Propuesta de una red segura para la empresa de telecomunicaciones Telematica Ltda.

Johnnatan Camilo Diaz Castiblanco
Bogotá, Cundinamarca.
Universidad Piloto de Colombia
camilodiaz751@gmail.com

Abstract. This document aims to identify the flaws in the network of the telecommunications company Telematica Ltda, having clear the sector where the company performs, as well as the services and products it offers to its customers. Subsequently, propose actions to be taken to minimize the risk of a Hackening type attack or any other that may affect the provision of services to its customers. This proposal is focused on a Defense Deep model, where by means of several layers a better security is offered to prevent, identify and delay an attack. It is important to indicate that the information contained in this document is limited by security policies of the company Telematica Ltda. Finally, the conclusions and recommendations found in the development of the document are reported to have a secure network, and in this way guarantee availability, integrity and confidentiality of the assets of the company.

Palabras Clave- Ataque, Hackening, DDos, Vulnerabilidades, Clúster, hardening, VLAN, HSRP, Firewall, Router, switch, LAN

I. INTRODUCCIÓN

El artículo describe el escenario actual de una empresa del sector de telecomunicaciones la cual ofrece varios servicios y productos de actualidad. Entendiendo ese escenario, y aplicando el modelo de defensa en profundidad, se propondrán varias recomendaciones a la empresa para evitar que esta sea blanco de algún tipo de ataque interno o externo que afecte la operación y prestación de sus servicios.

En la actualidad se encuentran varias empresas del sector de telecomunicaciones que no aplican ningún modelo de protección, dejándolas vulnerables a algún ataque de tipo Hackening, DDoS (Denegación del servicio), ping de la muerte, Man-In-The-Middle y puertos TCP/UDP abiertos para atacar vulnerabilidades, entre otros. Por ello, en este artículo se cita una empresa de telecomunicaciones para poder abordar los aspectos más importantes y enfocarla al modelo de defensa en profundidad para minimizar el riesgo de cualquier ataque.

El modelo de defensa en profundidad que se empleara permite una mayor seguridad ya que cuenta con varias capas para prevenir, identificar y retardar algún ataque que se vaya a presentar. Estas capas a su vez cuentan con varios niveles de seguridad independientes, las cuales se describen a continuación:

Figura 1. Modelo de Defensa en Profundidad [1]

II. CONTEXTUALIZACION TELEMATICA LTDA.

A. La organización

Telematica Ltda, es una empresa de telecomunicaciones fundada en Casanare, Colombia en 1997, la cual presta servicios de telecomunicaciones a empresas del sector petrolero y la industria en general. Entre los principales servicios ofrecidos son los siguientes:

- Instalación de redes vía microonda, fibra óptica y satelital.
- Implementación de redes para telemetría.
- Acceso dedicados a internet (ADI)
- Carrier de Telecomunicaciones en los departamentos de Meta y Casanare.

Para la prestación de los servicios la empresa cuenta con una infraestructura propia de radio microondas, lo cual permite una cobertura en los departamentos del Meta y Casanare enfocada especialmente para el sector petrolero. Adicionalmente se cuentan con canales dedicados de fibra óptica para la interconexión de las sedes principales.

Telematica cuenta con su sede principal en la ciudad de Yopal (Casanare) y cuenta con 3 sedes remotas en Bogotá (Cundinamarca), Puerto Boyacá (Boyacá) y Puerto Gaitán (Meta).

B. Infraestructura de red actual

Teniendo en cuenta que Yopal es la sede principal, en ella se encuentran los principales equipos de red y base de datos para la operación y prestación de los servicios de la empresa. En Yopal se cuenta con una granja de servidores para base de datos, servidores de monitoreo de red (disponibilidad de servicios, SNMP, Syslog Log de eventos), aplicativo Geminus para la gestión contable, y algunos servicios tercerizados con otro proveedor como la página Web y servicios de correo electrónico.

Las sedes de Yopal, Puerto Gaitán y Puerto Boyacá, cuentan con un firewall de borde para administrar la seguridad perimetral, la sede de Bogotá a diferencia está conectada directamente al proveedor de internet y los usuarios acceden a los aplicativos corporativos mediante una VPN Cliente-Servidor implementada en el Firewall principal de Yopal.

A continuación se describe la topología de red actual, la cual será de posterior análisis con el modelo de Defensa en Profundidad:

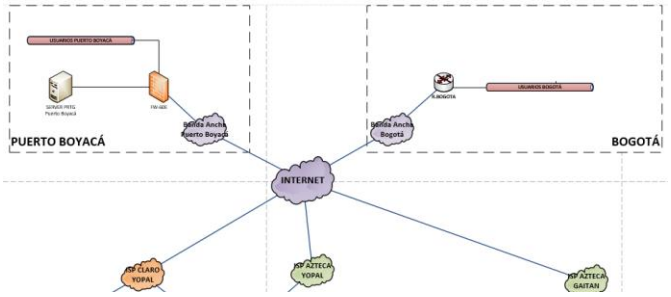

Figura 2. Topología de red Puerto Boyacá y Bogotá.

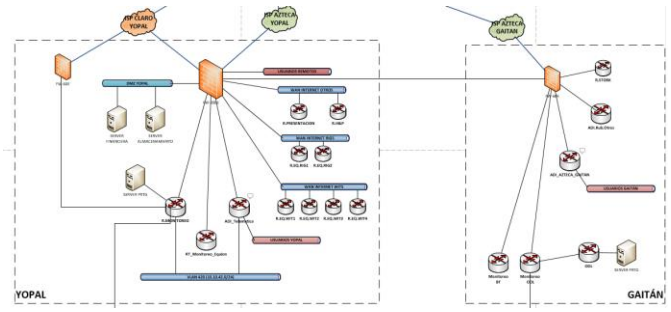

Figura 3. Topología de red en Yopal y Puerto Gaitán.

Como se observa en la anterior imagen, cada uno de los routers corresponden a servicios prestados a los clientes. Estos están centralizados en un único firewall él cuenta con las políticas de seguridad para restringir la comunicación ente estos.

C. Hallazgos encontrados en la organización

A continuación se describen algunos hallazgos encontrados en la organización que pone en riesgo la disponibilidad, integridad y confidencialidad de los servicios e información de la organización:

- Se evidencia que en la sede Yopal, toda la infraestructura esta dependiente de un único equipo Firewall, el cual puede presentar alguna falla o ataque, dejando a la organización sin opción de dar continuidad al negocio.

- Para garantizar la disponibilidad de los servicios prestados por la empresa, en ninguna sede se cuenta con protocolos de redundancia como HSRP de cisco o similares que permita continuar con la conectividad si algún equipo router o switch (capa 3) llegara a fallar.

- No se evidenciaron conexiones de redundancia a nivel de capa de distribución y de acceso.

- No se evidencia implementación de ningún protocolo tipo AAA (Autenticación, Autorización y Contabilización) para control de acceso a la red. Tampoco se observa algún servidor de directorio activo para la gestión o administración de los usuarios que requieren acceder a la red.

- En la sede de Bogotá se encuentran las gerencias de comercial y contabilidad, donde no se observa la implementación de un equipo de seguridad perimetral Firewall, dejando vulnerabilidades con posibles ataques en esta sede.

III. DEFENSA EN PROFUNDIDAD

Teniendo como base el modelo de defensa en profundidad, se realizan las observaciones correspondientes en cada capa:

A. Políticas, Procedimientos, Concientización

- Desarrollo del Sistema de Gestión de la seguridad de la Información. SGSI. Implementación de ISO 27000.

- Procedimientos, manuales, responsabilidades, registros del SGSI. Capacitaciones, actualizaciones y continuo seguimiento del SGSI.

- Auditorías Internas y externas. Así como el seguimiento a los contratos de contratistas y acuerdos de niveles de servicio con proveedores.

- Controles de ingreso de personal a la empresa.

- Gestion de contraseñas para acceso remoto y administración de equipos.

- Documentación y procedimientos establecidos para el control de cambios. Esto para hacer el debido seguimiento a los cambios realizados en la infraestructura de la organización y prevenir alguna afectación sobre los servicios prestados. Estos deben ser aprobaros por las autoridades de áreas (Seguridad física, perimetral, red interna y de aplicaciones).

B. Seguridad Física

- Se recomienda un esquema de seguridad en 4 capas, la cuales inician en seguridad perimetral (Seguridad privada edificio), seguridad en instalaciones (Guardia interno o recepción), seguridad Centro de computo (Autoridad de Área), y seguridad en Rack (Responsable y Custodio de llaves). Este modelo en capas imposibilita alguna acción de ataque, alteración o conexión no autorizada a la infraestructura de red de la empresa.

- La empresa Telematica Ltda. cuenta con cámaras de seguridad en las sedes de Bogotá y Puerto Boyacá. Se recomienda la instalación de sistemas de CCTV y control de acceso en la totalidad de las sedes (Puerto Gaitán y Bogotá) concentrado la información de registros y Videos en servidores locales con posibilidad de replicar la información a la nube.

- Las 4 (cuatro) sedes de la empresa deben contar con sistemas de energía de respaldo como plantas de energía por combustible o soluciones de energía solar que cumplan con una autonomía determinada por el personal especializado.

- Registro de ingresos a la empresa, así como registro de ingreso a los cuartos de comunicaciones de cada sede.

- Política de apagado de puertos físicos para evitar el acceso no autorizado a la red.

- Capacitaciones y actualizaciones al personal de seguridad física en cuanto a nuevas modalidades de ingresos no autorizados a instalaciones de la organización.

- Para los servicios de Carrier, ADI y telemetría, esta capa de seguridad debe ser acordada con el cliente de manera contractual para definir responsabilidades de las partes.

C. Perímetro

- En Yopal la empresa actualmente cuenta con un único Firewall que soporta toda la operación, se recomienda la instalación de un segundo Firewall o secundario que permita la configuración en modo Clúster con el principal para garantizar la redundancia y seguridad de la red. Estos equipos operaran en estado Activo – Activo para mantener continuo seguimiento de su correcta operación.

- En la sede de Bogotá, se recomienda la instalación de un Firewall, para gestionar la seguridad perimetral en la sede.

- Según la criticidad de los servicios en las sedes de Puerto Gaitán y Puerto Boyacá, se recomienda una arquitectura similar al Clúster de firewall recomendado para Yopal. Esto ya que genera sobrecostos en la implementación pues actualmente solo cuentan con uno de estos equipos.

- Se recomiendan hacer pruebas de penetración por lo menos una vez cada 3 meses para identificar las vulnerabilidades que podrían explotar los atacantes.

- Configuración de VPN Site – to – Site sobre los canales de datos dedicados y sobre internet con proveedores para minimizar el riesgo de fuga de información o ataques a la red interna de la organización. Configuración mediante túneles con cifrado IPSEC o SSL.

- La empresa cuenta con una zona restringida para el acceso a los servidores de aplicaciones, bases de datos y monitoreo. Se debe llevar esta configuración a las demás sedes.

- Para los servicios de telemetría prestados por la empresa, se continúa con la configuración de túnel VPN de origen a vestido de la data para evitar que tenga alguna manipulación en su recorrido. Esto sigue controlado de manera contractual con los clientes.

- Para los clientes de acceso dedicado a internet (ADI), se realiza la separación lógica mediante VLANs independientes por clientes hasta el Core de la empresa y posteriormente enrutar el tráfico a internet. Esto para evitar comunicación entre cada uno de ellos y ofrecer niveles de seguridad a nivel de firewall.

D. Red Interna

- Configuración de un protocolo de redundancia a nivel de LAN como HSRP (Hot Standby Router Protocol) u otro.
- Hardening mediante un protocolo AAA (Autenticación, Autorización y Contabilización), como lo es RADIUS para el control de acceso a la red que operare con un protocolo de directorio activo como lo es LDAP. De esta forma se restringe el acceso a la red de personal no autorizado.

- Para los usuarios visitantes en las instalaciones, se recomienda la configuración de un portal cautivo de cualquier tipo hardware o software, para que ellos a su vez tengan un acceso restringido a la red.

- Se mantiene la configuración de VLANs para separar lógicamente el tráfico de cada una de las

dependencias así como evitar problemas de tormenta de broadcast en la red.

- Configuración de listas de acceso ACL en los router o switches capa 3 en cada una de las sedes para evitar comunicación entre segmentos o equipos no requeridos.

E. Host

Se deben mantener actualizados los sistemas operativos de los equipos de cómputo, así como el antivirus, malware y firmware de estos dispositivos.

Se recomienda realizar escaneo de vulnerabilidades con regularidad a los Host para hacer las correcciones debidas y evitar que estas sean explotadas por algún atacante.

Configuración de sesiones para usuarios con las debidas restricciones evitando que estos hagan uso indebido del equipo. También la creación de sesiones de administración para la gestión de seguridad en los equipos.

F. Aplicación

Desarrollo de aplicación con técnicas de programación seguro.

Aplicación de un protocolo de control de acceso a aplicaciones como lo es LDAP, el cual emplea un directorio activo para permitir o denegar servicios.

Pruebas de penetración (PenTest) por lo menos una vez cada 3 meses y de esta forma atender vulnerabilidades en las aplicaciones. Estas pruebas se pueden desarrollar sobre la granja de servidores de la empresa, así como el servidor de contabilidad Geminus. En estos se encuentra la información más crítica de la empresa.

G. Datos

Algoritmos de encriptación seguros como AES256, CHAP u otros para la transferencia de la información. Así como protocolos de encriptación como WAP2, IPSec, SSL entre otros para contraseñas y túneles VPN.

Aplicación de hardening en los equipos de almacenamiento para evitar fuga o alteración de la información.

Políticas definidas en el ámbito forense para las bases de datos. Esto para la correcta gestión y eliminación de la data en la empresa.

IV. TOPOLOGIA DE RED PROPUESTA

A continuación se relaciona la topología propuesta para la empresa de telecomunicaciones Telematica Ltda. Es importante indicar que la infraestructura de red de la empresa en un 90% es de marca Cisco, por lo cual se pueden implementar protocolos como HSRP interconectados a los firewall de marca Fortigate para toda la seguridad perimetral de la empresa.

Teniendo en cuenta que la sede de Yopal es la principal de la empresa, se propone la siguiente topología para garantizar la continuidad de los servicios ante alguna falla o ataque:

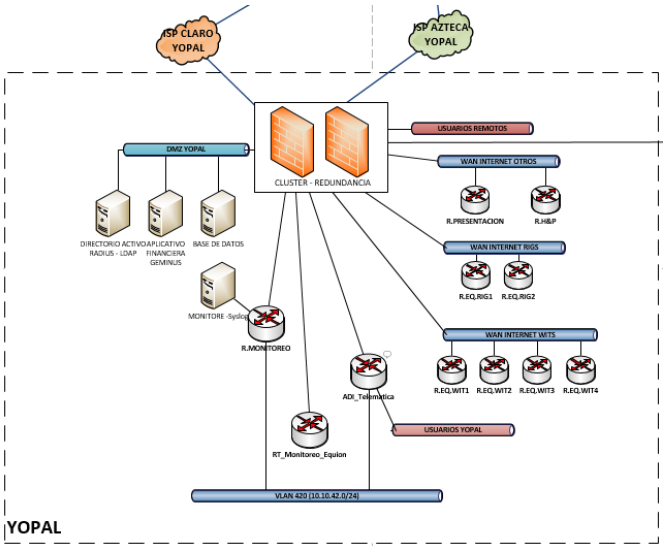

Figura 4. Topología propuesta para la red de Yopal

Para las sedes de Puerto Boyacá y Puerto Gaitán como son las sedes donde tiene mayor presencia y operación la empresa, se propone la implementación de una arquitectura como Yopal. Eso sí teniendo en cuenta que es importante tener planes claros de migración a la nube para todos los servicios tanto de base de datos, aplicaciones de financiera y monitoreo para que cumplan con los niveles de disponibilidad y no dependan de equipos físicos de Yopal.

V. MODELO JERARQUICO EN CAPAS DE CISCO

Luego de implementar el modelo de defensa en profundidad anteriormente descrito en cada una de sus capas con sus respectivas observaciones, se recomienda la implementación del modelo Jerárquico en capas de Cisco. Esto garantiza un diseño de red organizado por capas que permite la implementación de varias funciones específicas a la red.

Las arquitecturas de red planas son poco escalables y si se requiere alguna configuración, esta a su vez afecta en gran medida la operatividad de toda la red.

Un diseño de red LAN jerárquico incluye las siguientes tres capas [2]:

- Capa de Núcleo
- Capa de Distribución
- Capa de Acceso

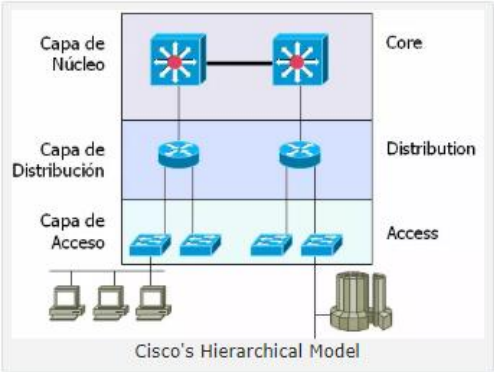

Figura 5. Modelo Jerárquico por capas de Cisco

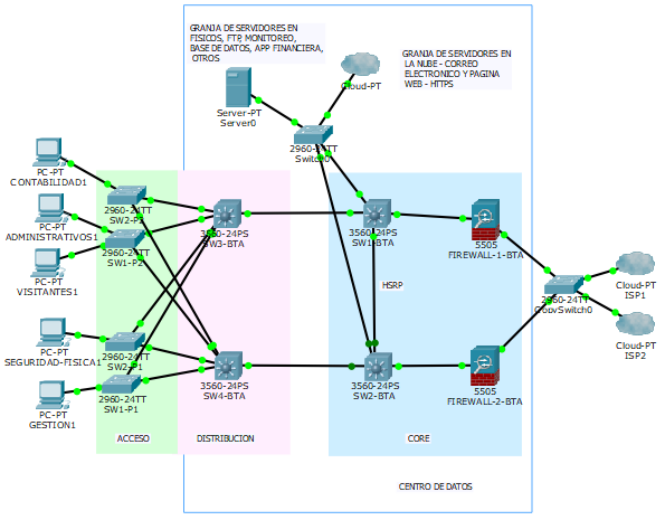

Figura 5. Topología propuesta para Yopal con el modelo jerárquico por capas de Cisco.

A. Capa de Núcleo

Esta capa estará conformada por los equipos de red como firewall, routers y switches capa 3; los cuales son los encargados de hacer el enrutamiento interno de la empresa para la disponibilidad de todos los servicios. Adicionalmente, son los encargados de establecer la comunicación con equipos externos (nube o equipos de clientes remotos) para prestación del servicio.

En esta capa están alojados los firewall en modo de clúster para garantizar la redundancia de la red de la empresa.

Políticas de seguridad aplicadas para la restricción a bases de datos a personal no autorizado, así como el bloqueo de puertos FTP. SNMP, SMTP, POP, TELNET u otros para evitar el acceso a recursos críticos de la empresa.

Configuración de protocolos de enrutamiento dinámico como EIGRP propietario de Cisco u OSPF para la interconexión de cada una de las sedes. Se recomienda la configuración de un protocolo como OSPF ya que es compatible con varios fabricantes. Es importante configurar políticas de seguridad del protocolo para evitar ataques por este en toda la red. Adicionalmente, para la gestión de la red o equipos, se recomienda la configuración de enrutamiento estático para evitar perdida de gestión de equipos si el protocolo de enrutamiento dinámico fuese alterado por algún atacante.

Segmentos de Gestion configurados para administrar todos los equipos de red mediante protocolos seguros como SSH en su versión 2 o 3 preferiblemente.

B. Capa de Distribución

Políticas de seguridad para el apagado de puertos físicos que no se encuentran habilitados.

Teniendo en cuenta que la infraestructura de red de la empresa Telematica Ltda no es muy grande, se recomienda conectar a puertos de Giga o TenGiga la granja de servidores, servidores de monitoreo y servidores de aplicaciones a los equipos switch capa 2 o 3 dentro de esta capa de distribución.

La finalidad de esta capa es brindar una redundancia a los equipos Switch de cada piso, donde sus puertos físicos deben estar bajo el esquema de configuración Activo/Stanby y las troncales entre los switch de acceso y los switch de distribución deben operar a 1 Gbps o 10 Gbps.

C. Capa de Acceso

En esta capa es donde los usuarios mediante sus dispositivos se conectan a la red para acceder a los servicios corporativos o públicos. Para ello, es importa que en la empresa se apliquen las respectivas políticas de seguridad a nivel de la red alámbrica e inalámbrica.

Configuración de VLANs para la debida segmentación de la red en cada una de las sedes de la empresa.

Política de apagado de puertos para evitar la conexión de usuarios no autorizados a la red.

Se emplean protocolos AAA para el control de acceso a la red como el protocolo Radius que mediante la autenticación en un directorio activo permite o deniega el acceso de equipos a la red.

Para el control de acceso a la red de visitante en las sedes de la empresa se recomienda la configuración de un portal cautivo con parámetros específicos (tiempo, restricción de páginas, publicidad) según criterios de la empresa.

Como se puede evidenciar en esta capa de acceso del modelo de Cisco, varias de las recomendaciones se relacionan con las aplicadas en la capa de red Interna del modelo de defensa en profundidad indicada al inicio del documento.

VI. CONCLUCIONES

- Para una red segura y operativa se propone la implementación de un modelo de defensa en profundidad, el cual debe estar elaborado con los lineamientos de buenas prácticas en el diseño de la red. Entre estas buenas prácticas se puede aplicar el modelo jerárquico en capas de Cisco.
- Para poder brindar recomendaciones a la empresa Telematica Ltda. en cuanto a la seguridad en su red, se debió primeramente contextualizar la organización e identificar la infraestructura de red actual para poder hacer las recomendaciones más acertadas a la realidad de la organización.
- La empresa Telematica Ltda. La cual opera en el sector de telecomunicaciones debe tener diseñada e implementada una red segura para que todos los servicios ofrecidos por la empresa cuenten con estándares de calidad. Para lo anterior se recomiendo la gestión de un SGSI mediante ISO 27000, así como la implementación de ISO 310000.
- Se recomienda invertir en infraestructura de red como es el caso de la sede de Yopal, donde se requiere la implementación de un clúster a nivel de firewall para garantizar la continuidad del servicio si el equipo firewall principal dejase de operar.
- La adopción del modelo jerárquico por capas de Cisco proporciona una arquitectura de red segura y permite la escalabilidad sin tener afectación de los servicios actualmente prestados. Esto debido a que si la arquitectura es plana, todos los cambios pueden presentar un alto impacto sobre la infraestructura de red en general.
- Se recomienda realizar periódicamente por lo menos dos veces al año hardening a los equipos físicos o virtuales involucrados en cada una de las capas del modelo de defensa en profundidad. Esto para evitar que nuevas vulnerabilidades puedan ser explotadas por algún atacante.
- Se recomienda a la empresa Telematica Ltda en sus equipos de seguridad perimetral como Firewall bloquear todos los servicios disponibles (Puertos TCP/UDP) e ir habilitándolos a medida que estos se vayan requiriendo con previa autorización. Esto para mantener el debido control de todos los servicios que la empresa esta operando.

REFERENCIAS

[1] Implementación de seguridad en aplicaciones y datos [Online]. Available: http://download.microsoft.com/download/d/1/a/d1af3504-adb7-40ce-a460-ac8ba4a8a044/implementingapplicationsecurity_es.ppt

[2] Resumen de diseño de la red LAN cableada del campus [Online]. Available: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Johnnatan Camilo Diaz Castiblanco, nació en Bogotá, Colombia, el 3 de noviembre de 1988. Se graduó en la Universidad Industrial de Santander como Ingeniero Electrónico y se encuentra realizando una especialización en Telecomunicaciones en la Universidad Piloto de Colombia. Titulado como Ingeniero con la tesis de grado “Diseño y construcción del prototipo de una herramienta magnética para el tratamiento a muestras de crudo del Campo Escuela Colorado (UIS - ECOPETROL)”, estando enfocado al tema de precipitación de ceras tipo parafínicas. Certificado en implementación Cisco MPLS. Diplomado Internetworking Cisco(r) CCNA – FEUD – fundación de egresados universidad distrital. Ejerció profesionalmente en la empresa Skynet Colombia y Gilat Colombia como Ingeniero de proyectos para los trabajos de los Kioscos Vive Digital en todo el territorio nacional colombiano. Adicionalmente, labora en la compañía Telematica Ltda con sede principal en la ciudad de Yopal, Casanare, Colombia, donde opera como Profesional especialista y administración de la red para la prestación de todos los servicios de la empresa. En esta última compañía, ha liderado la implementación de varios proyectos de conectividad para empresas del sector de petróleos. Estos servicios están diseñados para brindar acceso a internet, telefonía IP, telemetrías y sistemas de radio troncalizado.
Capacitado por fabricantes como Cisco, TRENDnet, HID, Motorola y otros para la prestación de los servicios de telecomunicaciones.
Entre sus campos de interés están la implementación de redes seguras en los protocolos de enrutamiento dinámicos como EIGRP, OSFP, BGP, asi como la implementación de redes MPLS para dar cobertura a nivel de capa 2 y 3 a varios de sus clientes en los departamentos del Meta y Casanare.