**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE INGENIERÍA**

# Soporte remoto para redes empresariales

**INFORME DE ACTIVIDADES PROFESIONALES**

Que para obtener el título de

**Ingeniera en Computación**

**P R E S E N T A**

María del Consuelo Carbajal Domínguez

**ASESOR DE INFORME**

Dr. Eduardo Espinosa Ávila

**Ciudad Universitaria, Cd. Mx., 2022**

## *Agradecimientos*

A mi padre, porque sé que le dará muchísimo gusto que este logro sea uno más.

A mi madre, porque desde siempre me extendió la mano de manera incondicional cuando más la necesitaba, para lograr todas mis metas que tuviera y porque en este ciclo que está por concluir me dio los ánimos suficientes para armarme de valor y así cerrar esta etapa tan importante de mi vida.

A mis dos hermanos menores, por considerarme un gran ejemplo a seguir, lo cual me dio ánimos para tomar la decisión de terminar con este ciclo y porque de corazón espero que ellos muy pronto tengan este mismo logro.

A mis abuelos maternos (mis segundos padres), por el apoyo incondicional que me brindaron en todos los aspectos desde que tengo uso de razón, y porque sin ellos este camino hubiera sido más difícil. El logro también es de ellos.

A los pocos amigos que sabían que yo andaba haciendo este proyecto, porque siempre me dijeron que nunca era tarde para lograr esta meta, que lo importante era alcanzarla y que nunca pierda las ganas de seguir superándome.

A mi queridísima UNAM, porque mi sueño de ser parte de ella se cumplió el día que fui admitida para entrar al bachillerato y por vivir muy orgullosa de pertenecer a la máxima casa de estudios. Siempre la llevaré en mi corazón.

A la empresa donde estoy trabajando actualmente, por haberme dado la oportunidad de hacer la experiencia laboral que me permitió escribir este trabajo y porque a diario me demuestra que siempre hay algo nuevo por aprender y retos por afrontar.

A la doctora Tanya Sandoval, porque me ayudó a obtener la herramienta más importante para terminar este ciclo: la confianza en mí misma.

Y a DIOS, porque permitió todo lo anterior, porque me dio la oportunidad de terminar mi carrera, de alcanzar este logro, de tener el trabajo que tengo, por la salud y la vida.

# ÍNDICE

# INTRODUCCIÓN

Este reporte contiene una descripción de la función que estoy desempeñando como empleada dentro de la empresa Unired, en la que me encuentro laborando desde el 25 de enero del 2016 a la fecha. Con base en la descripción mencionada se mostrará la relación existente entre ella y las materias del módulo de redes y seguridad, en específico de las de redes, de la carrera de Ingeniería en Computación.

En el primer capítulo hablaré sobre la empresa Unired: historia, misión, visión, principios empresariales y hablaré sobre el concepto del centro de trabajo donde laboro.

El segundo capítulo es el marco histórico de este informe, el cual habla sobre las redes de computadoras: un poco de historia, concepto, usos de las redes de computadoras, tipos, componentes de las redes de computadoras, y ya que se tenga conocimiento de los conceptos mencionados trataré sobre las redes empresariales: aplicaciones, impacto de la tecnología sobre las redes empresariales y soporte a las mismas.

En el tercer capítulo trataré acerca de la descripción de mi puesto de trabajo, donde retomaré conceptos vistos en el marco teórico, ya que suelo emplear términos técnicos para precisamente detallar mis actividades laborales.

El cuarto capítulo es un glosario de términos, el cual contiene aquellos conceptos o tecnicismos que podrían dificultar el entendimiento de este informe a cualquier persona que lo llegue a leer.

## OBJETIVO

Describir mis funciones como ingeniera de soporte remoto o también conocido como operador multiplataforma dentro de la empresa donde me encuentro laborando actualmente, a partir de los conceptos de redes que adquirí en diversas asignaturas del plan de estudios de la carrera de Ingeniería en Computación, correspondientes al módulo de redes y seguridad, en específico de redes.

# CAPÍTULO 1.

# EMPRESA: UNIRED

## 1.1 HISTORIA

UNIRED S.A. de C.V. es una empresa 100% mexicana, líder en el mercado nacional de las telecomunicaciones, dedicada al diseño e integración de soluciones corporativas de comunicación de voz, datos, video y servicios administrados de tecnologías de información. Es una filial de Teléfonos Mexicanos.

A continuación se muestran datos de la empresa de manera general:

**Año de creación**

1991

**Tipo de empresa**

De financiación privada

**Especialidades**

Negocios TELCO y servicios IP, *Data center*, *cloud* y servicios administrados TI, servidores virtuales, soluciones de negocio verticales (de acuerdo a la actividad de la empresa cliente), centros de monitoreo especializados, comunicaciones unificadas.

**Sedes:**

Sede de Ciudad de México

Sede de Querétaro

### 1.1.1 MISIÓN Y VISIÓN

Es importante mencionar tanto la misión como visión de la empresa, debido a que, la misión se refiere al propósito para la que la empresa fue creada y la visión habla acerca de los objetivos a corto, mediano o largo plazo.

- Misión: "Ser un grupo líder en telecomunicaciones proporcionando a nuestros Clientes soluciones integrales de gran valor, innovadoras y de clase mundial, a través del desarrollo humano y de la aplicación y administración de tecnología de punta."

- Visión: "Consolidar el liderazgo de Unired en el mercado nacional, expandiendo su penetración de servicios de telecomunicaciones en todos los mercados posibles, para ubicarnos como una de las empresas de más rápido y mejor crecimiento a nivel mundial."

### 1.1.2 VALORES

Los valores apoyan la misión, y sustentan tanto los principios empresariales como principios de conducta. Los valores son las cualidades que distinguen a la empresa y la orientan. Es necesario que en la labor cotidiana se tengan presentes siempre y se lleven a la práctica.

Los valores de cultura corporativa son:

a. Trabajo: Es cualquier actividad humana que satisface una necesidad, ya sea económica, emocional o de crecimiento personal. Es un valor, porque sólo a través de él podemos cubrir nuestras necesidades y al mismo tiempo servir a los demás.

b. Crecimiento: Cada persona conforme a sus capacidades debe mantener un desarrollo y una superación a lo largo de toda su existencia. Las personas son seres en potencia y desarrollo, por lo que sólo a través del crecimiento conocen y desarrollan nuevas capacidades.

c. Responsabilidad social: Hoy en día es imposible vivir de manera aislada. Toda actividad, ya sea personal o colectiva repercute en la sociedad, por lo que se necesita compromiso y actitud de servicio hacia la comunidad. La responsabilidad social busca encontrar un bien común abarcando conductas como el cumplimiento de leyes gubernamentales hasta el cuidado y manejo de todo tipo de recursos.

d. Austeridad: Cuidado y utilización eficiente de recursos gastando solamente lo necesario. Es una posibilidad para crear, aprovechar, imaginar y crecer.

### 1.1.3 PRINCIPIOS EMPRESARIALES

Estos principios indican las características particulares de la empresa con relación a su actividad específica que son las Telecomunicaciones. Los principios empresariales de Unired son los siguientes:

a. Servicio al cliente: El cliente es la razón fundamental de las actividades en la empresa. La atención a ellos es esencial para seguir contando con su preferencia. El cliente debe ser tratado con respeto y cumpliéndole cabalmente las condiciones de servicio pactadas con él.

b. Calidad: La atención y servicio hacia el cliente se logra con la disponibilidad de servicios y productos que satisfagan sus expectativas de manera eficiente y oportuna. Cuidar la calidad del servicio comprende una serie de factores intangibles que repercuten en la preferencia del cliente, como la atención cortés, adecuada ubicación, instalación y operación de nuestros centros de atención, oportunidad y veracidad de nuestras respuestas.

c. Vanguardia tecnológica: La calidad, servicio al cliente y liderazgo sólo son posibles con la incorporación de tecnología más moderna en la empresa. Mantenerse a la vanguardia tecnológica es indispensable tanto para el desarrollo de la empresa como para ofrecer al cliente más y mejores servicios.

## 1.2 CENTRO NACIONAL DE OPERACIÓN DE REDES DE CLIENTES

### 1.2.1 Contexto organizacional del Centro de Operación de Redes

El Centro de Operación de Redes Empresariales NOC (del inglés *Network Operation Center*) es una unidad de negocio perteneciente a Unired, la cual forma parte de las empresas de Teléfonos Mexicanos, enfocada a la integración de redes y la provisión de servicios administrados.

En este contexto el cliente empresarial representa a la entidad que contrata los servicios del NOC de Unired a través de Teléfonos Mexicanos, siendo este último el responsable de la comercialización, facturación y cobro de dichos servicios hacia el cliente empresarial. Cabe mencionar que es responsabilidad de Teléfonos Mexicanos, el manejo y administración de los contratos derivados de dicha relación.

Con base en las premisas de negocio para los servicios administrados en Teléfonos Mexicanos, se crea la unidad de negocio denominada NOC, enfocado en la entrega de soluciones de administración, gestión y monitoreo de acuerdo con lo estipulado en su portafolio de Servicios de Negocio.

Como parte de la confianza que Teléfonos Mexicanos deposita en esta unidad de negocio y con el objetivo de lograr la diversificación de mercados se crean torres de servicio especializadas en la atención y soporte de mercados específicos. Estas torres se encuentran en diferentes localidades del país.

### 1.2.2 Sistema de Gestión Integrado (SGI)

El NOC se rige por un sistema llamado SGI

El SGI es un conjunto de elementos (estrategias, objetivos, políticas, estructuras, recursos y capacidades, métodos, tecnologías, procesos, procedimientos), interrelacionados entre sí que permiten a la Alta Dirección planificar, ejecutar y controlar todas sus actividades al logro de los objetivos de calidad preestablecidos.

El NOC cuenta con tres certificaciones las cuales conforman en el Sistema de Gestión Integrado.

* ISO/IEC 20000-1 Sistema de Gestión de Servicios de Tecnologías de la Información

* ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información

* ISO 22301Sistema de Gestión de continuidad

POLÍTICAS GENERALES DEL SGI

- POLÍTICA DE GESTIÓN DEL SERVICIO DE TI: Brindar servicios administrados de clase mundial a través de nuestro catálogo de servicios y tecnóloga, bajo un marco de estándares internacionales implementados por el NOC y los organismos reguladores dentro de un sistema de mejora continua, soportado por un equipo humano competente; con el fin de satisfacer el servicio comprometido con los clientes así como los objetivos del negocio de manera efectiva y eficiente.

- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: Garantizar la integridad, confidencialidad y disponibilidad de los entregables de los Servicios de Negocio del NOC, específicamente lo siguiente: Reportes entregados a los clientes, portal de consulta de información y los datos obtenidos sobre el desempeño mensual, entregados mediante el servicio administrado y la mesa de servicios, a través del cumplimiento de estándares internacionales de seguridad de la información implementados por el NOC, y las leyes aplicables, dentro de un sistema de mejora continua.

- POLÍTICA DE CONTINUIDAD DE SERVICIOS: Garantizar la continuidad de las actividades críticas que soportan los servicios de negocio del NOC en situaciones de crisis derivadas de una contingencia; específicamente lo siguiente: atención de eventos, portal de consulta de información y reportes entregados a los clientes, teniendo como premisas; la salvaguarda de la vida humana, la protección de los activos y el impacto al negocio, a través del cumplimiento de estándares internacionales de Continuidad del Negocio implementados por el NOC y las leyes aplicables, dentro de un sistema de mejora continua.

# CAPÍTULO 2.

# MARCO TEÓRICO: REDES DE COMPUTADORAS

## 2.1 INTRODUCCIÓN A LAS REDES DE COMPUTADORAS

### 2.1.1 Un poco de historia

La necesidad de comunicación en el ser humano ha existido desde el inicio de los tiempos. A lo largo de la historia de la humanidad se han desarrollado sistemas que han cambiado la forma de establecer la comunicación y de procesar la información a transmitir.

El siglo XX se caracteriza por el desarrollo de la tecnología, donde se vio la instalación de redes de telefonía a nivel mundial, la invención de la radio y televisión, nacimiento y evolución de la computación, de satélites de comunicaciones y la invención de la internet.

En los años cuarenta y cincuenta hicieron su aparición las primeras computadoras, las cuales eran aparatos grandes, costosas y poco eficientes (en comparación con las que conocemos en la actualidad), las cuales sólo estaban al alcance de universidades, grandes empresas u organizaciones. Las mismas se encargaban del almacenamiento y procesamiento de la información que se recibía a través de las terminales pasivas o terminales tontas que estaban conectadas directamente a ellos. Las terminales tontas sólo permiten la entrada y salida de datos, y no tiene capacidad de almacenar o procesar información. Estas terminales compartían un mismo espacio físico y se encontraban ubicadas cerca del o de los equipos centrales a los que se conectaban.

Con el paso del tiempo se tuvo la necesidad de que las terminales se comunicaran con la computadora central a distancias más grandes. Para lograr esa conexión entre terminales a mayores distancias hicieron su aparición los módems, los cuales tenían como funcionalidad convertir una señal telefónica en una señal de datos. Los módems también servían para conectar computadoras entre sí, y es así como aparecieron las primeras redes de computadoras. La función del módem llamó la atención de grandes empresas, lo que hizo que las compañías de teléfonos fueran desarrollando tecnología adecuada para transportar grandes cantidades de datos en las grandes empresas.

## 2.2 REDES DE COMPUTADORAS

A partir de la información expuesta en el punto anterior voy a plasmar los conceptos básicos de las redes de computadoras:

### 2.2.1 Concepto y uso de las redes de computadoras

Una red de computadoras es un conjunto de dos o más elementos conectados entre sí, con el objetivo de intercambiar información y compartir recursos. Las infraestructuras de red pueden variar dependiendo del tamaño del área, del número de usuarios conectados y de los diferentes tipos de servicios disponibles dentro de ésta.

La mayoría de las empresas, desde las pequeñas hasta las más grandes cuentan con un gran número de computadoras, de hecho en casi todas se tiene una computadora por empleado, debido a que, por ejemplo, se tiene al personal de recursos humanos para gestionar documentación y nómina de los empleados, también se tiene al personal del área de sistemas para dar el soporte a nivel hardware o software al personal de la empresa, también se tiene al personal administrativo, etcétera. Cada área tiene una función a cumplir y por tanto diferente información a procesar.

Todas las áreas de una empresa comparten recursos en común. Un ejemplo muy popular son las impresoras, ya que ningún usuario necesita de una impresora propia o privada; también se comparten extensiones telefónicas, computadoras personales; un servidor interno, donde se almacenan los datos correspondientes a las actividades realizadas por determinada área y a la que sólo puede acceder cierto personal; un servidor externo, donde suele almacenarse información presentada al público o información pública; en ocasiones también suelen compartirse teléfonos celulares. El hecho de compartir todos los recursos mencionados tiene como ventaja ahorrarle a la empresa espacio y costo.

Las empresas grandes se componen de una oficina central o matriz y las sucursales. En la oficina central es donde a menudo se alojan equipos o servidores (de los cuales hice referencia en el párrafo anterior) que concentran datos valiosos a los que los usuarios ubicados en las sucursales necesitan acceder de manera remota.

Para acceder a ese tipo de información a los usuarios se les proporcionan credenciales de acceso. Esas credenciales son de carácter personal y deberán actualizarse cada determinado tiempo. En otras palabras, hacer cambio de contraseña. Las credenciales también suelen clasificarse de acuerdo con el puesto o cargo dentro de la empresa, por ejemplo, un empleado tiene credenciales que le permiten gestionar cierta información, mientras que su supervisor o jefe tiene accesos que le permiten visualizar o hasta manipular datos.

Los equipos donde se almacenan estos datos se denominan servidores. Por otro lado, los usuarios al tener acceso de forma remota desde las sucursales a los servidores de la oficina central se les denominan clientes. Los servidores se encuentran bajo la gestión del administrador de la red de la oficina central, quien es la entidad que puede manipular ese equipo y en caso de que un tercero solicite realizarle un cambio, movimiento o intervención el administrador de la red es el responsable de autorizar o no lo solicitado. A este modelo de red se le conoce como cliente-servidor. Este modelo de red es del que estaré haciendo referencia de forma muy constante en el próximo capítulo, donde daré la descripción de mis actividades laborales.

### 2.2.2 Tipos de redes

Las redes de computadoras se clasifican con base en la ubicación geográfica en la que están instaladas:

- Red de área personal PAN (*Personal Area Network*): Se refiere al conjunto de dispositivos que se conectan dentro del rango de una persona. Un ejemplo es la red inalámbrica a través de la cual un usuario conecta su teclado, *mouse*, impresora o módem con su laptop o computadora. Este tipo de red suele ubicarse en un cuarto o despacho

- Red de área local LAN (*Local Area Network*): es una red de propiedad privada que opera dentro de un solo edificio, casa, sucursal, cafetería o incluso restaurantes. Este tipo de red se utiliza para conectar computadoras con el fin de compartir e intercambiar información, ubicadas en una misma construcción física.

- Red de Área Amplia WAN (*Wide Area Network*): este tipo de red abarca una extensa área geográfica, por lo general un estado, país o continente. Un ejemplo muy claro de esta red es una empresa con sucursales en diferentes ciudades o países.

- Red de Área Metropolitana MAN (*Metropolitan Area Network*): es una red que cubre una gran ciudad o campus. Su alcance es de 10 a 50 kilómetros.

## 2.3 COMPONENTES DE UNA RED DE COMPUTADORAS

A partir de los conceptos de red de computadoras, usos y tipos, dados en los puntos anteriores, hablaré acerca de los componentes que las conforman:

### 2.3.1 Componentes en una red WAN

Para tratar sobre redes WAN pondré como ejemplo una empresa que tiene sucursales ubicadas en diferentes estados de la República Mexicana. Cada sucursal cuenta con un número de computadoras destinadas para el uso del personal que labora ahí. Cada una de estas máquinas recibe el nombre de *host*. La conexión entre estos hosts se le denomina subred. La subred tiene como función transportar la información de host a host. Las subredes a través de una línea de comunicación se conectan a un *switch*. Una línea de comunicación puede ser un cable UTP u ondas, es decir por *access point* (puntos de acceso inalámbricos, normalmente ubicados en el techo).

Un cable UTP es un cable de par trenzado no blindado. Es el cable más utilizado para establecer comunicación entre los equipos que conforman una red. Este cable cuenta con dos conductores eléctricos entrelazados, con la finalidad de evitar interferencias provocadas por medios externos. También se utiliza para conectar las computadoras de casa hacia el ISP proporcionado por el proveedor de internet.

Un *switch* es un dispositivo que conecta dos o más líneas de comunicación con la finalidad de que entre ellas se comparta información y haya comunicación entre sí. El switch recibe la información y la dirige hacia donde debe ser enviada. En un edificio o sucursal puede haber más de un switch, donde cada uno podría representar la red de un piso y/o de las diferentes áreas del corporativo.

El *router* es un dispositivo que se conecta al *switch* o *switches* que componen a la sucursal o al edificio, ya que es la cabeza de la red, debido a que es el dispositivo que hace posible que se tenga salida a internet porque va directamente conectado al *ISP* o equipo perteneciente al proveedor de servicio de internet. En la arquitectura de red de una empresa cada sucursal se representa con un *router*. Una red WAN está siendo representada por un *router*, por lo que, para este tipo de red se le da más énfasis a este dispositivo. Un ejemplo de lo que acabo de escribir se muestra en la figura 01:

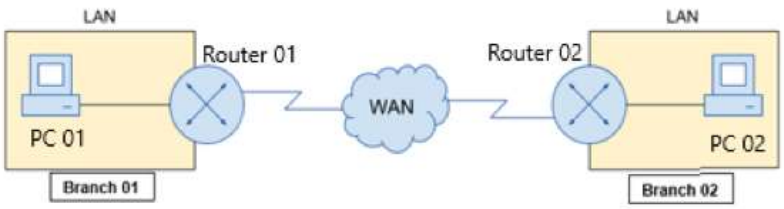



**Figura no. 01:** Red tipo WAN entre sucursales de una empresa

En la figura 01 se muestran dos oficinas, de lado izquierdo se tiene *Branch* 01 y de lado derecho *Branch* 02, donde cada una de las oficinas representa a diferentes sucursales de una empresa. En cada oficina se tiene una computadora conectada (PC) a un *router*, representando a una red LAN en cada oficina y a su vez esos dos *routers* se encuentran conectados entre sí. De esa forma las diferentes sucursales de una empresa se encuentran conectadas, representando a una red WAN.

Los *routers* tienen la capacidad de conectarse y compartir información entre sí a través de las conexiones WAN mencionadas en la figura 01. A su vez todos estos *routers*, además de conectarse a los *routers* de las sucursales también se conectan a uno o varios *routers* ubicados en la oficina central o matriz de la empresa.

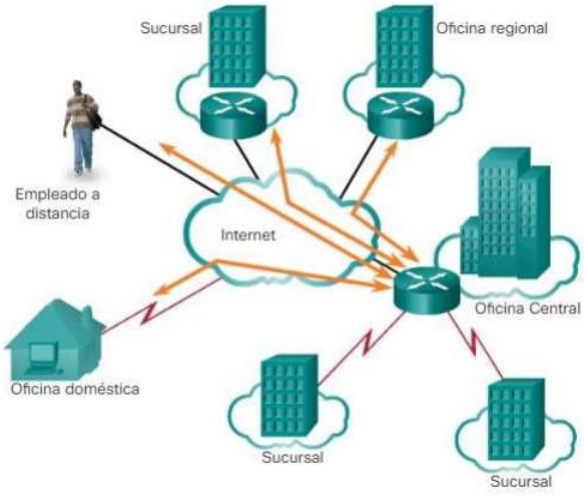



**Figura no. 02:** Conexiones de una red empresarial global

En la figura 02 se muestra que la oficina central tiene un *router*, el cual está conectado al *router* de la oficina regional, al de cada una de las sucursales u oficinas pequeñas y a la oficina doméstica. Ésta última hace referencia a la conexión que utiliza un empleado desde su casa para realizar *home office*.

### 2.3.2 Componentes en una red LAN

Como mencioné, el *router* es el único dispositivo de la red que va conectado al ISP o también conocido como equipo del proveedor del servicio de internet ISP (del inglés *Internet Service Provider*). Un ISP ofrece diversos servicios, donde cada uno está diseñado para diferentes tipos de clientes: casas habitación, negocios y grandes empresas. El servicio para grandes empresas transporta grandes cantidades de datos a altas velocidades de transmisión. El ISP o equipo del proveedor de internet que se tiene en el sitio es de tres tipos: uno es NTU (*Network Termination UNIT,* para medio de transmisión de cobre), la ONT (*Optical Network Teminal*, empleado para medio de transmisión de fibra óptica) y el demarcador (para medio de transmisión de carrier Ethernet, el cual transporta servicio de video, de datos, servicios en la nube de manera unificada para mercados empresariales y residenciales).

El *router* se conecta al *switch*. Un *switch* es un dispositivo que permite conectar varios dispositivos pertenecientes a una misma red pequeña con el objetivo de establecer comunicación entre sí. En una red LAN el *switch* es el dispositivo más importante, ya que es el dispositivo que encabeza a este tipo de redes.

La computadora personal o estación de trabajo es el medio que le permite al usuario interactuar con los servicios e información existente en la red a la que está conectada. Las computadoras personales van conectadas al *switch*, ya que éste es el que les proporciona el servicio de internet.

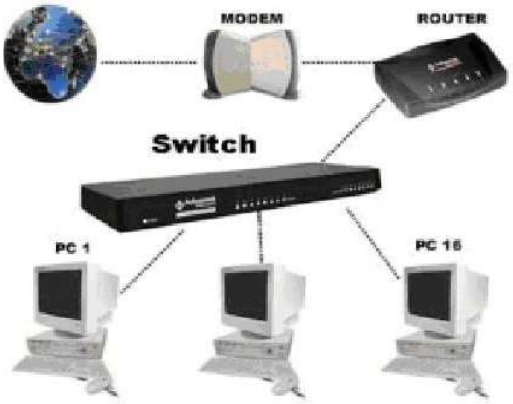



Figura no. 03: **Red LAN**

En la figura 03 se muestran tres computadoras personales conectadas a un *switch*, el cual se conecta al *router* que a su vez va conectado al ISP, a través del cual la red LAN accede a internet.

En las redes LAN también se cuenta con servidores. Un servidor es un conjunto de *hardware* y *software* que tiene como función devolver respuesta a las peticiones recibidas de los equipos conectados a la misma red. Por ejemplo, en una empresa se tiene el servidor de correo electrónico. Ese servidor de correo está preparado para procesar y recibir peticiones de todos los usuarios de la red como tal.

En las redes LAN es muy común también el uso de los puntos de acceso (*access points*), los cuales son equipos que crean una red inalámbrica a partir de una red alámbrica, para permitir la conexión entre dispositivos móviles y la red alámbrica. Estos dispositivos tienen el objetivo de hacer que la cobertura de red inalámbrica dentro de una oficina o edificio sea la mayor disponible eliminando puntos sin señal que pudieran existir dentro de este tipo de red. El uso de estos dispositivos es muy común sobre todo en oficinas grandes, debido a la gran cantidad de usuarios existentes en la red.

El *access point* funciona de tres formas: en modo maestro, repetidor y puente:

- En modo maestro múltiples usuarios utilizan el mismo *access point* como punto de acceso a la red al mismo tiempo;
- en el modo repetidor se extiende la señal de la red dentro de un área donde se puede acceder a un *access point* en modo maestro, para no perder el acceso a la red;
- en el modo puente se establece una conexión inalámbrica entre dos *access points,* donde la comunicación sólo existe entre estos. Se utiliza para comunicar zonas donde la instalación de cableado no es fácil o no resulta económica.

La forma en que un *access point* se conecta a un *switch* es a través de un cable UTP, ya que el *switch* es el dispositivo que integra al *access point* a la red en la que se encuentra configurado. Para los access point hay dos casos: conexión al switch a través de un *PoE.* Un *PoE (Power over Ethernet)* es un mecanismo que provee alimentación eléctrica sobre el mismo cable de red donde pasan los datos; y para *access point* que tienen dos conexiones, donde una va por cable UTP al switch y la otra va hacia el adaptador de corriente alterna (a través del cual se mantiene encendido). Dentro de mis actividades en la empresa se utiliza más la conexión por PoE.

En la figura 04 se muestra la forma en la que se hace la cobertura de un *access point* en un sitio.

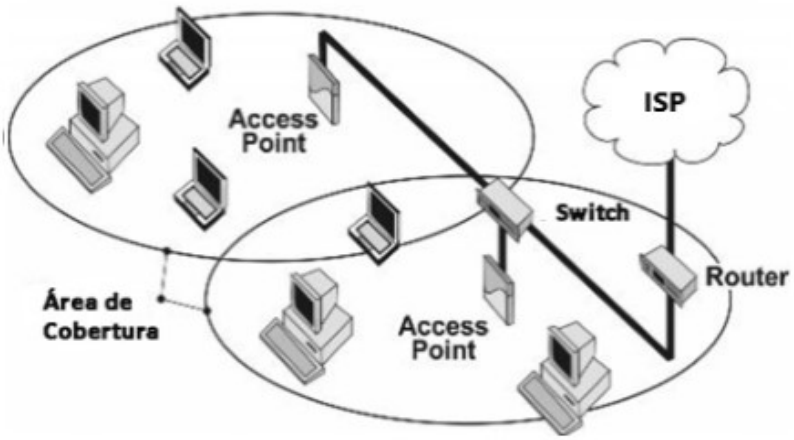



**Figura no. 04:** Redes inalámbricas

Del lado derecho de la figura 04, de arriba hacia abajo se observa la conexión del ISP hacia el switch (explicada anteriormente). Se observa que el *switch* tiene conectados dos *access points,* donde los círculos representan el área de cobertura que tiene cada uno de estos puntos de acceso.

Algunos clientes cuentan con dispositivos que tiene como función proporcionar energía eléctrica a todos los equipos que componen la red LAN, llamados UPS (*Uninterruptible Power Supply*) o Sistema de Fuerza Ininterrumpible, los cuales tienen como objetivo proteger los equipos que componen a una red LAN de variaciones de voltaje, descargas eléctricas y almacenar energía eléctrica para que los equipos continúen encendidos en caso de que en el sitio se tenga una falla en el suministro eléctrico. Estos equipos también son conocidos como banco de baterías.

## 2.4 CONEXIONES EN UNA RED WAN

Hoy en día, las empresas de comunicaciones que son proveedoras de servicios de redes WAN cuentan con un área que diseña y propone la infraestructura de redes WAN, utilizando enlaces privados, los cuales son: Enlaces IDE (Internet Directo Empresarial), WiFi, MPLS, satelitales, etcétera. Dentro de la infraestructura que propone el proveedor se encuentra el equipamiento para realizar la conectividad de esos enlaces WAN, entre los que se encuentran el *router*, *switch*, *access point*, equipo satelital o de microondas, etcétera, dependiendo de lo que el cliente desee, debido a que algunos cliente sólo requieren del equipo IPS y *router*. De igual forma se proponen los protocolos y tecnologías que cumplan los requerimientos de conectividad solicitados por el cliente.

Como ya mencioné, las redes LAN de una empresa deberán contar con la forma de comunicarse entre sí. Las redes WAN se utilizan para conectar redes LAN remotas, sin importar la ubicación geográfica que haya entre ellas, de hecho, este tipo de redes están diseñadas para dar cobertura a una ciudad, país o continente. El proveedor de servicios de internet es el propietario de las redes WAN, y las empresas, como usuarias de esos servicios deberán pagar cierta tarifa para hacer uso de estos enlaces.

Entre los proveedores de servicios WAN existe una red telefónica, televisión por cable, servicio satelital, etcétera. Estos proveedores proporcionan enlaces para que los sitios remotos puedan enviarse datos, video y voz.

Mientras las conexiones WAN le pertenecen al proveedor de servicios, las conexiones LAN le pertenecen a la empresa o al cliente. En las redes LAN se conectan computadoras, teléfonos u otros dispositivos que comparten un mismo espacio físico o área geográfica pequeña. El equipo perteneciente a la sucursal o al sitio del cliente es llamado equipo propietario del cliente (CPE).

Dentro de las redes WAN se encuentran los siguientes términos, los cuales ayudan a describir una conexión WAN:

- Equipo propietario del cliente (CPE): se refiere a todos cables internos y dispositivos ubicados en el perímetro empresarial, conectados a un enlace de una proveedora de servicios. El suscriptor es dueño del CPE o alquila este equipo al proveedor de servicios. El suscriptor es una empresa que utiliza los servicios WAN de un proveedor de servicios.

- Equipo de comunicación de datos (DCE): son los dispositivos que se utilizan para conseguir acceso a un enlace de comunicación en la red de datos WAN. Un ejemplo son los ISPs.

- Equipo terminal de datos (DTE): son los dispositivos que son la fuente o destino de la información. Puede ser un terminal, una impresora o un ordenador.

- Punto de demarcación o caja de conexiones de cables: Es la caja de conexiones del cableado, ubicada en las instalaciones del cliente, que conecta los cables del CPE a la red WAN del proveedor de servicios. El punto de demarcación es el lugar donde la responsabilidad de la conexión pasa del usuario al proveedor de servicios. Es aquí donde se determina si el problema es dentro de la instalación del cliente o del lado del proveedor de servicios.

- Oficina central (CO): es una instalación o edificio perteneciente al proveedor de servicios que conecta el CPE a la red del proveedor.

- Bucle local: cable de cobre o fibra óptica que conecta la red del cliente a la CO del proveedor de servicios. También se le conoce como la "última milla".

- Red interurbana: consta de líneas de comunicación, *switches*, *routers*, equipos de largo alcance y de fibra óptica dentro de la red o nube del proveedor de servicios WAN.

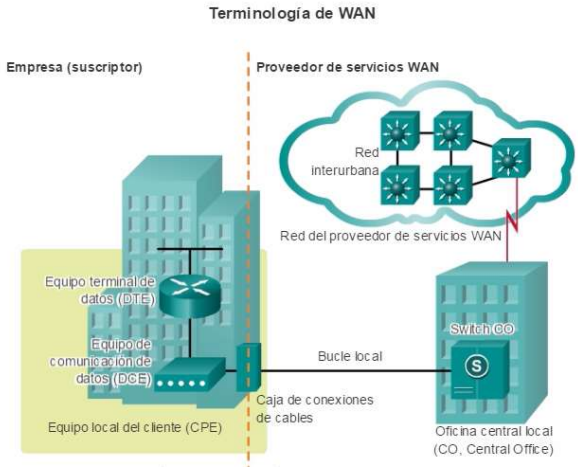



**Figura no. 05:** Componentes que describen la conexión en una red WAN.

En la figura 05 se observa la conexión WAN entre un sitio de cliente (ya sea oficina regional, central o, sucursal) y el proveedor de servicio de enlaces WAN. Del lado izquierdo de la línea punteada naranja se observa el CPE y del lado derecho el PE. Todo lo que suceda del lado izquierdo es responsabilidad del cliente mientras que, todo lo que suceda del lado derecho es responsabilidad del proveedor de servicios.

### 2.4.1 Red Privada Virtual

Explicaré la forma en la que una sucursal establece comunicación con la oficina central o matriz.

La conexión existente entre la oficina central y las sucursales de una empresa se establece a través de una red privada virtual VPN (del inglés *Virtual Private Network*), la cual es una conexión cifrada entre un dispositivo y una red. Esta conexión permite que los dispositivos que se encuentren en diversos espacios físicos operen como si estuvieran todos en la misma red local, lo que permite que los empleados ubicados en las diferentes sucursales tengan acceso a la misma red empresarial, estén donde estén. Por ello la VPN tiene gran aplicación en entornos corporativos.

En las VPN existe la conexión de sitio a sitio, la cual conecta la oficina central o corporativa con las oficinas de las sucursales. Se utiliza cuando la distancia hace que no sea viable hacer conexiones de red de manera directa entre estos puntos.


**Figura no. 06:** Conexiones VPN en la red de una empresa

En la figura 06 se observa que, el sitio central u oficina matriz está enlazada a través de una conexión VPN con las sucursales, con oficina regional y con los usuarios que a través del home office o trabajo en casa tienen conectividad a la red de la empresa.

### 2.4.2 Enlace IDE

Este enlace es una conexión directa al servicio de internet, que ofrece un servicio con velocidades de transmisión desde 4 hasta 1000 Mbps (megabits por segundo), donde el cliente únicamente requiere de un *router*. Este tipo de enlace tiene el mismo ancho de banda tanto de subida (*upload*) como de bajada (*download*).

Este enlace opera con el protocolo de BGP.

### 2.4.3 Enlace RPV

Es una Red Privada Virtual basada en tecnología MPLS (*Multiprotocol Label Switching*), producto de la evolución de las redes actuales, la cual permite ofrecer servicios diferenciados acordes a la calidad de servicios (*QoS*) que demandan las aplicaciones del cliente. Permite integrar en una sola red los servicios de voz, datos y video. La Calidad de Servicio (*QoS*) se refiere a la capacidad de proveer un mejor servicio dentro del tráfico de la red, lo que permite clasificar y priorizar el tráfico de la red para evitar pérdida de paquetes o degradación del servicio.

### 2.4.4 Enlace satelital

El internet satelital es una forma de llevar la conexión a internet a lugares a través de satélites que orbitan a baja altitud. Este sistema se compone de tres elementos: un *router*, una antena en tierra y el satélite emisor. La desventaja es que este tipo de conexión es la latencia, es decir, que los tiempos de respuesta para recibir los datos son altos, por lo tanto, los servicios de video llamada o de *streaming* no son los recomendables para este tipo de servicio. En zonas rurales urbanizadas donde existan servicios convencionales como los ya mencionados, la conexión satelital a internet se convierte en la mejor alternativa de comunicación en situaciones de emergencia o de desastres, puesto que no se verá afectada.

El HUB o estación terrena es el encargado de dirigir todo el tráfico de todas las terminales remotas hacia internet, el cual es recibido por el satélite. Es la puerta de salida hacia el mundo de toda la comunicación. Este *hub* se encuentra en las instalaciones del proveedor de enlaces satelitales. En la figura 07 se muestra cómo es una conexión a internet satelital.

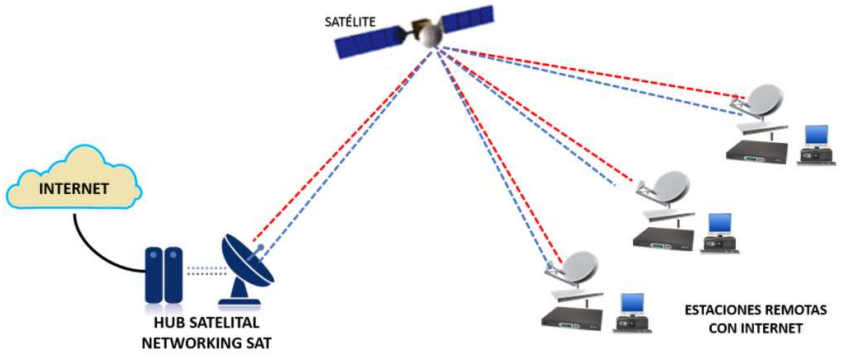



**Figura no. 07:** Red satelital

El internet satelital es el más utilizado por las empresas, donde el *hub* se encuentra en la oficina central del proveedor mientras que las estaciones remotas se encuentran en las sucursales del cliente que tenga contratado este tipo de enlace.

## 2.5 MEDIOS DE TRANSMISIÓN

Un medio de transmisión es un canal que permite el envío y recepción de datos de un punto origen a un punto destino dentro de una red.

Se distinguen dos tipos de medios de transmisión:

- Guiados: son los componentes tangibles por los cuales viaja la información. Ejemplos: cobre, fibra óptica, cable UTP, entre otros.

  a) cobre: es un medio adecuado para señales de voz. Su ancho de banda puede llegar a transmitir 500 MHz en tan solo 100 metros. Transmite hasta 100 Mb, sin embargo este medio de transmisión presenta mayor atenuación y pérdidas de señal. Los electrones en el cobre viajan a menos del 1% de la velocidad de la luz. La limitación de distancia es de 2000 metros. Este medio es más sensible a factores ambientales como la temperatura y las interferencias electromagnéticas.

  b) fibra óptica: su rendimiento llega a ser de hasta 10 Gbps (10000 Mbps). Su ancho de banda es de hasta 1000 veces mayor que el cobre y su alcance es de hasta 100 veces más lejanas. La fibra óptica transmite información en forma de luz y alcanza velocidades de hasta 200 000 km/h. El cable de fibra óptica es menos susceptible a factores ambientales que el de cobre. Por ejemplo, el cobre degrada su calidad de transmisión en un tramo de 2 kilómetros mientras que un cable de fibra óptica mantiene una transmisión altamente fiable. Además, la fibra también es más resistente a factores ambientales como la temperatura, fauna e interferencias electromagnéticas, lo que ayuda a evitar la degradación del servicio de internet. Las fibras ópticas se instalan de forma aérea, subterránea y en cables submarinos intercontinentales.

- No guiados: son los que realizan la transmisión de datos a través de aire, debido a que se utilizan las ondas electromagnéticas para la misma. Ejemplo: red satelital.

  Red satelital: Es una red de internet donde su método de conexión a Internet es mediante ondas electromagnéticas, utilizando como medio de comunicación un satélite y una estación terrena o remota. Es un sistema de acceso muy recomendable en aquellos lugares donde no hay cobertura o infraestructura para tipos de conexión tradicional como la celular 3G, 4G o 5G. Hoy en día, existen alternativas de conexión que resuelven el problema de tener que instalar infraestructura complejas y costosa, como por ejemplo, el Internet de microondas y el Internet satelital.

Las microondas son un método de transmisión de datos que se realiza a través de ondas de radio electromagnéticas que utilizan las frecuencias de 2,5 a 5,8 GHz. Se instalan antenas que sólo hacen conexión entre ellas sin que la misma se vea afectada por objetos que podrían obstaculizarla, como por ejemplo: construcciones grandes, flora o condiciones de clima. De esta forma se conectan lugares retirados con una alta velocidad, utilizando una transmisión de datos simétrica. Su ventaja es que permite una conexión rápida y no es necesaria la instalación telefónica.

## 2.6 PROTOCOLOS DE RED EN LOS ENLACES WAN

Los protocolos de red con los que trabajan estos enlaces son: BGP y OSPF

- BGP (*Border* Gateway *Protocol*, Puerta de enlace de frontera): es el protocolo que se utiliza para intercambiar información entre los diferentes proveedores de servicios registrados en internet. Ese intercambio de información se realiza utilizando la ruta más corta, lo que hace que la comunicación sea rápida.

BGP permite mostrar información de ruteo entre 2 *routers*. Ambos *routers* deben tener establecida una sesión BGP entre ambos, y así es como se determina que son vecinos. La sesión BGP se basa en el establecimiento previo de una conexión TCP. El tipo de relación BGP entre ambos está determinada por el sistema autónomo al cual pertenece cada uno de ellos Cada *router* es capaz de tomar decisiones sobre la información de ruteo recibida. Estas decisiones definen, a su vez, la información de ruteo que van a anunciar.

- *Idle*: se envía el inicio de una sesión TCP, escucha la inicialización de una sesión TCP y pasa al estado *Connect*

- *Connect*/*Active*: Estados relacionados con el progreso del establecimiento de la sesión TCP. Indica que un enlace se encuentra fuera de servicio.

- Open *Sent* Luego del establecimiento de la sesión TCP, se envía un mensaje BGP Open. Espera el mensaje BGP Open del vecino.

- Open *Confirm* Se recibe (sin errores) el mensaje BGP Open del vecino. Se envía un *keepalive* y si se recibe un *keepalive* del otro extremo se *transiciona* al estado *Established*

- Established Conexión BGP completamente establecida (*full*). Los vecinos (*peers* o *neighbors*) están en condiciones de intercambiar información de ruteo.

OSPF (Open *Shortest Path First*): los *routers* implementan un algoritmo llamado SPF (*shortest path first*) para escoger la mejor ruta. Tiene la capacidad de operar con redes de tamaño pequeño y grandes redes, facilitando la escalabilidad. SPF se caracteriza por agrupar los diferentes costos que se encuentran en las rutas para alcanzar el destino. Una vez establecidas las rutas, OSPF se encarga de guardarlas en la de enrutamiento para un posterior uso. Se calcula dividiendo el ancho de banda de referencia (100 Mbps por defecto) entre el ancho de banda de la interfaz donde está configurado el protocolo. La mejor ruta es el costo más bajo.

## 2.7 COMUNICACIÓN CON LA NUBE DE PROVEEDOR

Al hablar de este término me refiero al conjunto de *routers* pertenecientes al proveedor (PE), donde cada uno tiene configurado un gran número de enlaces o servicios en sus interfaces lógicas. Para acceder a estos equipos se logra a través de tres servidores: uno donde se tienen enlaces IDE, otro donde se tienen enlaces RPV y otro donde se accede a la nube de *routers* mencionada. Desde un NOC es posible acceder a todo este conjunto de *routers* y buscar un enlace WAN que se desea gestionar.

El personal del NOC (o entidad que gestiona las redes de diversos clientes) accede a una herramienta que se comunica a través del protocolo *secure Shell* hacia un servidor TACACS que se tiene en el nodo donde se encuentran físicamente los *routers* de la nube. En el servidor se tiene un *Active Directory* que tiene almacenados los datos de las personas autorizadas al acceso a la nube. La conexión SSH va encriptada de principio a fin, donde sólo ambas puntas tienen la llave para des encriptar la información y esta información viaja por la red pública de internet.

Una vez que se haya validado por TACACS este acceso entonces se manda una solicitud al servidor donde se encuentra el PE al que se quiere entrar.

## 2.8 APLICACIONES DE LAS REDES DE COMPUTADORAS

La tecnología ha tenido una gran influencia en la manera en que funciona el mundo, desde la forma en que la humanidad realiza sus actividades diarias, en la de comunicarse y hasta en la forma en la que trabajan las grandes empresas. Sin duda las redes de computadoras tienen muchas aplicaciones, pero para fines de este trabajo escrito trataré únicamente sobre las aplicaciones de las redes de computadoras en las redes empresariales.

### 2.8.1 Redes empresariales

Para entender mejor el concepto de una red empresarial iniciaré con el concepto de qué es una empresa:

- **Concepto de empresa:** Una empresa es un sistema social integrado por un conjunto de personas y medios con los que se consiguen unos objetivos. El logro eficaz de esos objetivos se da a través de una organización que coordine todos los medios y personas que formen parte de esta. Es, a su vez un lugar o medio en el que se desarrolla una parte importante de la vida de las personas que aportan su trabajo a la misma. La integración de un trabajador a la empresa comienza a partir de que éste consigue un puesto de trabajo dentro de la misma ya que a partir de ese momento se le exige al trabajador cumplir con su responsabilidad asignada.

Esa integración se da cuando el trabajador asume de manera responsable el cargo que se le asignó con sus subordinados, la relación con sus superiores, cuando empieza a conocer tanto su función en su puesto de trabajo como la cultura de la empresa.

- **Concepto de red empresarial:** Es un mecanismo de cooperación entre empresas pequeñas, medianas y grandes, donde la empresa participante, manteniendo su independencia jurídica, autonomía gerencial y su giro decide voluntariamente participar en un esfuerzo conjunto con otras para la búsqueda de un objetivo común.

### 2.8.2 La influencia de las nuevas tecnologías en las empresas

El uso y demanda de las redes sociales, los teléfonos inteligentes, el almacenamiento de la información en la nube, son algunos aspectos de cómo las nuevas tecnologías han impactado en el día a día en las empresas, ya que han cambiado la forma en que las mismas han estado operando.
Algunos aspectos que más se han visto transformados con las nuevas tecnologías son los siguientes:

- Relación con el cliente: el uso de las redes sociales brinda una mayor rapidez y formas para contactar al cliente al momento de resolver problemas urgentes o que requieran una solución inmediata. Por ejemplo: *Whats App, Skype*, video llamadas, videoconferencias, entre otras.

- Internacionalización: La expansión de internet y la difusión de las empresas a través de las redes sociales ha permitido que las empresas puedan darse a conocer incluso en otros países.

- Productividad: El almacenamiento de información en la nube o en servidores virtuales ha facilitado el proceso de trabajo y ha hecho que las empresas alcancen incluso mayores niveles de productividad en todos sus ámbitos.

- Conciliación: Gracias al acceso remoto el personal de la empresa tiene posibilidad de trabajar desde casa utilizando sus herramientas de trabajo sin problemas (como si estuvieran físicamente en la oficina), adaptando esta modalidad de trabajo a las necesidades del empleado. Este modo de trabajo ha sido muy acentuado en los últimos años.

- Competitividad: El uso de nuevas tecnologías ha hecho que las empresas vendan productos o servicios más innovadores, haciéndolas competentes en el mercado, por lo que si no adaptan esas nuevas tecnologías se quedan incluso estancadas, ya que, todo cliente de una empresa (sin importar su giro) es atraído precisamente por la innovación que la misma le ofrece.

Las nuevas tecnologías en las empresas tienen muchas ventajas, pero por ello existen retos a considerar, las cuales se mencionan las siguientes:

- Inversión: la integración de los avances tecnológicos a los procesos empresariales implica una inversión inicial grande. Como la tecnología se encuentra en cambio constante la empresa debe considerar un plan de ahorro para no dejar de contar con esas innovaciones, desde licencias de *software* hasta nuevo *hardware*.

- Dependencia: Supone la paralización de la empresa, ya que hoy en día toda empresa funciona a través de internet, por lo que es importante que cualquier falla en las nuevas tecnologías sea resuelta a la brevedad posible. Por ello en todas las empresas se cuenta con un área de TI (tecnologías de la información), donde se resuelven estas problemáticas

- Tiempo en formación a los empleados: los avances tecnológicos contribuyen a que el trabajador conozca los procesos de manera rápida. Cada área de trabajo cambia sus procesos de manera constante, y ello requiere capacitaciones constantes en el uso de aplicativos, cambios en la manipulación de información, renovación de credenciales de acceso a la información cada determinado periodo de tiempo, etcétera.

# CAPÍTULO 3.

# ACTIVIDADES DE MI PUESTO DE TRABAJO

Mi trayectoria laboral dentro de la empresa inició el día 25 de enero del 2016. Dentro de la empresa estoy desempeñando la función de Operador Multiplataforma, Gestión y Soporte, en el centro de operaciones de redes empresariales. En otras palabras, desempeño labores dentro de un NOC (*Network Operation Center*). El centro cuenta con dos sedes: una en la Ciudad de México y otra en el estado de Querétaro. En ambas sedes el horario laboral es de 24 horas los 7 días de la semana los 365 días del año. Los turnos laborales son: matutino, vespertino y nocturno.

La función principal del NOC es prevenir problemas en la red de sus clientes, y entre sus funciones podemos enumerar las siguientes:

- Monitoreo de la red.
- Asignar y coordinar ingenieros para la resolución de los diferentes problemas en las redes de los clientes.
- Dar seguimiento a incidentes.
- Proporcionar reportes al cliente para mantenerlo informado sobre el estatus de los eventos que acontezcan en su red.
- Automatizar procedimientos de recuperación posteriores a las incidencias.
- Supervisar el buen funcionamiento de elementos de la red como servidores, *routers*, *switches*, etcétera.

Se gestionan alrededor de 100,000 servicios en el NOC, el cual se divide en las siguientes áreas:

- **Operaciones Nacionales:** atención a incidentes y soporte remoto para clientes nacionales, tanto de la Ciudad de México como de todo el interior de la República.
- **Operaciones Internacionales:** atención a incidentes y soporte remoto para clientes internacionales, de países como Estados Unidos de América y Brasil, principalmente.
- **Altas, Bajas y Cambios**: Se encarga de alta, baja y cambios o modificaciones de servicios o enlaces de los diferentes clientes en la base de datos de la empresa, conocida como CMDB.
- **Soporte segundo nivel**: Se encargan de realizar el soporte cuando se trate de problemas más complejos, es decir, cuando el área de Operación ya hizo hasta su último esfuerzo para determinar el diagnóstico y solución de una falla, por ejemplo.
- **Voz**: Solución y gestión de problemas de telefonía hacia los diferentes clientes que gestiona el centro de monitoreo.
- **Herramientas**: se encarga de darle soporte técnico a los aplicativos que el personal del centro de monitoreo utiliza para llevar a cabo las actividades correspondientes.
- **Entrega de servicio**: Se encarga de la gestión de la documentación, cierre, entrega y análisis de los incidentes que se atienden día a día en el centro de monitoreo.
- **Ingeniería de campo**: Es el área que gestiona al personal requerido para acudir a los sitios de los clientes a revisar los servicios.

En mi caso, me encuentro dentro del área de Operación Nacional. En esta área se atienden únicamente a clientes de México. Los clientes se dividen, de acuerdo con su giro en varios sectores:

- **Gobierno**: entidades gubernamentales
- **Financiero**: entidades bancarias y financieras
- **Industrial**: fábricas
- **Servicios**: tiendas de autoservicio y departamentales, universidades

Para cada sector se tiene un determinado grupo de ingenieros que gestionan los diferentes clientes que componen a estos sectores. En mi caso me encuentro dentro del sector Gobierno.

Toda red gestionada por el NOC se divide en dos partes: red LAN (red del cliente) y red WAN (red de Teléfonos Mexicanos).

- **Red LAN**: Las redes de los clientes se componen de: oficinas matrices y sucursales. Cada red de cliente (la mayoría de estas redes) tienen sedes o sucursales distribuidas en toda la República Mexicana, mientras que algunas redes se distribuyen únicamente en la Ciudad de México o el algún estado de la República Mexicana específicamente, por ejemplo: Gobierno Puebla, es una red que se encuentra instalada únicamente en el estado de Puebla. Cada sucursal cuenta con una red de datos que se compone de uno o más de los siguientes dispositivos de red (vistos en el capítulo dos): *router*, *switch*, *access point* un equipo del ISP, que en este caso pertenece a Teléfonos Mexicanos.

  El número de dispositivos que componen la red del cliente depende de la magnitud de esta en cada sucursal, ya que, en algunas sucursales, sobre todo en las oficinas centrales o matrices se tienen hasta 6 *routers*, 5 *switches* en cada piso, etcétera.

  La red de cada cliente se compone de forma diferente, por lo que, para algunos clientes, de parte del centro de monitoreo se administra únicamente el *router* y se gestiona el ISP, mientras que para otros clientes se administran todos los dispositivos mencionados anteriormente, pero eso depende del contrato que se tenga con cada cliente, de lo cual se encarga el área comercial o administrativa.

**Red WAN:** Todos los clientes pertenecientes al NOC cuentan con el servicio de internet contratado con Teléfonos Mexicanos. Como parte de mis funciones en mi puesto de trabajo se tiene el evaluar el servicio del cliente concentrado en la infraestructura de Teléfonos Mexicanos.

La infraestructura de Teléfonos Mexicanos contratada por cada cliente se divide en dos partes: planta exterior y planta interior:

a) La planta exterior es el conjunto de elementos que enlazan a la red de un cliente con la central telefónica de Teléfonos Mexicanos. La planta externa se clasifica en aérea y subterránea.
b) La planta interior es el conjunto de equipos ubicados dentro de la central telefónica y las conexiones entre centrales telefónicas.

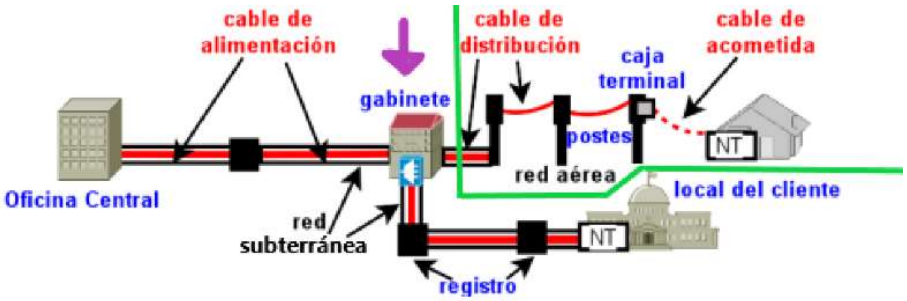



**Figura no. 08:** Red de planta externa

En la figura 08 se muestran los elementos que componen a una red de planta exterior. Los componentes que se encuentran por arriba de la línea verde componen a la red aérea mientras que lo que está por debajo de la línea verde es la red subterránea.

- Acometida: es la conexión que va desde el ISP (NT) del cliente hacia la caja terminal, perteneciente a Teléfonos Mexicanos. Estas cajas se encuentran instaladas en los postes.
- Caja terminal: es una caja que permite la conexión entre la acometida y el gabinete.
- Cableado aéreo o cable de distribución: es aquel conjunto de cables que cuelga de los postes.
- Gabinete: es una caja grande donde se encuentran conectados los servicios desde la red aérea o subterránea con la central de Teléfonos Mexicanos, oficina central o central de Teléfonos Mexicanos.
- Registros: son cajas subterráneas que conectan la red del cliente saliente de la NT con el gabinete.
- Cables de alimentación: conectan al gabinete con la central.

La mayoría de los clientes gestionados por el centro de monitoreo cuentan con sucursales distribuidas en toda la República Mexicana, lo que significa que la red de Teléfonos Mexicanos es amplia. Para la atención de la red a nivel ISP Teléfonos Mexicanos cuenta con 10 Centros de Atención, donde cada centro es el responsable de atender las fallas de la red de Teléfonos Mexicanos reportadas en ciertos estados y regiones del país:

- Metropolitano 1: Ciudad de México (clientes premier), Estado de México, Guerrero, Cuernavaca
- Metropolitano 2: Ciudad de México, Estado de México, Guerrero, Cuernavaca
- Monterrey: Nuevo León, Zacatecas, Tamaulipas, Aguascalientes, San Luis Potosí
- Querétaro: Querétaro, Guanajuato, Michoacán
- Puebla: Puebla, Tlaxcala, Veracruz, Hidalgo
- Guadalajara: Jalisco, Colima, Nayarit
- Hermosillo: Sinaloa, Sonora, Baja California Sur
- Chihuahua: Chihuahua, Coahuila
- Mérida: Oaxaca, Yucatán, Campeche, Chiapas, Quintana Roo, Tabasco
- NORTE: Baja California Norte

Cada oficina, sucursal, y sitio de los clientes gestionados por el centro de monitoreo cuenta tanto con esa infraestructura externa (red de planta exterior) como con equipo interno instalado en el sitio del cliente, por ejemplo el ISP .

## 3.1 FUNCIONES COMO INGENIERA DE NOC

Como Operador Multiplataforma, Gestión y Soporte mi propósito es diagnosticar y solucionar los incidentes que se presentan en las redes de los clientes a través del monitoreo, el cual se realiza con las herramientas de gestión, análisis de los incidentes, detección de las causas que provocan las afectaciones y de la determinación de una acción correctiva para la falla o incidente detectado, con la finalidad de garantizar la disponibilidad y desempeño de las redes de los clientes del NOC. La infraestructura, herramientas y personal que demanda la gestión de las redes para algunas empresas suele ser muy costoso y por ello recurren a la prestación de este servicio por un tercero, en este caso, un NOC.

El personal que labora en el NOC debe tener el conocimiento sobre la forma en que se componen las redes y experiencia necesaria sobre la solución a fallas (experiencia laboral previa en otros NOC), para de esta manera solventar rápidamente cualquier incidente que se llegase a presentar. Aunado a ello, se debe contar con una herramienta adicional para la bitácora y seguimiento, es decir, una forma de realizar un documento donde se describa a detalle la forma en la que son resueltas las fallas. Con esto último me refiero a un reporte o incidente.

### 3.1.1 Competencias específicas

Como Operador Multiplataforma, Gestión y Soporte es importante contar con la alta capacidad de resolver problemas técnicos. Durante la carrera de Ingeniería, el estudiante se capacita en dar soluciones a los problemas prácticos a través de la teoría. En este puesto de trabajo, al tratarse de la operación de redes de comunicaciones es importante que el empleado cuente con los conocimientos básicos de redes de computadoras, para que al momento de tener que dar soluciones a los problemas técnicos lo haga determinando un diagnóstico a partir de esos conocimientos, tomando en cuenta que se está trabajando sobre redes en producción, por lo que e4s importante saber dar una buena solución para que la red del cliente tenga las menos afectaciones posibles.

Para una empresa que presta su servicio a otras es importante llevar a cabo buenas prácticas para gestionar las operaciones de los servicios de TI (Tecnologías de la Información), es decir, asegurar una gestión eficaz de sus procesos y garantizar una buena experiencia a los clientes. Es importante que el aspirante al puesto de trabajo tenga conocimiento básico sobre ITIL, el cual es un conjunto de conceptos y mejores prácticas para la gestión de servicios que describen funciones y procesos para ayudar a una organización a lograr gestionar de manera adecuada los servicios de TI.

En la tabla 01se muestran los conocimientos que demanda el puesto para cumplir con su propósito. En la columna nivel de dominio se indica el conocimiento específico de acuerdo con la escala mostrada en la tabla 01:

C = Comprensión: Entendimiento de los conceptos del área de conocimiento.

A = Aplicación: Hacer uso de los conocimientos al desempeñar el puesto.

E = Evaluación: Se refiere al conocimiento teórico y práctico valorado para proponer soluciones.

**Tabla 01**: Competencias dentro del puesto de trabajo

| Área de conocimiento | Especificación | Nivel de dominio |
|---|---|---|
| Administración de sistemas de gestión | Atención a fallas (proceso de solución a una afectación presente en la red de un cliente, de principio a fin) | E |
| | Configuración (cambios requeridos por el cliente en su red) | E |
| | Mantenimiento (mejoras y correcciones en la red de un cliente) | E |
| Hardware | Atención a fallas (determinar el diagnóstico de causa de afectación en equipos administrados por el NOC en la red del cliente) | E |
| | Configuraciones (cambios realizados en la red de un cliente para resolver una falla, tanto en equipos administrados por el NOC) | E |
| | Mantenimiento y gestión de equipos adminsitrados por el NOC | E |
| Redes de computadoras | Dispositivos de red (*switch*, *router*, *access point*, | A, C |
| | Enrutamiento *(routing)* | A, C |
| | Protocolos de red BGP, OSPF, EIGRP | A, C |

Se requiere personal con experiencia en otros NOC o en centros de operación de redes empresariales y con certificación de HCNA (de Huawei), CTN (*Certificación Teldat Networking*, de Teldat), ACSA (Aruba *Certified Switching Associate*, de Aruba) o CCNA R and S (*Cisco Certified Network Associate Routing and Switching*, de Cisco). Cabe destacar

que aproximadamente el 75% de los dispositivos administrados por el NOC son de la marca Cisco.

También es requerida la certificación de ITIL en cualquiera de sus niveles: *Foundation, Practitioner o Master.*

Cada año, por parte del NOC se aplican exámenes de conocimientos en redes, para a partir de ahí determinar los cursos de preparación que deberá tomar el personal que labora en el NOC.

### 3.1.2 Gestión de incidentes como base de mis actividades laborales

La gestión de incidentes es la base de las actividades diarias dentro del NOC. Permite mantener y garantizar el buen funcionamiento de una red. Es el proceso responsable de resolver los eventos de falla presentes en la red de los clientes. Una falla es un suceso que interfiere en el buen funcionamiento y rendimiento de una red. Los eventos de falla que se presentan en una red son los siguientes:

- Pérdida de conectividad, donde un enlace que corresponde a una oficina central o sitio del cliente se queda fuera de servicio. En otras palabras, se tiene un nodo aislado o incomunicado.
- Saturación de enlace (alto consumo de ancho de banda de una red)
- Degradación o intermitencia en una red
- Afectación en la operación de un equipo perteneciente a la red del cliente, ya sea en un *router*, un *switch*, un *access point,* un UPS.

La meta de la gestión de incidentes es que las fallas se atiendan conforme a las severidades definidas (o clasificaciones) de los servicios establecidas por el centro de monitoreo, donde la severidad alta consiste en que la falla sea resuelta en el menor tiempo posible. La severidad refleja el estado de afectación del negocio del cliente.

Las severidades se establecen de la forma en que son mostradas en la tabla 02:

| **Tabla 02**: Tipos de severidad de afectación en la red de un cliente | |
|---|---|
| **Severidad** | **Criterios** |
| 1 Alta | Aplica cuando se tiene un nodo o sitio aislado, es decir, incomunicado. Ejemplo: una oficina central, un sitio de suma importancia para el cliente. |
| 2 Media | Aplica para un sitio que cuenta con un enlace principal y uno de respaldo, donde uno de los dos está fuera de servicio y el otro está operando. |
| 3 Baja | Aplica para enlaces que no estén fuera de servicio, pero que presenten degradación o para dispositivos que no afecten de forma considerable a la red de un sitio. Esta severidad aplica para *switches* que cubren un área muy pequeña dentro de un sitio, *access points* |

En el centro de monitoreo se gestionan las redes de diversos clientes. Cada red de cada cliente es muy diferente, por lo que, la composición de cada red es algo que siempre se debe de tomar en cuenta al momento de resolver fallas, ya que, entre mejor se conozca la red de un cliente es más fácil la solución rápida a las fallas.

En el centro de monitoreo hay una herramienta llamada *Incident Manager*, la cual nos ayuda a realizar la gestión de incidentes para todos los servicios gestionados por el NOC. Esta herramienta monitorea cada dispositivo de las redes de los clientes que se encuentran bajo la gestión del centro de monitoreo a través del protocolo SNMP (*Simple Network Management Protocol* o en español, Protocolo Simple de Administración de Redes).

En mi caso, al gestionar clientes de Gobierno, el *Incident Manager* me permite hacer la gestión de todos los servicios pertenecientes a los clientes mencionados anteriormente. Para tener acceso a esta herramienta se debe contar con un acceso y contraseña asignados por el área de herramientas.
La contraseña de acceso deberá cambiarse cada tres meses y es de uso personal, es decir, cada operador debe contar con sus propias credenciales de acceso. Una vez se haya ingresado a la herramienta nos encontramos habilitados para realizar el proceso de gestión de incidentes: inicio, seguimiento y cierre de los reportes.

De acuerdo con la forma en que los clientes del NOC están clasificados (por su giro) se tiene a un grupo destinado de personas para gestionar a cada sector. Por ejemplo, cierto grupo de personas responsables de gestionar las redes del sector Gobierno, otro grupo de personas para gestionar las redes del sector Financiero, etc. En mi caso, al encontrarme dentro del grupo de personas que gestionan las redes de Gobierno contamos con un perfil de usuario configurado dentro de la herramienta del *Incident Manager*, para que al momento de que se presente afectación en algún componente de las redes que gestionamos seamos los responsables del inicio, seguimiento y cierre de los reportes correspondientes a las redes de los clientes. Estos perfiles se guardan dentro de la base de datos del *Incident Manager.*

En el *Incident Manager* los reportes se generan de manera automática al momento de que un dispositivo perteneciente a las redes gestionadas presente alguna de las afectaciones mencionadas anteriormente. Los reportes se generan por cada dispositivo que compone una red, por ejemplo, si el sitio de un cliente se compone de un *router* y un *switch* y ambos dispositivos quedaron incomunicados se generaría un reporte para el *router* y otro para el *switch*. En el momento en que se genera un reporte de manera automática el *Incident Manager* verifica qué dispositivo se alarmó (o presentó afectación) y a qué cliente le pertenece. Una vez que la herramienta identificó al cliente verifica si los operadores que tienen configurado el perfil para gestionar a ese cliente se encuentran con sesión iniciada dentro de la herramienta y al ver que efectivamente los operadores se encuentran disponibles le asigna de manera automática el o los reportes generados a uno de ellos.

Cada reporte generado en el *Incident Manager* contiene una breve descripción sobre la falla que está presentando el dispositivo, lo que da una primera idea sobre el tipo de falla a enfrentar. El proceso para trabajar los reportes es llamado gestión de incidentes.

La gestión de incidentes se lleva a cabo a través de las siguientes fases:

1) Inicio y registro de incidente: Es el momento en que se genera un reporte por el *Incident Manager,* el cual contiene la hora y fecha en que se generó la falla, el identificador o número de reporte, nombre del cliente y del sitio donde se encuentra el servicio afectado, al igual que el dispositivo que presentó la falla. Dentro del reporte hay un campo donde viene la IP WAN con la que un enlace de un sitio o la IP con la que un *switch*, *access point* o servidor está configurado. Aunado a todo esto el reporte contiene un campo que describe la falla que está presentando el servicio afectado.

2) Análisis y verificación: aquí se comprueba que efectivamente la descripción de la afectación coincida con la que está presentando el servicio, ya que en algunos momentos puede diferir, lo que implica dar un seguimiento inadecuado al problema, y a partir de la identificación de la falla verificar qué tanto impacta esa falla dentro de la red.

3) Comunicación con el cliente: se establece llamada telefónica o conversación vía *Whats App* con el cliente, para notificarle la falla que se ha presentado en su red

4) Investigación y diagnóstico: se investiga cuál o cuáles son las causas que estarían ocasionando la afectación del servicio para determinar un diagnóstico.

5) Solución: A partir del diagnóstico hecho se realizan acciones correctivas para restablecer la operación de la red o del servicio.

6) Validación y cierre: Se verifica con el cliente que la falla ha sido resuelta y se obtiene su visto bueno para finalizar la atención al reporte y efectuar su cierre. En ocasiones no es posible obtener el visto bueno del cliente, pero se puede validar que la falla ya no esté presente, a través de pruebas o de las herramientas que utilizamos para gestionar los servicios.

Independientemente de la falla a la que le estemos dando atención, la gestión de incidentes debe llevarse a cabo a través de las fases mencionadas, para el cumplimiento de la función principal del NOC.

Para llevar a cabo la gestión de incidentes en el NOC se cuenta con herramientas que nos permiten trabajar adecuadamente cada fase.

### 3.1.3 Herramientas de gestión de incidentes

Como ya se mencionó, el *Incident Manager* es la herramienta a través de la cual se realiza el proceso de gestión de incidentes, ya que en ella es donde se procesan los reportes correspondientes a las fallas presentes en las redes de los clientes.

El reporte es el documento electrónico donde se escribe todo el proceso llevado a cabo para detectar, diagnosticar y solucionar la falla.

Cada sitio o sucursal de cada cliente tiene un identificador de sitio (o *site ID*), el cual sirve para hacer referencia a un sitio de todos los demás que son gestionados por el NOC. Por ejemplo, la red de Farmacias Hernández cuenta con una sucursal en Cancún (donde se tiene un *site* ID01), otra en Hermosillo (*site* ID02) y otra en Guadalajara (*site* ID03), y así para cada una de las sucursales de Farmacias Hernández y de cada cliente del NOC. Esto informa que, para el ejemplo de Farmacias Hernández Cancún (*site* ID01) todos los dispositivos que se tengan gestionados por parte del NOC para Farmacias Hernández Cancún tendrán el *site* ID01, es decir, si para ese sitio se tiene un *router*, un *switch* y un *access point* estos componentes compartirán el mismo *site* ID01 dentro del *Incident Manager.* Esto ayuda a llevar un control del total de sitios y componentes gestionados para cada cliente.

En la figura 09 se muestran las partes de un reporte generado por el *Incident Manager*. Se observa que en el reporte viene los datos que hacen referencia al sitio que se está revisando: siteID, referencia (identificador de enlace), dirección IP, número de reporte, descripción del problema presente en el sitio, entre otros.)

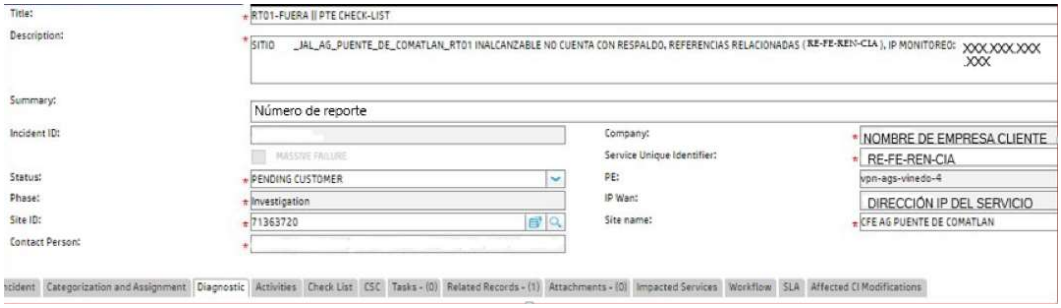



**Figura 09:** Partes de un reporte del *Incident Manager*

Para visualizar todos los componentes que conforman a un sitio del cliente sólo basta con hacer la búsqueda dentro del mismo *Incident Manager*, ya sea utilizando el nombre del cliente y del sitio o el *site* ID, aunque este segundo caso es el más práctico. El *Incident Manager* nos muestra todos los componentes que se encuentran dentro del sitio del cliente correspondiente al *site* ID que colocamos en el campo de búsqueda. Es decir, nos muestra el o los *routers*, *switch*, *access point* y todo el equipo localizado en el sitio. Para cada equipo se muestra el número de serie, marca, IP, los enlaces (referencias) con la o con las que cuenta el sitio y el ancho de banda de cada enlace. Hay sitios que cuentan con únicamente un enlace (mostrado como *circuit*) mientras que otros cuentan con 2, 3 o 4, dependiendo de la red de cada cliente.

En la figura 10 se muestra la forma en que se visualizan los componentes de un sitio (o sucursal del cliente) cuando en el *Incident Manager* se hace la búsqueda de determinado sitio de manera que se muestren los dispositivos que lo componen:

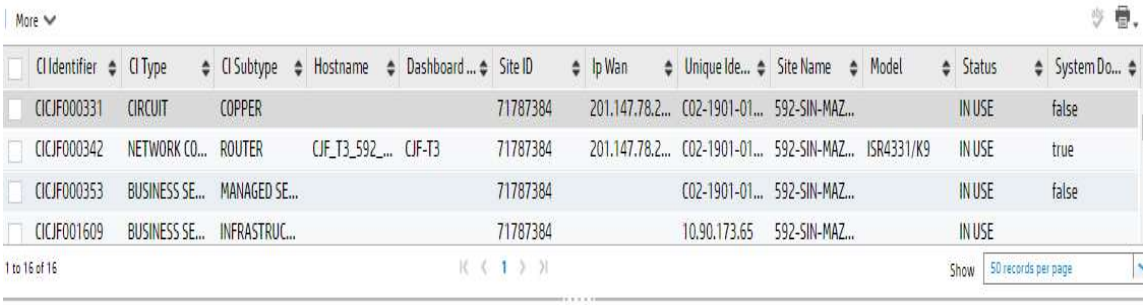



**Figura 10:** Componentes de un sitio del cliente visualizados en *Incident Manager*

También mencioné que, es importante conocer cómo están compuestas las redes de los clientes porque eso ayuda a diagnosticar y resolver fallas de una manera más rápida. Sin embargo en el sector Gobierno se gestionan más de 30 clientes, y aprenderse de memoria todas esas redes es muy complicado, además de que las mismas van cambiando de manera constante. En el NOC se cuenta con un **Portal de Operaciones**. Este portal es una página interna del NOC donde se encuentra la lista de clientes organizados por cada sector del NOC, los accesos a los equipos del cliente y el diagrama de red de cada cliente. Estos datos cambian conforme el cliente haga cambios o alteraciones en su red. En la figura 11 se muestra la interface gráfica del Portal de Operaciones donde se almacena la información descrita antes:


**Figura 11:** Portal de Operaciones del NOC

Una mejor manera de visualizar la forma en la que se compone cada red gestionada por el NOC es a través de una herramienta llamada ***Panel***. En el *Panel* se cuenta con un campo de búsqueda, donde sólo hay que teclear el nombre del cliente que queremos visualizar y muestra el total de servicios gestionados por el NOC para ese cliente, el número de servicios afectados, activos, en suspensión (cuando se trata de sitios o servicios en proceso de baja del NOC). En la pantalla se muestran los servicios sombreados en rojo, los cuales representan los servicios afectados, mientras que los servicios sombreados en verde son los servicios activos. La búsqueda de un sitio de cliente se puede realizar a través del *site* ID, una vez que se tenga visualizada la red de un cliente. Por ejemplo, si para el cliente de RAN quisiera visualizar los componentes que conforman al sitio de Querétaro primero hago la búsqueda en *Panel* del cliente RAN, y una vez que ya se visualice la red del cliente entonces se puede buscar al sitio, por nombre o por *site* ID en el campo de búsqueda, como se aprecia en la figura 12:


**Figura 12:** Visualización de la red de un cliente en el *Panel*

El *Panel* también funciona para sacar las gráficas que muestren el comportamiento un enlace, ya sea que haya quedado fuera de servicio, haya presentado saturación o degradación.

En el NOC cada cliente cuenta también con acceso a *Panel*, es decir, a través de esta herramienta los clientes pueden verificar el estado en que se encuentran sus redes.

Una herramienta utilizada en el NOC que también sirve para gestionar las redes de los clientes se llama NAM, en la cual se encuentran las configuraciones de todos los *routers* y *switches* gestionados por el NOC. Estas configuraciones son las más recientes de cada equipo y son requeridas al momento de hacer un cambio de *router* o *switch*. Sólo hay que descargar la configuración del dispositivo a cambiar para colocarla en la nueva refacción. Cada que hay cambios en la configuración de algún *router* o *switch* es guardada también en este servidor.

En el campo donde dice "IP o *hostname*" deberá colocarse la IP que tiene configurada el enlace o dispositivo, y como resultado arrojará un log de la configuración más reciente del servicio.

En la figura 13 se muestra la interface gráfica de la herramienta NAM, en la cual se observa de lado izquierdo que se tiene el campo donde se pide la dirección IP o *hostname* del sitio que se desea revisar, en la parte central se observa la lista de dispositivos que han tenido una actualización reciente en su configuración, la fecha en que fue aplicado la actualización o cambio y del lado derecho se tiene habilitada la opción de ver la configuración actual para cada dispositivo:

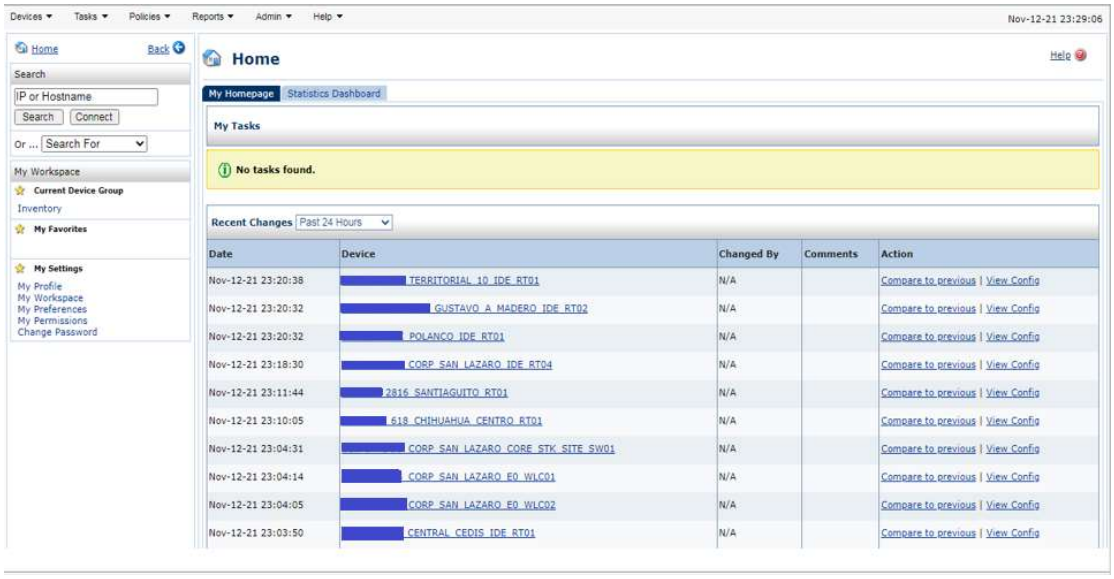



**Figura 13:** Búsqueda de un sitio en NAM.

Las herramientas ya mencionadas nos ayudan a monitorear las redes y son útiles en el proceso de gestión de incidentes, sin embargo, el interactuar con los componentes (equipos) de la red del cliente nos ayuda a determinar de manera más certera un diagnóstico.

Esta interacción se logra a través del ***Terminal CRT.*** *Terminal CRT* es una herramienta que cuenta con una ventana de comandos que nos permite conectarnos a los equipos de manera segura y remota. También permite conectarnos a diversos equipos de diferentes redes de cliente, ya que en la herramienta se pueden personalizar estas conexiones a través de botones o scripts que con tan sólo ejecutarlos nos conectamos al equipo que se quiere gestionar.

Esta herramienta nos permite ingresar a los equipos de los clientes a través de protocolos como SSH y TELNET, dependiendo de cuál tenga configurado cada cliente para acceder a su red. Las contraseñas con las que se accede a los equipos de cada cliente son proporcionadas por el mismo.

El TERMINAL CRT permite también administrar las redes. Esta herramienta se conecta a la nube del NOC (o *backbone* de UNIRED). Hay clientes que cuentan con una nube propia, en la que están conectadas todos sus enlaces WAN. Para acceder a esa nube se hace a través de un servidor con el que, como personal del NOC tenemos acceso mediante el TERMINAL CRT. En resumen, a través del TERMINAL CRT se tiene acceso tanto a la nube de UNIRED como a la nube WAN de cada cliente (los que la tengan, eso depende de la forma en que cada red está compuesta).

En la figura 14 se muestra la interface gráfica de la herramienta Terminal CRT. Se observa que es muy parecida a una ventana de comandos como la que se utiliza en Windows. A través de esta herramienta es como tenemos acceso a los equipos que componen las redes de los clientes:

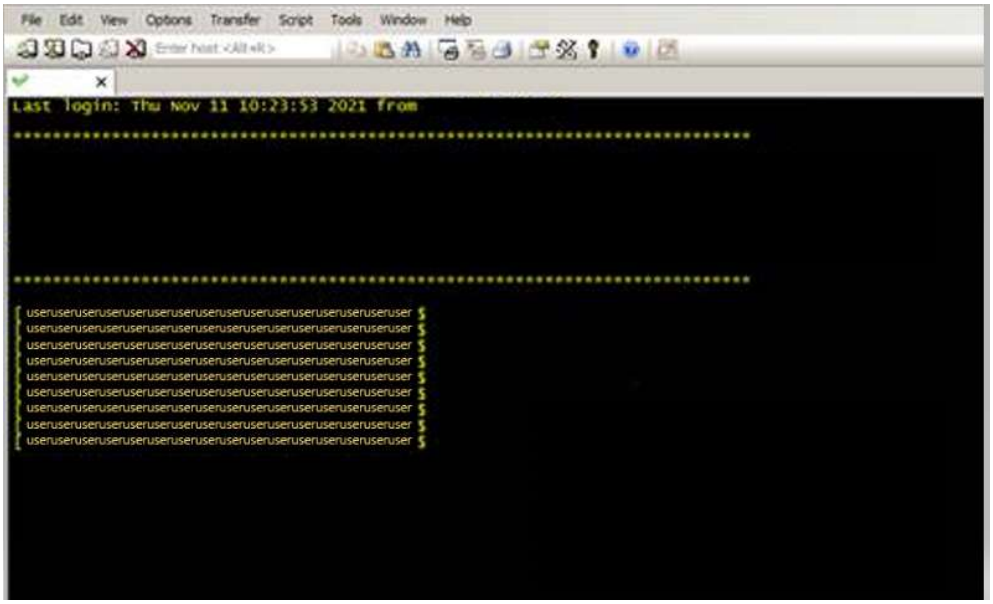



**Figura 14:** Interface de *TERMINAL CRT*

Otra herramienta que es de gran importancia dentro de mi puesto como Operador Multiplataforma es el **correo electrónico**, debido a que es un medio más con el que contamos para comunicarle al cliente las fallas que se presentan dentro de su red (en caso de que lo requiera por ese medio).

### 3.1.4 Atención a fallas en las redes de cliente

La atención a fallas es la función principal de un Operador Multiplataforma, Gestión y Soporte (o ingeniero de NOC).

Se inicia turno laboral abriendo el correo electrónico del NOC, *Panel*, portal de operaciones, *Terminal CRT*, a las herramientas de monitoreo que el cliente proporcionó para su red (en dado caso) y al ***Incident Manager.***

Como ya se mencionó, las fallas que se presentan dentro de la red de cliente son:

- Pérdida de conectividad (un nodo aislado o incomunicado)
- Saturación de enlace (alto consumo de ancho de banda de una red)
- Degradación o intermitencia en una red
- Afectación en la operación de un equipo perteneciente a la red del cliente, ya sea en un *switch*, un *access point,* un UPS.

Para la atención de cualquiera de las fallas, como ingeniero de NOC realizo la atención a las fallas de la siguiente forma:

**a)** Pérdida de conectividad (un nodo aislado o incomunicado)

Al momento en que un sitio perteneciente a una de las redes de los clientes que gestiono se queda con el enlace WAN fuera de servicio se genera de manera automática el reporte dentro del *Incident Manager.* Reviso la descripción del reporte para saber el tipo de afectación presente. Cuando la descripción dice "*Node down*" significa que el enlace se encuentra fuera de servicio, por lo tanto, el sitio está incomunicado. La revisión del sitio incomunicado se realiza en las siguientes etapas:

**1)** Revisión desde la nube o *backbone* del proveedor:

**En el caso de un enlace RPV** lo que hago es verificar dentro del reporte en qué *router* de la nube de proveedor se tiene configurado este servicio. Suponiendo que se tiene el router de la nube llamado vpn_jalisco_zona1. Una vez que se tenga el nombre del router de la nube se ingresa a él con los comandos mostrados en la tabla 03:

**Tabla 03**: Comandos de equipos CISCO en la nube del proveedor

| Comando | Función |
|---|---|
| getnode vpn_jalisco_zona1 | muestra la IP que el *router* vpn_jalisco_zona1 tiene configurada |
| ssh –l user XXX.XXX.XXX.XXX | se ingresa al *router* via ssh con la IP arrojada por el comando anterior, donde "user" representa l usuario para acceder y las "X" representan los octetos de la IP. Posteriormente se coloca el password. |
| show running interface \| include CYY-YYYY-YYYY | Donde CYY-YYYY-YYYY es la referencia del servicio que se está revisando. Este comando muestra la interface del *router* de la nube de proveedor en la que la referencia del sitio afectado está configurada |
| show run interface | Muestra el estatus de la interface perteneciente al enlace que se está revisando. Permite verificar cuál es la vrf perteneciente al servicio. VRF (virtual *routing* and *forwarding*) es una red privada virtual configurada entro de un *router* físico. Por cada enlace gestionado por el NOC se tiene una vrf diferente configurada. |
| sho bgp vrf VRFYYYYYYY summary \| include XXX.XXX.XXX.XXX | Muestra la sesión de bgp asociada al enlace que estamos revisando, donde VRFYYYYYYY se obtiene del comando anterior y XXX.XXX.XXX.XXX se refiere a la IP asociada a la sesión de BGP que se está revisando. |

**En el caso de un enlace IDE** abrimos una sesión en el TERMINAL CRT para acceder al servidor (nube de proveedor) y desde el servidor dar un ping a la IP WAN del enlace. En caso de que no responda significa que el enlace está afectado. Una revisión más a detalle implica ingresar al PE de la nube del proveedor y

verificar en qué interface está configurada el enlace, y desde ahí verificar si el servicio está afectado.

En la tabla 04 se muestran los comandos que se utilizan para revisar un enlace IDE en la nube del proveedor:

**Tabla 04**: Segunda tabla de comandos de equipos CISCO en la nube del proveedor

| Comando | Función |
|---|---|
| getnode vpn_jalisco_zona1 | muestra la IP que el *router* vpn_jalisco_zona1 tiene configurada |
| ssh –l user XXX.XXX.XXX.XXX | se ingresa al *router* via ssh con la IP arrojada por el comando anterior, donde "user" representa l usuario para acceder y las "X" representan los octetos de la IP. Posteriormente se coloca el password.e ingresa al *router* via telnet con la IP arrojada por el comando anterior, donde las "X" representan los octetos de la IP. |
| show running interface \| include CYY-YYYY-YYYY | Donde CYY-YYYY-YYYY es la referencia del servicio que se está revisando. Este comando muestra la interface del *router* de la nube de proveedor en la que la referencia del sitio afectado está configurada |
| show arp interface GX/X/X | Debe mostrar dos direcciones MAC: una que corresponde al PE o al *router* de la nube del proveedor donde se tiene configurado el servicio y la otra MAC deberá ser la del CPE o la del *router* en sitio del cliente. En caso de que no se observa la dirección MAC del CPE es cuando se determina que el servicio está afectado. |

**En el caso de un enlace satelital** abrimos una sesión en el TERMINAL CRT para acceder al servidor (nube de proveedor) y desde el servidor dar un ping a la IP WAN del enlace. En caso de que no responda significa que el enlace está afectado. Estos enlaces no van amarrados a algún equipo de la nube del proveedor, por lo que la única forma de verificar si están afectados o no es por esta.

**2)** Revisión del servicio afectado en herramientas de monitoreo: una vez que se comprobó en la nube del proveedor que efectivamente el servicio está afectado se revisa en *Panel* que el servicio se encuentre alarmado también.

**3)** Proceso de *check-list*: una vez que se haya detectado que el enlace se encuentra fuera de servicio se busca en los incidentes anteriores del sitio en cuestión un nombre y teléfono de alguna persona (por parte del cliente) en el sitio para informarle que el enlace presenta afectación. Hay clientes que proporcionan un directorio donde vienen los nombres y números de cada persona que se encuentra en cada uno de sus sitios o en ocasiones se recibe llamada del cliente donde reporta el servicio con afectación.

Una vez que se haya logrado establecer contacto con el cliente en sitio se le pide validar que no tenga fallas de energía o equipos apagados, ya que, en cuando se confirme que esa es la causa del incidente sólo es cuestión de que restablezca el suministro eléctrico para encender equipos y validar que el servicio esté en función.

En caso de que el cliente confirme que no hay fallas de energía se le proporciona la marca, modelo y número de serie del *router*.

El *router*, al ser el dispositivo que encabeza toda red LAN deberá ser el primero en ser revisado. Los datos del *router* se buscan de la manera descrita en la figura 9. El cliente deberá localizar el equipo que se le indica y revisar que esté encendido, que la conexión o el cable que va del *router* hacia el equipo ISP (según el medio de transmisión utilizado) se encuentre bien conectado, en buen estado y que no haya sido alterado removido.

En ocasiones los clientes, llegan a remover o a retirar los cables por condiciones de mantenimiento y al querer volver a conectarlos los colocan en el puerto del *router* o del ISP diferente al que debería conectarse, debido a que no recuerdan cómo van las conexiones.

Se le pregunta al cliente cuál es la marca y modelo de ISP que se encuentra en sitio. Los equipos ISP que se encuentran en sitio normalmente son los mostrados en la tabla 05:

| **Tabla 05**: Equipos ISP<br>Marca | Ilustración |
|---|---|
| Huawei Hg8245h5 (ONT) |  |
| ADVA FSP150CC (Demarcador)) |  |
| ALCATEL LUCENT 1521 CLIP (Demarcador) |  |
| RAD ETX-203AX (Demarcador) |  |
| Tellabs 8110 N (NTU) |  |
| WATSON 5 (NTU) |  |

Una vez que el cliente identificó el ISP se le pide revisar que esté encendido y si presenta alarmas. Las alarmas en estos equipos se aprecian cuando se tiene un foco o led rojo encendido o que el puerto del ISP donde se conecte al *router* no parece establecer comunicación entonces se valida que la falla podría estar en el medio de transmisión.

Las marcas más comunes de equipo router (CPE) son: Cisco, Teldat y Huawei.

En ocasiones hay clientes que no tienen conocimiento sobre los equipos que se encuentran en el sitio, es decir, desconocen la forma de revisarlos al momento de tener una falla en el servicio de internet. En casos como este lo que hacemos, como ingenieros de NOC es solicitar la visita de un ingeniero de campo (IDC) al sitio del cliente, para que realice el *checklist*.

**4)** Canalización de falla en caso de que la misma se encuentre a nivel transmisiones: Ya que se realizó el *checklist* y se haya determinado que la falla podría estar en el medio de transmisión entonces se procede a levantar un reporte llamando al centro de atención correspondiente a la región donde se encuentra el servicio, para que el medio sea revisado. Por ejemplo, si el servicio revisado pertenece a la ciudad de Tepic se deberá reportar la falla al CASE Guadalajara, debido a que Tepic se encuentra en el estado de Nayarit, y el estado de Nayarit es gestionado por el CASE Guadalajara (en la página 26 se encuentran los centros de atención por región del país).

El personal de transmisiones es el responsable de revisar la infraestructura que compone al servicio donde se tiene la falla, desde la red de planta exterior (acometida, cable subterráneo o aéreo, gabinete, etcétera) hasta la red de planta interior (centrales telefónicas).

A partir de que el servicio afectado haya sido canalizado a transmisiones se deberá solicitar actualización de la falla cada hora al centro de atención donde fue reportado el servicio, a través de llamada o correo. Para agilizar la atención de parte de transmisiones se lleva a cabo el proceso de escalación con el área técnica, después con el área de supervisión, subgerencia, gerencia y coordinación de cada centro de atención telefónica. La escalación se lleva a cabo reportando la falla a los diferentes niveles de jerarquía den centro de atención telefónica, es decir, la falla se reporta con el área técnica y después de una hora, al no recibir actualización se reporta con el área de supervisión, luego con la de sugerencia, etcétera, hasta que se proporcione un tiempo estimado de solución o el servicio haya restablecido.

**5)** Recuperación de la operación del servicio: Una vez que el servicio restableció se procede a llamarle al cliente para validar que el enlace ya esté funcionando correctamente, y con ello dar por terminada la falla. La forma de verificar si el servicio ya está activo es ingresando al CPE utilizando la IP WAN, ya sea a través de telnet o *ssh*. Una vez dentro del equipo se verifica el estatus del mismo con la lista de comandos que se muestra en la tabla 06:

| **Tabla 06**: Comandos de equipos CISCO en un *router* | |
|---|---|
| Comando | Función |
| show version | Muestra la versión de software y el tiempo que el equipo lleva encendido. |
| show ip bgp summary | En un *router* muestra el tiempo que lleva en operación la sesión de BGP, ya que, este es el protocolo por el que el sitio tiene acceso a internet |
| show interface summary | Sirve para verificar que en la interface donde se tiene el enlace configurado tenga tráfico. |
| show log | Muestra todos los eventos acontecidos en el equipo, tanto en un *router* como en un *switch*. |

Para el caso de los sitios que cuenten con *router* Teldat, los comandos de verificación son los mostrados en la tabla 07:

| **Tabla 07:** Comandos de equipos TELDAT | |
|---|---|
| Comando | Función |
| *p 3 | Se habilita el modo de monitorización en el *router* |
| configuration | Muestra la hora en el *router*, el tiempo que lleva encendido el equipo, y la versión de software. |
| pro bgp<br>summary | Nos ayuda a visualizar el tiempo que la sesión de BGP del servicio lleva operando |
| p ip<br>interface | Muestra las interfaces del *router* |
| p arp<br>dump | Muestra las direcciones MAC de los equipos que están conectados al *router* y la IP que tienen configurada |

Para el caso de los sitios que cuenten con *router* Huawei, los comandos de verificación son los mostrados en la tabla 08:

| **Tabla 08**: Comandos de equipos HUAWEI | |
|---|---|
| Comando | Función |
| ssh –l user XXX.XXX.XXX | Acceso a *router* por protocolo ssh, donde "*user*" es el usuario proporcionado por el cliente, para gestionar su red y donde XXX.XXX.XXX es la IP WAN del enlace |
| dis version | Muestra la versión de software cargada en el *router*, el tiempo de encendido del equipo |
| display current-configuration | Muestra la configuración actual. |
| dis bgp peer | Nos ayuda a visualizar el tiempo que la sesión de BGP del servicio lleva operando |

En ocasiones, cuando el personal de transmisiones reparó el servicio pero el mismo aun así continúa afectado entonces se programa a un IDC para que acuda al sitio y revise a detalle los equipos que encuentre. Si el IDC detecta que el *router*, el *switch* o *access point* pudieran tener alguna falla, ya sea porque no enciendan, porque tengan olor a quemado, hagan ruidos extraños, se detecte que no sirven los ventiladores, o porque se haya perdido algún equipo o se haya quemado por descargas de energía entonces se solicita la refacción de la pieza que se desea cambiar. En el caso del *router* y el *switch*, al ser equipos que serán reemplazados se deberá descargar de la página del NAM la última configuración para que, cuando el IDC haga el cambio de dispositivo coloque la configuración adecuada y así poner el equipo en marcha.

Algunas veces se requiere de una visita en conjunto, la cual es aquella donde se requiere tanto de un IDC como de personal de transmisiones en el sitio del cliente, para determinar de una manera más rápida la causa de la falla en el servicio. En estos casos se hace lo mismo con el IDC: indicarle que revise el *router*, *switch*, la conexión entre el *router* y el demarcador.

**b)** Saturación de enlace (alto consumo de ancho de banda de una red)

Al momento en que un sitio perteneciente a una de las redes de los clientes presenta saturación en su enlace WAN se genera de manera automática el reporte dentro del *Incident Manager.* Si la descripción del reporte dice "*high input utilization*" significa que el enlace se encuentra saturado, lo que provoca lentitud y descarte de tráfico en el servicio. Cuando un servicio presenta saturación únicamente presenta un alto consumo de ancho de banda.

El tráfico en una red se presenta cuando la capacidad de envío o recepción de datos sea utilizada en un alto porcentaje. Esto debido al gran número de usuarios conectados a esa red, lo que provoca un aumento de tráfico y causa de esto es la lentitud para el envío y recepción de datos.

El *Incident Manager* está configurado para arrojar una alarma de saturación cuando esa capacidad para enviar o recibir datos se encuentre por arriba del 80% de uso.

El procedimiento para revisar la saturación del servicio es el siguiente:

**1)** Se ingresa por ssh al *router* correspondiente al sitio reportado, utilizando su IP WAN.

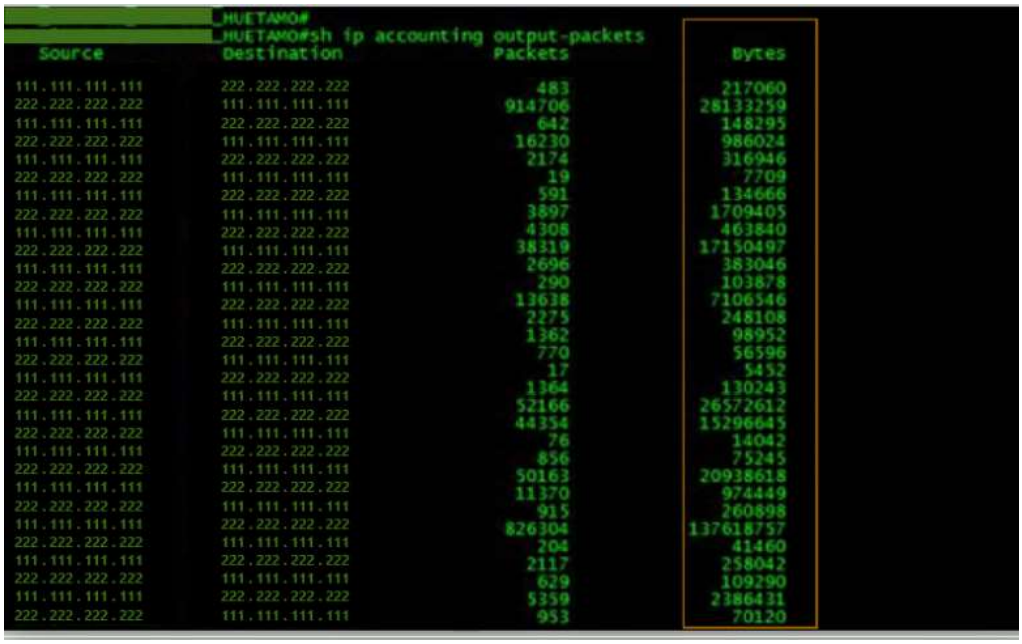
**2)** Una vez dentro del *router* se revisa la saturación del servicio con los comandos mostrados en la tabla 09:

| **Tabla 09**: Segunda parte de comandos de equipos CISCO en un *router* | |
|---|---|
| Comando | Función |
| show interface description | Muestra la descripción que tiene cada interface del *router*. Esto nos ayuda a distinguir rápidamente el puerto donde se entrega el servicio. |
| show ip interface brief | Muestra el estado y la IP que cada interface tiene configurada. Si en alguna de ellas se observa la IP WAN (con la que se entró al *router*) significa que en esa interface es donde se está entregando el servicio. Esta es otra forma de encontrar la interface del servicio. |
| show interface GX/X/X | Se utiliza para ver la información de la interface donde se entrega el servicio. Aquí es donde hay que visualizar la siguiente línea:<br><br>reliability 255/255, txload 150/255 rxload250/255<br><br>Se puede observar que la capacidad de recepción está casi a su totalidad, por lo que se determina que efectivamente hay saturación |

**3)** Una vez detectada la saturación, dentro del *router* se ejecuta el comando que se muestra a continuación, el cual nos ayuda a verificar qué servicio podría estar ocasionando la saturación:

| | |
|---|---|
| show ip accounting output-packets | Ver conteo de paquetes |

El resultado de ese comando es una lista de direcciones IP, el número de paquetes de salida en una columna y de entrada en la otra, como se muestra en la figura 15, donde bytes hace referencia al tamaño de los paquetes (ver columna marcada con el rectángulo naranja)



```
HUETAMO#
HUETAMO#sh ip accounting output-packets
Source          Destination         Packets     Bytes
111.111.111.111 222.222.222.222         483    217060
222.222.222.222 111.111.111.111      914706  28133259
111.111.111.111 222.222.222.222         642    148295
222.222.222.222 111.111.111.111       16230    986024
111.111.111.111 222.222.222.222        2174    316946
222.222.222.222 111.111.111.111          19      7709
111.111.111.111 222.222.222.222         591    134666
222.222.222.222 111.111.111.111        3897   1709405
111.111.111.111 222.222.222.222        4308    463840
222.222.222.222 111.111.111.111       38319  17150497
111.111.111.111 222.222.222.222        2696    383046
222.222.222.222 111.111.111.111         290    103878
111.111.111.111 222.222.222.222       13638   7106546
222.222.222.222 111.111.111.111        2275    248108
111.111.111.111 222.222.222.222        1362     98952
222.222.222.222 111.111.111.111         770     56596
111.111.111.111 222.222.222.222          17      5452
222.222.222.222 111.111.111.111        1364    130243
111.111.111.111 222.222.222.222       52166  26572612
222.222.222.222 111.111.111.111       44354  15296645
111.111.111.111 222.222.222.222          76     14042
222.222.222.222 111.111.111.111         856     75245
111.111.111.111 222.222.222.222       50163  20938618
222.222.222.222 111.111.111.111       11370    974449
111.111.111.111 222.222.222.222         915    260898
222.222.222.222 111.111.111.111      826304 137618757
111.111.111.111 222.222.222.222         204     41460
222.222.222.222 111.111.111.111        2117    258042
111.111.111.111 222.222.222.222         629    109290
222.222.222.222 111.111.111.111        5359   2386431
111.111.111.111 222.222.222.222         953     70120
```

**Figura 15:** Conteo de paquetes de un servicio

**c)** Degradación o intermitencia en una red

Al momento en que un sitio perteneciente a una de las redes de los clientes que gestiono presenta intermitencia en su enlace WAN se genera de manera automática el reporte dentro del *Incident Manager.* Reviso la descripción del reporte para saber el tipo de afectación presente. Cuando la descripción dice "*degraded link*" significa que el enlace presenta degradación. En la saturación el enlace mostraba alto consumo de ancho de banda pero no quedaba fuera de servicio, sin embargo, la intermitencia significa que el enlace se levanta y se cae constantemente.

El proceso para saber si un enlace presenta intermitencia es el siguiente:

**1)** Desde el servidor de la nube del proveedor para el caso de un enlace IDE) o desde el servidor de Gobierno (para el caso de enlaces RPV) se deja ejecutando un ping de manera contínua a la IP WAN y se puede observar cuando deja de responder ese ping, es decir, se observa que el pingo a ratos no responde.

Otra forma de verificar la intermitencia en un servicio es entrar al *router* del sitio (en caso de que el servicio se encuentre activo) y ejecuta los comandos que son mostrados en la tabla 10, conforme al orden mostrado:

| **Tabla 10**: Tercera parte de comandos de equipos CISCO en un *router* | |
|---|---|
| Comando | Función |
| show version | Muestra la versión de software y el tiempo que el equipo lleva encendido. Esto ayuda a descartar que la intermitencia haya sido provocada por cortes de energía o apagado de equipo |
| show ip bgp summary | Muestra el tiempo que lleva en operación la sesión de BGP. Si este tiempo es consideradamente menor al tiempo mostrado con el comando de *show version* significa que posiblemente la intermitencia sea provocada por una falla en el medio de transmisión. |
| show interface description | Muestra la descripción que tiene cada interface del *router*. Esto nos ayuda a distinguir rápidamente el puerto donde se entrega el servicio. |
| show interface GX/X/X | Muestra el estatus de la interface donde se entrega el enlace. Ahí se observa la confiabilidad del enlace, la cual se muestra como 255/255. En caso de que en ambos lados de la diagonal se muestren números diferentes significa que el medio de transmisión se encuentra afectado, por lo que el enlace deberá ser reportado al área correspondiente.<br>En esta misma interface muestra los errores crc, los cuales indican que en la red se tiene pérdida de paquetes y quedaron de manera cíclica viajando e la red, sin llegar a su destino por alguna falla en el medio de transmisión o en el cableado interno del cliente.<br><br>Este comando se va ejecutando varias veces y si se observa que hay incremento de errores hay que reportarse al área correspondiente. |
| show log | Muestra todos los eventos acontecidos en el equipo. Si se observa que la interface donde se tiene configurado el servicio muestra eventos de *down* y up significa que el servicio oscilaba. |
| clear interface GX/X/X | Reinicia las estadísticas de la interfaz. Se utiliza sobre todo para después de haber arreglado la falla en el medio de transmisión o del lado del cliente para asegurar de que ya no se tiene falla en el servicio. |

Una vez que el servicio fue reportado al área de transmisiones y la falla haya sido arreglada se procede a monitorear la sesión de BGP para vigilar que no vuelva a presentar las oscilaciones y validar con el cliente que el servicio ya esté trabajando correctamente. En el caso de que se determine que la causa de la falla sea del lado del cliente entonces se procede a realizar *checklist* con usuario para revisar cableado entre *router*, demarcador o en los mismos equipos. Para esto también podrían enviarse a un IDC.

**d)** Afectación en la operación de un equipo perteneciente a la red del cliente, ya sea en un un *switch*, un *access point,* un UPS.

- Revisión de un *switch*: Al momento en que un sitio perteneciente a una de las redes de los clientes que gestiono presenta afectación en un *switch* se genera de manera automática el reporte dentro del *Incident Manager.* Reviso la descripción del reporte para saber el tipo de afectación presente. Cuando la descripción dice "*switch down*" significa que el equipo se encuentra fuera de operación.

  Las causas más comunes que presenta un switch son:

  - Apagado o desconexión de un *switch* por usuario
  - Daño en cable o en conectores del cable que conecta al *switch* con el *router*
  - Daño en puertos de *switch*
  - Daño en *switch*

  Las marcas de switch más comunes en los sitios de cliente son Cisco y Extreme.

  Primero se revisa si el sitio (enlace) al que pertenece el *switch* también se encuentra fuera de servicio o presentando degradación, buscando en *Panel* el sitio en cuestión, para visualizar los equipos que lo componen y revisar el *router* (donde se entrega el enlace). E caso de que el enlace tenga afectación significa que la afectación del *switch* podría derivarse de la del enlace. En caso de que el enlace no tenga afectación entonces se procede a contactar al cliente en sitio para que se realice el *checklist*. En el *checklist* se revisa que el *switch* afectado esté encendido, que no haya sido apagado por el usuario, debido a que hay usuarios que suelen apagar sus equipos en fines de semana o en periodos vacacionales. Se valida si el *switch* va conectado a un banco de baterías (UPS), a un no break o si se encuentra directamente conectado a un contacto.

  En caso de que un *switch* esté encendido se revisa la conexión existente entre el *router* del sitio y el *switch*, checando que el cable que hay entre los dispositivos no se

encuentre en mal estado, desconectado y probar ese cable con un probador de cables de red, para descartar daño en el mismo. En caso de que el *switch* se encuentre desconectado del *router* se revisa dentro del *router* cuál es el puerto que se tiene configurado para el *switch* y conectarlo donde corresponde. Se conecta el cable, se restablece conexión entre el switch y el router y se valida con cliente.

Si el cable que se encuentra entre el *switch* y el *router* presenta falsos o desconexiones, ya sea del lado del *switch* o del lado del *router* se procede a realizar el cambio de conector RJ45. Esta prueba se realiza conectando y desconectando el cable primero del lado del *router* ingresando al equipo y con el comando "term mon" para monitorear los sucesos acontecidos en el equipo en ese momento en que lo estamos revisando. Si observamos que el puerto correspondiente al *switch* presenta intermitencias primero habrá que conectar y desconectar el cable a otro puerto disponible del *router* y verificar si se presenta el mismo comportamiento. En caso de que en otro puerto del router se vean las intermitencias habrá que cambiar el conector del lado del *router* y monitorear que ese comportamiento no vuelva a darse. Al momento de verificar del lado del *switch* se hace lo mismo: ingresar al equipo, con el comando "term mon" y si se observa intermitencia del lado del *switch* pero no del *router* habrá que probar en otro puerto del *switch* si el puerto sigue intermitente, y en caso de que sí significa que del lado del *switch* el conector está dañado y se procede a realizar el cambio.

Hay ocasiones en las que los conectores se encuentran en buen estado pero al probar en diferentes puertos se observa que no se detecta el cable en el *router* o *switch*, pero si ese mismo cable es probado en otros puertos de otros equipos significa que ese *router* o *switch* tiene el o los puertos dañados. Cuando se detecte que un *switch* o *router* cuenten con varios puertos dañados se realiza cambio de equipo con ayuda de un IDC en sitio.

La mayoría de las veces los clientes en sitio no cuentan con las herramientas necesarias o con los conocimientos para llevar a cabo este proceso de *troubleshooting*, por lo que se programa a un IDC para que realice el proceso de revisión y con el mismo se realiza todo lo descrito anteriormente, y en caso de que se detecte que algún equipo esté dañado se procede a pedirle una ventana de mantenimiento al cliente para realizar el cambio de equipo.

- Revisión de un *access point*: al momento en que un sitio perteneciente a una de las redes de los clientes que gestiono presenta afectación en un *access point* se genera de manera automática el reporte dentro del *Incident Manager.* Reviso la descripción del reporte para saber el tipo de afectación presente. Cuando la descripción dice "*ap down*" significa que el equipo se encuentra fuera de operación.

Primero se revisa si el *switch* del sitio al que pertenece el *access point* también se encuentra fuera de servicio o presentando degradación, buscando en *Panel* el sitio en cuestión, para visualizar los equipos que lo componen y revisar el *switch* de ese sitio. En caso de que el *switch* tenga afectación significa que la afectación del *access point* podría derivarse de la del *switch*.

En caso de que el *switch* no tenga afectación entonces se procede a revisar el *access point*. La marca más común de *access point* en los sitios de cliente es Cisco.

Hay sitios que cuentan con más de un *switch* y con varios *access point*, esto dependiendo de cómo tenga cada cliente diseñada su red. Sólo algunos clientes, al momento de contratar con el NOC el servicio de monitoreo incluyen *access point*. Cuando se tiene un *access point* fuera de servicio se le llama al cliente para que apoye con la revisión del equipo en sitio, se le pide que verifique y proporcione la dirección MAC de ese *access point*, se ingresa al *switch* o *switches* del sitio y se ejecutan los comandos que se muestran en la tabla 11:

**Tabla 11:** Cuarta parte de comandos de equipos CISCO en un *router*

| Comando | Función |
|---|---|
| show mac address-table \| include ABCD | Muestra todas las direcciones *MAC* existentes en el *switch* que tengan la terminación ABCD, por ejemplo. Si no arroja información significa que el *access point* podría estar conectado a otro *switch*, pero si arroja información indicará cuál es la IP asociada a esa *MAC address,* al igual que el puerto en donde se conecta esa *MAC address*<br><br>*Si la IP amarrada a esa MAC address* difiere a la que se tiene en monitoreo se realiza el amarre entre el AP y la *MAC address* correspondiente |
| show cdp neighbors int GX/X/X detail | Muestra que se tenga la IP de monitoreo correspondiente a la mac address del access point |

Para validar que los pares de cableado del cable UTP del *access point* al *switch* se encuentre en buen estado se ejecutan los comandos mostrados en la tabla 12:

**Tabla 12**: Cuarta parte de comandos de equipos CISCO en un *router*

| Comando | Función |
|---|---|
| test cable-diagnostics tdr interface + "interface a revisar" | Ejecuta la prueba parta verificar pares de cableado del cable UTP |
| show cable-diagnostics tdr interface + "interface a revisar" | Muestra el estatus de los cuatro pares de cableado, A, B, C y D. Si el cableado se muestra "open" en los cuatro pares significa que posiblemente esté desconectado, pero si sólo un par se muestra en "open" significa que se tiene daño en el cable, por lo que el mismo deberá ser reemplazado. |

Por lo general el cliente en sitio no cuentas con los conocimientos técnicos ni herramientas para revisar equipos en sitio, por lo que se programa a un IDC con el equipo adecuado y relacionamiento de AP o de cable en caso de ser necesario, para que se haga el cambio.

Hay veces en que al momento de hacer uh *checklist* se detecta que el AP ya no enciende o que la *MAC address* no se visualiza en el *switch* de donde se conecta, por lo que deberá reemplazarse el AP.

- Revisión de un UPS: al momento en que un sitio perteneciente a una de las redes de los clientes que gestiono presenta afectación en un UPS se genera de manera automática el reporte dentro del *Incident Manager.* Reviso la descripción del reporte para saber el tipo de afectación presente. Cuando la descripción dice "*ups down*" significa que el equipo se encuentra fuera de operación.

La marca de UPS más común en los sitios de cliente es Trip Lite. Sólo algunos clientes, al momento de contratar con el NOC el servicio de monitoreo incluyen al UPS.

Se le llama al cliente en sitio para pedirle apoyo en realizar *checklist*. Se le pide validar que el UPS se encuentre encendido y conectado a un contacto de corriente eléctrica y checar qué y qué equipo se encuentra conectado a él. Del UPS deberá conectarse el o los *router*, *switch* o *switches* y equipo ISP. En caso de que esté apagado se le pedirá encenderlo y validar que ya se encuentre operando.

Hay clientes que solicitan hacer pruebas de apagado y encendido de UPS por dos horas o hasta más tiempo, para verificar que cumpla con su función de retener carga.

En caso de que el UPS esté encendido pero se verifica que hace un sonido de alerta significa que la batería del UPS ya no retiene carga, por lo que ya no está cumpliendo su función como respaldo de energía eléctrica al momento de haber una ausencia de luz en el sitio. Para ello se solicita a Servicios en campo la refacción de la batería para ser reemplazada por un IDC en sitio, realizar el cambio, hacer pruebas de apagado y encendido para verificar que la batería nueva cumpla con su función y así validar con cliente que la falla ha sido resuelta.

Otra falla que podría presentar es que la tarjeta SNMP ya no le funcione. El UPS está encendido sin embargo no se tiene gestión remota del equipo, por lo que se le pide al cliente o se envía a un IDC para que revise el equipo y le haga un reinicio físico, valide que el cable de corriente eléctrica del UPS se encuentre en buenas condiciones, se realiza verificación de voltaje pero si aún así no se tiene gestión del dispositivo se solicitará un cambio de tarjeta SNMP, pidiendo la refacción a servicios en campo y a un IDC para efectuar el cambio.

# GLOSARIO DE TÉRMINOS

**Access point**: es una antena que integra a cualquier dispositivo a una red cableada a través de una conexión inalámbrica.

**BGP** (*Border Gateway Protocol*). Puerta de enlace de frontera, el cual es el protocolo de red más utilizado para intercambiar información entre los diferentes proveedores de servicios de internet.

**Cable UTP** (Unshielded Twisted Pair): cable de par trenzado no blindado.

**Comandos**: Se refiere al conjunto de instrucciones que el ingeniero de NOC utiliza para interactuar con un sistema o elemento informático.

**Costo** (en OSPF): Es una métrica utilizada dentro del protocolo OSPF utilizada para encontrar la ruta más corta entre dos puntos de una red.

**Credenciales de acceso**: término que se le atribuye al usuario y contraseña proporcionados por una entidad para la gestión de su información.

**CPE** *(Customer Premises Equipment):* Equipo Local del Cliente, el cual hace referencia al equipo que se localiza en el sitio o instalaciones del cliente.

**DCE** (*Data Communication Equipment*): Equipo de Comunicación de Datos, el cual se refiere al equipo que permite la conexión a una nube WAN.

**Demarcador**: dispositivo que proporciona a una red LAN

**DTE** (Data Terminal Equipment): Equipo Terminal de Datos, es el equipo donde se visualiza la información que el usuario envía y/o recibe.

**Enlace:** es un canal de comunicación que conecta a dos o más nodos dentro de una red de comunicaciones con el propósito de transmitir datos.

**Enlace IDE** (Internet Directo Empresarial): es una conexión directa al servicio de internet sin necesidad de una línea telefónica, y cuenta con la misma velocidad de carga y descarga de datos.

**Enlace RPV**: Es una red privada virtual que permite ofrecer servicios diferenciados de acuerdo a la calidad de servicio requerida o demandada por el cliente. Esa calidad de servicio permite priorizar y clasificar el tráfico de la red del cliente para garantizar un mejor servicio.

**Gbps** (Gigabit por Segundo): es la unidad que mide la velocidad a la que viajan los datos sobre un medio de transmisión.

**Hardware**: recurso informático tangible.

**Home office:** Modalidad de trabajo que permite al empleado de una empresa realizar sus actividades laborales vía remota, por lo que no hay necesidad de hacer acto de presencia en la oficina.

**Host:** se refiere a cualquier computadora o dispositivo conectado a una red.

**Hub (en red satelital)**: es un equipo que se encuentra en la oficina central del proveedor y se encarga de transmitir el servicio de internet hacia un satélite, y el satélite se encarga de distribuirla a todos los sitios remotos.

**ISP** (*Internet Service Provider*): Proveedor de Servicio de Internet, es decir, la compañía con la que el cliente tiene contratado el servicio de internet.

**ITIL (***Information Technology Infrastructure Library):* Biblioteca de Infraestructura de Tecnologías de la Información. Es un término que hace referencia al conjunto de conceptos, procesos y funciones para llevar a cabo una gestión de servicios de tecnologías de información con calidad y eficiencia.

**Latencia**: es un término utilizado para describir el tiempo que tarda un paquete de datos para ir de un nodo origen a un nodo destino. En Informática la latencia se mide en milisegundos (ms), por lo que, entre más bajo sea la trasmisión de datos en milisegundos es más rápida la red.

**MAC** (*Media Access Control*): Son las siglas que se utilizan para hacer referencia a la dirección física que el fabricante asigna a cada dispositivo de su propiedad, la cual es un identificador hace único a cada dispositivo.

**Mbps** (Megabits por Segundo): es la unidad que mide la velocidad a la que viajan los datos sobre un medio de transmisión.

**Módem**: dispositivo que convierte una señal telefónica en una señal de datos y viceversa.

**Monitoreo**: es la supervisión y observación de elementos de una red con el objetivo de detectar fallas y anomalías en la misma de manera oportuna.

**NOC** (*Network Operation Center*): Es un centro que se encarga del monitoreo, administración, identificación y solución a las fallas que afectan a las redes empresariales que gestiona.

**NTU** (*Network Terminal Unit*): Unidad Terminal de Red, la cual es un dispositivo que vincula a una red LAN con una red telefónica, es decir a una red de cobre.

**Nube de proveedor:** Se refiere a la infraestructura perteneciente al proveedor (routers, aplicativos, servidores conectados entre sí) a través de la cual se le proporciona al cliente el servicio de internet y le sirve al personal que labora en el NOC para la gestión de los servicios que se le proporcionan al cliente.

**Oficina_matriz**: o también conocida como oficina central, la cual es la más grande e importante de una empresa, al ser la que funciona como centro de control de la misma.

**Onda electromagnética:** son aquellas que no necesitan un medio físico o material parta propagarse. Entre ellas encontramos las ondas de readio, televisión, telefonía, etcétera.

**ONT** (*Optical Network Terminal*): Terminal de Red Óptica, la cual es un dispositivo que convierte la señal recibida de un medio de fibra óptica en señal eléctricas que pueden ser interpretadas por un *router* de datos.

**OSPF** *(Open Shortest Path First*): es un protocolo de red que tiene como función escoger la ruta más corta entre un punto inicial y un punto final dentro de una red.

**PE** *(Provider Equipment)*: Equipo del Proveedor, el cual hace referencia a los *routers* que conforman la nube del proveedor.

**PoE** *(Power over Ethernet)*: es un mecanismo a través del cual se le proporciona energía eléctrica a un dispositivo de red por el mismo cable de datos con el que se conecta.

**Protocolo de red:** es un estándar que define la forma en la que se realizará la transmisión de datos a través de la red

**Red**: conjunto de elementos interconectados entre sí con el propósito de intercambiar información.

**Red LAN** (*Local Area Network*): Red de Área Local, la cual se configura en un edificio o sucursal.

**Red MAN** (*Metropolitan Area Network*): Red de Área Metropolitana, la cual se configura en una misma ciudad.

**Red PAN** (*Personal Area Network*): Red de Área Personal.

**Red WAN** (*Wide Area Network*): Red de Área Amplia, la cual se utiliza para conectar ciudades y países.

**Router**: es el dispositivo que administra y distribuye el servicio de internet a una red LAN que recibe del equipo del ISP.

**Servidor**: es un recurso informático que tiene como función dar respuesta a una petición realizada un cliente o usuario.

**SNMP** (*Simple Network Management Protocol*): Protocolo Simple de Administración de Red: es el protocolo que le permite a un administrador de red monitorear, resolver fallas y manipular los dispositivos que la componen.

**Software**: recurso informático no tangible.

**Streaming**: es un tipo de tecnología multimedia que permite visualizar y escuchar contenido de audio y video desde cualquier dispositivo con capacidad de acceso a internet, ya sea un celular, una *tablet*, una *laptop*, etc.

**Sucursal**: es una oficina perteneciente a una empresa, la cual es controlada y gestionada por su oficina matriz.

**Switch**: dispositivo de red que tiene como función conmutar la información que recibe del *router* hacia los dispositivos que tiene directamente conectados.

**TCP** (*Transmission Control Protocol*): Protocolo de Control de Transmisión. Se encarga de controlar, ordenar y manejar los datos, aseguràndose de que llegan a su destino sin que haya pèrdidas de los mismos.

**Terminal tonta**: es el término con el cuál se hace referencia a los dispositivos que sólo permitían la entrada y salida de datos, sin la capacidad de almacenar ni de procesar información.

**TI:** es la abreviatura del término Tecnologías de la Información, el cual se refiere al conjunto de *software*, *hardware* y redes utilizados para la manipulación y procesamiento de datos.

**UPS** (*Uninterruptible Power Supply*): Sistema de Fuerza Ininterrumpible, el cual es un dispositivo que almacena energía eléctrica para mantener encendidos los equipos que tiene directamente conectados en caso de que se tenga una falla en el suministro eléctrico. También es conocido como banco de baterías.

**VPN** (*Virtual Private Network*): Red Privada Virtual, la cual es una conexión cifrada que enlaza a un dispositivo remoto con una red privada o red local.

# CONCLUSIONES

Durante el estudio de la carrera de Ingeniería en Computación fui desarrollando la capacidad de solucionar problemas a partir del empleo del conocimiento científico y técnico, el cual se adquiere desde las asignaturas de ciencias básicas hasta los temas del módulo de salida, que en mi caso se refiere al módulo de redes y seguridad.

Esa capacidad se practica al emplearse en el campo laboral. Los años que llevo trabajando dentro del NOC me han permitido ir mejorando mis habilidades para cumplir con las dos principales funciones de mi puesto de trabajo: la solución de problemas presentes en las redes empresariales o en producción y el buen desempeño de las mismas. La solución de problemas me ha permitido identificar cuáles son los factores que más influyen en la afectación de las redes de los clientes, la cual impacta en el buen funcionamiento de la misma y por lo tanto en el servicio que el NOC se comprometió a proporcionarle al cliente al momento de que éste contratara sus servicios de gestión de red. Esta identificación de factores, al ser parte de la gestión de redes permite que al cliente se le propongan planes de mejora (implementación de soluciones) para que su red tenga un mejor desempeño. Esa gestión de problemas tiene como beneficio hacer que el cliente se dedique de lleno al giro para el que está hecho. Por ejemplo, una empresa que se dedica a la fabricación y venta de bebidas refrescantes en lugar de preocuparse porque la red de todas y cada una de sus sucursales o fábricas esté trabajando correctamente se va a dedicar de lleno a la promoción de su producto a diferentes clientes, desde personas hasta otras empresas con las que puede hacer convenio para hacer crecer su venta de bebidas. Esa empresa que fabrica bebidas refrescantes va a contratar a otra entidad que se encargue precisamente del buen funcionamiento de su red para no perder de vista su función.

Este puesto de trabajo me deja bases para que en algún futuro pueda desenvolverme en la implementación y diseño de redes, debido a que, al haber adquirido la habilidad para resolver problemas se tienen mejor identificados los componentes que interfieren en el buen funcionamiento de una red, desde el equipamiento hasta la infraestructura del proveedor.

# REFERENCIAS

**Libro**

Andrew S. Tanenbaum y David J. Wetherall, Redes de computadoras, México, Pearson educación, quinta edición, 2012, 816 páginas.

**Documento con autor empresarial**

Comité de Normas y Prácticas Corporativas, Unired. (2017). Código de ética Unired. El valor de lo que se debe ser… y hacer (cuarta edición). Ciudad de México

**Páginas Web:**

A. (2021, 8 abril). ¿Qué es Internet Satelital? NetworkingSat. https://networkingsat.com/blog/que-es-internet-satelital/

Altamirano, F. (2016, 19 abril). Centro de Operaciones de Red - NOC. Francisco Altamirano - Academia.edu. https://www.academia.edu/24568554/Centro_de_Operaciones_de_Red_NOC

Axess Networks. (2019). Tecnologia satelital VSAT: ¿Qué es y cómo funciona ?. Recuperado de https://axessnet.com/tecnologia-satelital-vsat-que-es/

Casos Prácticos de BGP. (2021, 10 septiembre). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

Certificación ITIL foundations V4. (s. f.). Informática integrada internetworking: Cursos en TI, redes, sistemas, seguridad, telecomunicaciones. http://informaticaintegrada.com.mx/dip_itil_v4.htm

Configuración de una red inalámbrica mediante un punto de acceso inalámbrico (WAP). (s. f.). Cisco. https://www.cisco.com/c/es_mx/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5530-set-up-a-wireless-network-using-a-wireless-access-point-wap.html

D. (2022, 16 febrero). Direccionamiento y subredes TCP/IP - Windows Client. Microsoft Docs. https://docs.microsoft.com/es-ES/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting

Diferencias entre Internet satelital e Internet por microondas – ENI Networks. (n.d.). Retrieved April 18, 2022, from https://www.eninetworks.com/blog-diferencias-entre-internet-satelital-e-internet-por-microondas/

Garces, D. (2013, 2 junio). Servicios y Tecnologías en Arquitecturas Carrier Ethernet. Servicios y Tecnologías en Arquitecturas Carrier Ethernet. https://gblogs.cisco.com/cansac/servicios-y-tecnologias-en-arquitecturas-carrier-ethernet/

Grup, I. D. (2019, 3 mayo). El efecto de las nuevas tecnologías en las empresas. ID Grup. https://idgrup.com/efecto-las-nuevas-tecnologias-las-empresas/

Kionetworks.com. (2021). ¿Cómo medir la latencia? . Recuperado de https://www.kionetworks.com/blog/data-center/c%C3%B3mo-medir-la-latencia

Los 3 modos de un access point. (s. f.). Share and Discover Knowledge on SlideShare. https://www.slideshare.net/MARIUXI29/los-3-modos-de-un-access-point

M. (2013, 17 septiembre). Historia de Internet - Nacimiento y evolución | Redes Telemáticas. Redes Telemáticas. https://redestelematicas.com/historia-de-internet-nacimiento-y-evolucion/

R. (2021, 10 junio). El soporte proactivo es el que mayor beneficios reporta a las redes. RCG Comunicaciones. https://rcg-comunicaciones.es/beneficios-del-soporte-proactivo/

Walton, A. (2021, 22 febrero). Tipos Comunes de Redes (LAN, WAN) ». CCNA desde Cero. https://ccnadesdecero.es/tipos-redes-informaticas-lan-wan-man/

TIPOS DE MEDIOS. (s. f.). Plataforma Virtual Educativa ITCA-FEPADE: Entrar al sitio. https://virtual.itca.edu.sv/Mediadores/irmfi1/IRMFI_04.htm

¿Qué es un router? Definición y usos. (2021, 18 octubre). Cisco. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html#%7Ehow-to-choose-small-business-routers.