Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

ANÁLISIS DE LAS VULNERABILIDADES EN EL SERVICIO DE NAVEGACIÓN EN UNA RED HFC

Keneht Josué Alexander Zacarías Velásquez
Asesorado por el Ing. Luis Fernando García Cienfuegos

Guatemala, septiembre de 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS DE LAS VULNERABILIDADES EN EL SERVICIO DE NAVEGACIÓN EN UNA RED HFC

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

KENEHT JOSUÉ ALEXANDER ZACARÍAS VELÁSQUEZ
ASESORADO POR EL ING. LUIS FERNANDO GARCÍA CIENFUEGOS

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, SEPTIEMBRE DE 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Luis Diego Aguilar Ralón
VOCAL V	Br. Christian Daniel Estrada Santizo
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

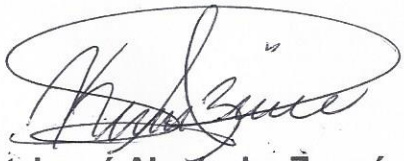
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
EXAMINADOR	Ing. Julio César Solares Peñate
EXAMINADOR	Ing. Otto Fernando Andrino González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS DE LAS VULNERABILIDADES EN EL SERVICIO DE NAVEGACIÓN EN UNA RED HFC

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 7 de noviembre de 2017.



Keneht Josué Alexander Zacarías Velásquez

Guatemala, 22 de Mayo de 2019

Ingeniero
Otto Fernando Andrino González
Director de la Escuela de Mecánica Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimado Ing. Andrino

Por medio de la presente hago constar mi aprobación del trabajo de graduación con título **"ANÁLISIS DE LAS VULNERABILIDADES EN EL SERVICIO DE NAVEGACIÓN EN UNA RED HFC"** elaborado por el estudiante de la carrera de Ingeniería Electrónica, Keneht Josue Alexander Zacarías Velásquez, quien se identifica con número de registro académico 200614801 y CUI 2283744720101.

Agradeciendo de antemano su atención a la presente.

Me suscribo a usted.

(f)_____
Luis Fernando Garcia Cienfuegos
Ingeniero Electrónico
Colegiado 8631

LUIS FERNANDO GARCÍA CIENFUEGOS
Ingeniero Electrónico
Colegiado No. 8631

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 28 de mayo de 2019

Señor Director
Ing. Otto Fernando Andrino González
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado **ANÁLISIS DE LAS VULNERABILIDADES EN EL SERVICIO DE NAVEGACIÓN EN UNA RED HFC,** desarrollado por el estudiante **Keneht Josué Alexander Zacarías Velásquez**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

FACULTAD DE INGENIERIA · UNIVERSIDAD DE SAN CARLOS DE GUATEMALA · DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA

Ing. Julio César Solares Peñate
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

REF. EIME 36. 2019.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto bueno del Coordinador de Área, al trabajo de Graduación de el estudiante: KENEHT JOSUÉ ZACARÍAS VELÁSQUEZ titulado: ANÁLISIS DE LAS VULNERABILIDADES EN EL SERVICIO DE NAVEGACIÓN EN UNA RED HFC, procede a la autorización del mismo.

Ing. Otto Fernando Andrino González

FACULTAD DE INGENIERÍA · UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA

GUATEMALA, 30 DE JUNIO 2019.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 383.2019

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **ANÁLISIS DE LAS VULNERABILIDADES EN EL SERVICIO DE NAVEGACIÓN EN UNA RED HFC,** presentado por el estudiante universitario: **Keneht Josué Alexander Zacarías Velásquez,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Anabela Cordova Estrada
Decana

Guatemala, septiembre de 2019

/gdech

ACTO QUE DEDICO A:

Dios	Por su gran amor al darnos a su único hijo para que por medio de él obtengamos la salvación y vida eterna.
Mis padres	Arnulfo Zacarías y Victoria Velásquez (q. e. p. d.), por su amor y apoyo incondicional para lograr este triunfo, en especial a mi madre por enseñarme a ser fuerte y valiente al enfrentar la vida; siempre estarás en mi corazón y en mis pensamientos toda mi vida, besos y abrazos hasta el cielo.
Mi hermano	Roberto Zacarías, por haberme cuidado siempre y brindarme su amistad, apoyo y cariño.
Mis sobrinos	Ariana y Roberto Zacarías, por alegrarme la vida con su compañía.
Mis tías	Lidia y Mely Velásquez, por el gran apoyo que le brindaron a mi madre hasta en sus últimos momentos.
Mi novia	Aleyda Flores, por su amor, paciencia y apoyo para lograr esta meta.

Mi cuñada Alba Pérez, por su gran apoyo incondicional.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudios que me brindó el conocimiento académico para realizarme como profesional.
Facultad de Ingeniería	Por haberme brindado la oportunidad de estudiar la especialidad de la electrónica.
Ing. Luis García	Por su gran amistad y enseñarme el ejemplo de caminar con Cristo.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
dB	Decibel
Hz	Hercio
Mbps	*Megabytes* por segundo
Msim/seg	Mega símbolos por segundo
sps	Símbolos por segundo

GLOSARIO

3DES	Triple estándar de cifrado de datos.
BPI	Interfaz de privacidad de línea base.
BPKM	Gestión de claves de privacidad de línea base.
CATV	Redes de televisión por cable.
CM	Cable módem.
CMTS	Sistema de terminación de cable módem.
DHCP	Protocolo de configuración dinámica de host.
Docsis	Especificación de interfaz para servicios de datos sobre cable.
FM	Frecuencia Modulada.
HFC	Híbrida de Fibra y Coaxial.
IP	Protocolo de Internet.
IPV6	Protocolo de Internet Versión 6.

LAN	Red de área local.
MAC	Control de acceso al medio.
MIB	Gestión de información de base.
OFDM	Multiplexión por división en frecuencias ortogonales.
OID	Identificador de objeto.
OSS	Sistema de soporte de operaciones.
QAM	Modulación de amplitud de cuadratura.
QoS	Calidad de servicio.
QPSK	Modulación por desplazamiento de fase cuadratura.
SNMP	Protocolo simple de administración de red.
TFTP	Protocolo de transferencia de archivo simple.

RESUMEN

En los últimos años las tecnologías han crecido exponencialmente, unificando arquitecturas tales como red de fibra y cable coaxial, esto con el fin de brindar un mejor servicio al consumidor final de Internet. Una de estas tecnologías es la red HFC, a medida que va aumentando el número de usuarios en esta red, también las personas mal intencionadas han buscado cómo vulnerar su seguridad para poder manipularla a su antojo y lo han encontrado.

Por tal motivo en este trabajo se realizará un estudio de los principales problemas de seguridad que presenta la red HFC en el servicio de Internet, estudiando su arquitectura, el estándar Docsis implementado y sus limitaciones, dando posibles soluciones a cómo implementar rutinas de control para disminuir el riesgo para que el usuario no se vea afectado con el servicio y la empresa proveedora no pueda tener pérdidas en sus ingresos.

OBJETIVOS

General

Identificar las posibles vulnerabilidades que afectan el servicio de Internet en una red HFC.

Específicos

1. Analizar el funcionamiento del servicio de Internet en una red HFC.

2. Analizar los diferentes tipos de vulnerabilidades de seguridad.

3. Analizar el estándar Docsis para la conexión de Internet.

4. Estudiar los esquemas de privacidad implementados por Docsis.

5. Analizar las posibles soluciones de los problemas de acceso en los sistemas de seguridad.

INTRODUCCIÓN

Las redes HFC son un conjunto de medios técnicos que permite la comunicación a distancia entre equipos para transmitir datos, audio y video a través de la unión de medios de fibra óptica y cable coaxial. Estas redes han evolucionado en los últimos años, expandiendo su cobertura geográficamente y permitiendo el acceso al Internet y la facilidad de obtener grandes anchos de banda a la disposición del cliente, siendo así una de las redes más rentables y flexibles.

Desde que se ha implementado la red para manejar las comunicaciones de banda ancha, multimedia y video, ha presentado debilidades en su seguridad y esto ha sido aprovechado por los *hackers* para vulnerar sus restricciones de seguridad, haciendo de ello un negocio rentable.

Debido al impacto que ha tenido el bajo nivel de seguridad que ha afectado a los usuarios y a las compañías proveedoras de servicio, se estará analizando el funcionamiento de la red HFC y sus diferentes métodos de acceso no autorizado, para brindar algunas medidas de prevención y seguridad básica viables para reducir el riesgo de que este problema continúe.

1. MARCO TEÓRICO

1.1. Redes Híbridas de Fibra Coaxial (HFC)

Las redes HFC (Híbrido de Fibra y Coaxial) en telecomunicaciones es un término que define una incorporación tanto de fibra óptica como de cable coaxial, para crear una red de banda ancha en la cual se puede obtener una capacidad de 1GHz de ancho de banda, esto ayuda a las grandes operadoras de cable a cubrir grandes distancias de una región geográfica, ya que puede transportar datos por fibra óptica y posteriormente a cableado coaxial, lo que permite al cliente tener una excelente calidad del servicio de TV por cable, Internet de alta velocidad y voz sobre IP.

Esta tecnología permite el acceso a Internet de banda ancha utilizando las redes CATV existentes. Se puede dividir la topología en dos partes. La primera consiste en conectar al abonado por medio de cable coaxial a un nodo zonal y posteriormente interconectar los nodos zonales con fibra óptica. Esta tecnología comienza a implementarse a través de operadores por cable, que además de brindar el servicio de televisión por cable anexaron transportar por el mismo medio la señal de Internet de banda ancha.

A través del uso de cada una de estas tecnologías, la red es capaz de aprovecharse de los beneficios y minimizar el impacto de las limitaciones inherentes a cada una.

Esta tecnología utilizada para abaratar el despliegue se lleva la fibra óptica hasta la central o nodo y después llega a casa de los clientes con cable coaxial

como el que se usa para conectar la antena de televisión. Esta tecnología permite altas velocidades y se cataloga como red de nueva generación.

Con la fusión entre la tecnología de fibra y la ya conocida de cable coaxial, es posible encontrar una plataforma que se define como una red de multiservicios en la cual se puede encontrar:

- Internet
- Telefonía fija
- Telefonía móvil
- Videollamadas
- Distribución de TV analógica y digital
- Distribución de canales de radio FM
- Servicio Pay Per View y video de baja demanda
- Servicio de videojuegos interactivos
- Bases de datos
- Videotelefonía o videoconferencia
- Comercio electrónico
- *E-learnig*
- Telemetría
- Telefonía IP

Las redes HFC por su estructura pueden tener un arreglo topológico según la necesidad del servicio a prestar.

La topología es un arreglo físico o lógico donde los dispositivos o nodos de una red se conectan sobre un medio de comunicación, como lo puede ser computadora, servidores, entre otros. La topología determina la forma de comunicación entre sus dispositivos. Existen arreglos de redes donde la

intercomunicación entre sus dispositivos es muy sencilla y otras donde es muy compleja. La mala decisión al elegir una topología puede ocasionar que la red no opere de manera eficaz. Una topología puede determinar el número de dispositivos que se conectarán en su red, dependiendo de cuáles sean los requerimientos que se desean implementar.

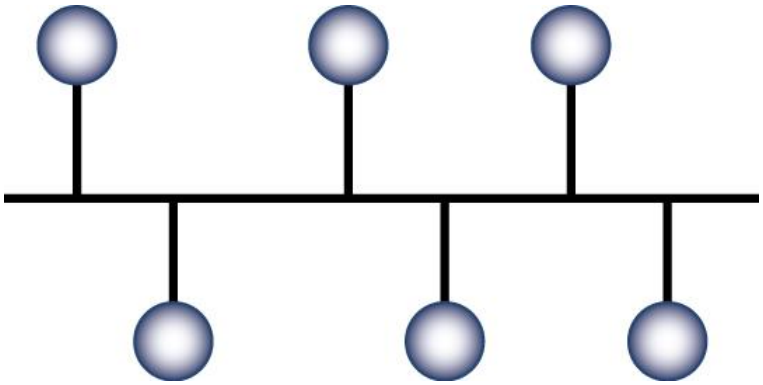
Las topologías pueden ser de dos tipos:

- Topología física: es el diseño físico del medio de transmisión de la red.
- Topología lógica: es la implementación de la transferencia de información en la red.

Las topologías físicas más comunes son:

- La topología de bus está caracterizada por contar con un único canal principal de comunicación entre los dispositivos de red interconectados a lo largo del canal. Estos arreglos son considerados como topologías pasivas. Las computadoras escuchan al bus, cuando estas están listas para transmitir se aseguran de que no haya otro dispositivo transmitiendo en ese instante, entonces envían sus paquetes de información. Estas redes comúnmente utilizaban cable coaxial como medio físico. Estas son las más utilizadas por la facilidad de instalación y bajo costo.

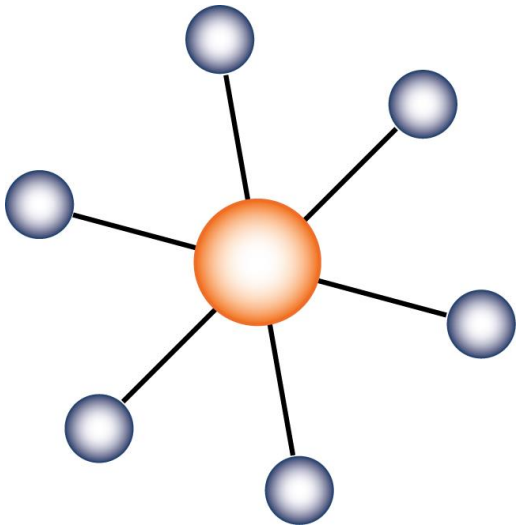
Figura 1. **Topología de bus**



Fuente: MARTÍNEZ, Evelio. *Topologías de red*. http://eveliux.com/mx/curso/topolog.html. Consulta: 17 de noviembre de 2018.

- En una topología de estrella los ordenadores en la red se conectan a un punto central conocido como concentrador *hub* o a un conmutador de paquetes *switch.* Cada ordenador se conecta con su propio cable normalmente con par trenzado, que va conectado a un puerto del dispositivo central elegido. Este tipo de red sigue siendo pasiva. La desventaja más grande de este arreglo es que si el dispositivo central falla, toda la red estará fuera.

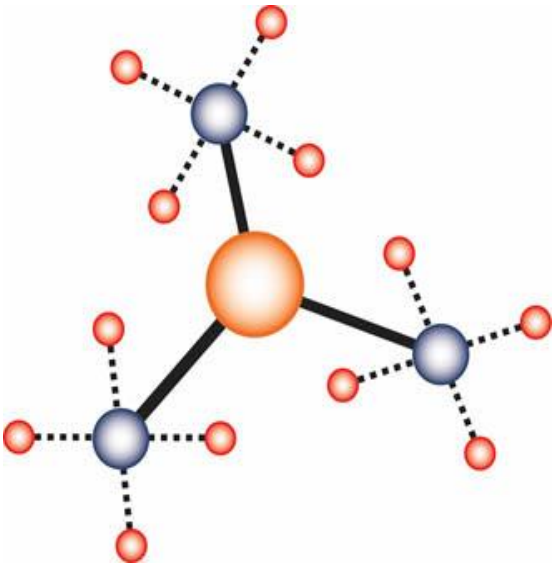
Figura 2. **Topología de estrella**



Fuente: MARTÍNEZ, Evelio. *Topologías de red*. http://eveliux.com/mx/curso/topolog.html. Consulta: 23 de noviembre de 2018.

- La topología estrella extendida es parecida a la de estrella con la diferencia de que cada nodo se conecta con el nodo central, en un ambiente LAN es muy fácil de configurar, de costo accesible y tiene más redundancia que la topología de bus. Con este arreglo se permite extender la longitud y el tamaño de la red. También reduce la probabilidad de fallo en esta.

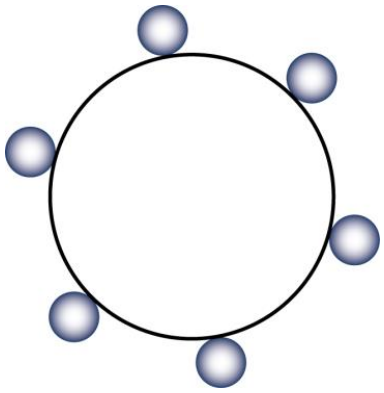
Figura 3. **Topología de estrella extendida**



Fuente: MARTÍNEZ, Evelio. *Topologías de red*. http://eveliux.com/mx/curso/topolog.html. Consulta: 23 de noviembre de 2018.

- Una topología de anillo conecta los ordenadores de red uno seguido de otro sobre el mismo cable en un círculo físico. Este arreglo de anillo envía información sobre el cable en una dirección y es considerada como una topología activa, los ordenadores en la red retransmiten los paquetes de información que reciben y los envían al siguiente ordenador en la red, el acceso al medio de la red es otorgado a un ordenador en particular por medio de un *token* o paquete de datos, este circula alrededor del anillo y cuando una computadora desea enviar datos espera al *token*, la computadora entonces envía los datos sobre el cable. La computadora destino envía un mensaje a la computadora que envió los datos que ya fueron recibidos correctamente.

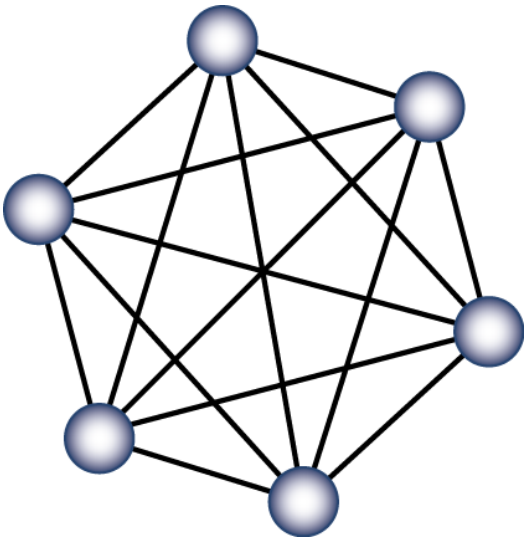
Figura 4. **Topología de anillo**



Fuente: MARTÍNEZ, Evelio. *Topologías de red*. http://eveliux.com/mx/curso/topolog.html. Consulta: 1 de diciembre de 2018.

- La topología de malla es la que utiliza conexiones redundantes entre los dispositivos de la red, este arreglo no requiere un nodo central como en algunas de las anteriores topologías, cada dispositivo en la red está conectado a todos los demás, este tipo de tecnología requiere mucho cable si fuera la conexión física, pero también podría ser inalámbrico y con esto hay costos de mantenimiento. Pero debido a la redundancia, este arreglo puede seguir operando si una conexión llegara a fallar. La información únicamente es enviada a los dispositivos que se encuentran conectados evitando colisiones.

Figura 5. **Topología de malla**



Fuente: MARTÍNEZ, Evelio. *Topologías de red*. http://eveliux.com/mx/curso/topolog.html. Consulta: 1 de diciembre de 2018.

- Las topologías híbridas son de las más comunes y se derivan de la combinación de dos o más arreglos en una misma red. La implementación de esta topología se debe a la complejidad de la solución de la red o bien al número elevado de dispositivos conectados. Esta topología tiene un elevado costo debido a los requerimientos de administración y mantenimiento. Algunas de las combinaciones de arreglos podrían ser la de bus-estrella o estrella-estrella.

Las topologías lógicas describen cómo los dispositivos de red acceden a través de las topologías físicas, es decir cómo los dispositivos simultáneamente ingresarán al medio de comunicación de una manera ordenada, existen dos tipos de topologías lógicas:

- Topología con medio compartido: este arreglo establece que todos los dispositivos tienen la habilidad de acceder en cualquier momento al medio de comunicación compartido. Esto puede ocasionar colisiones en la red debido a que dos más nodos puedan transmitir al mismo tiempo y por lo tanto se puedan perder paquetes de información y se deba enviar nuevamente hasta que no haya colisiones. Esto puede funcionar para redes pequeñas, para mejor funcionamiento se recomienda segmentar las redes con números pequeños de nodos. Estas pueden ser típicamente implementadas en topologías físicas, como bus, estrella o híbridas.

- Topología basada en *token:* este arreglo funciona utilizando un paquete *token* para proveer acceso al medio físico, lo cual recorre en un orden lógico en la red. Para que un dispositivo pueda transmitir o recibir información, es necesario obligadamente tener el *token* en su poder para poder hacerlo en ese momento. Una de las principales desventajas es la espera de tiempo para que el *token* pueda recorrer toda la red y llegue nuevamente al nodo para que pueda volver a transmitir.

Los medios de transmisión son los elementos físicos por donde se transporta la información, haciendo que llegue con la menor cantidad de señal de ruido y distorsión a todos los elementos que involucran la red de comunicación. A nivel de campo deben permitir bastante flexibilidad en cuanto a manejo físico del mismo y al incremento del número de elementos de manera simple.

Una de las principales características de un medio de transmisión guiado es la existencia de un cable físico en una envoltura de uno o más hilos conductores eléctricos u ópticos.

Depende de la forma de conducir la señal a través del medio, estos medios de transmisión guiados pueden ser:

- Par trenzado
- Cable coaxial
- Fibra óptica

En lugares donde resulta complicado instalar un tendido de cable es recomendable utilizar un enlace inalámbrico. Actualmente este tipo de enlaces está teniendo un gran auge debido a la implementación de sistemas de enlace como Wifi y Bluetooth, que resuelven las comunicaciones entre dispositivos en distancias cortas. También hay enlaces mediante medios no guiados generalmente usados para cubrir largas distancias punto a punto.

La transmisión de datos mediante enlaces no guiados puede ser:

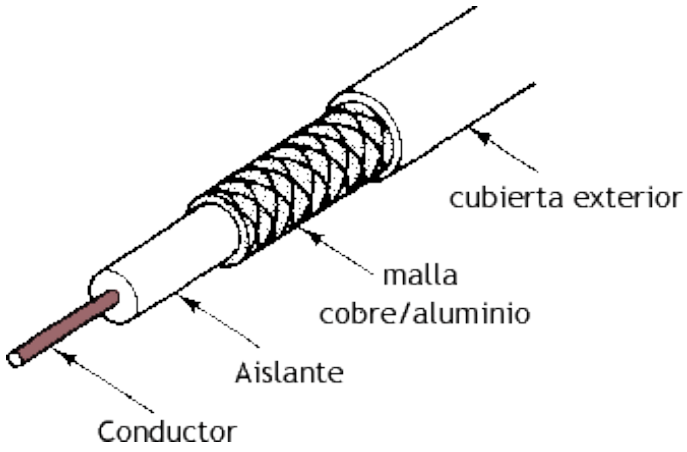
- Radiofrecuencia
- Microondas
- Luz (infrarrojos, láser)

El cable coaxial está formado por un núcleo de cobre rodeado de material aislante y un conductor exterior trenzado denominado comúnmente malla, se dispone en una estructura concéntrica. Cubriendo a todo el conjunto se encuentra externamente una cubierta protectora de material plástico. La capa exterior evita que las señales de otros cables o que la radiación electromagnética afecten la información conducida por el cable coaxial.

El cable coaxial es tal vez el medio de transmisión más adaptable, por lo que está siendo cada vez más utilizado en las redes de telecomunicaciones,

especialmente en las redes de TV por cable. Se usa para trasmitir señales analógicas y digitales. El cable coaxial tiene una respuesta en frecuencia superior a la del par trenzado, permitiendo por tanto mayores frecuencias y velocidades de transmisión.

Figura 6. **Estructura genérica de un cable coaxial**



Fuente: MARTÍNEZ, Evelio. *Cable coaxial*. http://eveliux.com/mx/curso/cable-coaxial.html. Consulta: 1 de diciembre de 2018.

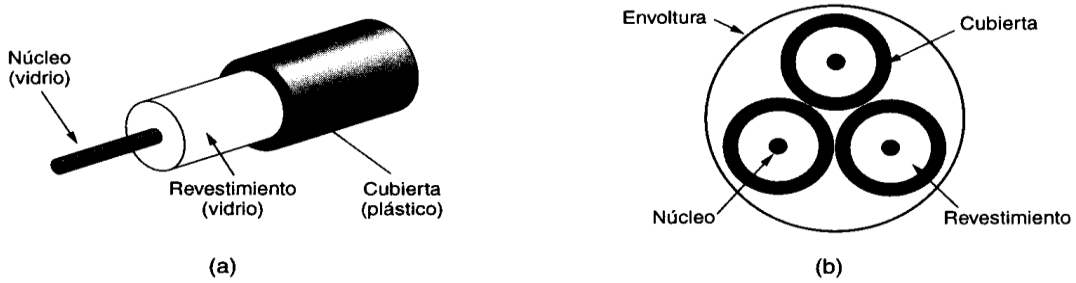
La fibra óptica está construida por un núcleo muy fino de fibra de vidrio circular, que al tener un elevado índice de refracción permite conducir la energía óptica en su interior. Este núcleo está envuelto por un recubrimiento opaco de aísla la fibra óptica de posibles interferencias.

La fibra óptica es un medio flexible y fino capaz de confinar un haz de naturaleza óptica. Para construir la fibra se puede usar diversos tipos de cristales y plásticos. Las pérdidas menores se han conseguido con la utilización de fibras de silicio fundido ultrapuro. Las fibras ultrapuras son muy difíciles de

fabricar, las fibras de cristal multicomponentes son más económicas y proporcionan unas prestaciones suficientes.

La fibra se basa en la propagación de ondas electromagnéticas de frecuencias luminosas gracias a su reflexión interna en las paredes de fibra de materiales muy transparentes. Las señales luminosas se transmiten a través de un cable guía compuesto por fibra de vidrio con un alto índice de refracción, rodeado de una capa de material similar con un índice de refracción ligeramente menor.

Figura 7. **Estructura de fibra óptica**



Fuente: FERNÁNDEZ, Manuel. *Medios de transmisión*. p. 19.

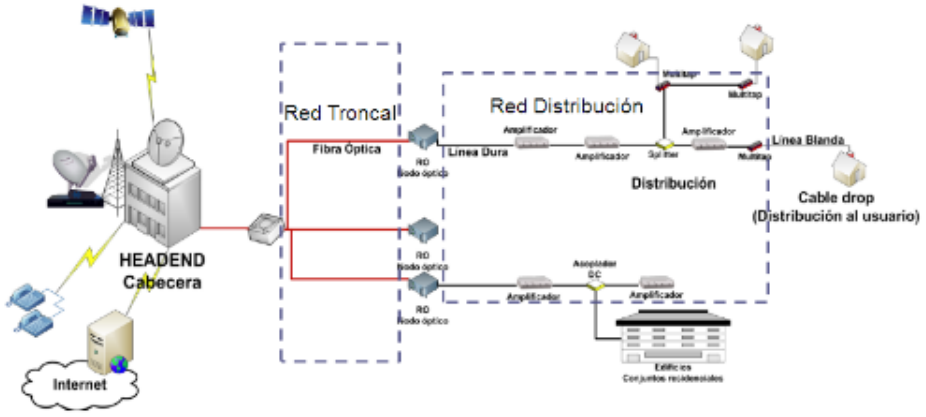
1.2. Estructura de la red HFC

Esta estructura de HFC representa la evolución de las redes clásicas de televisión por cable (CATV) que combinan la velocidad y confiabilidad de la fibra óptica y la economía y ancho de banda del cable coaxial para la transmisión de datos, imágenes y voz con alta fidelidad y flexibilidad de servicios.

Una red de HFC está compuesta básicamente por:

- Cabecera de red
- Red troncal
- Red de distribución

Figura 8. **Diagrama de estructura de una red HFC**



Fuente: *Tecnologías de telecomunicaciones*. https://es.slideshare.net/william2475/tecnologia-para-la-transmision-de-datos-cable-modem. Consulta: 1 de diciembre de 2018.

La cabecera en la red HFC es la parte central desde donde se controla todo el sistema. A menudo dispone de una serie de antenas que reciben las señales de los canales de televisión y radio de los diferentes sistemas de distribución, así como de enlaces de comunicación de otras cabeceras o estudios de televisión. También tiene otros tipos de redes que aportan información capaz de ser distribuida a los clientes a través del sistema de cable.

Originalmente las redes de CATV fueron diseñadas para la distribución de señales de TV en una sola dirección, por lo que la cabecera era simplemente un concentrador que recogía las señales de TV y las adaptaba a su transmisión por medio de su red de cable.

Dentro las principales funciones de la cabecera están:

- Recolectar las señales digitales de video, datos y RF.

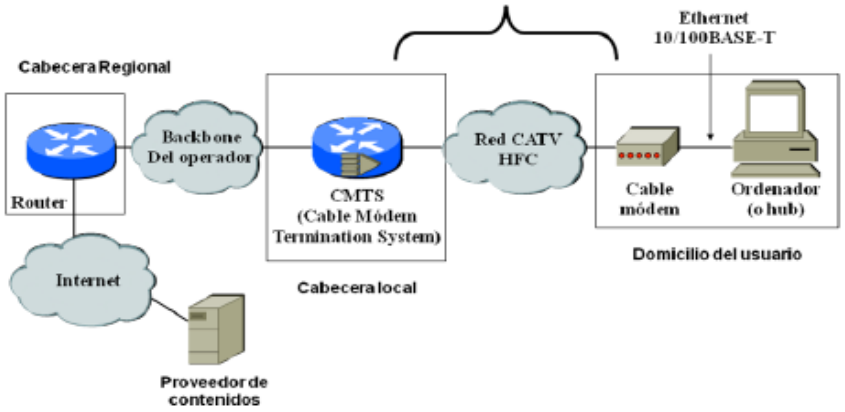
- Entrega de señales satelitales analógicas y digitales, difusión de RF, video pregrabado, microondas AM y FM, video de banda base, datos y telefonía.

- Combinar las señales (intercaladas) para la entrada en el sistema de distribución.

El sistema de terminación de módem de cable conocido como CMTS proporciona conectividad de datos y funcionalidad complementaria a los módems de cable a través de la red de acceso HFC. También proporciona conectividad a redes de área amplia, es utilizado para proveer servicios de datos de alta velocidad como Internet por cable o voz sobre IP. El CMTS es el encargado de recibir todo el tráfico de Internet y permite distribuirlo por cable hacia todos los abonados. El CMTS se encuentra en la cabecera del sistema de televisión por cable o en el centro de distribución.

Desde la red HFC al equipo CMTS llegan 4 canales ascendentes que son distribuidos por los clientes del servicio, mientras que desde el CMTS parte un canal descendente hacia el cable módem. Este equipo determina las políticas y mensajes para que se produzcan los eventos dentro de la red.

Figura 9. **Diagrama de ubicación CMTS en la red HFC**



Fuente: *Redes HFC*. https://docplayer.es/12961354-Introduccion-1-redes-hfc-hybrid-fiber-coaxial.html. Consulta: 5 de diciembre de 2018.

La mayoría de CMTS tienen conexiones con puertos Ethernet (u otras interfaces de alta velocidad más tradicionales) como interfaces RF, de esta forma el tráfico que llega de Internet puede ser direccionado mediante la interfaz Ethernet, a través del CMTS y después a las interfaces RF que están conectadas a la red HFC de la compañía de cable. El tráfico viaja por la red HFC para terminar en el módem de cable del domicilio del cliente. Obviamente, el tráfico que sale del domicilio del abonado pasará por el cable módem y saldrá a Internet siguiendo el camino contrario.

El CMTS es responsable de asignar y programar el ancho de banda ascendente y descendente de acuerdo con las solicitudes del CM y las autorizaciones de QoS establecidas por el controlador de puerta.

Algunas características de los equipos de CMTS son:

- Los CMTS manejan tráfico IP hacia el cable módem.
- El CMTS provee al equipo del cliente una dirección IP mediante un servicio DHCP (protocolo de configuración de *host* dinámico).
- El CMTS asigna un *gateway* al cable módem para acceder al servidor DNS (Domain Name System).
- El CMTS puede funcionar como un puente (*bridge*) o enrutador (*router*).
- La fusión de la programación de TV se alimenta con los datos de radiofrecuencia de un CMTS.
- Proporciona calidad de servicio (QoS) requerida al CM en función de las solicitudes de Docsis que se verifican en las políticas.
- Asigna un ancho de banda ascendente de acuerdo con las solicitudes de CM y las políticas de QoS de la red.
- Clasificar cada paquete que llega desde la interfaz de la red troncal y asignarlo a un nivel de QoS según las especificaciones de filtro definidas.

La red troncal en la red HFC es la encargada de distribuir la señal compuesta generada por la cabecera a todas las arterias principales de distribución de la red de cable y que va adquiriendo diferentes topologías. En esta es posible encontrar la evolución de las redes clásicas todo coaxial de CATV con varias alternativas como las híbridas de fibra coaxial a nivel de

diseño en las redes de telecomunicaciones por cable. A medida que fueron evolucionando las redes HFC se tuvo que sustituir las largas cascadas de amplificadores y el cable coaxial de la red troncal por enlaces punto a punto de fibra óptica.

Posteriormente, la introducción de la fibra en la red de cable ha ido en aumento y la red troncal se ha convertido en una estructura con anillos redundantes que unen nodos ópticos entre sí. Estos nodos donde se encuentran las señales ópticas procedentes de la fibra y posteriormente convertida a eléctrica, que es la señal descendente, van hacia el hogar del cliente a través de la red de distribución de coaxial. En los sistemas bidireccionales los nodos ópticos también se encargan de recibir las señales del canal de retorno o ascendentes (del cliente a la cabecera) para convertirlas en señales ópticas y transmitirlas a la cabecera.

La red de distribución es la encargada de llevar la señal de banda ancha desde la red troncal hasta los clientes. Está compuesta por una estructura tipo bus coaxial que lleva las señales descendentes hasta la última derivación antes del hogar del cliente. En el caso de la red HFC normalmente la red de distribución contiene un máximo de 2 ó 3 amplificadores de banda ancha y abarca grupos de unas 500 viviendas.

En otros casos la fibra óptica de la red troncal llega hasta el pie de un edificio, de ahí sube por la fachada del mismo para alimentar un nodo óptico que se instala en la azotea y este parte el coaxial hacia el grupo de edificios a los que alimenta.

2. ESTÁNDAR DOCSIS

2.1. Estudio del estándar Docsis

La especificación Docsis (*data over cable service interface specification*) es un conjunto de estándares aprobado por *CableLabs* (Cable Television Laboratories) que garantiza la interoperabilidad de la tecnología empleada en la transmisión de datos a una alta velocidad sobre una red de cable.

La rápida comunicación de datos se ha convertido en la necesidad básica del mundo actual e Internet se ha convertido en el corazón del ecosistema de comunicación, de dispositivos como los teléfonos móviles, computadoras portátiles, entre otros. Tienen necesidad de conectividad hacia Internet, que principalmente se usa para navegar por la web, ahora también se están utilizando para la comunicación por voz. Así que las tecnologías convergen o se mezclan para proporcionar una comunicación accesible, rápida y fácil.

Lo mismo sucedió con la infraestructura de televisión por cable que inicialmente se configuró para recibir señales de televisión del operador de cable a los suscriptores de la casa. La necesidad de transmitir y recibir datos o paquetes IP se hizo sentir en la infraestructura de televisión por cable existente.

Algunos módems de cable fueron diseñados por proveedores para satisfacer esta necesidad, pero la falta de interoperabilidad fue un problema importante con el que se tuvieron que enfrentar. Para estandarizar la infraestructura de televisión por cable que soporta el flujo de datos IP (desde

Internet a módem por cable y viceversa), la tecnología Docsis entró en existencia.

CableLabs se encarga de certificar al equipo que cumpla las especificaciones y normas que indica Docsis, garantizando su adecuado funcionamiento en las redes de cable que adoptaron el estándar. El proceso de desarrollo comenzó a mediados de la década de los 90, en 1997 se publicó la primera versión de Docsis, dos años después se certificó el primer equipo que cumplía con la especificación modificada (versión 1.1) y en el año 2001 se publicó la versión 2.0.

La versión de Docsis 3.0 se presentó al mercado en el primer semestre del 2006, la versión 3.1 apareció en el año 2014. Este se convirtió en el estándar en donde se desarrollaría la mayoría de las innovaciones tecnológicas de la industria de cable.

La llegada de Internet potenció la capacidad bidireccional de las redes HFC en el año de los 2000, Docsis evolucionó durante más de una década tratando de seguir los cambios de la demanda que exigía año con año mayores velocidades de acceso, de esta manera el estándar protegió la inversión que los operadores de servicios por cable hicieron para reconstruir sus redes.

Docsis define un canal de subida y uno de bajada que permite la comunicación bidireccional entre un sistema de terminación de módem de cable (CMTS) en la cabecera y un cable módem (CM) del cliente.

La señal descendente o de bajada conocida como *downstream* combina frecuencias que salen de la cabecera de red, es entregada a los transmisores ópticos encargados de convertir la señal eléctrica en ópticas, para ser

encaminadas a *hubs* o a nodos ópticos de acuerdo al diseño estructurado que se tiene en la red HFC.

La transmisión de bajada permite modulaciones 64-QAM y 256-QAM sobre canales de 6 Mhz de ancho de banda, en el esquema 64-QAM la máxima tasa nominal de transferencia de datos que puede alcanzarse es de aproximadamente 27 Mbps.

Se considera tasa nominal de transferencia de datos a la transmisión relacionada con la detección y corrección de errores, mientras que la tasa total de transferencia representa la misma transmisión, pero sin tomar en cuenta los errores que se presentan en la red. La tasa de transferencia de símbolos es otra medida relacionada a la transmisión de datos que representa el número de símbolos que pueden ser enviados.

Debido a que un símbolo puede tener diferentes estados, este estará formado por más de un bit, razón por la cual la tasa de transferencia de símbolos es menor a la tasa de datos. Como podrá observarse, 64-QAM utiliza símbolos de 6 bits y como consecuencia, su tasa de transferencia de símbolos será de aproximadamente 5 Msím /seg.

En la modulación 256-QAM, 8 bits constituyen un símbolo, lo que representa una transmisión de aproximadamente 5,3 Msím/seg, equivalente a una tasa máxima total de transferencia de datos de 42,88 Mbps y una tasa nominal máxima de aproximadamente 38 Mbps. Como se ha dicho anteriormente la transmisión de bajada ocupa un canal de 6 MHz de ancho de banda dentro de un rango de frecuencias de 50 a 860 MHz, correspondiente al espectro *downstream* del cable.

En términos de retraso para la transmisión en dirección al usuario se considera aceptable un tiempo máximo de 0.8 ms para el tráfico entre la cabecera y el CM del suscriptor más alejado. La relación portadora a ruido se refiere a la razón, expresada en decibeles, entre el nivel de la portadora de la señal y el nivel del ruido, Docsis indica que esta relación no deberá ser menor a 35 dB para la transmisión de bajada.

Tabla I. **Características de QAM *dowstream***

Parámetro	**Formato 64 QAM**	**Formato 256 QAM**
Modulación	64 QAM, codificación rotacionalmente invariante	256 QAM, codificación rotacionalmente invariante
Separación de canales	6 MHz	54 a 860 MHz
Velocidad de símbolo	5,056941 Msps	5,360537 Msps
Banda de transmisión	54 a 860 MHz	54 a 860 MHz
Velocidad binaria de información	26,97035 Mbps	38,81070 Mbps

Fuente: *Cable Television Laboratories*. https://www.cablelabs.com/. Consulta: 20 diciembre de 2018.

La señal de canal ascendente o de subida conocida como *upstream,* proveniente de los clientes a la red, llega a través de la red de distribución al nodo óptico, el cual recibe la señal eléctrica entregada por el cable coaxial y la convierte en señal óptica, esta señal es llevada a un *hub* en donde se recibe y transmite nuevamente a la cabecera en donde se convierte en señal eléctrica, en la red troncal el canal de bajada y el de subida viajan por caminos separados.

En la transferencia de canal ascendente, Docsis acepta dos formatos de modulación QPSK y 16-QAM y cinco diferentes tasas de transferencia de símbolos, relacionados con el ancho de banda del canal que se ocupa. Para un canal de 0,2 MHz de ancho de banda, la tasa de transferencia de símbolos será de 160 ksím/seg, lo que representa una tasa nominal de datos para modulación QPSK de aproximadamente 0,3 Mbps y de 0,6 Mbps para 16-QAM.

La presencia de pertubaciones de mayor magnitud se evidencia en las frecuencias menores a 15 Mhz, razón por la cual se trata de evitar el uso de dichas frecuencias, es importante tener en cuenta que la relación portadora a ruido no deberá ser menor a 25 dB, y el retraso entre el CM más alejado y el CMTS o CM más cercano no podrá exceder 800 ms.

Figura 10. **Asignación de frecuencia**

Fuente: VOLPE, Brady. *Docsis y cable módem*. https://volpefirm.com/docsis101_rf-fundamentals/. Consulta: 15 de diciembre de 2018

El estándar Docsis se crea con la finalidad de desarrollar sistemas de comunicaciones en los que los operadores de cable puedan transmitir a grandes velocidades una amplia gama de servicios haciendo uso de paquetes de datos en la red HFC, en la cual durante este tiempo se han ido mejorando

las versiones para un mejor desempeño en la red y en la velocidad de navegación.

Como se mencionaba anteriormente en marzo de 1997 se define la primera especificación de Docsis, la cual fue la versión 1.0 que incluía elementos funcionales de anteriores productos de cable módem y se define como servicio de acceso a Internet para los clientes.

Las principales características de la versión Docsis 1.0 son:

- Especificación base
- Acceso a Internet de alta velocidad
- No soporta especificaciones de calidad de servicio (QoS)
- Transferencia de datos *downstream* 27Mbps o 40Mbps
- Frecuencia de *downstream* 88-860 MHz
- Ancho de canal de *downstream* 6MHz
- Modulación de *dowstream* 64QAM y 256QAM
- Transferencia de datos *upstream* 320Kbps hasta 10Mbps
- Frecuencia de *upstream* 5-42MHz
- Ancho de banda de canal 0,2 hasta 3,2 MHz en 5 intervalos
- Modulación para *upstream* QPSK y 16QAM

La versión Docsis 1.1 surge en abril de 1999, en donde se establece la especificación estandarizada de calidad del servicio (QoS) y seguridad.

Las principales características de la versión Docsis 1.1 son:

- Telefonía IP.
- Soporte de QoS.

- Disminuir retardos e incrementar la utilización de ancho de banda *upstream.*
- Mismas velocidades de Docsis 1.0.

La versión Docsis 2.0 fue lanzada en diciembre del 2001, fue revisada para mejorar las velocidades de transmisión de retorno, esto se debió al aumento de la demanda de servicios simétricos, como la telefonía IP.

Las principales características de la versión Docsis 2.0 son:

- Servicios simétricos.
- Incremento del ancho de banda en *upstream* y agrega módulo 64 QAM.
- Mejora la eficiencia espectral.
- Velocidad de *downstream* no cambia.
- Se triplica la velocidad de *upstream* 30 Mbps.
- Es compatible con Docsis 1.x.
- Servicios IP *multicast*.
- Mayor inmunidad al ruido y la interferencia.
- Agrega codificación S-CDMA (acceso múltiple por división de código sincronía).

La versión de Docsis 3.0 fue lanzada en marzo del 2006, la especificación fue revisada para aumentar significativamente la velocidad de trasmisión, la fortaleza de esta versión radica básicamente en dos importantes innovaciones: la unión de canales y el soporte de IPv6, el protocolo de Internet de próxima generación.

El cable módem escucha varias portadoras descendentes y no solo una como ocurría en las versiones anteriores de Docsis, las tramas descendentes y

de retorno se mezclan en diferentes frecuencias. La unión de canales es también de gran importancia en esta versión, el término se refiere a que los datos se transmitirán desde y hacia los módems de cable utilizando múltiples canales de RF en vez de uno solo, como solía hacerse en las dos versiones anteriores de Docsis.

Los canales no están físicamente unidos para transmitir la señal modulada digitalmente, sino que se unen de manera lógica para ensanchar el canal de comunicación. En el CMTS se distribuye la información para que viaje por diferentes canales y en el cable módem se recolecta y se ordena.

Las principales características de la versión Docsis 3.0 son:

- Permite agrupar varios canales para alcanzar velocidades más altas (*channel bonding*).
- Rompe vinculación física que existía entre puertos de *upstream* y *downstream*.
- Habilita módulo 128 QAM para el *upstream*.
- Incorpora soporte IPV6.
- Servicios avanzados, multimedia y en tiempo real.
- Mejora las técnicas de encriptación.

La versión de Docsis 3.1 fue lanzada en octubre de 2013, actúa como un turbo para las redes de cable, sus mejoras técnicas permiten a los operadores

aumentar significativamente el rendimiento de sus redes de cable en el enlace descendente y ascendente sin tener que realizar costosas modificaciones en la infraestructura de red HFC.

El estándar Docsis 3.1 cubre los distintos anchos de banda de Europa, América o Asia. Y puesto que es compatible de forma retroactiva, facilita la transición al estado más actual y reduce así al mínimo los gastos y el riesgo de los operadores.

Las principales características de la versión Docsis 3.1 son:

- Rompe la atadura con la vieja canalización de 6 MHz que Docsis tomó como legado de la TV analógica.
- Mejora la eficiencia espectral.
- Capacidad de apoyo de al menos 10Gbps de bajada y 1Gbps de subida.
- Múltiples perfiles de modulación.
- Habilita nuevos rangos de frecuencia.

Este estándar ha evolucionado conforme ha surgido la necesidad de las innovaciones tecnológicas y de las telecomunicaciones, aumentando considerablemente la velocidad de transmisión de datos en ambos sentidos y así mismo implementando protocolos de seguridad y calidad de servicio, modulaciones, anchos de banda, entre otros.

Tabla II. **Comparación de velocidades de Docsis**

Versión	**Servicio**	***Downstream***	***Upstream***
Docsis 1.0	Acceso a Internet de alta velocidad	40Mbps	10Mpbs
Docsis 1.1	Telefonía VoIP	40Mbps	10Mpbs
Docsis 2.0	Servicios simétricos	40Mbps	30Mbps
Docsis 3.0	Servicios avanzados, multimedia	480Mbps	120Mbps
Docsis 3.1	Videos 4K y 3D	10Gbps	2.5Gbps

Fuente: elaboración propia.

Tabla III. **Comparación de modulación de Docsis**

Versión	**Modulación**	
	Dowstream	***Upstream***
Docsis 1.0	64/256-QAM	QPSK/16-QAM
Docsis 1.1	64/256-QAM	QPSK/16-QAM
Docsis 2.0	64/256-QAM	QPSK/64-QAM
Docsis 3.0	64/256-QAM	QPSK/64-QAM
Docsis 3.1	4096 QAM OFDM/TDMA	4096 QAM OFDM/TDMA

Fuente: elaboración propia.

Tabla IV. **Comparación de canal de RF de Docsis**

Versión	**Canal de RF**	
	Dowstream	***Upstream***
Docsis 1.0	6MHz	200KHz - 3.2MHz
Docsis 1.1	6MHz	200KHz - 3.2MHz
Docsis 2.0	6MHz	200KHz - 3.2MHz
Docsis 3.0	Canal múltiple 6MHz	Canal múltiple 6.4MHz
Docsis 3.1	24MHz - 192MHz	24MHz - 192MHz

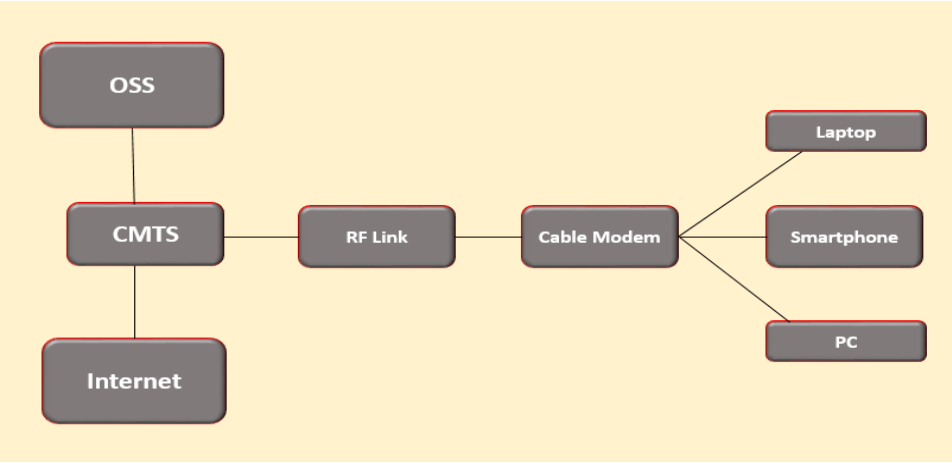
Fuente: elaboración propia.

2.2. Topología de las redes Docsis

Una topología Docsis incluye dos componentes fundamentales: un cable módem CM ubicado en las instalaciones del cliente y un CMTS ubicado en la cabecera de televisión por cable o nodo.

El CMTS es el dispositivo típico que alberga los puertos de bajada y subida. Si bien las comunicaciones aguas abajo y aguas arriba de viaje se dan en una línea compartida coaxial en las instalaciones del cliente, la principal función del CMTS es hacer un puente entre la red HFC y la red IP, en este equipo se encuentran conectados todos los módems de cable, conforme el tiempo transcurre estos equipos siguen evolucionado para obtener nuevas funciones.

Figura 11. **Topología de una red Docsis**



Fuente: elaboración propia, empleando PowerPoint 2010.

En una topología básica de Docsis se encuentran los siguientes elementos:

- Dispositivos conectados al CM.

- El CM se encuentran ubicado físicamente en el domicilio del cliente.

- CMTS en el extremo del operador de cable ubicado en la cabecera de la red HFC.

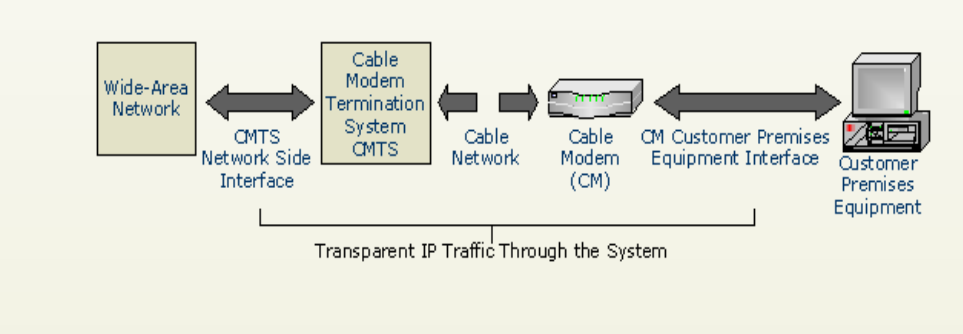
- La comunicación entre el CM y el CMTS es a través de la red HFC.

- La red de Internet y otros servidores están conectados con el CMTS.

- El OSS (Operation Support Service) conocido comúnmente como el sistema de aprovisionamiento, en donde se encuentran los servidores DHCP, TFTP, DNS y ToD, que proveen la configuración a los módems de cable.

- El flujo de datos entre los equipo es bidireccional, se conducen sobre las rutas conocidas como canal de subida y canal de bajada.

Figura 12. **Flujo de datos en una topología Docsis**



Fuente: *Cable Television Laboratories*. https://www.cablelabs.com/. Consulta: 5 enero de 2019.

2.3. Funcionamiento de cables módems

Un cable módem es un tipo especial de dispositivo diseñado para modular las señales de datos sobre una arquitectura de televisión por cable. El concepto de Internet por cable indica que hay una distribución de un servicio de conectividad hacia Internet sobre esta infraestructura de telecomunicaciones.

El cable módem se utiliza principalmente para que el cliente pueda tener el acceso a Internet de banda ancha, aprovechando las características de ancho de banda que no se utiliza en la red de televisión por cable. Los clientes de una misma zona comparten el ancho de banda proporcionado por una única línea de cable coaxial.

Una gran debilidad de las redes por cable al usar una línea compartida con varios usuarios es el riesgo de la pérdida de privacidad, especialmente considerando la disponibilidad de herramientas de *hacking* para cables módems. De este problema se encarga la encriptación de datos y otras características de privacidad especificadas en el estándar Docsis utilizado por la mayoría de cables módems. Los dispositivos electrónicos se conectan al cable módem a través de un puerto Ethernet, USB o señal inalámbrica.

El interior de un cable módem se puede estructurar de la siguiente manera:

- Sintonizador: conecta con la parte física del módem, generalmente con un elemento añadido llamado *splitter*, que separa las señales de datos de Internet con la programación normal de CATV. Al recibir los datos de Internet por un canal que no se está usando, el sintonizador simplemente recibe la señal digital modulada y la pasa al demodulador.

- Demodulador: un demodulador QAM reúne una señal de radiofrecuencia que tiene información decodificada en su interior al variar la amplitud de la onda, y la transforma en una simple señal que puede ser procesada por un convertidor de señal analógica a señal digital.

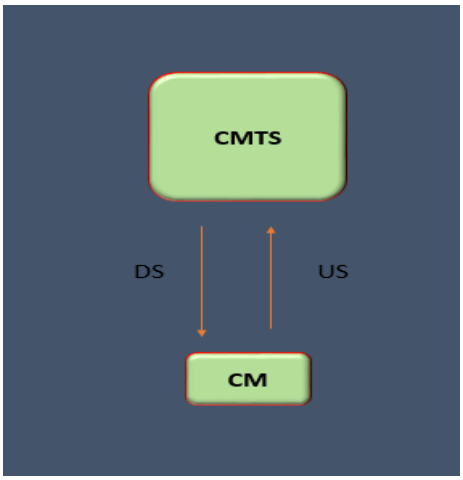
- Modulador: el módem utiliza el sistema por cable para la subida de tráfico, esta etapa se utiliza para convertir los datos digitales del ordenador en señales de radiofrecuencia para su transmisión.

- MAC: se localiza entre las parte de subida y bajada en el cable, y actúa como un interfaz o puente entre las partes físicas y lógicas para los distintos protocolos que se emplean en la red. Todos los equipos y dispositivos de red tienen una MAC, pero en el caso de los módems de cable, las tareas son más complejas que en una simple tarjeta de red.

- Microprocesador: la tarea de este elemento depende de alguna manera de si el módem está designado a ser parte de un sistema de ordenadores más grande o dar acceso a Internet sin más asignaciones. Básicamente lo que hace es gestionar todos los procesos y funciones del módem.

Para el proceso de inicialización del cable módem, en primera instancia este comienza a buscar en el espectro de bajada de RF una portadora modulada en forma digital. Una vez que se sincronizó con la portadora adecuada el CM solicita al CMTS que le envíe los parámetros de configuración necesarios para poder operar en la red de cable (dirección IP y otros datos adicionales) utilizando el protocolo de comunicaciones DHCP. Luego el cable módem solicita al servidor ToD la hora del día y la fecha exacta que se utilizará para almacenar los eventos de acceso al cliente.

Figura 13. **Estableciendo comunicación Docsis**

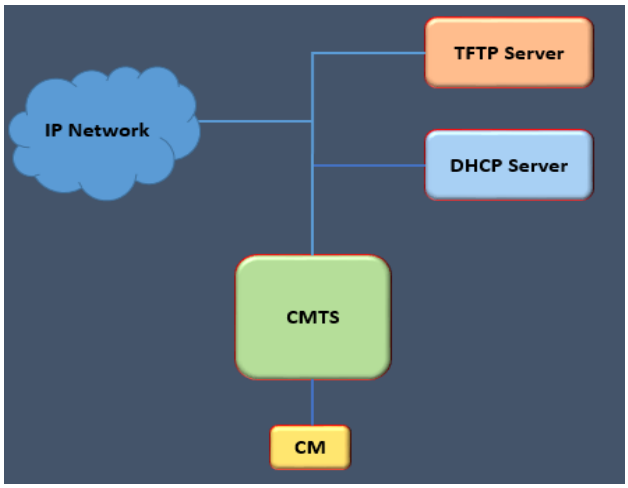


Fuente: elaboración propia, empleando PowerPoint 2010.

La configuración propia del cable módem se lleva a cabo después de las solicitudes DHCP y ToD. El CMTS le envía ciertos parámetros de operación vía TFTP, tras lo cual el módem realiza un proceso de registro y, en el caso de utilizar la especificación Docsis de privacidad de línea de base BPI en la red, deberá adquirir la información necesaria de la central y seguir los procedimientos para inicializar el servicio.

Asumiendo que el proceso de inicialización se ha desarrollado satisfactoriamente, el cable módem está listo para utilizar la red como cualquier otro dispositivo Ethernet sobre los estándares de transmisión admitidos por Docsis. El servidor que brinda las respuestas a las peticiones DHCP, TFTP y ToD es conocido como servidor de aprovisionamiento (OSS), sin embargo puede haber servidores específicos para cada uno de esos servicios, los cuales se encuentran en una red llamada red de aprovisionamiento.

Figura 14. **Envío de configuración hacia CM**



Fuente: elaboración propia, empleando PowerPoint 2010.

Tabla V. **Flujo de aprovisionamiento de un cable módem**

Especificación	Descripción
Sintonización	CM busca un canal de datos *downstream*, sincroniza con QAM.
Ranging	CM ajusta niveles de potencia.
Conectividad	CM obtiene su IP a través del servidor DHCP, el CM obtiene su hora haciendo una petición al servidor ToD.
Configuración	CM obtiene su archivo de configuración vía TFTP.
Registro	CM se pondrá en línea solo hasta después que se registre con el CMTS y reporte que todos los parámetros de configuración adquiridos son aplicables.
Mantenimiento	CM mantiene comunicación periódica con el CMTS para ecualización, ajuste de niveles de potencia, entre otros. Cuando menos cada 30 seguidos.

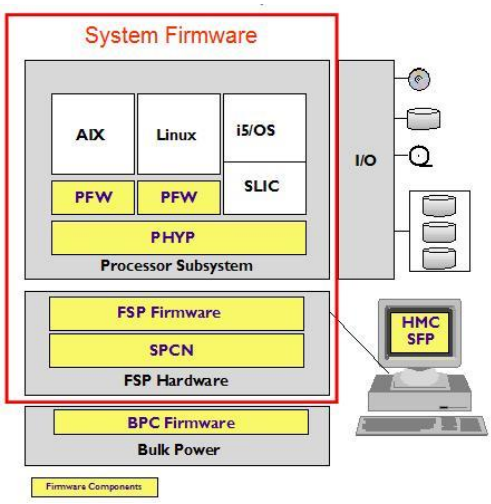
Fuente: elaboración propia.

3. VULNERABILIDADES DE SEGURIDAD

3.1. *Firmware*

Un firmware es un sistema que se desarrolla para establecer un lazo entre la parte física y lógica del sistema, de ahí proviene su denominación, la cual fue empleada por primera vez en los años 60 para señalar a un conjunto de normas insertado en una tarjeta electrónica para que un componente más grande ejecutara una función automática. Si bien es cierto que el *firmware* es creado desde un código fuente que se escribe a través de un software, este tiene una relación más física que cualquier programa pueda ejercer sobre un equipo.

Figura 15. **Arquitectura del *firmware***



Fuente: *Firmware.* http://firmware-santiago.blogspot.com/. Consulta: 10 de enero de 2019.

Cabe destacar que el usuario por lo general cuenta con la posibilidad de actualizar el *firmware* de un dispositivo para corregir errores o mejorar sus prestaciones. Estas actualizaciones, de todas formas, son riesgosas, ya que si se produce algún fallo en el proceso el dispositivo puede dejar de funcionar.

Un CM es básicamente una computadora pequeña diseñada con la capacidad para realizar muchas tareas. El hardware dentro de un módem no realiza estas tareas directamente, pero en realidad se utiliza para operar un sistema virtual de gama alta que es el núcleo del CM. Este sistema virtual se implementa mediante el *firmware* que se ejecuta en el sistema en el inicio.

Dado que el *firmware* es el cerebro del cable módem, cambiarlo o modificar su código afectará directamente la forma en que funciona. Esto permite a los desarrolladores controlar cada aspecto del CM y les brinda la posibilidad de cambiar o agregar características en el futuro simplemente actualizando la imagen del *firmware.* Al corromper un cable módem, el *firmware* es un punto muy importante, por tal motivo es importante entender su funcionamiento.

El hardware en el CM realiza tareas de bajo nivel, el conjunto de *chips* tiene una MAC integrada que se utiliza para demodular la frecuencia en sentido descendente y modular esa frecuencia en sentido ascendente.

El sistema virtual maneja todas las tareas de alto nivel, estas tareas incluyen la transferencia de datos entre el puerto Ethernet y la red coaxial, el registro del CM con el CMTS, la actualización del *firmware*, la ejecución de un servidor HTTP y la administración de dispositivos, el sistema de gestión de SNMP y otros servicios de red.

Estas tareas se realizan mediante el uso de un sistema operativo similar a Unix llamado VxWorks, que es el sistema operativo utilizado en la mayoría de CM. Todos los módems compatibles con Docsis deben ser actualizables. Algunos módems tienen un método de actualización redundante que garantiza que no se volverá inútil en caso de un intento de actualización incorrecto.

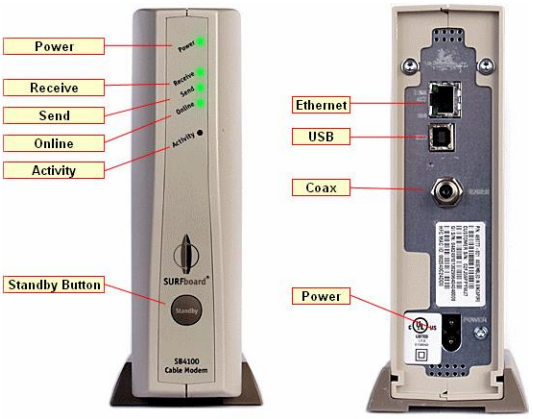
La capacidad de cambiar el *firmware* al *hackear* un cable módem le da más control sobre su dispositivo que su proveedor de servicios. Esto puedo ser posible encontrando una falla de seguridad, permitiendo al usuario acceder al sistema del cable módem y ejecutando sintaxis de comandos para realizar los cambios necesarios en el funcionamiento.

3.2. Clonación de cables módems

El cable módem, como ya se ha visto anteriormente, es el equipo que se encuentra ubicado físicamente en la casa del cliente que contrata el servicio de navegación de Internet con un proveedor de servicio.

El cable módem es un equipo especial que opera en la arquitectura de la red HFC, estipulada bajo los estándares de televisión por cable, la clonación de estos equipos es posible mediante procedimientos que las personadas mal intencionadas han encontrado y requiere de un arduo trabajo evitarlo.

Figura 16. **Cable módem físico**

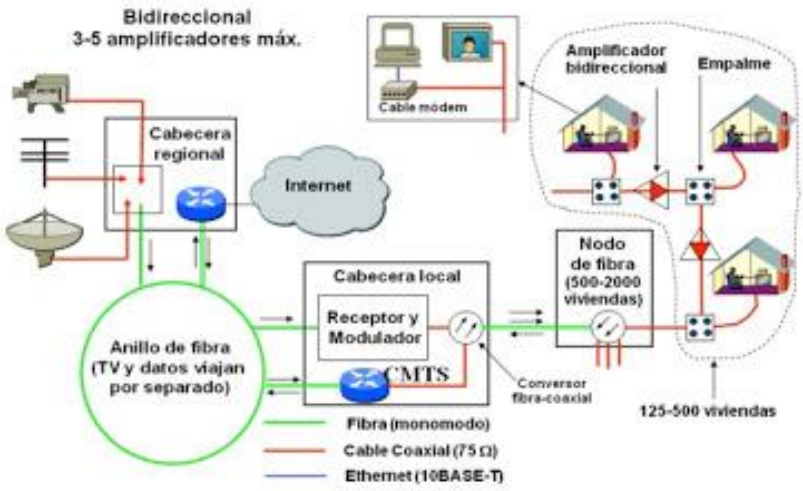


Fuente: *Cable módem troubleshooting.* https://www.simplehelp.net/2006/07/04/cable-modem-troubleshooting-motorola-sb4100/. Consulta: 10 de enero de 2019.

La red HFC está construida por segmentaciones llamadas nodos, eso es necesario en la actualidad ya que pueden ser muy grandes, y dependiendo de la zona geográfico que los compone, la clonación o la copia de la configuración de estos dispositivos en esta red está ocurriendo frecuentemente. Cada CMTS cuenta con una cantidad de nodos asignados, cada nodo tiene cierta cantidad de usuarios o clientes conectados al mismo, cuando un nodo no tiene servicio por alguna falla, todos sus clientes no tendrán servicio, sin embargo los demás clientes conectados a otros nodos no tendrán ningún inconveniente con su servicio.

Debido a que esta red puede llegar a ser tan grande por la cantidad de usuarios, es común que un CMTS pueda tener hasta decenas de nodos dependiendo de la capacidad del equipo.

Figura 17. **Diagrama de un CMTS con un nodo**



Fuente: *Redes HFC.* http://redes150432.blogspot.com/. Consulta: 20 de enero de 2019.

Para que el cable módem pueda engancharse a la red HFC y pueda tener servicio de Internet, hay un parámetro que es muy importante para este proceso y es la dirección MAC. Este es un identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados, desde un ordenador o impresoras u otros dispositivos.

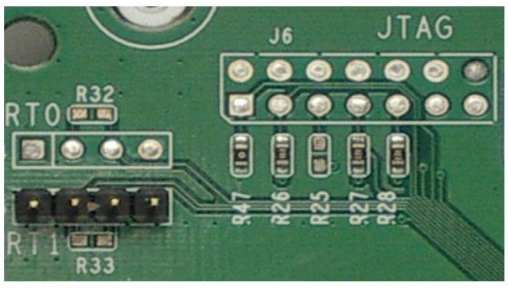
La MAC del cable módem es el parámetro que se utiliza para registrarse en los CMTS y en el sistema de aprovisionamiento del proveedor de servicio. Debido a esto las personas que intentan vulnerar esta red lo realizan clonando la dirección MAC del cable módem y conectando el equipo en otro CMTS distinto para obtener el servicio de forma fraudulenta. Hay algunos procesos con los que se puede modificar la dirección MAC de un CM, esto depende del modelo y marca del cable módem que se va a modificar.

Un método para poder alterar las direcciones MAC del equipo es por medio del puerto JTAG. Es una interfaz estándar presente en las placas de circuito impreso que se utiliza para interactuar con un circuito integrado. Fue desarrollado en 1990 y originalmente se usaba para probar circuitos integrados.

JTAG puede utilizarse para pruebas de interconexiones y funcionalidad en circuitos integrados hasta programación de memoria *flash* de sistemas implementados en el campo y todo lo que se encuentre en el medio. Es una solución maravillosa, pero también un gran recurso para los *hackers.* Desde una perspectiva de seguridad, JTAG se utiliza principalmente para:

- Manipular pines individuales en circuitos integrados
- Cambiar estados de los componentes
- Alterar la memoria *flash*
- Obtener acceso a utilidades de depuración

Figura 18. **Puerto JTAG**



Fuente: FERRARI, Luciano. *Seguridad IoT*. https://www.lufsec.com/iot-security-starting-with-jtag-hacking/. Consulta: 5 de febrero de 2019.

3.3. Uncap

Básicamente con este método se utiliza una técnica llamada envenenamiento ARP, lo cual hace que el CM envíe su propio archivo de configuración. La idea de cambiar el archivo de configuración del cable módem para modificarlo a gusto se debe plasmar subiendo el archivo de configuración desde la propia interfaz de red del cable módem desde la tarjeta de un ordenador personal.

El cable módem siempre accede al servidor TFTP a través de la red de cable, es decir por el coaxial, el paso básico consiste en hacer que el propio ordenador haga la vez de servidor TFTP y el cable módem baje el archivo de configuración que ha sido modificado a gusto particular.

Evidentemente para ello se necesita algún programa que cree un servidor TFTP en la máquina, y lo único que se tiene que hacer es poner la dirección IP adecuada. Una vez el cable módem acepta el archivo, el CMTS debe aceptar la conexión. Se puede dar el caso de que el cable módem no valide el fichero por muchas causas, por ejemplo un fichero con una configuración inválida.

Debe destacarse que no todos los CM permiten realizar esto, solo algunos modelos concretos de Motorola y de 3com permiten el *uncapping*. Es posible decir que estos modelos sufren de algún fallo o algún tipo de *bug* que permite que el cable módem acepte archivos de configuración a través del interfaz de red. La mayoría de los módems utilizan el CmMic para determinar si el archivo de configuración descargado es válido, no es corrupto o bien está completo. El CMTS utiliza el CmtsMic para validar el archivo de configuración.

Hay algunos pasos para realizar este tipo de método que a continuación se describe:

- Conocer la dirección IP del servidor TFTP del proveedor de servicio: normalmente este servidor suele ser el mismo que el servidor DHCP, esto se puede averiguar con alguna línea de comando o con algún programa especial para esta tarea.

- Descargar el archivo de configuración: se puede descargar bien desde el servidor TFTP, aunque los proveedores toman medidas para evitar la descarga, o bien se puede crear el propio fichero. Se puede descargar con alguna aplicación o mediante línea de comandos (tftp -i <dirección servidor dhcp> GET <nombre de fichero> C:\<nombre_de_fichero>).

- Cambiar el archivo de configuración: estos archivos están codificados, de manera que para visualizar su contenido se debe usar una aplicación de decodificación para luego cambiar los valores de velocidad de bajada y subida.

- Cambia la dirección IP: a continuación se debe cambiar la IP del ordenador con una IP para que el cable módem crea que el ordenador es el servidor TFTP. Será necesario reiniciar el cable módem para que al buscar el fichero de configuración lo haga a través del servidor creado. El cambio de IP se hará en función del sistema operativo.

El método de *uncapping* es una actividad fraudulenta que se está realizando al proveedor de servicio. El fin de esta configuración es el cambio de velocidad de subida en el cable módem, ya que esta velocidad es compartida

por todos los usuarios y por ende es una velocidad supervisada por el proveedor a nivel de la calidad de servicio.

3.4. Método de los *bitfiles*

El modo de fábrica es un método de administración secreta en la serie de cable módems *SURFboard* de Motorola, también conocido como método de *bitfiles.* Cuando un cable módem está en modo de fábrica, el usuario puede usar una cuenta SNMP local para cambiar varios de los parámetros de configuración predeterminados del cable módem.

El MIB (*Management Information Base*) de fábrica es una lista de OID (*Object Identifier*) que tiene funciones únicas. Al cambiar los valores de los OID en este MIB, pueden cambiar muchos de los ajustes predeterminados del cable módem, como las direcciones USB, Ethernet, MAC y el archivo de certificación del cable módem. También puede modificar directamente la memoria, lo que le permite cambiar los datos o el código directamente en el módem.

Debido a que el modo de fábrica está destinado a ser utilizado solo por personal del fabricante, cuando las pruebas finalizan los dispositivos son vendidos con la opción deshabilitada.

4. MEDIDAS DE SEGURIDAD Y PREVENCIÓN

4.1. Restricción de acceso y mejoras en *firmware*

Como se ha visto en el capítulo anterior, hay varias formas con las que se puede vulnerar los equipos y poder obtener un servicio de forma fraudulenta que afecta directamente al proveedor de servicio y en ocasiones al cliente final, por ende hay ciertas restricciones que los proveedores especifican para que estas no sean utilizadas de forma anómala.

Para verificar las restricciones que se han colocado en el acceso a Internet por cable se debe saber que existen y tener el deseo de encontrarlas. Saber cómo funcionan los dispositivos le permitirá comprender mejor las limitaciones que pueden surgir en su camino.

Algunas de las limitaciones son útiles y evitan que se destruya o se haga un mal uso del dispositivo, mientras que otras simplemente evitan que se use el dispositivo en todo su potencial. Hay algunas razones por las que un desarrollador de hardware o un proveedor de servicios deben imponer un límite al uso de un dispositivo o de una tecnología, estas razones a menudo pueden ser las siguientes:

- Proteger el equipo
- Reducir los costos de fabricación o servicio
- Vender las características retenidas

Cuando se trata de las razones reales, los límites a menudo son solo parte de una estrategia de negocios por parte de los proveedores. Es muy común establecer límites en un dispositivo de red, como un cable módem, para proteger al equipo y no solo su equipo, sino también el de otros clientes y al de los proveedores de servicios.

Por ejemplo, una de las razones por las que el proveedor de servicio puede reducir su velocidad de carga a un máximo valor, es garantizar que todos los clientes puedan cargar al mismo tiempo. O bien, podrían limitar el sintonizador de cable coaxial de su módem a un cierto nivel de energía para asegurarse de que su módem no interrumpa el servicio de nadie más. Esto reduce el costo de mantenimiento al minimizar las perturbaciones de hardware que podrían causar interrupciones del servicio.

La mayoría de las restricciones impuestas a los módems de cable están especificadas por el estándar Docsis, como ya se ha visto anteriormente que se utiliza para certificar a los módems de cable dependiendo de la versión con la que cuenten los equipos. Este estándar requiere que el módem esté seguro contra la manipulación o alteración por parte del usuario final. Por lo tanto, las características como la capacidad de actualización de *firmware* están deshabilitadas.

Docsis indica que solo el proveedor de servicio puede actualizar el *firmware* del módem, a través de la red HFC, esto garantiza que un usuario no pueda arruinar accidentalmente el módem con un código malicioso, o que intente utilizar una modificación de *firmware* no autorizada.

El Protocolo SNMP (protocolo simple de administración de red) está presente en cada módem, es la herramienta principal utilizada por el proveedor

de servicio para controlar el equipo del cliente. Cuando un módem se enciende por primera vez, SNMP se desactiva y borra de cualquier configuración anterior. Una vez que el módem se registra con el CMTS, el servidor SNMP puede inicializarse y asegurarse para responder solo al CMTS en donde se registró, momento en el cual se pueden aplicar ciertas configuraciones al cable módem para restringir sus funciones.

El servidor SNMP tiene mucha potencia sobre el cable módem, ya que se puede usar para deshabilitar el demonio HTTP interno del cable módem, que se usa principalmente con fines de diagnóstico, también puede bloquear y restringir ciertos puertos de conexión por ejemplo, permitir que su proveedor de servicio bloquee el puerto 25 en su módem, y puede monitorear e informar el uso de su ancho de banda directamente, esto con el fin de limitar aún más su velocidad o para agregar un recargo a su factura mensual.

Ciertas restricciones se configuran en el CMTS, algunas configuraciones deben inicializarse durante el período de registro del módem haciendo que el mismo descargue un *script* de configuración desde el CMTS antes de registrarse en la red. Este *script* de configuración puede contener muchas configuraciones que se aplicarán una vez que el módem de cable se haya registrado en la red.

Algunas restricciones para el usuario en el cable módem son:

- Actualización del *firmware*
- Utilización de puertos de red del CM
- Modificación de velocidad de bajada o subida
- Cantidad de dispositivos conectados al CM
- Asignación de dirección IP

Todos los cables módems están diseñados para permitir que su *firmware* se actualice de forma remota, de modo que el proveedor de servicio pueda actualizar el CM para admitir nuevos servicios o mejoras al equipo. Sin embargo, los diseñadores de Docsis reconocieron la posibilidad de que los módems necesitarán actualizaciones de *firmware* para corregir fallas de diseño que los hagan vulnerables y puedan ser alterados maliciosamente.

Ningún sistema de hardware o software es inquebrantable, ya que se ha demostrado que incluso los dispositivos de una gama de alta seguridad han sido perpetuados por personas no confiables. Dado que nadie sabe qué explotaciones podrían descubrirse en el futuro, el proceso de actualización del *firmware* se implementa de una manera que hace que sea más eficiente para los proveedores lanzar y actualizar el *firmware* para solucionar los problemas de seguridad recién descubiertos.

A fines de 2001 muchos tutoriales comenzaron a aparecer en Internet que explicaban exactamente cómo explotar un cable módem y eliminar los límites de velocidad de bajada y subida. Muchos módems fueron vulnerables a este tipo de ataque.

4.2. Encriptación de datos

BPI es la interfaz de privacidad de línea base que proporciona un esquema simple de encriptación de datos para proteger los datos enviados desde y hacia los módems de cable en una red de datos Docsis. Un objetivo secundario de BPI es proporcionar a los operadores de una protección básica contra el robo del servicio de Internet.

Para proporcionar una protección sólida contra este robo, el CMTS necesitaría autenticar los CM del cliente, el CMTS necesitaría establecer una identidad única y verificable para un módem por cable y autenticar las solicitudes de claves que afirman ser de ese CM. Además, el CMTS necesitaría vincular la identidad del CM a un suscriptor que paga y a los servicios de datos a los que el suscriptor está autorizado a acceder.

Cuando se inicia BPI, los paquetes de datos que fluyen a través de la red privada del proveedor de servicio se cifran utilizando el algoritmo DES y un sistema de llave criptográfica pública/privada conocido como el esquema KEK (clave cifrado clave).

Durante el proceso de registro, el CM envía al CMTS una clave pública generada dinámicamente o una clave almacenada en el archivo. El CMTS genera una clave privada conocida como clave de autenticación y la cifra mediante la clave pública del CM. El CMTS envía esta clave (ahora conocida como la clave compartida) al CM.

En este punto, tanto el CMTS como el CM comparten una clave secreta que solo ellos conocen. La clave de autenticación del CMTS se usa luego para intercambiar un nuevo conjunto de claves de cifrado entre el CMTS y el módem, conocida como clave de cifrado de tráfico (TEK). Esta es la clave que realmente se usa para cifrar los datos en la red de cable.

Ahora el CM y el CMTS comparten una clave privada que se utiliza para proteger los datos intercambiados entre ellos. Estos pares de claves son únicos, y el CMTS tiene una clave separada para cada módem que está conectado a este. Un cable módem no tiene acceso a las claves utilizadas por otros

módems. Por lo tanto, un módem solo puede descifrar los datos de red que el CMTS le envía, y solo el CMTS puede descifrar los datos de red que envía.

4.3. Certificaciones digitales y configuración dinámica

La versión de Docsis 1.1 se enfocó bastante en mejorar las características de seguridad de BPI, para fortalecer el estándar de seguridad se implementó BPI+. Estos archivos de certificación se utilizan para la autenticación de los dispositivos, la actualización segura del *firmware* y la privacidad de los datos en forma de cifrado.

En los primeros sistemas de datos basados en cable, a veces no había protección contra tales escuchas ilegales, lo que dejaba a los usuarios de computadoras sofisticados libres para acceder a la información de las máquinas de otros usuarios y también para examinar el tráfico que pasaba por el cable coaxial.

La versión actual de Docsis evita esto al implementar un mecanismo llamado BPI + (Baseline Privacy Interface Plus). Una mejora a la anterior versión BPI, ya que BPI+ es considerablemente más segura.

Desafortunadamente, no todos los proveedores de cable se toman la molestia de utilizar BPI +, ya que se deben tomar medidas adicionales en el CMTS para poder usarlo, como instalar un certificado confiable de Docsis.

BPI+ no discrimina entre los tipos de datos que fluyen a través del cable. Todos los paquetes de datos de usuario transmitidos por el cable están protegidos por igual por los protocolos de seguridad BPI+. El mecanismo utilizado para asegurar las comunicaciones entre un CM y su CMTS

correspondiente es el cifrado de los flujos de tráfico entre los dos dispositivos. BPI+ comprende dos protocolos que son:

- Un protocolo de encapsulación, utilizado para cifrar y descifrar los paquetes. Este protocolo define el formato para los paquetes cifrados, el conjunto de cifrados compatibles y las reglas para aplicar los algoritmos criptográficos a los datos en paquetes.

- Un protocolo de administración de claves (Baseline Privacy Key Management, BPKM) que proporciona un método seguro para distribuir material de claves entre el módem de cable y su CMTS.

BPI+ cifra solo los datos de trama MAC (datos de usuario). No encripta los encabezados de trama MAC. Además, no se utiliza para proteger los mensajes de administración de MAC, estos siempre viajan visiblemente.

BPI+ reconoce tres tipos de asociaciones de seguridad (SA) que pueden existir entre un CM y su CMTS:

- Se establece una SA primaria durante el registro de MAC. Es una asociación que permanece en el lugar entre el CM y el CMTS siempre que el CM retenga la energía y sea exclusivo del par CM/CMTS.

- Las SA estáticas se han preestablecido dentro del CMTS. Varios CM pueden compartir la misma SA estática con un solo CMTS.

- Las SA dinámicas se crean y se destruyen sobre la marcha en respuesta a la creación y terminación de flujos de tráfico descendentes específicos, varios CM pueden compartir la misma SA dinámica con un solo CMTS.

En la gestión de clave de privacidad de línea base (BPKM), en la mayoría de los sistemas de seguridad basados en la criptografía, la administración de claves es la parte más complicada del sistema. Asegurarse de que las claves se generen aleatoriamente y se compartan de manera segura suele ser un problema complejo y las soluciones también son complicadas.

BPKM utiliza certificados X.509, el algoritmo de cifrado de clave pública es RSA y 3DES, esto con el fin de asegurar el intercambio de claves entre un CM y su CMTS.

Tabla VI. **Tipo de seguridad según versión Docsis**

Versión	**Seguridad**
Docsis 1.0	BPI; básico, no muy segura
Docsis 1.1	BPI+; autenticación de dispositivo
Docsis 2.0	BPI+; autenticación de dispositivo
Docsis 3.0	BPI+ mejorado, seguridad AES

Fuente: elaboración propia.

A través de módulos de QoS adicionales, un operador de cable puede implementar características como la configuración dinámica. La configuración dinámica es un módulo que permite al servidor de aprovisionamiento OSS generar archivos de configuración sobre la marcha cuando un cable módem está intentando registrarse en la red. Este tipo de configuración de equipo permite que los equipos de cada cliente se configuren individualmente según sea necesario, en lugar de usar archivos de configuración predefinidos.

Los archivos de configuración dinámica también mejoran e incrementan la seguridad del cable módem. Al generar archivos sobre la marcha, una copia física del archivo no se almacena en el servidor TFTP. Esto evita que los clientes lo descarguen y lo guarden, y también evita otras formas de acceso no autorizado. Un sistema de configuración dinámica también se puede utilizar para modificar rápidamente el perfil de un solo cliente.

Aunque la configuración dinámica dificulta que el usuario final descubra los archivos de configuración, no lo hace imposible. Puede usar un CM clonado que ejecuta un complemento especial para capturar y guardar el archivo de configuración destinado a la dirección MAC de su módem en tiempo real durante el proceso de aprovisionamiento. Para descargar otros archivos de configuración que pueden generar valores de rendimiento más altos en la configuración, puede usarse un *firmware* modificado para cambiar la dirección MAC de su interfaz de red a la de otro módem que puede aprovisionarse a una velocidad mayor.

4.4. Actualización de equipos

La seguridad es una batalla constante, los piratas informáticos intentan penetrar en un sistema, mientras que sus administradores intentan mantenerlo invulnerable. Estos dos grupos de personas representan a equipos opuestos y el equipo que tenga una mejor comprensión de la tecnología de seguridad va a ganar.

No hay garantía de que pueda proteger completamente un dispositivo o red o que se pueda crear una medida de seguridad que nunca necesitará una actualización futura. Los métodos de seguridad como los algoritmos de cifrado, las verificaciones de integridad de los mensajes o las actualizaciones de

firmware se modifican de forma rutinaria para hacerlos más difíciles de descifrar.

Durante los últimos años, los sistemas de cable de banda ancha compatibles con Docsis en todo el mundo han sido vulnerables a una variedad de métodos de *hackeo.* Esto ha permitido a los usuarios malintencionados robar el servicio de Internet poniendo en práctica el conocimiento público.

Los piratas informáticos han utilizado estos métodos para recibir el servicio de Internet gratuito y para eliminar las limitaciones de descarga y carga establecidas por sus proveedores de servicios. Esto ha sido posible en parte porque los administradores de red no han invertido suficiente tiempo en investigar métodos de piratería y aprender cómo deshabilitarlos.

Es muy importante actualizar el software de los dispositivos cuando una versión está disponible. Los principales motivos son por seguridad y soluciones de errores. La seguridad es uno de los motivos más importantes y claves que se recomienda actualizar. Son muchos *hackers* mal intencionados que se dedican a desarrollar herramientas de software que les permiten encontrar fácil acceso y pueden ser vulnerables, con las actualizaciones de software se logran cerrar esas puertas y por ende brindan mayor seguridad a los equipos.

Uno de los mayores beneficios de las actualizaciones de software es el de solucionar errores. También hay otras actualizaciones que añaden nuevas funcionalidades y cambios y si se quiere disfrutarlos tendrá que realizarse actualizaciones. No es obligatorio en el caso de lo segundo, pero sí recomendado para disfrutar de una mejor y nueva experiencia.

Hay 3 motivos principales para actualizar un sistema:

- Las que añaden un parche de seguridad (corrigen vulnerabilidades)
- Las que solucionan errores
- Las que añaden funcionalidades nuevas

Los ingenieros que brindan soporte a la red HFC son los encargados de asegurar y mantener el funcionamiento de la red, este proceso requiere de invertir bastante tiempo y es costoso, especialmente cuando se requieren capacitaciones para los ingenieros y la compra de equipo nuevo.

4.5. Supervisión recurrente

Como se vio en el punto anterior, es muy importante la actualización de los sistemas, para una mejor protección tanto en la red como en los equipos, esto no quiere decir que se garantiza la cobertura total en seguridad de la red y del servicio.

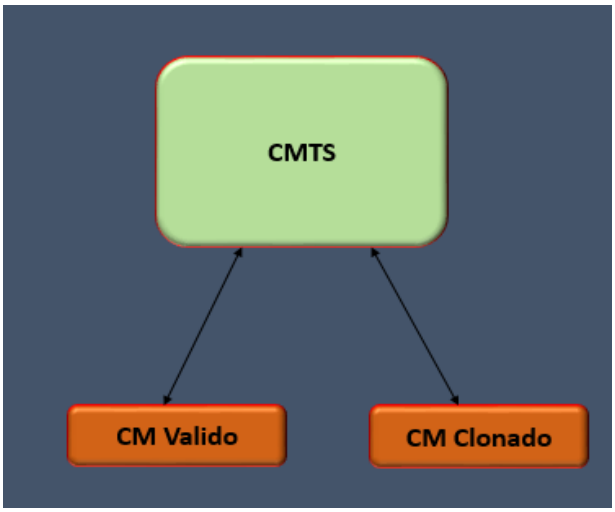
La configuración de los dispositivos que integran la red es una parte importante, ya que un CMTS se puede configurar como la mayoría de enrutadores comerciales, debido a que ambos utilizan comandos y sintaxis parecidos para visualizar o configurar parámetros que dan funcionalidad a la red.

El gran problema que se tiene identificado en los últimos años es cuando dos CM intentan conectarse con la misma dirección MAC, esta condición es conocida como colisión de MAC. Este problema ocurre cuando el primer CM (cliente valido) se registró en el CMTS y luego se desconecta por algún motivo,

posteriormente el segundo CM (cliente fraudulento clonado) se conecta a la red y se registra en el CMTS obteniendo el servicio correcto.

Cuando el primer CM intenta nuevamente conectarse a la red, ahí es donde se genera la colisión, que ocasionará que el segundo CM se desconecte y el otro se conecte, este proceso se repetirá indefinidamente, manteniendo a los CM fuera de línea.

Figura 19. **Colisión de MAC**



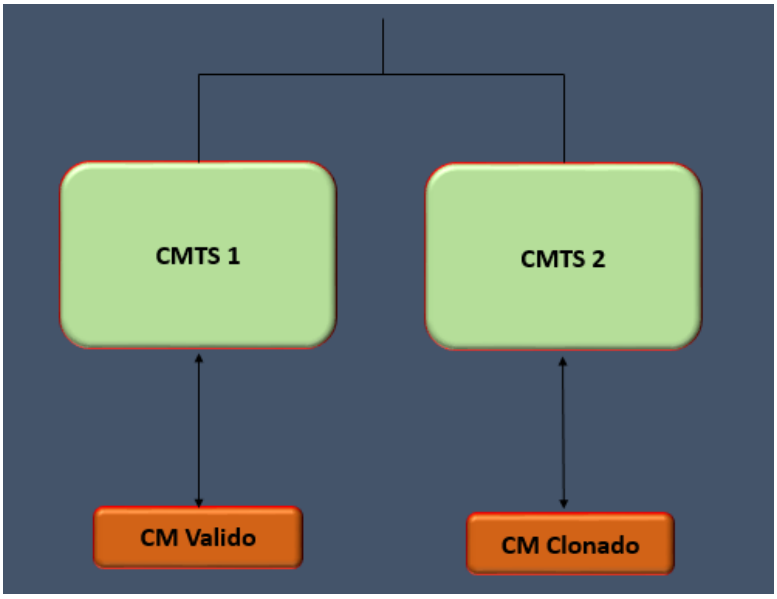
Fuente: elaboración propia, empleando PowerPoint 2010.

Sin embargo, en la práctica se cuenta con un problema mayor y es cuando se produce una colisión de MAC en una red HFC, debido a que los grandes proveedores de servicio implementan grandes redes que utilizan varios nodos de fibra para crear subconjuntos dentro de grandes áreas geográficas. Es decir que se incluyen varios equipos CMTS dependiendo de la capacidad y demanda del servicio, esto ocasiona que cuando un cable módem intenta registrarse en

un CMTS (cliente válido) y logra conectarse a la red obtendrá el servicio que ha contratado.

Cuando el cable módem (cliente fraudulento clonado) intente registrarse en otro CMTS de la red que no sea donde se encuentre el cliente correcto, este podrá enganchar a la red obteniendo el servicio de forma fraudulenta y es ahí donde entra el gran negocio de la clonación de servicio de Internet en la red HFC.

Figura 20. **Clonación de servicio de Internet en red HFC**



Fuente: elaboración propia, empleando PowerPoint 2010.

Para brindar mayor seguridad y control en la red de datos en una red HFC, se puede sugerir el uso de *scripts* personalizados en los CMTS. Un *script* es un archivo de texto básico que contiene comandos, argumentos y condiciones con los que se le interroga al equipo y este devolverá cierta información, pudiendo

instalar sus propios *scripts* personalizados. Los *scripts* brindarán una variedad de información de parámetros de CM.

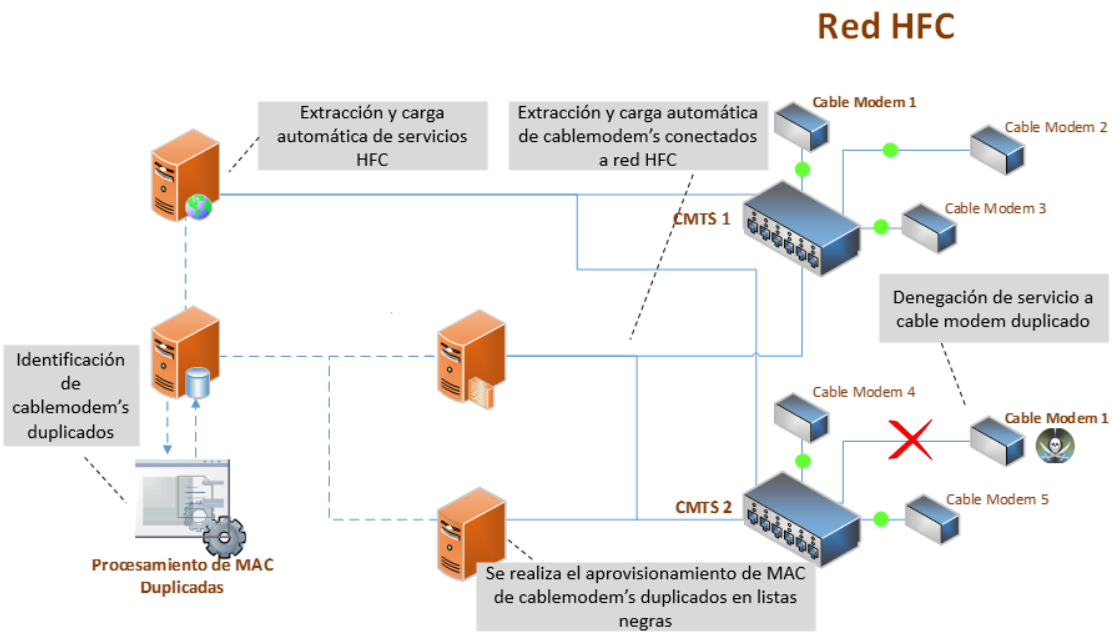
En la información que se extrae con los *scripts* es complicado visualizar todos los campos registrados que se tienen debido a la tabulación o formato con que cuentan, ya que todas las configuraciones de cables módems se encuentran en un texto plano y no es posible visualizar las configuraciones que ayudarán a realizar el análisis que se desea.

Por tal motivo se emplea un método que realiza una lectura de los archivos planos, extrayendo únicamente la información útil para realizar el análisis. Estas configuraciones son ingresadas en registros en tablas a una base de datos, debido a que cada CMTS puede tener cientos de clientes conectados a sus interfaces.

Todas las configuraciones de cada cable módem son extraídas de cada CMTS e ingresadas a una base de datos, posteriormente esta información es conciliada o comparada con los sistemas de aprovisionamiento (OSS) y sistemas de facturación del proveedor de servicio, esto con el fin de validar todos los servicios que están conectados en la red de datos HFC.

El proceso de conciliación o comparación devolverá información de los servicios que se encuentran clonados en la red, estos serán ingresados a un proceso de bloqueo en donde el cable módem clonado no podrá conectarse nuevamente a la red. Es con este método que se ha podido atacar estas debilidades o vulnerabilidades que tiene la red HFC en el servicio de Internet.

Figura 21. **Proceso de bloqueo de un CM**



Fuente: elaboración propia, empleando PowerPoint 2010.

5. RESULTADOS

5.1. Detección de equipos clonados por dirección MAC

Como se comenta en el capítulo anterior, es conveniente implementar un proceso recurrente en el cual se pueda realizar la detección y corrección de los servicios de Internet clonados sobre la red HFC. Como resultado del proceso de detección de clonación de dirección MAC, se han podido depurar las inconsistencias en la red hasta marzo de 2019.

Tabla VII. **Cantidad de cables módems clonados en la red**

Año	Guatemala	El Salvador	Honduras	Nicaragua	Total
2017	4	215	1 619	9 460	13 315
2018	1	305	6 329	30 172	38 825
2019	0	33	291	7 573	9 916
Total	5	553	8 239	47 205	56 002

Fuente: elaboración propia.

5.2. Impacto económico por servicios clonados en la red HFC

Cuando se habla de la clonación del servicio de Internet, a menudo no es el cliente final el perjudicado, si no que la empresa proveedora es la que sufre la pérdida económica por este tipo de fraude que se realiza en su propia red.

Tabla VIII. **Impacto económico por clonación de servicio**

Año	Guatemala	El Salvador	Honduras	Nicaragua	Total
2017	$152	$8 170	$61 522	$359 480	$431 341
2018	$38	$11 590	$240 502	$1 146 536	$1 400 684
2019	$0	$1 254	$11 058	$287 774	$302 105
Total	$190	$21 014	$313 082	$1 793 790	$2 128 076

Fuente: elaboración propia.

CONCLUSIONES

1. Las redes HFC están diseñadas para brindar servicios y proporcionar soluciones eficientes de gran capacidad accesibles al cliente como Internet, telefonía IP y video.

2. El estándar Docsis ha permitido evolucionar la transmisión de datos a una gran velocidad, esto depende de la inversión que el proveedor de servicio realice en su red para una mejora continua y una mejor calidad de servicio que ofrezca al cliente final.

3. Existen varios métodos que utilizan los *hackers* para vulnerar la seguridad de los equipos de la red HFC, en especial el cable módem, que es el equipo que contiene los parámetros de configuración para poder enganchar a la red y obtener servicio de Internet, por tal motivo los *hackers* se han concentrado en métodos para extraer la información necesaria para invadir de forma fraudulenta la red.

4. Es importante realizar las actualizaciones de los sistemas ya que por medio de eso se logra mitigar riesgos de errores de software, problemas de seguridad, como lo es BPI+ ya que este incorpora certificados digitales, encriptaciones de datos más seguras y se eleva el nivel de seguridad en el cable módem.

5. Es importante conocer el funcionamiento de la red HFC para implementar controles en los que se pueda detectar anomalías o

inconsistencias en los servicios de Internet que no afecten a la operación de los sistemas.

RECOMENDACIONES

1. Implementar inspecciones físicas periódicas para revisar la estructura HFC y detectar la presencia de puntos de accesos hacia la red de clientes que ya no cuentan con servicio activo con el proveedor de servicio.

2. Verificar regularmente la disponibilidad de nuevas actualizaciones de seguridad para los equipos y analizar las aplicaciones de las mismas tales como *firmware* o el estándar Docsis.

3. Inhabilitar cualquier modo de prueba que sea inseguro en los equipos, comprobando los protocolos proporcionados por el fabricante, para que no pueda ser manipulado por personas ajenas a la empresa proveedora de servicio, ya que con esto se podría estar realizando algún método de fraude que perjudique a los ingresos de la empresa.

4. Crear una herramienta que pueda validar la presencia de direcciones MAC clonadas en los equipos CMTS, para luego poder proceder a ingresar a una lista negra para bloqueo de servicio fraudulento y así minimizar el riesgo de fraude para el proveedor de servicio.

5. Educar al personal de la empresa para que no pueda divulgar información sensible y crítica con gente externa para que no pueda afectar la operación de la red HFC.

BIBLIOGRAFÍA

1. AGUSTÍN PALACIOS, Otoniel René. *Análisis de ruido en la señal transmitida en un cable coaxial*. Trabajo de graduación de Ing. Electrónica. Universidad de San Carlos de Guatemala. Facultad de Ingeniería, 2006. 100 p.

2. ARDIONS, Andrea. *¿Por qué es importante actualizar el software?.* [en línea]. <https://androidstudiofaqs.com/conceptos/importante-actualizar-software>. [Consulta: 25 de marzo de 2019].

3. DER, Engel; HARRIS, Ryan. *Hacking the cable modem: what cable companies don't want you to know*. Washington, USA: Free Press, 2006. 330 p.

4. EVANS, D. *Baseline privacy interface plus the cable access link*. 2001. [en línea]. <http://www.informit.com/articles/article.aspx?p=167851&seqNum=7>. [Consulta: 7 de marzo de 2019].

5. FERRARI, Luciano. *IoT security: starting with JTAG hacking*. 2018. [en línea]. <https://www.lufsec.com/iot-security-starting-with-jtag-hacking/>. [Consulta: 22 de febrero de 2019].

6. FM, Yúbal. *Qué es la dirección MAC de tu ordenador, del móvil o de cualquier dispositivo*. [en línea]. <https://www.xataka.com/basics/que-es-la-direccion-mac-de-tu-ordenador-del-movil-o-de-cualquier-dispositivo>. [Consulta: de 10 febrero de 2019].

7. JIMÉNEZ, Gerald. *Vulnerabilidades de seguridad en el servicio de Internet de banda ancha en redes HFC: impacto y posibles soluciones*. Ecuador: Escuela Superior Politécnica del Litoral, 2010. 174 p.

8. MARTÍNEZ, Evelio. *Topologías de red*. [en línea]. <http://eveliux.com/mx/curso/topolog.html>. [Consulta: 23 de diciembre de 2018].

9. MONZÓN, Rafael. *Clonación de cable módem.* 2017. [en línea]. <https://mentecuriosa.net/clonacion-de-cable-modem/>. [Consulta: 1 de marzo de 2019].

10. NANDO, A. *Seguridad en sistemas de información*. [en línea]. <https://norbertomn.files.wordpress.com/2014/02/curso-seguridad-en-sistemas-de-informacion.pdf>. [Consulta: 5 de diciembre de 2018].