UNIVERSIDAD NACIONAL.

Facultad de Ciencias Exactas y Naturales.

Escuela de Informática.

Proyecto de Graduación para optar por el grado de Licenciatura en Informática con Énfasis en Sistemas de Información.

Implementación de una solución de telemática que permita llevar de forma transparente y segura, los servicios de red de la sede central de Fundación Omar Dengo a sus 9 sedes.

Autor: Ing. Giovanni Arias Conejo.

Cédula de identidad 205180575.

Heredia, Costa Rica.

Febrero, 2021.

Este proyecto está dedicado a contribuir con la Fundación Omar Dengo, organización sin fines de lucro cuyo nombre se da en honor al destacado costarricense Omar Dengo Guerrero, formador de los primeros docentes de la historia del país, conocido como “Maestro de Maestros y educador de un pueblo”, quien vivió entre 1888 y 1928 y quien creyó firmemente que era educando a los ciudadanos y moldeando el espíritu de los jóvenes, que se engrandecería a Costa Rica; institución cuya misión es contribuir al mejoramiento de la calidad y equidad de las oportunidades de aprendizaje de la población, para potenciar su desarrollo humano, mediante propuestas y modelos educativos innovadores centrados en las personas y el aprovechamiento de las tecnologías digitales.

Agradecimientos

A la Fundación Omar Dengo y sus dirigentes por la oportunidad de desarrollar el proyecto. Un especial reconocimiento a Ricardo Samper Jimenez, coordinador de la unidad de infraestructura tecnológica de dicha institución por su apoyo y disposición incondicional para respaldar su ejecución. Agradezco al tutor Alfonso Chaves Abarca, a los lectores Jose Pablo Calvo Suarez y Ronny Hernández Díaz por su acompañamiento y guía en la realización de este proyecto y a la Universidad Nacional, en especial a la Escuela de Informática y sus profesores por continuar asentando positivamente los cimientos de mi vida profesional. Mi gratitud a Dios y a mi familia por la oportunidad de estudiar y finalmente las gracias a todas aquellas personas que de una u otra manera han sido partícipes en la concreción de este proyecto.

Resumen

La Fundación Omar Dengo es una organización sin fines de lucro, cuyo objetivo principal es el desarrollo de las capacidades de las personas por medio de propuestas educativas innovadoras, apoyadas en el aprovechamiento de nuevas tecnologías. El siguiente trabajo final de graduación tiene por finalidad implementar una solución telemática para llevar los servicios que provee la infraestructura tecnológica de la sede central de la Fundación Omar Dengo a las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD, distribuidas a lo largo y ancho del país, de forma transparente y segura.

A partir de un análisis de la situación de conectividad, seguridad, intercambio de información y uso de los servicios que ofrece la infraestructura tecnológica entre la sede central de la FOD y las sedes locales, se determinaron las necesidades y escenarios de solución, con lo cual se conceptualiza y se implementa el diseño lógico de red que permita la apropiación de tecnologías y la estandarización de los servicios de red para la relación de interconectividad entre la sede central y las otras sedes. Finalmente, se elabora una guía para la construcción de una bitácora que permita verificar el correcto funcionamiento de la red y, de esa manera, retroalimentar la gobernanza de las tecnologías de información y comunicación mediante el monitoreo de las estadísticas de los equipos de comunicaciones y de los servicios que ofrece la infraestructura tecnológica.

Con la implementación de la solución, se satisfacen las necesidades institucionales de crecimiento y desarrollo de las tecnologías de información y comunicación de forma controlada y estandarizada, dando lugar a la mejora continua de la infraestructura tecnológica, las comunicaciones, la seguridad y los sistemas para llevar a la institución a una escalabilidad y ruta de servicios tecnológicos acorde a su labor y bajo un enfoque en concordancia con el plan estratégico institucional y los marcos de referencia y buenas prácticas que le atañan.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

CAPÍTULO I
INTRODUCCIÓN

CAPÍTULO I: INTRODUCCIÓN

1.1 Antecedentes

La Fundación Omar Dengo desde su creación en 1987, ha llevado a la práctica en coordinación con el Ministerio de Educación Pública, el Programa Nacional de Informática Educativa MEP-FOD con el fin de contribuir con la mejora de la calidad de la educación pública a través de propuestas pedagógicas innovadoras apoyadas en las tecnologías digitales, concebidas como herramientas de aprendizaje.

Actualmente el Programa integra principalmente centros educativos de primaria y secundaria de todo el país, con una cobertura promedio de la mitad de la población estudiantil del sistema educativo público, que abarca desde el grado Preescolar hasta la Secundaria beneficiando a más de medio millón de estudiantes.

Dentro de los propósitos del Programa, la equidad en el acceso a las tecnologías digitales mediante su universalización juega un papel determinante, por lo que la FOD y el MEP han realizado inversiones y esfuerzos sostenidos para favorecer a través de todos estos años, un crecimiento constante de la cobertura y de la población meta, lo cual ha permitido incluir además de estudiantes, a educadores, profesionales, personas de las comunidades y pequeños empresarios, entre otros.

En este sentido, uno de los cursos de acción definidos por la institución en el año 2016 para éste crecimiento, fue la reorganización de las sedes del Programa Nacional de Informática Educativa MEP-FOD alrededor del país y el traslado a éstas de parte del personal destacado en su sede central con el fin de dinamizar el recurso humano en zonas y facilitar así las tareas de diseminación, monitoreo y evaluación de sus propuestas pedagógicas dirigidas al desarrollo de

competencias digitales, científicas y tecnológicas para la innovación, el emprendimiento y la participación ciudadana que plantea la estrategia institucional.

De acuerdo con lo anterior, nace entre otros requerimientos, la necesidad de implementar una solución telemática que permitiera llevar a las sedes locales del Programa, los servicios de infraestructura telemática que provee la Unidad de Infraestructura Tecnológica de la Fundación Omar Dengo en su sede central para que los usuarios puedan desarrollar sus procesos de trabajo de forma transparente y segura. Dentro de dichos servicios se destacan algunos como: la Telefonía IP , el servidor de fax, el sistema biométrico de control de asistencia, el controlador de dominio, la Intranet, los sistemas de información, el filtrado de contenido, la administración centralizada de la seguridad en los equipos (cortafuegos, Antivirus y AntiSpyware), los servidores de archivos, las herramientas colaborativas como el Skype Empresarial y el Jabber de Cisco, la mesa de servicio y el soporte remoto, entre otros.

Desde hace 13 años, las tecnologías de la red telemática de la Fundación Omar Dengo se han basado en plataformas Cisco y, gracias al soporte y asistencia brindada por los diferentes socios que representan a este fabricante en Costa Rica, la institución decidió renovar nuevamente en 2015 dicha plataforma y el soporte de la misma por 3 años más, por lo que conceptualizar y desarrollar un modelo para la relación de interconectividad entre la sede central y las sedes del Programa, proyecta una oportunidad no solo para propiciar el aprovechamiento de las tecnologías de información, sino además maximizar la inversión hecha, y, que en definitiva, persigue apoyar la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones prácticas y de amplia repercusión, siendo de esta manera consecuente con el desarrollo estratégico de las Tecnologías de Información en la institución.

En cuanto a la gestión y el control de dichas Tecnologías de Información, la Fundación Omar Dengo está regida bajo el marco de referencia “Normas técnicas para la gestión y el control de las Tecnologías de Información” (Contraloría General de la República, 2007), pero admite el uso de buenas prácticas en general y propiamente en el marco de proyectos de ésta índole, utiliza “Cobit” como estándar para la gobernanza de TI (IT Governance Institute, 2007) e “ISO/IEC 27002:2013” (Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, 2013) como estándar para las buenas prácticas para los controles de seguridad de la información, por lo que el desarrollo de proyectos de TI deberán enmarcarse en dicha normativa.

1.2 Planteamiento del problema.

Para el año 2016, no había sido necesario para la institución incorporar en el diseño de su red telemática ubicaciones geográficamente distribuidas a lo largo y ancho del país, por lo que se carecía de un modelo de infraestructura tecnológica que permitiera llevar apropiadamente a dichas ubicaciones, los servicios que provee la infraestructura tecnológica en su sede central para que los colaboradores del Programa Nacional de Informática Educativa MEP-FOD pudieran desarrollar sus procesos de trabajo de forma transparente y segura.

Antes del planteamiento de reorganización de las sedes, en general éstas eran pequeñas oficinas con poco personal asignado y poca permanencia de éstos en el lugar, por lo que únicamente se concibió la contratación de servicios de Internet residenciales (Enlaces de Internet Asimétricos) para que básicamente los colaboradores pudiesen acceder al correo electrónico institucional, transmitir información y sacar provecho de los recursos que lograran encontrar en Internet. Dado que estas oficinas fueron cambiando paulatinamente a través de los años, nunca se estableció que los enlaces fueran gestionados ni monitoreados por la Dirección de Tecnología, reflejando una la falta de control sobre el uso del recurso. Por otro lado, el hecho de que los enlaces

no sean corporativos (Enlaces de Internet Simétricos) y sean proporcionados por diferentes proveedores, dificulta la gestión de los enlaces y resta corpulencia a las acciones de negociación comercial ya que no existe el interés suficiente de parte del proveedor para identificar y satisfacer las necesidades de conectividad ni de ofrecer un excelente servicio posventa para asegurar la continuidad de la relación comercial. Así mismo, no ofrecen alta disponibilidad, por lo que los tiempos de respuesta para la atención de fallas no concuerdan con las necesidades de la institución, además, presenta un pobre nivel de sobresuscripción y no ofrecen flexibilidad para cambiar el ancho de banda según se requiriera y en algunos casos tampoco permiten solicitar direcciones IP públicas.

Ante este escenario, con la reorganización de las sedes y de los colaboradores del Programa Nacional de Informática Educativa MEP-FOD, éstos ven limitado el acceso y uso de servicios como los mencionados anteriormente en la sección de Antecedentes, lo cual conlleva a una inherente contracción, no solo de la productividad, la comunicación y la colaboración de los funcionarios en las sedes, sino que también disminuye la estandarización de los servicios y la seguridad de la información debido a que los colaboradores se ven en la obligación de resolver su día a día con los medios que estaban a su alcance, en un entorno ajeno de la gestión y el control de las Tecnologías de Información a cargo de la Dirección de Informática de la Fundación Omar Dengo, impactando negativamente la eficiencia y eficacia de los procesos de trabajo y conduciendo a una mala gestión del marco de seguridad de la información que el rol estratégico de las tecnologías de información y comunicación debería sopesar.

En términos de esfuerzo financiero, el no contar con un entorno de interconexión entre la sede central y las 9 sedes distribuidas geográficamente a lo largo y ancho del país, implica un desaprovechamiento de la plataforma tecnológica actual y de los servicios de red que, además,

podría dar pie a la duplicidad de inversiones económicas para resolver necesidades puntuales en las sedes que ya son cubiertas por la infraestructura dentro de la sede central, encareciendo la operación del Programa.

En lo pertinente al marco jurídico, la Fundación Omar Dengo está sujeta a la fiscalización de la Controlaría General de la República y las situaciones expuestas hasta ahora están enmarcadas dentro del marco de control que proponen las "Normas técnicas para la gestión y el control de las Tecnologías de Información" (Contraloría General de la República, 2007), por lo que la inobservancia de su aplicación, implica una mala gestión institucional de las tecnologías de información y comunicación para apoyar el cumplimiento de la labor estratégica, por lo que desde dicha perspectiva, la problemática planteada requiere de atención y solución.

1.3 Justificación.

Para satisfacer las necesidades de crecimiento y desarrollo de las tecnologías de información y comunicación de forma controlada y estandarizada dentro de la Fundación Omar Dengo, es necesaria la mejora continua de la infraestructura tecnológica, sus servicios, la seguridad y los sistemas, para llevar a la institución a una escalabilidad y ruta de servicios tecnológicos acorde a su labor.

En este sentido, las "Normas técnicas para la gestión y el control de las Tecnologías de Información" (Contraloría General de la República, 2007) a las cuales está sujeta la Fundación Omar Dengo, así como el uso de las buenas prácticas que plantean "Cobit" (IT Governance Institute, 2007) e "ISO/IEC 27002:2013" (Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, 2013) para los controles de seguridad de la información, establecen que la institución debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo en

concordancia con el plan estratégico institucional (Fundación Omar Dengo, 2011), que plantea al Programa Nacional de Informática Educativa MEP-FOD como medio para aplicar modelos pedagógicos innovadores a través de tecnología de punta al 100% de las escuelas y colegios públicos costarricenses.

Estos mismos criterios también proponen en términos de la gestión de la seguridad, que la institución debe garantizar la confidencialidad, integridad y disponibilidad de la información, de manera que se cuente con las medidas de seguridad necesarias para el control de acceso a los recursos de TI y a la información, además de que se proteja la integridad de la información y se asegure una continuidad razonable de los servicios de TI.

Por otra parte, desde el enfoque financiero, las normas y buenas prácticas citadas exponen que la institución debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando y potenciando en la medida de lo posible, el logro de los objetivos de esa inversión.

Así, implementar una solución telemática que permita llevar hasta las sedes locales, los servicios de infraestructura tecnológica que actualmente provee la Unidad de Infraestructura Tecnológica de la Fundación Omar Dengo en su sede central, potencia el uso de los recursos tecnológicos facilitando el acceso, adopción y apropiación de los mismos a los colaboradores del Programa Nacional de Informática Educativa MEP-FOD ubicados en las sedes, de manera que éstos cuenten con las fuentes de información y herramientas de productividad, comunicación y colaboración necesarias para que puedan desarrollar sus procesos de trabajo de forma transparente y segura, con lo cual estaría asumiéndose a través de las tecnologías de información y comunicación, el rol estratégico necesario para apoyar la consecución de un proceso clave para la institución y de interés e impacto nacional como lo es el Programa.

1.4 Objetivos del Proyecto.

1.4.1 Objetivo General.

Implementar una solución telemática para llevar los servicios que provee la infraestructura tecnológica de la sede central de la Fundación Omar Dengo a sus sedes regionales, de forma transparente y segura, por medio de la extensión de una red de área metropolitana.

1.4.2 Objetivos Específicos.

1. Analizar la situación actual de conectividad, seguridad, intercambio de información y uso de los servicios que ofrece la infraestructura tecnológica entre la sede central y las otras sedes para determinar las necesidades y escenarios de solución.
2. Definir el modelo del diseño lógico de red telemática, que permita la apropiación de tecnologías y la estandarización de los servicios de red entre la sede central y las sedes locales.
3. Implementar una solución telemática que permita extender de forma homogénea, los servicios de red de la sede central de la FOD a las otras sedes.
4. Elaborar una guía para la construcción de una bitácora que permita la verificación del funcionamiento correcto de la red.

CAPÍTULO II
MARCO TEÓRICO

CAPÍTULO II: MARCO TEÓRICO

2.1 Marco referencial

La Fundación Omar Dengo (FOD), es una organización sin fines de lucro, cuyo objetivo principal, es el desarrollo de las capacidades de las personas, por medio de propuestas educativas innovadoras, apoyadas en el aprovechamiento de nuevas tecnologías.

Desde su creación en 1987, la FOD de Costa Rica gesta y ejecuta proyectos nacionales y regionales en el campo del desarrollo humano, la innovación educativa y las nuevas tecnologías. Estas iniciativas, han contribuido en forma decisiva a entender el uso de las tecnologías en la educación, como instrumentos para ampliar las potencialidades y funcionalidades de las personas.

Cuenta con un grupo fundador integrado por profesionales de diversos sectores, ampliamente reconocidos. Posee un equipo multidisciplinario, altamente calificado, que le permite poner en acción redes de trabajo internas e interinstitucionales para llevar a cabo programas ambiciosos de impacto real. Un grupo de asesores del Ministerio de Educación Pública (MEP), completa el equipo de la FOD, articulando la implementación de propuestas educativas en el marco del Programa Nacional de Informática Educativa (PRONIE MEP-FOD).

Sus diferentes proyectos han beneficiado a cientos de miles de personas en todo el territorio nacional, incluyendo niños y jóvenes estudiantes, educadores, profesionales, personas de las comunidades, pequeñas empresarias, personas con discapacidad y adultos mayores, con énfasis en la igualdad de oportunidades. Específicamente el PRONIE MEP-FOD, atiende a más de 652.400 estudiantes y a sus docentes, con una cobertura al cierre del 2017, de más de 87% de los estudiantes matriculados en la educación diurna, desde preescolar hasta III ciclo. (Fundación Omar Dengo, 2019)

Dentro de los propósitos del Programa, la equidad en el acceso a las tecnologías digitales mediante su universalización juega un papel determinante, por lo que la FOD y el MEP han realizado inversiones y esfuerzos sostenidos para favorecer a través de todos estos años, un crecimiento constante de la cobertura y de la población meta, lo cual ha permitido incluir además de estudiantes, a educadores, profesionales, personas de las comunidades y pequeños empresarios, entre otros.

En este sentido, uno de los cursos de acción definidos por la institución para éste crecimiento, planteó en 2016, la reorganización de las sedes del Programa Nacional de Informática Educativa MEP-FOD alrededor del país y el traslado a éstas de parte del personal destacado en su sede central con el fin de dinamizar el recurso humano en zonas y facilitar así las tareas de diseminación, monitoreo y evaluación de sus propuestas pedagógicas dirigidas al desarrollo de competencias digitales, científicas y tecnológicas para la innovación, el emprendimiento y la participación ciudadana que plantea la estrategia institucional.

2.2 Marco conceptual

2.2.1 Áreas de Conocimiento

Para el desarrollo del proyecto, las áreas de conocimiento requeridas dentro del campo de las tecnologías de información y comunicación serán:

a. Telemática: Para conceptualizar y desarrollar la solución, se requiere entendimiento sobre tipos de redes, dispositivos y medios de red, tecnologías de acceso a Internet, tendencias de red, seguridad de red, sistemas operativos de red, direccionamiento IP, reglas de comunicación, protocolos y estándares de red, conceptos y configuración de conmutación, enrutamiento, VPN y supervisión de la red. Para esta área de conocimiento, se requiere de un proceso de comprensión y profundización que permita conceptualizar el modelo lógico de red, definir los requerimientos técnicos del modelo, implementar la solución y monitorearla.
b. Seguridad: La solución telemática deberá estar acorde a las buenas prácticas planteadas por las "Normas técnicas para la gestión y el control de las Tecnologías de Información" (Contraloría General de la República, 2007) a las cuales está sujeta la Fundación Omar Dengo, así como el uso de las buenas prácticas que plantean "Cobit" (IT Governance Institute, 2007) e "ISO/IEC 27002:2013" (Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, 2013) para los controles de seguridad de la información. Para esta área de conocimiento, se requiere un proceso de comprensión y profundización que permita concebir una solución con los niveles de seguridad de la información que indica la normativa.

c. Administración de Proyectos: Para administrar el proyecto, se hará uso de la Guía de los Fundamentos para la Dirección de Proyectos (Project Management Institute, Inc., 2008) como referencia para aplicar buenas prácticas en lo referente a la gestión de proyectos.

2.2.2 Red de área local

La Fundación Omar Dengo cuenta en su sede central con una red de área local (LAN, por sus siglas en inglés para Local Area Network) la cual actúa como infraestructura de red para proporcionar acceso a los usuarios y dispositivos a servicios de red como:

- Autenticación y control de acceso a los recursos de "Active Directory" de Microsoft Windows.
- Internet.
- Correo electrónico.
- Telefonía IP.
- Servidor de fax.
- VPN.
- Sistema biométrico de control de asistencia.
- Sistema de control de acceso.
- Sistema de gestión de video.
- Intranet.
- Sistemas de información.
- Filtrado de contenido.
- Administración centralizada de la seguridad en los equipos (Cortafuegos, Antivirus y AntiSpyware).

- Servidor de archivos.
- Servidor de actualizaciones.
- Servidor de respaldos.
- Dispositivos de impresión y digitalización de documentos.
- Herramientas colaborativas como el Skype Empresarial y el Jabber de Cisco.
- La mesa de servicio.
- Soporte remoto.

2.2.3 Red de área metropolitana

La solución telemática contempla en su modelo de red, la implementación de una red de área metropolitana (MAN, por sus siglas en inglés para Metropolitan Area Network) para poder establecer la relación de interconectividad entre la sede central y las sedes que se ubican a lo largo y ancho del país.

2.2.4 Internet

Para lograr la comunicación de los recursos de red de la sede central y las sedes locales, Internet será el canal que asuma el rol para interconectar dichas sedes, el cual será suplido por un proveedor de servicios de Internet (ISP, por sus siglas en inglés para Internet Service Provider).

2.2.5 Modelo OSI

Para desarrollar la metodología del proyecto, se referenciará el modelo de interconexión de sistemas abiertos (OSI, por sus siglas en inglés para Open System Interconnection), el cual lista en 7 categorías o capas, todas las funciones de red necesarias para enviar datos:

- Capa 7 - Aplicación: Es la más cercana al usuario final. Interactúa directamente con las aplicaciones de software para comunicarse a través de la red.

- Capa 6 - Presentación: Proporciona una representación común de los datos transferidos, asegurando que la información enviada desde la capa de aplicación de un dispositivo pueda ser leída por el dispositivo destino.
- Capa 5 Sesión: Es responsable de establecer, mantener y finalizar sesiones de comunicación entre aplicaciones que se ejecutan entre diferentes dispositivos.
- Capa 4 - Transporte: Se ocupa de segmentar, transferir y reensamblar los datos de extremo a extremo entre la fuente y el destino.
- Capa 3 - Red: Establece los protocolos enrutados y de enrutamiento para intercambiar paquetes a través de la red entre dispositivos finales identificados.
- Capa 2 - Enlace de datos: Define el formato para intercambiar tramas de datos entre dispositivos a través de un medio común.
- Capa 1 - Física: Define las especificaciones para los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia un dispositivo de red y desde él.

2.2.6 Dispositivos de red

Los elementos de hardware sobre los cuales se sustenta la solución telemática serán de naturaleza intermediaria: conmutador, puntos de acceso inalámbrico, enrutador y cortafuegos.

2.2.7 Medios de red

Para interconectar los dispositivos de red intermediarios, el medio de red a utilizar serán cables de cobre y fibra óptica según corresponda. La transmisión inalámbrica sería aplicada únicamente cuando no sean factibles los medios citados anteriormente.

2.2.8 Tecnologías de acceso a Internet

La Fundación Omar Dengo en su sede central utiliza como opción de conexión corporativa, enlaces de banda ancha sincrónicos (Misma velocidad de subida y bajada) de alta disponibilidad mediante fibra óptica. Para las sedes, dependerá de la factibilidad de los proveedores de servicios de Internet para colocar enlaces de banda ancha sincrónicos mediante fibra óptica o transmisión inalámbrica cuando no sea factible usar fibra óptica.

2.2.9 Tendencias de red

Por otro lado, la Fundación Omar Dengo como institución enfocada en la educación, la tecnología y el desarrollo, debe mantenerse vigente de cara a las tendencias de las nuevas tecnologías y tendencias en las redes para permitir que los usuarios, los dispositivos y la información estén conectados. Dichas tendencias se ven plasmadas en los ambientes de colaboración, el uso de la nube y el uso de dispositivos personales, por lo que la solución telemática debe ser consecuente con las tendencias para comunicarse y acceder a la información.

2.2.10 Seguridad de red

La seguridad es parte integral de la solución de interconexión que debe existir entre la sede central de la Fundación Omar Dengo y las sedes locales. Bajo este contexto, deberá proteger las comunicaciones, los datos y mantener la calidad de los servicios de red. Si bien es cierto muchas de las amenazas se propagan por Internet, las violaciones de seguridad de datos también se dan por los usuarios internos de la red, lo cual se atribuye a la pérdida o robo de dispositivos o al mal uso que los usuarios le puedan dar a la información ya sea malintencionadamente o no. Dentro de las amenazas comúnmente dadas están:

- Virus, gusanos y caballos de Troya: software malintencionado que se ejecuta en los dispositivos del usuario.

- Spyware y adware: software instalado en los dispositivos del usuario con el fin de recopilar datos sobre el usuario de forma secreta.
- Ataques por denegación de servicio: ataques diseñados para reducir o anular completamente servicios de red.
- Robo de datos: ataque para capturar información privada de la organización mediante la red.
- Phishing: ataque para robar las credenciales de inicio de sesión de un usuario a fin de acceder a datos privados mediante la suplantación de identidad.

Así mismo, una debilidad igualmente importante es la seguridad física de los dispositivos de red lo que puede denegar el uso de los servicios soportados por la red. Dentro de estas amenazas se encuentran:

- Hardware: daño físico de dispositivos y medios de red.
- Ambientales: temperatura o humedad extrema, desastres naturales.
- Eléctricas: picos/caídas de voltaje, ruido eléctrico y caída total del suministro eléctrico.
- Mantenimiento: descarga electrostática, falta de contratos de soporte que garanticen disponibilidad, cableado y etiquetado deficientes.

Por lo tanto, la solución telemática deberá abordar las amenazas de seguridad externas, internas y físicas.

2.2.11 Sistema operativo de red

La sede central de la Fundación Omar Dengo hace uso de tecnología Cisco para su infraestructura de red, por lo que el sistema operativo Internetwork (IOS, por sus siglas en inglés para Internetwork Operating System) de Cisco se refiere a los sistemas operativos de red que utiliza

el hardware Cisco para su funcionamiento, los cuales suelen tener diferentes características dependiendo del hardware, su uso y capacidad. Para la solución telemática será necesario conocer las capacidades de estos ya que en definitiva serán los encargados de soportar una comunicación segura entre la sede central y las sedes.

2.2.12 Direccionamiento IP

El uso de direcciones IP es lo que les permite a los dispositivos ubicarse entre sí para establecer la comunicación. Para poder establecer comunicación entre la sede central de la Fundación Omar Dengo y las sedes, será necesario contar con direccionamiento IP público de manera que los dispositivos de red intermediarios puedan llevar la comunicación a través de la Internet.

2.2.13 Reglas de comunicación

Las reglas de comunicación se refieren a los acuerdos o protocolos que definen los detalles sobre la forma en que los mensajes se transmitirán entre la sede central de la Fundación Omar Dengo y las sedes.

2.2.14 Protocolos y estándares de red

Los protocolos de red definen un formato y un conjunto de reglas comunes para intercambiar mensajes entre dispositivos que, aunado al uso de estándares en el desarrollo y la implementación de estos, permite asegurar que los dispositivos de red de distintos fabricantes puedan interactuar correctamente. Cuando se deba definir el modelo técnico de la solución, la definición clara de los protocolos y estándares de red será quien defina los requerimientos técnicos necesarios para garantizar la compatibilidad con los dispositivos de red con los que cuenta la sede central de la Fundación Omar Dengo.

2.2.15 Conceptos y configuración de conmutación

Los conmutadores serían los dispositivos de red responsables de controlar el flujo de datos y de dirigirlo a los recursos conectados a la red LAN. Estos dispositivos deben configurarse manualmente mediante su sistema operativo de red para ajustar las necesidades y seguridad de la red. Así mismo se habilitaría la administración remota de los mismos, de manera que puedan ser gestionados y monitorizados desde la sede central de la Fundación Omar Dengo.

2.2.16 Conceptos y configuración de enrutamiento

Los enrutadores serían los dispositivos de red encargados de controlar el flujo de datos a través de las distintas sedes que interconectaría la WAN. Estos dispositivos deben configurarse manualmente mediante su sistema operativo de red para ajustar las necesidades y seguridad de la red. Así mismo se habilitaría la administración remota de los mismos, de manera que puedan ser gestionados y monitorizados desde la sede central de la Fundación Omar Dengo.

2.2.17 VPN (Abreviatura de Virtual Private Network)

Para que el flujo de datos entre los enrutadores se dé de manera segura a través de un medio inseguro como lo es Internet, las redes privadas virtuales (VPN) establecerían la conexión virtual entre los enrutadores de las sedes y la sede central de la Fundación Omar Dengo para que el envío de información sea seguro.

2.2.18 ACL (Abreviatura de Listas de Control de Acceso)

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo con alguna condición.

2.2.19 IPSec (Abreviatura de Internet Protocol Security)

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

2.2.20 BGP (Abreviatura de Border Gateway Protocol)

El protocolo BGP se utiliza para intercambiar información mediante el establecimiento de una sesión de comunicación entre los enrutadores de frontera de los sistemas autónomos. Para conseguir una entrega fiable de la información, se hace uso de una sesión de comunicación basada en TCP en el puerto número 179. Esta sesión debe mantenerse activa debido a que ambos extremos de la comunicación periódicamente se intercambian y actualizan información. Al principio, cada enrutador envía al vecino toda su información de encaminamiento y después únicamente se enviarán las nuevas rutas, las actualizaciones o la eliminación de rutas transmitidas con anterioridad y periódicamente se envían mensajes para garantizar la conectividad.

2.2.21 Cortafuegos

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuego a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

2.2.22 Cisco IOS (Abreviatura de Internetwork Operating System)

Es el software utilizado en la gran mayoría de enrutadores y conmutadores de Cisco Systems. IOS es un paquete de funciones de enrutamiento, conmutamiento, trabajo de internet y telecomunicaciones que se integra estrechamente con un sistema operativo multitarea.

2.2.23 Supervisión de la red

Para poder evaluar el uso, eficacia y eficiencia de la solución, es necesario el monitoreo de las estadísticas de los equipos y servicios de red que ofrece la infraestructura tecnológica. La actividad operativa de los mismos en el transcurso del tiempo permitirá retroalimentar la gobernanza de las tecnologías de información y comunicación para la toma de decisiones estratégicas. En este sentido se deberá hacer uso de protocolos que permitan administrar el rendimiento de la red, detectar y resolver problemas de red, así como proporcionar estadísticas de uso.

2.2.24 Microsoft Active Directory

Se trata de una estructura de base de datos jerárquica que comparte información de infraestructura para localizar, proteger, administrar y organizar los recursos del equipo y de la red, como archivos, usuarios, grupos, periféricos y dispositivos de red.

2.3 Marco metodológico

El desarrollo de este proyecto se basa en la metodología CISCO Top-Down, la cual tiene por objetivo diseñar redes que cumplan con los objetivos y requerimientos técnicos de una organización, centrándose en iniciar en la capa de aplicación del modelo OSI, es decir, que no se seleccionan los dispositivos de red y tecnologías hasta que se analicen dichos objetivos y requerimientos (Oppenheimer, 2011). A continuación, el ciclo para el diseño e implementación de la red telemática que plantea el proyecto:

Ilustración 1. Ciclo de diseño e implementación de redes. Elaboración propia.

2.3.1 Analizar los requerimientos

Esta fase comienza con la identificación de objetivos y requisitos técnicos. La tarea de caracterizar la red existente, incluyendo la arquitectura y el rendimiento de los principales segmentos y dispositivos de red. El último paso en esta fase es analizar el tráfico de red, incluyendo el flujo de tráfico y la carga, protocolo y los requisitos de calidad de servicio (QoS).

2.3.2 Desarrollar el diseño lógico

Durante esta fase, el diseñador de red desarrolla la topología de red, la cual, dependiendo del tamaño de la red y las características del tráfico, puede ser simple o compleja, lo que requiere jerarquía y modularidad. El diseñador de red también diseña un modelo de direccionamiento de capa de red y selecciona los protocolos de conmutación y enrutamiento. El diseño lógico también

incluye planificación de seguridad, gestión de redes y la investigación inicial sobre qué proveedores de servicios pueden cumplir con los requisitos de redes de área amplia (WAN) y acceso remoto.

2.3.3 Desarrollar el diseño físico

Durante esta fase, se seleccionan tecnologías y productos específicos para realizar el diseño lógico. El diseño de red físico comienza con la selección de tecnologías y dispositivos para redes de campus, incluidos cableado, conmutadores Ethernet, puntos de acceso inalámbricos, puentes inalámbricos y enrutadores. La selección de tecnologías y dispositivos para el acceso remoto y las necesidades de redes de área amplia (WAN) continúa. Además, la investigación sobre los proveedores de servicios, que comenzó durante la fase de diseño lógico, debe completarse durante esta fase.

2.3.4 Probar, optimizar y documentar el diseño

Para esta fase, los pasos son escribir e implementar un plan de prueba, construir un prototipo o piloto, optimizar el diseño de la red y documentar su trabajo con una propuesta de diseño de red. Si los resultados de la prueba indican algún problema de rendimiento, durante esta fase debe actualizarse el diseño para incluir características de optimización como el modelado de tráfico y los mecanismos avanzados de conmutación y enrutamiento.

2.3.5 Implementar y probar

Esta fase propone la ejecutar el cronograma de implementación, implementar el diseño de red y validarlo.

2.3.6 Monitorear y optimizar:

Para esta fase, se monitorea la operación de la red en producción para detectar problemas de rendimiento y cualquier falla y dar pie a su optimización.

CAPÍTULO III
PROCEDIMIENTO METODOLÓGICO

CAPÍTULO III: PROCEDIMIENTO METODOLÓGICO

3.1 Desarrollo del proyecto

De acuerdo con el marco metodológico, se desarrollan las fases planteadas por la metodología CISCO Top-Down para el diseño e implementación de la red telemática que plantea el proyecto.

3.1.1 Análisis de requerimientos

En esta fase del ciclo de diseño e implementación de redes, se identifican los objetivos y beneficios que persigue el proyecto, así como los requerimientos técnicos para la red telemática, buscando asociar dichos objetivos con la tecnología disponible. Para determinar dichos requerimientos técnicos, se valida el estado actual de la red telemática, identificando su arquitectura y rendimiento. A continuación, los puntos desarrollados:

3.1.1.1 Análisis de metas del negocio

Comprender los objetivos y las limitaciones del negocio, es un aspecto fundamental en el diseño de la red. Además de los antecedentes mencionados en la sección 1.1 de este documento, se indaga cómo está estructurada la organización bajo una perspectiva de reconocer la estructura de gestión, las principales comunidades de usuarios y caracterizar el flujo de tráfico.

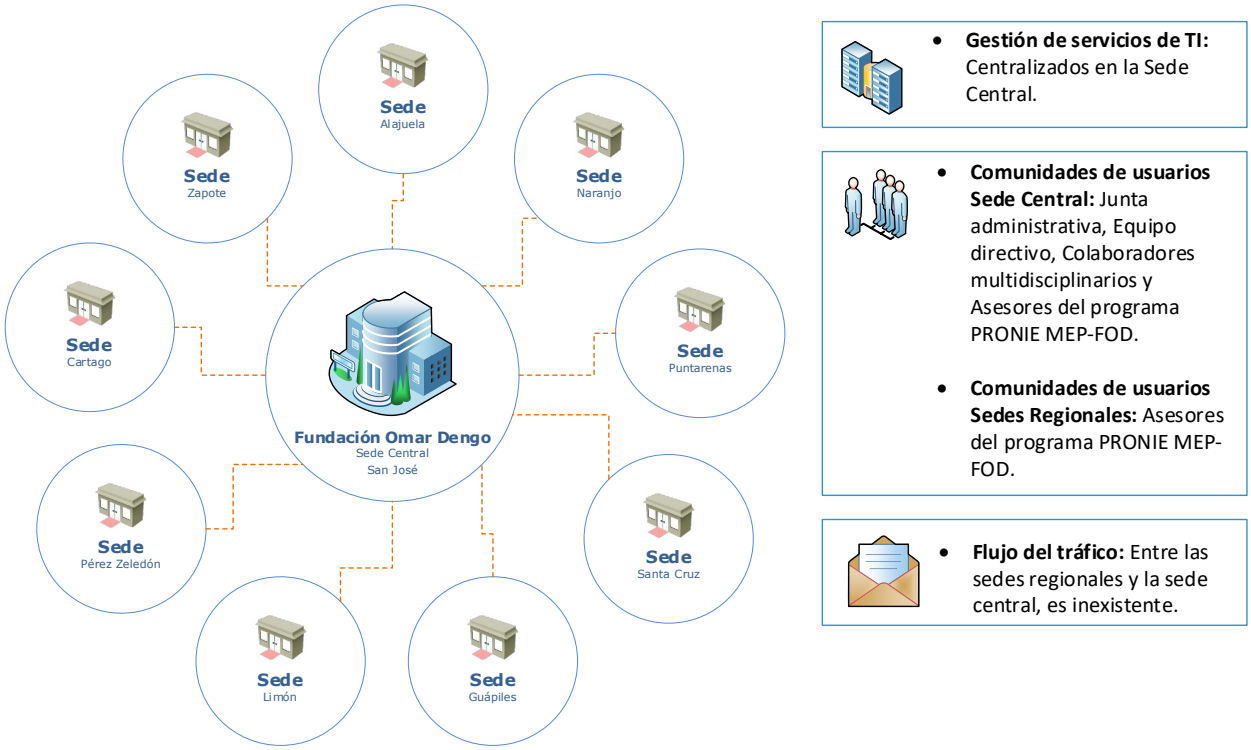


Ilustración 2. Estructura organizacional. Elaboración propia.

A partir de la problemática indicada en la sección 1.2 de este documento, a continuación, la representación gráfica del objetivo general del proyecto.

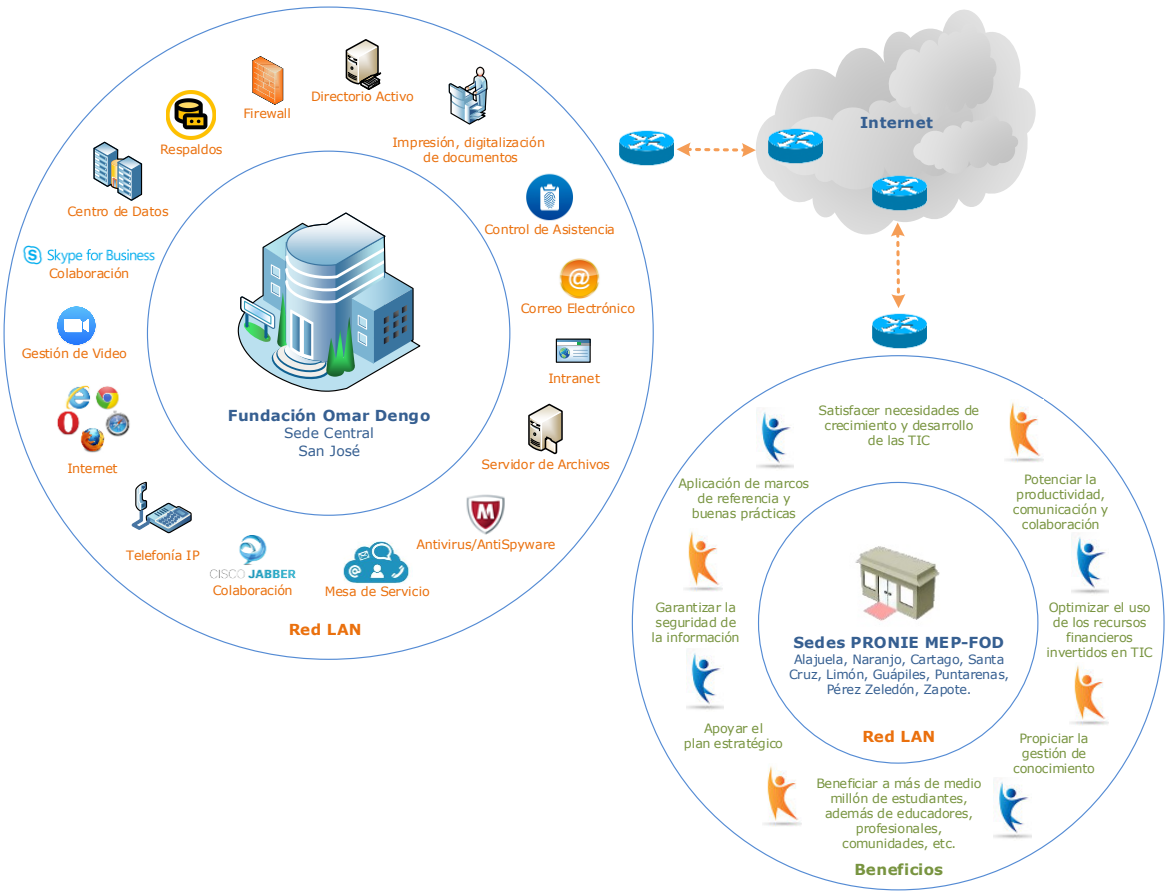


Ilustración 3. Objetivo general del proyecto. Elaboración propia.

Así, los beneficios esperados de la solución son:

1. Satisfacer las necesidades de crecimiento y desarrollo de las tecnologías de información y comunicación de la Fundación Omar Dengo, de forma controlada y estandarizada con base en un enfoque de eficiencia y mejoramiento continuo en concordancia con el plan estratégico institucional y los marcos de referencia y buenas prácticas que le atañan.
2. Contar en las sedes con enlaces corporativos que permitan una relación de negocio con el proveedor que facilite su gestión y negociación comercial, que ofrezcan una disponibilidad del 99.9 %, un mejor desempeño, así como la flexibilidad para cambiar el ancho de banda según se requiera y poder tener direccionamiento IP Público.

3. Garantizar la confidencialidad, integridad y disponibilidad de la información, de manera, que se cuente con las medidas de seguridad necesarias para el control de acceso a los recursos de TI y a la información, se proteja la integridad de la información y se asegure una continuidad razonable de los servicios de TI.
4. Optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando y potenciando en la medida de lo posible, el logro de los objetivos de esa inversión.
5. Potenciar el uso de los recursos tecnológicos facilitando el acceso, adopción y apropiación de estos a todos los colaboradores del Programa Nacional de Informática Educativa MEP-FOD ubicados a lo largo y ancho del país.
6. Asumir a través de las tecnologías de información y comunicación, el rol estratégico para apoyar la consecución de un proceso clave para la institución y de interés e impacto nacional como lo es el Programa Nacional de Informática Educativa MEP-FOD.

Al finalizar la ejecución del proyecto, la Fundación Omar Dengo contará con una solución telemática que permita la relación de interconectividad entre la sede central de la Fundación Omar Dengo y las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD ubicadas a lo largo y ancho del territorio nacional, de manera que todos los funcionarios cuenten con las fuentes de información y herramientas de productividad, comunicación y colaboración necesarias para desarrollar sus labores de la mejor manera posible.

En lo referente al estado actual de la red telemática, se determina que la conexión de los dispositivos que conforman el borde de la red se realiza de la siguiente manera:

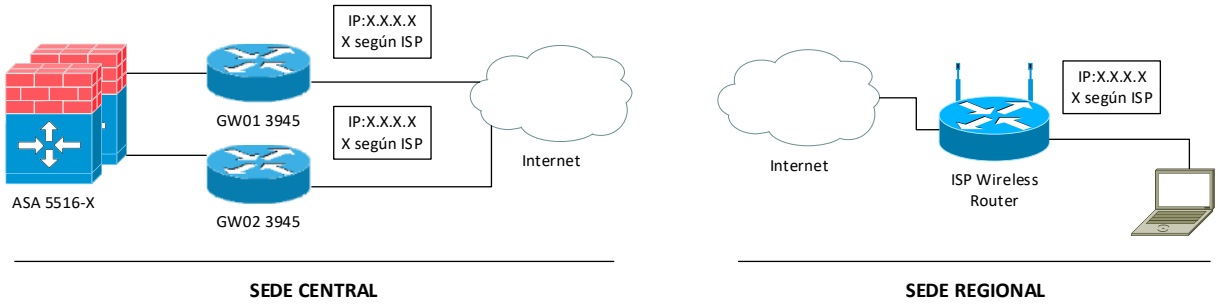


Ilustración 4. Estado actual de arquitectura. Elaboración propia.

Además, se establece que el rendimiento de la red telemática tanto para la sede central como para las sedes regionales está definido por las necesidades de desempeño del momento, es decir, no está claramente definido.

Para lograr implementar la solución de telemática, se encontró que la sede central cuenta con equipos que ofrecen las cualidades y capacidad necesarias para sumar las 9 sedes mencionadas a su red. En cuanto a las sedes, la institución cuenta con equipos en desuso, que reúnen las características técnicas necesarias para lograr dicha relación de interconectividad de forma segura con los equipos de la sede central.

Financieramente la institución cuenta con los recursos para invertir en el desarrollo del proyecto, así como para mantener la operación de este a través del tiempo. A continuación, se detalla el costo estimado del proyecto:

Tabla 1. Tabla de recursos y costos

Nombre del Recurso.	Tasa estándar.	Costo.
Administrador de Proyecto	₡10.500,00/hr	₡5.539.152,50
Patrocinador de Proyecto	₡12.500,00/hr	₡125.000,00
Encargado de Compras y Contrataciones	₡3.750,00/hr	₡147.000,00
Chofer	₡2.500,00/hr	₡112.500,00
Encargado de implementar el Proyecto	₡7.500,00/hr	₡3.232.500,00
Encargado de desarrollar el Proyecto	₡7.500,00/hr	₡2.580.000,00

Transporte y viáticos	₡50.000,00	₡1.800.000,00
Materiales de red	₡100.000,00	₡900.000,00
Enlaces (Mensualidad)	₡86.720,00	₡780.480,00
Equipos	₡350.000,00	₡3.150.000,00
	Total	**₡ 18.366.632,50**

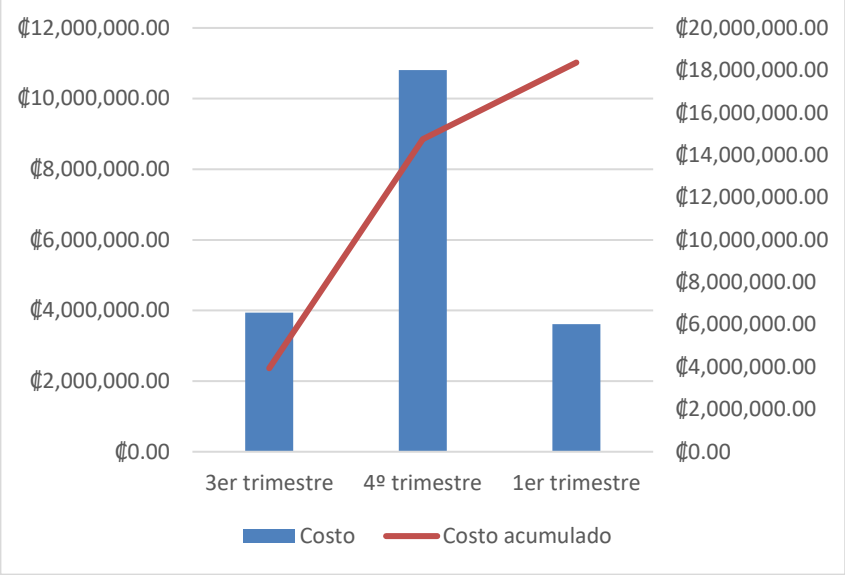


Ilustración 5. Flujo de caja (Línea base). Elaboración propia.

Además, se cuenta con el personal y recursos para desarrollar un proceso de comprensión y profundización en el área de las telecomunicaciones que permita conceptualizar el modelo lógico de red, definir los requerimientos técnicos del modelo, implementar la solución y monitorearla.

El desarrollo del proyecto no infringe ninguna norma o ley establecida, por lo que cuenta con la factibilidad legal necesaria para su ejecución y solo se debe velar por el cumplimiento de las "Normas técnicas para la gestión y el control de las Tecnologías de Información" (Contraloría General de la República, 2007) a las cuales está sujeta la Fundación Omar Dengo, así como aplicar las buenas prácticas que plantean "Cobit" (IT Governance Institute, 2007) e "ISO/IEC

27002:2013” (Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, 2013) para los controles de seguridad de la información.

3.1.1.2 Análisis de las metas técnicas

En este punto, se establecen los siguientes objetivos técnicos:

- Escalabilidad: en la medida de lo posible, se debe determinar el crecimiento que debe soportar el diseño de red para 1, 2 y 5 años. De acuerdo con el contexto de este proyecto, se plantea un crecimiento de 2 sedes con un promedio de 3 usuarios por sede durante los próximos 5 años y no se visualiza un mayor número de usuarios en las sedes regionales existentes del programa PRONIE MEP-FOD.
- Disponibilidad: se define la cantidad de tiempo que una red debe estar disponible para los usuarios en término de porcentaje de tiempo de actividad y se identifica su resiliencia, es decir, cuánto estrés puede manejar la red y la rapidez con la que la misma puede recuperarse de los problemas. Así mismo, se identifican los elementos de redundancia necesarios para alcanzar la disponibilidad definida. Este diseño de red estará sujeto, en la medida de lo posible, a los parámetros de disponibilidad definidos para la red existente de la Fundación Omar Dengo la cual es de un 99% anual, sin embargo, ello dependerá de la oferta de los proveedores de servicios de internet y de las características físicas del edificio de cada sede regional. Para ayudar a alcanzar dicha disponibilidad, cada sede regional contará con 1 enlace de internet de nivel empresarial, equipos de telecomunicaciones con servicios de soporte y garantía 8 x 5 x NBD (Next Business Day por sus siglas en inglés) y en términos de redundancia, con 1 sistema de protección y respaldo eléctrico para los equipos de telecomunicaciones.

- Rendimiento de la red: En la medida de lo posible se deben definir los requisitos de desempeño basados en un nivel de servicio acordado, o bien, hacer suposiciones sobre el rendimiento y el tiempo de respuesta. Este diseño de red supone un rendimiento promedio del 80% y un nivel de servicio de 8 x 5 x NBD (Next Business Day por sus siglas en inglés).
- Seguridad: Se identifican los activos de la red que deben protegerse analizando sus riesgos. Así mismo, se analizan amenazas potenciales, su probabilidad e impacto para la organización. Para este diseño de red, los equipos de interconexión serán ubicados físicamente en zonas dentro de las oficinas de las sedes regionales, a las cuales, únicamente tienen acceso el personal de la Fundación Omar Dengo.

  La gestión de los equipos de red estará protegida lógicamente por cuentas de usuario y derechos de acceso y se contará con respaldos y documentación de su configuración. En cuanto a la seguridad de la red, los usuarios y los datos estarán controlados mediante el servicio de autenticación del directorio activo y la transmisión de los datos entre las sucursales será protegida a través de una VPN. Así mismo los servicios de detección de intrusos y la protección de las aplicaciones y los datos proveídos por la sede central, se extenderán a las sedes regionales.
- Manejabilidad: Se establecen los objetivos con respecto a la capacidad de gestión que deben tener los administradores de la red. La gestión de los servicios de TI estará centralizada en la sede central de la Fundación Omar Dengo. La atención de los fallos y cambios de configuración será tramitada mediante la mesa de servicio, para lo cual se establecerán los incidentes y servicios, los acuerdos de servicio y especialistas encargados de su atención y solución. El administrador de red gestionará el rendimiento para analizar

el tráfico y el comportamiento de las aplicaciones con el propósito de optimizar la red. También supervisará y probará las políticas de seguridad, mantendrá y distribuirá las cuentas de usuario, y tendrá a su cargo la auditoría del cumplimiento de las políticas de seguridad.

- Usabilidad: Se fijan los objetivos con respecto a la facilidad de uso con la que los usuarios de la red pueden acceder a la red y sus servicios. Los usuarios de las sedes regionales accederán a la red de forma inalámbrica mediante usuario y contraseña para conectarse a la misma y los puntos de acceso harán uso del DHCP para la asignación dinámica de las direcciones IP a los equipos de los usuarios.
- Adaptabilidad: Al diseñar una red, debe intentarse evitar incorporar elementos que dificulten la implementación de nuevas tecnologías en el futuro. Para este diseño de red se seguirán las recomendaciones del fabricante de la red existente.
- Asequibilidad: Se validó que los costos de equipo no recurrentes y costos de operación de la red sean sostenibles presupuestalmente.

3.1.1.3 Análisis de la red existente

En este punto, se aborda y documenta la topología y estructura física, así como el rendimiento de la red, identificando cuellos de botella, dispositivos y enlaces que deban ser reemplazados para el nuevo diseño.

- Descripción de la infraestructura de red: Se comprende el flujo del tráfico mediante mapas de red para conocer la ubicación de los principales dispositivos de interconexión de redes y segmentos de red, indicando los nombres y direcciones de los principales dispositivos y segmentos, e identificando cualquier método estándar de direccionamiento. Así mismo se

toman en cuenta las restricciones arquitectónicas y ambientales, aspectos importantes que deben ser considerados.

- Mapas de red de las sedes:

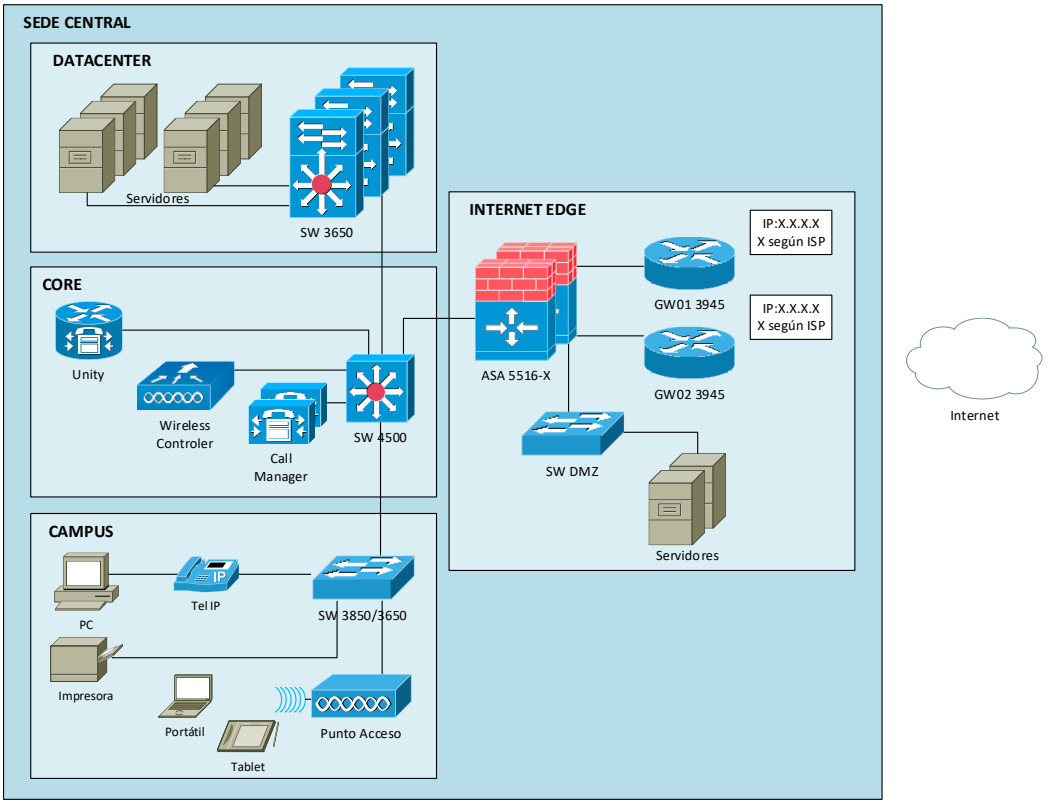


Ilustración 6. Mapa de red sede central. Elaboración propia.

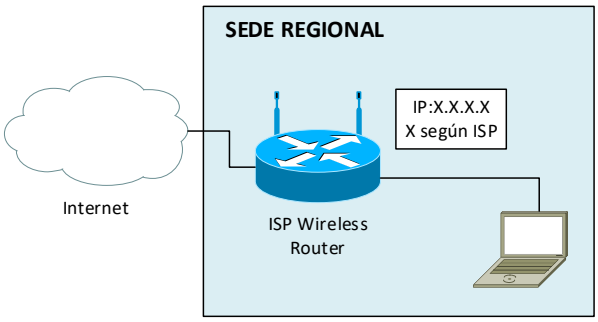


Ilustración 7. Mapa de red sede regional. Elaboración propia.

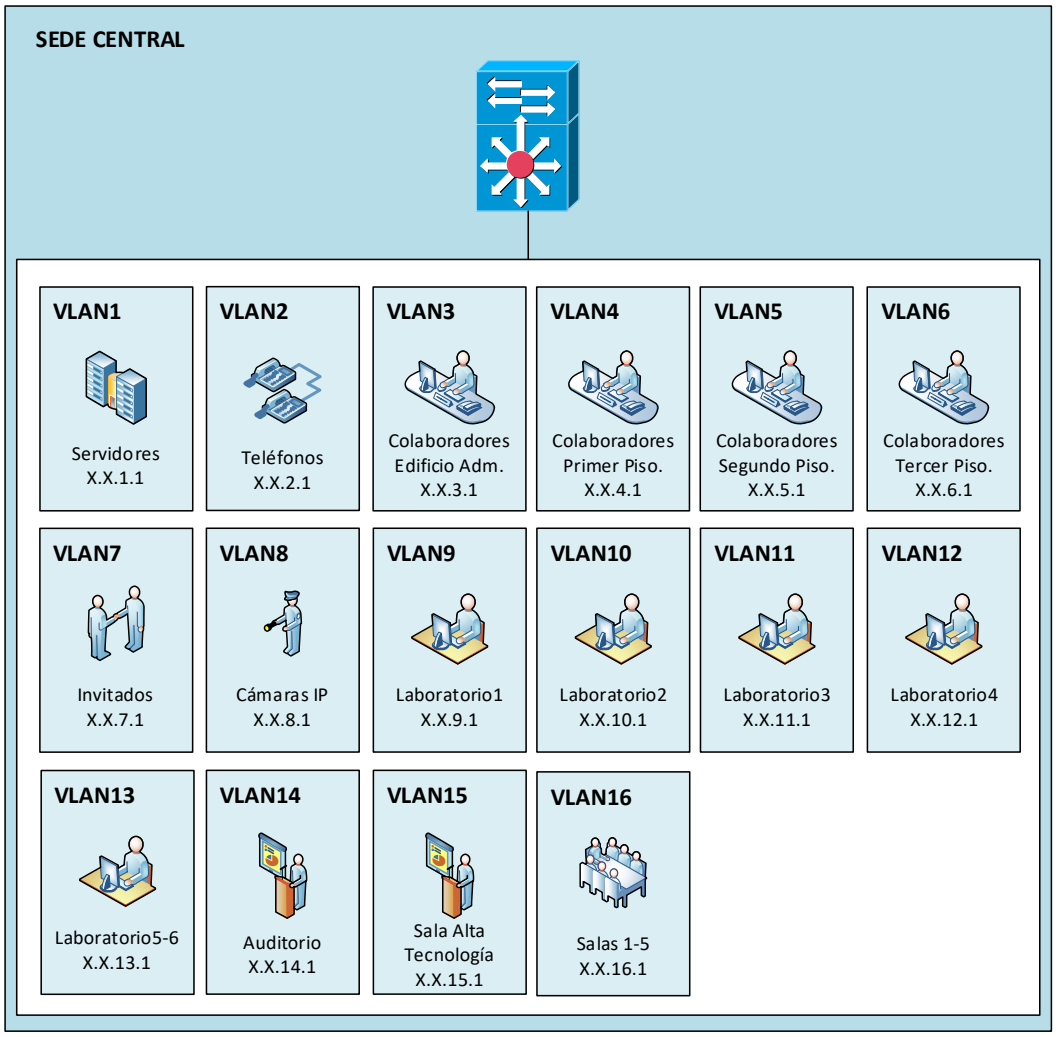


Ilustración 8. Mapa VLAN sede central. Elaboración propia.

- Direccionamiento y nombres de red: Se indaga sobre la nomenclatura o metodología para la asignación de nombres y direcciones de red, sin embargo, se carece de la existencia formal de la misma, por tanto, no es posible documentarla.
- Cableado y los medios: Si es posible, se deben documentar los tipos de cableado en uso, así como las distancias de los cables, de manera que se puedan planificar mejoras e identificar inconvenientes de cara a los objetivos de escalabilidad y disponibilidad para el nuevo diseño de red, sin embargo, el cableado y medios de

la red existente de la sede central, se encuentran certificados y no suponen ser parte del proyecto. En cuanto a las sedes regionales, el cableado y medios serán nuevos y estarán limitados a los equipos de red, impresora y lector biométrico dado que los usuarios se conectarán vía inalámbrica.

- Limitaciones ambientales y arquitectónicas: Se identifican situaciones medioambientales y legales, así como inconvenientes arquitectónicos que puedan afectar la viabilidad de la implementación del diseño de red. Se hace una visita a cada sede regional para identificar problemas de reflexión, absorción, refracción o difracción de la señal inalámbrica y en todos los casos, no se encuentra mayor inconveniente. Así mismo, al estar las sedes en edificios alquilados, se solicita a cada arrendatario su permiso para la realización de las tareas que representen cambios sobre la infraestructura física del inmueble.
- El estado actual: Se estudia el rendimiento de la red existente para contar con una medición de referencia a partir del cual medir el rendimiento de la nueva red. Así mismo, se examinan las características de disponibilidad de la red existente y se cuantifican los períodos de inactividad de la red existente. El esquema de las sedes regionales no ofrece un nivel de disponibilidad de acceso a internet de grado empresarial, no cuenta con fuentes de respaldo de energía para los equipos de red y los periodos de inactividad de la red han llegado al 12% anual. También se revisa la utilización de la red en términos del porcentaje de la capacidad de ancho de banda de internet utilizado en un periodo de tiempo determinado, llegando a consumirse el 100% en ocasiones debido a la demanda, o bien por sobresuscripción del servicio.

3.1.1.4 Análisis del tráfico existente

En este punto, se documenta el flujo de tráfico, el volumen de tráfico, el comportamiento del tráfico y los requisitos de calidad de servicio.

- Flujo de tráfico: Se deben identificar y documentar las fuentes y los destinos del tráfico de la red existente, así como analizar la dirección y simetría de los datos que viajan entre fuentes y destinos, sin embargo, el tráfico entre sede central y las redes regionales es inexistente, por lo que solo se identifican los grupos de usuarios y las aplicaciones y servicios de red, con lo cual se definirán los requisitos de calidad del servicio en las etapas de diseño.

Tabla 2. Comunidades de usuarios.

Nombre.	**Tamaño.**	**Ubicación.**	**Aplicaciones usadas.**
Sede Central: Junta administrativa, Equipo directivo, Colaboradores multidisciplinarios y Asesores del programa PRONIE MEP-FOD.	350.	San José.	Correo electrónico, navegador web, telefonía IP, impresión y digitalización de documentos, el servidor de fax, el sistema biométrico de control de asistencia, el controlador de dominio, la Intranet, los sistemas de información, el filtrado de contenido, servicios de seguridad como Cortafuegos, Antivirus y AntiSpyware, servicios de respaldo de información, los servidores de archivos, las herramientas colaborativas como el Skype Empresarial y el Jabber de Cisco, la mesa de servicio y el soporte remoto.

Sede Regional 01: Asesores del programa PRONIE MEP-FOD.	7	Alajuela.	Correo electrónico, Skype Empresarial y el navegador web.
Sede Regional 02: Asesores del programa PRONIE MEP-FOD.	4	Naranjo.	Correo electrónico, Skype Empresarial y el navegador web.
Sede Regional 03: Asesores del programa PRONIE MEP-FOD.	4	Puntarenas.	Correo electrónico, Skype Empresarial y el navegador web.
Sede Regional 04: Asesores del programa PRONIE MEP-FOD.	10	Santa Cruz.	Correo electrónico, Skype Empresarial y el navegador web.
Sede Regional 05: Asesores del programa PRONIE MEP-FOD.	4	Guápiles.	Correo electrónico, Skype Empresarial y el navegador web.
Sede Regional 06: Asesores del programa PRONIE MEP-FOD.	2	Limón.	Correo electrónico, Skype Empresarial y el navegador web.
Sede Regional 07: Asesores del programa PRONIE MEP-FOD.	4	Pérez Zeledón.	Correo electrónico, Skype Empresarial y el navegador web.
Sede Regional 08: Asesores del programa PRONIE MEP-FOD.	8	Cartago.	Correo electrónico, Skype Empresarial y el navegador web.

Sede Regional 09: Asesores del programa PRONIE MEP-FOD.	6	Zapote.	Correo electrónico, Skype Empresarial y el navegador web.

- Volumen de tráfico: Con el objetivo de evitar cuellos de botella, se investiga el comportamiento del tráfico de las principales aplicaciones de la sede central para la comunidad de usuarios de la sede central Asesores del programa PRONIE MEP-FOD, en donde se identifican los patrones de uso mediante la herramienta SolarWinds NetFlow Traffic Analyzer.

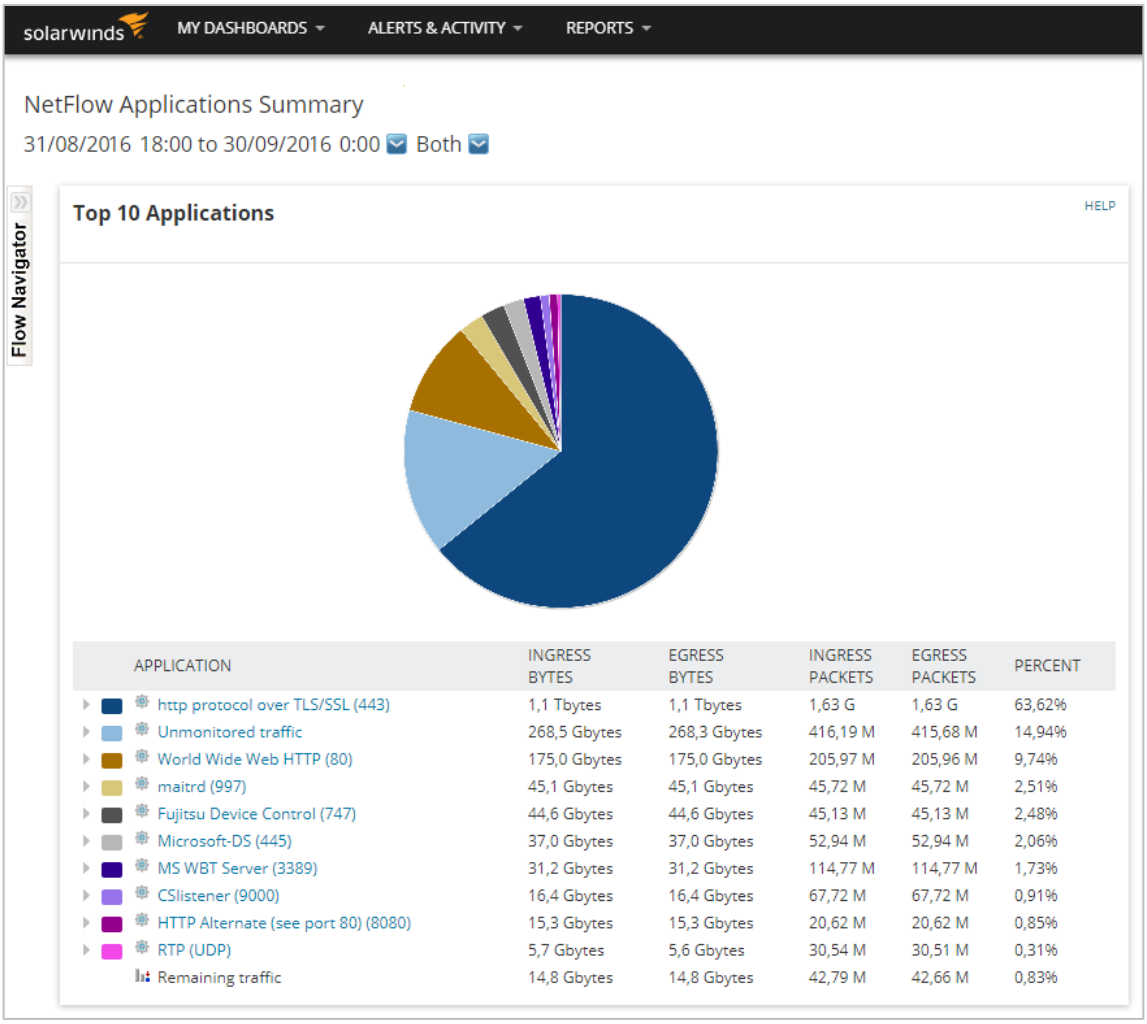


Ilustración 9. Volumen del tráfico - Aplicaciones. Elaboración propia.

Una forma de calcular la carga de tráfico consiste en determinar el número de estaciones que transmiten, la rapidez con la que cada estación genera mensajes, el tamaño de los mensajes, así como la estimación de la carga de tráfico causada por los protocolos de enrutamiento en relación con la topología de red. Se identifican los principales protocolos de enrutamiento que se ejecutan en la red existente.

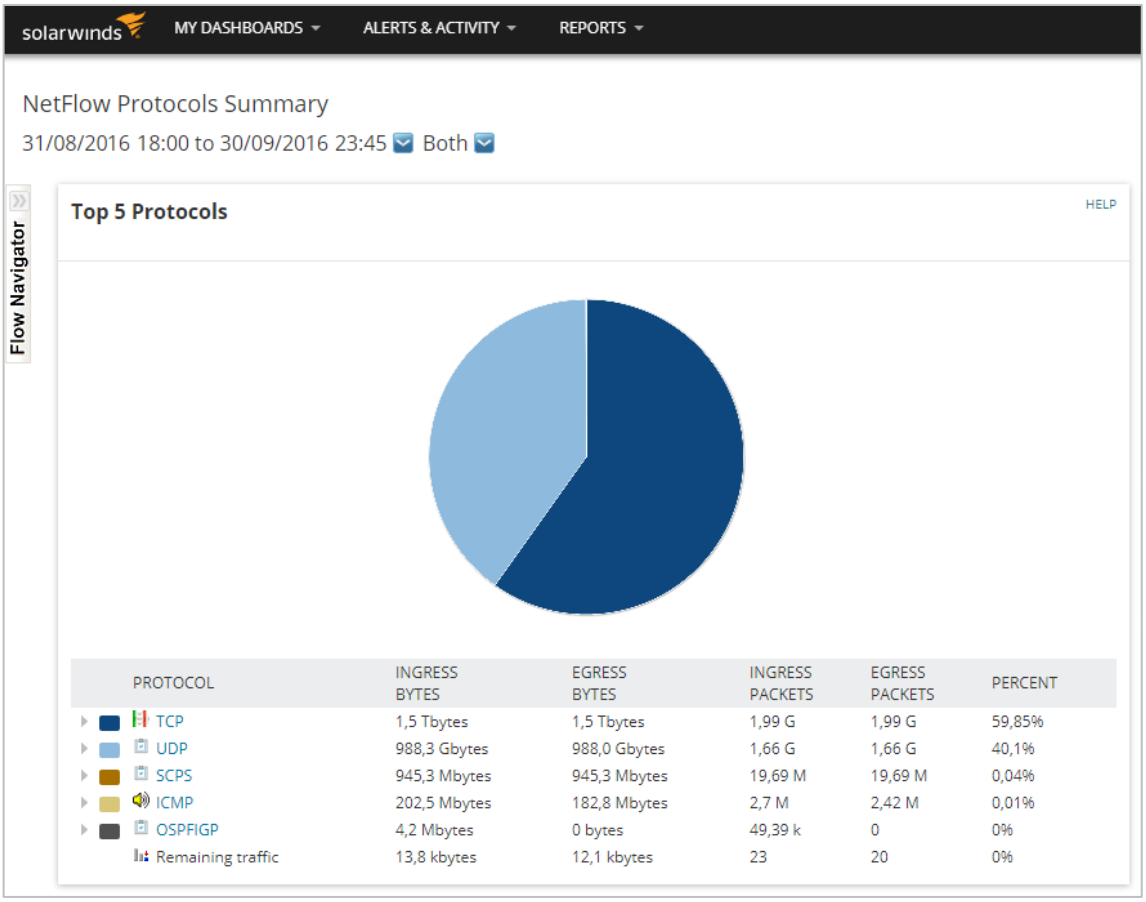


Ilustración 10. Volumen del tráfico - Protocolos. Elaboración propia.

- Comportamiento del tráfico: Se examina el uso del ancho de banda de las aplicaciones y los protocolos, tomando en cuenta cómo la interacción de los protocolos utilizados por la aplicación, control de flujo y mecanismos de recuperación de errores, afectan su comportamiento.

Tabla 3. Comportamiento del tráfico.

Aplicación.	**Comunidad de usuarios.**	**Tipo de tráfico.**	**Protocolo.**	**Ancho de banda aproximado.**	**Comportamiento.**

Correo electrónico.	Sede Central: Asesores del programa PRONIE MEP-FOD.	Cliente / Servidor	TCP	1.77 Kbps por usuario.	512 KB en promedio por mensaje, con un promedio de 10 correos entregados y 40 recibidos al día. (25,600 KB por usuario / 28,800 Seg) * 2 = 1.77 Kbps.
Navegador web.	Sede Central: Asesores del programa PRONIE MEP-FOD.		TCP	85.33 Kbps por usuario.	1,228,800 KB en promedio al día. (1,228,800 KB por usuario / 28,800 Seg) * 2 = 85.33 Kbps.
Jabber de Cisco.	Sede Central: Asesores del programa PRONIE MEP-FOD.		TCP	384 Kbps por usuario.	De acuerdo con las recomendaciones del fabricante para una red empresarial.
Servidores de archivos.	Sede Central: Asesores del programa PRONIE MEP-FOD.		TCP&UDP	42.66 Kbps por usuario.	614,400 KB en promedio al día. (614,400 KB por usuario / 28,800 Seg) * 2 = 42.66 Kbps.
Intranet.	Sede Central: Asesores del		TCP	35.55 Kbps.	512,000 KB en promedio al día. (400

	programa PRONIE MEP-FOD.	KB por usuario / 28,800 Seg) * 2 = 35.55 Kbps.

- Requisitos de calidad de servicio: Se clasifican y documentan las aplicaciones en flexibles o inflexibles, de manera que se pueda determinar la practicidad de tomar prestado ancho de banda de las aplicaciones flexibles para mantener la aplicación inflexible en funcionamiento.

Tabla 4. Requisitos de calidad de servicio.

Aplicación.	**Comunidad de usuarios.**	**Flexibilidad.**
Correo electrónico.	Sede Central: Asesores del programa PRONIE MEP-FOD.	Inflexible.
Navegador web.	Sede Central: Asesores del programa PRONIE MEP-FOD.	Flexible.
Jabber de Cisco.	Sede Central: Asesores del programa PRONIE MEP-FOD.	Inflexible.
Servidores de archivos.	Sede Central: Asesores del programa PRONIE MEP-FOD.	Inflexible.
Intranet.	Sede Central: Asesores del programa PRONIE MEP-FOD.	Inflexible.

3.1.2 Desarrollo del diseño lógico

Esta fase conceptualiza y define el modelo del diseño de red telemática. A partir de la fase anterior, se construye el diagrama de red telemática en donde se denota la topología, el

direccionamiento, protocolos de conmutación, estrategia de seguridad e identificación de proveedores de servicios.

3.1.2.1 Diseño de la topología de red

En este punto, se identifican redes y puntos de interconexión, el tamaño y el alcance de las redes y los tipos de dispositivos de interconexión que serán necesarios. Para los requerimientos de este proyecto, se aborda un modelo de perímetro empresarial, en donde se identifica el perímetro MAN para conectar las sedes, las VPN de sitio a sitio y acceso remoto, así como el perímetro para conectarse a la Internet a través de la infraestructura perimetral de un proveedor de servicios que permita cifrar los datos a través de un túnel IPSec.

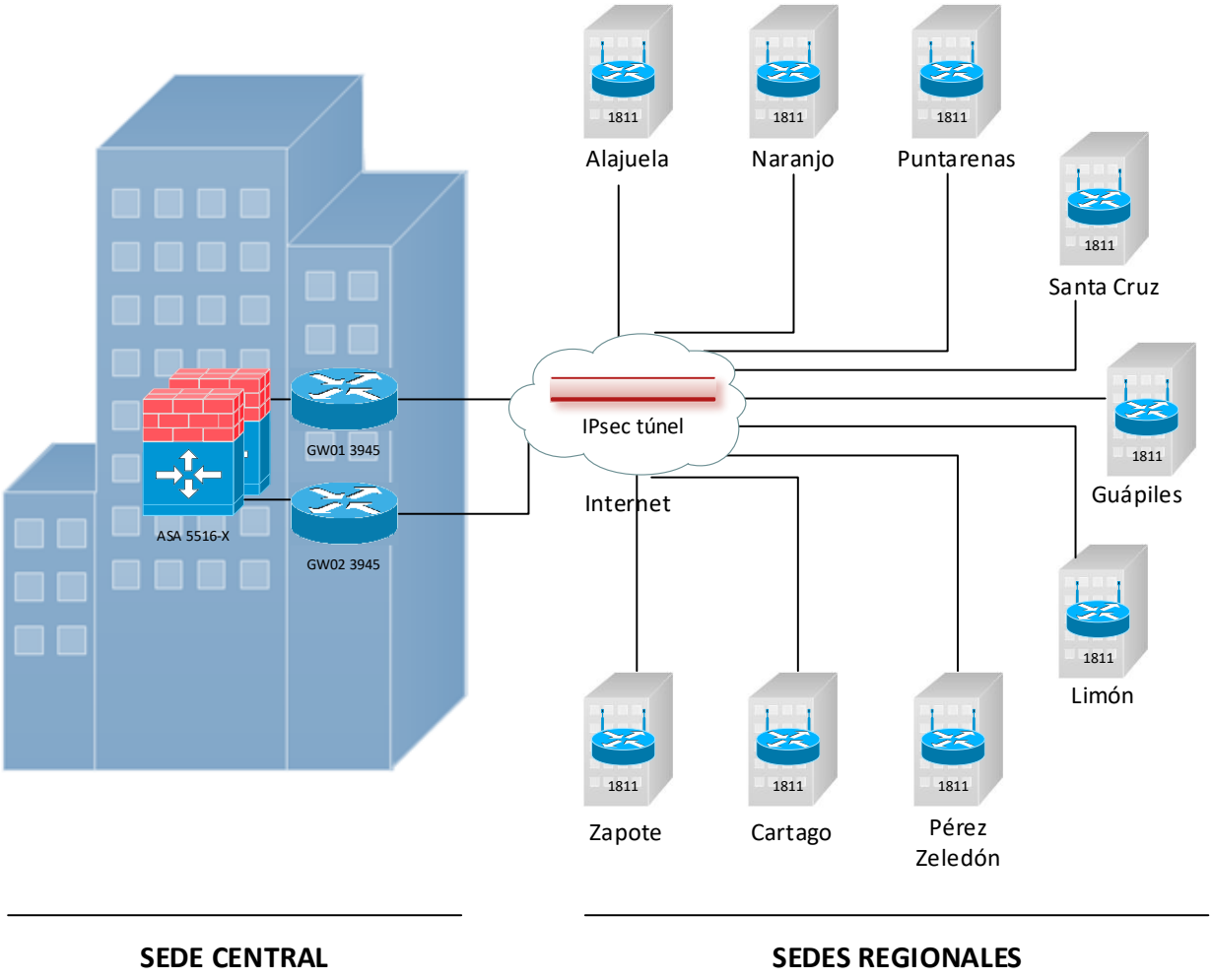


Ilustración 11. Modelo del perímetro empresarial. Elaboración propia.

A partir de dicho modelo, para la relación de conectividad entre la sede central y las sedes regionales, se identifica que el uso de una topología de red en estrella cumple con los requerimientos planteados para el proyecto.

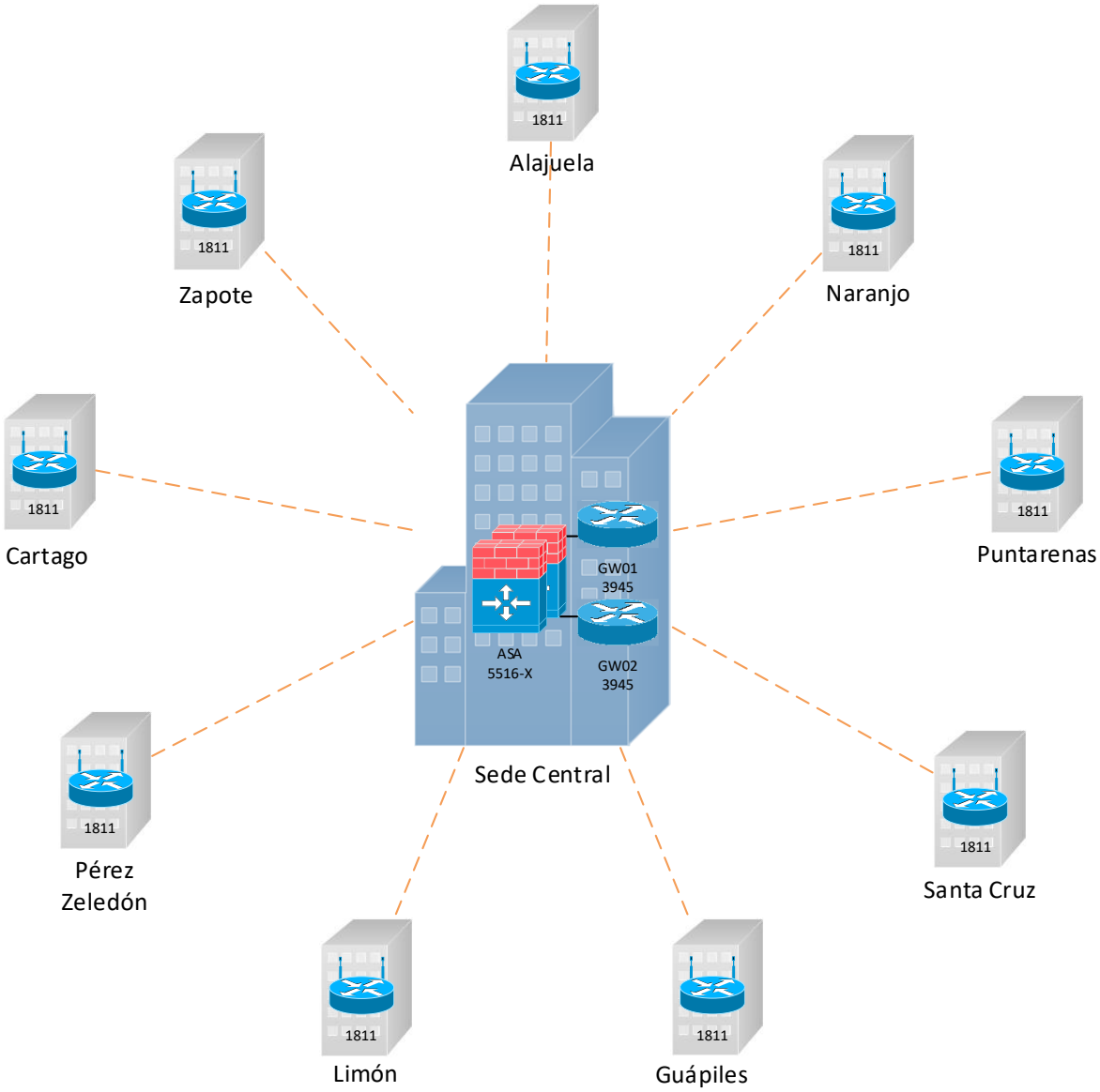


Ilustración 12. Diseño de topología de red entre sedes. Elaboración propia.

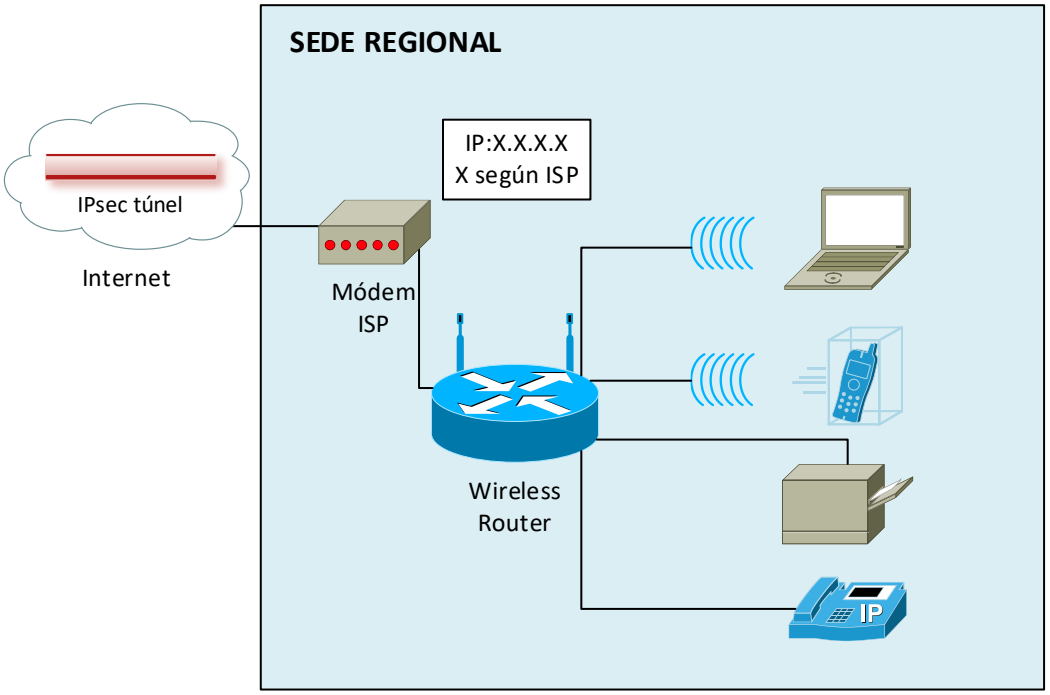


Ilustración 13. Diseño topología de red sedes regionales. Elaboración propia.

3.1.2.2 Diseño de los modelos de direccionamiento

Se asignan las direcciones y nombres a los componentes de red a partir de en un modelo estructurado que permita dicha asignación de manera sistemática, facilitando la escalabilidad, el rendimiento y la capacidad de gestión. A partir de la comprensión de la estructura organizativa identificada en la fase de "Analizar los requerimientos", se plantea el siguiente modelo para planificar las direcciones y nombres:

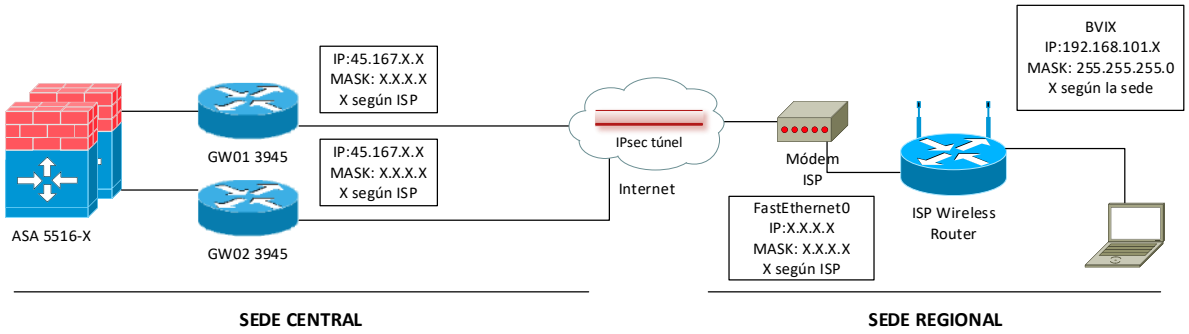


Ilustración 14. Diseño del modelo de direccionamiento. Elaboración propia.

3.1.2.3 Selección de los protocolos para conmutación y enrutamiento

Se validan los protocolos de enrutamiento y conmutación de acuerdo con los objetivos del negocio y a las metas técnicas, teniendo en cuenta:

- Las características del tráfico de red.
- El consumo de recursos de ancho de banda, memoria y procesamiento.
- El número aproximado de enrutadores o conmutadores en términos de escalabilidad.
- La capacidad de adaptarse rápidamente a cambios en la red.
- La capacidad de soportar características de seguridad.

La sede central utiliza el protocolo BGP para conmutación y enrutamiento, adecuándose idóneamente a las necesidades del proyecto. Para la comunicación entre la sede central y las sedes regionales, se hará mediante el protocolo IPSec, que en conjunto con listas de control de acceso y VLANS, dan pie a la extensión de la red de área metropolitana.

3.1.2.4 Desarrollo de las estrategias de seguridad

En cuanto a las políticas de seguridad, se plantea asegurar los componentes de la red telemática, considerando: las conexiones a Internet, el acceso remoto, redes y servicios de red,

usuarios y redes inalámbricas. En términos generales, el protocolo IPSec encripta la comunicación entre la sede central y las sedes regionales mediante la autenticación por contraseñas y en lo concerniente a los servicios de red, la seguridad se rige por las políticas de seguridad de la sede central, las cuales están enmarcadas por el servicio de Microsoft Active Directory.

3.1.2.5 Desarrollo de las estrategias de gestión de la red

En este punto, se debe definir una arquitectura de administración que permita medir qué tan bien se están cumpliendo los objetivos de diseño y ajustar los parámetros de la red si estos objetivos no se están cumpliendo. Al tratarse de una extensión de la red existente, se utilizarán las herramientas y recursos de administración aplicados en la sede central, como por ejemplo Cisco NetFlow.

3.1.3 Desarrollo del diseño físico

Para esta fase, se seleccionan las tecnologías y dispositivos que concuerden con lo definido en la fase de diseño lógico y se investigan las alternativas que ofrecen los proveedores de servicios de conectividad identificados en la fase anterior. Las tareas desplegadas son:

3.1.3.1 Selección de las tecnologías y dispositivos

La topología de cableado existente en la sede central está constituida por armarios de comunicaciones distribuidos en zonas estratégicas del edificio conectados a un cuarto de distribución principal mediante fibra óptica. Cada armario de comunicaciones habilita decenas de puntos de red mediante placas de pared con cableado UTP categoría 6a, así como puntos de acceso inalámbrico Wifi. Para cada una de las sedes regionales se utilizará 1 armario de cableado con puntos de red con cableado UTP categoría 5e para 1 teléfono IP, 1 impresora de red y el lector de huella digital. En cuanto al acceso a la red para los usuarios, se hará mediante el medio inalámbrico Wifi.

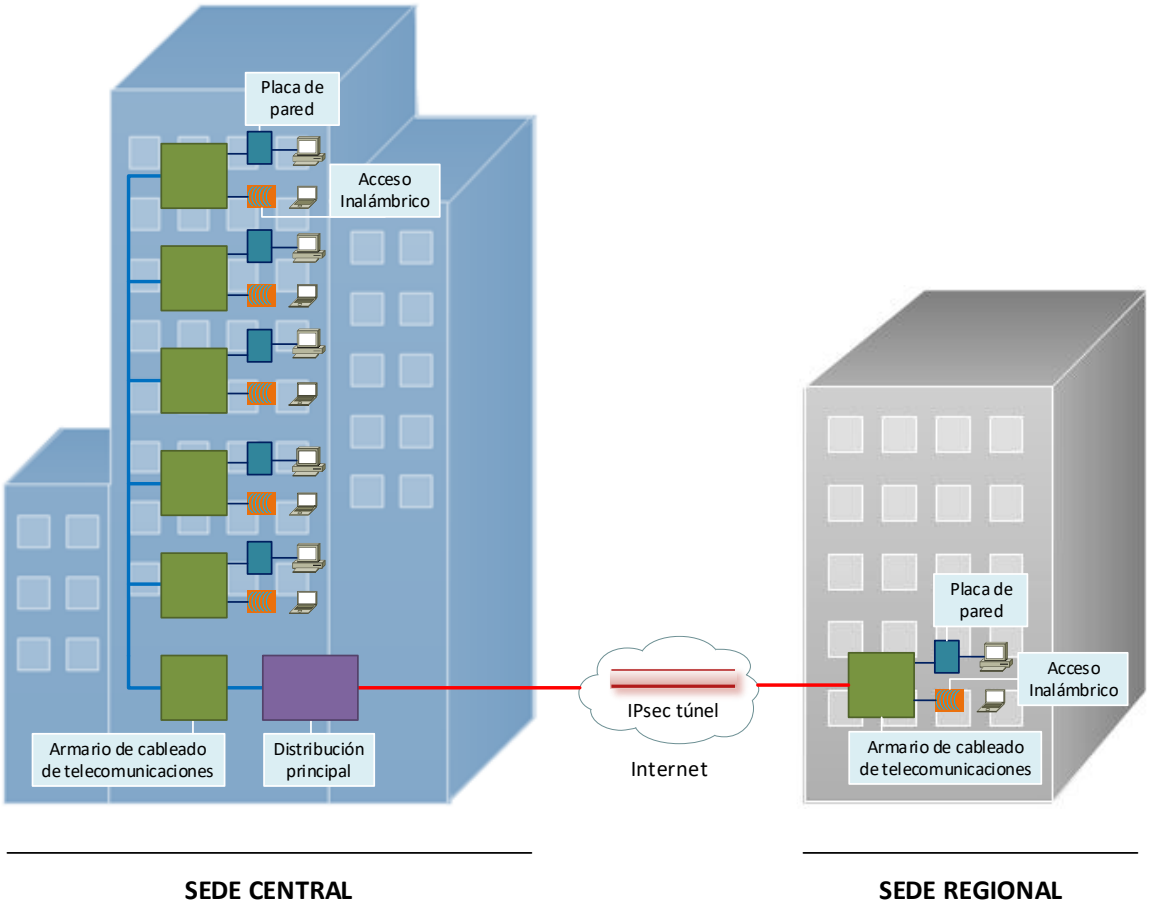


Ilustración 15. Topología del cableado. Elaboración propia.

En cuanto a los estándares de la capa física y de enlace de datos, se validan los utilizados en la red telemática existente:

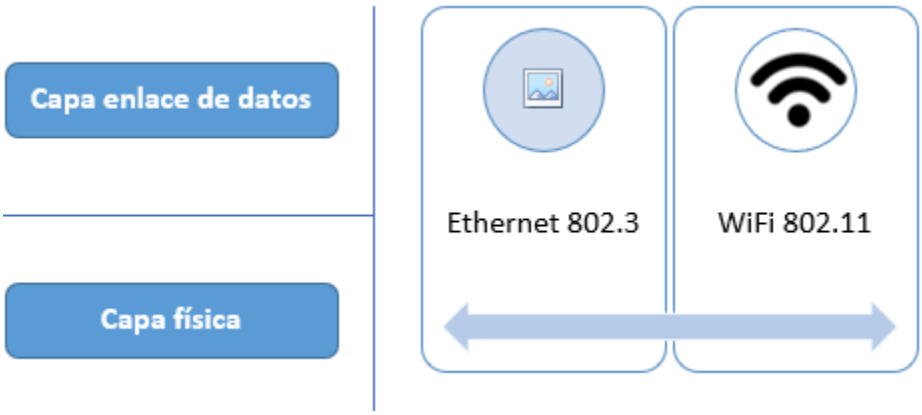


Ilustración 16. Estándares de capa física y enlace de datos. Elaboración propia.

Se validan los dispositivos de interconexión de red como conmutadores, enrutadores y puntos de acceso inalámbricos. La sede central cuenta con enrutadores de servicios integrados Cisco 3945 y Cisco ASA 5516 para gestionar el tráfico hacia internet y la seguridad. Consultando a especialistas e investigando las hojas de especificaciones de los equipos, éstos ofrecen características que permiten implementar servicios de VPN con seguridad IP (IPSec) para asegurar que el tráfico VPN no introduzca amenazas a la red LAN de la sede central. En cuanto a los equipos para las sedes, se cuenta con enrutadores de servicios integrados Cisco 1811, los cuales también soportan los servicios de VPN con seguridad IP (IPSec).

Se identifican como posibles proveedores de servicios de internet a:

- Tigo Business.
- Jasec.
- Kölbi Internet Empresarial.
- CableTica Empresarial.

No obstante, solo Tigo Business logra cubrir todas las áreas geográficas de las sedes regionales. En el anexo 1 se detalla la propuesta de servicios corporativos de Tigo Business por la cual se inclinó la Fundación Omar Dengo.

3.1.4 Pruebas, optimización y documentación del diseño

En esta fase se escribe e implementa un plan de prueba, se construye un prototipo y se optimiza, finalmente se documenta la propuesta de diseño de red telemática. Las tareas realizadas son:

3.1.4.1 Pruebas del diseño de red

Se construye un prototipo para verificar y demostrar el comportamiento del diseño de red mediante un enlace de internet corporativo de 512 Mbps ubicado en la sede central, un equipo Cisco 1811, una computadora portátil, un teléfono IP, una impresora de red y un lector biométrico. Para la configuración de los equipos, se toma como base la guía para configurar IPSec sitio a sitio entre un ASA y un enrutador del Cisco IOS detallada en el anexo 3. Como objetivos de las pruebas, se define:

1. Establecer la interconexión entre la sede central y el equipo Cisco 1811 de forma segura.
2. Conectar la computadora portátil al equipo Cisco 1811 de manera inalámbrica y acceder a los servicios de la red de la sede central.
3. Conectar el teléfono IP al equipo Cisco 1811 de manera cableada y validar el funcionamiento de las llamadas de voz.
4. Conectar la impresora de red al equipo Cisco 1811 de manera cableada, agregar la impresora al servidor de impresión de la sede central y realizar tareas de impresión.
5. Conectar el lector biométrico al equipo Cisco 1811 de manera cableada, agregar el dispositivo a la solución de control de asistencia y validar su funcionamiento.

A partir de los objetivos indicados, se despliegan las pruebas durante muchas ocasiones, en donde los criterios de aceptación consisten en que la solución sea funcional.

3.1.4.2 Optimización del diseño de red

A partir de la clasificación de las aplicaciones de red en donde se determinó la calidad de servicio (QoS) que requieren las aplicaciones, en la fase de "Analizar los requerimientos", se busca optimizar el diseño de red mediante técnicas que permitan usar el ancho de banda de manera eficiente, controlar el retardo y la fluctuación, y dar servicio preferencial a aplicaciones esenciales. En términos generales, durante las pruebas se trata de medir el rendimiento desde el punto de vista del usuario y se evalúa cuánto tiempo debe esperar un usuario al ejecutar operaciones típicas, sin embargo, el escenario de pruebas no permitía simular la ubicación real de una sede regional, ni la carga de muchos usuarios para validar aspectos de rendimiento. No obstante, el ciclo de diseño e implementación de redes enmarcado en la metodología de este proyecto considera una fase posterior a la implementación para el monitoreo y optimización de la red telemática, por lo que, de ser necesario, el diseño en términos de calidad de servicio (QoS), podría ser optimizado.

3.1.4.3 Documentación del diseño de red

Se escribe un documento de diseño integral que describe el desarrollo de las fases de requerimientos, diseño lógico, diseño físico, pruebas y optimización, que no es más que lo citado hasta este punto, al cual se le suma el plan de implementación del diseño de red definido en el siguiente cronograma general del proyecto.

Tabla 5. Calendario de hitos del cronograma del proyecto.

Hito.	**Inicio.**	**Fin.**
Etapa I – Gestionar Plan de Proyecto.	02/07/16	01/03/17

Etapa II – Análisis de situación, planteamiento de necesidades y escenarios de solución.	20/08/16	10/09/16
Etapa III – Propuesta del modelo de telecomunicaciones a implementar.	10/09/16	05/10/16
Etapa IV – Implementación de la solución modelada.	05/10/16	15/02/17
Etapa V – Evaluar el uso, eficacia y eficiencia de la solución.	15/02/17	18/02/17

Cronograma

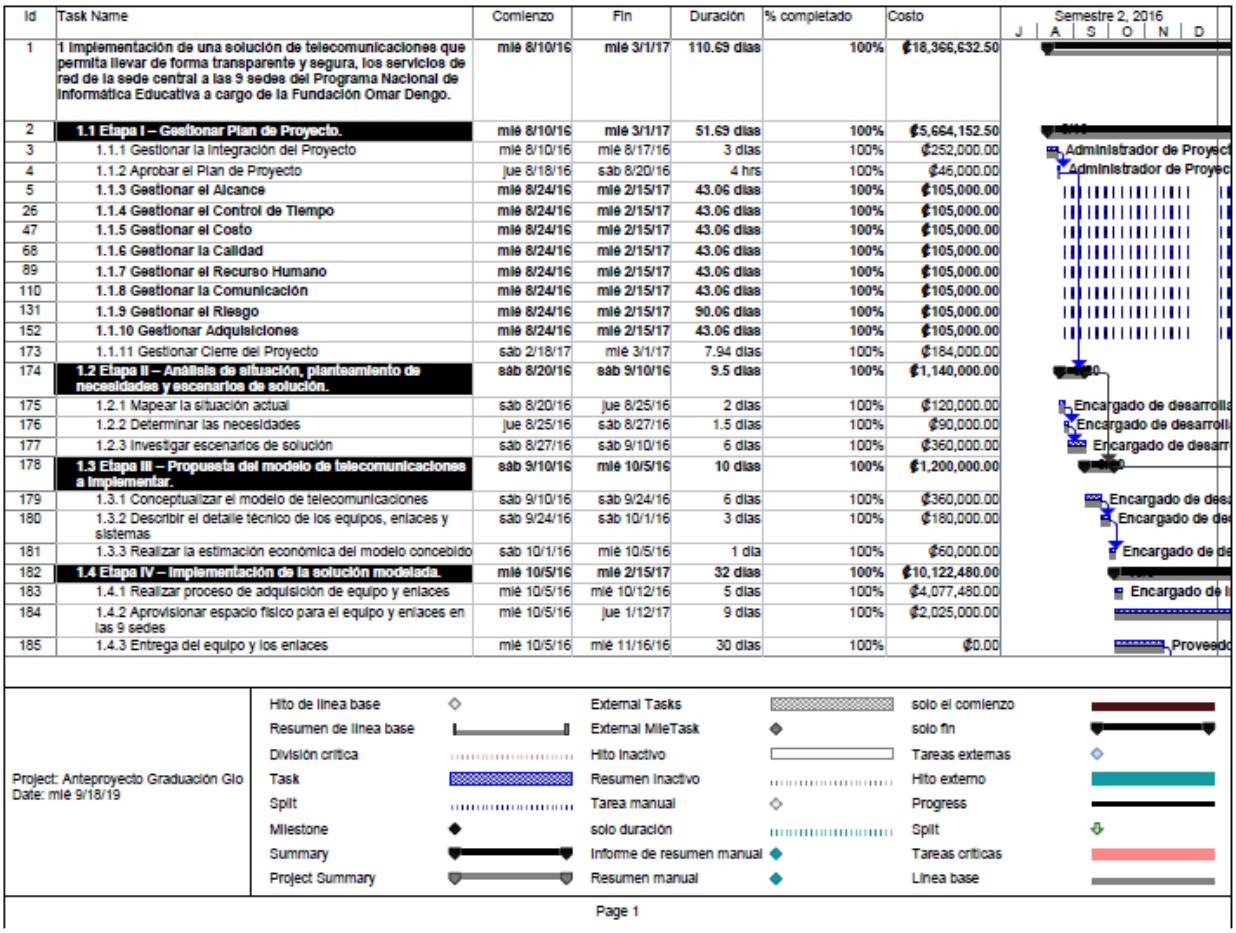


Ilustración 17. Diagrama de Gantt parte 1. Elaboración propia.

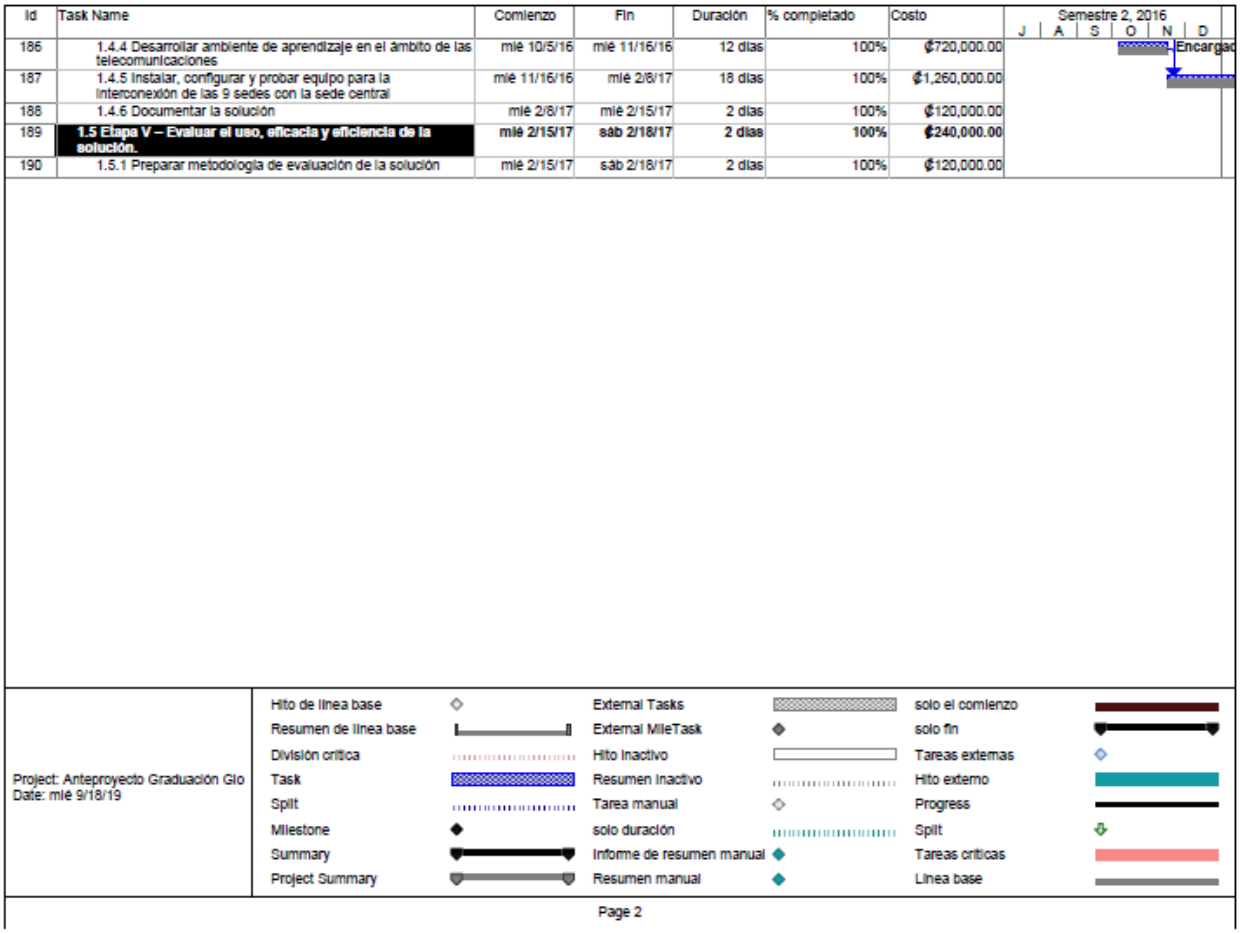


Ilustración 18. Diagrama de Gantt parte 2. Elaboración propia.

3.1.5 Implementación y pruebas.

Esta fase propone ejecutar el cronograma de implementación, implementar el diseño de red y validarlo. Las tareas por realizar son:

3.1.5.1 Ejecución del cronograma de implementación:

Se ejecutan las tareas de la etapa IV del cronograma Implementación de la solución modelada.

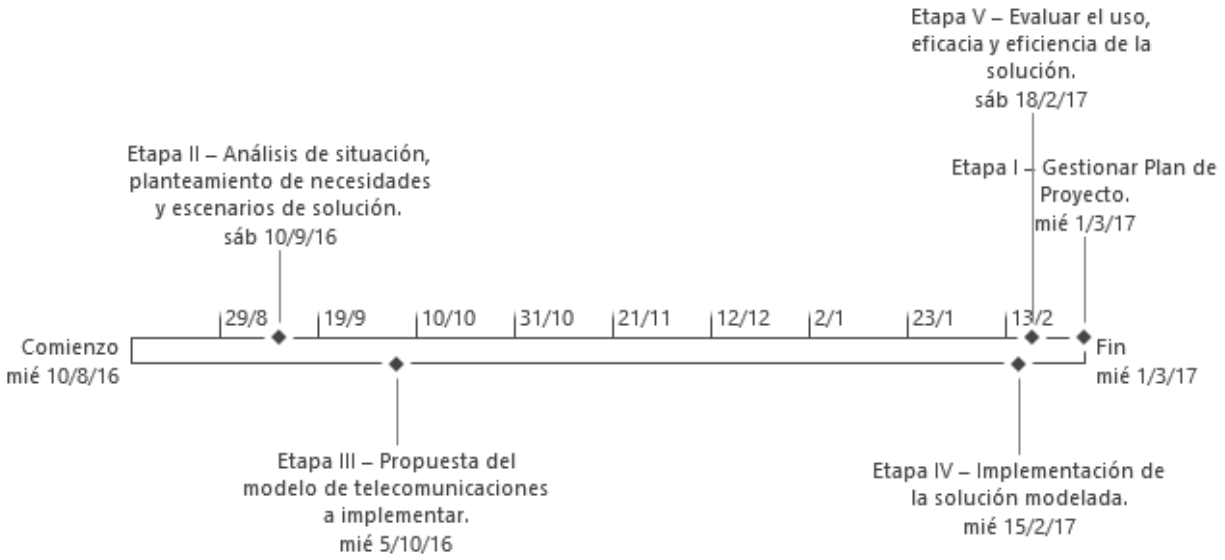


Ilustración 19. Calendario de hitos en el tiempo. Elaboración propia.

3.1.5.2 Implementación del diseño de red propuesto en la fase anterior:

Se inicia con la adquisición de equipos y enlaces de internet corporativos. Para ello se realizan las gestiones internas de solicitud de bienes y servicios, búsqueda de cotizaciones de materiales y propuestas de servicios de proveedores de servicios de internet. Dichos documentos se pueden ver con mayor detalle en la sección de anexos.

Se identifican y preparan los espacios físicos de las 9 sedes regionales para la instalación de las bandejas en donde se sujetarán los equipos de telecomunicaciones. Una vez que se reciben los materiales, equipos y enlaces, se realiza una segunda visita para su aprovisionamiento.

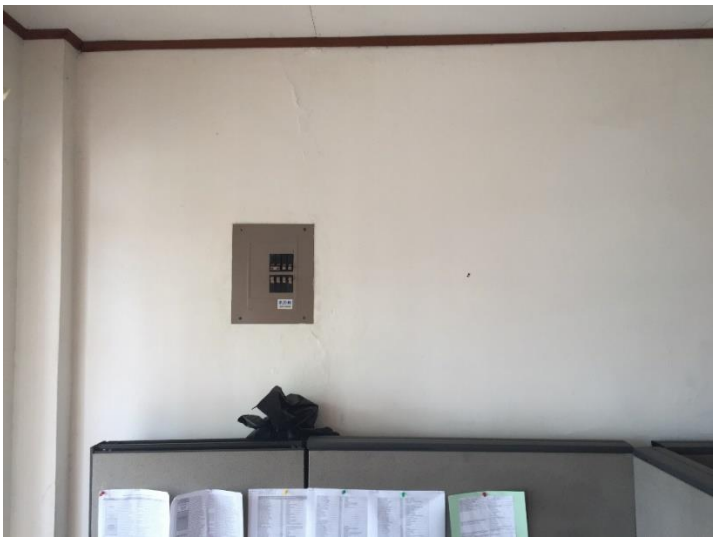


Ilustración 20. Foto 1 aprovisionamiento físico en la sede de Limón. Elaboración propia.

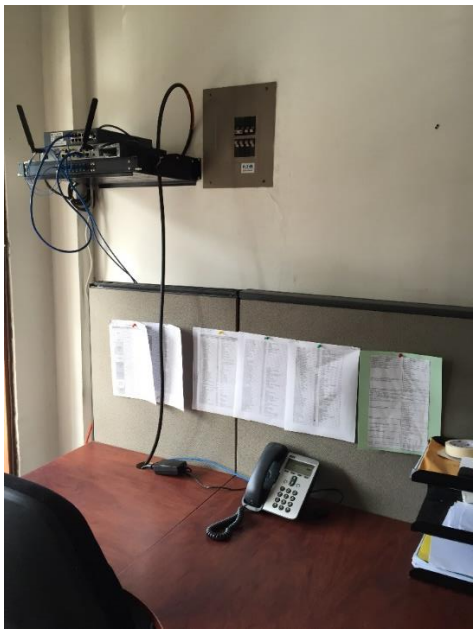


Ilustración 21. Foto 2 aprovisionamiento físico de la sede de Limón. Elaboración propia.

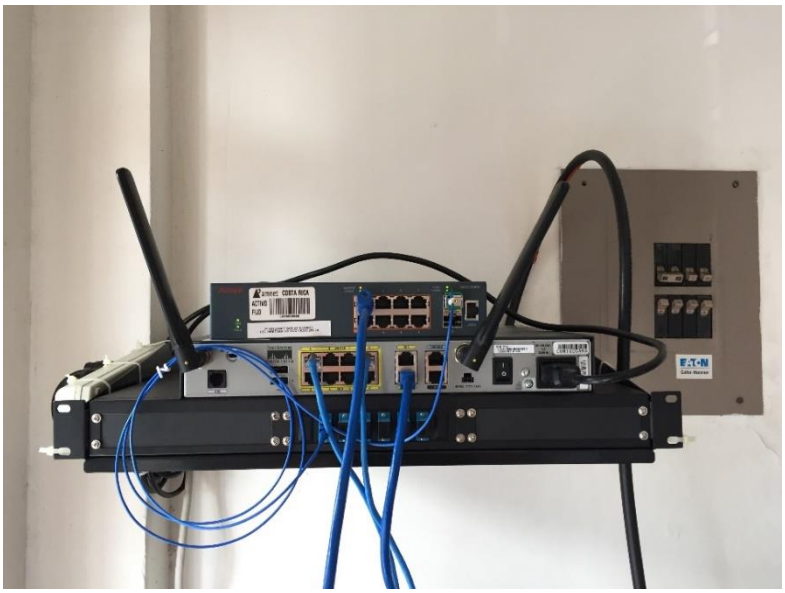


Ilustración 22. Foto 3 aprovisionamiento físico de la sede. Elaboración propia.

Ilustración 23. Foto 4 aprovisionamiento físico de la sede. Elaboración propia.

Una vez aprovisionados los equipos y enlaces, se realizan los ajustes técnicos en los equipos de la sede central y la sede regional.

En los Cisco ASA 5516:

1. Definir las listas de acceso:

   Supuestos: Segmento de red privado del equipo en la Sede 192.168.105.0 255.255.255.0

   access-list <SEDE_XXXX> extended permit ip any 192.168.105.0 255.255.255.0

   access-list <SEDE_XXXX> extended permit ip <IP_VLAN1> 255.255.255.0 192.168.105.0 255.255.255.0

   access-list <SEDE_XXXX> extended permit ip <IP_VLAN2> 255.255.255.0 192.168.105.0 255.255.255.0

   access-list <SEDE_XXXX> extended permit ip <IP_VLAN3> 255.255.255.0 192.168.105.0 255.255.255.0

2. Crear Crypto Map:

   Supuestos: IP Pública del equipo en la Sede

   crypto map outside_map <TAG_Ejemplo_140> match address <SEDE_XXXX>

   crypto map outside_map <TAG_Ejemplo_140>set pfs

   crypto map outside_map <TAG_Ejemplo_140>set peer <IP_PÚBLICA_SEDE>

   crypto map outside_map <TAG_Ejemplo_140>set ikev1 transform-set AES128_SHA1

   crypto map outside_map <TAG_Ejemplo_140>set ikev2 ipsec-proposal DES 3DES AES AES192 AES256

   crypto map outside_map <TAG_Ejemplo_140>set security-association lifetime seconds 7200

3. Configurar Contraseña:

   tunnel-group 186.176.205.6 type ipsec-l2l

   tunnel-group 186.176.205.6 ipsec-attributes

   ikev1 pre-shared-key <CONTRASEÑA>

En los Cisco 1811:

1. Definir IPs públicas para la interfaz:

   interface FastEthernet0

ip address <IP_PÚBLICA_SEDE> 255.255.255.252

ip default-gateway <IP_PÚBLICA_GATEWAY_SEDE>

ip route 0.0.0.0 0.0.0.0 <IP_PÚBLICA_GATEWAY_SEDE>

ip access-list extended WAN_IN

permit icmp <IP_PÚBLICA_WAN_SEDE> 0.0.0.3 <IP_PÚBLICA_WAN_SEDE> 0.0.0.3

permit esp host <IP1_X.X.X.X> host <IP_PÚBLICA_SEDE>

permit udp host <IP1_X.X.X.X> host <IP_PÚBLICA_SEDE> eq isakmp

permit udp host <IP1_X.X.X.X> host <IP_PÚBLICA_SEDE> eq non500-isakmp

permit esp host <IP2_X.X.X.X> host <IP_PÚBLICA_SEDE>

permit udp host <IP2_X.X.X.X> host <IP_PÚBLICA_SEDE> eq isakmp

permit udp host <IP2_X.X.X.X> host <IP_PÚBLICA_SEDE> eq non500-isakmp

deny ip any any

crypto isakmp policy 140

encr aes

authentication pre-share

group 2

lifetime 43200

crypto isakmp key < CONTRASEÑA> address <IP_PÚBLICA_SEDE> no-xauth

crypto isakmp key < CONTRASEÑA> address <IP_PÚBLICA_SEDE> no-xauth

crypto isakmp fragmentation

crypto ipsec transform-set AES128_SHA1 esp-aes esp-sha-hmac

crypto map VPN 140 ipsec-isakmp

set peer <IP1_X.X.X.X>

set peer <IP2_X.X.X.X>

set security-association lifetime seconds 7200

set transform-set AES128_SHA1

set pfs group2

match address VPN_HQ

En los enrutadores perimetrales Cisco 3945:

GW01:

ip route 192.168.105.0 255.255.255.0 <IP3_X.X.X.X> name <SEDE_XXXX>

ip access-list extended NAT

permit ip 192.168.105.0 0.0.0.255 any

ip access-list extended TIGO-55-1-10667913

GW02:

ip route 192.168.105.0 255.255.255.0 <IP3_X.X.X.X> name <SEDE_XXXX>

ip access-list extended NAT

permit ip 192.168.105.0 0.0.0.255 any

ip access-list extended TIGO-1

permit ip 192.168.105.0 0.0.0.255 any

3.1.5.3 Realización de la pila de pruebas

De manera conjunta con el proveedor, se documentan las características de cada uno de los enlaces aprovisionados en las sedes regionales y se realizan las siguientes pruebas:

- Prueba de ping y tracert.
- Prueba de velocidad.
- Prueba de registro de IPs públicas.
- Prueba de carga y descarga.
- Prueba de estrés.

Para profundizar más en lo anterior, se puede consultar el anexo 2.

A partir de los ajustes técnicos en los equipos de la sede central y la sede regional se procede a validar la correcta comunicación entre ambos sitios para asegurar que la red implementada, esté funcionando de acuerdo con lo diseñado.

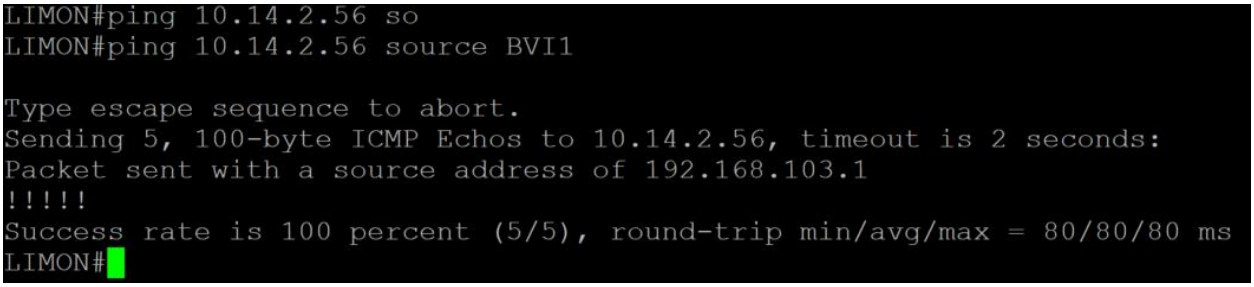


Ilustración 24. Prueba comunicación entre la sede regional y la sede central. Elaboración propia.

Finalmente se valida la conexión de los usuarios a la red inalámbrica, el acceso a los servicios de la red de la sede central, el funcionamiento de las llamadas de voz, la ejecución de tareas de impresión y el correcto funcionamiento del lector biométrico.

3.1.6 Monitoreo y optimización.

Para esta fase, se monitorea la operación de la red en producción para detectar problemas de rendimiento y cualquier falla y dar pie a su optimización.

3.1.6.1 Monitoreo de la operación de la red en producción:

Se debe monitorear y verificar constantemente el funcionamiento de la red para detectar y documentar cualquier situación que se deba subsanar. Para ello, se define una guía que permita a los encargados de la infraestructura de la red telemática, construir una bitácora de evaluación continua a través del tiempo, en donde se puedan visualizar las estadísticas de uso, eficacia y eficiencia de los equipos de telecomunicaciones y servicios de infraestructura tecnológica. Dicha guía se detalla en el anexo 5.

3.1.6.2 Optimización de la red:

Si las situaciones que inciden en el funcionamiento esperado de la red son frecuentes o incluso imposibles de gestionar, se debe rediseñar la red, sin embargo, al finalizar la implementación de la solución de interconexión de las sedes, no se presentaron dichas situaciones y será a partir del monitoreo que realice el personal a cargo de la red telemática, que se determine si se debe optimizar la red implementada.

CAPÍTULO IV
ANÁLISIS DE RESULTADOS

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

4.1 Medición de resultados

A partir de la metodología planteada en el marco metodológico, se desarrollaron las fases correspondientes según lo establecido en el cronograma y, en consecuencia, se logra implementar una solución telemática sostenible en el tiempo y acorde a los requerimientos establecidos para facilitar la ejecución de un proceso clave para la institución y de interés e impacto nacional como lo es el Programa Nacional de Informática Educativa MEP-FOD. La interconexión entre la sede central y las sedes regionales está permitiendo que los colaboradores a lo largo y ancho del país cuenten con las fuentes de información y herramientas de productividad, colaboración y comunicación para ejecutar sus labores de manera segura, con un mejor desempeño y bajo una continuidad razonable de los servicios de TI.

Desde la perspectiva de gestión de las tecnologías de información y comunicación, no solamente se logra potenciar el uso de los recursos tecnológicos y cumplir con las necesidades de crecimiento del plan estratégico institucional, sino que también se logra establecer el control y estandarización sobre los recursos tecnológicos, cumpliendo con la normativa vinculante. El contar con una guía para para la construcción de una bitácora que permita la verificación del funcionamiento correcto de la red, sirve como insumo para la gobernanza de las tecnologías de información y comunicación, elementos con lo que no se contaba anteriormente y que eran necesarios para respaldar la toma de decisiones o para identificar algún mal uso de los recursos de conectividad. Por otro lado, el hecho de que se pudiera contratar la totalidad de los enlaces a un mismo proveedor de servicios de internet, permitió establecer un vínculo comercial importante que le permite a la institución optimizar el uso de los recursos financieros y mejorar las condiciones de soporte y prestación del servicio. Dicha relación comercial también permite a la institución

aumentar o disminuir los anchos de banda según se requiera de manera ágil y flexible, algo que anteriormente era lento, caro y engorroso de tramitar.

El proyecto trajo consigo un ambiente de aprendizaje en el ámbito de las telecomunicaciones para poder contar con las competencias y conocimientos a lo interno de la institución que permitieran llevar a cabo los ajustes técnicos que se requería aplicar a las configuraciones de los equipos de comunicaciones tanto de la sede central como de las sedes del Programa, algo que sin duda fomentó el desarrollo profesional e impulsa el mejoramiento continuo de la plataforma tecnológica.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La implementación de una solución de telemática para llevar los servicios que provee la infraestructura tecnológica de la sede central de la Fundación Omar Dengo a las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD de forma transparente y segura, satisface las necesidades institucionales de crecimiento y desarrollo de las tecnologías de información y comunicación de forma controlada y estandarizada, dando lugar a la mejora continua de la infraestructura tecnológica, las comunicaciones, la seguridad y los sistemas para llevar a la institución a una escalabilidad y ruta de servicios tecnológicos acorde a su labor y bajo un enfoque en concordancia con el plan estratégico institucional y los marcos de referencia y buenas prácticas que le atañan.

Se logra contar en las sedes con enlaces corporativos de alta disponibilidad y un nivel de sobresuscripción adecuado, que, además, permitirán una relación de negocio en donde se facilita la gestión y negociación.

Con el nuevo modelo de interconexión, se garantiza la confidencialidad, integridad y disponibilidad de la información, contando con medidas de seguridad para el control de acceso a los recursos de TI y a la información, protegiendo la integridad de esta y asegurando una continuidad razonable de los servicios de TI.

En relación con el uso de los recursos financieros invertidos en la gestión de TI, se potencia el uso de estos mediante la extensión de los servicios de la sede central de la Fundación Omar Dengo a las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD, facilitando el acceso,

adopción y apropiación de los mismos a todos los colaboradores del Programa Nacional de Informática Educativa MEP-FOD ubicados a lo largo y ancho del país.

Con la ejecución de este proyecto, se asume a través de las tecnologías de información y comunicación, el rol estratégico para apoyar la consecución de un proceso clave para la institución y de interés e impacto nacional como lo es el Programa Nacional de Informática Educativa MEP-FOD.

5.2 Recomendaciones

El nuevo modelo de red telemática implementado requiere de una apropiación por parte del personal que administra la infraestructura en telecomunicaciones, siendo relevante que el mismo cuente con el conocimiento y la experticia para realizar cambios a las configuraciones existentes o bien a nuevas configuraciones para nuevas sedes.

Monitorear de manera constante la disponibilidad de la solución y comprender adecuadamente los protocolos para reportar averías al proveedor de servicios de internet.

Velar por el buen estado de los equipos, sus actualizaciones y las condiciones de éstos principalmente en las sedes y contar con equipos de respaldo que permitan remplazar algún equipo dañado.

Aplicar la guía para la construcción de la bitácora que permita la verificación del correcto funcionamiento de la solución, de manera que, se generen los insumos que permitan retroalimentar la gobernanza de las tecnologías de información y comunicación.

Planificar la sostenibilidad de la solución en términos financieros para garantizar su operatividad a través del tiempo.

Valorar con cierta periodicidad, principalmente cuando se renuevan equipos o se actualizan los sistemas operativos de los mismos, si el modelo de red telemática implementado puede ser mejorado.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Cisco. (29 de Febrero de 2016). *Cisco IOS VPN Configuration Guide*. Obtenido de http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg.html

Cisco. (2016). *Cisco 1811 Integrated Services Router*. Obtenido de https://www.cisco.com/c/en/us/products/routers/1811-integrated-services-router-isr/index.html

Cisco. (2016). *Cisco 3900 Series Integrated Services Routers Data Sheet*. Obtenido de https://www.cisco.com/c/en/us/products/collateral/routers/3900-series-integrated-services-routers-isr/data_sheet_c78_553924.html

Cisco. (2016). *Cisco ASA with FirePOWER Services Data Sheet*. Obtenido de Cisco 3900 Series Integrated Services Routers Data Sheet

Cisco. (29 de Febrero de 2016). *Cisco Branch Routers*. Obtenido de http://www.cisco.com/c/en/us/products/routers/branch-routers/index.html#~products

Cisco. (25 de Abril de 2016). *Cisco Network Academy, CCNA Routing and Switching*. Obtenido de https://www.netacad.com/es/courses/ccna/

Cisco. (25 de Abril de 2016). *Cisco Network Academy, CCNA Security*. Obtenido de https://www.netacad.com/es/courses/ccna-security/

Contraloría General de la República. (2007). *Normas técnicas para la gestión y control de las Tecnologías de Información (N-2-2007-CO-DFOE).* San José: La Gaceta Nro.119 del 21 de Junio de 2007.

Duoc UC. (01 de Septiembre de 2019). *Sitio web Investigación Aplicada | Biblioteca DUOC UC*. Obtenido de http://www.duoc.cl/biblioteca/crai/investigacion-aplicada

Fundación Omar Dengo. (2011). Plan estratégico 2011-2016. San José, Costa Rica.

Fundación Omar Dengo. (01 de Septiembre de 2019). *Sitio web Fundación Omar Dengo*. Obtenido de http://www.fod.ac.cr/

Fundación Wikimedia, Inc. (29 de Febrero de 2016). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/Wikipedia:Portada

Gutiérrez, M., & Torres Berríos, C. (25 de Abril de 2016). *Guía a la quinta edición del Publication Manual of the American Psychological Association 2001*. Obtenido de http://www.uazuay.edu.ec/bibliotecas/Manual_de_estilo_APA_para_Trabajos_Academicos.pdf

IT Governance Institute. (2007). Cobit 4.1. Rolling Meadows, IL 60008, EE.UU.

Normas APA. (29 de Febrero de 2016). *Normas APA Actualizadas 2016*. Obtenido de http://normasapa.com/

Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. (2013). Normas de buenas prácticas para los controles de seguridad de la información (ISO/IEC 27002:2013). Vernier, Ginebra, Suiza.

Project Management Institute, Inc. (2008). Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®) - Cuarta edición . Newtown Square, Pennsylvania, EE.UU.

Reid, A. (2006). *WAN Technologies CCNA 4 Companion Guide (Cisco Networking Academy).* Cisco Press.

Sampieri, R. H. (2014). *Metodología de la Investigación Sexta Edición.* México D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

A

AntiSpyware

Programa espía que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. 18, 29

Antivirus

Son programas que buscan prevenir, detectar y eliminar virus informáticos. 18, 29

C

Cisco

Empresa dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones. 19

Cobit

Guía de mejores prácticas dirigida al control y supervisión de tecnología de la información. 22

Controlador de dominio

Es el medio definido por Microsoft por el cual se garantiza o deniega a un usuario el acceso a recursos compartidos o a otra máquina de la red. 18, 28

Cortafuegos

Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. 18, 29

E

Enlaces de Internet Asimétricos

Son aquellos que no tienen la misma velocidad de subida como de bajada de datos. Estos se caracterizan por tener diferentes anchos de banda para cada dirección de la comunicación. 20

Enlaces de Internet Simétricos

Son aquellos que tienen la misma velocidad de subida como de bajada de datos. Estos se caracterizan por tener el mismo ancho de banda para cada dirección de la comunicación. 20

J

Jabber de Cisco

Es una aplicación de comunicaciones unificadas que combina capacidades de voz y vídeo, mensajería instantánea, presencia, mensajería de voz, conferencia y compartición de archivos de escritorio sobre plataformas PC, Mac, tablets y smartphones. 18, 29

N

Nivel de sobresuscripción

Se refiere a la cantidad de clientes que comparten un enlace de Internet 21

S

Skype Empresarial

Es un servicio de mensajería instantánea, lanzado por Microsoft Office Communications Server. 18, 29

T

Telefonía IP

Conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo de Internet. 18, 28

ANEXOS

8.1 Anexo 1. Solicitud de compra de bienes y servicios institucionales, cotización de materiales y solicitud de servicios corporativos a Tigo Business.

FUNDACION OMAR DENGO
DIRECCION DE OPERACIONES
UNIDAD DE COMPRAS Y CONTRATACIONES
SOLITIDUD DE COMPRA DE BIENES O SERVICIOS INSTITUCIONALES

FECHA DE SOLICITUD: 6/9/2016

DIRECCION O UNIDAD SOLICITANTE: Unidad de Infraestructura Tecnológica

#	ARTICULOS O SERVICIOS SOLICITADOS Detalle o Caracteristicas	CANTIDAD	CENTRO DE COSTO	PRESUPUESTO PREVISTO	FECHA DE ENTREGA REQUERIDA
1	Caja de Cable UTP Cat 5e calibre 24AWG de unos 300 metros	1	2A-01-01-03	90,000.00	Junio 16
2	Bandeja para rack ventilada de 2 Unidades de Rack x 19" x 14" de profundidad que soporte al menos 50 libras.	9	2A-01-01-03	140,000.00	Junio 16
3	ultima linea				
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
				230,000.00	

JUSTIFICACION DE LA SOLICITUD:
Materiales para tareas de mantenimiento sobre el cableado de la red y para el aprovisionamiento de los espacios para los equipos de telecomunicaciones de las sedes del PRONIE MEP-FOD

Para uso exclusivo de la Dirección Financiera

Monto Presupuestario autorizado: ₡

Efectivo disponible: SI NO

5-1-01-08-08-001

V°B° Dirección Financiera: Gustavo Arce Gómez

Para uso exclusivo de la Unidad de Compras y Contrataciones

Fecha y hora de recibo:

Persona que recibe:

Tipo de contratación:
Licitación Privada
Licitación Abreviada
Contratación Directa
Caja Chica

Tiempo promedio en trámite:

Ilustración 25. Solicitud de Bienes y Servicios. Recuperado de: Solicitud de Compra de Bienes y Servicios Institucionales.

UMC

UMC DE COSTA RICA S.A. **VIERNES 10 DE JUNIO DEL 2016**

Céd. Jur..: 3-101-153345

Teléfono..: (506)-228-30-817 (506)-283-08-18 Servicio Cliente: (506)-228-3081

Fax.....: (506)-228-38-010 (506)-283-80- 20

Factura Proforma No. 131558

CLIENTE: FUNDACION OMAR DENGO 000970 FECHA: 10/06/2016

ATENCION: TELEFONO: 5062-5762

AGENTE VENTAS: MORA CHAVERRI MAUREEN FAX: 5062-2216

COTIZADOR: MORA CHAVERRI MAUREEN

VIGENCIA OFERTA : 8 DIAS.

ENTREGA: 22 DIAS MONEDA: DOLARES

CONDICION PAGO: 30 DIAS. TIPO PAGO CREDITO

NOS COMPLACE PRESENTAR A SU CONSIDERACION LA SIGUIENTE OFERTA:

LIN.	CANT.	CODIGO	DESCRIPCION	% DESC.	PRECIO-U.	TOTAL
1	9,00	000283	Bandeja para Rack Newlink Ventilada 19"x14" 50lbs (	0,00	25,00	225,00
2	1,00	000265	Carrucha de cable Newlink Azul Cat 5 9805842	0,00	85,00	85,00

Monto en Letras

Trescientos cincuenta dolares con 30/100

SUBTOTAL	$	310,00
DESCUENTO	$	0,00
IMPUESTO	$	40,30
TOTAL	$	350,30

Estimado Cliente:

Favor revisar la oferta y verificar que cumple con lo que requiere.

PRECIOS SUJETOS A CAMBIO SIN PREVIO AVISO

FIRMA AUTORIZADA:_____

Pag. 1 de 1

Ilustración 26. Cotización de materiales. Recuperado de: Solicitud de Factura proforma de UMC #131558.

SOLICITUD DE SERVICIOS CORPORATIVOS
NUEVOS SERVICIOS N-1

tigo business

Ced. Jurídica: 3-006-0847
Cliente: **FUNDACIÓN OMAR DENGO**
Dirección: SAN JOSE, DE LA ANTIGUA CASA MATUTE GOMEZ 300 M ESTE Y 50 M SUR
Contacto: RICARDO SAMPER
Teléfono: 2527-6230
Célular: 0
E-mail: ricardo.samper@fod.ac.cr
Fecha: 13/1/2017

Millicom Cable Costa Rica, S. A.
Ced. Jur. 3-101-577518
JESSICA ROMERO CASTRO
PBX: 4031 3200 Ext. 3276
Movil: (506) 6195-4508
Santa Ana, Forum 2, Edificio D, 3° Piso

SERVICIOS DE FACTURACIÓN MENSUAL:

SERVICIO	CATEGORÍA	ANCHO BANDA	DESCRIPCIÓN	PRECIO UNIT	IMP. UNIT	CANT	TOTAL
Internet	Nuevo	4 Mbps	HEREDIA	$130,00	$0,00	1	$130,00
					$0,00	1	$0,00
					$0,00	1	$0,00

*CLIENTE EXCENTO DE IMPUESTOS

Subtotal $130,00
Imp Ventas $0,00
Total Pago Mensual $130,00

SERVICIOS Y PRODUCTOS DE FACTURACIÓN DE PAGO ÚNICO:

ITEM	MODELO	DESCRIPCIÓN	PLAZO	PRECIO UNIT	IMP. UNIT	CANT	TOTAL
Instalación	-	AMPLIACION DE LA RED	1 Mes	$200,00	$0,00	1	$200,00
		- UL -		$0,00	$0,00		$0,00

Subtotal $200,00
Imp Ventas $0,00**
Total Pago Contado $200,00

Gran Total $330,00

Importante:
(**) Impuesto de Venta Aplica sobre Conectividad, Telefonía y Hardware

Nota: Los detalles de cada producto o servicio se encuentran en la Propuesta Técnica

El CLIENTE entiende y acepta:

1 - Los servicios de TIGO se cobrarán inmediatamente después de recibido conforme (Firma en Boleta de Trabajo) y certificado la entrega del servicio (s); excepto los casos especiales que se hayan acordado previamente con otra fecha de inicio y especificado en este contrato.

2 - Cualquier ductería, canaleta, orificio, acometida, pintura u otra modificación necesaria para la instalación del servicio de TIGO en su infraestructura, serán de su responsabilidad y por lo tanto correrá por su cuenta.

3 - El suscrito firmante en su condición de representante legal acepta que la persona que se establece como contacto entre EL CLIENTE y TIGO en el presente documento será el encargado de dirigir, solicitar y firmar futuras órdenes de nuevos trabajos así como aquellos relacionados al presente servicio que se brinda.

4 - Cliente acepta que la terminación anticipada del presente por su parte le obliga a la cancelación total del monto correspondiente a la instalación sea lo suma de $976

Sello

Firma y Aprobación del Representante Legal

19-01-2017
Fecha

Tigo Business, San José, Costa Rica. Tel: (506) 4031-3200. www.tigo.cr Versión 1.2

Hoja 1 de 1

Ilustración 27. Solicitud de servicios corporativos a Tigo Business. Recuperado de: Solicitud de Servicios Corporativos Tigo Business.

8.2 Anexo 2. Propuesta de servicios corporativos de Tigo Business

Propuesta del modelo de telecomunicaciones a implementar.

Anexo 1

Propuesta de servicios corporativos Tigo Business

PROPUESTA DE SERVICIOS CORPORATIVOS

INTERNET CORPORATIVO

tigo business
Una solución para cada negocio

tigo business

1. Enlace de Internet por Fibra Óptica

Para presentar esta oferta se ha desarrollado una solución específica para supir las necesidades de conexión de su empresa.

Esta conexión se hará por medio de nuestra MAN (Red de Área Metropolitana), la cual permite brindar conectividad en los anchos de banda solicitados por su empresa.

Para este enlace se utilizará fibra óptica, el cual es conocido como un medio inmune a la interferencia y brinda capacidades altas de transporte.

1.1. Descripción técnica

Es un servicio más robusto que el Internet común, el cual es instalado por medio de Fibra Óptica y con esto se tiene una mayor flexibilidad de regular el Ancho de Banda de manera sencilla, permitiendo dar una mejor y más eficiente conectividad a los servicios de Internet como son:

- Web.
- Correo electrónico (SMTP).
- Transmisión de archivos (FTP y P2P).
- La mensajería instantánea y presencia.
- La transmisión de contenido y comunicación multimedia.
- (Telefonía (VoIP), Televisión (IPTV), los boletines electrónicos (NNTP), el acceso remoto a otras máquinas (SSH y Telnet) o los juegos en línea.

Al tener la posibilidad de un mayor Ancho de Banda tiene la ventaja de brindar un mejor servicio a las empresas que hoy en día requieren de mejores medios de comunicación con sus sucursales, clientes y con el resto del mundo.

Contamos con un variado portafolio de servicio de Internet en modalidades *Platino*, *Oro*, *Plata* y *Bronce* dependiendo de la necesidad de conectividad que tenga el cliente.

tigo business

1.2. Ventajas de la conexión con Fibra Óptica:

- Diámetro y peso reducido lo que facilita su instalación.
- Excelente flexibilidad
- Inmunidad a los ruidos eléctricos
- No existe diafonía (no hay inducción entre una fibra y otra)
- Bajas pérdidas, lo cual permite reducir la cantidad de estaciones repetidoras
- Gran Ancho de Banda que implica una elevada capacidad de transmisión.
- Estabilidad frente a variaciones de temperatura.
- Al no conducir electricidad no existe riesgo de incendios.
- No puede captarse información desde el exterior de la fibra.
- Servicio de Internet más robustos, control absoluto de utilización de abonados.
- No hay limitaciones para Upgrades.

tigo business

2. Nuestros Planes Corporativos

Actualmente la velocidad de los negocios hace indispensable contar con un servicio de Internet estable, de alta calidad y de excelente desempeño. Por ello, Tigo está revolucionando el mercado, con servicios que garantizan el Ancho de Banda Internacional, de tal manera que su compañía podrá obtener un mejor retorno de su inversión y la confianza que sus servicios de videoconferencia, voz o VPN podrán operar sin contratiempos y de manera continua.

Todos los servicios de Internet están respaldados por un **SLA (Service Level Agreement)** de un 99,9% del tiempo online, lo cual establece una garantía de estabilidad única.

Los diferentes niveles de Internet Corporativo ofrecido son los siguientes:

2.1. Internet Platino (1:1)
Garantía del 100% del Ancho de Banda Internacional, con canal privado hacia el NAP de las Americas. Ideal para servicios de videoconferencia, streaming y servicios de datacenter.

2.2. Internet Oro (1:3)
Especial para aplicaciones críticas de carácter regional. Diseñado para operar con aplicaciones como SAP, Oracle, Microsoft Dynamics, entre otras, y la generación de VPN's de alta seguridad o encriptación.

2.3. Internet Plata (1:5)
Internet de alta velocidad diseñado para compañías con requerimientos típicos como voz sobre IP, VPN, navegación constante y correo electrónico. Con gran flexibilidad referente al direccionamiento IP.

2.4. Internet Bronce (1:10)
Internet diseñado para la pequeña y mediana empresa. Ideal para la navegación y aplicaciones tradicionales no demandantes.

tigo business

3. Nuestra Propuesta de Enlace de Internet en Fibra:

3.1. Oferta exclusiva para Fundación Omar Dengo:

Nombre de la Sede	Ancho de banda requerido	Tiempo Instalación	Mensualidad
Alajuela	4 Mbps	18 días	$130
Naranjo	2 Mbps	18 días	$105
Cartago	4 Mbps	48 días	$130
Santa Cruz, Guanacaste	6 Mbps	18 días	$210
Limón	2 Mbps	48 días	$105
El Roble, Puntarenas	2 Mbps	18 días	$105
Guápiles, Limón	2 Mbps	18 días	$105
Pérez Zeledón, San José	4 Mbps	30 días	$234

En caso de necesitar ductería interna esta será responsabilidad del cliente.

Nota: Los precios indicados en el cuadro corresponden a una mensualidad y a un punto.

Precios no incluye impuestos.

****La sobresuscripción local es de 1:1**

tigo business

4. Nuestra RED

***Sobresuscripción internacional directa al NAP de las Américas es de 1:10.**

5. Servicio Soporte Técnico

5.1. Sistema de supervisión y ayuda remota en línea

- Control de sus enlaces mediante un sistema de gestión y monitoreo 24x7x365
- Equipo altamente calificado y recursos logísticos para el mantenimiento de los enlaces de su entidad
- El soporte técnico de **TIGO** se encuentra disponible las 24 horas del día, con servicio personalizado, a través del **1767** y soporte en línea soporiecr@tigo.co.cr *Este soporte no tiene ningún costo adicional.*
- Monitoreo activo para detectar pérdida de paquetes en los circuitos y caídas totales de los mismos.
- Disponibilidad de técnicos para solventar fallas aun en horas no hábiles.
- Acceso a soporte Técnico vía Web.

Llámenos al 4031-3253 o 4031-3215
www.tigo.cr

5.2. Servicio de Monitoreo

- TIGO proveerá una herramienta MRTG (Multi Router Traffic Grapher), la cual permitirá tener acceso seguro a cada uno de sus enlaces, mediante un usuario y un password asignado vía Web.
- Podrá ver en cualquier momento, el estado de cada uno de sus enlaces así como el tráfico que cada uno de ellos este llevando.
- El Ancho de Banda ofertado por TIGO en la presente propuesta es un Ancho de Banda garantizado "Guaranteed Throughput"

6. Instalación del Servicio

6.1. Plazos

El tiempo de instalación será el indicado en el cuadro de arriba, contados a partir de la firma del contrato y los formularios correspondientes para la formalización de la prestación de los servicios.

6.2. Proceso Interno de Instalación

- El cliente debe habilitar un ducto de 2" de diámetro con curvas abiertas dentro del cuarto de telecomunicaciones del punto a realizar la conexión.
- Habilitar un espacio en el bastidor o rack para instalación de un ODF, (distribuidor de fibra óptica), el cual es aportado por TIGO.
- Habilitar una bandeja para colocar un convertidor de medios en el rack.
- Se conecta un cable tipo UTP con terminales RJ45, (Ethernet).

tigo business

7. Equipos de enlaces

- Los equipos que serán instalados en la oficina del Cliente son propiedad de TIGO.
- El Cliente deberá asignar un espacio físico adecuado para la instalación de los equipos y garantizar las condiciones ambientales y de energía eléctrica recomendadas en el manual del fabricante para su óptimo funcionamiento como UPS y acometida eléctrica polarizada.

8. Vigencia del contrato

La vigencia del contrato será de **36 meses** y cuenta a partir de la fecha de firma del contrato, excepto cuando el cliente indique otro lapso, mayor o menor.

Durante la vigencia del contrato, el Cliente siempre tiene la opción de modificar los anchos de banda o incrementar la cantidad de enlaces con previo aviso.

8.3 Anexo 3. Documentación del enlace y pruebas ejecutadas

tigo business

Información de Nuevo Servicio | 2016

Atención
Ricardo Samper
Fundación Omar Dengo

Estimado señor,

Por medio del presente nos permitimos saludarle de la manera más atenta y a la vez hacer entrega formal del perfil de configuración para el servicio de Internet Corporativo.

Agradecemos de antemano la confianza depositada como su proveedor de servicios de telecomunicaciones.

El enlace identificado a continuación, ha sido implementado y se encuentra totalmente liberado para su utilización.

Socio	Fundación Omar Dengo - El Roble
ID Servicio	10669651 / Navega+ N/A
Tipo de Servicio	Internet
Tecnología	MPLS
Medio físico	Fibra Óptica
Ancho de Banda	2Mbps
Vlan de Servicio TIGO	778
Equipo Instalado	Avaya 3510GT -PWR+
IP de Gestión red TIGO	10.213.143.3
Fecha liberación del servicio	22 de Junio del 2016
Nodo TIGO	Roble
Activo / # Serie	C09B020979 / 00R06T
Interface HUB Tigo	Sas 2 / Puerto 1/2
Otras Interfaces	N/A
Equipo entregado al Cliente	N/A
Serie	N/A
IP de Gestión	N/A
Usuario	N/A

Llámenos al 4031-3253 o 4031-3215
www.tigo.cr

tigo business

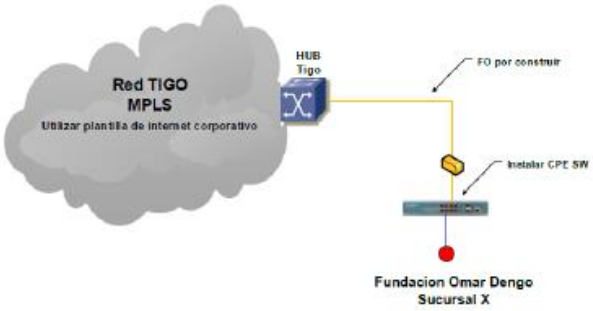
Información de Nuevo Servicio | 2016

Nombre de Red	186.177. . / 30
Gateway	186.177. . / 30
Cantidad IP's	3
IP's Utilizables	186.177. . / 30
Máscara	255.255.255.252
Dominio DNS Primario	dns5.amnet.co.cr
Dominio DNS Secundario	dns7.amnet.co.cr
DNS Primario	186.177.16.218
DNS Secundario	186.177.16.219

HLD (High Level Design)

HLD Enlace de Internet para Fundación Omar Dengo

tigo business



Sucursal	ID	Servicio	Capacidad	HUB
Alajuela	10669647	Internet	4 Mbps Bronce, 1 IP	MPLS Alajuela Corp
Naranjo	10669648	Internet	2 Mbps Bronce, 1 IP	MPLS Naranjo SAS
Cartago	10669649	Internet	4 Mbps Bronce, 1 IP	MPLS Cartago SAS
Limon	10669650	Internet	2 Mbps Bronce, 1 IP	MPLS Limon SAS
Roble	10669651	Internet	2 Mbps Bronce, 1 IP	MPLS Roble SAS
Guapiles	10669652	Internet	2 Mbps Bronce, 1 IP	MPLS Guapiles SAS
Perez Zeledon	10669653	Internet	4 Mbps Bronce, 1 IP	MPLS Sabana SAS 1 p1/1/3
Santa Cruz	10669654	Internet	6 Mbps Bronce, 1 IP	MPLS Santa Cruz

tigo	HLD: Fundación Omar Dengo	Jose Pablo Zuñiga Monge	
	TIGO Business, Technical Partner	Fecha Revisión : junio 1, 2016	Revision 1.0

Pruebas de Ping y Tracert

Se conecta el computador directamente al equipo de demarcación:

1. Se realizaron pruebas de ping hacia las siguientes direcciones IP's: 8.8.8.8 / 4.2.2.2:

2. Se realizaron pruebas de tracert hacia las siguientes direcciones IP's: 8.8.8.8 / 4.2.2.2:

Pruebas de Aplicación Speedtest

Se conecta el computador directamente al equipo de demarcación:

1. Se realizaron pruebas de Speedtest Externo 1: TIGO: http://tigo-si.speedtest.net

2. Se realizaron pruebas de Speedtest Externo 2: http://speedtest.comcast.net/

3. Se realizaron pruebas de Speedtest Externo 3: ICE: http://medidor.kolbi.cr

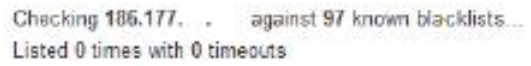
Su IP: 186.177.64.174 - Amnet Cable Costa Rica

Pruebas de Registro de IPs Públicas.

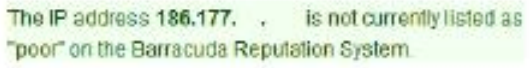
Se conecta el computador directamente al equipo de demarcación con la IP de Internet correspondiente:

1. http://www.spamhaus.org/lookup/

2. http://mxtoolbox.com/NetworkTools.aspx



3. http://www.barracudacentral.org/lookups

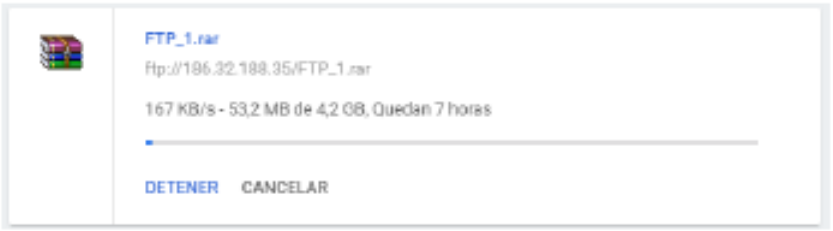


Pruebas Específicas

Pruebas de Descarga (Download)

Se conecta el computador directamente al equipo de demarcación:

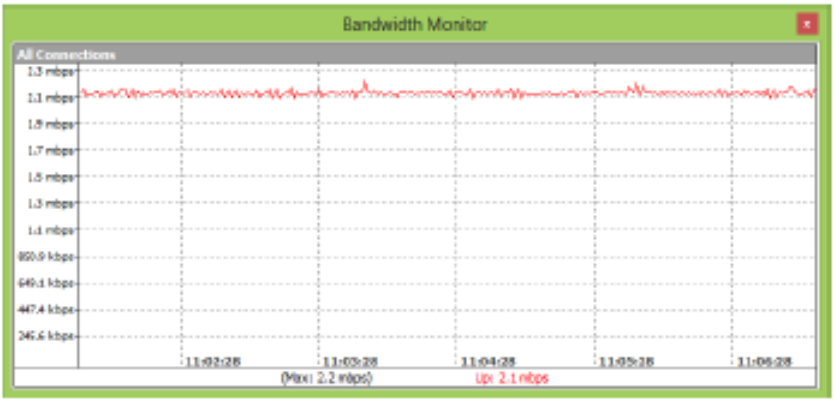
1. Se realizaron pruebas de medición de tiempo de descarga y tasa de transferencia:



Pruebas de Carga (Upload)

Se conecta el computador directamente al equipo de demarcación:

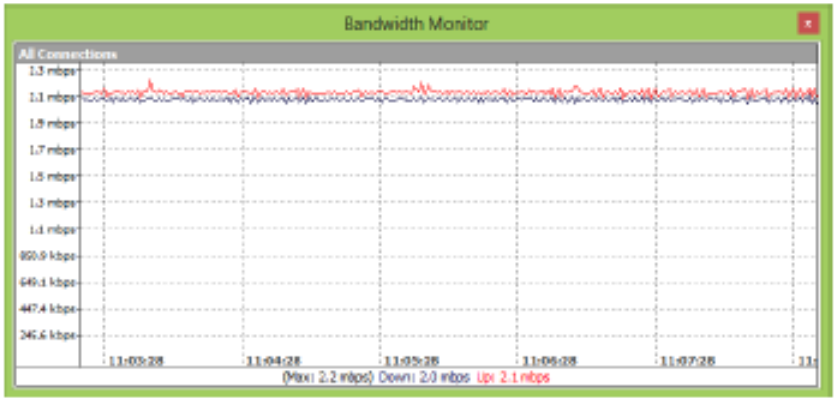
1. Se realizaron pruebas de medición de tiempo de subida y tasa de transferencia:



Pruebas Estrés Simétrico de Canal

Se conecta el computador directamente al equipo de demarcación:

1. Se realizaron pruebas de medición de tiempo de carga y descarga simultáneas:



Medición de Potencia

Fotografías (Ingreso de F.O.)

Fotografías (Instalación de equipos)

Boleta de Entrega

MILLICOM CABLE COSTA RICA, S.A.

ORDEN DE TRABAJO No. 10017178

Nombre del cliente
ID Servicio
Contacto
Trouble Ticket
Dirección
Teléfono
Fecha

Tipo de Atención		Información del Servicio y Equipo				Datos de Red Internet	
Instalación	☑	Ancho de Banda		Equipo		IP	
Avería	☐	Internet	☑	GPON	☐	Gateway	
Pruebas	☐	Datos	☐	Media C	☑	Mask	
Mantenimiento	☐	Local	☐	Otro	☐	Rango	desde
Otro	☐	Regional	☐		☐		hasta

Información del Equipo

Equipo	Modelo	Serie / Activo	Instalado/Retirado
			Instalado

Condiciones y ubicación en el sitio

Voltaje		Neutro y Tierra			Polaridad	SI / NO
Temperatura		Potencia	TX			☐ ☐
Humedad			RX			

Soporte Técnico

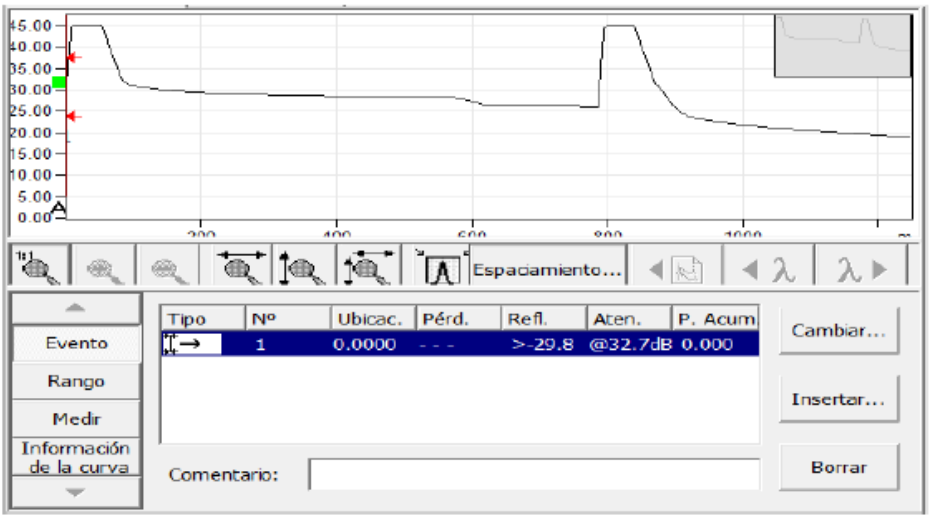
Pruebas Realizadas:

Observaciones:

Hora Inicio	10:00	Estado de la ODT	☑ Concluida	☐ Anulada
Hora Fin	11:10		☐ Alertada	☐ Pruebas
Tiempo de Viaje				

Cliente — Nombre y Firma | Técnico

OTDR (Optical Time-Domain Reflectometer)



tigo business

Información de Nuevo Servicio | 2016

A partir de la fecha de liberación y por un plazo de 3 días el equipo de instalación queda a su entera disposición para cualquier consulta y apoyo técnico en referencia a la activación de este servicio a través del email instalaciones@tigo.co.cr o tel: 4031 3200.

Posterior al plazo anteriormente indicado, recibiremos sus consultas a través del Soporte Corporativo TIGO para lo cual adjuntamos a continuación los datos de nuestros contactos así como el proceso de escalamiento a seguir para la apertura tiquetes de servicio; a través de helpdeskcorp@tigo.co.cr o tel: 4031 3233. (Se adjunta archivo: *Tabla Escalamiento Tigo Business Corporate CR-Oct-2014.pdf*).

Saludos cordiales.

Hellen Valverde Loría
Back Office Technical Partner
Office direct: +506 4031 3290
PBX: +506 4031 3200
e-mail: hellen.valverde@tigo.co.cr

Ricardo A. Ramírez Jaramillo
Deployment Services Corporate Chief
Office direct: +506 4031 3257
Mobile: +506 6066 9446
e-mail: ricardo.ramirez@tigo.co.cr

Instalaciones TIGO Business, Costa Rica
e-mail: instalaciones@tigo.co.cr
Forum 2 Office Park, Building D
San José, Costa Rica

8.4 Anexo 4. Guía "Configurar IPSec sitio a sitio entre un ASA y un enrutador del Cisco IOS"

Configure IPSec sitio a sitio un túnel IKEv1 entre un ASA y un router del Cisco IOS

Contenido

Introducción

Este documento describe cómo configurar un túnel de la versión 1 del intercambio de claves de Internet del IPSec del sitio a localizar (LAN a LAN) (IKEv1) vía el CLI entre un dispositivo de seguridad adaptante de Cisco (ASA) y un router que funcione con el software del ® del Cisco IOS.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- IOS de Cisco
- Cisco ASA
- Conceptos generales del IPSec

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5512-X Series ASA que funcionan con la versión de software 9.4(1)
- Router de los Servicios integrados de las Cisco 1941 Series (ISR) esa versión del Cisco IOS Software 15.4(3)M2 de los funcionamientos

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Esta sección describe cómo completar las configuraciones CLI ASA y del router IOS.

Diagrama de la red

La información en este documento utiliza esta configuración de la red:

Configuración ASA

Configure las interfaces ASA

Si las interfaces ASA no se configuran, asegúrese de que usted configure por lo menos los IP Addresses, interconecte los nombres, y los niveles de seguridad:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

> **Note**: Asegúrese de que haya Conectividad al interno y a las redes externas, y especialmente al peer remoto que será utilizado para establecer un túnel del VPN de sitio a sitio. Usted puede utilizar un ping para verificar la conectividad básica.

Configure la directiva IKEv1 y habilite IKEv1 en la interfaz exterior

Para configurar las directivas del Internet Security Association and Key Management Protocol (ISAKMP) para las conexiones IKEv1, ingrese el comando **crypto del <priority> de la directiva ikev1**:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

> **Note**: Una coincidencia de la directiva IKEv1 existe cuando ambas directivas de los dos pares contienen la misma autenticación, cifrado, hash, y Valores de parámetro de Diffie Hellman. Para IKEv1, la directiva del peer remoto debe también especificar un curso de la vida inferior o igual el curso de la vida en la directiva que el iniciador envía. Si los cursos de la vida no son idénticos, después el ASA utiliza el curso de la vida más corto.

> **Note**: Si usted no especifica un valor para un parámetro dado de la directiva, el valor predeterminado es aplicado.

Usted debe habilitar IKEv1 en la interfaz que termina el túnel VPN. Típicamente, ésta es la interfaz del exterior (o *público*). Para habilitar IKEv1, ingrese el **ikev1 crypto habilitan <interface name>** el comando en el modo de configuración global:

```
crypto ikev1 enable outside
```

Configure el grupo de túnel (el perfil de la conexión de LAN a LAN)

Para un túnel de LAN a LAN, el tipo del perfil de la conexión es ipsec-l2l. Para configurar la clave del preshared IKEv1, ingrese al modo de configuración de los IPSec-*atributos del grupo de túnel:*

```
crypto ikev1 enable outside
```

Configure el ACL para el tráfico VPN del interés

El ASA utiliza el Listas de control de acceso (ACL) para distinguir el tráfico que se debe proteger con la encripción de IPSec contra el tráfico que no requiere la protección. Protege los paquetes salientes que hacen juego un motor del control de la aplicación del permiso (ACE) y se asegura de que los paquetes de entrada que hacen juego un permiso ACE tenga protección.

```
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
```

> **Note**: Un ACL para el tráfico VPN utiliza los IP Address de origen y de destino después del Network Address Translation (NAT).

> **Note**: Un ACL para el tráfico VPN se debe duplicar en ambos pares VPN.

> **Note**: Si hay una necesidad de agregar una nueva subred al tráfico protegido, de agregar simplemente una subred/un host al objeto-grupo respectivo y de completar un cambio del espejo en el par del telecontrol VPN.

Configure una exención de NAT

> **Note**: La configuración que se describe en esta sección es opcional.

Típicamente, no debe haber NAT realizado en el tráfico VPN. Para eximir ese tráfico, usted debe crear una regla de la identidad NAT. La regla de la identidad NAT traduce simplemente un direccionamiento al mismo direccionamiento.

```
nat (inside,outside) source static local-network local-network destination static
remote-network remote-network no-proxy-arp route-lookup
```

Configure el IKEv1 transforman el conjunto

Un IKEv1 transforma el conjunto es una combinación de protocolos de Seguridad y los algoritmos que define la manera que el ASA protege los datos. Durante las negociaciones de la asociación de seguridad IPSec (SA), los pares deben identificar una transformación fijada o la oferta que sean lo mismo para ambos pares. El ASA entonces aplica correspondido con transforma el conjunto o la oferta para crear un SA que proteja los flujos de datos en la lista de acceso para esa

correspondencia de criptografía.

Para configurar el IKEv1 transforme el conjunto, ingresan el comando crypto del transforme el conjunto del IPSec ikev1:

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

Configure una correspondencia de criptografía y apliqúela a una interfaz

Una correspondencia de criptografía define una política IPSec que se negociará en IPSec SA y la incluye:

- Una lista de acceso para identificar los paquetes que conexión IPSec los permisos y protege
- Identificación del par
- Una dirección local para el tráfico IPSec
- Los IKEv1 transforman los conjuntos

Aquí tiene un ejemplo:

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

Usted puede entonces aplicar la correspondencia de criptografía a la interfaz:

```
crypto map outside_map interface outside
```

Configuración final ASA

Aquí está la configuración final en el ASA:

```
crypto map outside_map interface outside
```

Configuración CLI del router IOS

Configure las interfaces

Si las interfaces del router IOS todavía no se configuran, después por lo menos el LAN y las interfaces de WAN deben ser configurados. Aquí tiene un ejemplo:

```
crypto map outside_map interface outside
```

Asegúrese de que haya Conectividad al interno y a las redes externas, y especialmente al peer remoto que será utilizado para establecer un túnel del VPN de sitio a sitio. Usted puede utilizar un ping para verificar la conectividad básica.

Configure la directiva ISAKMP (IKEv1)

Para configurar las políticas isakmp para las conexiones IKEv1, ingrese el comando **crypto del <priority> de la política isakmp** en el modo de configuración global. Aquí tiene un ejemplo:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

> **Note**: Usted puede configurar las políticas IKE múltiples en cada par que participe en el IPSec. Cuando la negociación IKE comienza, intenta encontrar una directiva común que se configure en ambos pares, y comienza con las directivas más prioritarias que se especifican en el peer remoto.

Configure una clave Crypto ISAKMP

Para configurar una clave de autenticación del *preshared,* ingrese el **comando crypto isakmp key** en el modo de configuración global:

```
crypto isakmp key cisco123 address 172.16.1.1
```

Configure un ACL para el tráfico VPN del interés

Utilice el extendido o la lista de acceso denominada para especificar el tráfico que se debe proteger por el cifrado. Aquí tiene un ejemplo:

```
crypto isakmp key cisco123 address 172.16.1.1
```

> **Note**: Un ACL para el tráfico VPN utiliza los IP Address de origen y de destino después del NAT.

> **Note**: Un ACL para el tráfico VPN se debe duplicar en ambos pares VPN.

Configure una exención de NAT

> **Note**: La configuración que se describe en esta sección es opcional.

Típicamente, no debe haber NAT realizado en el tráfico VPN. Si se utiliza la sobrecarga NAT, después un route-map se debe utilizar para eximir el tráfico VPN del interés de la traducción. Note que en la lista de acceso que se utiliza en el route-map, el tráfico VPN del interés debe ser negado.

```
crypto isakmp key cisco123 address 172.16.1.1
```

Configure un conjunto de la transformación

Para definir un IPSec transforme el conjunto (una combinación aceptable de protocolos y de algoritmos de Seguridad), ingresan el **comando crypto ipsec transform-set** en el modo de configuración global. Aquí tiene un ejemplo:

```
crypto ipsec transform-set RSP-ARS-SHA esp-aes esp-sha-hmac
 mode tunnel
```

Configure una correspondencia de criptografía y aplíquela a una interfaz

Para crear o modificar una entrada de correspondencia de criptografía y ingresar al modo de configuración de la correspondencia de criptografía, ingrese el comando global configuration de la **correspondencia de criptografía**. Para que la entrada de correspondencia de criptografía sea completa, allí son algunos aspectos que se deben definir en un mínimo:

- Los peeres IPSec a quienes el tráfico protegido puede ser remitido deben ser definidos. Éstos son los pares con quienes un SA puede ser establecido. Para especificar a un peer IPSec en una entrada de correspondencia de criptografía, ingrese el **comando set peer**.
- Los conjuntos de la transformación que son aceptables para el uso con el tráfico protegido deben ser definidos. Para especificar los conjuntos de la transformación que se pueden utilizar con la entrada de correspondencia de criptografía, ingrese el **comando set transform-set**.
- El tráfico que debe ser protegido debe ser definido. Para especificar una lista de acceso ampliada para una entrada de correspondencia de criptografía, ingrese el **comando address del emparejamiento**.

Aquí tiene un ejemplo:

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set RSP-ARS-SHA
 match address 110
```

El último paso es aplicar el conjunto previamente definido de la correspondencia de criptografía a una interfaz. Para aplicar esto, ingrese el comando interface configuration de la **correspondencia de criptografía**:

```
interface GigabitEthernet0/0
crypto map outside_map
```

Configuración final IOS

Aquí está la configuración CLI final del router IOS:

```
interface GigabitEthernet0/0
crypto map outside_map
```

Verificación

Antes de que usted lo verifique si el túnel sea ascendente y ése pase el tráfico, usted debe asegurarse de que el tráfico del interés esté enviado hacia el ASA o el router IOS.

> **Note**: En el ASA, la herramienta del paquete-trazalíneas que hace juego el tráfico del interés se puede utilizar para iniciar el túnel IPsec (tal como paquete-trazalíneas entrado dentro de tcp 10.10.10.10 12345 10.20.10.10 80 detallado por ejemplo).

Verificación de la fase 1

Para verificar si IKEv1 la fase 1 esté para arriba en el ASA, ingrese el **comando show crypto isakmp sa**. El resultado esperado es considerar MM_ACTIVE el estado:

```
ciscoasa# show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.17.1.1
   Type    : L2L             Role    : responder
   Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

Para verificar si IKEv1 la fase 1 esté para arriba en el IOS, ingrese el **comando show crypto isakmp sa**. El resultado esperado es considerar el estado ACTIVO:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Verificación de la fase 2

Para verificar si IKEv1 la fase 2 esté para arriba en el ASA, ingrese el **comando show crypto ipsec sa**. El resultado esperado es considerar el Security Parameter Index entrante y saliente (SPI). Si el tráfico pasa a través del túnel, usted debe ver el encaps/los contadores de los decaps incrementar.

> **Note**: Para cada entrada ACL hay un SA entrante/saliente separado creado, que pudo dar lugar a una salida larga del **comando show crypto ipsec sa** (dependiente sobre el número de entradas de ACE en el ACL crypto).

Aquí tiene un ejemplo:

```
ciscoasa# show crypto ipsec sa peer 172.17.1.1
peer address: 172.17.1.1
    Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

      access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
     current_peer: 172.17.1.1


      #pkts encaps: 1005, #pkts encrypt: 1005, #pkts digest: 1005
      #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 8A9FBE19
     current inbound spi : D8639ED0

    inbound esp sas:
      spi: 0xD8639ED0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x8A9FBE19 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

Para verificar si IKEv1 la fase 2 esté para arriba en el IOS, ingrese el comando show crypto ipsec sa. El resultado esperado es considerar SPI entrante y saliente. Si el tráfico pasa a través del túnel, usted debe ver el encaps/los contadores de los decaps incrementar.

Aquí tiene un ejemplo:

```
Router#show crypto ipsec sa peer 172.16.1.1
```

```
interface: GigabitEthernet0/0
   Crypto map tag: outside_map, local addr 172.17.1.1

  protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2024, #pkts encrypt: 2024, #pkts digest: 2024
    #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639ED0(3630406608)
    PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8A9FB619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

     outbound esp sas:
      spi: 0xD8639ED0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

Fase 1 y verificación 2

Esta sección describe los comandos que usted puede utilizar en el ASA o el IOS para verificar los detalles por ambas fases 1 y 2.

Ingrese el comando de VPN-sessiondb de la demostración en el ASA para la verificación:

```
ciscoasa# show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1
```

```
Session Type: LAN-to-LAN Detailed

Connection    : 172.17.1.1
Index         : 2                     IP Addr       : 172.17.1.1
Protocol      : IKEv1 IPsec
Encryption    : IKEv1: (1)AES128  IPsec: (1)AES128
Hashing       : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx      : 100500                Bytes Rx      : 101400
Login Time    : 18:06:02 UTC Wed Jul 22 2015
Duration      : 0h:05m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
 Tunnel ID     : 2.1
 UDP Src Port : 500                   UDP Dst Port : 500
 IKE Neg Mode : Main                  Auth Mode     : preSharedKeys
 Encryption    : AES128               Hashing       : SHA1
 Rekey Int (T): 86400 Seconds         Rekey Left(T): 86093 Seconds
 D/H Group     : 2
 Filter Name   :

IPsec:
 Tunnel ID     : 2.2
 Local Addr    : 10.10.10.0/255.255.255.0/0/0
 Remote Addr   : 10.20.10.0/255.255.255.0/0/0
 Encryption    : AES128               Hashing       : SHA1
 Encapsulation: Tunnel
 Rekey Int (T): 3600 Seconds          Rekey Left(T): 3293 Seconds
 Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607901 K-Bytes
 Idle Time Out: 30 Minutes            Idle TO Left : 24 Minutes
 Bytes Tx      : 100500               Bytes Rx      : 101400
 Pkts Tx       : 1005                 Pkts Rx       : 1014

NAC:
 Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
 SQ Int (T)    : 0 Seconds            EoU Age(T)    : 309 Seconds
 Hold Left (T): 0 Seconds             Posture Token:
 Redirect URL :

ciscoasa#
```

Ingrese el comando de sesión de criptografía de la demostración en el IOS para la verificación:

```
Router#show crypto session remote 172.16.1.1 detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalive, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 172.16.1.1
      Desc: (none)
 IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
 IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383
```

```
Router#
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

> **Note**: Refiera a la información importante en los comandos Debug y el Troubleshooting de IP Security - entendiendo y con los documentos de Cisco de los comandos debug antes de que usted utilice los comandos debug.

Herramienta del inspector del LAN a LAN del IPSec

Para verificar automáticamente si la configuración de LAN a LAN del IPSec entre el ASA y el IOS sea válida, usted puede utilizar la herramienta del inspector del LAN a LAN del IPSec. Se diseña la herramienta de modo que valide una tecnología o un comando show running-config de la demostración de un ASA o del router IOS. Examina la configuración e intenta detectar si una correspondencia de criptografía basada túnel ipsec de LAN a LAN está configurada. Si está configurado, realiza un control de múltiples puntos de la configuración y resalta cualesquiera Errores de configuración y configuraciones para el túnel que sería negociado.

Debugs ASA

Para resolver problemas la negociación de túnel del IPSec IKEv1 en un Firewall ASA, usted puede utilizar estos comandos debug:

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

> **Note**: Si el número de VPN hace un túnel en el ASA es significativo, el par de la condición del debug crypto que utilizan al comando a.b.c.d debe antes de que usted permita a los debugs para limitar las salidas de los debugs para incluir solamente al par especificado.

Debugs del router IOS

Para resolver problemas la negociación de túnel del IPSec IKEv1 en un router IOS, usted puede utilizar estos comandos debug:

```
debug crypto ipsec
debug crypto isakmp
```

> **Note**: Si el número de VPN hace un túnel en el IOS es significativo, el par de la condición del debug crypto que A.B.C.D se utiliza ipv4 debe antes de que usted permita a los debugs para limitar las salidas de los debugs para incluir solamente al par especificado.

Tip: Refiera al L2L más común y al IPSec VPN del Acceso Remoto que resuelve problemas el documento de Cisco de las soluciones para más información sobre cómo resolver problemas un VPN de sitio a sitio.

Referencias

- Información importante sobre los Comandos de depuración
- Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración
- Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto
- Inspector del LAN a LAN del IPSec
- Soporte Técnico y Documentación - Cisco Systems

8.5 Anexo 5. Guía para construir una bitácora de evaluación continua a través del tiempo de la solución, en donde se puedan visualizar las estadísticas de uso, eficacia y eficiencia de los equipos de telecomunicaciones y servicios de infraestructura tecnológica.

Metodología de evaluación de la solución

Febrero de 2017

Objetivo.

El propósito de este documento es describir los pasos a seguir para construir una bitácora de evaluación continua a través del tiempo de la solución de interconexión de la sede central de la FOD y las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD, mediante la generación periódica de informes que muestren las estadísticas de uso, eficacia y eficiencia de la solución basado en los registros de los equipos de comunicaciones y de los servicios de la infraestructura tecnológica, de manera que los resultados de dicha bitácora permitan retroalimentar la gobernanza de las TI.

Marco conceptual.

Bitácora de evaluación: En una herramienta en donde se reportan los avances o resultados de un determinado proceso de evaluación. La misma se encuentra organizada de forma cronológica, registrando dichos avances o resultados según se van generando, de manera que se pueda establecer la trazabilidad de toda la labor realizada.

Informe técnico: Documento que describe el progreso o los resultados de una investigación técnica, o el estado de un problema técnico. Un informe de este tipo debe presentar, sistemática o cronológicamente, información suficiente para que un lector cualificado pueda juzgar, evaluar o proponer modificaciones a sus conclusiones o recomendaciones.

Errata: Equivocación material cometida en lo impreso o manuscrito.

Metodología.

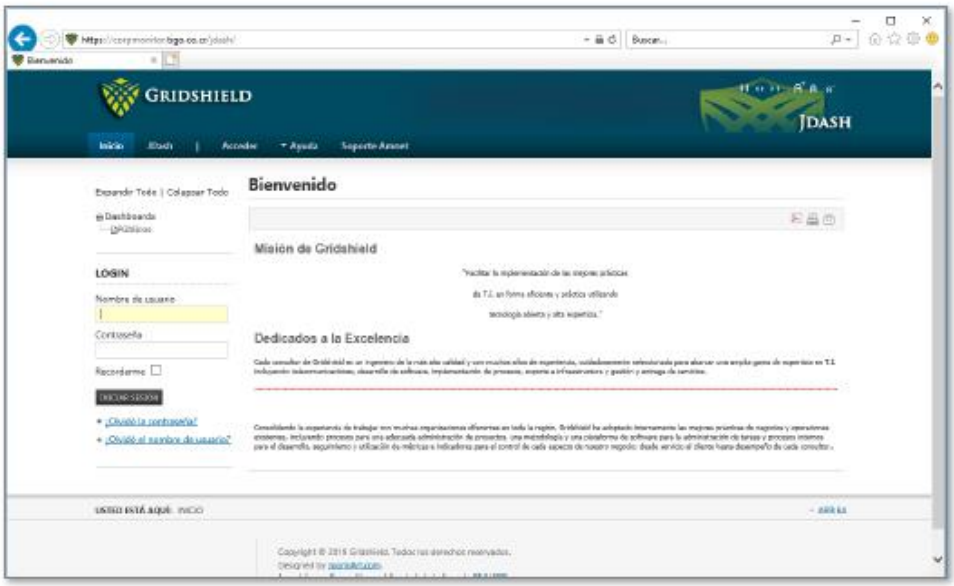
1. **Creación de la bitácora de evaluación:** Se creará una bitácora que resguarde la evaluación continua a través del tiempo de la solución mediante la generación periódica de informes que muestren las estadísticas de uso, eficacia y eficiencia de la solución basado en los registros de los equipos de comunicaciones y de los servicios de la infraestructura tecnológica, compuesta por las siguientes secciones:
    - **Portada:** En donde se indica el nombre de la institución, el departamento o unidad de trabajo encargada de mantener actualizada la bitácora y finalmente una descripción general que haga referencia a la solución de interconexión de la sede central de la FOD y las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD.
    - **Procedimientos:** Sección dedicada a escribir las actividades que se van desarrollar, su periodicidad y los responsables de llevarlas a cabo.

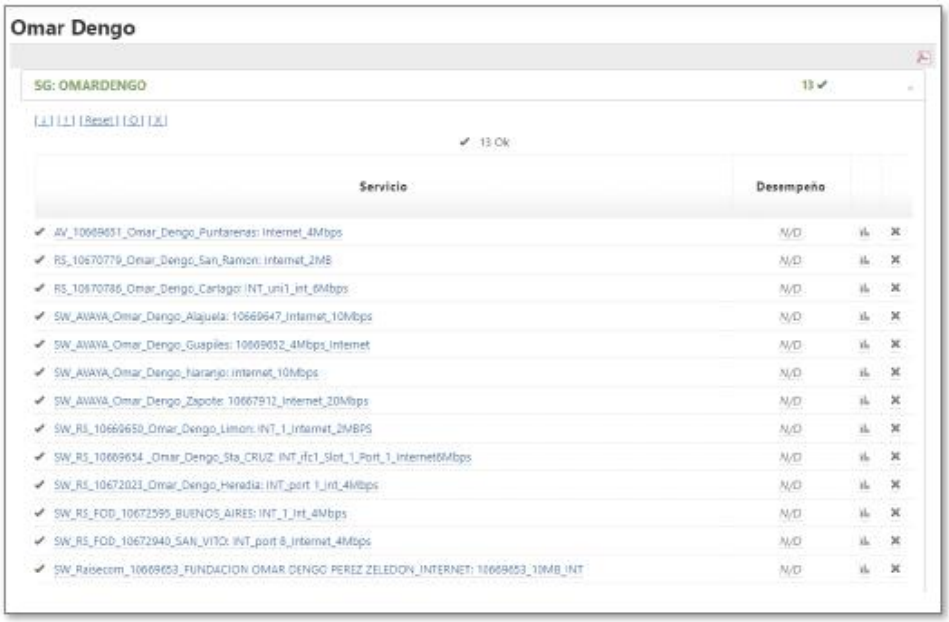
- **Detalle:** Espacio en donde se van agregando los informes técnicos en orden cronológico. Si se llega a cometer una equivocación material en alguno de los informes técnicos, deberá subsanarse mediante un segundo documento explicando la errata.

2. **Creación del informe técnico:** Se creará un informe que muestre las estadísticas de uso, eficacia y eficiencia de la solución de interconexión de la sede central de la FOD y las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD. basado en los registros de los equipos de comunicaciones y de los servicios de la infraestructura tecnológica, en donde el cuerpo del mismo esté compuesto por las siguientes secciones:
   - **Encabezado:** Indicar el número de informe técnico y el tema haciendo uso del siguiente formato: Informe técnico # [AñoMesDia] - [Tema]
   - **Información del Informe:** Registrar el propósito general del informe, la fecha, información del autor y de los participantes.
   - **Glosario:** Cuando el informe incluya términos técnicos, abreviaturas, signos o símbolos, registrar y hacer una breve definición de los mismos, de manera que puedan ser comprendidos por lectores no especializados en la materia.
   - **Tareas ejecutadas:** Anotar las actividades desarrolladas.
   - **Observaciones:** Plasmar las ideas y comentarios de los participantes de forma libre acerca de los resultados.
   - **Anexos:** Incorporar cualquier referencia de conformidad a las tareas ejecutadas.
   - **Aprobaciones:** Espacio para que los participantes validen y aprueben las tareas ejecutadas y observaciones del informe técnico.

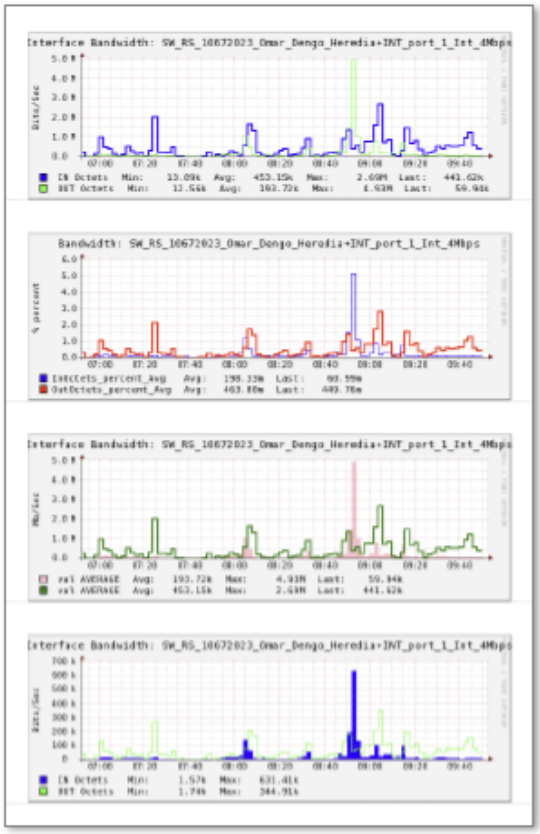
3. **Herramientas de evaluación:** Para poder evaluar la solución de interconexión de la sede central de la FOD y las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD, se dispone de 2 herramientas:
   - **La interfaz de monitoreo web de los enlaces de internet contratados:** Instrumento que permite validar en tiempo real, el estado de los enlaces de internet, continuidad y algunas estadísticas de uso.

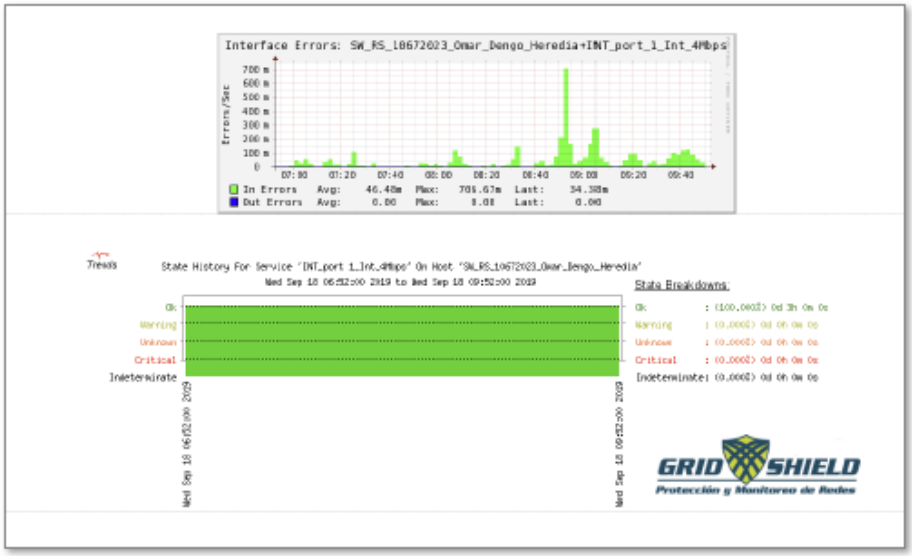
Metodología de evaluación de la solución





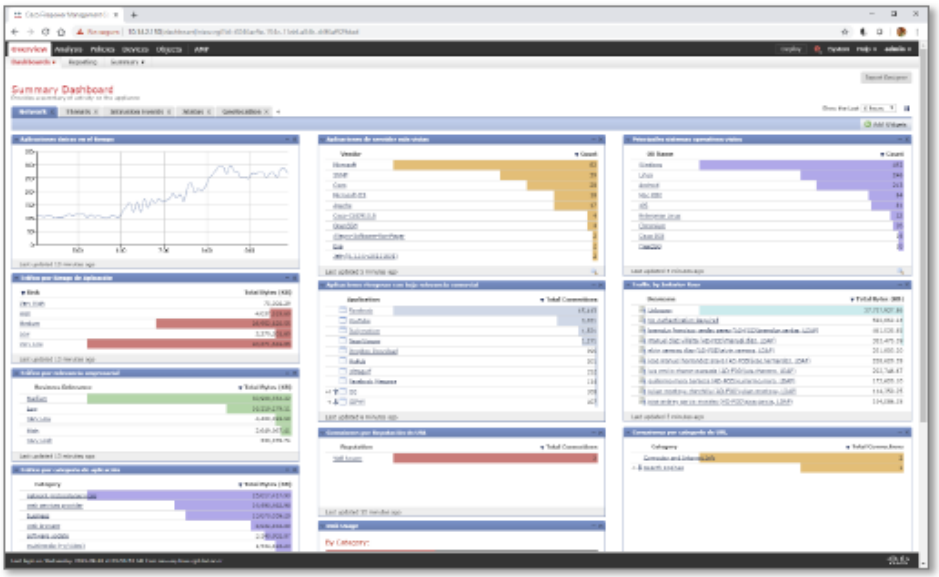
Metodología de evaluación de la solución

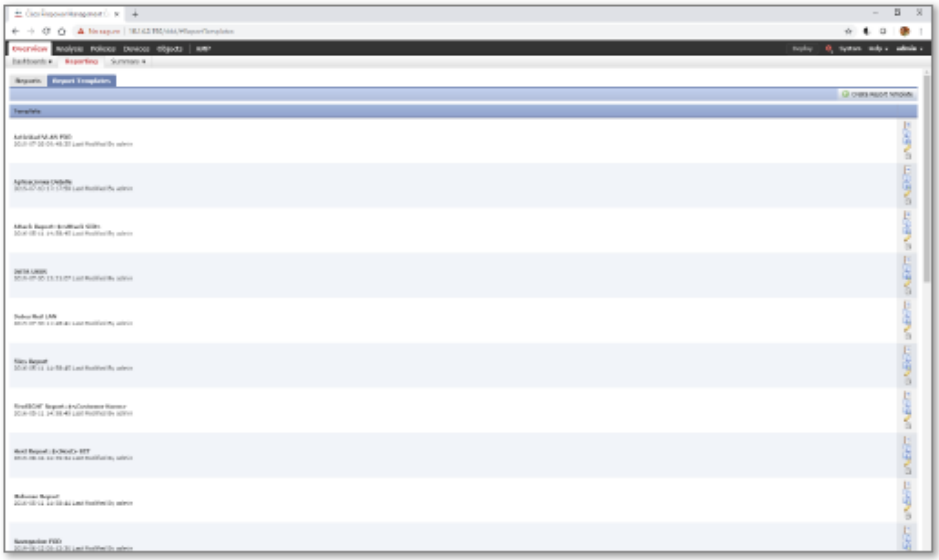




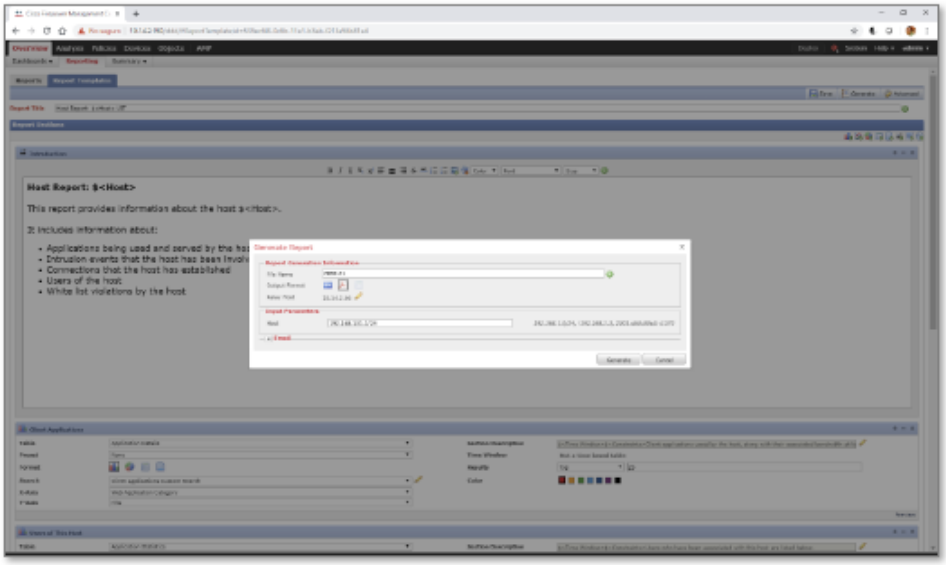
Metodología de evaluación de la solución

- **Los servicios Cisco FirePOWER:** Característica incorporada en el equipo de seguridad Cisco ASA de la serie 5516 que permite entre otras funciones, generar informes haciendo uso de plantillas predefinidas o personalizadas que muestren entre otros, estadísticas de uso, eficacia y eficiencia y caídas en la comunicación sobre la solución de interconexión de la sede central de la FOD y las 9 sedes del Programa Nacional de Informática Educativa MEP-FOD.





Metodología de evaluación de la solución



Host Report: 192.168.101.1/24 UIT

Introduction

Host Report: 192.168.101.1/24

This report provides information about the host 192.168.101.1/24.

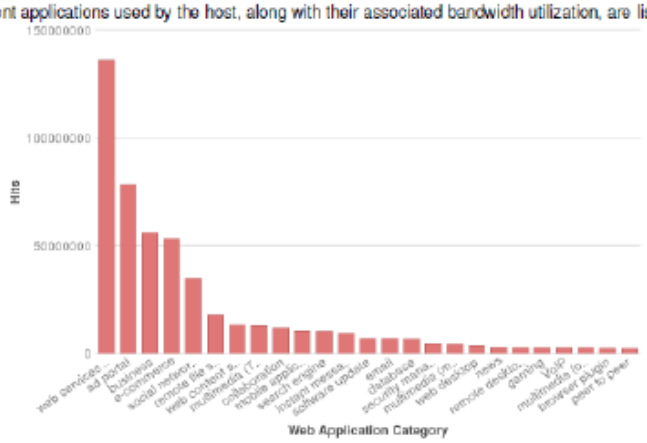
It includes information about:

- Applications being used and served by the host
- Intrusion events that the host has been involved with
- Connections that the host has established
- Users of the host
- White list violations by the host

Client Applications

Constraints: *IP Address = 192.168.101.0/24*

Client applications used by the host, along with their associated bandwidth utilization, are listed below.



Web Application Category	Hits
web services provider	135,930,918
ad portal	78,097,062
business	56,072,095
e-commerce	53,108,518
social networking	34,968,471
remote file storage	17,778,479
web content aggregators	13,286,084
multimedia (TV/video)	12,048,443
collaboration	11,785,905
mobile application	10,482,925
search engine	10,348,799
instant messaging	9,332,324
software update	6,897,611
email	6,881,051
database	6,527,570
security management	4,784,606
multimedia (music/audio)	4,568,765
web desktop	3,470,554
news	2,803,531
remote desktop control	2,615,222

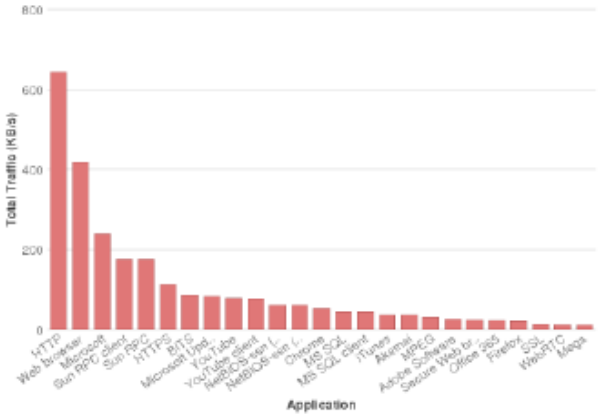
Metodología de evaluación de la solución

Host Report: 192.168.101.1/24 UIT

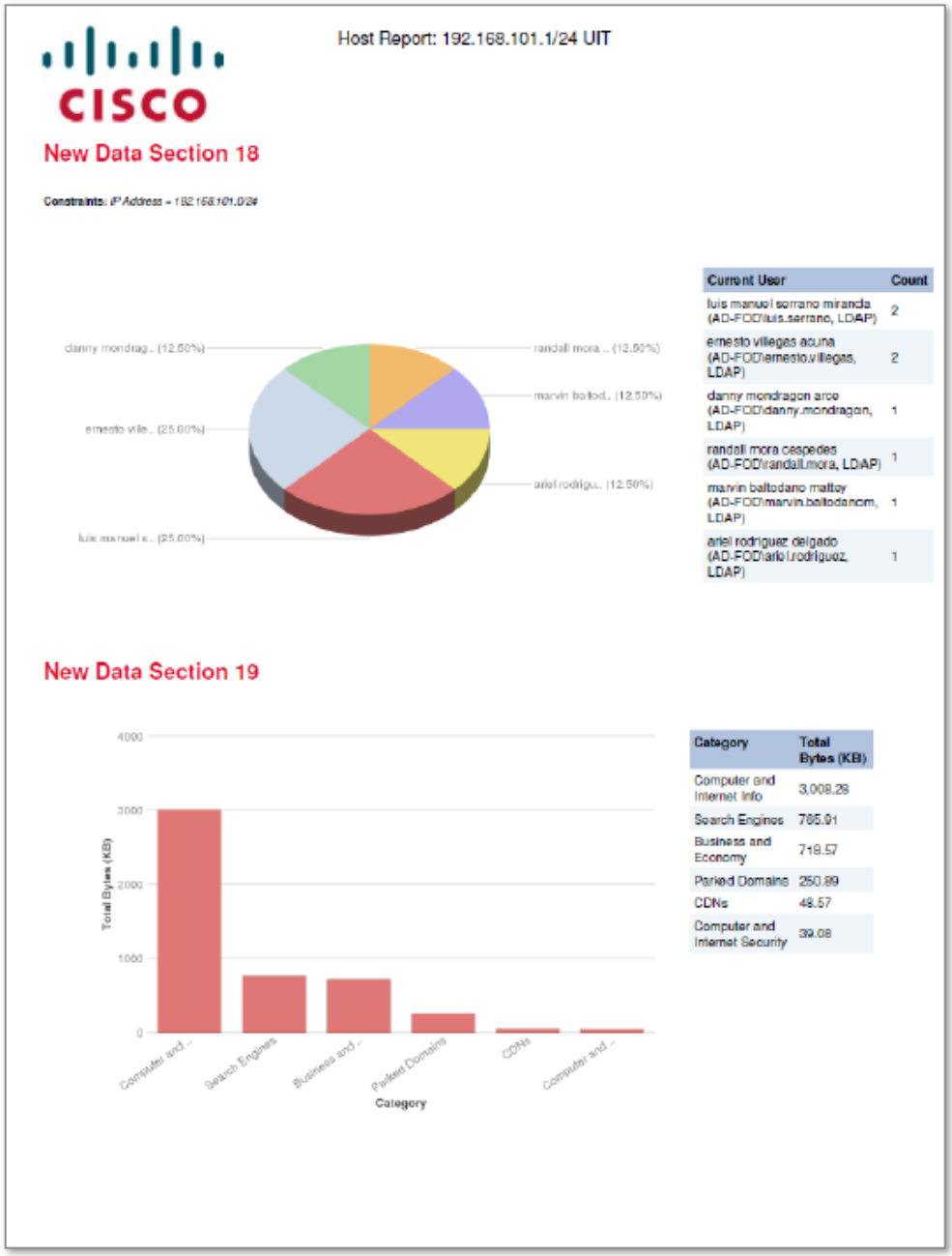
gaming	2,589,310
VoIP	2,513,486
multimedia (other)	2,510,716
browser plugin	2,222,530
peer to peer	2,075,007

Users of This Host

Users who have been associated with this host are listed below.



Application	Total Traffic (KB/s)
HTTP	644.64
Web browser	419.75
Microsoft	239.67
Sun RPC client	176.94
Sun RPC	176.94
HTTPS	114.39
BITS	88.89
Microsoft Update	84.36
YouTube	80.19
YouTube client	79.07
NetBIOS-ssn (SMB)	61.62
NetBIOS-ssn (SMB) client	61.62
Chrome	55.35
MS SQL	45.49
MS SQL client	45.49
iTunes	36.49
Akamai	35.70
MPEG	32.45
Adobe Software	27.62
Secure Web browser	24.85
Office 365	22.81
Firefox	22.60
SSL	15.70
WebRTC	13.49
Mega	13.15



Host Report: 192.168.101.1/24 UIT

New Data Section 18

Constraints: *IP Address = 192.168.101.0/24*

Current User	Count
luis manuel serrano miranda (AD-FOD\luis.serrano, LDAP)	2
ernesto villegas acuna (AD-FOD\ernesto.villegas, LDAP)	2
danny mondragon arce (AD-FOD\danny.mondragon, LDAP)	1
randall mora cespedes (AD-FOD\randall.mora, LDAP)	1
marvin baltodano mattoy (AD-FOD\marvin.baltodanom, LDAP)	1
ariel rodriguez delgado (AD-FOD\ariel.rodriguez, LDAP)	1

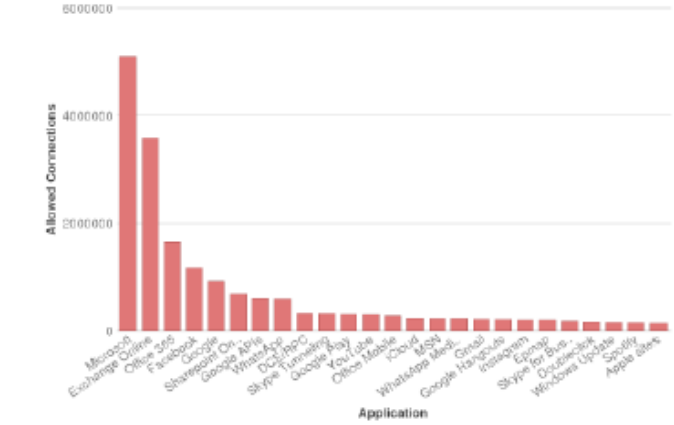
New Data Section 19

Category	Total Bytes (KB)
Computer and Internet Info	3,008.28
Search Engines	765.91
Business and Economy	718.57
Parked Domains	250.89
CDNs	48.57
Computer and Internet Security	39.08

Host Report: 192.168.101.1/24 UIT

New Data Section 7

Application Filter: *Web Applications*



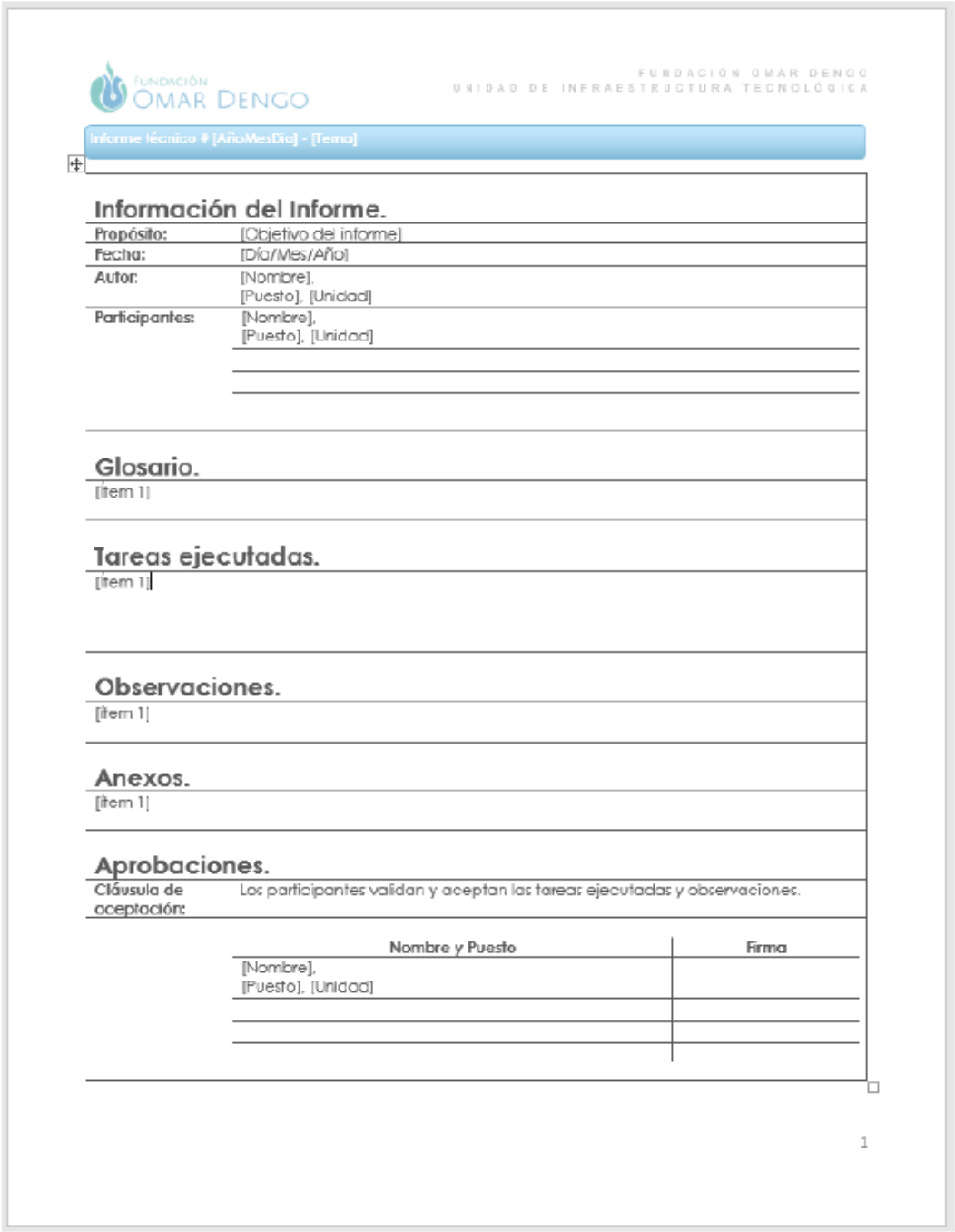
Application	Allowed Connections
Microsoft	5,095,900
Exchange Online	3,583,302
Office 365	1,656,406
Facebook	1,167,320
Google	921,543
Sharepoint Online	685,568
Google APIs	612,523
WhatsApp	601,542
DCE/RPC	330,611
Skype Tunneling	320,145
Google Play	299,936
YouTube	295,389
Office Mobile	279,664
iCloud	242,915
MSN	238,603
WhatsApp Media Message	236,746
Gmail	218,785
Google Hangouts	212,327
Instagram	201,057
Epmap	196,964
Skype for Business	183,091
Doubleclick	169,621
Windows Update	156,561
Spotify	145,314
Apple sites	137,206

Ing. Giovanni Arias C,

Bibliografía

Pensates, J. V. (2017). *Academia.edu*. Obtenido de https://www.academia.edu
Wikipedia. (2017). *Wikipedia*. Obtenido de https://es.wikipedia.org

Plantilla de Informe Técnico



FUNDACIÓN OMAR DENGO
UNIDAD DE INFRAESTRUCTURA TECNOLÓGICA

Informe técnico # [AñoMesDia] - [Tema]

Información del Informe.

Propósito:	[Objetivo del informe]
Fecha:	[Día/Mes/Año]
Autor:	[Nombre], [Puesto], [Unidad]
Participantes:	[Nombre], [Puesto], [Unidad]

Glosario.

[ítem 1]

Tareas ejecutadas.

[ítem 1]

Observaciones.

[ítem 1]

Anexos.

[ítem 1]

Aprobaciones.

Cláusula de aceptación:	Los participantes validan y aceptan las tareas ejecutadas y observaciones.

Nombre y Puesto	Firma
[Nombre], [Puesto], [Unidad]	

1