterior, a petición del personal directivo de la PGJE se eligieron las categorías que estarían bloqueadas por defecto, solo existirán excepciones al personal que lo solicite mediante oficio y con el consentimiento del personal directivo. El filtrado web aplica a toda navegación que se haga directamente a través de un navegador web por lo que no aplica, por ejemplo: aplicación Skype, torrents, entre otros. El resultado web de la organización se ejemplifica en la figura 4.14.

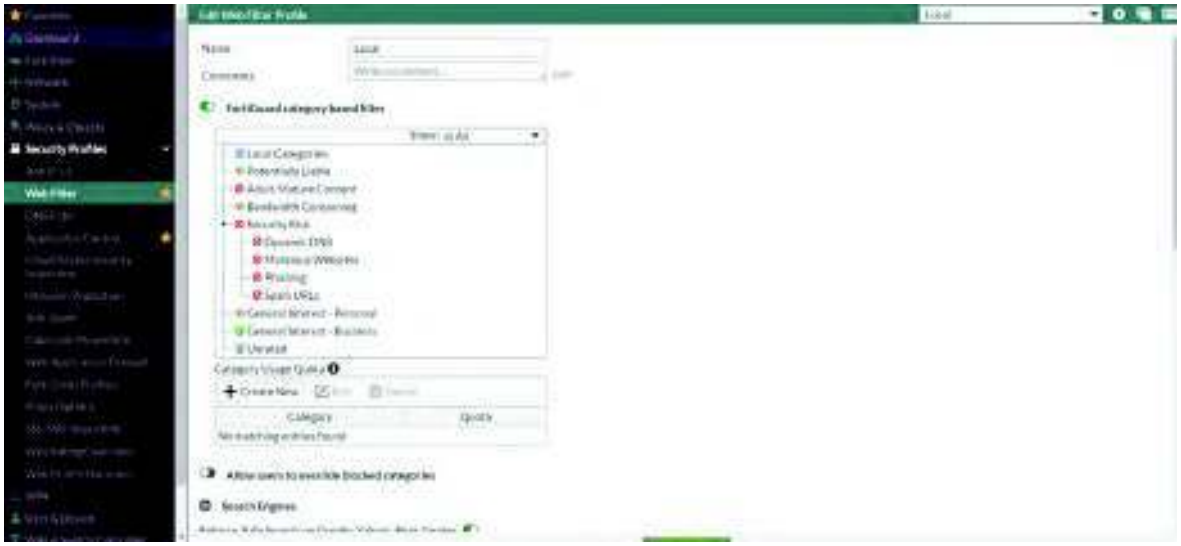


Figura 4.14 *Filtrado web por defecto de la PGJE*

En la parte de control de aplicaciones están asociado a las conexiones directas en entre la computadora y el servidor al cual se está accediendo. Se aclara lo anterior ya que, por ejemplo: si tienes permitido un filtrado web a la página de “Youtube” o “Facebook”, pero se tiene bloqueado la firma de los sitios mencionado en el perfil de Control de Aplicaciones quizás se pueda acceder al sitio web, pero en el caso de “Youtube” no se podrá reproducir ningún video. Por lo anterior se tiene que prestar atención al momento de combinar los perfiles cuando se crean las políticas de navegación de los usuarios. También se puede aprovechar en realizar bloqueos que consumen un ancho de banda considerable y no son propias de la organización como lo es con juegos, aplicaciones “P2P” (e.g. Ares, BitTorrent) y Proxy; este último utilizado normalmente para evadir los sistemas de filtrados y control de aplicaciones anteriormente mencionados. Como resultado de todo el estudio y las decisiones del

personal directivo se configuro las siguientes categorías de control de aplicaciones como se pueden observar en la figura 4.15.

Figura 4.15 *Control de aplicaciones por defecto de la PGJE*

Tanto las categorías de filtrado web y control de aplicaciones, como ya se mencionó pueden ser revisadas a fondo en la página de Fortiguard del fabricando Fortinet.

Se realizó la reestructuración de la red interna de la UA, con el fin de segmentar y aumentar el nivel de administración y seguridad de la misma como se muestra en la figura 4.16, por lo que se dividió como se describe a continuación:

- Computadoras: la red general de equipos de cómputo con direccionamiento IP dinámico (para evitar el problema de duplicado de IP).
- Equipos: direccionamiento para la administración de: firewall, switches, cámaras de video vigilancia, entre otros equipos de infraestructura de red, permitiendo solo conexiones SSH y HTTPS para su administración.
- Telefonía: creado con el fin de conectar los equipos de telefonía en un ambiente de capa 2 del modelo OSI, en este caso teléfonos IP y conmutador agilizando al momento de sincronizar los teléfonos y el conmutador.

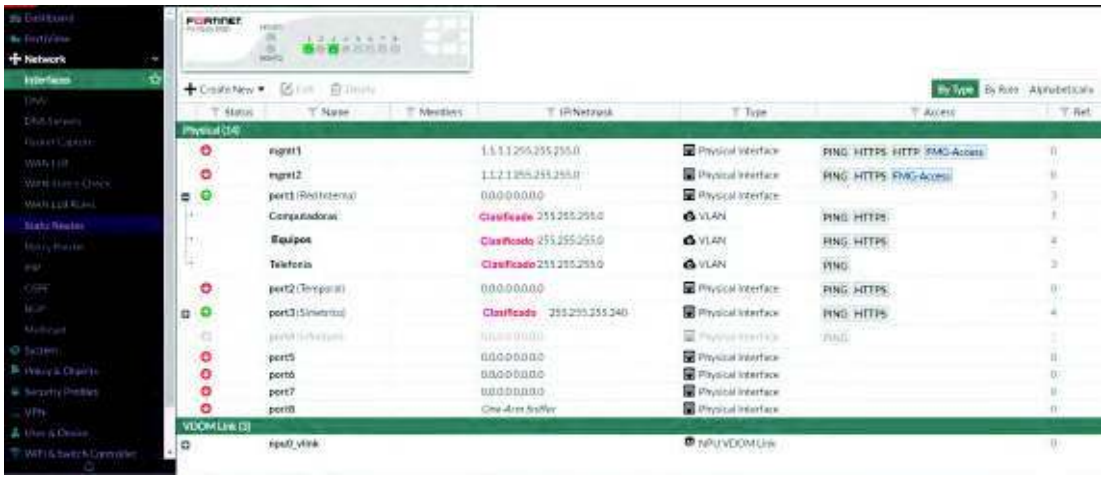


Figura 4.16 *Vlan's para la segmentación de la red*

4.5.2 Verificación y retroalimentación de implementación de sitio de bajo impacto

Al terminar el proceso de instalación en el sitio conocido como de bajo impacto en este caso el Hospital General del Estado, se mantuvo el monitoreo constante del túnel establecido de VPN. En este caso se monitoreó una semana de lunes a viernes en el horario de 8:00 a 20:00 horas en intervalos de 1 hora, para determinar la estabilidad del enlace utilizando la herramienta de monitoreo del mismo equipo Fortinet como se muestra en la figura 4.17; y así determinar si es factible replicar dicha configuración en todas las UA, que estaban proyectadas.

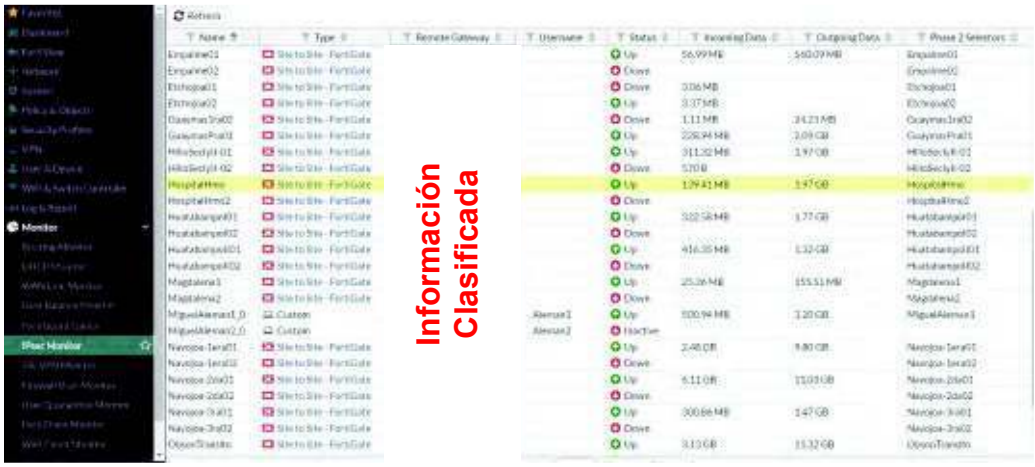


Figura 4.17 *Monitor de túnel IPsec/VPN*

También como medida de verificación se hacía una medición del comportamiento de dicho túnel, hablando vía telefónica con lo usuario de la Unidad Administrativa bajo estudio para que confirmarán el buen funcionamiento. Por otro lado, dicha verificación telefónica servía no solo para determinar la disponibilidad del enlace, sino también para verificar si el ancho de banda asignado a la UA era suficiente para realizar sus actividades laborales a través del túnel de VPN y así mismo para la navegación normal a Internet. En el caso de una respuesta negativa con la velocidad de los sistemas informáticos a través del túnel de VPN, se tendría que realizar un ajuste en las políticas de control de ancho apoyado en los perfiles de "Filtrado Web" o "Control de Aplicaciones".

4.5.3 Ajustes y rediseño de la propuesta de implementación

Al finalizar el proceso de verificación del sitio de bajo impacto, se obtuvieron resultados satisfactorios que no indicaban la necesidad de realizar un reajuste a la configuración planteada de manera inicial; al final en un plazo de 2 semanas después de la implementación en el sitio de bajo impacto se procedió a realizar una visita a dicho sitio, solo para verificar la conformidad de los usuarios de dicha UA y así proceder a la implementación general.

4.5.4 Implementación general de la solución propuesta y verificación

En esta etapa de la fase 5 al finalizar la verificación de la implementación del sitio de bajo impacto y al corregir o realizar los ajustes de configuración, que en nuestro caso no existió la necesidad, se procedió a replicar la implementación en el resto de las UA, ya que como se había mencionado tienen una similitud en la infraestructura de red con la que cuenta, teniendo variaciones en la cantidad de usuarios.

La implementación general se decidió comenzar por las UA más cercanas ubicadas geográficamente, ya que el Estado de Sonora es uno de los que tiene más extensión geográfica, así mismo como solo se contaba con la implementación del sitio de bajo impacto, se tenía la incertidumbre que podría haber algo distinto en alguna otra UA

que no fuera compatible al 100% con la arquitectura propuesta. Se comenzó por instalar las agencias de los municipios de poblado Miguel Alemán, Aconchi y Ures en ese mismo orden de instalación. Al comienzo de la instalación todo marchaba como lo proyectado, al llegar al tercero todo seguía como lo planeado, pero al día siguiente comenzaron los usuarios de dicha UA, a generar reportes de falla, los cuales a verificar en el sistema de monitoreo de VPN visualizábamos que el túnel no estaba establecido por lo que procedíamos a reestablecerlo, el problema mencionado se hizo más constante en promedio cada 2 horas era la intermitencia del servicio, por lo que se realizó un análisis de la situación detectando que el cambio de direccionamiento de IP pública cada vez que se presentaba dicho problema, se notificó al proveedor del servicio de Internet, para que realizará las configuraciones que estaban descritas en el contrato de servicio, pero la respuesta del proveedor no fue satisfactoria y pudimos observar que el servicio de DNS dinámico no es tan eficiente o tiene un tiempo de respuesta más alto al tiempo en el que la dirección IP pública de la UA cambiaba. Por lo anterior y como resultado de dicha problemática, investigando tanto en artículos de fabricante en este caso Fortinet, así como en foros de discusión y bases de conocimiento, en donde se presentaran los mismo problemas con respecto al servicio de DNS dinámico o bien se estaba buscando como reconfigurar el servicio con respecto a los tiempo de respuesta o los tiempos con los que detectaba el cambio de direccionamiento del servicio asociado, lo cual no se encontró nada de documentación, sin embargo se encontró documentación acerca de un procedimiento para realizar un “Dialup-Client de tipo Tunnel Mode”, para comprender este punto debemos mencionar que las VPN tipo Dialup normalmente son usadas para conexiones entre un cliente a un servidor de VPN, por ejemplo un empleado de una organización realizando una conexión desde de su hogar mediante su enlace de Internet a la red de la organización, por lo que en el caso que quisiéramos usar ese esquema de conexión desde una UA al COR de la PGJE, tendríamos que realizar dicha configuración de forma individual en cada computadora de dicha agencia como Fortinet lo representa en la figura 4.18.

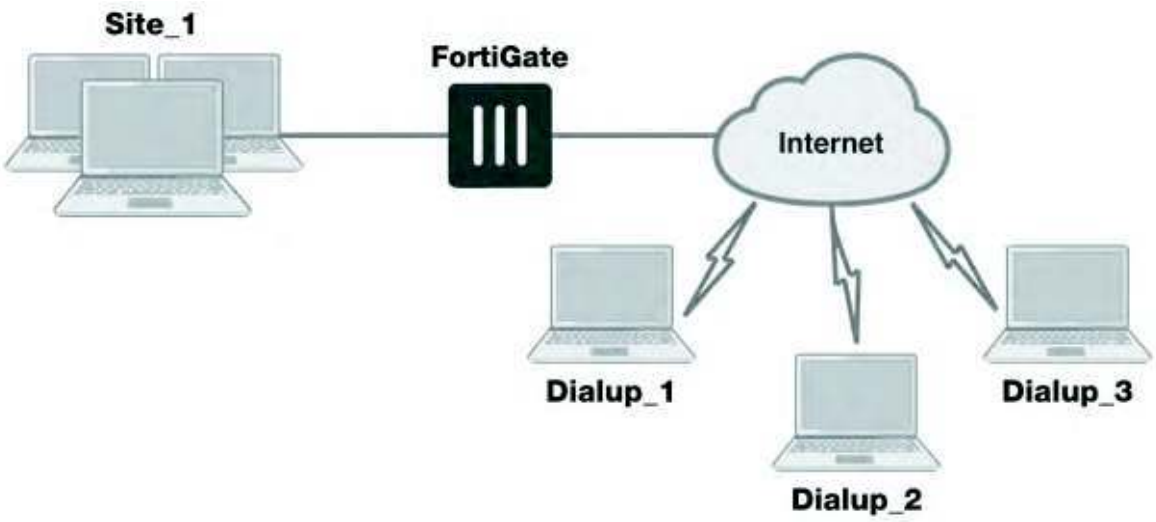


Figura 4.18 *VPN Dial-up Clientes remotos*

La ventaja de las conexiones de este tipo es que no es necesario una dirección IP pública del lado del cliente en este caso de la UA, solo se requiere una conexión con la posibilidad de conexión al COR, por lo que, si se necesita del lado del COR una dirección IP pública, para que en este caso el cliente genere la petición para establecer el túnel. Por lo anterior el fabricante Fortinet brinda la característica anteriormente mencionada de “Dialup-Client de tipo Tunnel Mode” donde uno de los dos equipos Fortigate tomará el papel de cliente como si fuera un usuario como se muestra en la figura 4.19, pero al mismo tiempo al realizar el túnel este sería funcional para transferir el tráfico de red generado por los usuarios que se encuentren conectado a dicho equipo Fortigate; para este caso particular y solo en los sitios con la problemática presentada de cambio de dirección de IP pública constante lo cual genera intermitencia en el túnel de VPN por la razones anteriormente asociadas al servicio de DNS Dinámico.

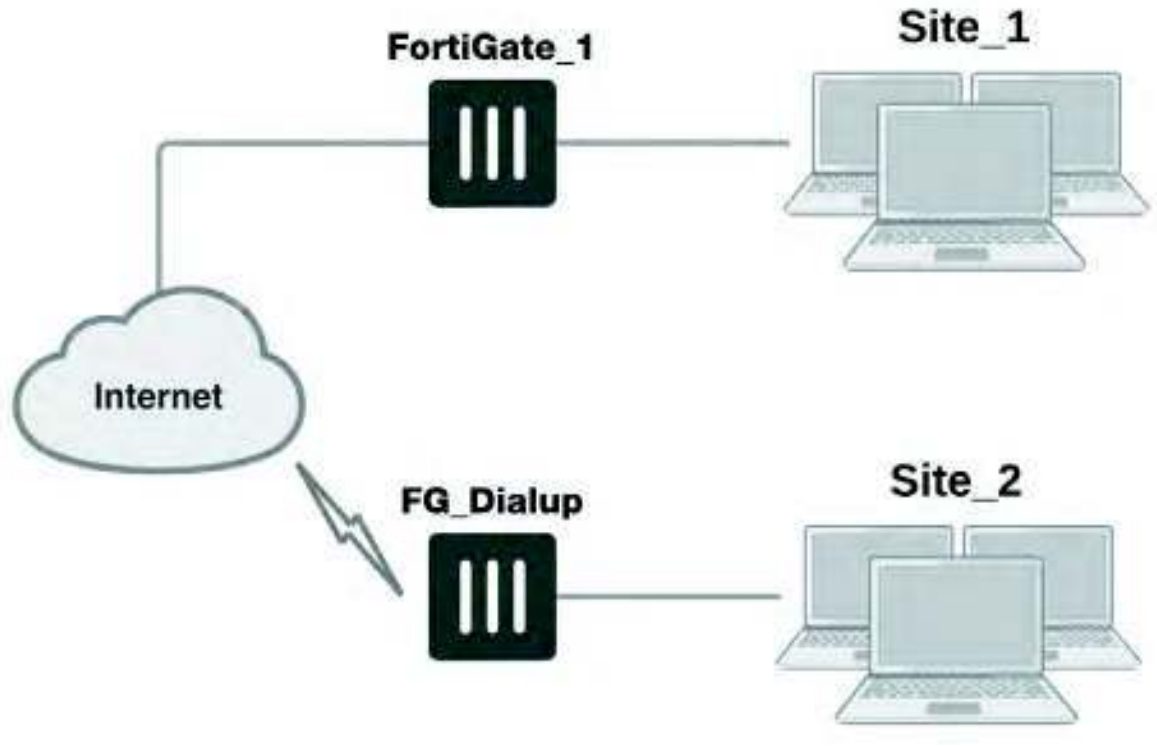


Figura 4.19 *Dialup-Client de tipo Tunnel Mode*

La configuración de la VPN mencionada se realizó utilizando el asistente de VPN/IPsec, como solo se está configurando en los sitios que se detecta el problema de cambio de direccionamiento IP, por lo que se configura inicialmente como una VPN "Site to Site" entre equipos Fortigate, en el caso de presentarse el problema de intermitencia en el túnel se procede a realizar el cambio a VPN tipo Dial-up, donde el equipo Fortigate permite modificar el túnel ya creado y personalizarlo (custom) como se muestra en la figura 4.20, donde al presionar el botón de "Convert To Custom Tunnel" automáticamente nos deja editar cada una de las opciones que se necesitan para realizar el túnel de VPN, las cuales se describen a continuación:

- Red: se encuentran las opciones del IP del equipo remoto, la interface por donde se realizará la conexión, NAT.
- Autenticación: método de autenticación donde puede ser por clave compartida o firma, IKE (Internet Key Exchange), modo de IKE.

- Fase 1: Encriptación de la conexión al realizar el túnel.
- Fase 2: donde se describen las políticas o bien las redes tanto locales y remotas que estarán transitando por el túnel de VPN.

Figura 4.20 *Dialup-Client de tipo Tunnel Mode*

Las configuraciones como se mencionó anteriormente son diferentes en la UA la cual representará la parte del cliente y el COR que representará la parte de sitio principal o Server. La configuración de una UA en Dialup se describe a continuación:

- Red: “Remote Gateway” se coloca la IP del equipo que se encuentra en el COR, no olvidemos que según la arquitectura en el sitio que será considerado como principal o Server debe de contar con IP pública fija; por otro lado, volviendo a la parte de la configuración de red, tenemos la selección de la interface por donde la UA estará conectada a Internet, se activa la parte de NAT y por último selecciona que siempre detecte el “peer” aunque este inactivo, como se muestra en la figura 4.21.

Figura 4.21 *Configuración de Red en la UA para Dialup*

- Autenticación: primero se eligió el método de autenticación, en este caso se eligió utilizar una clave compartida la cual tendrá que ser igual en la configuración del equipo instalado en el COR. Por otro lado, se seleccionó la versión de IKE tipo 1 y el modo que sea agresivo, por último, como lo realizaremos mediante Dialup y en si no tendremos una IP asociada al equipo para establecer el túnel de VPN, lo haremos utilizando un "Peer ID" para hacer la asociación del túnel mencionado, como se muestra en la figura 4.22.

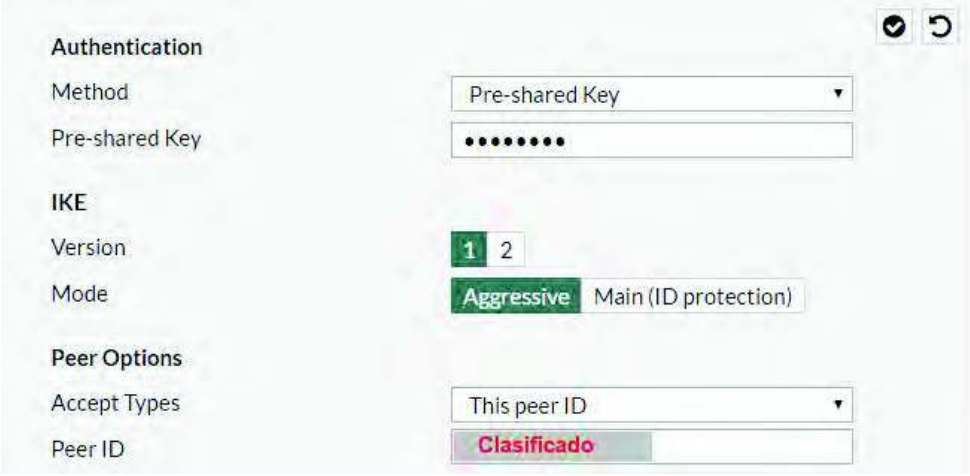


Figura 4.22 *Configuración de Autenticación en la UA para Dialup*

- Fase 1: en esta fase es donde elegimos el tipo de encriptación y autenticación va a tener el túnel, así como el identificador de local de la conexión que este es un nombre a criterio del usuario, como se muestra en la figura 4.23.

Figura 4.23 *Configuración de Fase 1 en la UA para Dialup*

- Fase 2: En esta fase no se realiza ningún cambio, como se muestra en la figura 4.24.

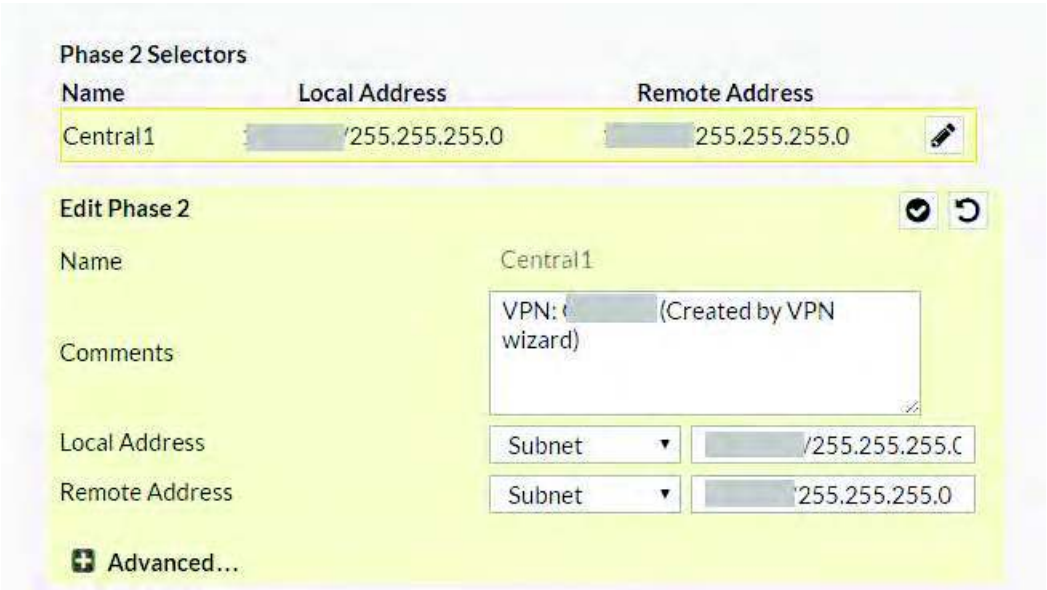


Figura 4.24 *Configuración de Fase 2 en la UA para Dialup*

Por otra parte, del lado del COR, hay ciertas variaciones en la configuración para realizar el túnel, ya que como se ha estado mencionando dicho equipo según el esquema de “Dialup-Client de tipo Tunnel Mode” juega el papel de “servidor” o equipo principal, por lo que a continuación se describe la configuración:

- Red: la diferencia a la configuración con la UA, es que en la sección con respecto al “Remote Gateway” se selecciona “Dialup User”, como se muestra en la figura 4.25.

Figura 4.25 *Configuración de Red en COR para Dialup*

- Autenticación: la diferencia a la configuración con la UA, de tipos de “Peer” aceptados seleccionaremos “especificar ID de Peer” el cual será el mismo que utilizamos en el equipo de la UA con la que se realizará el túnel, como se muestra en la figura 4.26.

Figura 4.26 *Configuración de Autenticación en COR para Dialup*

El resto de las configuraciones que son la fase 1 y fase 2 para generar el túnel de VPN, son las mismas tanto en el COR como en la UA, solo se intercambia en la parte de fase 2, las redes remotas y locales según sea el caso; como se mencionó la diferencia entre un tipo de túnel y otro es que, el Dialup no requiere direccionamiento IP fijo ya que no lo utiliza en la parte de la UA para realizar la conexión, así como para realizar el túnel si lo realizamos de la forma inicial el túnel solo se establece cuando hay actividad en cualquiera de los 2 sitios, en cambio el tipo Dialup siempre está forzando a que el túnel este establecido, por lo que si utilizamos el monitor y se encuentra que un túnel de la forma tradicional no se encuentra establecido, pueda deberse a que hay una inactividad en la agencia por lo que podemos hacer la prueba generando tráfico y revisar si se establece el túnel, por otro lado, en el caso de tipo Dialup, si existe una desconexión en el túnel que visualicemos en el monitor de IPsec, lo más probable es que se debe a que no se cuenta con servicio por parte del proveedor de Internet.

Otra de las situaciones que se presentó es que los contratos de servicio de Internet no tienen una especificación de la velocidad mínima que tienen que otorgar a las UA, por lo que en UA como Puerto Peñasco y Bacum era demasiado lento el túnel de VPN establecido por lo que se decidió realizar la conexión mediante C4 el cual era hasta 5 veces más estable y veloz.

4.5.5 Comparativo de resultados

Se realizó un comparativo de resultados con respecto a la cantidad de solicitudes de servicio derivado de falla de conectividad las cuales se pueden reflejar en algunos casos, como los que se describen a continuación:

- Problema de acceso a los sistemas: cuando no pueden entrar al sistema “nuevo” el cual como ya se explicó está centralizado por lo tanto requiere en todo momento una conexión establecida entre la UA y el COR, que en este caso en el túnel de VPN que hemos mencionado.

- Sin acceso a Internet: esto se refiere cuando el usuario comentaba que no podía acceder a la navegación normal que en la mayoría de los casos era casos reportaban no tener acceso al correo electrónico.
- Telefonía IP: no se contaba con el servicio de telefonía IP por diferentes razones, una de ellas es que hay UA que su equipo telefónico están registrados y enlazados al conmutador que se encuentra en el COR, por lo que al no tener el túnel de VPN el equipo dejaba de funcionar.
- Falla en replicación de información: este tipo de reporte era interno de la Dirección de Sistemas, ya que lo realizaba el administrador de base de datos, lo cual se debía a que no existía conectividad entre el servidor de la UA y el servidor central de replicación ubicado en el COR.

El comparativo mencionado se realizó con la información de 3 meses anterior a la implementación de la nueva arquitectura, así como 3 meses posterior a la instalación, como se había recomendado anteriormente la utilización del sistema de captura de servicios que usa el área de soporte técnico lo cual la organización accedió, dicho sistemas se capturan las llamadas telefónicas y oficios de solicitudes de servicio. También se midió los tiempos promedio de respuesta para la acción correctiva en cada una de la solicitud presentada. Los tiempos de medición para la situación antes de implementación contempla los meses de octubre, noviembre y diciembre de 2016 y se utilizó el mes de enero y febrero para realizar la implementación, por lo que los meses de comparación posterior a la implementación son marzo, abril y mayo de 2017. En ambos comparativos tanto número de solicitudes de servicio y tiempo fueron promedios de cada uno de los meses, para la parte de solicitudes fueron el número promedio diario capturados en el sistema los cuales podía ser vía telefónica, presencial o bien mediante oficio. Por otro lado, para la parte de tiempos de respuesta, se comenzó a registrar el tiempo de duración de la falla que va ligado al tiempo en que el técnico realizaba las acciones correctivas, en algunas ocasiones la falla va directamente al proveedor de Internet, por lo que en dichos casos no fueron omitidos tanto en la situación anterior y posterior a la implementación ya que son ajenas a las

acciones que pudiera realizar el personal correspondiente. A continuación, se representa de manera gráfica en las figuras 4.27 y 4.28 el comparativo entre las dos situaciones mencionadas.

Figura 4.27 *Comparativo de promedio diario de solicitudes por mes*

Figura 4.28 *Comparativo de promedio tiempo para corregir el reporte*

Como se puede observar en los gráficos anteriores tanto la cantidad de solicitudes diarias, así como el tiempo de respuesta para corregir el reporte o la solicitud recibida ambos tuvieron una disminución considerable, podría decirse de más de 50%, las variaciones entre los meses están asociadas a temporadas. Por ejemplo, el mes 3 “antes” es diciembre o el mes 2 “después” que es abril, ambos meses incluyen periodo vacacional lo cual al realizar el promedio diario presenta una disminución en comparación a los meses de su mismo ciclo, pero por la misma situación en la parte de tiempo de acción correctiva tuvo un aumento tanto en el mes de diciembre como en abril, ya que hay acciones correctivas que se requieren hacer en sitio y en algunas ocasiones no se encontraba el personal correspondiente. También hay muchas acciones que dependen de un tercero por ejemplo en el caso del personal de C4, que por la misma razón de periodo vacacional se dificultaba el contacto.

Adicional a la implementación se realizó la propuesta para que la organización actualizara o cambiara la forma de captura de solicitudes de servicio ya que el sistema que se utilizaba normalmente solo registra la orden, pero no nos brinda más información solo el detalle de la solicitud. Por lo que se le recomendó un sistema especializado para “help desk” en este caso se propuso el osTicket, ya que cuenta con ciertas funcionalidades a continuación, se mencionan algunas (Osticket, 2017):

- Personalización: como es una herramienta de código abierto, se puede personalizar a la necesidad de la organización o agregar información aparte de la recomendada, por ejemplo: temas de ayuda, información de los técnicos o del usuario, entre otros.
- Notificación mediante correo electrónico: interacción entre el usuario final y los técnicos.
- Organización de solicitudes: asignación de solicitudes para un solo técnico y así no tener duplicidad de información o confusiones entre los usuarios finales y los técnicos.
- Reportes: creación de reportes tanto de las solicitudes como del mismo personal técnico.

- Portal de acceso: el usuario puede crear su propia solicitud sin tener que llamar a la mesa de ayuda, así mismo puede darle el seguimiento o tener contacto directo con el técnico que fue asignado.

El sistema mencionado fue instalado y configurado para el uso de la organización, aún está en fase de ajustes, pero ya se está utilizando como se pueden observar en el anexo 2. También como el sistema tradicional de la organización sigue en funcionamiento y se requiere la información al menos de manera mensual para realizar lo que llaman “corte estadístico mensual” por lo que dicha información que se encuentra en los servidores de cada UA y se requiere replicar al servidor central y así poder concentrar la misma. Por lo anterior al realizar la configuración propuesta se tuvo un impacto significativo con respecto a esa operación de la organización, ya que solo se tenía la conectividad al 100% con 3 UA el resto estaba en una interconexión intermitente o nula con el COR como se muestra en la figura 4.29, donde entrevistando al personal correspondiente de recopilar dicha información se tenía que trasladar durante 2 semanas a lo largo de 22 municipios, lo cual indica que en ese lapso de tiempo no se tenía la información de dichas UA.

Figura 4.29 *Representación de UA conectadas antes de la implementación*

Por lo que al realizar la conectividad entre las UA y el COR, ya que era una operación obligatoria por la cuestión del nuevo sistema implementado que funciona de manera centralizada, se aprovechó para utilizar los túneles de VPN establecidos y se configuraron los servidores de las UA, para replicar la información de manera automática, por lo que ahora se cuenta con la información de las UA del viejo sistema en tiempo real, reflejándose en un ahorro económico al no tener que realizar los traslados mensuales para la recolección de la información, representando a continuación el cambio de conectividad en la figura 4.30.

Figura 4.30 *Representación de UA conectadas después de la implementación*

5 CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

En el presente trabajo de tesis se buscó desarrollar e implementar un procedimiento para el aprovechamiento de la infraestructura de red de la organización, con el fin de implementar una solución de una red administrada por software o bien optimizar las funcionalidades del equipamiento instalado en el caso de no tener la compatibilidad con SDN. Mediante el procedimiento desarrollado en el presente proyecto, la organización pudo resolver la problemática de la estabilidad y disponibilidad de la interconexión entre las Unidades Administrativas y el Centro de Operaciones de Red de la organización. Así mismo por la arquitectura de alta disponibilidad y tolerancia a fallos, se disminuyeron los reportes de fallas presentadas por la UA, así como los tiempos de respuesta al realizar acciones correctivas el caso de ser requerido, dicha arquitectura era funcional con respecto a la red interna tanto del edificio principal de la organización como de cada UA.

A continuación, se describen las conclusiones, recomendaciones y trabajos futuros derivados de esta investigación, con el fin de continuar con el proyecto y realizar mejoras.

5.1 Conclusiones

Se diseñó e implementó una arquitectura de red que mejora la estabilidad y disponibilidad de la red entre las UA y el servidor central de la PGJE mediante el procedimiento propuesto que consta de 5 fases e incluyen:

- Configurar el equipo seguridad perimetral de las UA para tener un funcionamiento automatizado y de alta disponibilidad con el servidor central.
- Diseñar un modelo de monitoreo del equipamiento de red, que alerté en el caso de falla y almacené los sucesos para su análisis posterior, como apoyo a la toma de decisiones.

- Optimizarlos recursos de red con el fin de automatizar los procesos y operaciones de red.

El procedimiento propuesto, además permite que en caso de que no se pueda implementar un modelo basado en SDN sea posible aplicar un modelo tradicional optimizado para brindar alta disponibilidad.

El análisis de la situación benefició a la organización, ya que, al contar con un inventario actualizado de su equipamiento instalado, así como de los servicios contratados, se detactaron duplicidades y servicios instalados que el personal de la Dirección de Sistemas no tenía conocimiento o sin utilizar.

Se desarrolló una propuesta de modernización que permitirá a futuro la implementación de SDN de manera progresiva. Esta propuesta apoya al área administrativa en la selección de los equipos a adquirir en el futuro, además se plantearon bien los requerimientos ya que tiene un alto impacto económico, y a su vez se pueda cumplir con todos los detalles necesarios para los procesos de adquisición que se sigue en el ámbito gubernamental.

Al terminar la fase 3 se hizo una propuesta de actualización tecnológica la cual aún no soporta una arquitectura de SDN, pero al recibir el equipamiento propuesto, la organización se encontraría a la vanguardia de equipamiento tecnológico, así como realizar lo necesario en temas de: seguridad, alta disponibilidad, interconectividad temas de los cuales carecía la organización.

Se detectó que los proveedores de Internet tenían diferente calidad de servicio según la región geográfica, por lo que se tuvo que realizar evaluaciones y ajustes al momento de la toma de decisiones en las contrataciones, así como al momento de implementar decidir cuál sería el enlace principal en la UA para realizar la conexión con el COR.

Al evaluar la arquitectura propuesta se pudo observar deficiencias en el sistema con el cual captura o registran las solicitudes de servicio, por lo que, al implementar el

sistema propuesto, se ajustó para ser el sistema de mesa de ayuda de la Dirección de Sistemas en general, dividiendo los casos en: soporte técnico, redes y el área de desarrollo de sistemas.

Así mismo, dados los resultados obtenidos, se puede observar que la implementación tuvo beneficios económicos y eficiencias en las funciones propias de la organización, agilizando los procesos y el flujo de información.

5.2 Recomendaciones

Con el fin de mejorar la arquitectura de red propuesta, así como el servicio que brinda la Dirección de Sistemas a la organización, a continuación, se enlistan una serie de recomendaciones para la optimización y eficiencia de la misma:

- Fase 3: se recomienda a la Dirección de Sistemas sea más participativa al momento de realizar las partidas presupuestales, ya que dicha Dirección es quien tienen el conocimiento real de las necesidades tecnológicas de la organización o bien adquirir lo necesario para optimizar la arquitectura tecnológica que se tiene.
- Fase 1: con respecto al registro de solicitudes de servicio se instaló un sistema para la mesa de ayuda, el cual se generalizó para todas las áreas de la Dirección de Sistemas. Se recomienda explotar más las funcionalidades de dicha plataforma, así como realizar un curso o manual de usuario, para que el usuario final tenga una mejor interacción y alimente de la información correcta a dicha plataforma, mejorando el tiempo de respuesta a la solicitud y a su vez dando la pauta de la creación de una base de conocimiento.
- Fase 4: mejorar el aspecto alta disponibilidad con respecto a las interconexiones de la UA con el COR, ya que hay sitios remotos que no se tiene conectividad por la red estatal de C4 y solo se tiene al proveedor de Internet o viceversa, solo se tiene C4 y no se tiene Internet, por lo que en dichos sitios realizó el estudio para tener una interconectividad “punto a punto” mediante inalámbrico a la UA

más cercana geográficamente y así cumplir con el criterio de alta disponibilidad (redundancia de enlace).

- Monitoreo de red: es recomendable contar con un sistema de alertas automatizadas que notifique al personal correspondiente ya que actualmente, tienen que acceder al sistema de monitoreo y solo así tienen conocimiento si existe un problema.

5.3 Trabajos Futuros

Se ha logrado un avance muy importante en la arquitectura tecnológica de la organización, así como en la calidad del servicio que brinda la Dirección de Sistemas al resto de la organización. Aun no se logró alcanzar el total de las UA con las que cuenta la organización solo las mencionadas anteriormente, derivado de la limitante y alcance del proyecto por cuestiones del tiempo que se tiene para resolver la problemática. El procedimiento propuesto puede ser muy beneficioso si se analiza al detalle el resultado que se espera y la situación actual de la organización, así como poder replicarlo al 100% en toda la organización. Algunos de los trabajos futuros podrían ser:

- Trabajar en el desarrollo de aplicaciones específicas de SDN aun sin contar con equipamiento que soporte el protocolo de OpenFlow, como por ejemplo realizar aplicaciones de optimización utilizando el protocolo estándar de CAPWAP, como es en el caso de la PGJE que cuenta con equipamiento de controlador inalámbrico y puntos de acceso marca Fortinet.
- Capacitación y optimización del sistema osTicket para explotar la parte de interacción con el usuario, así mismo identificar los problemas claves para la creación de un catálogo para la creación y organización de las solicitudes de servicio.
- Definir requerimientos tecnológicos en la UA restantes para reproducir la arquitectura de red en el 100% de la organización.

- Implementar un sistema de monitoreo integral para toda la infraestructura de red, como por ejemplo SolarWinds el cual es de licenciamiento o bien el Cacti que es de código abierto.
- Instalar un software especializado que mida la velocidad de ancho de banda del túnel establecido entre la UA y el COR, con el fin usarlo como herramienta para la toma de decisiones al momento de elegir cuál de los enlaces será el principal en la UA, entre C4 y el proveedor de Internet.

6 REFERENCIAS

Akhunzada, A. et al., 2015. Securing software defined networks: Taxonomy, requirements, and open issues. IEEE Communications Magazine, 53(4), pp.36–44.

Alharbi, T. y Portmann, M., 2015. The (In) Security of Topology Discovery in Software Defined Networks The (In) Security of Topology Discovery in Software Defined Networks. , (October), pp.502–505.

Bindra, N. y Sood, M., 2016. Is SDN the Real Solution to Security Threats in Networks? A Security Update on Various SDN Models. Indian Journal of Science and Technology, 9(32). Available at: http://www.indjst.org/index.php/indjst/article/view/100214.

Bondkovskii, A. et al., 2016. Qualitative comparison of open-source SDN controllers. Proceedings of the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, (Noms), pp.889–894.

Casta, M.E.Z., 2011. Sistema multi-agente para el monitoreo de tráfico LAN y recursos usados por los equipos * 1 [Multi-agent system for monitoring LAN traffic and resources used by equipment] Resumen Introducción. , (c), pp.57–76.

Cui, H. et al., 2014. Design of intelligent capabilities in SDN. 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2014 - Co-located with Global Wireless Summit.

Elsadek, W.F. y Mikhail, M.N., 2016. Inter-domain Mobility Management Using SDN for Residential/Enterprise Real Time Services. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp.43–50.

Fraser, B. et al., 2013. Are We Ready for SDN ? Implementation Challenges for Software-Defined Networks. , (July), pp.36–43.

Han, Y. y Hyun, J. y Hong, J.W., 2016. Graph Abstraction Based Virtual Network Management Framework For SDN. , pp.16–17.

Kim, W. et al., 2016. OFMon: OpenFlow monitoring system in ONOS controllers. IEEE NETSOFT 2016 - 2016 IEEE NetSoft Conference and Workshops: Software-Defined Infrastructure for Networks, Clouds, IoT and Services, pp.397–402.

Lin, Y.D. et al., 2016. Fast failover and switchover for link failures and congestion in software defined networks. 2016 IEEE International Conference on Communications, ICC 2016.

Luan, M. et al., 2015. Controllable network architecture based on SDN. Proceedings - 2015 2nd International Conference on Information Science and Control Engineering, ICISCE 2015, pp.174–180.

Martín, A. et al., 2012. A framework for development of integrated intelligent knowledge for management of telecommunication networks. Expert Systems with Applications, 39(10), pp.9264–9274.

Nakayama, H. et al., 2014. An implementation model and solutions for stepwise introduction of SDN. APNOMS 2014 - 16th Asia-Pacific Network Operations and Management Symposium, 1, pp.2–5.

Naudts, B. et al., 2016. Deploying SDN and NFV at the speed of innovation: Toward a new bond between standards development organizations, industry fora, and open-source software projects. IEEE Communications Magazine, 54(3), pp.46–53.

Patel, K., 2016. Software Defined Networking : Architecture , Application , Issues and Challenges. , 5(5), pp.78–81.

Pontarelli, S. et al., 2016. Stateful OpenFlow: Hardware proof of concept. IEEE International Conference on High Performance Switching and Routing, HPSR, 2016–June.

Rufaida Ahmed, M.N., 2016. Fast Failure Detection and Recovery Mechanism for Dynamic Networks Using Software -Defined Networking. , pp.167–170.

Salman, O. et al., 2016. SDN Controllers: A Comparative Study. , (978), pp.18–20.

Shin, J.W. et al., 2016. Access Control with ONOS Controller in the SDN Based WLAN Testbed. , pp.656–660.

Shu, Z. et al., 2016. Security in Software-Defined Networking: Threats and Countermeasures. Mobile Networks and Applications, pp.1–13.

Wang, M. et al., 2016. An Approach for Protecting the OpenFlow Switch from the Saturation Attack. , (Nceece 2015), pp.729–734.

Yang, S. y Chang, Y., 2011. Expert Systems with Applications An active and intelligent network management system with ontology-based and multi-agent techniques. , 38, pp.10320–10342.

Ipv6.udg.mx. (2016). IPv6 OpenFlow. [en linea] disponible en: http://www.ipv6.udg.mx/oess.php [accedido 17 Mar. 2016].

Opendaylight.org. (2016). Research Government | OpenDaylight. [en linea] disponible en: https:// www.opendaylight.org/research-ed-government [accedido 24 Mar. 2016].

Opendaylight.org. (2016). Platform Overview | OpenDaylight. [en linea] disponible en: https://www.opendaylight.org/platform-overview [accedido 13 Oct. 2016].

Hpe.com. (2017). Data sheet. [en linea] disponible en: https://www.hpe.com/h20195/v2/getpdf.aspx/4aa3-0717enw.pdf [accedido 12 Ene. 2017].

Osticket.com. (2017). Features. [en linea] disponible en: http://osticket.com/features [accedido 22 Ene. 2017].

Gns3.com. (2017). SDN 101: Using Mininet and SDN Controllers. [en linea] disponible en: https://gns3.com/news/article/sdn-101-using-mininet-and-sdn-co [accedido 22 Feb. 2017].

Gartner.com. (2017). doc: Magic Quadrant for Enterprise Network Firewalls. [en linea] disponible en: https://www.gartner.com/doc [accedido 22 Mar. 2017].

7 ANEXOS

7.1 Anexo 01: Solicitud de servicio mediante oficio

Orden de servicio realizada mediante oficio la cual van dirigidas a la Directora de Tecnologías de Información, la descripción de la solicitud y la firma del solicitante, la cual sirve para determinar la ubicación física del usuario.

LIC. REBECA SALAZAR FALCONON
C. ENCARGADA DE LA DIRECCION
GENERAL DE TECNOLOGIAS DE
INFORMACION Y COMUNICACIONES
DE LA FISCALIA GENERAL DE JUSTICIA
DEL ESTADO DE SONORA.
P R E S E N T E:

Por este medio solicito a Usted en CARACTER URGENTE tenga a bien autorizar
revisión, configuración, internet e instalación de Sistema Integral de Apoyo al Ministerio
Público (SIAMP) y Sistema Información de Gestión Integral (SIGI) en los equipos que se
encuentran en días en resguardo de esta fiscalía siendo los siguientes:

SERIE	SOLICITUD
MXL9490949	Revisión y Diagnostico
MXL9490952	(En caso que quedara
MXL9490944	funcional instalar
	SIAMP Y SIGI)
MXL9490962	Configuración e instalación
	De SIAM y SIGI.
MXL9491387	Configuración de internet
MXJ7000178	
MXJ007GGLV	

Asimismo se solicita servicio completo a todos los equipos de computo en
resguardo de esta fiscalía los cuales se encuentran en sitio, así como también el de
mantenimiento para la impresora HP LASER JET 600 M602, lo anterior por ser necesario
para el buen funcionamiento de esta Fiscalía.

Sin ningún otro particular por el momento, me valgo la seguridad de mi atenta y
distinguida consideración.

A T E N T A M E N T E
SUFRAGIO EFECTIVO. NO REELECCION
LA C. AGENTE DEL MINISTERIO PUBLICO ESPECIALIZADA EN DELITOS
SEXUALES Y VIOLENCIA FAMILIAR

LICENCIADA SABRINA VERONICA MARTINEZ

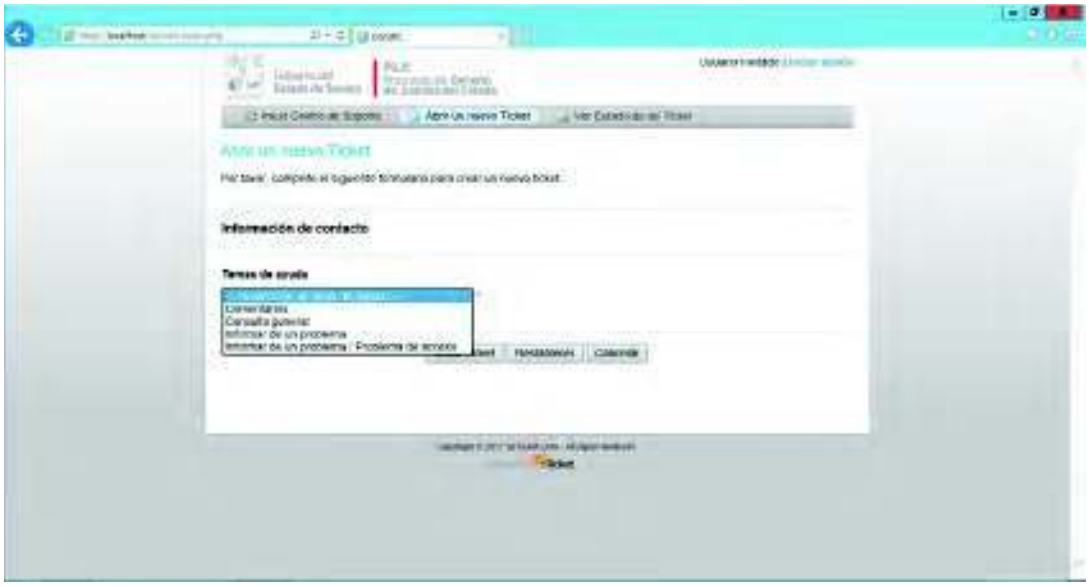
7.1 Anexo 02: Sistema de mesa de ayuda personalizado

Pantalla de inicio del sistema de OsTicket el cual fue personalizado con la imagen que usa la organización para sus sistemas internos.

Pantalla de inicio después de autenticarse, donde le permite al usuario ver el estado de sus solicitudes pendientes o bien crear una nueva solicitud de servicio.

Ventana de registro de cuenta en donde se crean la contraseña del usuario y se define la zona horaria.

Al abrir una nueva solicitud se puede utilizar temas de ayuda los cuales, permiten agilizar la identificación del sistema y así mismo la asignación del técnico más competente para la resolución del problema.



Ventana de registro de creación de solicitud donde se especifica información del usuario solicitante y descripción de la solicitud de servicio.

Representación de la carátula de una impresión del formato de solicitud de servicio en donde está la información del usuario, el técnico asignado, descripción del lugar y descripción de solicitado.

"El saber de mis hijos hará mi grandeza"

Hermosillo, Sonora a 17 de agosto de 2017

JOSE ISMAEL CAMARENA VIDALES

Con fundamento en el artículo 66, fracción III, del Reglamento de Estudios de Posgrado vigente, otorgamos a usted nuestra aprobación de la fase escrita del examen de grado, como requisito parcial para la obtención del Grado de Maestro en Ingeniería.

Por tal motivo este jurado extiende su autorización para que se proceda a la impresión final del documento de tesis: **DISEÑO E IMPLEMENTACIÓN DE UNA RED DE TELECOMUNICACIONES INTELIGENTE: CASO PROCURADURÍA GENERAL DE JUSTICIA DEL ESTADO** y posteriormente efectuar la fase oral del examen de grado.

ATENTAMENTE

Dr. Gerardo Sánchez Schmitz
Director de Tesis y Presidente del Jurado

Dr. Alonso Pérez Soltero
Codirector y Vocal del Jurado

Dr. René Francisco Navarro Hernández
Secretario del Jurado

Dr. Mario Barceló Valenzuela
Vocal del Jurado

MSI. Francisco Javier Rosas Ibarra
Vocal Externo del Jurado

RESUMEN

Dado el apoyo y facilidad que brindan las telecomunicaciones a las organizaciones para el desarrollo de sus actividades y que gracias a ellas pueden tener presencia en diferentes sitios distribuidos geográficamente, en la actualidad, las organizaciones son más dependientes de las redes de telecomunicaciones, refiriéndose a las interconexiones entre las oficinas de la misma organización asi como para la conexión al mismo servicio de Internet. Por lo anterior las redes de telecomunicaciones y su administración se han vuelto más complejas, por lo que se tienen que desarrollar mecanismos automatizados para el monitoreo, control y administración de las mismas. Actualmente existe una arquitectura automatizada administrada por software, la cual facilitan la administración y a su vez optimiza la conectividad, dichas arquitectura es conocida como SDN (Software Defined Networking) y tiene como objetivo transformar una red “pasiva” en una “proactiva”.

El presente proyecto se desarrolló en la Procuraduría General de Justicia del Estado de Sonora (PGJE), específicamente en la Dirección de Sistemas. La mencionada Dirección apoya en el desarrollo y mantenimiento de los Sistemas Informáticos con los cuales la organización desarrolla sus actividades, así mismo tiene la función de interconectar las Unidades Administrativas (UA) con el edificio central de la PGJE, para que las UA puedan acceder a los sistemas y servicios hospedados dentro del edificio principal.

Derivado a que la organización está en la implementación del Nuevo Sistema de Justicia Penal, el cual cambió el esquema de red de telecomunicaciones de distribuido a centralizado, se hizo vital la interconexión entre la UA y el edificio central de la PGJE y dado a que no todas las UA cuentan con una conexión o bien las que sí tienen son demasiado lentas que no soportan la utilización de los sistemas de información requeridos para el desarrollo de sus actividades. También la infraestructura de red

interna propia tanto de las UA como la de la PGJE se encuentran en un estado tecnológico obsoleto.

Una vez realizado un proceso de investigación documental, no se encontró una metodología o procedimiento el cual ayude a resolver las problemáticas particulares que se presentaron en la organización, es por esto que se hizo el planteamiento de un procedimiento con el fin hacer una evaluación de la situación actual de la organización, teniendo como objetivo realizar una implementación de SDN, que considerara, que en el caso de no contar con una factibilidad técnica o bien que la implementación de SDN no resuelva las problemáticas planteadas de la organización recomendara optimización de los recursos de infraestructura actuales, así como un análisis de requerimientos para hacer más eficiente la red de telecomunicaciones y resolver las problemáticas planteadas.

La implementación de dicho procedimiento ayudó a resolver las problemáticas de interconexión entre las UA y el edificio central, así como optimizó y mejoró las infraestructuras de red interna tanto de la UA como de edificio central de la PGJE, donde dicha infraestructura no cumplía con los requerimientos para el buen funcionamiento de los sistemas de información. También se facilitó la administración y control de la red para el personal encargado de administrarla, automatizando procesos y disminuyendo los tiempos de reacción para la realización de acciones correctivas.

ABSTRACT

Currently the organizations are more dependent of telecommunication networks, for the interconnection between offices of the same organization as well for the Internet service connection. Giving the support and ease provided by telecommunications to the business for the development of their activities, telecommunications provide the ability to have presence in different geographical distributed points is it that their demand has grown. Based on the foregoing, the telecommunication networks and their administration has become more complex, reason why is required the development of automated mechanisms for the monitoring, control and administration. Currently exists an architecture administered by software which eases the administration and at the same time automate the connectivity. This architecture is known as SDN (Software Defined Networking), having as main objective to transform a passive network to a proactive network.

The present project was developed in the Attorney General of Justice of the State of Sonora, specifically in the Systems Division, This Division supports the development and maintenance of information systems in which the organization develops its activities and it provides the required interconnection between the administrative units and the central building giving the required access to the services and systems hosted in the central building.

Due to that the organization is implementing the new accusatory system, the architecture of the telecommunication network changed from a distributed to a centralized model. Thereby the interconnection between the administrative units and the central building became vital. Having that not all the administrative units are connected and that they have a slow connection that does not allow to use the information systems required to develop their activities. Along with these, the internal network infrastructure in the central building and in the administrative units is obsolete.

Because we were not able to find a methodology or procedure to help us solve the difficulties present in the organization, we propose a procedure to evaluate the actual situation of the organization to implement a SDN architecture, in such case that organization does not have the technical viability or that the SDN implementation does not solve the difficulties exposed, recommend instead the optimization of the current organization infrastructure resources and the analysis of the requirement needed to transform in to a more efficient telecommunication network and to solve the difficulties exposed.

The implementation of the procedure help us to solve the difficulties of interconnection of the administrative units with the central building, and to optimize and improve the internal infrastructure in the administrative units and the central building of the Attorney General of Justice of the State of Sonora, having thus that the infrastructure implemented accomplish the needed requirements for the optimal performance of the information systems, facilitating also the administration and control of the telecommunication network for the employees responsible for managing it, by process automation which decreased the time to accomplish corrective actions.

DEDICATORIAS

“Si la oportunidad no llama, construye una puerta”

A mi prometida Dalia Corral, a mis padres Ismael Camarena y Luz Cristina Vidales, a Trinidad Corral y Rosa Guerrero, familiares y amigos que estuvieron a lo largo de este ciclo en mi vida.

AGRADECIMIENTOS

Primeramente, a Dios por brindarme la capacidad y fortaleza para culminar esta etapa de mi vida y darme la fuerza de siempre seguir adelante.

A mi prometida Dalia Corral, por su amor y apoyo incondicional alentándome siempre a un crecimiento personal y profesional.

A mis padres Ismael Camarena y Luz Cristina Vidales, que siempre me han apoyado y confiado en que puedo alcanzar mis objetivos.

Al Dr. Guzmán Gerardo Alfonso Sánchez Schmitz por su apoyo y consejos para la realización de este proyecto, así como la confianza y amistad brindada.

Al Dr. Mario Barceló Valenzuela por todo el apoyo brindado y aconsejarme a lo largo del proyecto de tesis.

Al Procuraduría General de Justicia del Estado de Sonora por todo el apoyo y la oportunidad del desarrollo del proyecto, en especial a la directora Lic. Rebeca Salazar Pavlovich y Lic. Jesus Ariel Gándara Toledo.

A mis compañeros y al cuerpo académico de la maestría que estuvieron siempre brindando su apoyo.

Al Consejo Nacional de Ciencia y Tecnología (CONACYT) y al Programa de Fortalecimiento de la Calidad Educativa (PFCE 2016) por su apoyo económico, el cual me facilitó en gran medida el logro de esta meta.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN

En la actualidad utilizar aplicaciones dependientes de las tecnologías de telecomunicaciones es cada vez más común, debido a ello su crecimiento es acelerado, haciendo su administración y mantenimiento más compleja (Yang y Chang, 2011). La complejidad de una red de telecomunicaciones está dada por la demanda de múltiples servicios y versatilidad. Los modelos de administración actuales son inadecuados para soportar la gran demanda de servicios. En la administración tradicional de una arquitectura de red, el objetivo es simplemente reportar y actualizar el estatus de los dispositivos conectados (Martín et al., 2012). Hay organizaciones que hacen poca supervisión sobre el ancho de banda que consumen por cada servicio y los recursos de hardware que utilizan, propiciando ineficiencia y dificultad en la detección de fallas (Casta, 2011).

El propósito de la administración de la red es gestionar eficientemente el equipamiento involucrado en la infraestructura de red, identificar problemas presentados y realizar las acciones correctivas correspondientes, utilizando de herramientas de apoyo que permitan la detección inmediata de falla, brindando así un servicio de calidad, siendo esto último el reto más importante de la administración de las redes modernas (Yang y Chang, 2011).

Por lo que, en función de una estructura de red tradicional que se ha vuelto más compleja, la capacidad de control cada vez es menor y difícil de garantizar la calidad en el servicio. El “software defined networking” (SDN) proporciona una nueva forma de resolver los problemas anteriores mediante un nuevo tipo de arquitectura presentada por “CleanSlate”, un equipo de investigación de la Universidad de Stanford (Luan et al., 2015). La aparición de SDN transforma la red “pasiva” en una “proactiva”, de modo que la red puede manejar el tráfico de forma activa y flexible (Cui et al., 2014).

Dado que SDN permite al administrador de la red gestionarla de manera más fácil y flexible, se espera superar los problemas tales como, construir una red con equipos de

conmutación de diferentes fabricantes teniendo así un lenguaje de configuración diferente, eliminar problemas provenientes de la intervención de la mano humana (Nakayama et al., 2014).

1.1 Presentación

El proyecto se realizó en la Procuraduría General de Justicia del Estado (PGJE), la cual cuenta con varias direcciones en su organigrama, específicamente se desarrollará en la Dirección General de Sistemas de Información y Política Criminal (DGSIPC) la cual está enfocada en mantener los servicios informáticos utilizados por la dependencia, el desarrollo de nuevos sistemas y la interconectividad entre las Unidades Administrativas (UA). La Dirección se divide en cuatro direcciones de área: Dirección de Sistemas de Información y Base de Datos, Dirección de Estadística y Política Criminal, Dirección Sistema de Apoyo al Ministerio Público y Dirección de Innovación Tecnológica de Sistemas Biométricos, teniendo un total de 23 empleados incluyendo al Director General.

Actualmente dentro la PGJE se está implementando el nuevo Sistema de Justicia Penal (SJP), por lo que la dirección DGSIPC está a cargo de poner en marcha un nuevo sistema de información que cumpla con los requerimientos del nuevo esquema de Justicia. El acceso al sistema y la interconectividad entre las UA se han convertido en parte fundamental para el desarrollo de las actividades de las mismas.

El sistema de información utilizado en el esquema de Justicia anterior sigue en funcionamiento hasta que se termine de implementar el nuevo esquema, lo cual se está realizando por fases en todo el Estado, con respecto al anterior sistema tiene un funcionamiento descentralizado donde cada UA cuenta con su propio servidor, la información se replica a un servidor central para su recolección y así facilite el análisis estadístico, consulta de información y respaldo de los datos. La replicación de la información presenta problemas ya que no todas las UA cuentan con un enlace al servidor central o en algunos casos el servicio es demasiado lento o intermitente. Por otro lado, el nuevo Sistema de Información que se encuentra en fase de

implementación es un esquema centralizado, por lo que se ve afectado directamente por la problemática descrita anteriormente ya que se encuentra hospedado en el servidor central.

La infraestructura de telecomunicaciones con la que cuenta la PGJE y las diferentes UA es muy heterogénea lo que hace difícil para los administradores de la red el monitoreo y su administración, ocasionando que el tiempo de ejecución de acciones correctivas al presentarse una situación anómala o de falla sean muy largos o bien que solo una persona tenga la capacidad de solucionar los eventos presentados.

1.2 Planteamiento del Problema

La Procuraduría General de Justicia del Estado está implementado el SJP mediante un Sistema de Información en el cual accedan todas las UA del Estado, por lo que es crítico contar con una conexión estable y de alta disponibilidad con el servidor central, así mismo es necesario mejorar la arquitectura de red para un monitoreo y administración eficiente que reduzca los tiempos de acciones correctivas en el caso de falla.

1.3 Objetivo General

Diseñar e implementar una arquitectura de red administrada por software, con el fin de mejorar la estabilidad y disponibilidad de la red entre las UA y el servidor central de la PGJE; así mismo permita crear procesos automatizados de monitoreo y administración del equipamiento involucrado en la infraestructura de red.

1.4 Objetivos Específicos

- Configurar el equipo seguridad perimetral de las UA para tener un funcionamiento automatizado y de alta disponibilidad con el servidor central.
- Diseñar un modelo de monitoreo del equipamiento de red, que alerté en el caso de falla y almacené los sucesos para su análisis posterior, como apoyo a la toma de decisiones.

- Optimización de los recursos de red con el fin de automatizar los procesos y operaciones de red.
- Evaluar los tiempos de ejecución de acciones correctivas y cantidad de errores presentados en un periodo determinado, con la arquitectura actual y posterior a la implementación propuesta.
- Crear una arquitectura de red de alta disponibilidad para tener tolerancia a fallos.

1.5 Hipótesis

Implementar una arquitectura de red que permita la administración y control del equipamiento red mediante software y/o la automatización de operaciones de red, así como la interconexión entre las UA y el servidor central, disminuirá la inestabilidad y desconexiones, así como los tiempos en la ejecución acciones correctivas en el caso de fallas en la red.

1.6 Alcances y Delimitaciones

El proyecto se ha enfocado en implementar una arquitectura de alta disponibilidad entre las UA y el servidor central, y se basará solo en las UA que cuenten con al menos dos enlaces de Internet o intranet y equipamiento que soporte las configuraciones necesarias de la arquitectura propuesta. La arquitectura para la administración y control de la infraestructura de red, será implementada únicamente UA que además de los enlaces de interconexiones cuenten con el equipamiento de red para realizar la propuesta.

1.7 Justificación

La utilización del nuevo Sistema de Información se ha convertido en parte fundamental para las actividades de la PGJE, por lo que, si una UA pierde la conexión al servidor central y no se puede acceder al Sistema, ocasiona deficiencia en el servicio brindado a la ciudadanía, más grave aún la incongruencia o pérdida de información.

La arquitectura de red se ha desarrollado como apoyo al servicio de red y telecomunicaciones de la PGJE, debido a que no cuenta con un esquema adecuado de monitoreo en tiempo real que este analizando el estado de la red y con la capacidad de alertar a los administradores en el caso de presentarse alguna falla, tanto en la interconexión entre las UA y el servidor central, como dentro de la misma infraestructura de la PGJE, reflejándose en largos tiempos de ejecución de acciones para la solución de los problemas presentados.

La optimización y automatización de los procesos de red, simplifica la administración y control del equipamiento de red, así mismo la solución de fallas o configuraciones adicionales.

Por lo tanto, la implementación de dicha arquitectura beneficio a realizar acciones correctivas eficientes en el caso de presentarse problemas o anomalías en la red que afectan directamente a las principales actividades de la PGJE, así mismo se almaceno las fallas y soluciones de los eventos suscitados permitiendo su análisis posterior como apoyo a la toma de decisiones. Por último, habilito un esquema de alta disponibilidad en la conectividad con el servidor central con una operatividad automatizada de corrección de errores, resultando esto en un servicio estable durante todo el día, ya que el personal a cargo del soporte de la red tiene un horario laboral que difiere del personal vespertino/nocturno, donde en el caso de presentarse falla, se interrumpe el servicio y se espera a la solución hasta el día posterior.

2 MARCO DE REFERENCIA

En este capítulo se presenta la revisión bibliográfica, la cual sustenta el desarrollo del presente proyecto. Se aborda solo conceptos avanzados relacionados con las redes de telecomunicaciones, así como de herramientas de software diseñadas para la administración y monitoreo del equipamiento de la infraestructura de red. Así mismo se presenta estudios previos relacionados con el tema de esta investigación. Se aclara que los conceptos básicos de redes, sus protocolos y propiedades no se describen ya que son temas de conocimiento general de los administradores de red.

2.1 Redes definidas por software

La aparición del SDN ha creado el potencial y la esperanza de superar las necesidades de las siguientes generaciones de redes de telecomunicaciones, dando seguridad, flexibilidad, confiabilidad y una mejor administración. Con SDN se centraliza la administración a un controlador externo al equipamiento, haciendo más sencillo la programación de todo el hardware. Las características que ofrece SDN obviamente son muy notables, como una arquitectura innovadora, rentable y programable independientemente del fabricante de tecnología. Aunque se muestran muchas características positivas del utilizar SDN, existe la preocupación por parte de los expertos acerca del tema de la seguridad, lo cual consideran que debe de tratarse de forma muy minuciosa (Akhunzada et al., 2015).

En la arquitectura tradicional cada equipo dentro de la red se podría decir que es un controlador por lo que cada decisión de enrutamiento u otro protocolo es realizado por cada equipo. Por otro lado, en la arquitectura de SDN existen varios componentes responsables en la entrega de los paquetes de extremo a extremo como se muestran en la figura 2.1., 1- Interface de red: cada dispositivo en la red cuenta con interfaces con las cuales se interconectan para comunicarse con otros dispositivos, 2- Dirección Norte (Aplicación), es la interacción entre las aplicaciones que se ejecutan dentro la infraestructura de red y el controlador de SDN, 3- Dirección Sur (Aplicación), esta zona

se utiliza normalmente en protocolo de OpenFlow, en donde se define una serie de reglas para el desvío de los datos, lo cual permite al equipamiento de enrutamiento y conmutación el entendimiento de la topología de red, así mismo las solicitudes enviadas desde los aplicación de la dirección norte; 4- el Controlador, es lógicamente un controlador centralizado responsable de: a) Interpretación de los requisitos previos de la aplicación de SDN hasta el plano de datos, b) proporciona una visión de red que puede incluir Notificación de eventos, reportes estadístico, reenvío de paquetes, entre otros (Patel, 2016).

SDN promete simplificar la implementación y la operación de la red de telecomunicaciones, a la par reducir los costos de administración de la misma, brindando servicio de red programables (Fraser et al., 2013).

Debido a su paradigma de control centralizado, SDN está siendo adoptado para las redes como, los centros de datos, redes móviles, redes de trasporte y las redes empresariales, por lo que es muy importante la resistencia a las fallas, existen dos tópicos para atacar las problemáticas mencionadas que es la restauración y protección. La restauración, cuando un switch detecta un fallo en el enlace de la conectividad, entonces un mensaje de notificación se envía al controlador para que calcule un nuevo camino al flujo de la interconexión entre los switches. En la protección, el controlador calcula varias rutas de interconexión entre los switches, instalando las entradas en cada uno de ellos con anterioridad, con el fin de que el caso de fallo el switch puede dirigir al tráfico a otra ruta previamente cargada sin tener que esperar las órdenes del controlador. Además de la perdida de enlace, otro de los problemas que tienen los administradores de red es la congestión en los enlaces, el cual es derivado de sobre saturación de datos por un mismo enlace, efecto que ocasionaría una reducción en el rendimiento de la red (Lin et al., 2016).

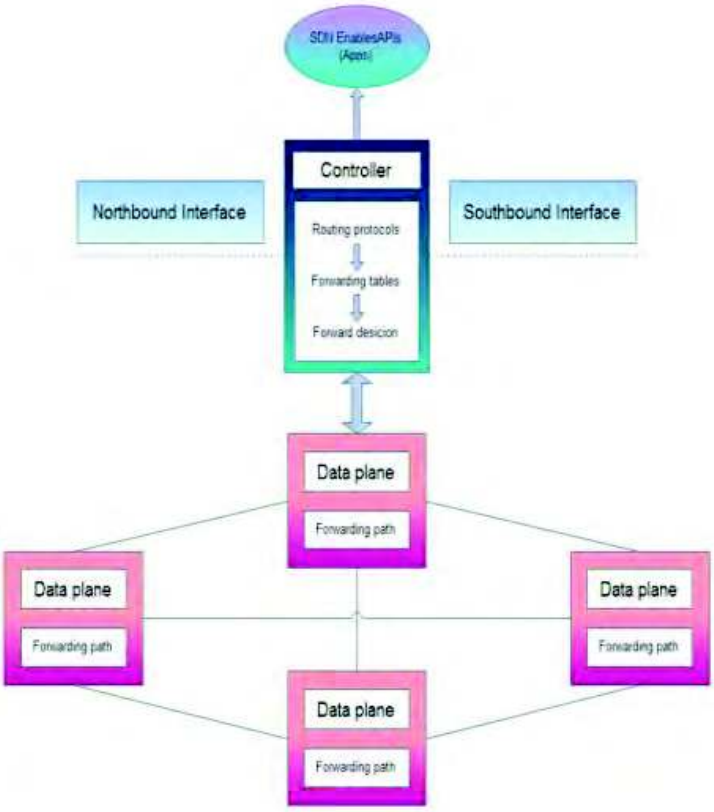


Figura 2.1 *Representación de SDN (Patel, 2016)*

2.2 Principales protocolos de monitoreo y control de SDN

Los protocolos populares para SDN son el ForCES (Forwarding and Control Elements Separation) y OpenFlow. Ambos protocolos utilizan el principio fundamental de SDN que es separar los planos de control y datos (Patel, 2016).

OpenFlow un protocolo presentado por primera vez en el año 2008, es un protocolo de comunicación para la manipulación remota el reenvió de enrutadores y conmutadores; es considerado por algunos como el sinónimo de SDN y ahora es un elemento clave dentro de las iniciativas industriales de SDN, actuando como protocolo utilizado por los controladores de SDN (Bondkovskii et al., 2016). Openflow ha ganado en los últimos años la atención de los investigadores con respecto a la red de

telecomunicaciones. La contribución de Openflow es que era una interfaz donde se programaba el reenvió de tráfico dentro de los equipos de conmutación (switch), lo que fue la inspiración para el lanzamiento de lo que hoy conocemos como SDN, ya que se presenta deficiencias en las reglas de reenvío programados en los equipos de conmutación son de forma estáticas por lo que es requerido un controlador para automatizar y hacer dinámico los ajustes den la reglas en el caso de cambios (Pontarelli et al., 2016). El protocolo Openflow tiene tres componentes: Switch OpenFlow, un canal para el OpenFlow y un controlador. Un Switch OpenFlow consiste en una o diversas tablas de flujos las cuales transitan a través del canal de flujo al controlador externo con el fin de manejar los paquetes de tráfico (Shin et al., 2016).

Uno de los servicios esenciales dentro de una red de SDN es el descubrimiento de la topología de red, la cual soporta las aplicaciones de alto nivel como es el enrutamiento y el reenvió de paquetes. Si bien no hay una norma oficial para el mecanismo de descubrimiento en una arquitectura de SDN, se podría decir que existe un estándar OFDP (OpenFlow Discovery Protocol), todos los principales controladores de SDN implementan esencialmente este mecanismo de descubrimiento (Alharbi y Portmann, 2015).

2.3 Principales plataformas de SDN de open source

El controlador central de SDN permite tener un seguimiento del rendimiento y funcionalidad de la red, así como realizar la reconfiguración si es necesario, supervisa de manera puntual el tráfico de los paquetes y los enlaces de conectividad, con el fin de restaurar si hay una pérdida de enlace, esto con el objetivo general de cualquier red, el garantizar la conectividad de un punto a otro. Uno de los protocolos más tradicionales para esto dentro del SDN es el OpenFlow, el cual funciona en la zona norte de la arquitectura entre el plano de control y el plano de datos. Por desgracia OpenFlow no implementa rápidos mecanismos de recuperación de fallos, los cuales son necesarios para una red de telecomunicaciones confiables, así mismo OpenFlow utiliza un esquema de programación de muy bajo nivel, limitando las capacidades de

control de brinda el control de SDN, por lo que los investigadores están proponiendo mecanismo de recuperación de fallos en OpenFlow (Rufaida Ahmed, 2016).

Las características principales de un controlador de SDN son:

- Multiplataforma: Fácil de aprender, buen uso y manejo de la memoria del computador, característica esencial de los lenguajes de programación, siendo lo más comunes Python, C++ y Java, teniendo ventajas y desventaja cada uno de ellos.
- Southbound API´s, permite el control sobre la red, donde el controlador utiliza estas API´s para realizar cambios necesarios en las reglas de envío de tráfico que se encuentran instaladas en los equipos del plano de datos, como lo son: switches, routers por mencionar algunos.
- Northbound API´s, son utilizadas para la comunicación del controlador con la capa de aplicación, por lo que son parte fundamental de SDN, ya que la interacción adecuada de estas, proporciona un mejor servicio.
- OpenFlow es un habilitador clave para SDN, fue la primera interfaz estandarizada de Southbound, permite la manipulación directa del plano de reenvío de tráfico.
- La programación de la red es unos de los beneficios más importantes de SDN, por la complejidad en el control y administración derivado de la gran cantidad de dispositivos conectados a la red, así como la necesidad de nuevos servicios. Por lo anterior no es factible la administración tradicional de la red que es equipo por equipo de manera individual, por lo que SDN viene a resolver estas dificultades de gestión de red.
- Eficiencia, es un término utilizado para varios parámetros: rendimiento, escalabilidad, fiabilidad y seguridad, así mismo tiene métricas como la cantidad de interfaces que puede administrar, latencia, entre otros. La parte de centralización es un reto con respeto a términos de rendimiento y fiabilidad, por lo que existen propuesta de varios controladores distribuidos con el fin de la alta disponibilidad y tolerancias a fallos.

- Asociación, se refiere a la compatibilidad con productos o soluciones de múltiples fabricantes como por ejemplo: CISCO, Linux, Intel, IBM, Juniper, entre otros (Salman et al., 2016).

2.3.1 Controladores y plataformas de SDN

Open Network Operating System (ONOS) es el primer SDN de código abierto dirigido a proveedores de servicio y a redes de telecomunicaciones de misión crítica. ONOS desde que era conocido como Network Operating System (NOS) tiene como función: administración de los recursos finitos, aislamiento y protección de los usuarios por mencionar algunas (Shin et al., 2016). Aunque con ONOS se puede resolver lo que es cuello de botella del plano de control, todavía sigue siendo problemático el decidir cuándo y cómo distribuir la carga de trabajo del plano del control, además es un factor que puede afectar e rendimiento del plano de control tales como el intercambio de comunicación entre el controlador. Por lo tanto, la mayoría de los controladores deberán exigir el sistema de seguimiento del plano de control (Kim et al., 2016).

NOX es una pieza de las redes SDN, en concreto se trata de una plataforma para el desarrollo de aplicaciones para el control de la red, donde al comienzo Openflow fue reconocido como la primera tecnología de SDN, NOX fue desarrollado en paralelo como el primer controlador de OpenFlow (Noxrepo.org, 2016).

POX es el hermano menor de NOX, el cual, en esencia, es una plataforma para el rápido desarrollo y creación de prototipos de software de control de red utilizando Python con el fin de ayudar a escribir a un controlador de OpenFlow. También es utilizado como base para ayudar a construir redes SDN (Noxrepo.org, 2016).

Opendaylight (ODL) es una plataforma modular de código abierto de SDN para las redes independientes a la escala y tamaño de las mismas. ODL permite los servicios de red a través de un entorno múltiples vendedores de hardware, proporcionando al usuario el administrar y controlar múltiples protocolos y aplicaciones (Opendaylight.org, 2016).

2.3.2 Comparativo de controladores de SDN

A continuación, se muestran en la tabla 2.1 el comparativo de algunos controladores de SDN.

	Programming Language	GUI	Documentation	Modularity	Distributed/ Centralized	Platform Support	Southbound APIs	Northbound APIs	Partner	Multithreading Support	OpenStack Support	Application Domain
ONOS	Java	Web Based	Good	High	D	Linux, MAC OS, And Windows	OF1.0, 1.3, NETCONF	REST API	ON.LAB, AT&T, Ciena, Cisco, Ericsson, Fujitsu, Huawei, Intel, Nec, NsfNtt Comunnication, Sk Telecom	Y	N	Datacenter, WAN and Transport
Open-Day-Light	Java	Web Based	Very Good	High	D	Linux, MAC OS, And Windows	OF1.0, 1.3, 1.4, NET-CONF/ YANG, OVSDB, PCEP, BGP/LS, LISP, SNMP	REST API	Linux Foundation With Memberships Covering Over 40 Companies, Such As Cisco, IBM, NEC	Y	Y	Datacenter
NOX	C++	Python + QT4	Poor	Low	C	Most Supported On Linux	OF 1.0	REST API	Nicira	NOX _MT	N	Campus
POX	Pyth on	Python + QT4	Poor	Low	C	Linux, MAC OS, And Windows	OF 1.0	REST API	Nicira	N	N	Campus
RYU	Pyth on	Yes	Fair	Fair	C	Most Supported On Linux	OF 1.0, 1.2, 1.3, 1.4, NETCONF, OF-CONFIG	REST For Southb ound	Nippo Telegraph And Telephone Corporation	Y	Y	Campus
Beacon	Java	Web Based	Fair	Fair	C	Linux, MAC OS, And Windows	OF 1.0	REST API	Stanford University	Y	N	Research
Maestro	Java	-	Poor	Fair	C	Linux, MAC OS, And Windows	OF 1.0	REST API	RICE, NSF	Y	N	Research
Floud-Light	Java	Web/ Java Based	Good	Fair	C	Linux, MAC OS, And Windows	OF 1.0 , 1.3	REST API	Big Switch Networks	Y	N	Campus
Iris	Java	Web Based	Fair	Fair	C	Linux, MAC OS, And Windows	OF 1.0, 1.3, OVSDB	REST API	ETRI	Y	N	Carrier-Grade
MUL	C	Web Based	Fair	Fair	C	Most Supported On Linux	OF 1.4, 1.3, 1.0, OVSDB, OF-CONFIG	REST API	Kaicloud	Y	Y	Datacenter
Runos	C++	Web Based	Fair	Fair	D	Most Supported On Linux	OF 1.3	REST API	ARCCN	Y	N	WAN, Telecom and Datacenter
Lib-Fluid	C++	-	Fair	Fair	-	Most Supported On Linux	OF 1.0, 1.3	-	ONF	Y	N	-

Tabla 2.1 *Comparativo de Controladores de SDN* (Salman et al., 2016)

2.4 La seguridad y SDN

La administración de la red ha pasado al siguiente nivel, pero también viene con las cuestiones de seguridad y vulnerabilidades. Un administrador de red puede controlar el equipamiento desde una consola central, sin tener que tocar cada uno de los equipos, esto también aplica para las redes inalámbricas, lo que hace más flexibles, escalables y agiles, que las redes tradicionales. La parte de seguridad de SDN puede ser divida en tres áreas: 1.- amenazas actuales como ataques de negación de servicio, ataques distribuidos de negación de servicio, troyanos, hackeo y robo de información sensibles, 2.- Vulnerabilidad en los softwares utilizados para SDN y 3.- único punto de falla por utilizar una arquitectura centralizada (Bindra y Sood, 2016).

Desde el surgimiento de SDN el tema de la seguridad de la red ha sido muy relevante. Los nuevos paradigmas de las redes traen grandes beneficios a la parte de la seguridad de la red, se mencionan tres características que diferencias las redes de SDN con las redes Tradicionales: la perspectiva de la seguridad, visión global de la red, auto-corrección de errores y el aumento en la capacidad de control y administración de la red. Sin embargo, algunos problemas de seguridad son específicos de la arquitectura de SDN y los cuales no han sido abordados, centrándolo es la parte de ataques de las comunicaciones en el plano del control, ataques contra los controladores y falta de mecanismos para asegurar la confianza entre las aplicaciones de administración específicas de SDN y el controlador, donde dichas vulnerabilidades se pueden reflejar en graves desastres dentro de la red (Wang et al., 2016).

2.4.1 Tipos de ataques comunes

Al tener una arquitectura de SDN, también conlleva tener una serie de vulnerabilidades o ataques, que ocasionen interrupción en la comunicación a continuación, se mencionan algunos de los ataques más comunes:

- (Man-in-middle attack between switch and controller) es un método clásico de ataque a la red, donde implica colocar un nodo intermedio entre la comunicación del nodo fuente con el nodo destino, lo cual es utilizado para interceptar datos y manipularlo sin ser detectado por ninguno de los dos nodos participantes en la comunicación.
- (DoS attack to saturate the flow table and flow buffer) el ataque de negación de servicio es una inundación de paquetes en la red y como en la arquitectura de red, cada vez que un paquete vaya a un destino desconocido se genera una nueva regla de flujo dentro del switch, por lo que si se comienza a genera de manera simultánea y rápidamente paquetes a múltiples destinos saturando la capacidad de almacenamiento de tablas de flujo del switch (Shu et al., 2016).

2.4.2 Ventajas y desventajas de seguridad de SDN

La utilización de SDN a comparación de las redes tradicionales, tiene amenazas aún más concentradas por el esquema centralizado, a diferencia de un esquema más distribuido o disperso como lo es el tradicional, por lo que SDN tiene ventajas y desventajas con respecto a la seguridad:

Ventajas:

- Eficiencia al monitorear tráfico anormal, debido que el controlador de SDN tiene conocimiento de todo el tráfico de la red de manera simultánea, por lo que facilita observar un comportamiento anómalo.
- Tratamiento oportuno de las vulnerabilidades, el administrador puede programar la forma de analizar y tratar dicha vulnerabilidad, a diferencia de cuando se depende del fabricante lo resuelva y actualice el software del equipamiento involucrado.

Desventajas:

- Vulnerabilidad del Controlador, ya que la mayoría de las acciones tales como, recopilación de la información de la red, la configuración del equipamiento de

red y cálculo de enrutamiento, se concentran en el controlador, por lo que, si un atacante logra conseguir la administración de un controlador de SDN, puede causar una parálisis total de los servicios de red afectando toda la red, donde el controlador tenga cobertura.

- Riesgo a causa de interfaces abiertas programables, debido a su naturaleza abierta, SDN se hace más susceptible a las amenazas de seguridad.
- Más puntos de ataque debido a que la arquitectura de SDN se divide en 3 capas y la comunicación entre ellas será necesaria y más frecuente, como se representa en la figura 2.2 (Shu et al., 2016).

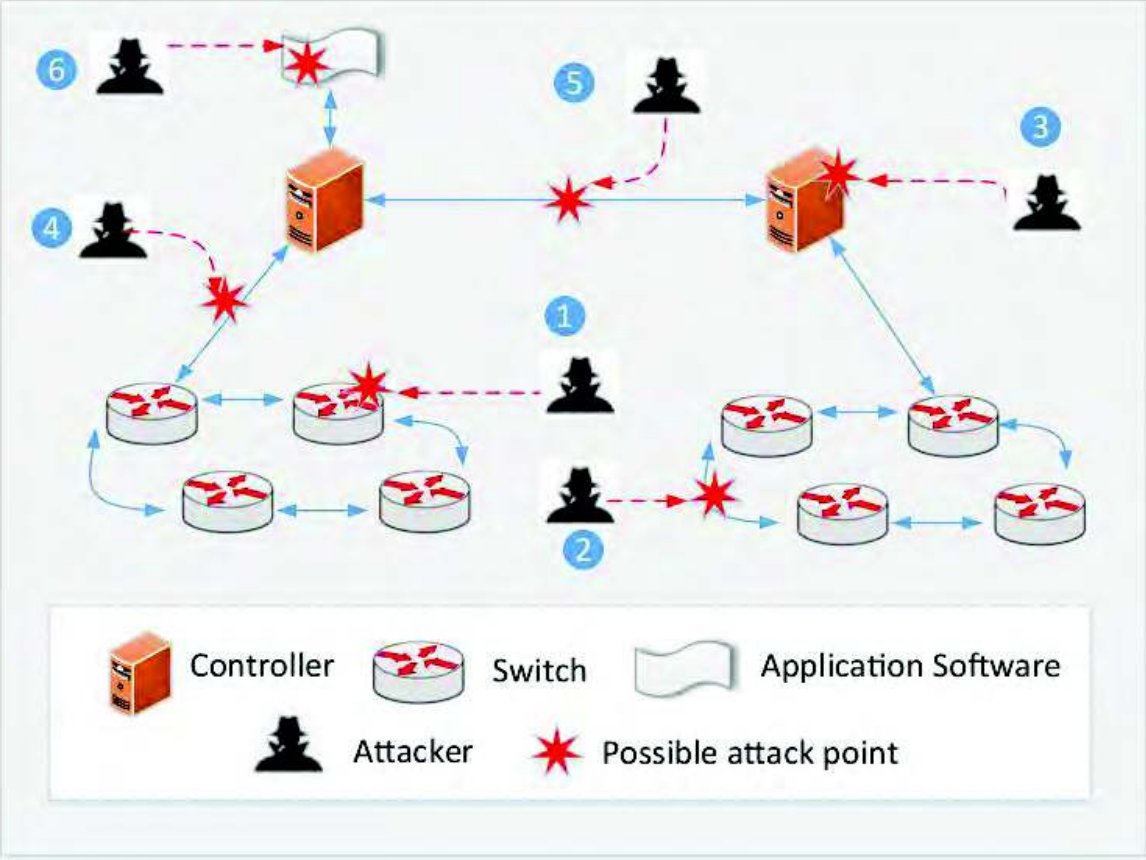


Figura 2.2 *Múltiples puntos de ataque en SDN* (Shu et al., 2016)

2.5 Virtualización y SDN

La virtualización de la red es un método que provee una ilusión de una red dedicada por encima de los recursos de hardware, la cual permite compartir los mismos recursos de hardware a múltiples usuarios sin ocasionar alguna interferencia entre ellos. La virtualización de red puede tener varias ventajas, como la flexibilidad, compartición de recursos, escalabilidad, agilidad y bajos costos económicos y de operación. Desafortunadamente este tipo de soluciones de virtualización se centran en tecnologías como VMware y Hyper-V utilizando un método de túnel fácil de implementar y sin tener que realizar cambios de configuración en la red, pero al trabajar de esta forma genera sobrecarga del túnel, por lo que se requiere un equipamiento especializado como son conmutadores virtuales o controladores (Han et al., 2016).

SDN (Software Defined Networking) y NFV (Network Function Virtualization) son paradigmas que se complementan como se muestra en la figura 2.3, donde SDN se centra en el control de los recursos de red mediante software para proveer un servicio, mientras NFV se centra en el ciclo de vida de algunos servicios de red. De hecho, SDN puede ser utilizado para el control de los servicios en una arquitectura de red tradicional, virtualizada o un combinación de ambas (Naudts et al., 2016).

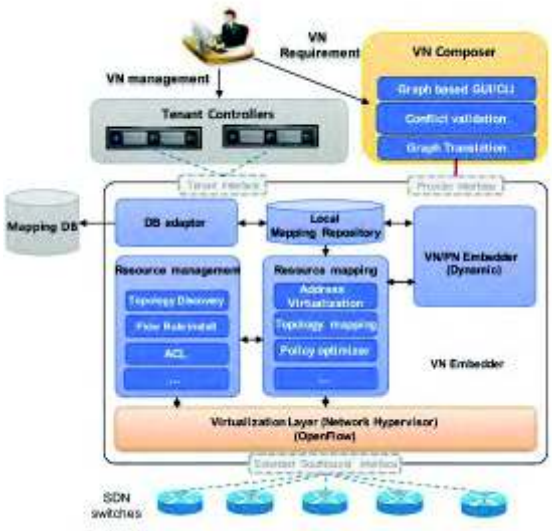


Figura 2.3 *Virtualización con SDN* (Han et al., 2016)

2.5.1 Usos y Ventajas de SDN

SDN y OpenFlow proporcionar varias ventajas al utilizar la virtualización en la red, ya que provee la abstracción en hardware de los switches. Con OpenFlow se pueden asignar los recursos físicos para cada una de las virtualizaciones a través de tablas de flujo segmentadas, por lo que ha este enfoque es llamada enfoque de red virtual segmentado. Actualmente existen varias herramientas para el enfoque anteriormente mencionado los cuales están disponibles como, FlowVisor, OpenVirtex y FlowN. Al utilizar este enfoque basado en segmentos se soluciona la parte de la sobrecarga de los túneles, así mismo, proporciona un mejor nivel de control para la parte de calidad y nivel de servicio en el tráfico de red. El principal problema que se presenta con la implementar SDN y Virtualización es que se requiere un infraestructura de red basada en OpenFlow (Han et al., 2016).

2.7 Estudios Previos

En base a la revisión de la literatura, a continuación, se presentan estudios previos relacionados con el tema de esta investigación.

2.7.1 Universidad de Guadalajara y SDN

La nueva dorsal de telecomunicaciones la Universidad de Guadalajara ha comenzado la implementación de funcionalidades con SDN, ya que los equipos cuentan con circuitos integrados programables (FPGAs, similares a las aplicaciones de los ASICs) que son lo suficientemente sofisticados para reconocer diferentes tipos de paquetes y tratarlos de forma diferente. Con la finalización de la primera etapa de implementación de SDN en la red de comunicaciones universitaria, permite el fortalecimiento e innovación de la red por medio de OpenFlow, ofreciendo al administrador de red la capacidad de controlar los flujos de tráfico de manera dinámica, desde una consola centralizada (web) sin tener que tocar los switches en lo individual, cambiar cualquier regla de los switches cuando sea necesario agregando o quitando prioridad, o hasta bloquear tipos específicos de paquetes con un nivel de control muy detallado por medio de APIs de programación, disponibles en plataformas como OpenDayLight, (Ipv6.udg.mx, 2016).

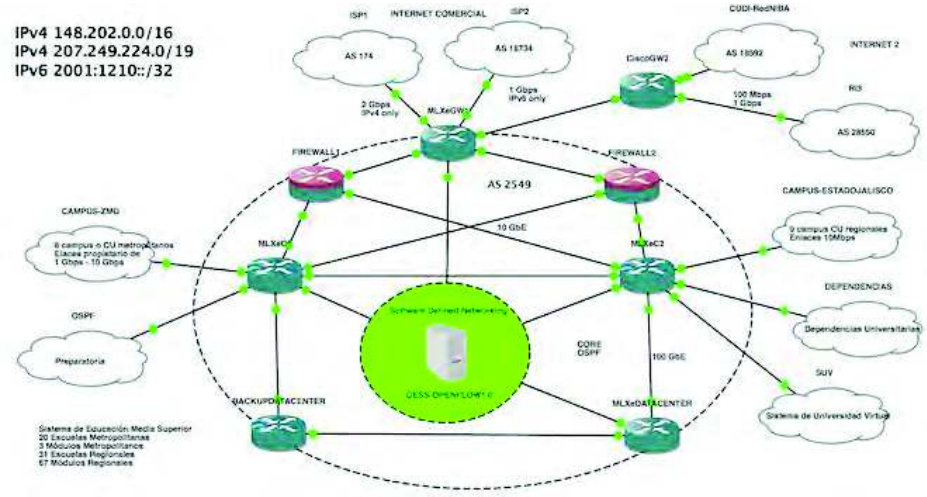


Figura 2.4 *Ruteo utilizando SDN* (Ipv6.udg.mx)

2.7.2 GEANT

GEANT está introduciendo las capacidades de SDN en su infraestructura principal para un servicio de ancho de banda bajo demanda (BoD). Este servicio utiliza el

DynPaC Framework como se muestra en la figura 2.5, el cual ofrece ingeniería de trafico dinámico y adaptable utilizando el cálculo de enrutamiento. DynPaC proporciona un uso eficiente de las capacidades de la red, así como flexibilidad en el caso de fallas en los enlaces, teniendo tiempos de recuperación de errores más rápidos, como una reducción de costos operativos y una mejora significativa en la supervisión y monitoreo de la red, recopilando la información. El administrador de servicios DynPaC actúa como un coordinador de las interacciones entre los otros módulos del Framework mencionado y supervisando los eventos para determinar cómo reaccionar, utilizando movimiento de flujos a rutas alternativas resultando en resiliencia y recuperación de fallas (Opendaylight.org, 2016).

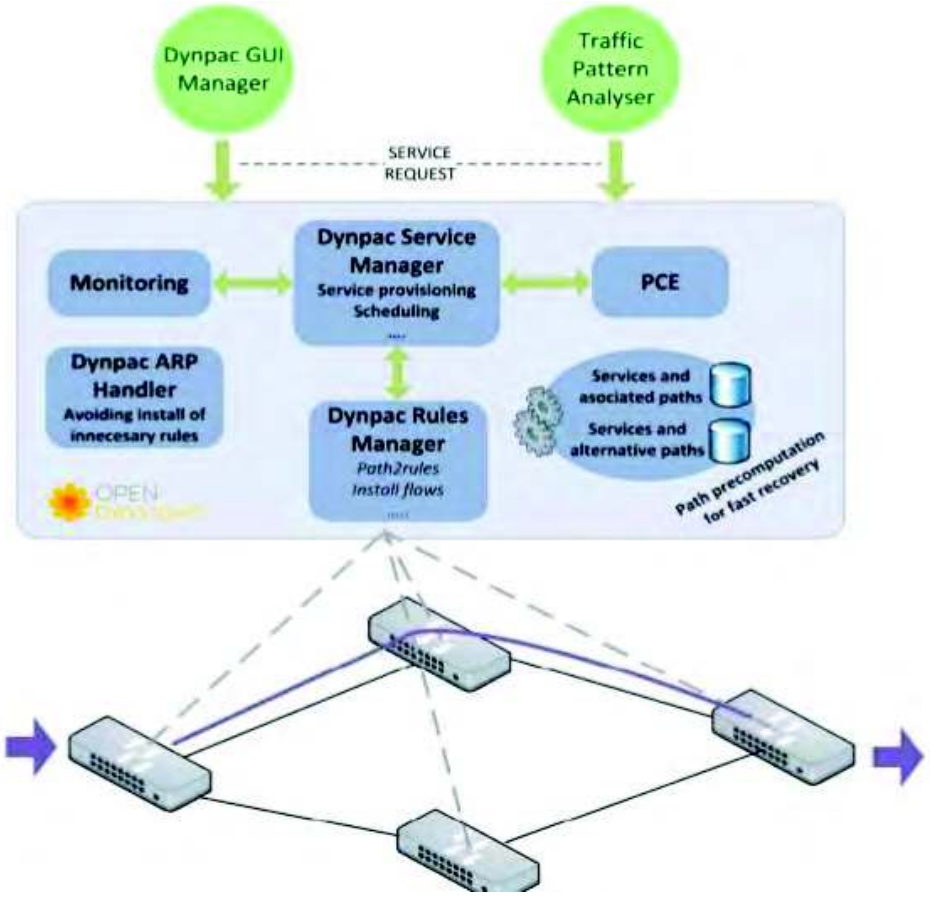


Figura 2.5 *DynPaC Framework* (Opendaylight.org, 2016)

3 PROCEDIMIENTO

En este capítulo se presenta un procedimiento creado para aprovechar de la infraestructura de red, identificar las necesidades de adecuaciones y mejoras para la optimización del flujo de información dentro de la organización, así como el mejoramiento del servicio que se brinda a los usuarios en general. Como se puede observar la figura 3.1, el procedimiento consta de 5 fases, donde se comienza con el análisis de la situación actual de la organización para conocer el equipamiento de infraestructura con el que cuenta, así como lo servicios de interconectividad que utiliza. Después se realizará las adecuaciones para la implementación de una arquitectura de SDN, en el caso de que la infraestructura de red actual de la organización no cuente con los requerimientos mínimos necesario para la implementación de SDN, se realiza la fase 3 la cual tiene como objetivo realizar las adecuaciones y reestructuraciones a la red actual, también realizar propuestas económicas y operativas de los requerimientos para cumplir la meta de la implementación de SDN, si las propuestas son aceptadas y se adquieren lo necesario se procede a realizar las actividades de la fase 2, si el caso por cuestiones técnicas y presupuestales no se cuenta con lo necesario para realizar la arquitectura de SDN, se procederá a realizar la fase 4, en la cual se optimizará los recursos y la infraestructura actual para reestructurar el esquema y funcionamiento con el fin de resolver las problemáticas planteadas. Según sea el caso, implementar la arquitectura SDN o la optimización de la infraestructura actual, se probó en un sitio de bajo impacto definido por la organización en el caso de no tener uno definido se procederá a realizar la implementación de la solución de manera general.

Figura 3.1 *Procedimiento para el aprovechamiento de la infraestructura de red*

A continuación, se explica detalladamente cada una de las fases del procedimiento, para entender cada uno de los pasos a seguir, así como el resultado de cada una de ellas.

3.1 Análisis de la situación actual

El objetivo de esta fase es analizar de manera inicial la organización de los sitios de red, así como los recursos (equipamiento de red), así mismo tener un panorama de la situación con respecto a las solicitudes que han sido generadas en un intervalo de tiempo, para tener un punto de referencia al momento de evaluar la implementación de la solución propuesta (véase en figura 3.2).

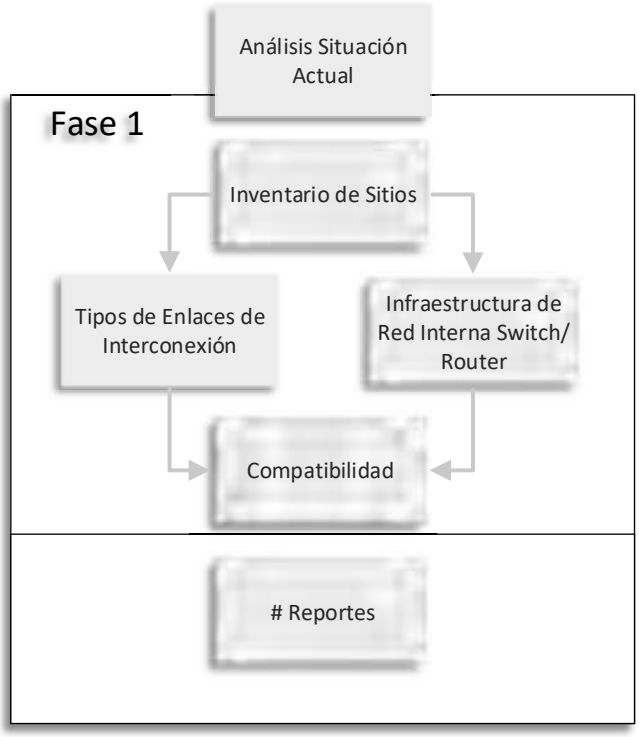


Figura 3.2 *Fase 1: Análisis de la situación actual.*

Fase 1: Análisis de la situación actual de la organización.

- Sitios de red: Definición de espacio físico (edificación/domicilio) donde se encuentra concentrado el equipamiento de red, tanto equipo de infraestructura como servidores.
- Enlaces de interconexión: Anchos de banda, proveedores, equipamiento y protocolos de ruteo, relacionados con los servicios de Internet o de red LAN de la organización, utilizados para la interconexión con uno o más sitios.

- Equipamiento de red: Equipamiento de infraestructura de telecomunicaciones y de servidores, involucrado directamente en las actividades del sitio en estudio.
- Compatibilidad: Revisión exhaustiva de cada uno de los equipos anteriormente mencionados, con el fin de verificar si cuentan con la posibilidad de utilizar el protocolo de OpenFlow, el cual es pieza importante para el desarrollo de la arquitectura de SDN.
- Solicitudes de servicios y/o correcciones: Se refiere a la cantidad de eventos registrados que implicaron alguna modificación en el equipamiento de red, lo cual puede ser capturado en un sistema especializado para HelpDesk o bien hoja de cálculo o cualquier método que utilice la organización para el registro de reportes de fallas o solicitudes de servicios, correspondientes al área de redes de telecomunicaciones.

Productos esperados al finalizar la fase:

- Base de Datos de sitios
    - Dirección/Domicilio
    - Cantidad de usuarios concurrentes
    - Cantidad de enlaces de interconexiones
    - Anchos de banda de los enlaces
    - Equipamiento de infraestructura de red asociado
- Base de Datos de Equipamiento
    - Tipo de equipo (Router/Switch/Punto de Acceso)
    - Marca
    - Modelo
    - Propósito de uso
    - Cantidad de usuarios a los que brinda servicio
    - Subnet/Vlan (Direccionamiento y propósito)

3.2 Solución y Pruebas de SDN

En esta fase se realizará el estudio a fondo sobre las diferentes plataformas disponibles para realizar una arquitectura de SDN, así mismo se trabaja a detalle por separado en las siguientes áreas que le compete al tema de SDN: Controlador, Seguridad, Virtualización y Aplicativos, lo anterior con el fin de tener el dominio del tema y la selección de herramientas que más se adecuan a las necesidades de la organización como se puede observar en la figura 3.3.

Se realizará la simulación mediante software para comprender el funcionamiento de la arquitectura y realizar los ajustes que sean necesarios para trasladarlo a un ambiente de pruebas real, antes de una implementación de producción.

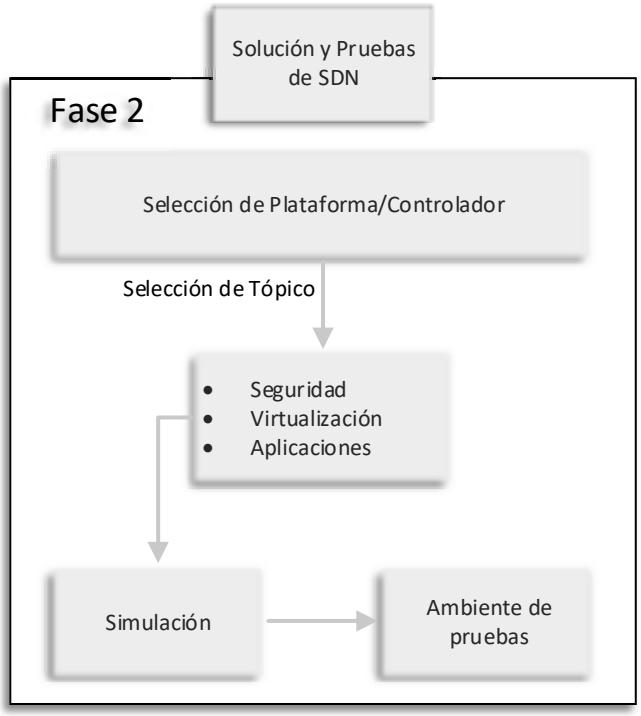


Figura 3.3 *Fase 2: Solución y Pruebas de SDN*

Fase 2: Solución y Pruebas de SDN:

- Selección de plataforma de SDN: Se refiere de elegir la plataforma de SDN a utilizar, basándose en los estudios previos y literatura, dependiendo del objetivo que se quiere alcanzar con la implementación de SDN.
- Tópico a desarrollar: Se tiene que seleccionar uno o más de los propósitos para los que se utilizará SDN.
- Simulación: Utilizar una plataforma de simulación (software) seleccionada después de la investigación literaria y probar el esquema propuesto, tratando de aproximar lo más posible el ambiente a la realidad. Se recomienda la utilización de la plataforma de simulación de redes GNS3, ya que permite crear ambientes con distintos controladores de SDN, como se muestran en las figuras 3.4,3.5 y 3.6.

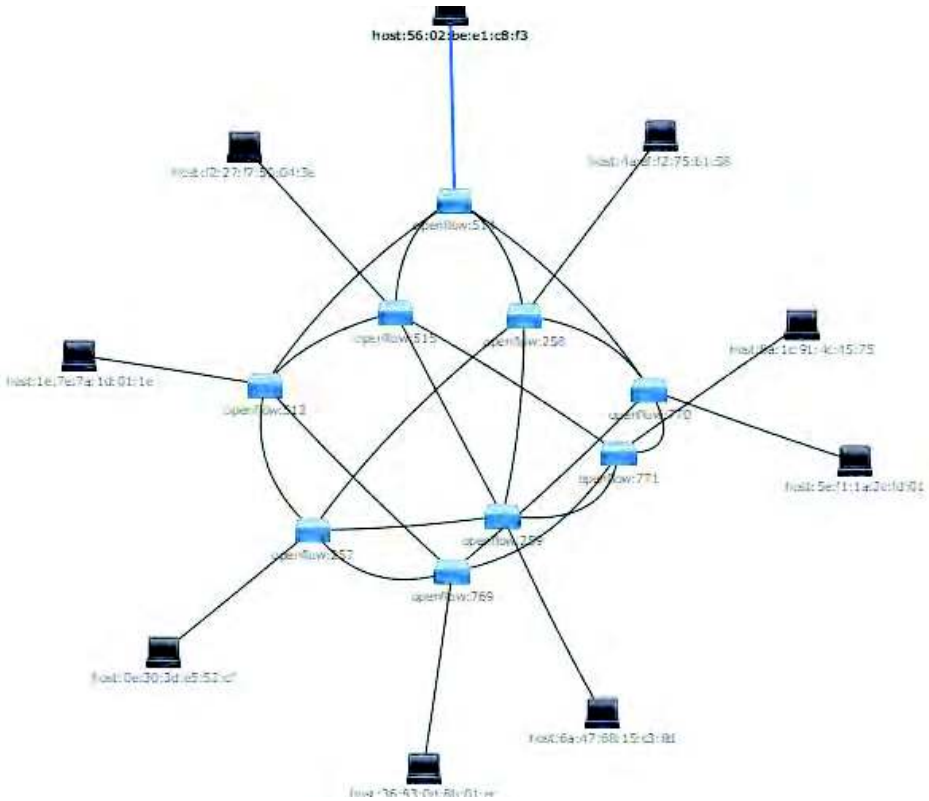


Figura 3.4 *Simulación utilizando OpenDaylight* (Gns3.com, 2017)

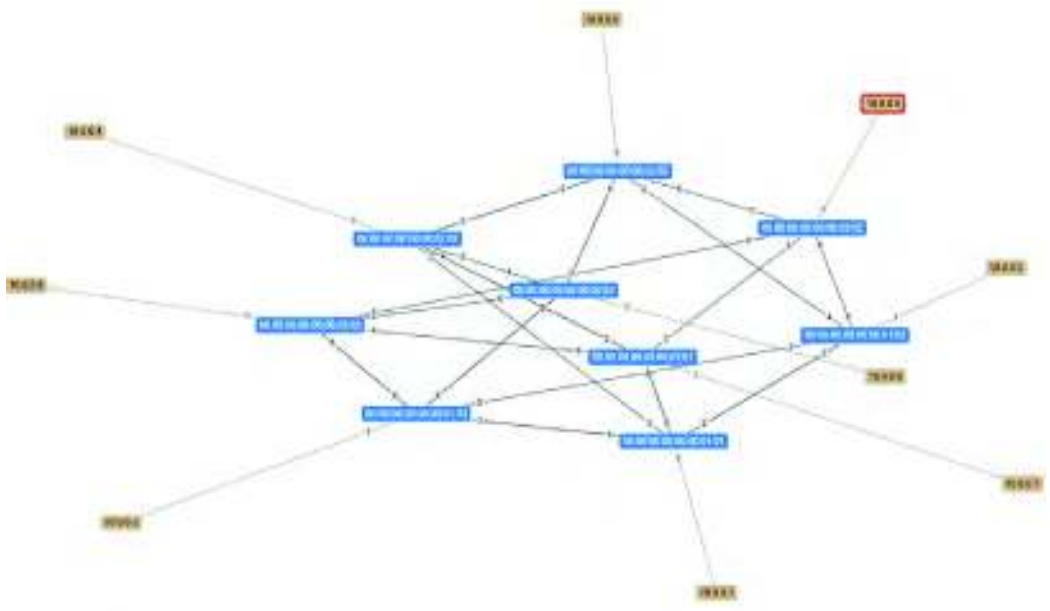


Figura 3.5 *Simulación utilizando HP VAN* (Gns3.com, 2017)

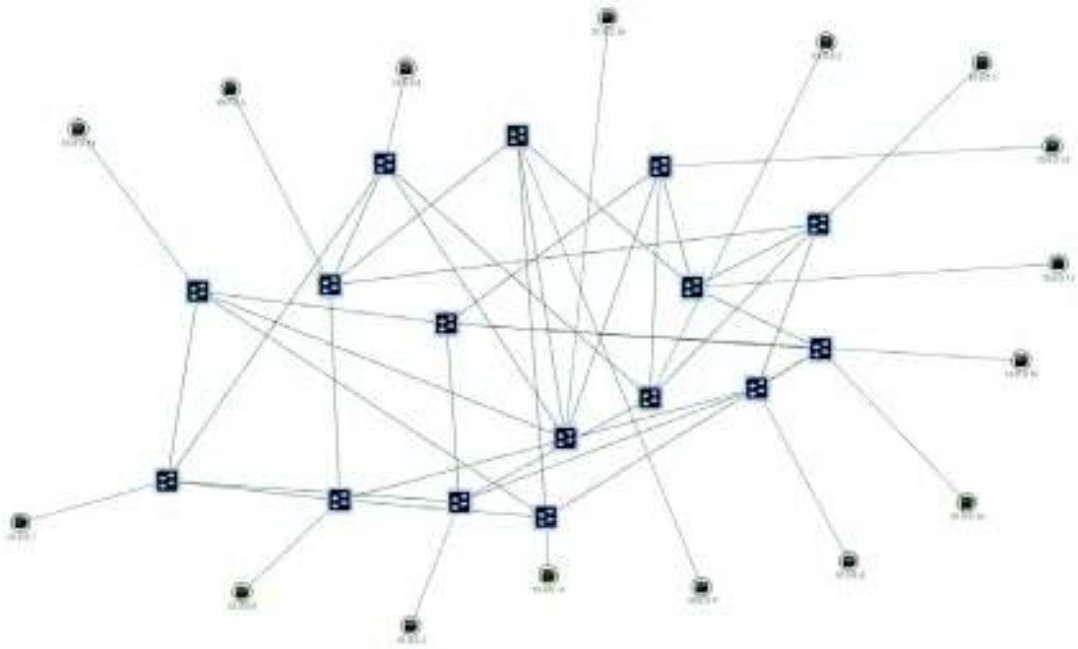


Figura 3.6 *Simulación utilizando ONOS* (Gns3.com, 2017)

- Ambiente de pruebas: Realizar pruebas de laboratorio con el equipamiento (modelos y marcas) de la organización, a partir del modelo resultante de la simulación.

Productos esperados al finalizar la fase:

- Comparativo y selección de plataforma de SDN a utilizar.
- Criterios para realizar la propuesta:
    - Selección de controlador y protocolos de conexión
    - Definición de aplicaciones para aplicar calidad de servicio
    - Definir herramientas o complementos de seguridad para fortalecer la arquitectura centralizada propuesta
- Reporte de datos generado con el software de simulación para ver el ambiente real y la nueva arquitectura (latencia/Ruteo dinámico).
- Reporte en ambiente de pruebas con infraestructura de equipo activo.

3.3 Estudio Económico y Requerimientos

Esta fase es presentar el panorama de la situación actual a la Dirección, mediante diagramas y propuestas de mejora utilizando la infraestructura existente. También se realizará una propuesta económica en el caso de requerir equipamiento o servicios nuevos para la optimización de la red lo cual sea compatible con una arquitectura SDN o HDN.

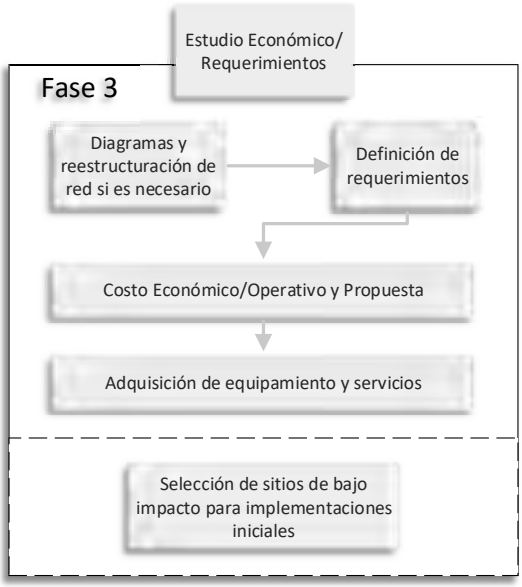


Figura 3.7 *Fase 3: Estudio Económico/Requerimientos*

Fase 3: Estudios económicos y de requerimientos técnicos para una implementación de SDN u optimizar la arquitectura existente.

- Diseños y diagramas: Análisis de la situación actual con respecto a la topología de red y el rediseño si es necesario para adecuarlo a la arquitectura de SDN.
- Definición de requerimientos: Se refiere a los cambios de topologías, equipamiento, servicios de interconexión, necesarios para la mejora y optimización de la red actual. Dependiendo el equipamiento que se requiera, como, por ejemplo: equipos de Telefonía IP, switches, puntos de acceso inalámbrico, entre otros. Se puede utilizar una compañía que se dedica evaluar equipamiento de tecnología como lo es Gartner. A continuación, se muestra la representación gráfica de la evaluación en la figura 3.8:

Figura 3.8 *Cuadrante de Gartner de Firewall tipo empresarial* (gartner.com, 2017)

- Costo económico y operativos: Se describen los aspectos monetarios y de labores extraordinarias, definidas en el punto anterior (requerimientos).
- Adquisición de equipamientos y servicios: se refiere a la adquisición de los equipos y servicios propuestos para el desarrollo de una implementación de SDN.
- Definición de prioridad de los sitios: Análisis de cada uno de los sitios con respecto a la cantidad de personas involucradas, así como las actividades que realizan con el fin de definir prioridad y niveles entre los sitios, para conocer el impacto en el caso de realizar una implementación donde no se obtengan los resultados esperados y se requiera un rediseño y ajustes.

Productos esperados al finalizar la fase:

- Rediseño de arquitectura de red (Diagramas/Ruta crítica):
  - Definición y organización de direccionamiento IP (información confidencial para la empresa)
  - Definición de requerimientos de equipamiento para cada oficina con respecto a los servicios y usuarios concurrentes (dimensionamiento del hardware/equipamiento de infraestructura que soporte la demanda de usuarios)
  - Definición de anchos de banda por oficina con respecto a la demanda de usuarios y las actividades del sitio en estudio.
- Reporte Económico de gastos generados por los cambios de arquitectura y equipamiento necesarios para optimizar los servicios (Cotizaciones/tablas comparativas/anexos).
- Definición de prioridad/impacto de cada sitio con relación de la cantidad de usuarios y la carga de trabajo.

3.4 Optimización de Infraestructura Existente

El objetivo de esta fase es realizar una propuesta de optimización de recursos y equipamiento actual. En caso de que no se tenga lo necesario para efectuar un proyecto de arquitectura de SDN, se puede realizar una reestructura tomando los problemas de más impacto, para después simular una solución que pueda ser implementada en un ambiente real.

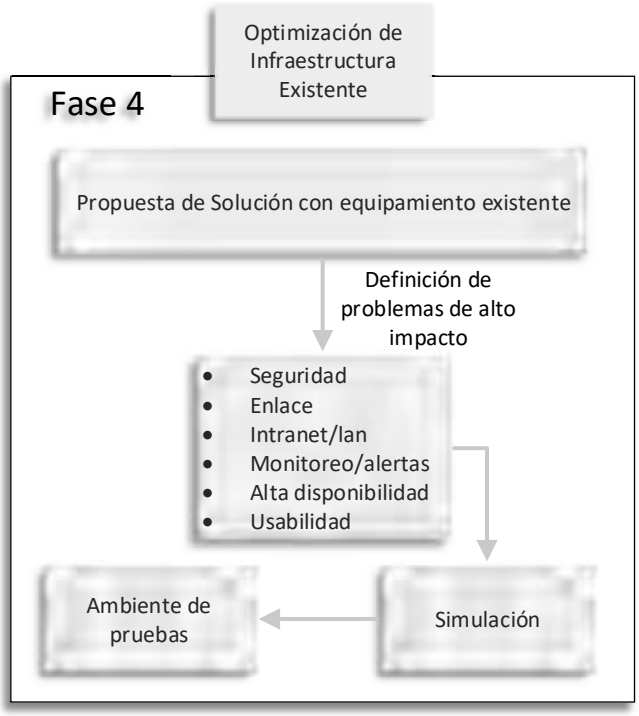


Figura 3.9 *Fase 4: Optimización de Infraestructura Existente*

Fase 4: Optimización de infraestructura existente:

- Propuesta de solución: Se refiere a la verificación a detalle del equipo existente, para investigar sus funcionalidades y recursos que sean capaces para de resolver los problemas planteados y así tener una solución integral con el objetivo de automatizar las operaciones de la red de telecomunicaciones.
- Definición de problemas de alto Impacto: Es identificar las problemáticas que se puedan clasificar en los tópicos descritos, ya que cada uno de ellos pertenece a funcionalidades específicas de un tipo de equipamiento de red.
- Simulación: Utilizar una plataforma de simulación (software) seleccionada después de la investigación literaria y probar el esquema seleccionado, tratando de aproximar lo más posible el ambiente a la realidad.
- Ambiente de pruebas: Realizar pruebas de laboratorio con el equipamiento (modelos y marcas) de la organización, a partir del modelo resultante de la simulación.

3.5 Implementación de solución y verificación de resultados

El objetivo de esta fase es poner en marcha la solución propuesta y poder verificar el funcionamiento, para realizar los ajustes en el caso de ser necesario. También tienen como objetivo validar si la solución propuesta, mejoró la problemática planteada y en qué nivel fue la mejora.

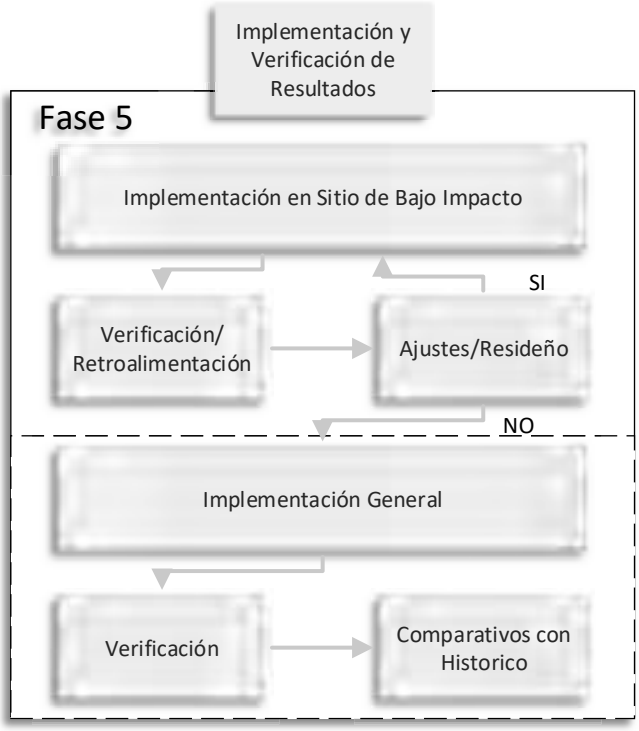


Figura 3.10 *Fase 5: Implementación y Verificación Resultados*

Fase 5: Implementación y verificación de resultados:

- Sitio de bajo impacto: Se refiere a las pruebas físicas, previas a realizarlas en un ambiente real, las cuales son ejecutadas en un sitio de bajo impacto, para tomar en cuenta todas las variables que puedan surgir y comprobar el comportamiento de nuestra propuesta.
- Verificación y retroalimentación: Comprobar si la implementación no realizo una afectación negativa o bien si se puede realizar mejoras al modelo.

- Ajuste y rediseño: Se refiere a realizar los ajustes, resultantes de la verificación y comprobarlo de nuevo dentro en el ambiente real.
- Implementación general: Implementar el modelo resultante de las pruebas en el sitio de bajo impacto.
- Verificación: Recolectar la información del modelo implementado.
- Comparativo: Realizar un comparativo de los resultados y el número de solicitudes de servicio, así como los eventos anómalos presentados con respecto al histórico previo a la implementación.

4 IMPLEMENTACIÓN

En este capítulo se presenta el desarrollo y la implementación del procedimiento propuesto en el capítulo anterior, el cual fue aplicado en la Dirección de Sistemas de la Procuraduría General de Justicia del Estado.

A continuación, se detallan las actividades que se realizaron en cada una de las fases que componen el procedimiento para el aprovechamiento de la infraestructura de red de la organización.

4.1 Análisis de la situación actual de la organización

En esta fase inicial de la implementación, se realiza un estudio a fondo de la situación actual de la organización, pero desde una perspectiva técnica y de funcionalidad de su esquema de red, con el fin de optimizar lo existente o realizar una reestructuración general de toda la infraestructura.

4.1.1 Inventario de sitios

Al realizar el estudio de los sitios se decidió trabajar en un total de 56 unidades administrativas distribuidas a lo largo de Estado de Sonora en un total de 24 municipios, ya que son las que cuentan con un equipamiento similar y se podría realizar una configuración estándar para cada una de ellas, las cuales tienen servicios y funciones diferentes dependiendo el tipo de unidad administrativa, las cuales se enlistan a continuación:

- Agencia adscrita al juzgado mixto
- Agencia adscrita al juzgado primero de lo penal
- Agencia adscrita al juzgado segundo de lo penal
- Agencia adscrita al juzgado tercero de lo penal
- Agencia especializada en delitos
- Agencia especializada en delitos de abigeatos
- Agencia especializada en delitos de querella y tránsito

- Agencia especializada en procuración de justicia para adolecentes
- Agencia Investigadora del Ministerio Público
- Agencia Investigadora del Ministerio Público especializada en delitos sexuales
- Agencia Investigadora del Ministerio Público Sector I
- Agencia Investigadora del Ministerio Público Sector II
- Agencia Mixta
- Agencia primera del Ministerio Público especializada en delitos ocasionado por el tránsito de vehículos
- Delegación regional
- Centro de atención temprana
- Centro integral de procuración de justicia

La mayoría de los tipos de unidades administrativos anteriormente mencionadas comparten una función en común, lo cual es realizar una replicar de la información capturada resultantes de las actividades propias de la unidad administrativa.

4.1.2 Tipos de enlaces de interconexión de las unidades administrativas

Los enlaces de interconexión hacen referencia a como una unidad administrativa accede al centro de operaciones de red (COR) ubicado en el edificio de la PGJE, al realizar la investigación se identificaron tipos de enlaces, proveedores y anchos de bandas, así mismo se identificó un enlace otorgado por el centro de control, comando, comunicación y cómputo (C4) el cual simula una interconexión LAN en una escala Estatal. A continuación, se describen todas las variaciones de conexión que se presentaron entre una UA y el COR:

- Tipos y anchos de banda de los enlaces
    - Simétricos de 20 Mbps, 50 Mbps y 100 Mbps
    - Asimétricos de 1 Mbps, 2 Mbps, 5 Mbps, 10 Mbps y 100 Mbps
- Proveedores
    - ISP Iusacel (Enlace TP)

- ISP Megacable (Metrocarrier)
- ISP Telmex
- C4 (gubernamental)

Los enlaces de ISP que son utilizados para realizar conexiones directas a los servidores tanto de sistemas informáticos como los de bases de datos, son realizados mediante una conexión segura de una red privada virtual VPN (virtual private network) véase en la figura 4.1, en los casos de C4 es una conexión directa, ya que los servicios prioritarios de la organización no son visibles desde el ámbito público (Internet) véase en figura 4.2.

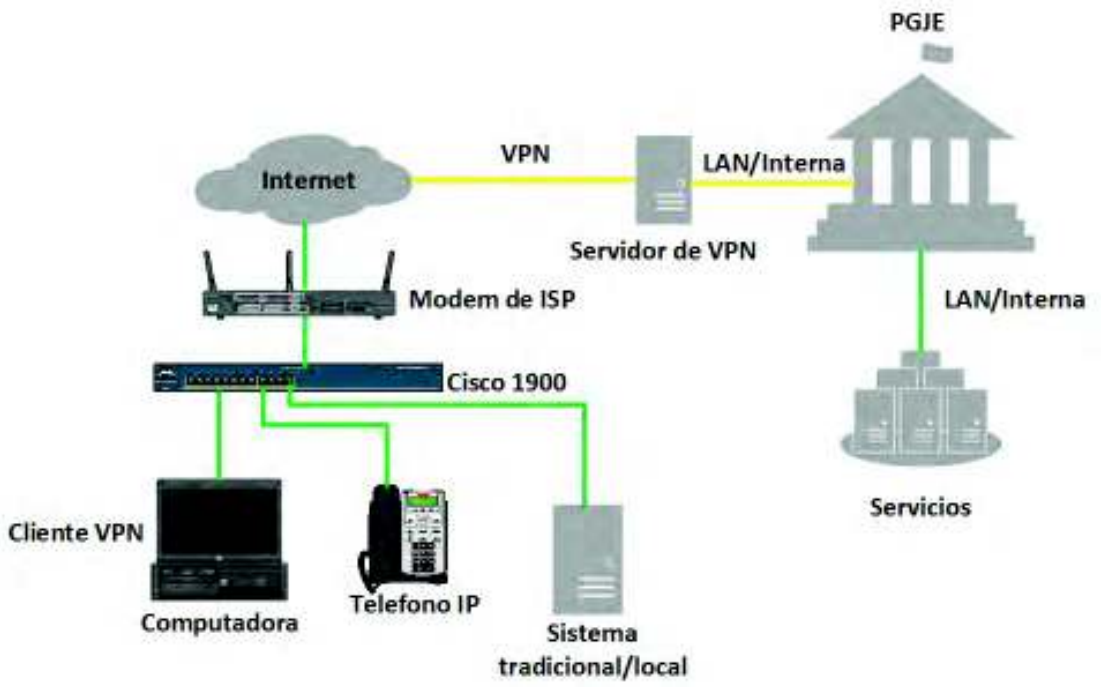


Figura 4.1 *Unidad Administrativa conectada por VPN*

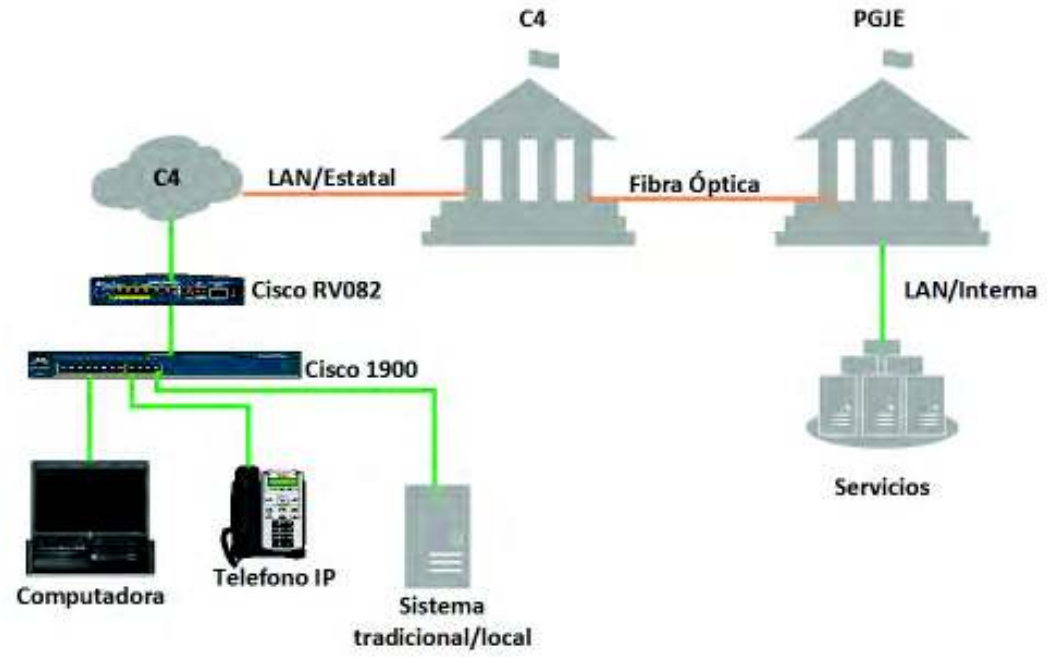


Figura 4.2 *Unidad Administrativa conectada a la PGJE mediante C4*

4.1.3 Inventario de infraestructura de red interna

Se realizó un inventario del equipamiento involucrado en la infraestructura de red, donde se dividió en el equipamiento instalado del COR ubicado en la PGJE y por cada unidad administrativa. Se encontró que en las unidades administrativas contaban con un equipo router cisco RV082 y un switch cisco catalyst 1900, este último solo está en las UA que la población de usuarios concurrentes es mayor a 7, ya que sobrepasa la capacidad de interfaces ethernet disponibles en el cisco RV082 véase a detalles y por UA en el anexo 1. Por otro lado, con respecto al equipamiento instalado dentro de la PGJE, existe una serie de equipamiento cisco, 3com, mikrotik, entre otros, los cuales en su mayoría es obsoleto. También se tiene un equipamiento de red de alto nivel de otros proyectos de las marcas: HPE y Fortinet, el cual no está en operación por falta de configuración y un proyecto para darle una funcionalidad.

4.1.4 Compatibilidad para implementación SDN

Basados en la literatura y con el propósito de utilizar una arquitectura innovadora y más automatizada, se buscó la implementación de una solución en una plataforma de

SDN tanto en el plano de control, así como en la parte de desarrollo de aplicativos específicos, por lo que, a partir del inventario del equipamiento de la infraestructura de red, se investigó en las hojas de especificaciones de cada uno para saber si contaban con la funcionalidad del protocolo de OpenFlow, por lo que el resultado fue poco favorable, ya solo 2 equipos soportan en su totalidad lo que es OpenFlow, en este caso fueron 2 switches HPE FlexNetwork 7500 series que soportan OpenFlow versión 1.3 (Hpe.com, 2016). Por lo anterior y falta de recursos en equipamiento y económicos, se decidió realizar una optimización de los recursos actuales tanto financieros como del equipamiento de la organización y así resolver los problemas ya planteados, descartando la posibilidad de desarrollar una arquitectura de SDN.

4.1.5 Solicitudes de servicios o reportes de fallas

Actualmente la organización tiene personal para la atención de usuarios con respecto a reportes de fallas o solicitudes de servicios, se identificó que, en el área de soporte técnico la cual se encarga de ver el buen funcionamiento del equipo de cómputo existente o bien la instalación de equipo nuevo según sea el caso, se cuenta con un sistema para la captura de las llamadas recibidas por parte de los usuarios (empleados de la organización) sobre solicitudes de servicios o reporte de fallas. Por otro lado, el área de redes y telecomunicaciones no cuentan con un sistema para el seguimiento de los reportes de fallas o solicitudes de servicios, por lo que se le recomendó utilizar el mismo sistema que es utilizado por el área de soporte técnico. Por otro lado, se identificó que un gran número de órdenes de servicio no son cuantificables de manera inmediata, ya que las realizan de manera formal por oficio (Anexo 01) y la respuesta o atención se hace de igual forma por oficio, por lo que solo se tiene una evidencia física no clasificada de las solicitudes o reportes para un servicio, tanto del área de redes y se soporte técnico.

4.2 Solución y pruebas de SDN

Como se mencionó después de realizar el estudio de compatibilidad donde el resultado fue negativo a la implementación de una arquitectura de SDN, las características y funcionalidades del equipamiento de red utilizados por la organización no cumplen el requerimiento mínimo que es el protocolo OpenFlow, por lo anterior se decide estudiar a fondo las funcionalidades del equipamiento actual para su optimización y así dar solución a las problemáticas presentadas. Existe equipamiento adquirido para seguridad perimetral y ruteo de la marca Fortinet, el cual para la parte de controlador inalámbrico utiliza el protocolo CAPWAP el cual propone la gestión centralizada de múltiples puntos de acceso inalámbricos (AP) (Elsadek y Mikhail, 2016) y es soportado por un controlador SDN OpenDayLight (Opendaylight.org, 2016), este último es uno de los controladores más conocidos para una solución de SDN, cuando se desea realizar una solución de código abierto y sin un costo económico.

4.3 Estudio económico, diseño y requerimientos

En esta fase de implementación una vez determinado la incompatibilidad del equipamiento para una arquitectura de SDN que resuelva las problemáticas planteadas, se desarrolla un plan secundario el cual se refiere a la optimización de los recursos para explotar las funcionalidades que apoyen a la solución de las problemáticas y así mismo a la automatización de las operaciones de red, en los tópicos de: arquitectura de alta disponibilidad, interconectividad redundantes, administración de anchos de banda y automatización de procesos de red. Por lo anterior se realizaron una serie tareas y operaciones desde técnicas a económicas, las cuales son presentadas a continuación.

4.3.1 Diagrama y reestructuración de red

Al realizar el trabajo de análisis de los sitios tanto de las UA como el COR de la PGJE, se decidió hacer una propuesta de reestructuración con el fin de solventar las problemáticas planteadas, por lo que inicialmente se hizo un diagrama de la situación actual (figura 4.3) donde se puede observar falta de redundancia de interconexión, así como de un esquema de tolerancia a fallos en el equipamiento de infraestructura.

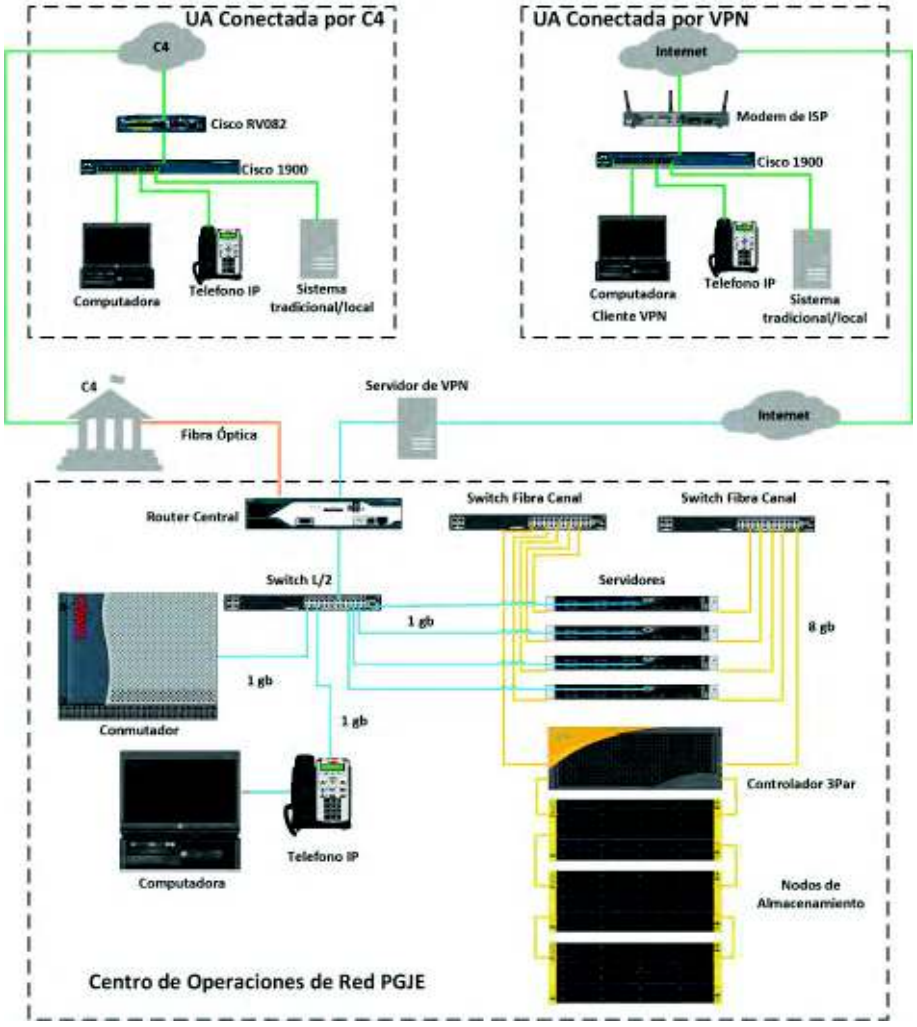


Figura 4.3 *Diagrama de red actual de la organización*

Como anteriormente se mencionó en la parte de inventario de equipo, la organización cuenta con equipamiento nuevo y que aún no está en operación como lo son los HPE Flexfabric 7503 y equipos Fortigate, así mismo se recomendó a la organización la adquisición de servicios de Internet en las diferentes UA con el fin de contar con redundancia de enlace, al tener la posibilidad de utilizar la VPN por un ISP y la conexión LAN/Estatal mediante C4, logrando un esquema de alta disponibilidad en los enlaces como se puede observar en la figura 4.4.

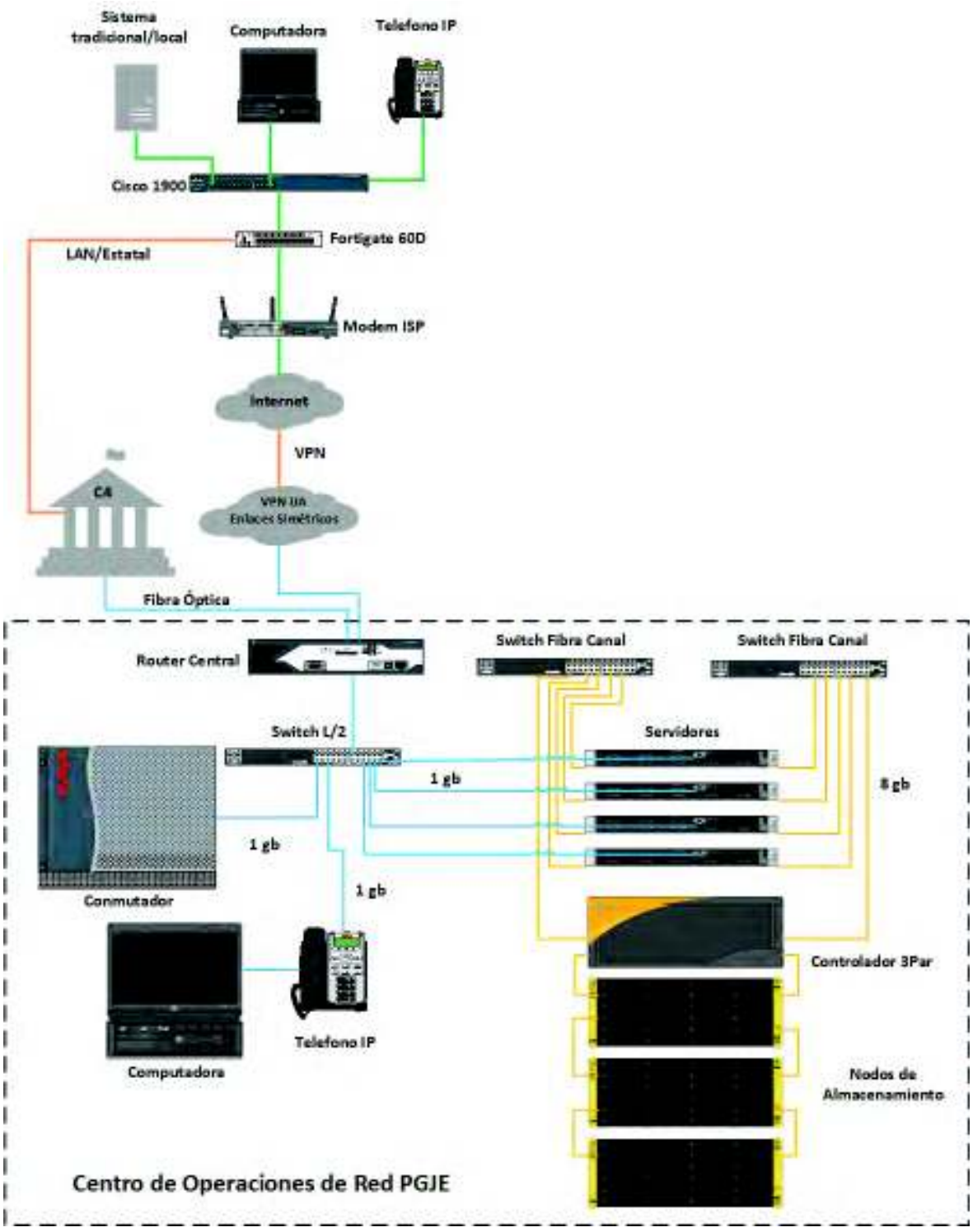


Figura 4.4 *Diagrama de red propuesto para la interconexión entre UA y COR*

4.3.2 Definición de requerimientos

Una vez realizado el diagrama propuesto para la organización, se crea un listado de requerimientos técnicos y de equipamiento para lograr dicha implementación, así mismo nuevamente se revisa el equipamiento con el que ya se cuenta para así pedir solo lo mínimo necesario, como se muestran en la tabla 4.1.

Cantidad	Equipo	Descripción
2	FG100D	Firewall central en alta disponibilidad
6	FG60D	Firewall de UA
35	FG50E	Firewall de UA
1	FG30E	Firewall de UA
6	DL360 G9	Servidores central en cluster
1	Exp 3PAR	Expansión de sistema de almacenamiento
15	FS448D	Switch para equipamiento de frontera
8	FAP221C	Punto de acceso inalámbrico para edificio central
6	Licencias	Licenciamiento de Windows Server
38	Enlace	Enlaces de Internet
4	Enlace PTP	Enlaces inalámbricos punto a punto
1	FMG400D	Consola de administración para firewall
1	FAZ400D	Servidor de recolección de información de firewall

Tabla 4.1 *Requerimientos mínimos para realizar la arquitectura propuesta*

Lo anterior es resultado de un comparativo mínimo de 3 marcas por tipo de equipamiento, utilizando varios criterios: costo, usabilidad, operatividad, funcionalidad y que cumpliera con lo necesario para el desarrollo de la arquitectura propuesta. Con respecto a los equipos de seguridad/router se eligió sobre 3 de las marcas más conocida: Palo Alto Networks, Check Point Software Technologies y Fortinet, resultado del estudio “Magic Quadrant for Enterprise Network Firewalls” publicado el 25 de mayo de 2016 (gartner.com, 2017), por cuestiones de presupuesto y facilidad de adquisición se eligió al fabricante Fortinet, aunque los 3 cumplían con los requisitos planteados de la nueva arquitectura propuesta. Por otro lado, en la parte de consola de administración, recolector de información del firewall, switches y puntos de acceso inalámbricos se optó por elegir al mismo fabricante, ya que se puede tener una solución integral y ofrece funcionalidades propietarias, para ambientes donde se usa equipamiento de la misma marca, así como una administración centralizada. El equipo

mencionado fue adquirido mediante la gestión de recursos Estatales y Federales, así como convenios con el gobierno de Estados Unidos, así mismo se realizó anexos técnicos del equipamiento como requisito para la publicación de las partidas de licitación.

Con respecto a los enlaces de Internet y con asesoría de los mismo proveedores de Internet, en este caso Telmex, Metrocarrier y Enlace TP, tomando en cuenta la cantidad de usuarios en Unidades Administrativas, se solicitaron enlaces desde 5 mb/s a 20 mb/s, con al menos una IP fija, solo en el COR de la PGJE se cuentan con al menos 2 enlaces de 100 mb/s, dedicados para realizar la interconexión con la UA, por otro lado también en el edificio mencionado se cuenta con una serie de enlaces asimétricos de 20 mb/s con el propósito de ser utilizado para la navegación de Internet de los usuarios.

4.3.3 Selección de sitio de bajo impacto

La definición de sitios fue a criterio de la organización utilizando las siguientes variables: población de usuarios, cantidad de información o casos capturados en promedio, tipo de agencia o delitos. Por lo anterior se eligió a la agencia ubicada dentro del Hospital General del Estado, ya que se solo captura casos de las personas que ingresan al hospital, por lo que fue el sitio autorizado por la organización para realizar la instalación inicial y así poder estar monitoreando para hacer los ajustes y modificaciones en la configuración en el caso de ser necesarios, así mismo, otro de los motivos de la selección del sitio mencionado, fue porque se encuentra en la misma ciudad sede donde se está trabajando de manera presencial lo que facilitaría en el caso de tener que trasladarse a la UA.

4.4 Optimización de infraestructura existente

Si nos encontramos en esta etapa, es porque no contamos con lo necesario para la realización de un proyecto de SDN. Por lo anterior se realiza la optimización del equipamiento actual y en el caso de haberlo adquirido y que no fue compatible con SDN, se quiere explotar las funcionalidades del equipamiento actual y el nuevo con el fin de automatizar los procesos de red, en este caso que resuelva y/o mejore la interconexión entre las UA´s y el COR, así como también mejorar una serie de aspectos de la red interna de cada UA y el COR.

4.4.1 Propuesta de solución con equipamiento existente

En esta etapa de la fase 4 y al no contar con lo necesario para la implementación de SDN, se realiza un estudio a fondo de los equipos descritos en el inventario de equipamiento de la organización, para ver las funcionalidades y características que se pueden explotar de los mismos, nos apoyamos en las hojas técnicas de cada uno, así como en la documentación de manuales de configuración y de esquemas propuestos por cada uno de los fabricantes. Lo anterior está asociado al equipamiento, por el lado de la organización se observan los problemas de alto impacto de los siguientes temas según sean las necesidades y problemáticas a resolver en la organización:

- Seguridad: Se refiere con respectos de políticas de acceso de firewall, las cuales protegen la red interna y equipamiento. En el caso particular de la organización bajo estudio, se aumentará la protección a los servidores internos, así como la protección de los usuarios con respecto a ataques desde Internet.
- Enlaces: En este punto se estudia los enlaces de interconexión entre oficinas, en este caso entre las UA y el COR, pero también se realiza un estudio con respecto a la necesidad de navegación de Internet de la organización. Por lo que generalizando en cualquier organización se tomaría en cuenta optimizar los anchos de banda de Internet y de enlaces de interconexión según sea el caso.
- Intranet/LAN: Se realiza un inventario de la segmentación de red interna de la organización, nos referimos al direccionamiento interno y el propósito del

mismo. Por ejemplo, creación de redes exclusivas para servidores, equipamiento de infraestructura de red (router, switch, conmutadores), equipos para video vigilancia, por mencionar algunos. También dicha segmentación nos ayudaría al momento de estar realizando las políticas de seguridad, así como facilitar la administración y control a los administradores de la red.

- Monitoreo/alertas: Se refiere a desarrollar mecanismos de monitoreo de red, los cuales pueden estar asociados a software especializado para dicho propósito o bien también a rutinas o nuevos esquemas de administración del personal quien administra la red.
- Alta disponibilidad: En esta etapa según sea el giro de la organización y las prioridades de los procesos internos de la misma, se realizan esquemas de alta disponibilidad, los cuales pueden ser en servicios, equipamiento de infraestructura y servidores; en el mejor de los casos si la organización tiene actividades criticas de alto impacto o manejo de información sensible, se puede plantear la implementación de un sitio alterno en el caso de una eventualidad que tenga grandes afectaciones del COR de la organización, tener un sitio donde se esté replicando la información y tener todo lo necesario para mantener en funcionamiento las actividades prioritarias de organización.
- Usabilidad: Este punto impacta directamente a la administración y control de la red, así mismo se tiene un impacto positivo a la percepción del usuario final, quien es el que utiliza la infraestructura de red. Aquí se refiere en crear procesos automatizados que ayuden a administrar de una forma más eficiente la red, por lo que este punto está ligado a todos los demás, así mismo como es un apoyo directo a los administradores de red, tiene como resultado disminuir el tiempo de respuesta para la resolución de problemas en la red.

Al terminar de definir cada uno de los puntos anteriores y visualizando las problemáticas y el diagrama de reestructuración de red anteriormente propuesto en la Fase 3, se tiene un ajuste y nueva propuesta de arquitectura de red como se muestra en la figura 4.5.

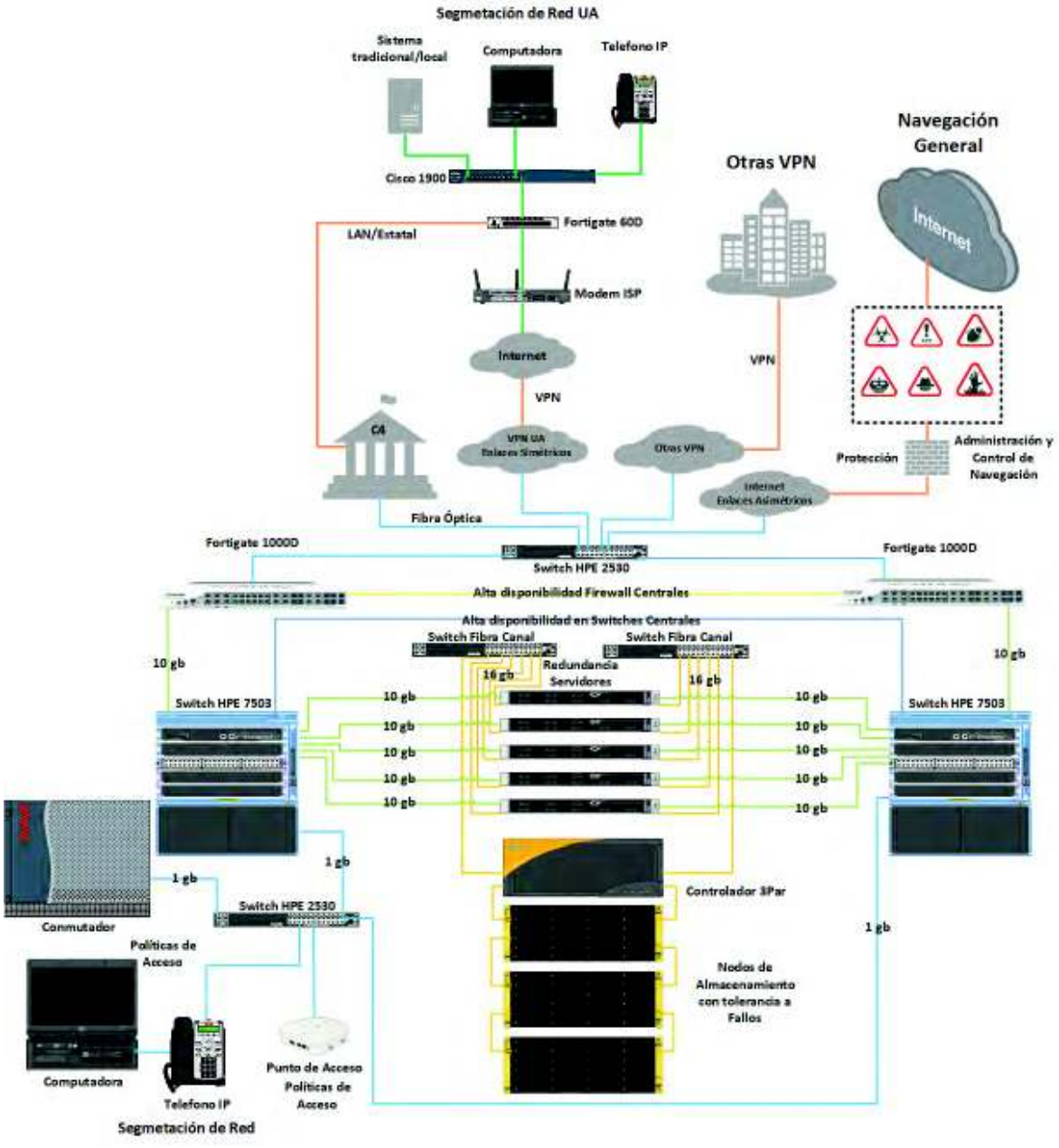


Figura 4.5 *Nueva propuesta de arquitectura de red optimizada*

4.5 Implementación de solución y verificación

En esta etapa nos encontramos con una arquitectura propuesta ya validada, según sea el caso el cual puede ser implementación de SDN o bien la optimización de la infraestructura actual, cualesquiera de las dos situaciones mencionadas comenzarán con el proceso de ajustes y modificaciones en el caso de ser requerido, así como la fase de pruebas en el sitio descrito de bajo impacto, para posteriormente realizar la instalación general en todos los sitios (Unidades Administrativas), que fueron delimitadas en el proyecto.

4.5.1 Implementación en sitio de bajo impacto

Al contar con el equipamiento y servicios solicitados para la arquitectura mencionada, se procedió realizar la instalación en el sitio piloto conocido como de bajo impacto (Hospital General del Estado). La primera fase de dicha fase fue realizar la interconexión entre la UA y el edificio de la PGJE, por lo que aprovechando la conectividad que se obtuvo con el servicio contratado de enlace de Internet, se procedió a realizar una conexión de VPN punto a punto (Site to Site) entre los equipos los equipos Fortinet adquiridos como se muestra en la figura 4.6, lo cual es muy sencillo utilizando el asistente, como se muestra en la figura 4.7.

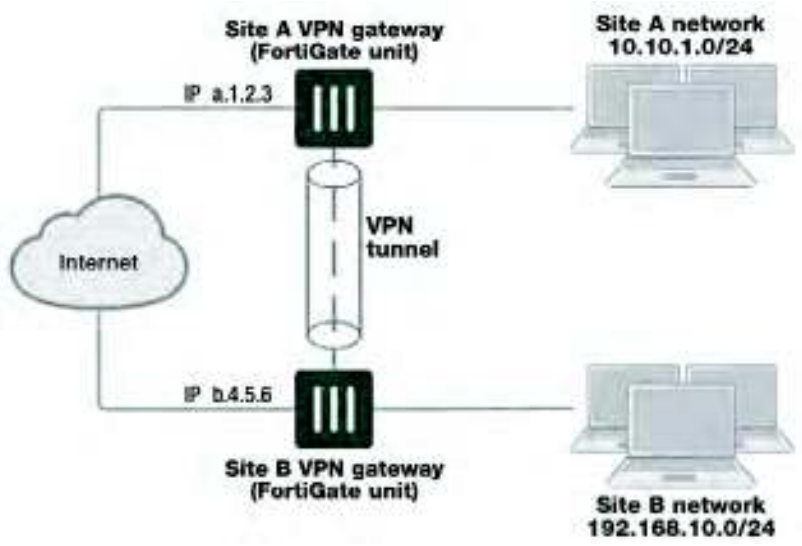


Figura 4.6 *VPN "site to site" entre equipos Fortigate*

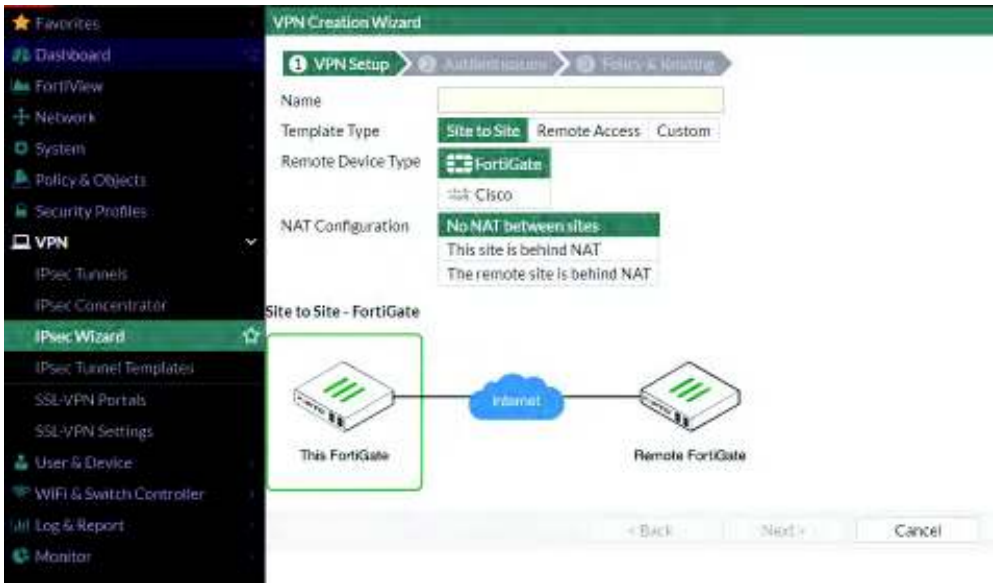


Figura 4.7 *Paso 1: creación de VPN sitio a sitio utilizando el asistente*

Como se puede observar en la figura 4.7, el primer paso para la creación del túnel de VPN consiste en otorgarle un nombre a dicho túnel, si se quiere utilizar una plantilla de configuración predeterminada por el equipo, así como el tipo de equipo con el que va a realizarle el túnel y por ultimo si va tener alguna configuración de NAT (Network Address Translation); lo anterior es para hacer una conexión trasparente entre los sitios pero al mismo tiempo realizando una conexión segura entre los mismo. En el paso 2 como se muestra en la figura 4.8, se determinar una serie de parámetros como la dirección IP del equipo remoto con el cual se va a conectar o bien esta la posibilidad de realizarlo por nombre, mediante un registro de DNS dinámico en el caso que en el sitio el proveedor de Internet no otorgue una dirección IP fija, en este caso se cuenta con un direccionamiento de IP fijo contratado, pero en la fase de monitoreo se observó que aún descrito en la contratación del servicio como IP fija, estaba cambiando y fue notificado a la brevedad con el proveedor de Internet, no se recibió una respuesta satisfactoria y por cuestiones de tiempo se decidió realizarlo con registro de nombre dinámico el cual es un servicio prestado por Fortinet por lo que no genera un costo adicional a la solución como se muestra en la figura 4.9; por último se selecciona la interface por donde está la conexión de Internet por donde se realizará la conexión de

VPN, así como si utilizaremos un clave compartida entre equipos para realizar la conexión o bien un certificado que autentifique la conexión entre los mismo.

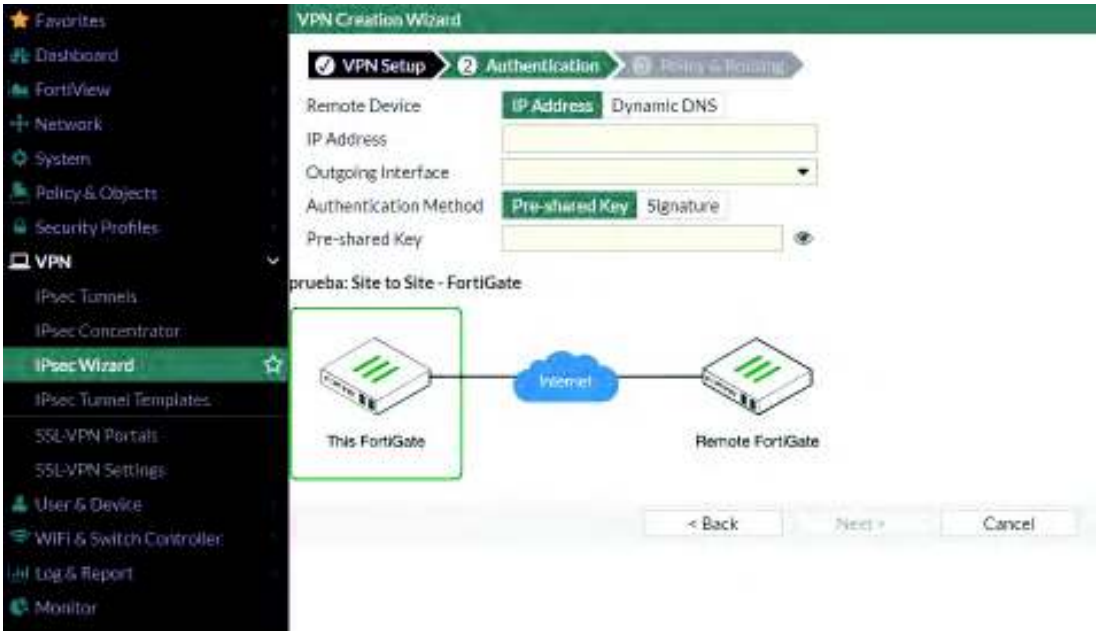


Figura 4.8 *Paso 2 creación de VPN sitio a sitio utilizando el asistente*

Figura 4.9 *Servicio de DNS dinámico de Fortinet*

Al terminar lo anterior se puede realizar las ultimas configuraciones de la VPN, las cuales son requeridas en el paso 3 como se muestra en la figura 4.10, donde prácticamente son temas de ruteo y de políticas de firewall, para indicar cuales redes en cada uno de los sitios tendrán interacción a través del túnel de VPN. Por lo que como se puede observar en la figura mencionada, se tiene que elegir la interface de la red interna de la UA o bien de la misma Procuraduría, así como también el direccionamiento IP que estará permitido realizar intercambio de información tanto local como remoto.

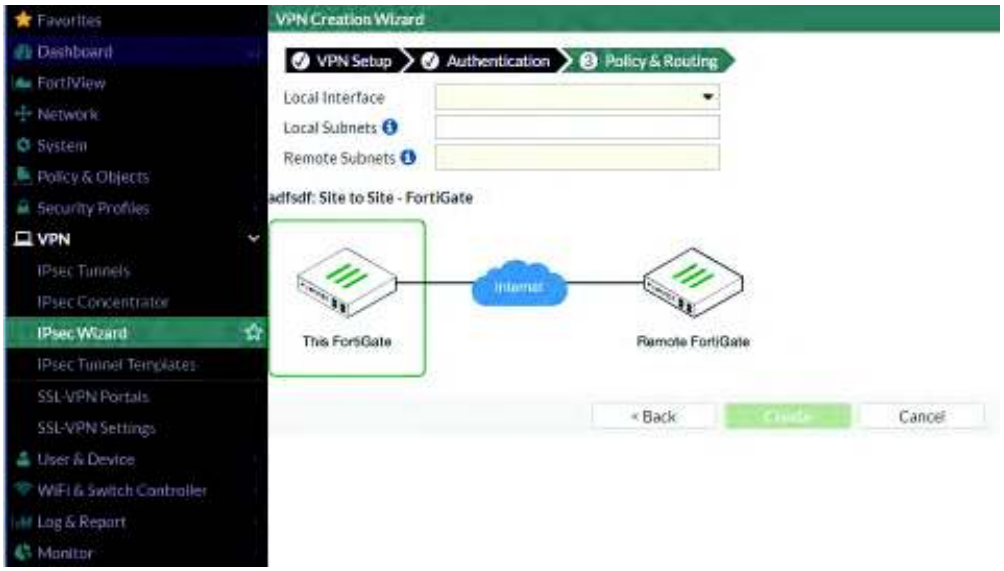


Figura 4.10 *Paso 3 creación de VPN sitio a sitio utilizando el asistente*

Una vez realizada el túnel de VPN, se realizan pruebas desde un equipo de cómputo de la UA verificando si cuentan con acceso a los sistemas correspondientes. Por otro lado, se realiza la ruta de enlace alterno por C4 utilizando ruteo estático y modificando lo que es la distancia administrativa lo cual indica cual es el enlace principal por donde se realizará la interconexión en la UA y el edificio de la Procuraduría, como se muestra en la figura 4.11.

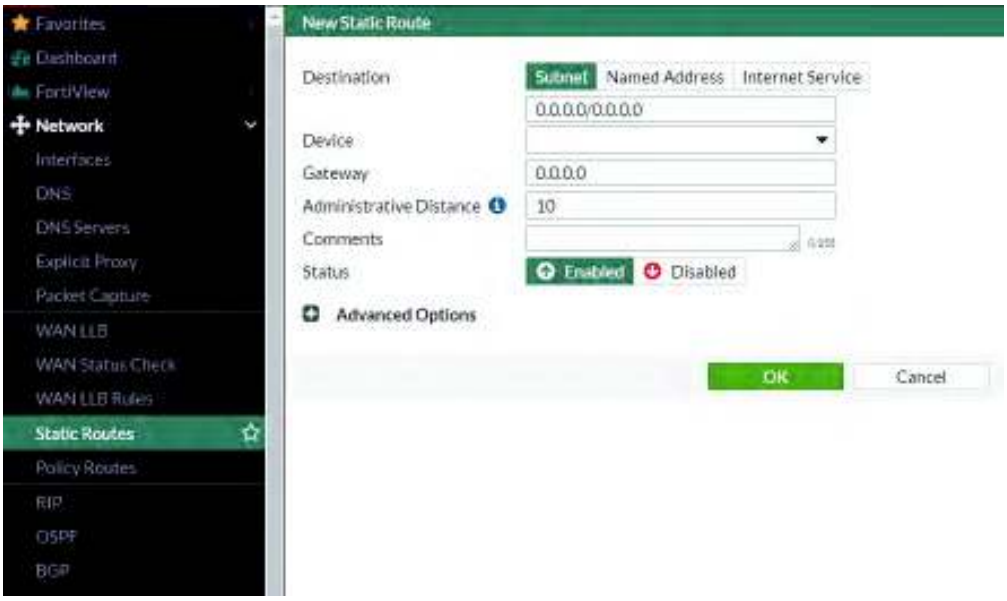


Figura 4.11 ***Configuración de ruteo definiendo distancias administrativas***

Al finalizar la parte de implementación de VPN y realizar la configuración de ruteo automatizado, se realizó una segunda un segundo túnel de VPN, ya que el Centro de Operaciones de Red ubicado en el edificio de la Procuraduría cuenta con un segundo enlace dedicado (Simétrico) y con un proveedor de Internet distinto al utilizado anteriormente en el túnel de VPN ya creado, por lo que se decidió crear un segundo túnel realizando los paso anteriormente descrito, así se aumenta la tolerancia a fallos y la alta disponibilidad en el caso de que el ISP primario falle en COR de la PGJE. Para mejorar el rendimiento de los enlaces de VPN entre las UA y el COR de la PGJE, se decidió habilitar las funciones de “Control de Aplicaciones” y el “Filtrado Web” del equipo Fortinet, ya que el mismo enlace que es utilizado para realizar la VPN es el mismo que se utiliza para el acceso a Internet, por lo que se aplicaron una serie de políticas de navegación, restringiendo una serie de categorías definidas por el mismo fabricante (Fortinet) como por ejemplo: contenido para adultos, consumo de ancho de banda, riesgo de seguridad, por mencionar algunos, dichas definiciones tanto para una aplicación, página web, virus, entre otros pueden ser consultados en la página web https://fortiguard.com como se muestra en las figuras 4.12 y 4.13.

Figura 4.12 *Barra de búsqueda de Fortiguard*

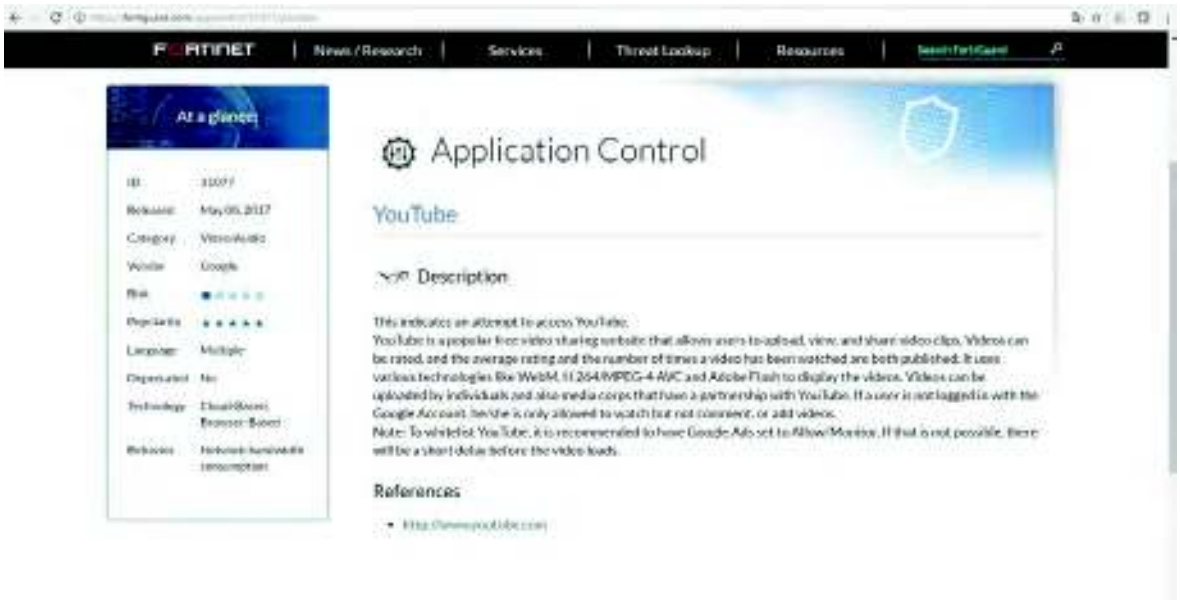


Figura 4.13 *Resultado de búsqueda en Fortiguard*

Por lo anterior, a petición del personal directivo de la PGJE se eligieron las categorías que estarían bloqueadas por defecto, solo existirán excepciones al personal que lo solicite mediante oficio y con el consentimiento del personal directivo. El filtrado web aplica a toda navegación que se haga directamente a través de un navegador web por lo que no aplica, por ejemplo: aplicación Skype, torrents, entre otros. El resultado web de la organización se ejemplifica en la figura 4.14.

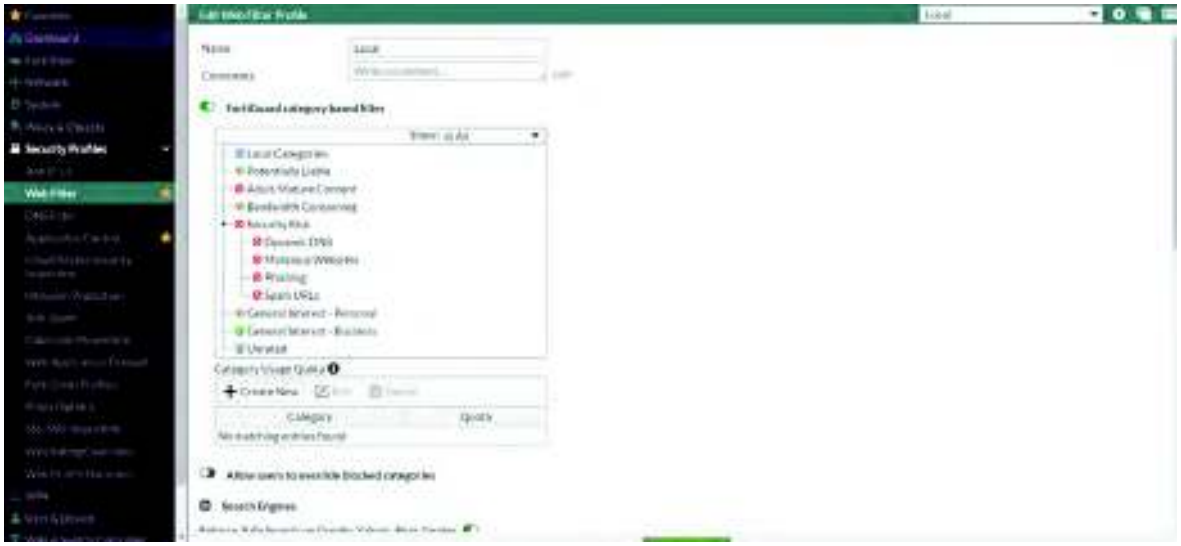


Figura 4.14 *Filtrado web por defecto de la PGJE*

En la parte de control de aplicaciones están asociado a las conexiones directas en entre la computadora y el servidor al cual se está accediendo. Se aclara lo anterior ya que, por ejemplo: si tienes permitido un filtrado web a la página de “Youtube” o “Facebook”, pero se tiene bloqueado la firma de los sitios mencionado en el perfil de Control de Aplicaciones quizás se pueda acceder al sitio web, pero en el caso de “Youtube” no se podrá reproducir ningún video. Por lo anterior se tiene que prestar atención al momento de combinar los perfiles cuando se crean las políticas de navegación de los usuarios. También se puede aprovechar en realizar bloqueos que consumen un ancho de banda considerable y no son propias de la organización como lo es con juegos, aplicaciones “P2P” (e.g. Ares, BitTorrent) y Proxy; este último utilizado normalmente para evadir los sistemas de filtrados y control de aplicaciones anteriormente mencionados. Como resultado de todo el estudio y las decisiones del

personal directivo se configuro las siguientes categorías de control de aplicaciones como se pueden observar en la figura 4.15.

Figura 4.15 *Control de aplicaciones por defecto de la PGJE*

Tanto las categorías de filtrado web y control de aplicaciones, como ya se mencionó pueden ser revisadas a fondo en la página de Fortiguard del fabricando Fortinet.

Se realizó la reestructuración de la red interna de la UA, con el fin de segmentar y aumentar el nivel de administración y seguridad de la misma como se muestra en la figura 4.16, por lo que se dividió como se describe a continuación:

- Computadoras: la red general de equipos de cómputo con direccionamiento IP dinámico (para evitar el problema de duplicado de IP).
- Equipos: direccionamiento para la administración de: firewall, switches, cámaras de video vigilancia, entre otros equipos de infraestructura de red, permitiendo solo conexiones SSH y HTTPS para su administración.
- Telefonía: creado con el fin de conectar los equipos de telefonía en un ambiente de capa 2 del modelo OSI, en este caso teléfonos IP y conmutador agilizando al momento de sincronizar los teléfonos y el conmutador.

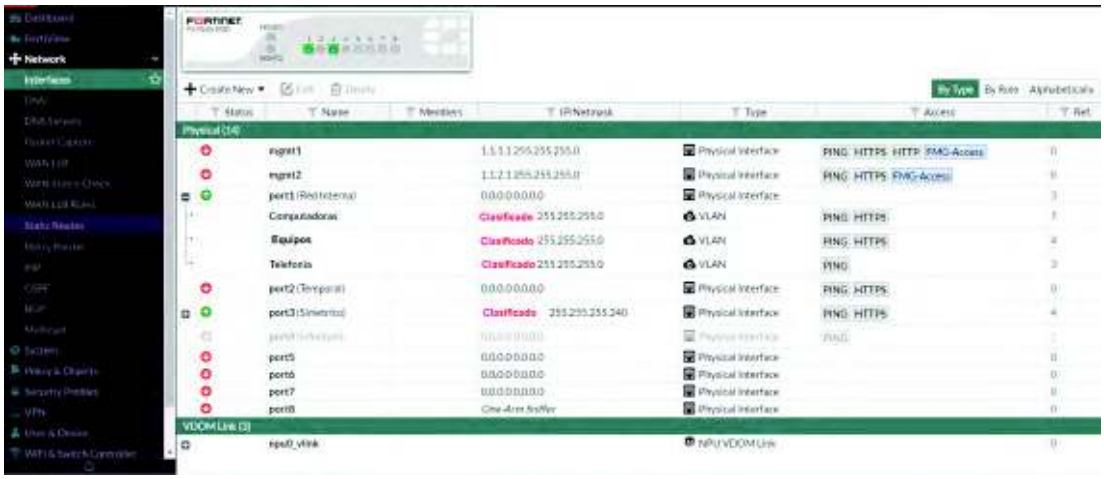


Figura 4.16 *Vlan's para la segmentación de la red*

4.5.2 Verificación y retroalimentación de implementación de sitio de bajo impacto

Al terminar el proceso de instalación en el sitio conocido como de bajo impacto en este caso el Hospital General del Estado, se mantuvo el monitoreo constante del túnel establecido de VPN. En este caso se monitoreó una semana de lunes a viernes en el horario de 8:00 a 20:00 horas en intervalos de 1 hora, para determinar la estabilidad del enlace utilizando la herramienta de monitoreo del mismo equipo Fortinet como se muestra en la figura 4.17; y así determinar si es factible replicar dicha configuración en todas las UA, que estaban proyectadas.

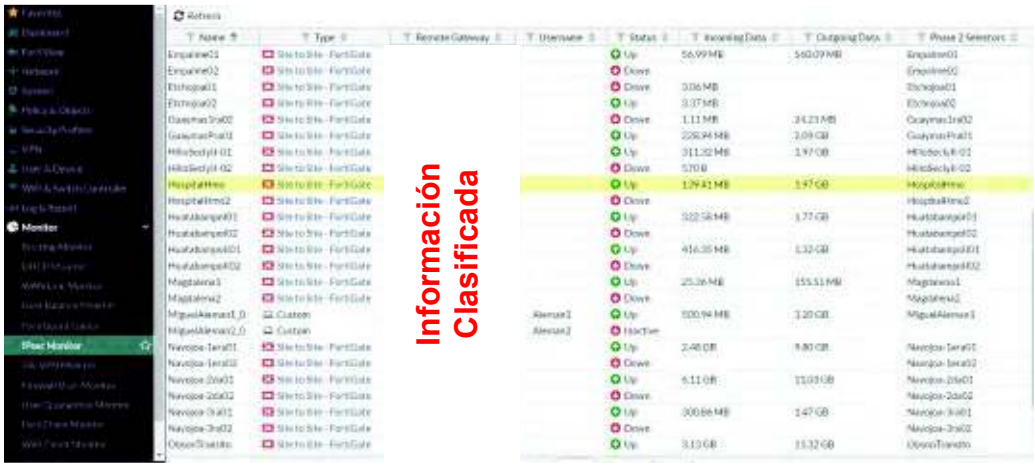


Figura 4.17 *Monitor de túnel IPsec/VPN*

También como medida de verificación se hacía una medición del comportamiento de dicho túnel, hablando vía telefónica con lo usuario de la Unidad Administrativa bajo estudio para que confirmarán el buen funcionamiento. Por otro lado, dicha verificación telefónica servía no solo para determinar la disponibilidad del enlace, sino también para verificar si el ancho de banda asignado a la UA era suficiente para realizar sus actividades laborales a través del túnel de VPN y así mismo para la navegación normal a Internet. En el caso de una respuesta negativa con la velocidad de los sistemas informáticos a través del túnel de VPN, se tendría que realizar un ajuste en las políticas de control de ancho apoyado en los perfiles de “Filtrado Web” o “Control de Aplicaciones”.

4.5.3 Ajustes y rediseño de la propuesta de implementación

Al finalizar el proceso de verificación del sitio de bajo impacto, se obtuvieron resultados satisfactorios que no indicaban la necesidad de realizar un reajuste a la configuración planteada de manera inicial; al final en un plazo de 2 semanas después de la implementación en el sitio de bajo impacto se procedió a realizar una visita a dicho sitio, solo para verificar la conformidad de los usuarios de dicha UA y así proceder a la implementación general.

4.5.4 Implementación general de la solución propuesta y verificación

En esta etapa de la fase 5 al finalizar la verificación de la implementación del sitio de bajo impacto y al corregir o realizar los ajustes de configuración, que en nuestro caso no existió la necesidad, se procedió a replicar la implementación en el resto de las UA, ya que como se había mencionado tienen una similitud en la infraestructura de red con la que cuenta, teniendo variaciones en la cantidad de usuarios.

La implementación general se decidió comenzar por las UA más cercanas ubicadas geográficamente, ya que el Estado de Sonora es uno de los que tiene más extensión geográfica, así mismo como solo se contaba con la implementación del sitio de bajo impacto, se tenía la incertidumbre que podría haber algo distinto en alguna otra UA

que no fuera compatible al 100% con la arquitectura propuesta. Se comenzó por instalar las agencias de los municipios de poblado Miguel Alemán, Aconchi y Ures en ese mismo orden de instalación. Al comienzo de la instalación todo marchaba como lo proyectado, al llegar al tercero todo seguía como lo planeado, pero al día siguiente comenzaron los usuarios de dicha UA, a generar reportes de falla, los cuales a verificar en el sistema de monitoreo de VPN visualizábamos que el túnel no estaba establecido por lo que procedíamos a reestablecerlo, el problema mencionado se hizo más constante en promedio cada 2 horas era la intermitencia del servicio, por lo que se realizó un análisis de la situación detectando que el cambio de direccionamiento de IP pública cada vez que se presentaba dicho problema, se notificó al proveedor del servicio de Internet, para que realizará las configuraciones que estaban descritas en el contrato de servicio, pero la respuesta del proveedor no fue satisfactoria y pudimos observar que el servicio de DNS dinámico no es tan eficiente o tiene un tiempo de respuesta más alto al tiempo en el que la dirección IP pública de la UA cambiaba. Por lo anterior y como resultado de dicha problemática, investigando tanto en artículos de fabricante en este caso Fortinet, así como en foros de discusión y bases de conocimiento, en donde se presentaran los mismo problemas con respecto al servicio de DNS dinámico o bien se estaba buscando como reconfigurar el servicio con respecto a los tiempo de respuesta o los tiempos con los que detectaba el cambio de direccionamiento del servicio asociado, lo cual no se encontró nada de documentación, sin embargo se encontró documentación acerca de un procedimiento para realizar un “Dialup-Client de tipo Tunnel Mode”, para comprender este punto debemos mencionar que las VPN tipo Dialup normalmente son usadas para conexiones entre un cliente a un servidor de VPN, por ejemplo un empleado de una organización realizando una conexión desde de su hogar mediante su enlace de Internet a la red de la organización, por lo que en el caso que quisiéramos usar ese esquema de conexión desde una UA al COR de la PGJE, tendríamos que realizar dicha configuración de forma individual en cada computadora de dicha agencia como Fortinet lo representa en la figura 4.18.

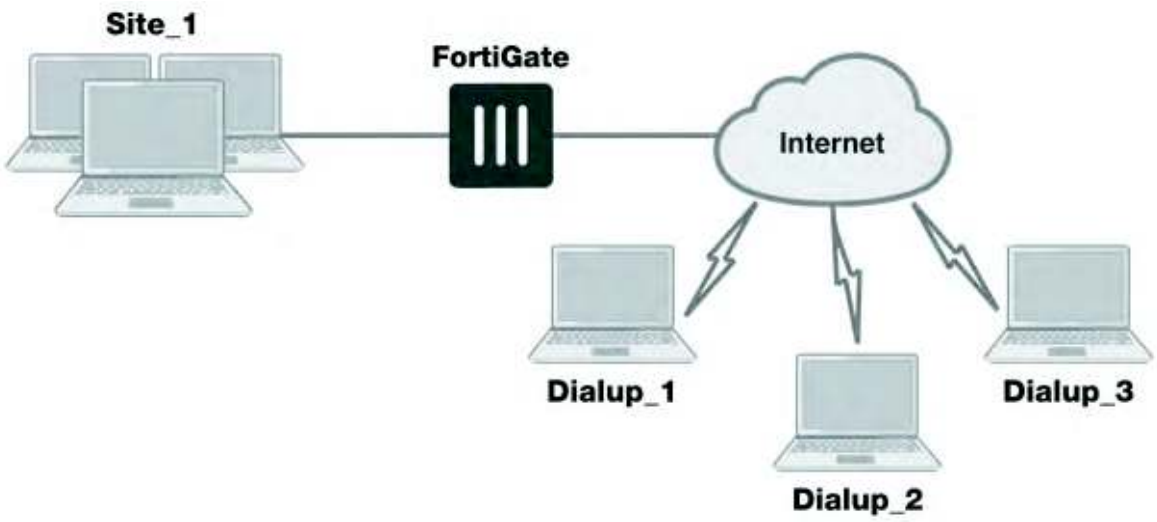


Figura 4.18 *VPN Dial-up Clientes remotos*

La ventaja de las conexiones de este tipo es que no es necesario una dirección IP pública del lado del cliente en este caso de la UA, solo se requiere una conexión con la posibilidad de conexión al COR, por lo que, si se necesita del lado del COR una dirección IP pública, para que en este caso el cliente genere la petición para establecer el túnel. Por lo anterior el fabricante Fortinet brinda la característica anteriormente mencionada de “Dialup-Client de tipo Tunnel Mode” donde uno de los dos equipos Fortigate tomará el papel de cliente como si fuera un usuario como se muestra en la figura 4.19, pero al mismo tiempo al realizar el túnel este sería funcional para transferir el tráfico de red generado por los usuarios que se encuentren conectado a dicho equipo Fortigate; para este caso particular y solo en los sitios con la problemática presentada de cambio de dirección de IP pública constante lo cual genera intermitencia en el túnel de VPN por la razones anteriormente asociadas al servicio de DNS Dinámico.

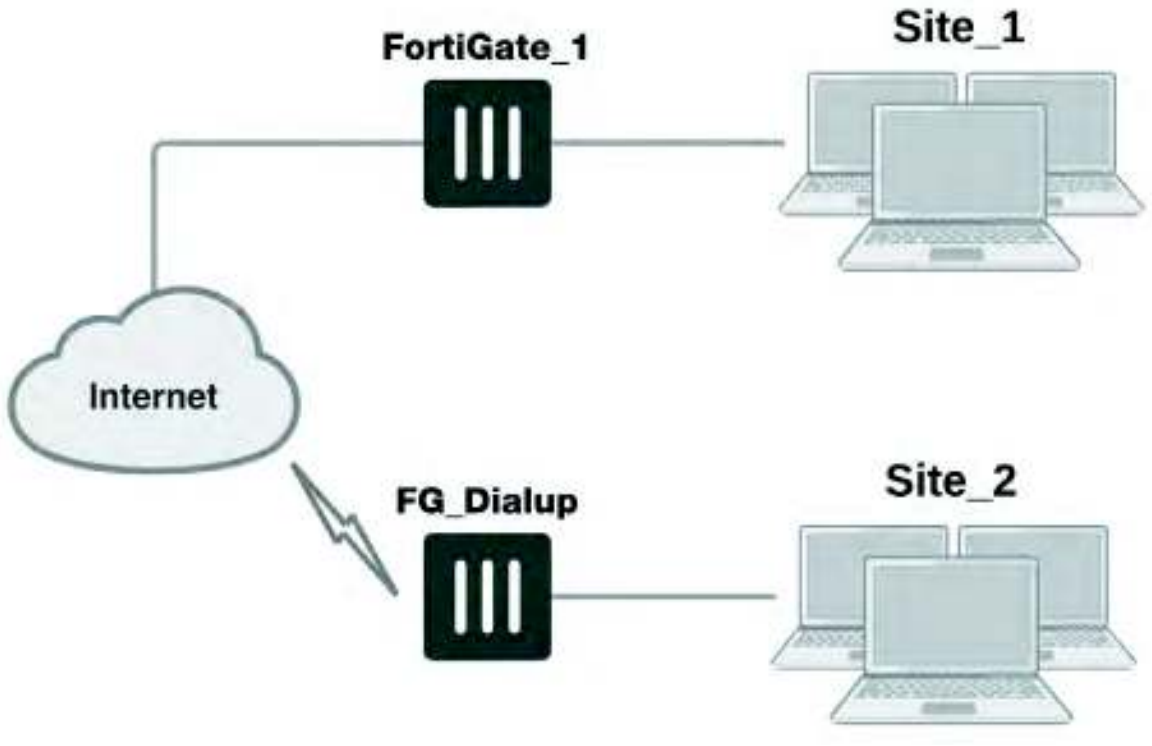


Figura 4.19 *Dialup-Client de tipo Tunnel Mode*

La configuración de la VPN mencionada se realizó utilizando el asistente de VPN/IPsec, como solo se está configurando en los sitios que se detecta el problema de cambio de direccionamiento IP, por lo que se configura inicialmente como una VPN "Site to Site" entre equipos Fortigate, en el caso de presentarse el problema de intermitencia en el túnel se procede a realizar el cambio a VPN tipo Dial-up, donde el equipo Fortigate permite modificar el túnel ya creado y personalizarlo (custom) como se muestra en la figura 4.20, donde al presionar el botón de "Convert To Custom Tunnel" automáticamente nos deja editar cada una de las opciones que se necesitan para realizar el túnel de VPN, las cuales se describen a continuación:

- Red: se encuentran las opciones del IP del equipo remoto, la interface por donde se realizará la conexión, NAT.
- Autenticación: método de autenticación donde puede ser por clave compartida o firma, IKE (Internet Key Exchange), modo de IKE.

- Fase 1: Encriptación de la conexión al realizar el túnel.
- Fase 2: donde se describen las políticas o bien las redes tanto locales y remotas que estarán transitando por el túnel de VPN.

Figura 4.20 *Dialup-Client de tipo Tunnel Mode*

Las configuraciones como se mencionó anteriormente son diferentes en la UA la cual representará la parte del cliente y el COR que representará la parte de sitio principal o Server. La configuración de una UA en Dialup se describe a continuación:

- Red: “Remote Gateway” se coloca la IP del equipo que se encuentra en el COR, no olvidemos que según la arquitectura en el sitio que será considerado como principal o Server debe de contar con IP pública fija; por otro lado, volviendo a la parte de la configuración de red, tenemos la selección de la interface por donde la UA estará conectada a Internet, se activa la parte de NAT y por último selecciona que siempre detecte el “peer” aunque este inactivo, como se muestra en la figura 4.21.

Figura 4.21 *Configuración de Red en la UA para Dialup*

- Autenticación: primero se eligió el método de autenticación, en este caso se eligió utilizar una clave compartida la cual tendrá que ser igual en la configuración del equipo instalado en el COR. Por otro lado, se seleccionó la versión de IKE tipo 1 y el modo que sea agresivo, por último, como lo realizaremos mediante Dialup y en si no tendremos una IP asociada al equipo para establecer el túnel de VPN, lo haremos utilizando un "Peer ID" para hacer la asociación del túnel mencionado, como se muestra en la figura 4.22.

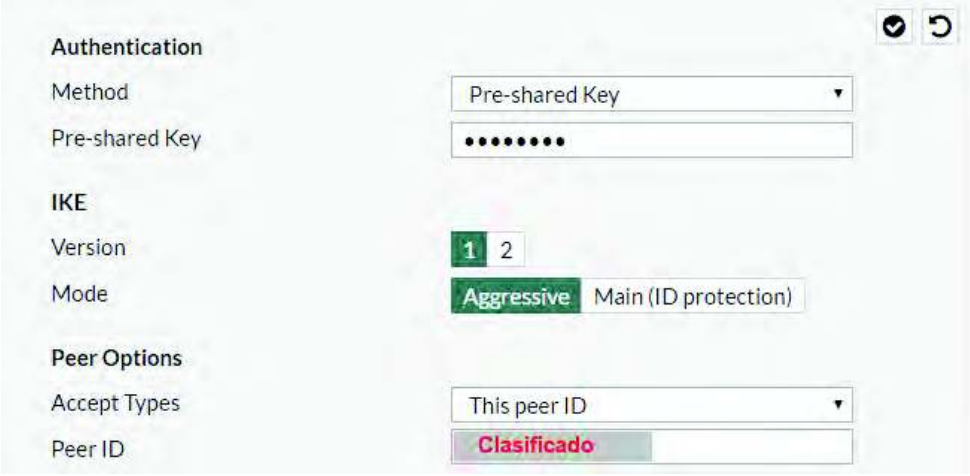


Figura 4.22 *Configuración de Autenticación en la UA para Dialup*

- Fase 1: en esta fase es donde elegimos el tipo de encriptación y autenticación va a tener el túnel, así como el identificador de local de la conexión que este es un nombre a criterio del usuario, como se muestra en la figura 4.23.

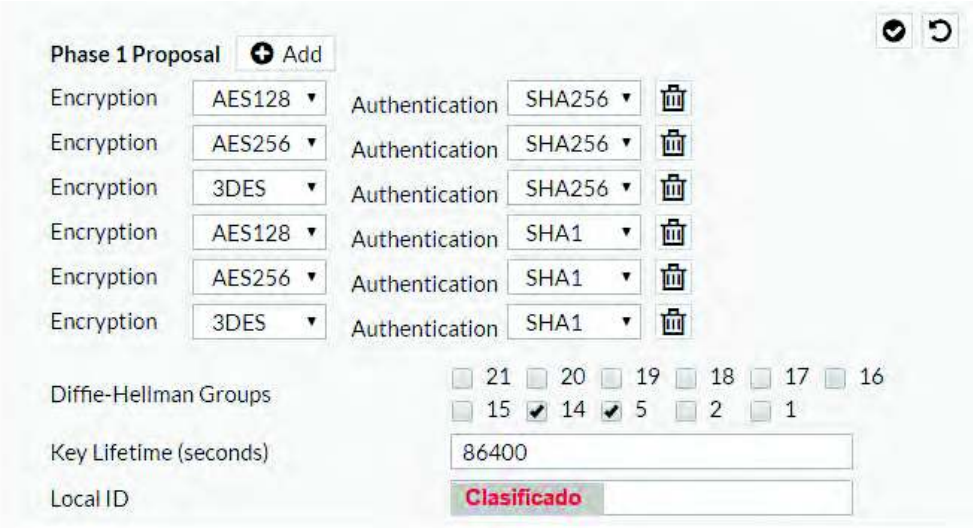


Figura 4.23 *Configuración de Fase 1 en la UA para Dialup*

- Fase 2: En esta fase no se realiza ningún cambio, como se muestra en la figura 4.24.

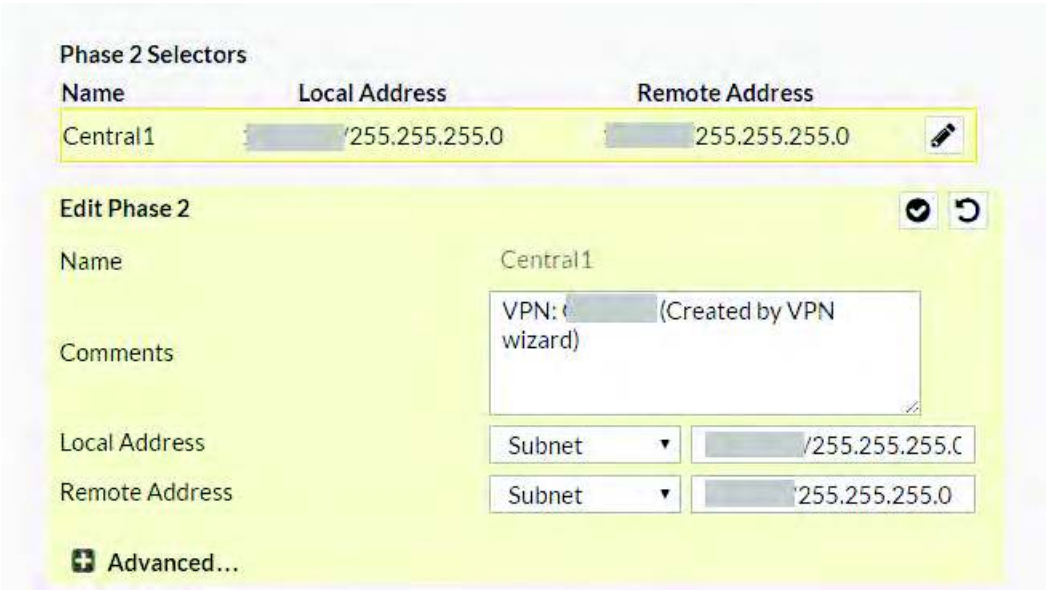


Figura 4.24 *Configuración de Fase 2 en la UA para Dialup*

Por otra parte, del lado del COR, hay ciertas variaciones en la configuración para realizar el túnel, ya que como se ha estado mencionando dicho equipo según el esquema de “Dialup-Client de tipo Tunnel Mode” juega el papel de “servidor” o equipo principal, por lo que a continuación se describe la configuración:

- Red: la diferencia a la configuración con la UA, es que en la sección con respecto al “Remote Gateway” se selecciona “Dialup User”, como se muestra en la figura 4.25.

Figura 4.25 *Configuración de Red en COR para Dialup*

- Autenticación: la diferencia a la configuración con la UA, de tipos de “Peer” aceptados seleccionaremos “especificar ID de Peer” el cual será el mismo que utilizamos en el equipo de la UA con la que se realizará el túnel, como se muestra en la figura 4.26.

Figura 4.26 *Configuración de Autenticación en COR para Dialup*

El resto de las configuraciones que son la fase 1 y fase 2 para generar el túnel de VPN, son las mismas tanto en el COR como en la UA, solo se intercambia en la parte de fase 2, las redes remotas y locales según sea el caso; como se mencionó la diferencia entre un tipo de túnel y otro es que, el Dialup no requiere direccionamiento IP fijo ya que no lo utiliza en la parte de la UA para realizar la conexión, así como para realizar el túnel si lo realizamos de la forma inicial el túnel solo se establece cuando hay actividad en cualquiera de los 2 sitios, en cambio el tipo Dialup siempre está forzando a que el túnel este establecido, por lo que si utilizamos el monitor y se encuentra que un túnel de la forma tradicional no se encuentra establecido, pueda deberse a que hay una inactividad en la agencia por lo que podemos hacer la prueba generando tráfico y revisar si se establece el túnel, por otro lado, en el caso de tipo Dialup, si existe una desconexión en el túnel que visualicemos en el monitor de IPsec, lo más probable es que se debe a que no se cuenta con servicio por parte del proveedor de Internet.

Otra de las situaciones que se presentó es que los contratos de servicio de Internet no tienen una especificación de la velocidad mínima que tienen que otorgar a las UA, por lo que en UA como Puerto Peñasco y Bacum era demasiado lento el túnel de VPN establecido por lo que se decidió realizar la conexión mediante C4 el cual era hasta 5 veces más estable y veloz.

4.5.5 Comparativo de resultados

Se realizó un comparativo de resultados con respecto a la cantidad de solicitudes de servicio derivado de falla de conectividad las cuales se pueden reflejar en algunos casos, como los que se describen a continuación:

- Problema de acceso a los sistemas: cuando no pueden entrar al sistema “nuevo” el cual como ya se explicó está centralizado por lo tanto requiere en todo momento una conexión establecida entre la UA y el COR, que en este caso en el túnel de VPN que hemos mencionado.

- Sin acceso a Internet: esto se refiere cuando el usuario comentaba que no podía acceder a la navegación normal que en la mayoría de los casos era casos reportaban no tener acceso al correo electrónico.
- Telefonía IP: no se contaba con el servicio de telefonía IP por diferentes razones, una de ellas es que hay UA que su equipo telefónico están registrados y enlazados al conmutador que se encuentra en el COR, por lo que al no tener el túnel de VPN el equipo dejaba de funcionar.
- Falla en replicación de información: este tipo de reporte era interno de la Dirección de Sistemas, ya que lo realizaba el administrador de base de datos, lo cual se debía a que no existía conectividad entre el servidor de la UA y el servidor central de replicación ubicado en el COR.

El comparativo mencionado se realizó con la información de 3 meses anterior a la implementación de la nueva arquitectura, así como 3 meses posterior a la instalación, como se había recomendado anteriormente la utilización del sistema de captura de servicios que usa el área de soporte técnico lo cual la organización accedió, dicho sistemas se capturan las llamadas telefónicas y oficios de solicitudes de servicio. También se midió los tiempos promedio de respuesta para la acción correctiva en cada una de la solicitud presentada. Los tiempos de medición para la situación antes de implementación contempla los meses de octubre, noviembre y diciembre de 2016 y se utilizó el mes de enero y febrero para realizar la implementación, por lo que los meses de comparación posterior a la implementación son marzo, abril y mayo de 2017. En ambos comparativos tanto número de solicitudes de servicio y tiempo fueron promedios de cada uno de los meses, para la parte de solicitudes fueron el número promedio diario capturados en el sistema los cuales podía ser vía telefónica, presencial o bien mediante oficio. Por otro lado, para la parte de tiempos de respuesta, se comenzó a registrar el tiempo de duración de la falla que va ligado al tiempo en que el técnico realizaba las acciones correctivas, en algunas ocasiones la falla va directamente al proveedor de Internet, por lo que en dichos casos no fueron omitidos tanto en la situación anterior y posterior a la implementación ya que son ajenas a las

acciones que pudiera realizar el personal correspondiente. A continuación, se representa de manera gráfica en las figuras 4.27 y 4.28 el comparativo entre las dos situaciones mencionadas.

Figura 4.27 *Comparativo de promedio diario de solicitudes por mes*

Figura 4.28 *Comparativo de promedio tiempo para corregir el reporte*

Como se puede observar en los gráficos anteriores tanto la cantidad de solicitudes diarias, así como el tiempo de respuesta para corregir el reporte o la solicitud recibida ambos tuvieron una disminución considerable, podría decirse de más de 50%, las variaciones entre los meses están asociadas a temporadas. Por ejemplo, el mes 3 “antes” es diciembre o el mes 2 “después” que es abril, ambos meses incluyen periodo vacacional lo cual al realizar el promedio diario presenta una disminución en comparación a los meses de su mismo ciclo, pero por la misma situación en la parte de tiempo de acción correctiva tuvo un aumento tanto en el mes de diciembre como en abril, ya que hay acciones correctivas que se requieren hacer en sitio y en algunas ocasiones no se encontraba el personal correspondiente. También hay muchas acciones que dependen de un tercero por ejemplo en el caso del personal de C4, que por la misma razón de periodo vacacional se dificultaba el contacto.

Adicional a la implementación se realizó la propuesta para que la organización actualizara o cambiara la forma de captura de solicitudes de servicio ya que el sistema que se utilizaba normalmente solo registra la orden, pero no nos brinda más información solo el detalle de la solicitud. Por lo que se le recomendó un sistema especializado para “help desk” en este caso se propuso el osTicket, ya que cuenta con ciertas funcionalidades a continuación, se mencionan algunas (Osticket, 2017):

- Personalización: como es una herramienta de código abierto, se puede personalizar a la necesidad de la organización o agregar información aparte de la recomendada, por ejemplo: temas de ayuda, información de los técnicos o del usuario, entre otros.
- Notificación mediante correo electrónico: interacción entre el usuario final y los técnicos.
- Organización de solicitudes: asignación de solicitudes para un solo técnico y así no tener duplicidad de información o confusiones entre los usuarios finales y los técnicos.
- Reportes: creación de reportes tanto de las solicitudes como del mismo personal técnico.

- Portal de acceso: el usuario puede crear su propia solicitud sin tener que llamar a la mesa de ayuda, así mismo puede darle el seguimiento o tener contacto directo con el técnico que fue asignado.

El sistema mencionado fue instalado y configurado para el uso de la organización, aún está en fase de ajustes, pero ya se está utilizando como se pueden observar en el anexo 2. También como el sistema tradicional de la organización sigue en funcionamiento y se requiere la información al menos de manera mensual para realizar lo que llaman “corte estadístico mensual” por lo que dicha información que se encuentra en los servidores de cada UA y se requiere replicar al servidor central y así poder concentrar la misma. Por lo anterior al realizar la configuración propuesta se tuvo un impacto significativo con respecto a esa operación de la organización, ya que solo se tenía la conectividad al 100% con 3 UA el resto estaba en una interconexión intermitente o nula con el COR como se muestra en la figura 4.29, donde entrevistando al personal correspondiente de recopilar dicha información se tenía que trasladar durante 2 semanas a lo largo de 22 municipios, lo cual indica que en ese lapso de tiempo no se tenía la información de dichas UA.

Figura 4.29 *Representación de UA conectadas antes de la implementación*

Por lo que al realizar la conectividad entre las UA y el COR, ya que era una operación obligatoria por la cuestión del nuevo sistema implementado que funciona de manera centralizada, se aprovechó para utilizar los túneles de VPN establecidos y se configuraron los servidores de las UA, para replicar la información de manera automática, por lo que ahora se cuenta con la información de las UA del viejo sistema en tiempo real, reflejándose en un ahorro económico al no tener que realizar los traslados mensuales para la recolección de la información, representando a continuación el cambio de conectividad en la figura 4.30.

Figura 4.30 *Representación de UA conectadas después de la implementación*

5 CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

En el presente trabajo de tesis se buscó desarrollar e implementar un procedimiento para el aprovechamiento de la infraestructura de red de la organización, con el fin de implementar una solución de una red administrada por software o bien optimizar las funcionalidades del equipamiento instalado en el caso de no tener la compatibilidad con SDN. Mediante el procedimiento desarrollado en el presente proyecto, la organización pudo resolver la problemática de la estabilidad y disponibilidad de la interconexión entre las Unidades Administrativas y el Centro de Operaciones de Red de la organización. Así mismo por la arquitectura de alta disponibilidad y tolerancia a fallos, se disminuyeron los reportes de fallas presentadas por la UA, así como los tiempos de respuesta al realizar acciones correctivas el caso de ser requerido, dicha arquitectura era funcional con respecto a la red interna tanto del edificio principal de la organización como de cada UA.

A continuación, se describen las conclusiones, recomendaciones y trabajos futuros derivados de esta investigación, con el fin de continuar con el proyecto y realizar mejoras.

5.1 Conclusiones

Se diseñó e implementó una arquitectura de red que mejora la estabilidad y disponibilidad de la red entre las UA y el servidor central de la PGJE mediante el procedimiento propuesto que consta de 5 fases e incluyen:

- Configurar el equipo seguridad perimetral de las UA para tener un funcionamiento automatizado y de alta disponibilidad con el servidor central.
- Diseñar un modelo de monitoreo del equipamiento de red, que alerté en el caso de falla y almacené los sucesos para su análisis posterior, como apoyo a la toma de decisiones.

- Optimizarlos recursos de red con el fin de automatizar los procesos y operaciones de red.

El procedimiento propuesto, además permite que en caso de que no se pueda implementar un modelo basado en SDN sea posible aplicar un modelo tradicional optimizado para brindar alta disponibilidad.

El análisis de la situación benefició a la organización, ya que, al contar con un inventario actualizado de su equipamiento instalado, así como de los servicios contratados, se detactaron duplicidades y servicios instalados que el personal de la Dirección de Sistemas no tenía conocimiento o sin utilizar.

Se desarrolló una propuesta de modernización que permitirá a futuro la implementación de SDN de manera progresiva. Esta propuesta apoya al área administrativa en la selección de los equipos a adquirir en el futuro, además se plantearon bien los requerimientos ya que tiene un alto impacto económico, y a su vez se pueda cumplir con todos los detalles necesarios para los procesos de adquisición que se sigue en el ámbito gubernamental.

Al terminar la fase 3 se hizo una propuesta de actualización tecnológica la cual aún no soporta una arquitectura de SDN, pero al recibir el equipamiento propuesto, la organización se encontraría a la vanguardia de equipamiento tecnológico, así como realizar lo necesario en temas de: seguridad, alta disponibilidad, interconectividad temas de los cuales carecía la organización.

Se detectó que los proveedores de Internet tenían diferente calidad de servicio según la región geográfica, por lo que se tuvo que realizar evaluaciones y ajustes al momento de la toma de decisiones en las contrataciones, así como al momento de implementar decidir cuál sería el enlace principal en la UA para realizar la conexión con el COR.

Al evaluar la arquitectura propuesta se pudo observar deficiencias en el sistema con el cual captura o registran las solicitudes de servicio, por lo que, al implementar el

sistema propuesto, se ajustó para ser el sistema de mesa de ayuda de la Dirección de Sistemas en general, dividiendo los casos en: soporte técnico, redes y el área de desarrollo de sistemas.

Así mismo, dados los resultados obtenidos, se puede observar que la implementación tuvo beneficios económicos y eficiencias en las funciones propias de la organización, agilizando los procesos y el flujo de información.

5.2 Recomendaciones

Con el fin de mejorar la arquitectura de red propuesta, así como el servicio que brinda la Dirección de Sistemas a la organización, a continuación, se enlistan una serie de recomendaciones para la optimización y eficiencia de la misma:

- Fase 3: se recomienda a la Dirección de Sistemas sea más participativa al momento de realizar las partidas presupuestales, ya que dicha Dirección es quien tienen el conocimiento real de las necesidades tecnológicas de la organización o bien adquirir lo necesario para optimizar la arquitectura tecnológica que se tiene.
- Fase 1: con respecto al registro de solicitudes de servicio se instaló un sistema para la mesa de ayuda, el cual se generalizó para todas las áreas de la Dirección de Sistemas. Se recomienda explotar más las funcionalidades de dicha plataforma, así como realizar un curso o manual de usuario, para que el usuario final tenga una mejor interacción y alimente de la información correcta a dicha plataforma, mejorando el tiempo de respuesta a la solicitud y a su vez dando la pauta de la creación de una base de conocimiento.
- Fase 4: mejorar el aspecto alta disponibilidad con respecto a las interconexiones de la UA con el COR, ya que hay sitios remotos que no se tiene conectividad por la red estatal de C4 y solo se tiene al proveedor de Internet o viceversa, solo se tiene C4 y no se tiene Internet, por lo que en dichos sitios realizó el estudio para tener una interconectividad “punto a punto” mediante inalámbrico a la UA

más cercana geográficamente y así cumplir con el criterio de alta disponibilidad (redundancia de enlace).

- Monitoreo de red: es recomendable contar con un sistema de alertas automatizadas que notifique al personal correspondiente ya que actualmente, tienen que acceder al sistema de monitoreo y solo así tienen conocimiento si existe un problema.

5.3 Trabajos Futuros

Se ha logrado un avance muy importante en la arquitectura tecnológica de la organización, así como en la calidad del servicio que brinda la Dirección de Sistemas al resto de la organización. Aun no se logró alcanzar el total de las UA con las que cuenta la organización solo las mencionadas anteriormente, derivado de la limitante y alcance del proyecto por cuestiones del tiempo que se tiene para resolver la problemática. El procedimiento propuesto puede ser muy beneficioso si se analiza al detalle el resultado que se espera y la situación actual de la organización, así como poder replicarlo al 100% en toda la organización. Algunos de los trabajos futuros podrían ser:

- Trabajar en el desarrollo de aplicaciones específicas de SDN aun sin contar con equipamiento que soporte el protocolo de OpenFlow, como por ejemplo realizar aplicaciones de optimización utilizando el protocolo estándar de CAPWAP, como es en el caso de la PGJE que cuenta con equipamiento de controlador inalámbrico y puntos de acceso marca Fortinet.
- Capacitación y optimización del sistema osTicket para explotar la parte de interacción con el usuario, así mismo identificar los problemas claves para la creación de un catálogo para la creación y organización de las solicitudes de servicio.
- Definir requerimientos tecnológicos en la UA restantes para reproducir la arquitectura de red en el 100% de la organización.

- Implementar un sistema de monitoreo integral para toda la infraestructura de red, como por ejemplo SolarWinds el cual es de licenciamiento o bien el Cacti que es de código abierto.
- Instalar un software especializado que mida la velocidad de ancho de banda del túnel establecido entre la UA y el COR, con el fin usarlo como herramienta para la toma de decisiones al momento de elegir cuál de los enlaces será el principal en la UA, entre C4 y el proveedor de Internet.

6 REFERENCIAS

Akhunzada, A. et al., 2015. Securing software defined networks: Taxonomy, requirements, and open issues. IEEE Communications Magazine, 53(4), pp.36–44.

Alharbi, T. y Portmann, M., 2015. The (In) Security of Topology Discovery in Software Defined Networks The (In) Security of Topology Discovery in Software Defined Networks. , (October), pp.502–505.

Bindra, N. y Sood, M., 2016. Is SDN the Real Solution to Security Threats in Networks? A Security Update on Various SDN Models. Indian Journal of Science and Technology, 9(32). Available at: http://www.indjst.org/index.php/indjst/article/view/100214.

Bondkovskii, A. et al., 2016. Qualitative comparison of open-source SDN controllers. Proceedings of the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, (Noms), pp.889–894.

Casta, M.E.Z., 2011. Sistema multi-agente para el monitoreo de tráfico LAN y recursos usados por los equipos * 1 [Multi-agent system for monitoring LAN traffic and resources used by equipment] Resumen Introducción. , (c), pp.57–76.

Cui, H. et al., 2014. Design of intelligent capabilities in SDN. 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2014 - Co-located with Global Wireless Summit.

Elsadek, W.F. y Mikhail, M.N., 2016. Inter-domain Mobility Management Using SDN for Residential/Enterprise Real Time Services. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp.43–50.

Fraser, B. et al., 2013. Are We Ready for SDN ? Implementation Challenges for Software-Defined Networks. , (July), pp.36–43.

Han, Y. y Hyun, J. y Hong, J.W., 2016. Graph Abstraction Based Virtual Network Management Framework For SDN. , pp.16–17.

Kim, W. et al., 2016. OFMon: OpenFlow monitoring system in ONOS controllers. IEEE NETSOFT 2016 - 2016 IEEE NetSoft Conference and Workshops: Software-Defined Infrastructure for Networks, Clouds, IoT and Services, pp.397–402.

Lin, Y.D. et al., 2016. Fast failover and switchover for link failures and congestion in software defined networks. 2016 IEEE International Conference on Communications, ICC 2016.

Luan, M. et al., 2015. Controllable network architecture based on SDN. Proceedings - 2015 2nd International Conference on Information Science and Control Engineering, ICISCE 2015, pp.174–180.

Martín, A. et al., 2012. A framework for development of integrated intelligent knowledge for management of telecommunication networks. Expert Systems with Applications, 39(10), pp.9264–9274.

Nakayama, H. et al., 2014. An implementation model and solutions for stepwise introduction of SDN. APNOMS 2014 - 16th Asia-Pacific Network Operations and Management Symposium, 1, pp.2–5.

Naudts, B. et al., 2016. Deploying SDN and NFV at the speed of innovation: Toward a new bond between standards development organizations, industry fora, and open-source software projects. IEEE Communications Magazine, 54(3), pp.46–53.

Patel, K., 2016. Software Defined Networking : Architecture , Application , Issues and Challenges. , 5(5), pp.78–81.

Pontarelli, S. et al., 2016. Stateful OpenFlow: Hardware proof of concept. IEEE International Conference on High Performance Switching and Routing, HPSR, 2016–June.

Rufaida Ahmed, M.N., 2016. Fast Failure Detection and Recovery Mechanism for Dynamic Networks Using Software -Defined Networking. , pp.167–170.

Salman, O. et al., 2016. SDN Controllers: A Comparative Study. , (978), pp.18–20.

Shin, J.W. et al., 2016. Access Control with ONOS Controller in the SDN Based WLAN Testbed. , pp.656–660.

Shu, Z. et al., 2016. Security in Software-Defined Networking: Threats and Countermeasures. Mobile Networks and Applications, pp.1–13.

Wang, M. et al., 2016. An Approach for Protecting the OpenFlow Switch from the Saturation Attack. , (Nceece 2015), pp.729–734.

Yang, S. y Chang, Y., 2011. Expert Systems with Applications An active and intelligent network management system with ontology-based and multi-agent techniques. , 38, pp.10320–10342.

Ipv6.udg.mx. (2016). IPv6 OpenFlow. [en linea] disponible en: http://www.ipv6.udg.mx/oess.php [accedido 17 Mar. 2016].

Opendaylight.org. (2016). Research Government | OpenDaylight. [en linea] disponible en: https:// www.opendaylight.org/research-ed-government [accedido 24 Mar. 2016].

Opendaylight.org. (2016). Platform Overview | OpenDaylight. [en linea] disponible en: https://www.opendaylight.org/platform-overview [accedido 13 Oct. 2016].

Hpe.com. (2017). Data sheet. [en linea] disponible en: https://www.hpe.com/h20195/v2/getpdf.aspx/4aa3-0717enw.pdf [accedido 12 Ene. 2017].

Osticket.com. (2017). Features. [en linea] disponible en: http://osticket.com/features [accedido 22 Ene. 2017].

Gns3.com. (2017). SDN 101: Using Mininet and SDN Controllers. [en linea] disponible en: https://gns3.com/news/article/sdn-101-using-mininet-and-sdn-co [accedido 22 Feb. 2017].

Gartner.com. (2017). doc: Magic Quadrant for Enterprise Network Firewalls. [en linea] disponible en: https://www.gartner.com/doc [accedido 22 Mar. 2017].

7 ANEXOS

7.1 Anexo 01: Solicitud de servicio mediante oficio

Orden de servicio realizada mediante oficio la cual van dirigidas a la Directora de Tecnologías de Información, la descripción de la solicitud y la firma del solicitante, la cual sirve para determinar la ubicación física del usuario.

LIC. REBECA SALAZAR PAVLOVICH
C. ENCARGADA DE LA DIRECCION
GENERAL DE TECNOLOGIAS DE
INFORMACION Y COMUNICACIONES
DE LA FISCALIA GENERAL DE JUSTICIA
DEL ESTADO DE SONORA.
P R E S E N T E:

Por este medio solicito a Usted en CARACTER URGENTE [illegible] revisión, configuración, internet e instalación de Sistema Integral de Apoyo al Ministerio Público (SIAMP) y Sistema Informático de Gestión Integral (SIGI) en los equipos que se encuentran en sitio en resguardo de esta fiscalía siendo los siguientes:

SERIE	SOLICITUD
MXL5490448	Revisión y Diagnóstico
MXJ549052J	(En caso que quedara
MXJ549044J	funcional, instalar
	SIAMP Y SIGI)
MXJ549056Z	Configuración e instalación
	De SIAM y SIGI.
MXL5491367	Configuración de internet
MXJ70201TR	
MXJ5510GLV	

Asimismo se solicita servicio completo a todos los equipos de computo en resguardo de esta fiscalía los cuales se encuentran en sitio, así como también kit de mantenimiento para la impresora HP LASER JET 600 M602, lo anterior por ser necesario para el buen funcionamiento de esta Fiscalía.

Sin ningún otro particular por el momento, les reitero la seguridad de mi atenta y distinguida consideración.

A T E N T A M E N T E
SUFRAGIO EFECTIVO. NO REELECCIÓN
LA C. AGENTE DEL MINISTERIO PÚBLICO ESPECIALIZADO EN DELITOS
SEXUALES Y VIOLENCIA FAMILIAR

LICENCIADA [illegible] VERÓNICA MARTÍNEZ [illegible]

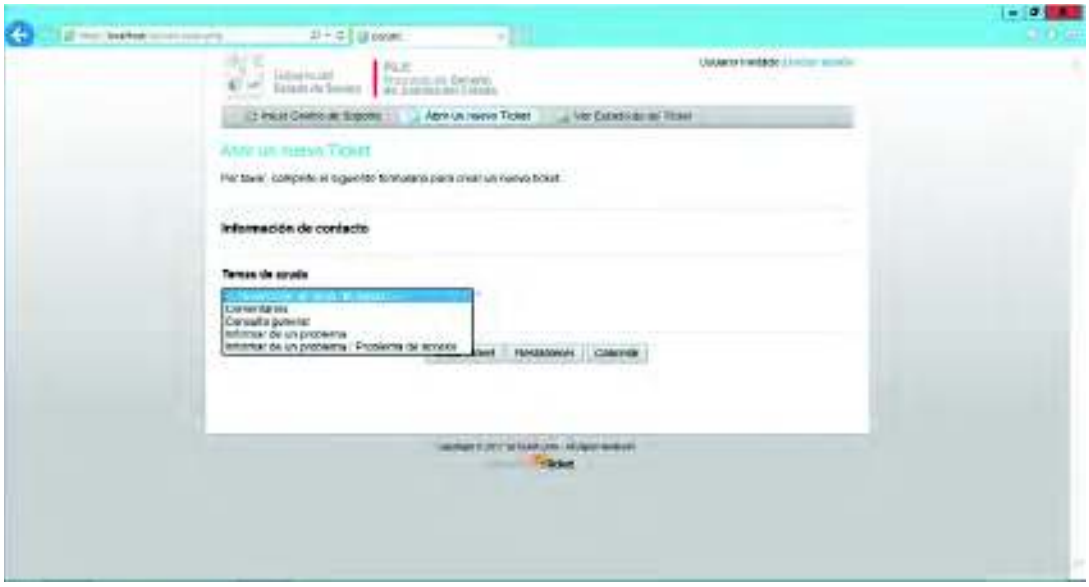
7.1 Anexo 02: Sistema de mesa de ayuda personalizado

Pantalla de inicio del sistema de OsTicket el cual fue personalizado con la imagen que usa la organización para sus sistemas internos.

Pantalla de inicio después de autenticarse, donde le permite al usuario ver el estado de sus solicitudes pendientes o bien crear una nueva solicitud de servicio.

Ventana de registro de cuenta en donde se crean la contraseña del usuario y se define la zona horaria.

Al abrir una nueva solicitud se puede utilizar temas de ayuda los cuales, permiten agilizar la identificación del sistema y así mismo la asignación del técnico más competente para la resolución del problema.



Ventana de registro de creación de solicitud donde se especifica información del usuario solicitante y descripción de la solicitud de servicio.

Representación de la carátula de una impresión del formato de solicitud de servicio en donde está la información del usuario, el técnico asignado, descripción del lugar y descripción de solicitado.