UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN NOVIEMBRE 2020 – MAYO 2021

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

Estudio de las medidas de seguridad en la red GPON de CNT-EP en la zona 1, sector Cerro Santa Ana de la Ciudad de Guayaquil.

EGRESADA:

Cesia Jemima Santillán Villota

TUTOR:

Ing. Miguel Zúñiga Sanchez

Año 2021

RESUMEN

La Corporación Nacional de Telecomunicaciones – EP ofrece servicios de conectividad a los usuarios por medio de la tecnología GPON en el Cerro Santa Ana de la Ciudad de Guayaquil. El propósito de esta investigación es el estudio de las medidas de seguridad de la mencionada red, debido a la antigüedad que presentan siendo las bases para la expansión de la tecnología GPON a las demás zonas de la ciudad, la falta de mantenimiento a nivel físico y los grandes volúmenes que se transmiten por el cable de la fibra, pueden convertirlas en blancos atractivos para las personas maliciosos, provocando que existan las vulnerabilidades tanto a nivel lógico como físico. La metodología que se empleó en el desarrollo de la investigación es la cuantitativa, las misma que con la ayuda de la entrevista como técnica y del cuestionario como instrumento permitieron realizar el análisis respectivo, para determinar que la empresa no tiene establecido vulnerabilidades especificas en las redes GPON y se desconoce que cuente con medidas de seguridad, sin embrago se consideran importantes que estas existan y que los técnicos estarían dispuestos a ser capacitados respecto a los puntos vulnerables y amenazas comunes que puedan existir en la red GPON.

Palabras Claves: GPON, medidas, seguridad, vulnerabilidades, amenazas, mantenimiento.

ASTRACT

The National Telecommunications Corporation - EP offers connectivity services to users through GPON technology in Cerro Santa Ana in the City of Guayaquil. The purpose of this research is to study the security measures of the aforementioned network, due to the age they present, being the bases for the expansion of GPON technology to other areas of the city, the lack of physical maintenance and the large volumes that are transmitted over the fiber cable can make them attractive targets for malicious people, causing vulnerabilities to exist both at a logical and physical level. The methodology that was used in the development of the research is quantitative, the same that with the help of the interview as a technique and the questionnaire as an instrument allowed to carry out the respective analysis, to determine that the company has not established specific vulnerabilities in the networks GPON and it is unknown that it has security measures, however it is considered important that these exist and that the technicians would be willing to be trained regarding the vulnerabilities and common threats that may exist in the GPON network.

Keywords: GPON, measures, security, vulnerabilities, threats, maintenance.

INTRODUCCIÓN

El impacto de la internet en la vida cotidiana ha llevado a la modernización de las ciudades lo que se ha convertido en los principales puntos para el desarrollo de plataformas en la que se le atribuyen los distintos usos a nivel empresarial, educativo, gubernamental y comercial, lo que conlleva el incremento constante de la demanda de los servicios de telecomunicaciones (internet, telefonía fija y televisión), por lo cual les obliga a los proveedores de mencionados servicios realizar migraciones desde las redes tradicionales (cobre) hacia redes de fibra óptica de alta calidad.

Actualmente el uso frecuente de tecnología GPON (red ópticos pasivos de gigabytes) permite la convergencia de tres servicios (datos, video y voz) al mismo tiempo que el usuario final recibe una gran banda ancha, además, de que el alcance de distancia es cuatro veces mayor a las redes tradiciones de conexiones ADSL y VDSL, este estándar está aprobado y garantizado por el Sector de Normalizaciones de las Telecomunicaciones, cuya sede está ubicado en Suiza, dicha organización ha establecido normativas (ITU-T) que proporcionan información sobre las especificaciones y antecedentes para el desarrollo e implementación de la fibra óptica.

La corporación Nacional de Telecomunicaciones, Empresa Pública, es una institución que brinda servicios de televisión satelital, telefonía móvil y fija, e Internet, las mismas que se pueden adquirir en paquetes o en muchos casos solicitar solo un tipo de servicio como el de telefonía de línea fija. En lo que respecta en el área de internet la empresa en muchas de las ciudades del país aún tienen implementado redes tradicionales de cobre, sin embargo, en el año 2015 en la zona 1 en el Cerro Santa de la ciudad de Guayaquil iniciaron las primeras migraciones a las redes de tecnología GPON, la cual son áreas y canalizadas, siendo las bases para la expansión a las zonas de la ciudad que en la actualidad ya cuentan con el uso de estas redes bajo la norma ITU G.657.A2,

Por lo que concierne, debido a la antigüedad que presentan, el desgaste de la protección que contienen los dispositivos y la demandan que está adquiriendo esta tecnología los convierte en puntos sensibles ante posibles ataques cibernéticos tanto a nivel físico y lógico.

Por lo antes mencionado la presente investigación se proyecta al estudio de la necesidad de las medidas de seguridad de las redes de fibra óptica GPON de la red de CNT-EP, con el propósito de establecer los principales puntos de vulnerabilidad ante futuros ataques y las amenazas más comunes que pueden existir en la mencionada red.

Para el análisis y elaboración del presente trabajo de investigación se va a emplear la metodología cuantitativa, la misma que utiliza como recopilación de datos la técnica de la encuesta y como instrumento el cuestionario, lo que permitirá la evaluación de la opinión de las personas encuestadas.

La línea de investigación es Sistemas de información y comunicación, emprendimiento e innovación y la sub línea redes y tecnologías inteligentes de software y hardware.

DESARROLLO

La popularidad de Internet en la familia es el medio básico para hacer frente a la pandemia. La digitalización de viviendas permite a los residentes seguir realizando muchas tareas diarias que antes requerían contacto físico. Revelar la brecha digital existente entre y dentro de los países y su impacto en la igualdad. La conectividad de los países / regiones está más enfocada a fines de entretenimiento, transformada en redes sociales, transmisiones de audio y video, y ahora es más importante para obtener servicios productivos y socialmente significativos. (Agudelo, y otros, 2020).

Debido al incremento de la demanda de la utilización del internet en los últimos tiempos se ha requerido que las tecnologías que permiten la prestación de este servicio se mantengan en constante mejora, puesto que las actividades a nivel educativo, laboral, productivo y entre otras áreas actualmente se realizan y concluyen por el uso del internet, por ende, cada vez se necesita el uso de más banda ancha hacia al usuario final dejando atrás las redes de cobre y migrando a las redes de fibra óptica.

El monitoreo en la fibra óptica juega un papel fundamental ya que permite la mejora de la productividad del personal técnico y la gestión de las redes de forma remota manteniendo la respectiva documentación de las incidencias ocurridas y con ello poder medir el rendimiento de la red a largo plazo, además, de permitir que el sistema no se mantenga caído por mucho tiempo gracias a la precisión que puede brindar ante los fallos de la misma. (Viavi Solutions INC., 2020).

La seguridad de los datos es un aspecto primordial para las personas ya que les dará la garantía de realizar sus actividades con el uso del internet sin tener riesgo al robo de datos delicados que vayan circulando por medio del cable, por ende, las empresas que brindan servicios de

telecomunicaciones deben de tener los protocolos adecuados para poder garantizar a los usuarios la confiabilidad, integridad y la disponibilidad de la información. (Tecon, 2019)

La presente investigación proyecta el estudio de las medidas de seguridad en la red GPON de CNT-EP en la zona 1, sector Cerro Santa Ana de la ciudad de Guayaquil, además, de establecer los principales puntos de vulnerabilidad ante futuros ataques y las amenazas más comunes que pueden existir en la mencionada red.

La empresa CNT-EP es una de las instituciones que ofrece servicios de telecomunicaciones y lo que respecta en tecnología GPON tiene alrededor 25 mil kilómetros de fibra óptica a nivel nacional, las cuales tienen alcance a 20 provincias y 22 cantones, además, por medio de esta misma red se brinda servicios (voz, datos y video), los cuales requieren de la disponibilidad de una gran banda ancha, la tecnología GPON permite mejorar el diseño de telecomunicaciones en las ciudades a la cuales tienen alcance lo que le da una ventaja competitiva a la empresa pública.

En la ciudad de Guayaquil empezaron las primeras migraciones de redes tradicionales a fibra óptica en el 2015 en la zona 1 en el Cerro Santa Ana de la ciudad de Guayaquil, las mismas que fueron áreas y canalizadas, siendo estas las bases para la expansión de las redes GPON a los demás sectores que actualmente son 500 kilómetros que conectan a la ciudad.

La Corporación Nacional de Telecomunicaciones, Empresa Pública, no está involucrada directamente al 100% en la instalación, mantenimiento y reparo de las incidencias que pueden presentar las redes GPON tanto las canalizadas como las áreas, debido a que la institución solicita los servicios de terceros que son los responsables de mantener el adecuado funcionamiento de la red.

Por medio de la infraestructura de planta externa se debe de realizar un presupuesto óptico en el cual no le afecte a la operatividad al momento de establecer el enlace con el equipo ONT. La potencia entregada por la OLT es de más 3db la misma que va disminuyendo por cada fusión, patcheo, splitter y la distancia del cable, por ende, la potencia adecuada para la ONT es de -26 db.

Uno de los inconvenientes que presenta la mencionada empresa es que, una vez realizada la instalación de la fibra óptica para el hogar, ellos no mantienen un plan de mantenimiento preventivo y, por ende, no conocen el estado actual de los protectores del cable hasta que este no presenta una caída del servicio. Al no tener el debido control en los protectores se convierte en una vulnerabilidad a la extracción de señal por medio de curvatura y esto ocasionaría que un usuario mal intencionado acceda a la información que cruza por el cable.

Es así, que al tener un ataque activo a la red se debe de conectar físicamente al cable y poder cambiar el estado de la información ya que él envió de los paquetes alterados en este caso se realiza de manera bidireccional provocando una denegación de servicio y en su efecto alteraría el servicio a los usuarios, Además, que en el ataque pasivo se estaría realizando el Eavesdropping la cual se robaría la información sensible, pero una de los puntos vulnerables que presenta esta tecnología es que el enlace ascendente se transmite en texto plano, por lo tanto, la información es vulnerada sin dificultad.

Por ende, al descuidar la protección física de las redes antiguas y las recién instaladas desencadenan dificultades a los usuarios ya que en las redes GPON canalizadas están expuestas a la humedad del ambiente en donde están situadas y a los roedores. Mientras que en las redes aéreas por los elementos externos como lo son los fenómenos ambientales atenúan al cobertor, siendo estos factores que debilitan y dañan el cable provocando que el sistema cambie a un estado de fuera de servicio.

La metodología que se empleó es la cuantitativa la cual establece (Hernandez Sampiere, 2017) Suele ser parte de la estructura teórica aceptada por la comunidad científica sobre la que se formula una hipótesis sobre la relación esperada de las variables que forman parte del problema de investigación. Su verificación se realiza mediante la recaudación de información, que se emplea la técnica de la encuesta y el cuestionario se utiliza como herramienta.

La encuesta como técnica es una indagación social que permite la recolección de datos por medio de la cuestión de un grupo determinado de sujetos, que tienen como principal objetivo poder medir la opinión respecto a los conceptos de la problemática de una investigación construida previamente. (Lopez & Fachelli, 2016)

La encuesta fue dirigida a los técnicos asignados en el área de la zona 1 del Cerro Santa Ana de la ciudad de Guayaquil, los mismos que son un total de 10 personas, mediante la cual brindaron información para la realización del estudio de las medidas de seguridad.

El cuestionario como instrumento, está compuesto una lista de preguntas que permitirán adquirir de forma estandarizada la información, además, de ayudar a cuantificar las variables que son de utilidad para el desarrollo de una investigación. (Centro UC, 2019).

Referencias teóricas para el desarrollo de la investigación

La fibra óptica monomodo es aquella que únicamente permite un modo de propagación de luz dentro del núcleo siendo este paralelo con lo que respecta al eje de la fibra, permitiéndole alcanzar grandes distancias hasta un aproximado de 100km. Además, su ancho de banda puede ser de 10Ghz / Km y su diámetro suele ser de 8,1 a 125 micrones. Este tipo de fibra normalmente es aplicada en Campus, complejos industriales o TV por cable y redes de telecomunicaciones (Oscar, 2016)

Figura 1. Estructura de la fibra óptica monomodo. **Fuente** (Digital Azarias, 2016)

La Red GPON o Gigabit PON es una de las tecnologías que corresponden al diseño PON, la misma que está aprobado y recomendado por ITU-T, que son normas las cuales van tener los cables y la infraestructura dependiendo de cuál de las 4 recomendaciones se esté utilizando. Estas redes tienen como objetivo principal es de brindar un alto ancho de banda a diferencia de sus antecesoras y poder conseguir una mejor eficiencia en el transporte de los servicios que están basados en IP. La arquitectura de la red GPON son asimétricas lo que brinda hasta apropiadamente 2,488 Gbps, comparado con las anteriores tecnologías que van alrededor de 155 y 622 Mbps haciendo notar la evolución en escalabilidad y eficiencia (Sigcho & Ordóñez, 2018).

Las Recomendaciones UIT-R, establecido por (UTI, 2019) indica que componen una serie de medidas técnicas internacionales ejecutadas por el Sector de Radiocomunicaciones (anteriormente CCIR) de la UIT. Las mismas que son el resultado de análisis y estudios realizados por las Comisiones de Estudio de Radiocomunicaciones. Estas normativas indican los siguientes puntos según lo menciona (UTI, 2019):

- El uso de gama amplia en lo que respecta los servicios inalámbricos, conteniendo las tecnologías recientes de la comunicación móvil.

- La administración y el uso adecuado del espectro de radiofrecuencia, la cual cubre a todos servicios de radiocomunicación.
- Mejora en las radiocomunicaciones a través del satélite y la radiodifusión terrenal.
- Aumento en la transmisión de las ondas radioeléctricas.
- Eficiencia en las redes y sistemas orientados al servicio móvil, fijo y por satélite.

Las Recomendaciones UIT-R han sido aceptadas por consentimiento entre Miembros de la UIT, sin embargo, las aplicaciones de las mismas no son obligatorias, pero al ser elaboradas por expertos operadores y administradores que pertenecen al sector industrial e instituciones orientadas a las radiocomunicaciones alrededor del mundo, por ende, tienen una elevada reputación y su aplicación es a nivel mundial. (UTI, 2019).

Según (Unión Internacional de Telecomunicaciones, 2017) La fibra insensible a la flexión monomodo (G657) tiene una alta resistencia a la pérdida adicional causada por la macro flexión. Adecuado para montaje de cables, cables de puente y / o cables de interconexión en edificios. Además, son apropiado a la red de fibra al hogar o fiber to the home (FTTH).

PROPIEDADES GEOMÉTRICAS / MECÁNICAS	G.657.A1	G.657.A2 / B2	G.657.B3
Diámetro Revestimiento	125 ± 0.7 µm		125 ± 0.4 µm
Concentricidad Núcleo / Revestimiento	≤ 0.5 µm		≤ 0.3 µm
No Circularidad Revestimiento	≤ 0.7 %		≤ 0.3 %
Diámetro Recubrimiento Primario	242 ± 0.7 µm		242 ± 0.5 µm
Concentricidad Recubrimiento Primario / Revestimiento	≤ 12 µm	≤ 10 µm	≤ 12 µm
No Circularidad Recubrimiento Primario	≤ 5 %		
Proof Test	≥ 8.8 N / ≥ 1 % / ≥ 100 Kpsi		≥ 200 Kpsi

Figura 2. Propiedades Geométricas/Mecánicas de G.657.A1, G.657.A2/B2 y G.657.B3.
Fuente (Unión Internacional de Telecomunicaciones, 2017).

PROPIEDADES ÓPTICAS		G.657.A1	G.657.A2 / B2	G.657.B3
Atenuación con Curvatura* (1550 nm)	1 vuelta / Mandril 10mm	≤ 0.75	≤ 0.10	≤ 0.03
	10 vueltas / Mandril 15mm	≤ 0.25	≤ 0.03	
	1 vuelta / Mandril 7.5mm			≤ 0.08
	1 vuelta / Mandril 5mm			≤ 0.15
Diámetro Campo Modal (µm)	1310 nm	9.0 ± 0.4	8.5 – 9.3	8.8 ± 0.4
	1550 nm	10.1 ± 0.5	9.4 – 10.4	9.8 ± 0.5
Coeficiente Atenuación (dB/Km)	1310 nm	≤ 0.35	≤ 0.35	≤ 0.35
	1383 nm	≤ 0.35	≤ 0.35	≤ 0.35
	1460 nm	≤ 0.25	≤ 0.25	
	1550 nm	≤ 0.21	≤ 0.21	≤ 0.22
	1625 nm	≤ 0.23	≤ 0.23	≤ 0.24
Dispersión Cromática (ps/nm.Km)	1285 – 1330 nm	≤ |3|		
	1550 nm	≤ 18		
	1625 nm	≤ 22		
Longitud Onda Cero Dispersión (nm)		1300 – 1322	1300 – 1324	1300 – 1324
Pendiente Dispersión Cero (ps / nm^2 Km)		≤ 0.090	≤ 0.092	≤ 0.092
Longitud Onda Corte Cable (nm)		≤ 1260		
PMD (ps / (ps/√Km)	1550 nm	≤ 0.1		

Figura 3. Propiedades Ópticas de G.657.A1, G.657.A2/B2 y G.657.B3. **Fuente** (Unión Internacional de Telecomunicaciones, 2017)

La arquitectura que adopta la red GPON es la de punto a multipunto, por lo que se considera que la topología la cual utiliza es la de Árbol, la cual conecta por medio de los distribuidores pasivos al OLT y el ONT, este tipo de topología tiene como característica repartir la señal a los usuarios finales. Para la prevención de colisiones y evitar la pérdida de información los datos ascendente o upstream que comienzan a partir de la ONT al OLT, son transmitidos en un volumen de onda diferente a la trasmisión descendente o downstream. (Sigcho & Ordóñez, 2018).

Los paquetes que emite el enlace ascendente o upstream son enviados a través del ONT en forma Time División Múltiple Access (TDMA), los mismos que se reúnen en el Splitter y van a cada OLT abandonado, además, el TDMA tiene la característica en que el ONT va a transmitir siempre y cuando sea necesario previniendo las colisiones de datos internamente. (NASeros, 2017)

Los paquetes que envía el enlace descendente o downstream son transmitidos por el OLT de manera broadcast Time Division Multiplexing (TDM), es decir, que los paquetes de datos son enviados a todos los ONTs y los splitters existentes se encargan de replicar los datos, en el modo TMD perennemente está emitiendo datos en un tiempo transitorio fijo, sin importar que estos estén o no disponibles. Los ONT se encargan de filtrar paquetes de datos lo que conlleva a que a pesar de que a todos les envían la misma información únicamente serán leídos aquellos que se tienen acceso, esto gracias a la encriptación. (NASeros, 2017).

La encriptación de las redes GPON de madera descendente es el AES, esta característica va a ser en función de proveedor de internet, pero recurrentemente utilizan el esquema avanzado de cifrado por bloques, es decir, que en caso de que se vulnere la señal no sabrá en primera instancia lo que se está transmitiendo. La clave de acceso es enviada al ONT correspondiente para que sea capaz de ser el único que reciba la información y no el resto de ONTs, que estén en la misma red. El AES cifra los datos en bloques de 16 bytes lo que equivale a 128 bits, Mientras en la señal ascendente no cuenta con ningún cifrado ya que es transmitida en texto plano por la fibra óptica. (Sigcho & Ordóñez, 2018)

Extracción mediante curvatura de la fibra

La fibra óptica proporciona un alto nivel de seguridad que no se puede interponerse a través de elementos eléctricos convencionales como lo puede ser la inducción electromagnética o conducción superficial y es difícil perforar ópticamente. La luz atraviesa el centro de la fibra con poco o ningún escape. Incluso si la intervención es exitosa, se puede detectar monitoreando la señal de luz recibida al final de la fibra, esto se debe a la debilidad de la energía óptica durante la recepción. Además, la FO no está sujeta a las interferencias de radiofrecuencia o electromagnética, siendo una propiedad importante por la confidencialidad que deben mantener las aplicaciones de

alto nivel. La fibra puede mantener una señal impecable bajo los entornos menos adecuados, hasta en casos de se llegue a irradiar bajo ningún pronóstico otra fibra no puede capturarla. (UTO, 2016).

A pesar de lo antes mencionados no se puede descartar el hecho de que se puedan conectar en la fibra óptica, debido a esto es necesario que se proteja de forma similar a los mecanismos de cobre, es así que en los tendidos de fibra se deben de colocar ductos para prevenir daños directos al cable, adicionando la protección extra de personas que se quieran acceder fijamente al cable. Sin embargo, la fibra óptica tiene una reputación de ser prácticamente inmune a los espionajes, existen diferentes tipos de ataque las cuales están orientados a extraer la señal óptica, brindándole acceso a un ataque a los paquetes que viajan por la conexión. A pesar de que escuchar por la fibra óptica es más difícil que en los mecanismos de cobre, con los elementos y habilidades correctas esto puede ser una realidad. Por ende, los datos transmitidos por la fibra óptica son significativos debido al alto banda de ancha siendo llamativo para un hacker. (Sigcho & Ordóñez, 2018)

La fibra óptica remite una luz desde el transmisor hacia el receptor. En caso de que esta no llegue a ser trasmitida y tampoco recibida es probable que el cable a nivel físico este siendo maniobrado o se este enviado señal maliciosa por hackers. Aunque al intentar extraer la señal se disperse logrando que no llegue a su destinatario, existen técnicas las cuales permiten lograr la extracción de la señal sin que esta sufra caídas significativas en la potencia, lo que lo hace casi indetectable por las técnicas que emplean ciertas instituciones para la detección de estas incidencias. (Sigcho & Ordóñez, 2018).

La Extracción de la señal se obtiene cuando la fibra se dobla, el ángulo del incidente en la pared del núcleo cambiará por lo que no toda la luz se refleja, debido a una pequeña parte de la refracción. Si recolectamos la luz refractada, es altamente posible poder regenerar la señal. A pesar que el escape de información sea de 1 – 2% es suficiente, ya que este representa el 100% de los

datos que se transmiten, esto es posible ya que el revestimiento no es capaz de reemplazar la luminosidad al núcleo, provocando que se pierda a través de él. (CBD, 2016)

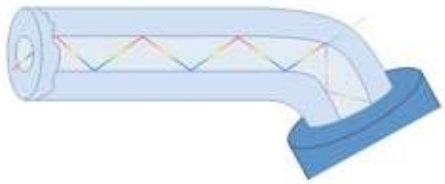


Figura 4. Refracción de la luz a través de la curvatura por fibra óptica. **Fuente** (CBD, 2016)

En la actualidad existen dispositivos diseñados para extraer la señal, aunque estos elementos pueden suministrar bastante atenuación, pero una vez conectado son difícilmente detectados ya que se puede confundir con una abertura o con un conector que ambos provocan atenuaciones en la señal. Por ende, cuando se extrae la información esta es retrasmitida a otro dispositivo que admita la recomposición de los datos a nivel de enlace, este procedimiento es complejo ya que en ciertos casos se tendrá que demultiplexar las distintas longitudes de la señal. (Sigcho & Ordóñez, 2018).

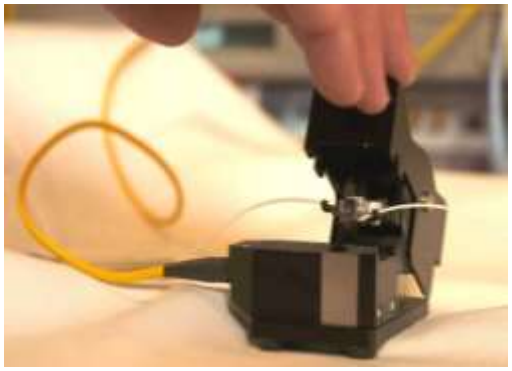


Figura 5. Dispositivo de extracción de fibra óptica – FOD 5503. **Fuente** (CBD, 2016)

Para (Sigcho & Ordóñez, 2018) el procedimiento de extracción de señal es la siguiente:

1. Se coloca un acoplador de microcovertura, para filtrar una cantidad pequeña de señal óptica;
2. Se recoge la señal por medio de detectores óptico;
3. Se pasa a un convertidor fotoeléctrico, la cual transporta la señal transformada, por medio de la conexión de Ethernet a un computador portátil;
4. Se examina con un sistema Snnifer como Wireshark.

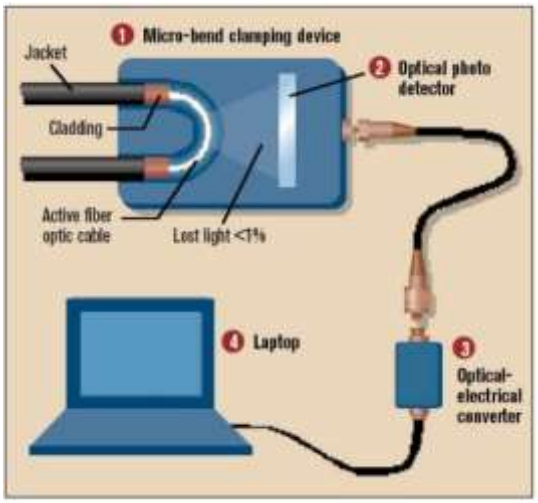


Figura 6. Procedimiento de Extracción de la señal en la fibra óptica. (TechTarget, 2016)

Las amenazas hacia la seguridad de la información pueden ser pasivas que pertenecen a la divulgación de datos delicados sin que el estado del sistema cambie y en estas actividades se incluyen la captura de información sea este encriptado o texto plano, mientras, que las activas se encargan de cambiar el estado del sistema y están presente en las actividades de denegación de sistema u ocultación en las situaciones de entidad autorizada (Sigcho & Ordóñez, 2018), además, establece categorías dependiendo del objetivo del atacante.

- Degradación en la calidad de servicios,
- Eavesdropping,
- Análisis de tráfico,

- Spoofing (Suplantación de identidad)

En las redes GPON el dowstream se emite en manera de broadcast, es decir, los datos llegan a todos los ONT/ONU en esa red, en el caso de que existe un usuario malicioso podría reprogramar su ONT y sería capaz de conocer escuchar todos los datos en el sentido dowstream de los usuarios que estén conectados al mismo OLT, esta amenaza se la conoce como escucha indebida, siendo uno de los inconvenientes a solucionar un sistema de seguridad de red GPON (ITU, 2020)

Por otro lado, dado que la arquitectura de la red GPON en el enlace ascendente es punto a punto, la ONT / ONU no puede observar el tráfico ascendente de otra ONU en la red GPON, donde los datos solamente se transmiten desde la ONT / ONU a él OLT, permitiendo que la información interna se emita upstream sin cifrar. (ITU, 2020)

Las comunicaciones GPON son susceptibles a problemas de seguridad graves, y dichas amenazas de seguridad se pueden tratar mediante mecanismos de seguridad implementados en la capa física o en la capa superior.

OLT Falsificado

En la actualidad no existen componentes de autentificación e identificación para los OLT, por lo que la ONT / ONU no puede detectar la OLT incorrecta. La unidad ONU / ONT puede ser autenticada por el número de serie de la OLT, pero la OLT no puede autenticarse, esto representa una amenaza, porque si un atacante puede acceder a la infraestructura de la red, puede agregar una OLT incorrecta y por lo tanto puede acceder a todo el tráfico que va pasando por la red GPON. (Sigcho & Ordóñez, 2018)

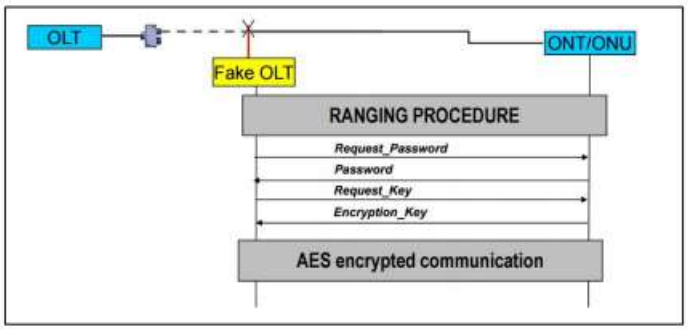


Figura 7. Falsificación de OLT. **Fuente** (TELECOM ITALIA GROUP, 2016)

Ataques (Man In The Middle- Hombre en el Medio)

Los Ataques pasivos para (Sigcho & Ordóñez, 2018) son la contraseña y la clave que se envían en texto sin cifrar, lo que es atractivo para que el atacante pueda interceptar el tráfico de datos, la cual incluye la información confidencial (no cifrada), como lo pueden ser claves de cifrado y contraseñas de autenticación que luego se utilizaran como, por ejemplo, la intercepción ilegal. Es decir, que el trafico puede ser interceptado añadiendo un ONT falso, facilitando el acceso a las claves de autenticación, debido que las mismas viajan a través de la red en texto plano.

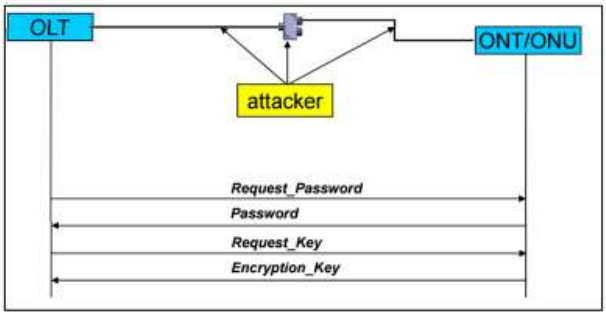


Figura 8. Intercepción de tráfico**. Fuente** (TELECOM ITALIA GROUP, 2016)

Ataques Activos según (Sigcho & Ordóñez, 2018) consiste en que los mensajes sensibles de Physical layer OAM messaging cannel (PLOAM) no se autentican como las claves y contraseñas de encriptado, por ende, los atacantes tienen la capacidad de editar información confidencial y que no esté cifrada y así se genere una denegación de Servicios.

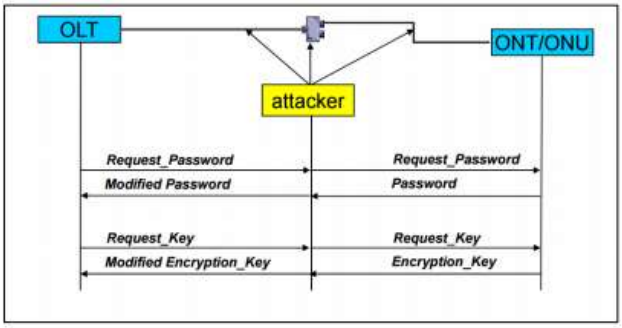


Figura 9. Modificación de información. (TELECOM ITALIA GROUP, 2016)

Los OLT transmites los datos en periodos de tiempos en la que consiste que cada ONT tiene esta misma propiedad, pero cuando estén disponibles, pero, los datos no se encriptan de ninguna manera lo que se convierte en un atributo relevante, debido a que el atacante desde el sentido descendente podrá leer las tramas transmitidas con tan solo tener el acceso físico a la fibra o al splitter. (Horvath, Munster, & Filka, 2016)

El splitter comúnmente se encuentra en un edificio o en un territorio accesible a todo público y en el sentido upstreams la comunicación de los paquetes es de manera unicast, por lo tanto, la persona maliciosa puede tocar la fibra antes del divisor. (Horvath, Munster, & Filka, 2016)

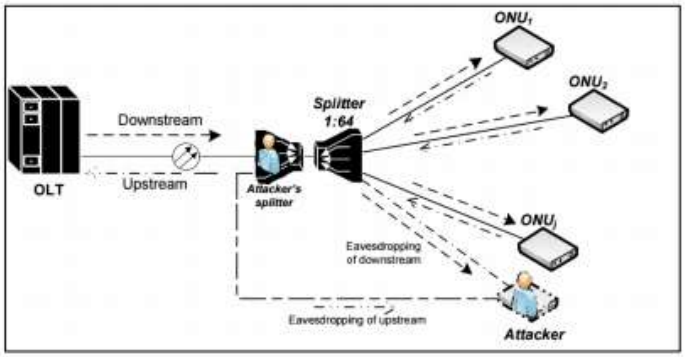


Figura 10. Descripción cuando el atacante puede escuchar en ambos sentidos**. fuente** (Horvath, Munster, & Filka, 2016)

Estado actual y medidas de seguridad físicas y lógicas de la red GPON de CNT-EP, en la zona 1, del Cerro Santa Ana de la ciudad de Guayaquil.

DESCRIPCIO	DISTRIB	DISTRITO	ARMARIO	CAJA	DIRECCION A	DIRECCION PARAMETRIZADA ACTUAL	
GPON. BOYA	4686	4686	F01M02	A1		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	A2		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	A3		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	A4		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	B1		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	B2		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	B3		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	B4		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	C1		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	C2		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	C3		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	C4		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	D1		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	D2		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	D3		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	D4		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	E1		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	E2		CERRO SANTA ANA 0	
GPON. BOYA	4686	4686	F01M02	E3		CERRO SANTA ANA 0	

Tabla 1. Lista de NAPs activas. Fuente: Consorcio Nplay

La tabla 1 nos indica la totalidad de Naps (19), además de información como: la descripción, distribución, distrito, la caja, y la dirección paramétrica que este situada en la zona 1, específicamente en el Cerro Santa Ana.

Figura 11. Alcance Geográfico en el espacio de estudio. Fuente: Consorcio Nplay.

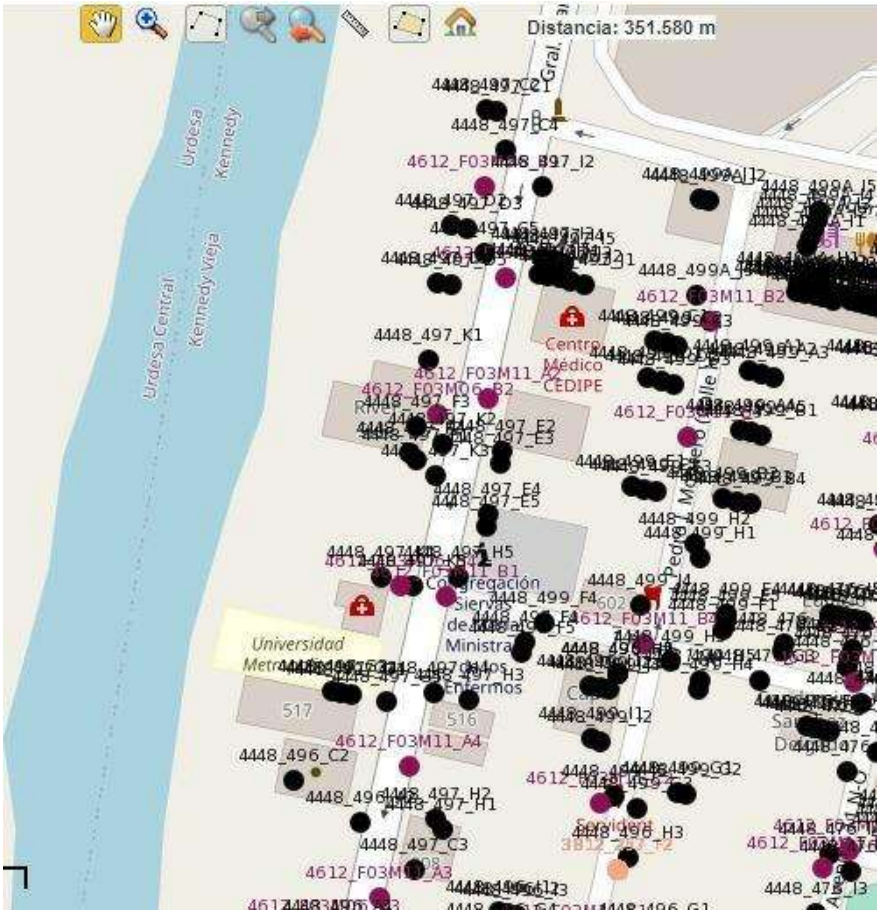


Figura 12. Ubicación Geográfica de las NAPS. Fuente: Consorcio NPlay

La figura 12 nos muestra las naps georreferenciadas distribuida en el Cerro Santa Ana (puntos rojos) y de los cajetines de cobre (puntos negros).

Figura 13. Medición con Power Meter. Fuente: Consorcio NPlay

En la figura 13 el uso del power meter es la de medir la potencia absoluta de la Nap(network access point) y con ello establecer si es factible realizar el enlace del servicio hacia el cliente. Una vez teniendo la potencia de la Nap realizamos el tendido de la fibra (aérea-canalizada), Teniendo en cuenta que la diferencia maxima que debe haber entre ambas potencias debe estar dentro del rango de -1,40.

Figura 14. Medición con OTDR. Fuente: Consorcio NPlay

La figura 14 La medición con OTDR nos muestra la perdida de la potencia, mide la longitud de la fibra y localiza fallos.

El sistema de monitoreo que emplea CNT-EP en la gestión de la seguridad es la U2000 la cual es un sistema que implementados en las OLT tanto corporativas como en las redes masivas (GPON), la cual permite la detección a nivel lógico de vulnerabilidades como la ONT intrusa, la extracción de la señal por medio de la curvatura y la ruptura de la señal de la fibra óptica. Las OLT

se encuentran ubicadas físicamente en una cámara denominada RAP, la cual cuentan con un control de acceso al personal autorizado, reportado al sistema con los cambios que se van a realizar, control de climatización, tarjetas de podes principal como la backup y la energía comercial, permitiendo que la fibra óptica no tenga inconvenientes a niveles eléctricos.

Descripción de los ataques que detecta el U2000 y las medidas de seguridad que se ejecutan a nivel lógico.

U2000 NMS GPON			
DETECCIÓN DE ATAQUE	**DESCRIPCIÓN**	**ALARMA**	**ACCIÓN DE SEGURIDAD**
ONT intrusa	Cada ONT posee un número de serie único, permitiendo solo la conexión a ONTs con un número de serie conocido por la red. Hasta que el administrador no apruebe su admisión en la red no podrá transmitir datos a la OLT.	**Minor** Se genera una alarma de prioridad menor (color amarillo), con la cual el operador de red se percata el lugar específico en que una ONT intrusa pretende conectarse.	En el proceso de activación de una ONT a la red, la OLT mediante un mensaje PLOAM pide el número de serie, al no estar este número de serie registrado en la red la OLT pone en estado de parada de emergencia a dicha ONT, donde la misma no podrá enviar tráfico a lared hasta que el administrador lo autorice.

Tabla 2. Seguridad que brinda el Sistema de Gestión de Seguridad U2000 para la ONT intrusa. **Fuente:** (Sigcho & Ordóñez, 2018)

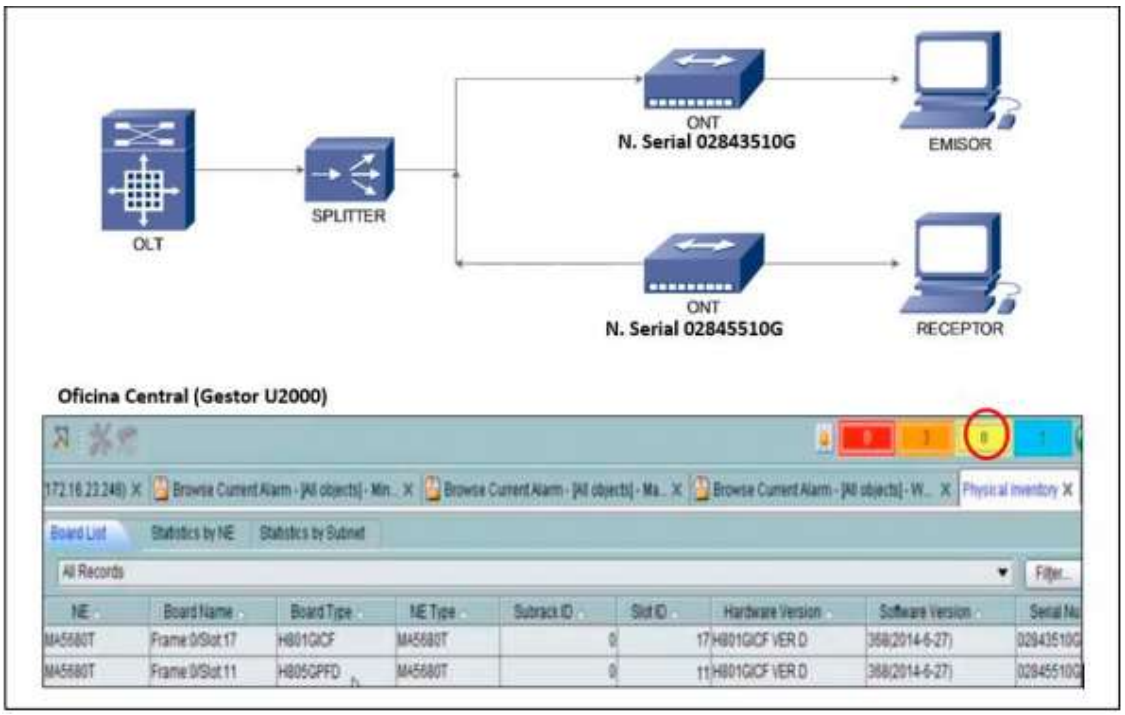


Figura 15. U2000 detección de una ONT Intrusa. **Fuente:** (Sigcho & Ordóñez, 2018)

Extracción de señal mediante curvatura de fibra	La adquisición de las potencias que reciben los equipos de la red, nos permite conocer en todo momento la atenuación que introduce la red en la señal y alertar de posibles alteraciones en ella. Al realizarse una extracción de la señal mediante curvatura, la señal de potencia baja, ya que la extracción de señal produce una pérdida de potencia recibida y permite al sistema informar sobre ello.	**Major** Se genera una alarma de prioridad mayor a la anterior (color naranja), ya que en este caso se ha producido la extracción de la información, y no hay forma de evitarlo, por tanto es importante, actuar de forma inmediata.	Verificación del punto donde estamos perdiendo potencia en la red, para de esta manera, evitar que el personal malicioso siga robando la información que está circulando a través de la red. Tomando en cuenta que la información que está circulando está cifrada en AES-256.

Tabla 3. Seguridad que brinda el Sistema de Gestión de Seguridad U2000 para la extracción de la señal por medio de la curvatura **Fuente:** (Sigcho & Ordóñez, 2018)

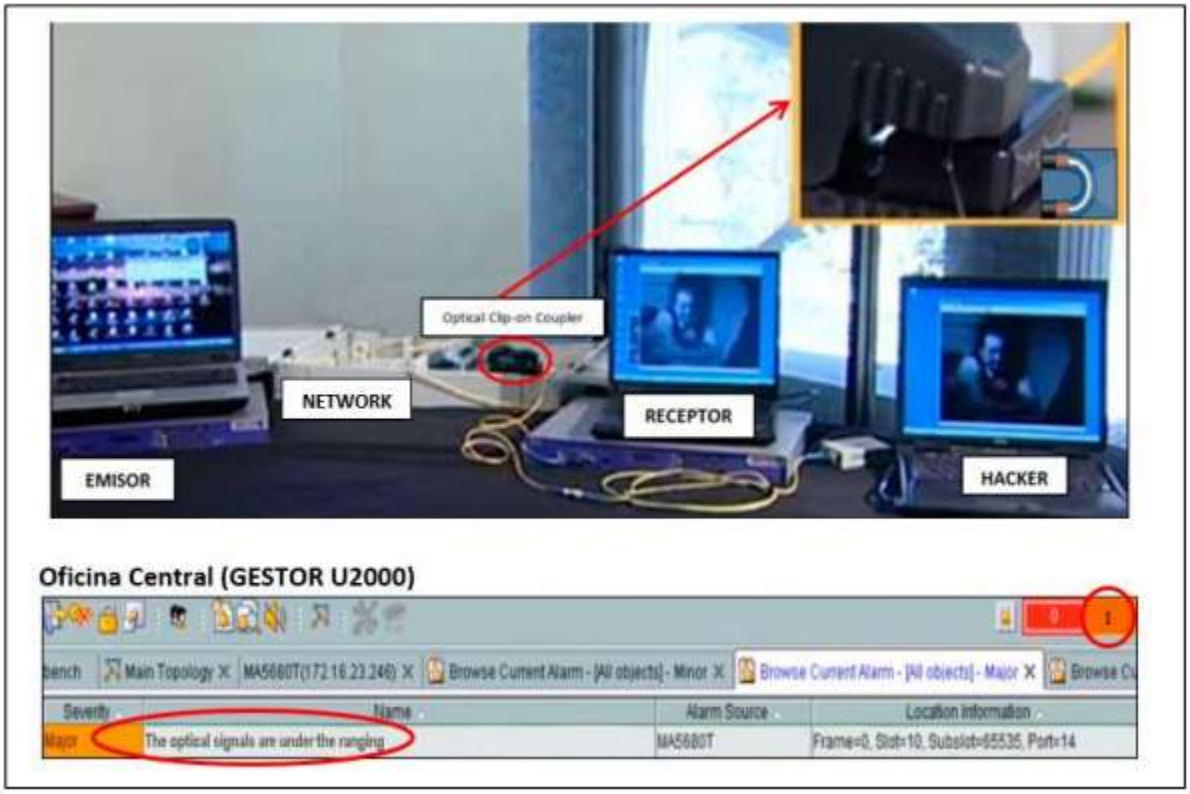


Figura 15. U2000 detección de la extracción de la señal por medio de la curvatura.

Fuente: (Sigcho & Ordóñez, 2018)

Ruptura de fibra	Controla el estado de conexión de los equipos, esto permite que el sistema proporcione un aviso en caso de que un equipo de la red se ha quedado sin conexión poniendo en peligro la seguridad de la misma.	**Critical** Se genera esta alarma (color rojo), debido a que muestra un estado de la red más crucial.	Gracias a que esta plataforma calcula distancias, se puede localizar la ubicación de la ruptura de la fibra, por tanto, un técnico especializado se dirige al lugar correcto y procede a reparar la fibra.

Tabla 4. Seguridad que brinda el Sistema de Gestión de Seguridad U2000 para la ruptura de la fibra óptica **Fuente:** (Sigcho & Ordóñez, 2018)

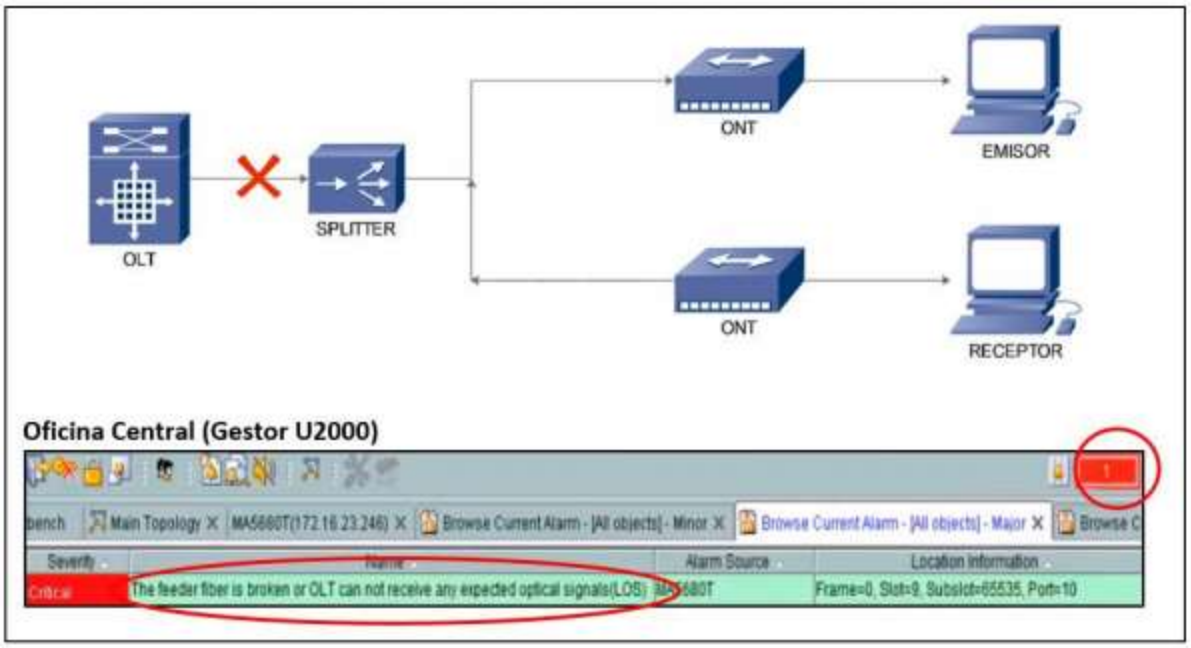


Figura 16. U2000 detección de la ruptura de la fibra óptica. **Fuente**: (Sigcho & Ordóñez, 2018)

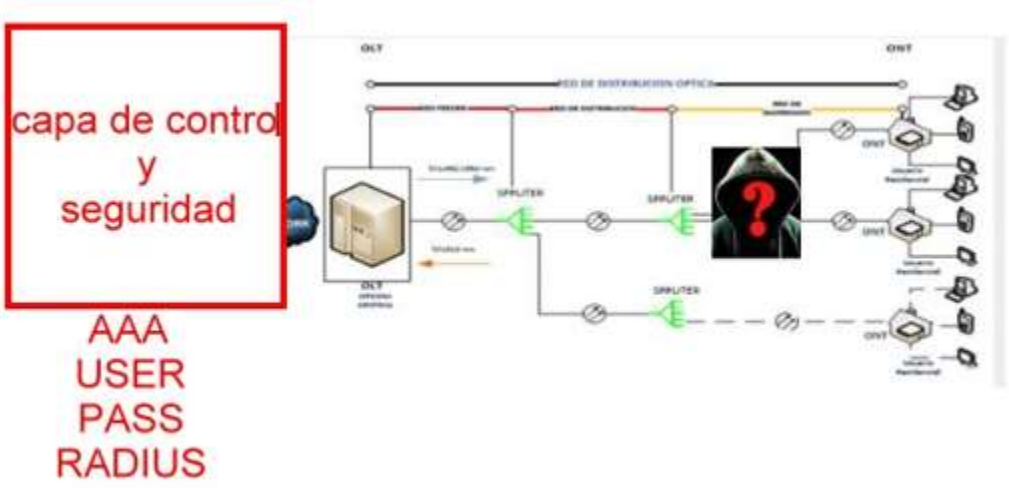


Figura 17. Medidas de seguridad para hombre en medio pasivo o activo. **Fuente:** CNT-EP

La figura 17 nos indica las medidas de seguridad para los ataques de hombre en medio tanto pasivo como activo se implementa una capa de control y seguridad en las cuales se valida el usuario, el password y la mac, las mismas que luego de autenticación entregan el servicio a cada uno de los clientes.

Análisis de los resultados obtenidos por la encuesta.

Pregunta 1: el 50% de las personas encuestadas consideran que la fibra óptica es relativamente ante ataques de hackers, mientras, que el 30% la creen segura y el 20% la suponen menos segura.

Pregunta 2: el 60% indicó que usualmente la fibra 30% menciono que a veces y el 10% estableció que siempre.

Pregunta 3: el 60% menciono que nunca se realizan mantenimientos en los protectores físicos de la fibra óptica, sin embargo, el 20% indicaron que a veces, aunque el 10% estableció que usualmente y siempre.

Pregunta 4: el 70% mencionaron que, si conocían la refracción de la luz por medio de fibra óptica, aunque el 30% dijo no saber.

Pregunta 5: el 70% mencionaron que, si conocían el OLT falsificado, mientras el 30% estableció no conocer.

Pregunta 6: el 50% de los encuestados aseguran conocer los ataques pasivos y activos en una red fibra óptica, pero el otro 50% manifestaron no saber.

Pregunta 7: el 60% mencionaron que la empresa CNT-EP no tiene establecido vulnerabilidades de las redes GPON.

Pregunta 8: el 60% de los encuestados aseguraron desconocer si la empresa cuenta con medidas de seguridad lógicas y físicas para la identificación de las posibles vulnerabilidades.

Pregunta 9: Todos los encuestados manifestaron que consideran muy importante que existan medidas de seguridad a nivel físico y lógico en las redes GPON.

Pregunta 10: Todos los encuestados indicaron que si participarían en capacitaciones respectos a los puntos vulnerables y principales amenazas que podrían existir en las redes GPON.

CONCLUSIONES

A partir de los resultados adquiridos por medio de la encuesta y la información proporcionada se realizan las siguientes conclusiones a discutir.

La red GPON de CNT-EP en la zona 1, del Cerro Santa Ana de la ciudad de Guayaquil usualmente presenta incidencias tanto en las redes canalizadas como en las aéreas, ya sea por roedores, manipulación por parte del cliente a las rosetas y daños en los conectores.

Los mantenimientos de los protectores físicos de la fibra óptica no se efectúan constantemente, las cuales estas son reparadas cuando se notifica la caída del enlace en un usuario especifico o en una NAP.

Los técnicos tienen conocimientos respectos a la refracción de la señal por medio de la curvatura, considerada una vulnerabilidad física, mientras que de las lógicas ellos conocen los ataques pasivos y activos, pero no de los OLT Falsificado.

La empresa CNT-EP no tiene establecido vulnerabilidades en lo que respecta a las redes GPON, además, que sus técnicos desconocen si la institución cuenta con medidas de seguridad lógicas y físicas para la mencionada tecnología, sin embargo, consideran importante que existan las medidas de seguridad que les permita identificar las vulnerabilidades en la red y que si asistirían a capacitaciones de las mismas.

Por lo tanto, la seguridad a nivel lógico se monitorea por medio de U2000 sistema implementado en las OLT de nivel corporativo y masivo (red GPON) lo que le permite detectar las vulnerabilidades en el tráfico de la información tales como la ONT intrusa, la extracción de la señal por medio de la curvatura y ruptura de señal, las mismas que tienen por cada uno medidas de seguridad a ejecutarse en el caso de una posible vulnerabilidad, además, en los RAPs que se

sitúan las OLT tienen control de acceso bajo llave y notificación al sistema de la persona que acceda y lo que vaya hacer, control de climatización y cámaras de seguridad, pero, a nivel físico a lo que se refiere al cable que va a las naps y a las ONT no se maneja el proceso adecuado de mantenimiento a los protectores de la fibra óptica, lo que conlleva que los mismos presenten incidencias usualmente e inconvenientes al brindar el servicio de internet.

BIBLIOGRAFÍA

Agudelo, M., Eduardo Chamolí, Jesús, S., Nuñez, G., Jordan, V., Rojas, F., . . . Callorda, F. (2020). *Las oportunidades de digitalización en América Látina frente al covid-19.*

CBD. (14 de Febrero de 2016). *SEGURIDAD EN FIBRA ÓPTICA - PARTE I: FUNDAMENTOS, MÉTODOS DE EXTRACCIÓN Y RIESGOS*. Obtenido de http://www.securitybydefault.com/2012/02/seguridad-en-fibra-optica-parte-i.html

Centro UC. (2019). *Desarrollo de instrumentos de evaluación: Cuestionarios .* México.

Digital Azarias. (2 de Febrero de 2016). *Ingeniería Systems.* Obtenido de Medios de fibra óptica: http://www.ingenieriasystems.com/2013/02/redes-y-comunicaciones-i-medios-de_21.html

Hernandez Sampiere, R. (2017). *Metodología de la investigación 6ta Edición.* México D.F: Mc Grall Hill Education.

Horvath, T., Munster, P., & Filka, M. (2016). *A Novel Unique Parameter for Increasing of Security in GPON Networks.* Obtenido de https://jcomss.fesb.unist.hr/index.php/jcomss/article/view/82

ITU. (20 de Octubre de 2020). *G.984.3 : Redes ópticas pasivas con capacidad de gigabits: Especificación de la capa de convergencia de transmisión*. Obtenido de Recomendaciones G.984.3: https://www.itu.int/rec/T-REC-G.984.3/es

Lopez, P., & Fachelli, S. (2016). *Metodologia de la investigación social cuantitativa.* Barcelona.

NASeros. (3 de Marzo de 2017). *Cómo funciona una conexión de fibra. GPON y FTTH*. Obtenido de https://naseros.com/2017/03/13/como-funciona-una-conexion-de-fibra-gpon-y-ftth/#:~:text=Hay%20muchos%20tipos%20de%20multiplexaci%C3%B3n,de%20luz%20l%C3%A1ser%20o%20LED.

Oscar, S. C. (2016). *Modulo Introductorio principios generales del sistema de fibra óptica.* Buenos Aires.

Sigcho, A., & Ordóñez, Á. (2018). *Estudio de la seguridad en redes Gpon.* Loja.

TechTarget. (1 de Noviembre de 2016). *Optical network security: Inside a fiber-optic hack*. Obtenido de https://searchsecurity.techtarget.com/magazineContent/Optical-network-security-Inside-a-fiber-optic-hack

Tecon. (28 de Enero de 2019). *Simplificando la Tecnologia* . Obtenido de La seguridad de la información: https://www.google.com/search?sxsrf=ALeKk03lriQAyk9OG6eBASDFzbbMD-HW1A%3A1616014697640&ei=aW1SYLTJJvLy5gKXw7K4Cg&q=seguridad+de+la+informacion&oq=la+seguridad+de+las+infom&gs_lcp=Cgdnd3Mtd2l6EAMYADIICAAQFhAKEB46BwgjELADECc6BwgAEEcQsAM6BAgjECc6AggAOgQIABBD

TELECOM ITALIA GROUP. (2016). *Next Generation Access Network (in) security.* Londres.

Unión Internacional de Telecomunicaciones. (16 de Febrero de 2017). *G.657 : Características de las fibras y cables ópticos monomodo insensibles a la pérdida por flexión*. Obtenido de Recomendación G.657: https://www.itu.int/rec/T-REC-G.657/es

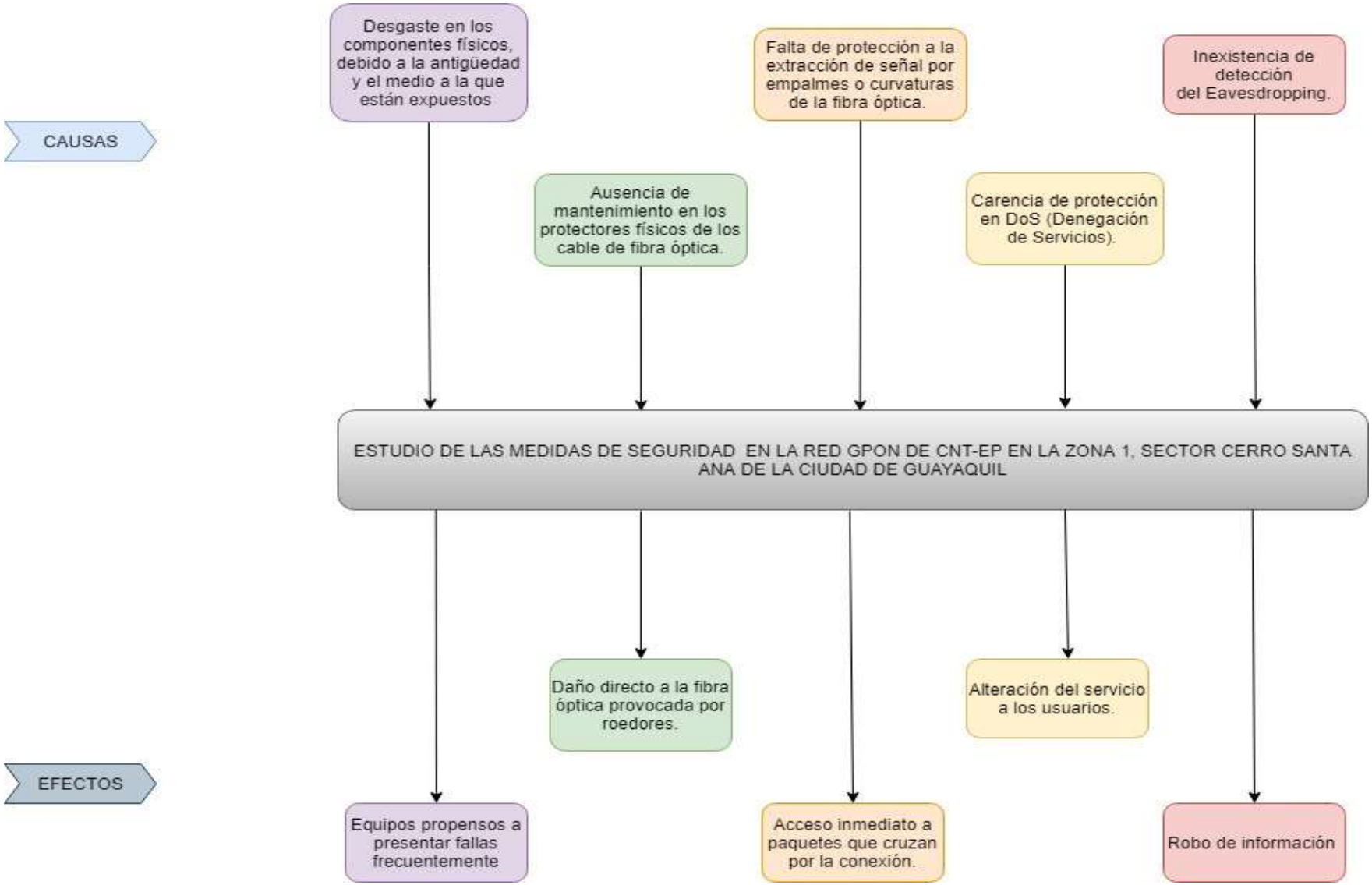
UTI. (2 de Mayo de 2019). *Recomendaciones UIT-R*. Obtenido de https://www.itu.int/pub/R-REC/es#:~:text=Las%20Recomendaciones%20UIT%2DR%2C%20constituyen,ex%20CCIR)%20de%20la%20UIT.

UTO. (2016). *Tópicos de Fibra óptica.* Bogota.

Viavi Solutions INC. (14 de Febrero de 2020). *ONMSi Sistema de monitorización de redes de fibra óptica*. Obtenido de https://www.viavisolutions.com/es-es/productos/onmsi-sistema-de-monitorizacion-de-redes-de-fibra-optica

ANEXOS

Anexo 1: Diagrama de Causa y Efecto



Anexo 2: Encuesta

Estudio de las medidas de seguridad en la Red GPON de CNT-EP en la zona 1, Sector Cerro Santa Ana de la ciudad de Guayaquil

El objetivo de la presente encuesta es de recolectar la opinión de los técnicos que laboran en el Cerro Santa Ana y posteriormente ser analizados en el caso de estudio.

1. **¿Qué tan segura considera usted la fibra óptica ante ataques de hackers?**
   - Muy Segura ☐
   - Relativamente Segura ☐
   - Poco Segura ☐
   - Nada Segura ☐

2. **¿Con qué frecuencia ocurren incidencias con la fibra óptica?**
   - Siempre ☐
   - Usualmente ☐
   - A veces ☐
   - Nunca ☐

3. **¿Con qué frecuencia se realizan mantenimientos en los protectores físicos de la fibra óptica?**
   - Siempre ☐
   - Usualmente ☐
   - A veces ☐
   - Nunca ☐

4. **¿Conoce usted lo qué es la refracción de la luz por medio de la curvatura de la fibra óptica?**
   - Si ☐
   - No ☐

5. **¿Conoce usted qué es un OLT Falsificado?**
   - Si ☐
   - No ☐

6. **¿Conoce usted los ataques pasivos (Eavesdropping) y activos (Denegación de Servicios) en la fibra óptica?**
   - Si ☐
   - No ☐

7. **¿Cuál de los siguientes ataques la empresa tiene establecido que son vulnerabilidades en la fibra óptica?**

- Extracción de la luz por medio de la curvatura de la fibra óptica ☐
- OLT Falsificado ☐
- Man In The Middle modo Pasivo ☐
- Man In The Middle modo Activo ☐
- No tienen establecido vulnerabilidades ☐
- Ninguna de las Anteriores ☐

8. **¿La institución cuenta con medidas de seguridad lógicas y físicas para la identificación de posibles vulnerabilidades en la fibra óptica?**

- Si ☐
- No ☐
- Desconozco ☐

9. **¿Qué tan importante cree usted son las medidas de seguridad que le permitan identificar las posibles vulnerabilidades que puedan existir en la red?**

- Muy Importante ☐
- Poco Importante ☐
- Nada Importante ☐

10. **¿Asistiría usted a capacitaciones con respecto a los puntos vulnerables y amenazas comunes que puedan existir en las Redes GPON?**

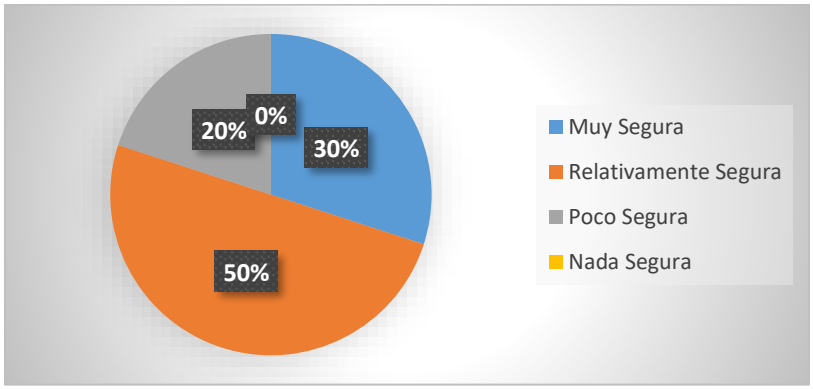
- Si ☐
- No ☐

Anexo 3: Tabulación de los resultados de la Encuesta

1. **¿Qué tan segura considera usted la fibra óptica ante ataques de hackers?**

Muy Segura	30%
Relativamente Segura	50%
Poco Segura	20%
Nada Segura	0%
Total	100%

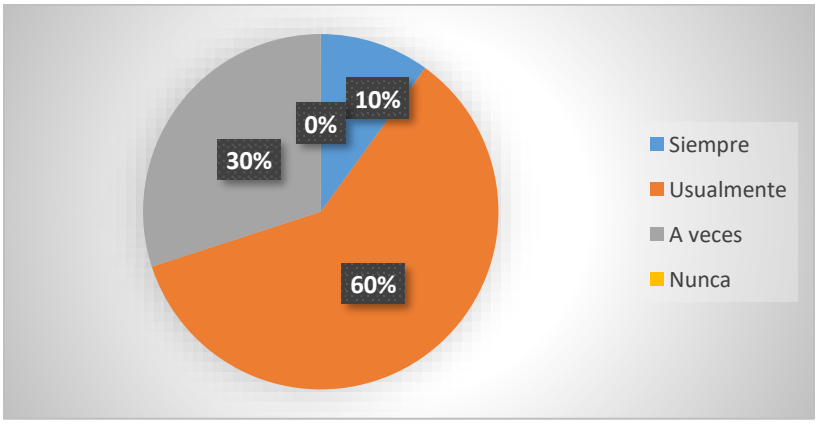
Elaboración: La Autora



2. **¿Con qué frecuencia ocurren incidencias con la fibra óptica?**

Siempre	10%
Usualmente	60%
A veces	30%
Nunca	0%
Total	100%

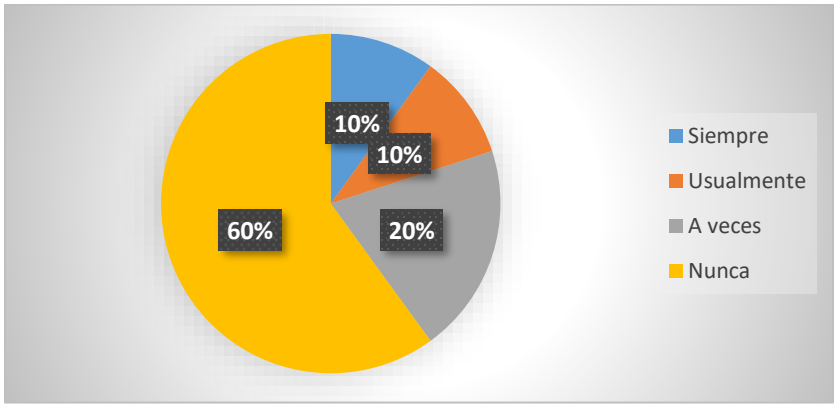
Elaboración: La Autora



3. **¿Con qué frecuencia se realizan mantenimientos en los protectores físicos de la fibra óptica?**

Siempre	10%
Usualmente	10%
A veces	20%
Nunca	60%
Total	100%

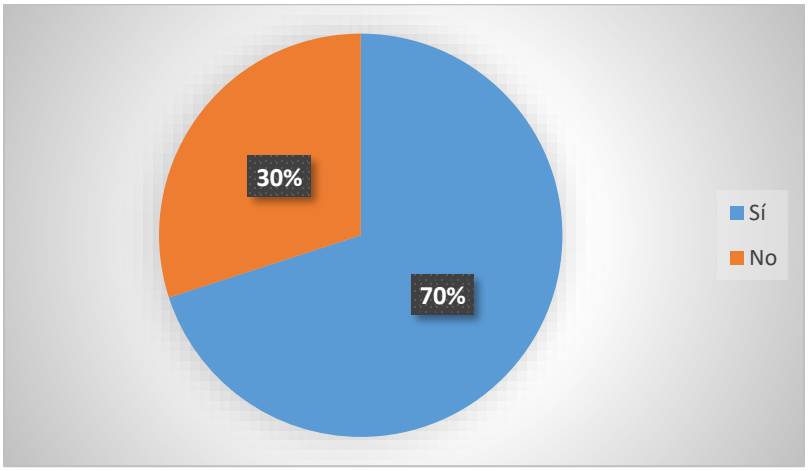
Elaboración: La Autora



4. **¿Conoce usted lo qué es la refracción de la luz por medio de la curvatura de la fibra óptica?**

Sí	70%
No	30%
Total	100%

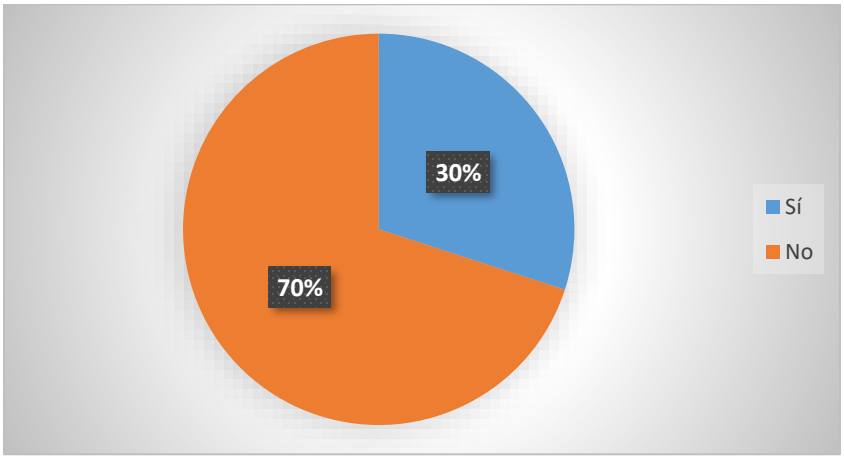
Elaboración: La Autora



5. **¿Conoce usted qué es un OLT Falsificado?**

Sí	30%
No	70%
Total	100%

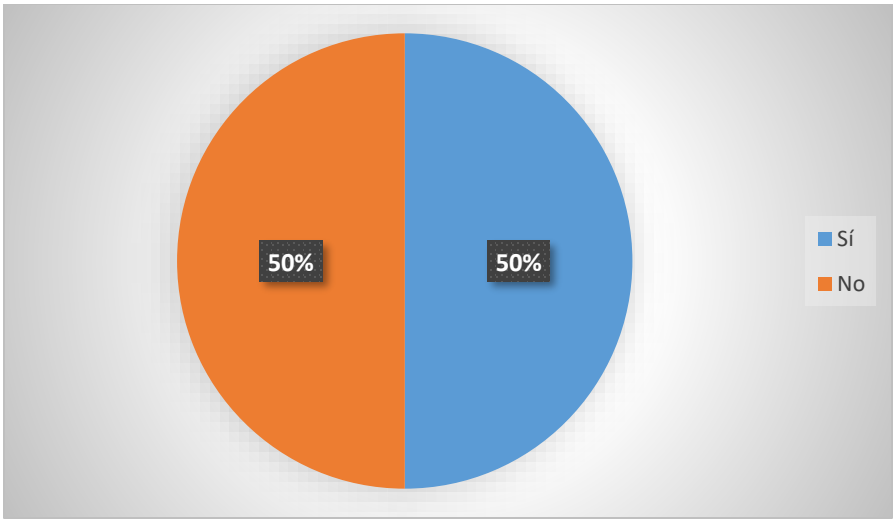
Elaboración: La Autora



6. **¿Conoce usted los ataques pasivos (Eavesdropping) y activos (Denegación de Servicios) en la fibra óptica?**

Sí	50%
No	50%
Total	100%

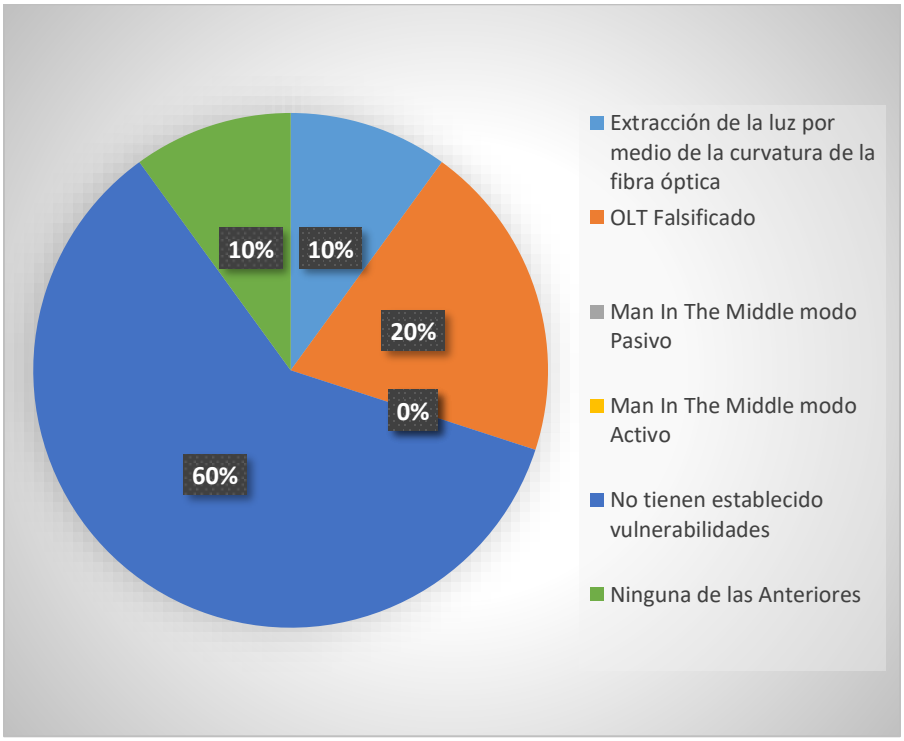
Elaboración: La Autora



7. **¿Cuál de los siguientes ataques la empresa tiene establecido que son vulnerabilidades en la fibra óptica?**

Extracción de la luz por medio de la curvatura de la fibra óptica	10%
OLT Falsificado	20%
Man In The Middle modo Pasivo	0%
Man In The Middle modo Activo	0%
No tienen establecido vulnerabilidades	60%
Ninguna de las Anteriores	10%
Total	100%

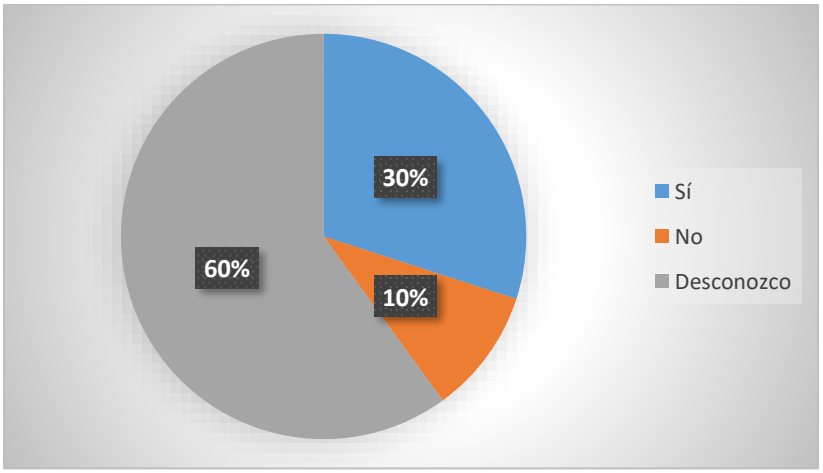
Elaboración: La Autora



8. **¿La institución cuenta con medidas de seguridad lógicas y físicas para la identificación de posibles vulnerabilidades en la fibra óptica?**

Sí	30%
No	10%
Desconozco	60%
Total	100%

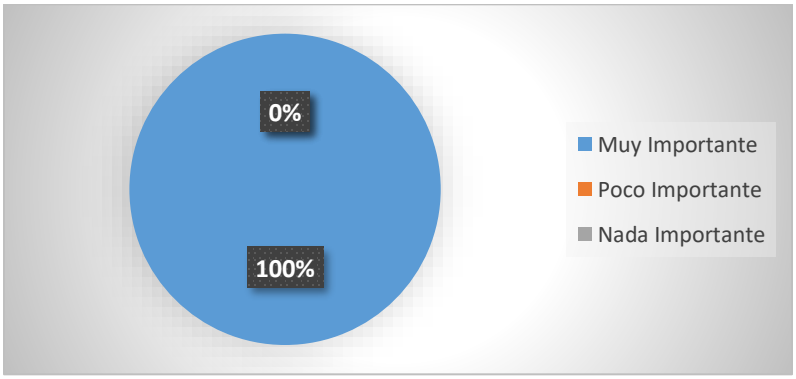
Elaboración: La Autora



9. **¿Qué tan importante cree usted son las medidas de seguridad que le permitan identificar las posibles vulnerabilidades que puedan existir en la red?**

Muy Importante	100%
Poco Importante	0%
Nada Importante	0%
Total	100%

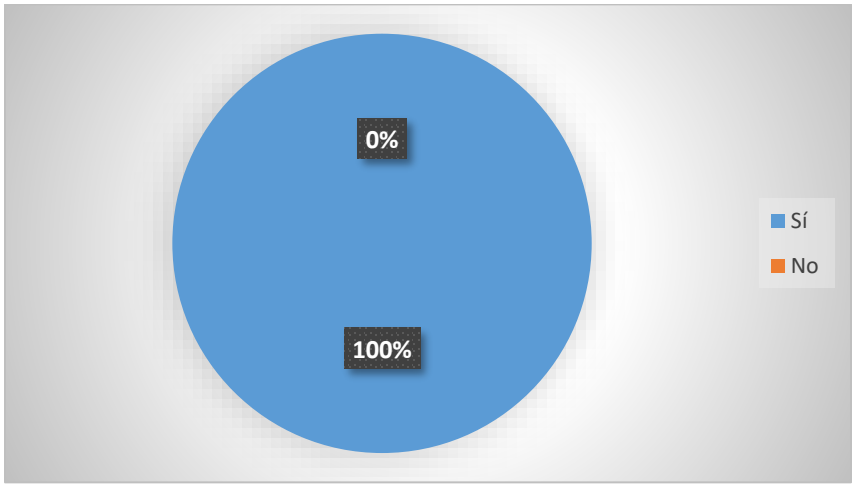
Elaboración: La Autora



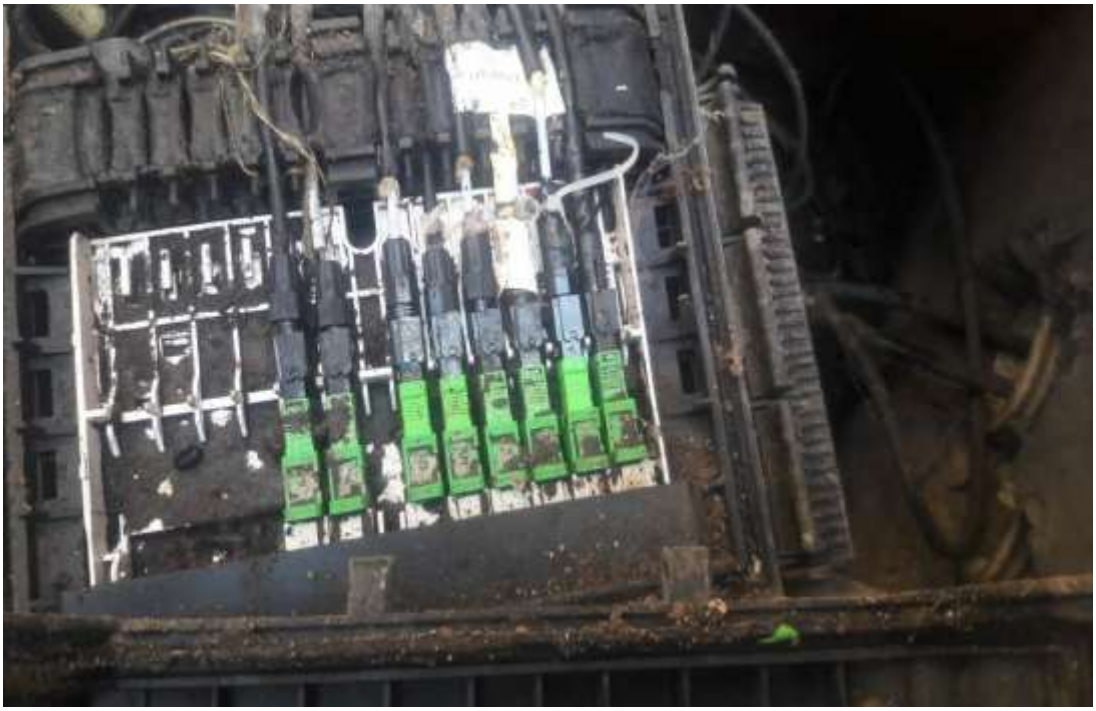
10. ¿Asistiría usted a capacitaciones con respecto a los puntos vulnerables y amenazas comunes que puedan existir en las Redes GPON?

Sí	100%
No	0%
Total	100%

Elaboración: La Autora



Anexo 4: Fotos de algunas instalaciones de redes GPON en el Cerro Santa Ana.




46
86
H2

Anexos 4: Solicitud y Autorización de la Empresa

UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Babahoyo, febrero 22 de 2021
D-FAFI-UTB-038-UT-2021

Ing.
Daniel Medrano Burgos
SUPERVISOR DE LA ZONA NORTE DE LA CIUDAD DE GUAYAQUIL DEL CONSORCIO NPLAY
Guayaquil. –

De mis consideraciones:

La Universidad Técnica de Babahoyo y la Facultad de Administración, Finanzas e Informática (FAFI), con la finalidad de formar profesionales altamente capacitados busca prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

La Señorita **SANTILLÁN VILLOTA CESIA JEMIMA,** con cédula de identidad No. 120684677-4, Estudiante de la Carrera de Ingeniería en Sistemas, matriculada en el proceso de titulación en el periodo Noviembre 2020 – Mayo 2021, trabajo de titulación modalidad Estudio de Caso para la obtención del grado académico profesional universitario de tercer nivel como **INGENIERA EN SISTEMAS.** El Estudio de Caso: **ESTUDIO DE LAS MEDIDAS DE SEGURIDAD EN LA RED GPON DE CNT-EP EN LA ZONA 1, SECTOR CERRO SANTA ANA DE LA CIUDAD DE GUAYAQUIL.**

Es por esta razón, solicito a usted, si es posible se sirva autorizar el permiso respectivo para que la Señorita **Santillán** pueda desarrollar la investigación en la institución de su acertada dirección.

Por su gentil atención al presente, se extiende el agradecimiento institucional.

Atentamente.

Lcdo. Eduardo Galeas Guijarro MAE.
DECANO

Recibido.
Autorizado.
07/03/2021

c.c Archivo

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanato@fafi.utb.edu.ec	Elaborado por: Mercedes Soto Valencia	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

CONSORCIO NPLAY

Guayaquil, marzo 07 del 2021
CNP - OFIC - 001 - DMB

Lcdo. Eduardo Galeas Guijarro MAE.
DECANO DE LA FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA DE LA UNIVERSIDAD TECNICA DE BABAHOYO.
Av. Universitaria K2 1/2 vía Montalvo
Tel: (05) 2572024

De mis consideraciones:

Yo, **DANIEL DAVID MEDRANO BURGOS**, con cargo de Supervisor Administrativo de la Zona Integral 1 en CNT por parte del CONSORCIO NPLAY, con cedula de identidad N° 120709983-7, por medio de la presente autorizo a la Señorita **CESIA JEMIMA SANTILLAN VILLOTA** el uso de la información de los trabajos realizados en la **ZONA 1** "instalaciones, reparaciones (DTH, GPON y COBRE)" asi como videos, fotos, audios y material escrito para los fines de investigación que se encuentra realizando.

Por la atención brindada les quedo agradecido, quedando a sus órdenes para cualquier duda, aclaración o comentario que pueda surgir en la información aquí presentada.

Saludos,

Daniel Medrano B.

Daniel Medrano, ING.
Supervisor
CONSORCIO NPLAY
E-mail: dmedrano@nplay.ec
Telefono: 0959064602
Guayaquil – Guayas