Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Maestría en Telecomunicaciones

Análisis de vulnerabilidades y amenazas de la red GPON del ISP TEKLINK CIA. LTDA.

Trabajo de Titulación previo a la obtención del título de Magíster en Telecomunicaciones

AUTOR:

Ing. Pablo Alexander Sanmartín Vásquez

DIRECTOR:

Ing. Andy Vega León, Mg. Sc.

LOJA – ECUADOR

2023

Certificación

Loja, 12 de mayo de 2023

Ing. Andy Vega León Mg. Sc.

DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Análisis de vulnerabilidades y amenazas de la red GPON del ISP TEKLINK CIA. LTDA**. Previo a la obtención del título de **Magíster en Telecomunicaciones,** de la autoría del estudiante **Pablo Alexander Sanmartín Vásquez**, con **cédula de identidad N° 1104261076,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

ANDY FABRICIO VEGA LEON
Firmado digitalmente por ANDY FABRICIO VEGA LEON
Fecha: 2023.05.18 10:45:06 -05'00'

Ing. Andy Vega León Mg. Sc.

DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, **Pablo Alexander Sanmartín Vásquez**, declaro ser autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación del Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma: Firmado electrónicamente por: PABLO ALEXANDER SANMARTIN VASQUEZ

Cédula de Identidad: 1104261076

Fecha: 17 de mayo de 2023

Correo electrónico: pasav25ing@gmail.com

Teléfono: 0998679500

Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica de texto completo, del Trabajo de Titulación.

Yo, **Pablo Alexander Sanmartín Vásquez**, declaro ser autor del Trabajo de Titulación denominado: **Análisis de vulnerabilidades y amenazas de la red GPON del ISP TEKLINK CIA. LTDA.**, como requisito para optar el título de **Magíster en Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los diecisiete días del mes de mayo de dos mil veintitrés.

Firmado electrónicamente por:
PABLO ALEXANDER
SANMARTIN VASQUEZ

Firma:

Autor: Pablo Alexander Sanmartín Vásquez

Cédula de Identidad: 1104261076

Dirección: Loja Ecuador

Correo electrónico: pasav25ing@gmail.com

Teléfono o celular: 0998679500

DATOS COMPLEMENTARIOS:

DIRECTOR DE TRABAJO DE TITULACIÓN: Ing. Andy Vega León Mg. Sc.

Dedicatoria

El presente trabajo se lo dedico con todo mi corazón, a mi familia que, sin su apoyo, su guía, y su amor incondicional, nunca habría llegado hasta aquí, en especial a Santiago, Ariana, Emmanuel y Viviana que han sido una fuente de inspiración y motivación para mí en cada paso del camino.

Pablo Alexander Sanmartín Vásquez

Agradecimiento

En primer lugar, mi agradecimiento a Dios por ser la guía en cada uno de mis pasos, a mi familia por su paciencia y comprensión mientras trabajaba en este proyecto. Sus palabras de aliento y sus consejos me ayudaron a mantenerme enfocado y a superar los momentos difíciles. Gracias por creer en mí y por estar a mi lado en todo momento.

A la UNL por brindar la oportunidad de promocionar nuevas maestrías a través de la modalidad virtual, así mismo a los docentes que han impartido sus conocimientos, los cuales permitieron desarrollar el presente trabajo de investigación.

A TEKLINK CIA. LTDA. por darme la oportunidad de realizar este proyecto, al brindarme la oportunidad de trabajar con ellos y entender sus necesidades.

Pablo Alexander Sanmartín Vásquez

Índice de Contenidos

Índice de Tablas:

Índice de Figuras:

Índice de Anexos:

1. Título

Análisis de vulnerabilidades y amenazas de la red GPON del ISP TEKLINK CIA. LTDA.

2. Resumen

En la actualidad la evolución global de las telecomunicaciones y la tecnología, ha generado una demanda por estar a la vanguardia, es así que los usuarios buscan suplir estas necesidades, es por esto que las empresas están implementando nuevas tecnologías para poder brindar servicios de banda ancha mejorada, una de estas tecnologías es la Red GPON (Gigabit-capable Passive Optical Networks).

El presente trabajo de titulación se enfoca en la red GPON de la empresa TEKLINK CIA. LTDA., la cual fue implementada para ofertar nuevos servicios a sus clientes y con ello generar una mejor competencia en su entorno.

Se inicia con el estudio de la infraestructura implementada, en la cual se detalla cada uno de los elementos, verificando los estándares de calidad e identificando las vulnerabilidades de la ODN, se continúa con las pruebas de la red GPON, esto nos ayuda a determinar los puntos críticos, estas pruebas se desarrollan desde diferentes escenarios, validando las políticas de seguridad implementadas, se finaliza el presente trabajo de titulación presentando procedimientos para mejorar la seguridad de la red GPON de la empresa TEKLINK CIA. LTDA., las mismas que están relacionadas con las existentes y ayudarán a mantener una red más segura.

Palabras Clave: Red GPON, vulnerabilidades, amenazas, ISP

2.1. Abstract

Currently, the global evolution of telecommunications and technology has generated a demand to be at the forefront. Users seek to meet these needs, which is why companies are implementing new technologies to provide improved broadband services. One of these technologies is the GPON (Gigabit-capable Passive Optical Networks) network.

This research focuses on the GPON network of the company TEKLINK CIA. LTDA., which was implemented to offer new services to its customers and generate better competition in its environment. It begins with the study of the implemented infrastructure, detailing each of the elements, verifying quality standards, and identifying vulnerabilities of the ODN.

It continues with the GPON network tests, which help to determine critical points. These tests are developed from different scenarios, validating the implemented security policies. Finally, this research presents procedures to improve the security of the GPON network of the company TEKLINK CIA. LTDA., which are related to existing ones and will help maintain a more secure network.

Keywords: GPON network, vulnerabilities, threats, ISP.

3. Introducción

Es fundamental realizar un análisis exhaustivo de las vulnerabilidades y amenazas en una red para garantizar la seguridad de los sistemas informáticos y los datos que se almacenan en ellos. En la actualidad, las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, por lo que las organizaciones deben tomar medidas proactivas para identificar y mitigar las vulnerabilidades existentes.

En este sentido, investigar las vulnerabilidades y amenazas en la red GPON de la empresa TEKLINK CIA. LTDA. puede ayudar a identificar los puntos débiles y tomar medidas preventivas y de mitigación para evitar posibles ataques. Esto puede garantizar la seguridad y protección de los sistemas informáticos, los datos y la infraestructura, cumpliendo con las normativas y estándares de seguridad. Es necesario implementar medidas de seguridad en la red GPON de la empresa TEKLINK CIA. LTDA. para proteger los datos y su confidencialidad, minimizando los ataques y manteniendo una infraestructura segura.

Este trabajo comienza con un marco teórico que explica los conceptos que se discuten. Luego, se detalla la red GPON de la empresa, estudiando sus fortalezas y debilidades para analizar las vulnerabilidades y amenazas. Finalmente, se presentan las conclusiones y recomendaciones del análisis desarrollado en todo el trabajo, exponiendo los resultados del análisis de las vulnerabilidades y amenazas discutidas.

Objetivos.

Objetivo General

Analizar las vulnerabilidades y amenazas que se puedan presentar en la red GPON de la empresa TEKLINK CIA. LTDA**.**

Objetivos específicos

- Analizar la infraestructura de la red GPON de la empresa TEKLINK CIA. LTDA. Ubicada en la zona urbana del cantón Catamayo.
- Identificar los puntos críticos que presenten vulnerabilidades y amenazas de la red GPON.
- Proponer recomendaciones y soluciones para mejorar la seguridad de la red GPON. de la empresa TEKLINK CIA. LTDA.

4. Marco Teórico

4.1. Red Óptica Pasiva con capacidad Gigabyte (GPON)

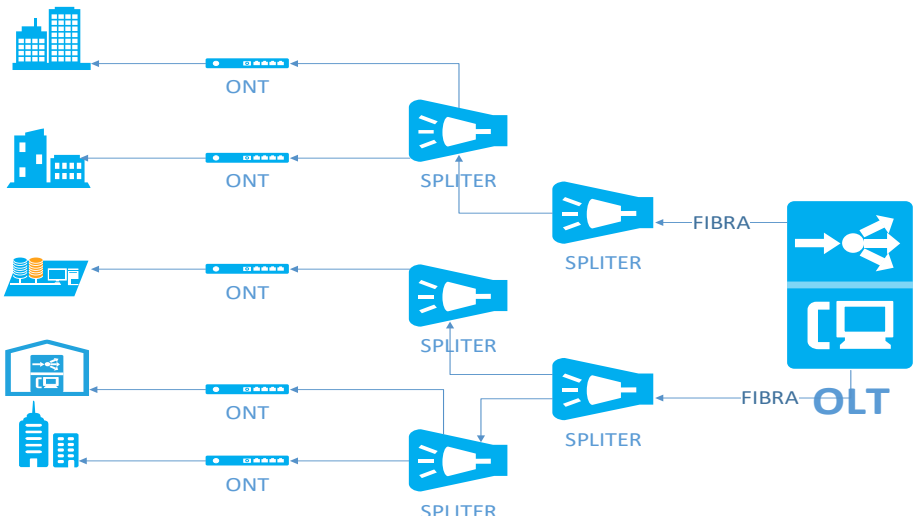
La tecnología GPON se refiere a una solución de comunicación de fibra óptica que facilita la transmisión de datos a largas distancias a velocidades extremadamente altas. En esta tecnología, una sola fibra óptica puede ser compartida por numerosos usuarios, lo que reduce significativamente la cantidad de fibra requerida para ofrecer servicios de alta velocidad. Además, la arquitectura de red pasiva de GPON elimina la necesidad de energía eléctrica activa en los puntos intermedios de la red, disminuyendo así los costos de operación y mantenimiento. Goh T., Lee K. L., (2014)

La transmisión de datos en una red GPON se lleva a cabo mediante señales de luz que se distribuyen a múltiples usuarios a través de un divisor óptico, lo que permite la transmisión de datos a velocidades de hasta 2,5 Gbps en la dirección descendente y hasta 1,25 Gbps en la dirección ascendente.

La Red Óptica Pasiva con Capacidad de Gigabit (GPON) es una tecnología de acceso de telecomunicaciones que utiliza fibra óptica para llegar hasta el suscriptor y sus estándares técnicos fueron aprobados por ITU-T en 2003-2004. Estas recomendaciones estandarizan las redes PON (Red Óptica Pasiva) a velocidades superiores a 1 Gbit/s, y posteriormente se han publicado recomendaciones adicionales, como G.984.6 y G.984.7, que extienden el alcance de la tecnología. Todos los fabricantes de equipos deben cumplir estos estándares para garantizar la interoperabilidad entre sus dispositivos. Goh T., Lee K. L., (2014).

Figura 1

Diagrama red GPON



Fuente: Adaptación Recomendación ITU-T G.984.1, 2009

4.1.1. Arquitectura GPON

La arquitectura de una red GPON (Red Óptica Pasiva con Capacidad de Gigabit) consta de tres componentes principales: la Optical Line Terminal (OLT), la Optical Network Unit (ONU) y la Optical Distribution Network (ODN).

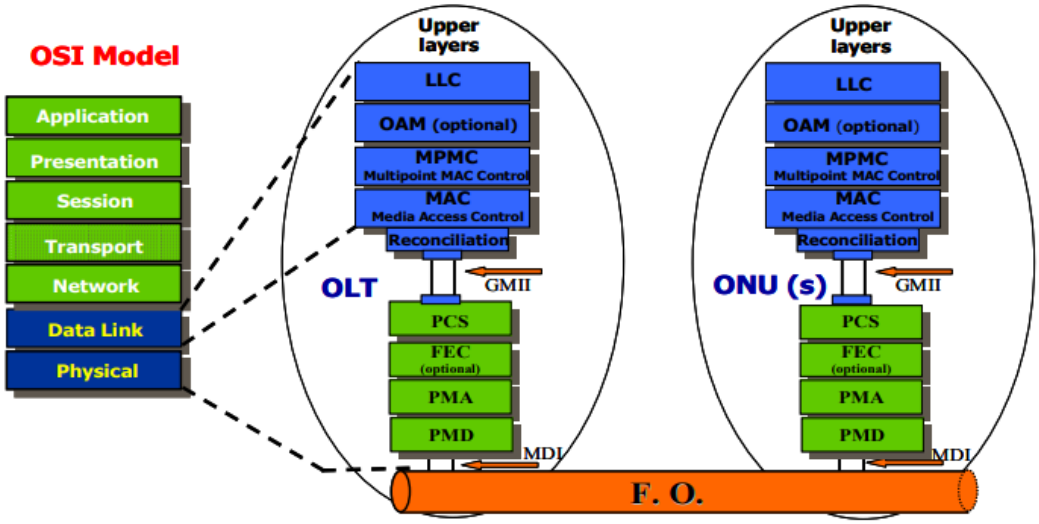
La OLT es el equipo que se encuentra en el extremo de la red de fibra óptica y se encarga de gestionar todas las comunicaciones entre la red de fibra óptica y los clientes. La OLT es responsable de enviar y recibir datos, así como de controlar el ancho de banda asignado a cada cliente. Goh T., Lee K. L., (2014)

La ONU es el equipo que se encuentra en el extremo del cliente y se encarga de recibir y enviar datos, voz y vídeo. La ONU se comunica con la OLT a través de la fibra óptica y se encarga de convertir la señal óptica en señal eléctrica para su uso por parte del cliente.

La ODN es la red de distribución óptica que conecta la OLT y la ONU. La ODN consta de cables de fibra óptica, splitters ópticos y otros componentes ópticos que se utilizan para dividir la señal en múltiples canales y distribuirla a los clientes. Goh T., Lee K. L., (2014),

Figura 2

Arquitectura red GPON



Fuente: Tomado de An overview of next generation PON technologies, IEEE Communications Surveys & Tutorials, vol. 16, no. 1, (p.3), 2014.

4.1.2. Red Pasiva

En una red GPON, la señal óptica se divide mediante splitters ópticos pasivos para llegar a múltiples clientes, lo que significa que no se requiere ningún dispositivo activo en la red para gestionar la división de la señal.

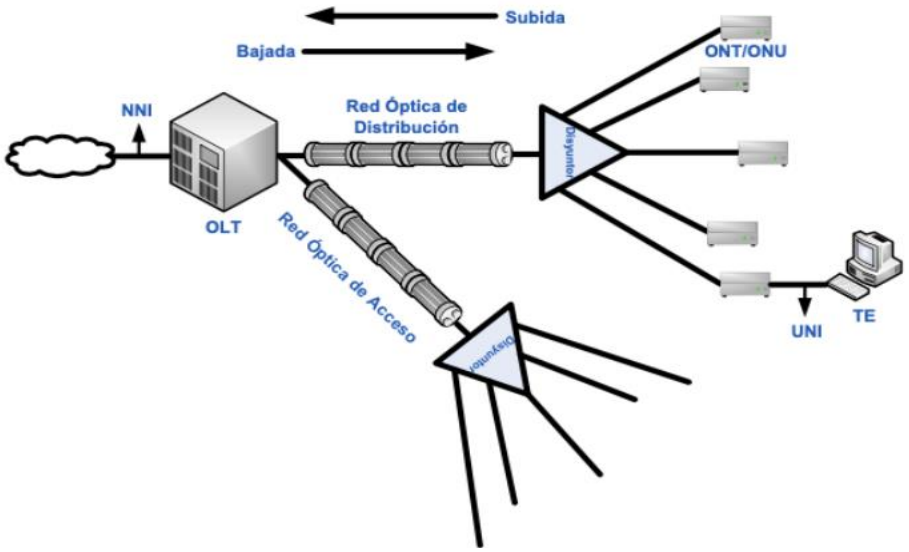
En una red GPON, la información se transmite mediante pulsos de luz a través de la fibra óptica, lo que proporciona una alta velocidad de transmisión de datos y un ancho de banda superior al de las redes tradicionales de cobre. La tecnología GPON también permite la transmisión de voz y vídeo de alta calidad, lo que la hace ideal para proveedores de servicios que ofrecen paquetes de triple play (datos, voz y video). Revista espacios N40, 2019

En una red GPON, el equipamiento principal se encuentra en la central de la red, donde se ubica la Optical Line Terminal (OLT), que se encarga de gestionar y controlar el tráfico de la red. Los clientes se conectan a la red mediante unidades de red óptica (ONU) situadas en su hogar o lugar de trabajo. Revista espacios N40, 2019

La Red Óptica Pasiva con Capacidad de Gigabit (GPON) es una tecnología de red eficiente, escalable y segura que se utiliza en todo el mundo para proporcionar servicios de telecomunicaciones a los clientes.

Figura 3

Elementos de una red pasiva



Fuente: Tomado de Red óptica pasiva para proveer de Internet a la ciudad de Riobamba – Ecuador (p.12), Revista espacios N40, 2019

4.1.3. Ventajas y desventajas de la red GPON

Ventajas:

- Permite conexiones de hasta 20 km entre el OLT y el ONT.
- Anchos de banda más grandes que permiten alcanzar los 2,4 Gbps de bajada y 1,2 Gbps de subida.
- No requiere equipos intermedios activos entre el OLT y el ONT.
- Reducción de costos para las operadoras, ya que permite el envío de muchos servicios a la vez por una misma conexión de fibra gracias a la multiplexación se puede enviar de forma simultánea: voz, datos y video.

Desventajas:

- Los instaladores deben tener cuidado con los empalmes mecánicos para no sufrir pérdidas y atenuaciones.
- Los conectores sucios o dañados, pueden generar problemas.
- No se puede instalar cualquier hardware, en las conexiones de fibra ONT debe estar registrado en la OLT. Goh T., Lee K. L., (2014),

4.2. Proveedor de Servicios de Internet (ISP)

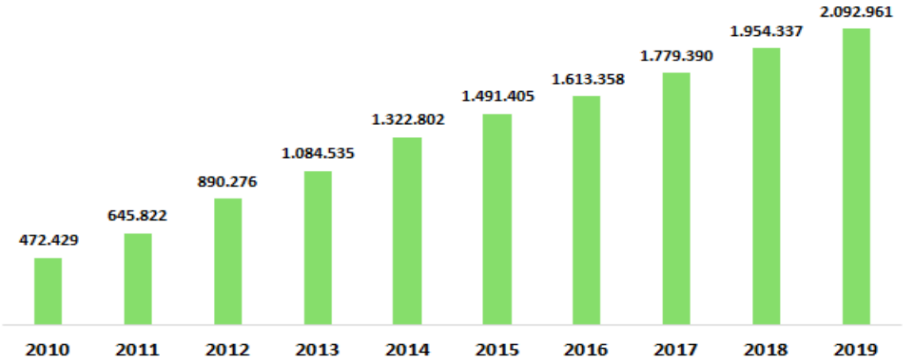
Un Proveedor de Servicios de Internet (ISP, por sus siglas en inglés) es una empresa que brinda acceso a Internet a los usuarios finales. Los ISP pueden ofrecer diferentes tipos de conexiones a Internet, como líneas de banda ancha, fibra óptica, radio enlace o diferentes medios de comunicación, en el Ecuador el ente regulador ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones) los ha denominado Servicio de acceso a internet (SAI).

4.2.1. Estadísticas.

El Estado y la población en general muestran un gran interés en el Servicio de Acceso a Internet (SAI), ya que su disponibilidad puede mejorar la provisión de servicios básicos como educación, salud, gobierno y comercio. En el cuarto trimestre de 2019, el 12,12% de la población ecuatoriana tenía una cuenta de internet fijo. En Ecuador, la definición de banda ancha se basa en los criterios establecidos por la Unión Internacional de Telecomunicaciones (UIT), que considera como banda ancha las velocidades iguales o superiores a 256 kbps, así como en la regulación nacional, que establece como banda ancha velocidades iguales o superiores a 1024 kbps. ARCOTEL (2020)

Figura 4

Histórico anual de cuentas de internet fijo



Nota. Representa el número de abonados en relación con el año. Tomado de estadísticas ARCOTEL (p.6), 2020

En Ecuador, el uso de conexiones de internet fijo a través de fibra óptica ha experimentado un aumento notable. En efecto, para finales del año 2019, este tipo de conexión representó el mayor porcentaje, con un 37,03%, seguido por las conexiones por cobre con un 33,65%, las conexiones por cable coaxial con un 21,89% y finalmente, las conexiones inalámbricas con un escaso del 7,43%. ARCOTEL (2020)

Figura 5

Conexiones de internet fijo por tecnología

Fuente: Tomado de Estadísticas ARCOTEL (p.6), 2020

4.2.2. Servicios ISP

Los proveedores de servicios de Internet (ISP) ofrecen una amplia gama de opciones que van más allá de la conectividad a la red. Además de planes de conexión a Internet que varían en velocidad y tecnologías, tales como ADSL (Asimetric Digital Subscriber Line), coaxial, fibra óptica e inalámbrica, también pueden brindar soluciones empresariales de redes y seguridad en línea para salvaguardar la privacidad y proteger los datos de los usuarios. Entre estos servicios adicionales, se encuentran las VPN (Virtual Private Network), que son una alternativa para las empresas.

4.2.3. Regulación y control en el Ecuador.

En Ecuador, el organismo encargado de regular y controlar las telecomunicaciones es la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). Esta entidad es responsable de supervisar y regular el uso del espectro radioeléctrico, garantizar la competencia leal en el mercado de las telecomunicaciones y promover el acceso a los servicios de telecomunicaciones en todo el país.

La ARCOTEL tiene el poder de otorgar y revocar licencias para la prestación de servicios de telecomunicaciones, así como de establecer tarifas para el uso de frecuencias de radio y otras formas de espectro. También tiene la tarea de garantizar que los proveedores de servicios de telecomunicaciones cumplan con las normas de calidad y seguridad establecidas por el gobierno.

4.3. Vulnerabilidades y Amenazas

En general, las vulnerabilidades son debilidades en el diseño de procedimientos o recursos y no se crean intencionalmente. Una vulnerabilidad puede ser cualquier falla en el diseño que permita que una amenaza afecte un recurso. Si hablamos de recursos informáticos, una vulnerabilidad se refiere a un error de diseño en un sistema, un sistema no actualizado o mal

configurado que permite que un agente externo acceda a un recurso o información que dicho sistema gestiona sin los permisos apropiados. Dependiendo del tipo de recurso en cuestión, existen diversas fuentes de información donde se pueden buscar vulnerabilidades aplicables a los sistemas disponibles.

Existen amenazas que son difíciles de controlar, como los desastres naturales o los errores humanos, pero es importante considerarlos al calcular los riesgos. Por ejemplo, una persona podría eliminar información accidentalmente de un servidor o enviar información confidencial a la persona equivocada por correo electrónico. Además, el hardware utilizado en los recursos informáticos de una empresa podría sufrir daños debido al uso, inundaciones, fallas eléctricas y otros factores similares. Por otro lado, existen amenazas voluntarias que se derivan de ataques deliberados, ya sea por parte de agentes internos o externos de una organización. Los agentes internos pueden incluir empleados descontentos o ex empleados cuyas credenciales de acceso no han sido revocadas. Los agentes externos pueden incluir competidores desleales, activistas, terroristas, cibercriminales y otros. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

4.3.1. Ataques en una red GPON

La superficie de ataque de una infraestructura IT está compuesta por diversos elementos que podrían presentar vulnerabilidades susceptibles de ser explotadas ya sea por un incidente natural o un ataque intencional. Entre estos elementos se incluyen dispositivos de red como routers, switches y firewalls, así como computadoras, servidores, sistemas de almacenamiento en red, sistemas operativos, aplicaciones y firmware. Incluso las personas que usan y administran estos equipos también son parte de la superficie de ataque debido a sus propias vulnerabilidades.

Los ataques pasivos consisten en la monitorización no invasiva del sujeto atacado, lo que permite obtener información almacenada o transmitida por la infraestructura, incluyendo información pública. Para ello se utilizan técnicas de monitorización de tráfico, como la búsqueda de documentos, contraseñas o información de fuentes abiertas conocidas como OSINT (Open Source INTelligence). El objetivo principal de los ataques pasivos es obtener información que

puede ser suficiente en sí misma o utilizarse para futuros ataques activos. Identificar un ataque pasivo puede alertar al usuario sobre posibles ataques activos. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

Por otro lado, los ataques activos son acciones directas que buscan penetrar la infraestructura, incluso de manera permanente, con el objetivo de sabotearla, robar información o desplegar malware para el espionaje o secuestro de equipos para otras actividades de ataque contra terceros. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

4.3.2. Amenazas de una red GPON

Las amenazas pueden afectar la seguridad y el rendimiento de una red GPON son situaciones en las que individuos con malas intenciones intentan acceder a los dispositivos, computadoras o servidores de la red para provocar daños. Estos ataques pueden tener diferentes formas, como se describen a continuación.

Tabla 1
Tipos de amenazas

TIPOS	AMENAZAS
Acceso no autorizado:	Los hackers pueden intentar acceder a la red para robar información, interrumpir el servicio o causar daños.
Ataques de denegación de servicio (DoS)	Pueden inundar la red con tráfico malintencionado, lo que puede hacer que la red sea inaccesible para los usuarios legítimos.
Intercepción de tráfico	Los hackers pueden intentar interceptar el tráfico de la red GPON para espiar las comunicaciones y robar información confidencial.
Inyección de paquetes	Los atacantes pueden intentar inyectar paquetes maliciosos en la red GPON para interrumpir el servicio o dañar los dispositivos conectados a la red.
Phishing	Es una técnica común utilizada por los hackers para engañar a los usuarios y hacer que revelen información confidencial, como contraseñas o detalles de la tarjeta de crédito.
Fallos en la red	Como cualquier red, una red GPON puede experimentar fallos debido a problemas técnicos, errores humanos o desastres naturales.

Fuente: Investigador.

Para mitigar estas amenazas, es importante implementar medidas de seguridad adecuadas, como autenticación y cifrado de datos, mantener los sistemas de software actualizados y parcheados para prevenir vulnerabilidades conocidas.

4.3.3. Vulnerabilidades en una red GPON

Una vulnerabilidad de una manera muy general es un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema, existen vulnerabilidades físicas y lógicas, donde existen algunos tipos de vulnerabilidades que son mecanismos aprovechados por los atacantes para infectar una red o robar información, en la siguiente tabla se mencionan algunos.

Tabla 2
Tipos de vulnerabilidades

TIPOS	VULNERABILIDAD
Configuración	Error de configuración como cuentas de usuario no seguras, contraseñas fáciles de descifrar
Protocolo	Al tener protocolos débiles como el HTTP, ICMP. FTP o SMTP
Cuentas	Utilizar cuentas por defecto o de fabrica
Políticas	Falta de políticas como el control de acceso

Fuente: Investigador.

4.4. Seguridad Informática

Cuando se habla de seguridad informática, es fundamental comprender los fundamentos en los que se basa esta disciplina. Uno de estos fundamentos es el concepto de seguridad, que implica un estado de bienestar en el que no existen riesgos debido a la confianza en una persona o cosa. En el contexto de la seguridad informática, este concepto se refiere a una ciencia interdisciplinaria que se enfoca en evaluar y gestionar los riesgos que pueden afectar a una persona, animal, ambiente o propiedad. En resumen, entender los pilares de la seguridad informática es esencial para comprender los aspectos más complejos de esta disciplina. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

La seguridad informática tiene como objetivo principal la reducción de los posibles riesgos que pueden provenir de múltiples fuentes, como la entrada de datos, el medio de transporte de la información, el hardware utilizado para la transmisión y recepción, los usuarios e incluso los protocolos implementados. El propósito final es lograr una mayor seguridad a través de la minimización de estos riesgos.

Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

4.4.1. Mecanismos preventivos

La seguridad informática es esencial para proteger la información de amenazas externas o internas, donde la prevención implica la identificación temprana de los riesgos y la adopción de medidas para evitar que ocurran problemas y riesgos.

Los antivirus y antimalware son programas que ayudan a prevenir y detectar la presencia de virus, malware y otras amenazas en los sistemas informáticos, así mismo es importante mantener actualizado el software, ya que las actualizaciones suelen incluir parches de seguridad que previenen vulnerabilidades, el uso de contraseñas seguras es esencial para prevenir accesos no autorizados a los sistemas, el control de acceso permite limitar el acceso a la información y sistemas de computación a usuarios autorizados, se pueden implementar diferentes mecanismos de control de acceso, como autenticación de usuarios y permisos de acceso. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

La instalación de un firewall, ya sea mediante software o hardware, tiene como objetivo filtrar el tráfico de red y evitar que conexiones no autorizadas accedan al sistema informático. Esta medida de seguridad previene el acceso no autorizado al sistema, es esencial implementar copias de seguridad para prevenir la pérdida de información en caso de fallas o ataques informáticos. Es importante que los usuarios estén informados sobre las amenazas informáticas y las medidas preventivas que pueden tomar, esta educación y conciencia sobre la seguridad informática es

fundamental para prevenir problemas y riesgos. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

4.4.2. Mecanismos correctivos

Los mecanismos correctivos de seguridad informática se refieren a las medidas que se implementan después de que se ha detectado una brecha de seguridad o un incidente en un sistema informático, con el fin de solucionar el problema y minimizar el impacto del mismo.

Un conjunto de medidas correctivas en seguridad informática incluye la implementación de un proceso de gestión de incidentes que se enfoca en detectar, investigar y responder a eventos de seguridad, con la finalidad de identificar la raíz del problema y aplicar medidas para reducir el impacto. También es importante actualizar regularmente el software o hardware con los parches de seguridad disponibles para solucionar vulnerabilidades conocidas y prevenir que los atacantes aprovechen dichas debilidades. En caso de que una contraseña haya sido comprometida, es fundamental restablecerla sin demora para impedir que el atacante continúe teniendo acceso. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

4.4.3. Mecanismos detectivos

Los mecanismos detectivos en seguridad informática consisten en las estrategias utilizadas para identificar posibles vulnerabilidades o ataques en un sistema de computación. Se basan en la premisa de que un atacante puede tener la capacidad de comprometer la seguridad y lograr un acceso total o parcial al sistema.

Dentro de los mecanismos, se contempla la inclusión de sistemas de monitoreo de seguridad que se encargan de vigilar de forma constante el tráfico de red, registros de eventos y otros indicadores de actividad con el fin de identificar patrones sospechosos. Si se detecta alguna actividad anormal, se emite una alerta para que los administradores de seguridad puedan investigar a profundidad, mediante el análisis enfocado del tráfico de red y la revisión exhaustiva de los

paquetes de datos transmitidos para detectar patrones de tráfico malicioso o intentos de acceso no autorizados. Es posible identificar la presencia de malware en la red mediante esta técnica.

Además, se llevan a cabo simulaciones controladas de ataques informáticos para intentar penetrar en el sistema y detectar posibles vulnerabilidades. También se realizan auditorías de seguridad de forma sistemática y exhaustiva, tanto interna como externamente, para identificar debilidades y sugerir recomendaciones que permitan mejorar la seguridad en general. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

4.4.4. Seguridad de una red GPON

Una red GPON (Red Óptica Pasiva con Capacidad de Gigabit) brindar servicios de banda ancha de alta velocidad a los usuarios finales, la cual se denomina pasiva, lo que significa que no se requiere energía en la red de distribución. Sin embargo, aunque la red GPON es generalmente segura, aún existen algunos riesgos de seguridad que deben tenerse en cuenta. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

La protección física es esencial para garantizar la seguridad de la red GPON. Es importante que los componentes de la red, como los terminales de usuario, los equipos activos y las fibras ópticas, estén protegidos de daños físicos y de acceso no autorizado, junto con la autenticación de usuarios se crea un mecanismo de seguridad importante que se utiliza para garantizar que solo los usuarios autorizados puedan acceder a la red GPON. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

El monitoreo de la red es una práctica importante para garantizar que la red GPON esté funcionando correctamente y que no se estén produciendo ataques o intentos de intrusión. Es importante utilizar herramientas de monitoreo de red para detectar y responder a cualquier actividad sospechosa, es primordial mantener el software de la red GPON actualizado para protegerla de las vulnerabilidades conocidas, las actualizaciones de software pueden incluir parches de seguridad y mejoras en el rendimiento. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

4.4.5. Seguridad de un ISP

Es crucial que los ISP garanticen la seguridad de la información personal y confidencial de sus clientes, ya que tienen acceso a una gran cantidad de datos sensibles. Para lograr esto, es esencial que se implementen medidas de seguridad adecuadas para proteger la red de posibles amenazas, como ataques de hackers, malware y virus. El ISP (Internet Service Provider) debe implementar soluciones de firewall, antivirus y antimalware en sus sistemas para prevenir ataques externos y garantizar que la información personal y confidencial de sus clientes, como sus direcciones de correo electrónico, contraseñas y detalles de pago, estén protegidos. Una forma de lograr esto es mediante el cifrado de datos y la implementación de políticas estrictas de privacidad. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

Es importante que los ISP monitoreen la actividad de sus usuarios para identificar cualquier actividad sospechosa, como botnets, phishing y otros intentos de fraude en línea. Además, los ISP deben enfocarse en capacitar y concientizar a sus empleados sobre la importancia de la seguridad informática, así como sobre los riesgos asociados con la manipulación de datos confidenciales. (Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo, Castillo, 2018)

5. Metodología

5.1. Recolección de la información

En esta sección detallamos la información de la empresa TEKLINK CIA. LTDA., donde se analiza la infraestructura de la red GPON (Red Óptica Pasiva con Capacidad de Gigabit), las vulnerabilidades y amenazas identificando los puntos críticos.

5.1.1. Empresa TEKLINK CIA. LTDA.

Es una empresa proveedora de servicios de internet, misma que se encuentra autorizada para prestar Servicios de Valor Agregado de Acceso a Internet de acuerdo a la Resolución N° ARCOTEL-2017-1129 otorgado el 23 de noviembre de 2017 e inscrito el 06 de diciembre de 2017 en el tomo 128, foja 12826, del Registro Público de Telecomunicaciones en la misma fecha.

Su misión es ofrecer servicios en telecomunicaciones, satisfaciendo las necesidades y expectativas de los clientes y la sociedad, mediante el suministro oportuno de servicios y soluciones de telecomunicaciones y su visión es ser la empresa que brinde soluciones en Telecomunicaciones, a través de tecnología que cumpla estándares de calidad, con un equipo humano altamente capacitado.

5.1.1.1. Ubicación

La empresa TEKLINK CIA. LTDA., se encuentra brindado sus servicios en los cantones de Loja y Catamayo, sus oficinas se encuentran en las calles Bernardo Valdivieso entre Imbabura y Quito en la ciudad de Loja y en la ciudad de Catamayo están ubicado en las calles Simón Bolívar entre Av. Catamayo y Primero de Mayo, y en la actualidad cuenta con una red GPON desplegada en el sector urbano del cantón Catamayo.

5.1.1.2. Servicios

El principal servicio prestado por la empresa TEKLINK CIA. LTDA, es el acceso a internet a través de planes corporativos y residenciales, al tener implementada una red GPON sus planes residenciales son los siguientes:

Figura 6

Planes empresa TEKLINK CIA. LTDA.

Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

5.1.1.3. Topología

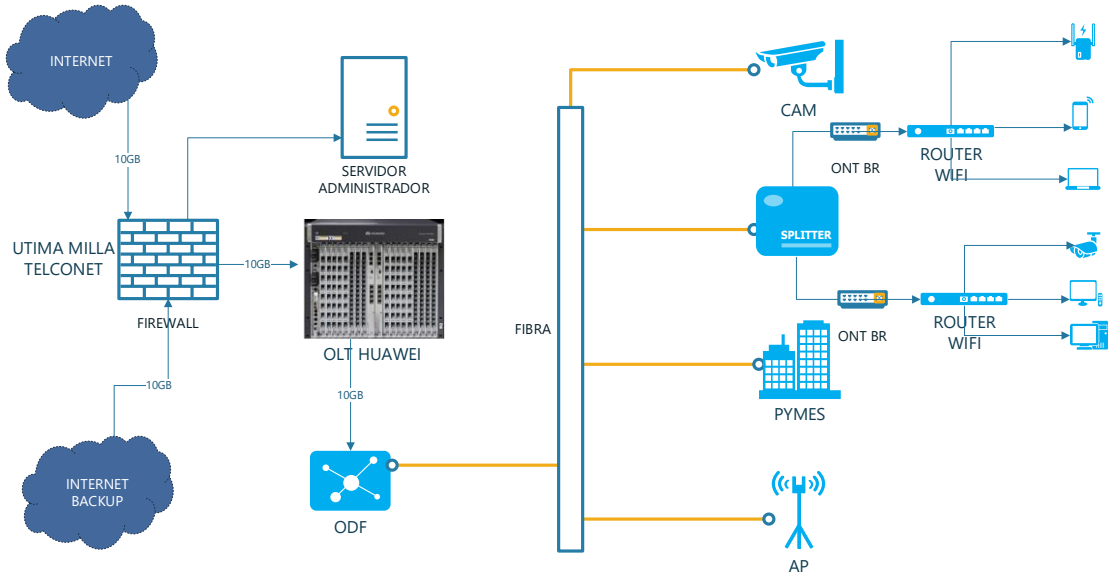
La topología de la red GPON (Red Óptica Pasiva con Capacidad de Gigabit) nos muestra la forma en que se interconectan los diferentes elementos que conforman la red, en el caso de la empresa TEKLINK CIA. LTDA., la topología es en forma de árbol, donde un único equipo central llamado OLT (Optical Line Terminal) se conecta con múltiples equipos remotos llamados ONT (Optical Network Termination) a través de una fibra óptica.

En esta topología, la señal se transmite en una dirección, desde el OLT hasta los diferentes ONT y no se produce comunicación directa entre los ONT. Esta topología en árbol reduce la complejidad de la red y mejora su rendimiento, ya que se minimizan las colisiones de tráfico y se

maximiza la eficiencia en el uso del ancho de banda de la fibra óptica, en la gráfica 7 se detalla los elementos implementados.

Figura 7

Topología red GPON TEKLINK



Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

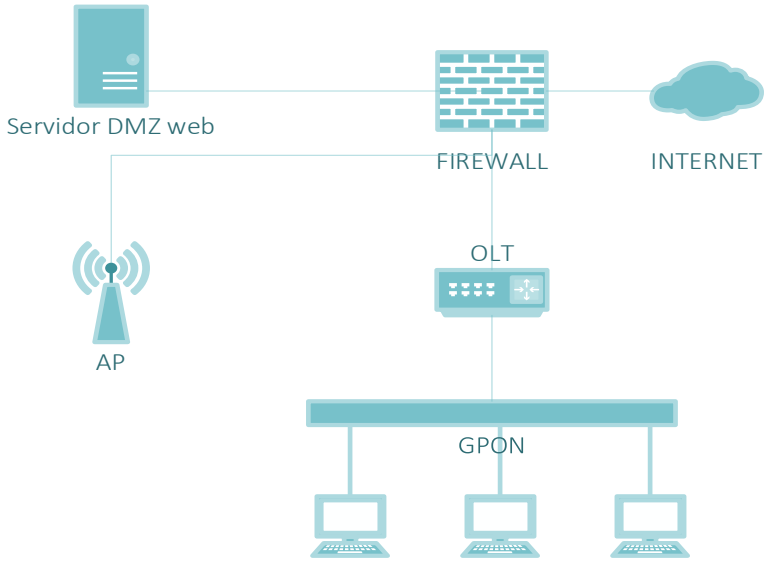
5.1.1.4. Firewall

El firewall de la red GPON, es un dispositivo de seguridad que se utiliza para proteger la red contra posibles amenazas externas, como virus informáticos, malware, ataques de hackers, entre otros, este actúa como una barrera de protección entre la red interna y el mundo exterior, permitiendo solo el tráfico de red autorizado y bloqueando cualquier tráfico no autorizado.

Además, realiza funciones de filtrado de paquetes, inspección de paquetes y control de acceso, lo que ayuda a garantizar la seguridad y privacidad de los datos que se transmiten a través de la red, a continuación, se muestra el diseño del firewall de la red GPON TEKLINK.

Figura 8

Firewall red TEKLINK



Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

La empresa cuenta con un firewall que le permite administrar la red GPON, y en el mismo realiza la protección de la red, segmentación de ancho de banda, filtro de paquetes, restricción de puertos, restricción de sitios web, restricción de aplicaciones, calidad de servicio QoS y la virtualización de la red, para ello cuenta con un equipo MIKROTIK el cual tiene las siguientes características.

Tabla 3

Características firewall

Característica	Descripción
Licencia level 6	Permite configuración ilimitada en los diferentes túneles, el acceso ilimitado de administradores, no tiene restricciones
Arquitectura TILE	Garantiza un rendimiento óptimo de alta disponibilidad y ayuda en la seguridad de la red
Puertos SFP 10GB	Permite conexiones de alta velocidad
CPU 1GHZ	Ayuda en el rendimiento
Memoria RAM 16GB	Facilita una mayor cantidad de procesos, mejorando el rendimiento
Consumo máximo de energía 125W	Se considera para optimizar el banco de baterías
Monitoreo de Voltaje y Temperatura	Ayuda a optimizar los recursos controlando los valores, ajustando con los requerimientos mínimos y máximos

Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

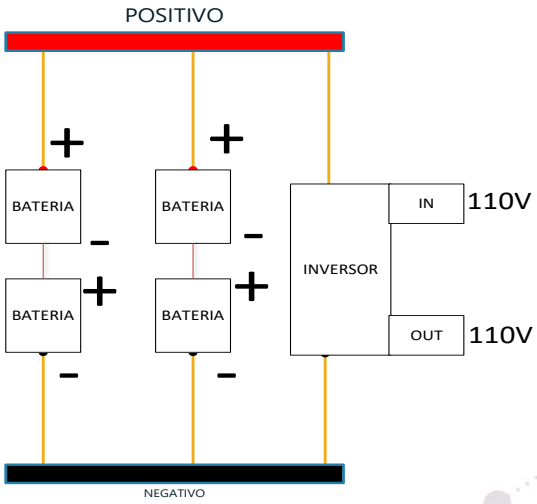
5.1.1.5. Respaldo de Energía

El banco de baterías es un sistema que se utiliza para proporcionar energía de respaldo, en caso de que falle el suministro de energía eléctrica principal, este respaldo esta implementado en la cabecera de la red GPON, en la que se encuentra la OLT (Optical Line Terminal), ODN (Red de Distribución Óptica), convertidores ópticos, firewall, servidores, última milla.

La capacidad es de 2KVA, incluyendo un sistema de monitoreo y alerta para notificar a los operadores de la red cuando la carga de las baterías es baja o cuando se requiere mantenimiento. El banco de baterías es esencial para garantizar la continuidad del servicio y proteger los dispositivos de la red contra daños eléctricos, en la gráfica 9 detallamos el diagrama de la misma.

Figura 9

Diagrama banco de baterías



Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

La empresa ha implementado este banco de baterías con el objetivo de proporcionar energía en caso de una interrupción del fluido eléctrico, el cual tiene las siguientes características.

Tabla 4
Características banco de baterías

Característica	Descripción
Inversor Xmart 2KVA	Permite optimizar la energía de las baterías, cargándolas cuando su voltaje es mínimo y asegurando una salida constante de 120V, permite recuperación en frío y adaptación en caliente, pantalla LED de monitoreo.
INPUT / OUTPUT 120V 50/60 Hz	Los equipos implementados en la cabecera trabajan a 120V lo que ayuda optimizando el rendimiento.
Baterías de GEL sellada 120AH	Libres de mantenimientos y de larga durabilidad
Regulación de voltaje incorporado	Ayuda a elevar o reducir el voltaje de entrada para llevarlo a niveles adecuados

Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

5.2. Análisis de la red GPON de la empresa TEKLINK CIA. LTDA.

5.2.1. Políticas de seguridad.

La empresa ha decidido implementar políticas de seguridad en dos ejes, en la parte administrativa y en la infraestructura, estas decisiones están encaminadas a optimizar los recursos, es importante tener en cuenta que estas políticas están adaptadas a las necesidades de la empresa.

El objetivo de estas políticas es proteger los activos de la empresa, mejorando la seguridad de la red, para ello se ha implementado normas y directrices específicas apuntado a puntos críticos.

5.2.1.1. Red GPON

Con el fin garantizar la privacidad, la integridad y la disponibilidad de los datos que se transmiten a través de la red GPON, la empresa ha implementado políticas específicas para cada activo las cuales se detallan en los siguientes párrafos.

La actualización del software de los equipos se realiza periódicamente, antes de un cambio se realiza pruebas del firmware a utilizar, con el fin de detectar errores o incompatibilidad con la configuración implementada.

Las contraseñas en general son generadas y autorizadas por el administrador de red, las mismas cuentan con la combinación de letras mayúsculas, minúsculas, números y por lo menos un carácter especial.

El firewall implementado contiene reglas de seguridad optimizando la protección contra ataques pasivos y activos en la red.

El acceso al equipo OLT (Optical Line Terminal), está restringido por el horario de trabajo del técnico, es decir no podrá ingresar en horarios no laborables.

En los equipos terminales (Router inalámbrico) se utiliza una plantilla con seguridades prestablecidas por el administrador la cual incluye la contraseña, administración remota, nombre de la red SSID (Service Set Identifier), clave red WIFI (Wireless Fidelity) y la seguridad, estos parámetros no serán borrados así se fuerce el reseteado del equipo.

5.2.1.2. Administrativas

A continuación, se detallan las políticas implementadas por la empresa TEKLINK CIA. LTDA.

El ingreso al Data Center y nodos de la empresa está restringido, para el personal técnico con la autorización de su inmediato superior y para personal externo se debe llenar una solicitud donde se asigna al responsable de la visita junto con el horario y fecha permitida, tanto al ingreso como salida se debe reportar al administrador de la red.

El personal técnico para administrar la red incluyendo el monitoreo, para acceder a la red, debe hacerlo con dirección IPS autorizadas por el administrador de red, en caso de hacer el ingreso remotamente utilizará la VPN (Virtual Private Network) autorizada para cada técnico.

Se lleva un reporte por día, semana, mes y año del tráfico de la red incluyendo un respaldo de toda la red y sus archivos LOG, esta información se almacena en la nube con restricción de acceso.

Se realiza una capacitación constante al personal administrativo en cuanto a la educación en seguridad y administración de la red.

5.2.2. Amenazas de la red GPON.

GPON (Red Óptica Pasiva con Capacidad de Gigabit) es una tecnología segura y eficiente, pero hay algunas amenazas potenciales que se deben tomar en cuenta, es por ello que la empresa TEKLINK CIA. LTDA., ha implementado medidas de seguridad adecuadas, mismas que se detallan a continuación.

Se ha implementado un respaldo de energía, a través de un banco de baterías en cada nodo de la empresa, en el nodo principal se tiene instalado un banco de baterías de 2KVA y el tiempo mínimo de respaldo es de 2 horas.

Implementar un Backup en la última milla del proveedor, con el fin de evitar pérdidas de conexión por cortes de fibra o accidentes fortuitos, este servicio es monitoreado por el proveedor y validado por la empresa TEKLINK CIA. LTDA.

Se utiliza actualizaciones periódicas en el firewall acompañadas de reglas de seguridad, con el fin de evitar ataques DoS y DDoS (Denial of Service and Destributed Denial of Service).

Cubrir los eventos fortuitos de la red GPON, durante las 24 horas del día, los 365 días del año, utilizando una cuadrilla de soporte con una respuesta máxima de 2 horas.

Los mantenimientos de nodos y la red GPON, se realizan en horarios de 4AM a 6AM, minimizando las intermitencias de los servicios, serán planificados con un mínimo de 2 días y se comunicará a los abonados con 24 horas de anticipación.

El monitoreo de la red incluye tráfico de red, puertos, calidad de servicio y control de ancho de banda, estos reportes están alojados en el firewall con un máximo de 3 meses.

5.3. Pruebas de vulnerabilidades y amenazas de la red GPON

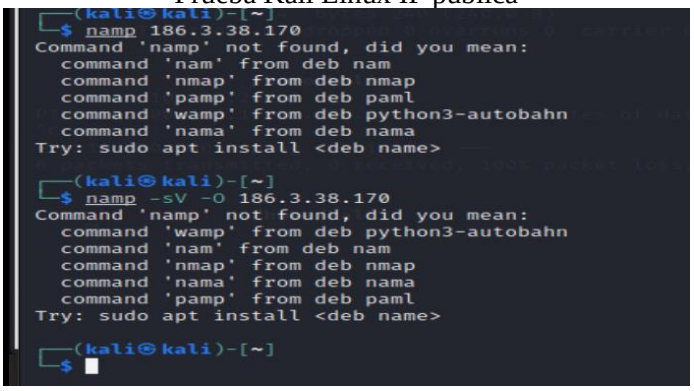
Para detectar posibles vulnerabilidades y amenazas en la red GPON, es necesario realizar pruebas que expongan los riesgos de seguridad, con el objetivo de proponer posibles soluciones, para ello se ha probado posibles escenarios con el fin de verificar la seguridad de los activos de la empresa, utilizando técnicas de simulación de ataques las cuales se detallan en los siguientes apartados.

5.3.1. Pruebas del Firewall.

Para las pruebas del firewall se ha utilizado una distribución de Linux denominada Kali Linux, las pruebas fueron aprobadas por el administrador de red y se utilizó para detectar vulnerabilidades en el firewall.

Se utilizó una máquina virtual con la distribución Debian, en la cual esta implementado Kali Linux, en primer lugar, se utilizó la herramienta nmap, para verificar los puertos abiertos disponibles, se inició desde fuera de la red a través de la dirección IP pública, donde no se pudo obtener información como se muestra en la figura 10.

Figura 10
Prueba Kali Linux IP publica



Fuente: Kali Linux nmap.

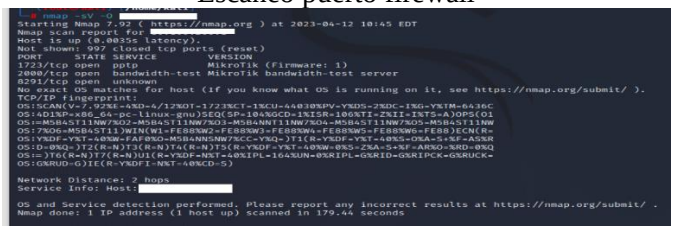
Con esta prueba se verifica que el acceso está restringido con autentificación de los puertos, como segundo paso se procede hacer un escaneo de la red para verificar posibles puntos críticos dentro de la red GPON, como se muestra a continuación:

Figura 11
Escaneo red GPON

Fuente: Kali Linux nmap.

Se observa diferentes equipos ONT con puertos disponibles de SSH, FTP, TELNET Y HTTP, los cuales son utilizados para la administración de los abonados, una vez identificado el firewall se procedió a escanear los puertos, como se muestra en la siguiente ilustración.

Figura 12
Escaneo puerto firewall



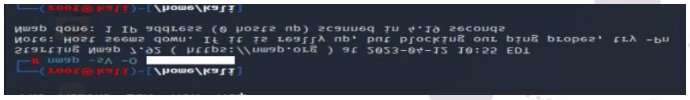
Fuente: Kali Linux nmap.

El equipo trabaja con diferentes puertos de administración que utilizan doble autentificación para su acceso, al ser un equipo MIKROTIK se verifica que tiene puertos abiertos para su administración y control de ancho de banda, los puertos SSH, FTP, TELNET, HTTP y HTTPS se encuentran deshabilitados, lo que mejora la seguridad del firewall.

5.3.2. Pruebas de OLT.

Se inicio con la herramienta Kali Linux, en busca de vulnerabilidades del equipo, se inició identificando la IP del equipo a través de un escaneo de la red como se muestra en la Figura 11, con la IP del equipo se procedió a identificar sus características, siendo este una OLT (Optical Line Terminal) de la serie MA de la marca Huawei, y se escaneo los puertos disponibles como se muestra a continuación.

Figura 13
Escaneo OLT



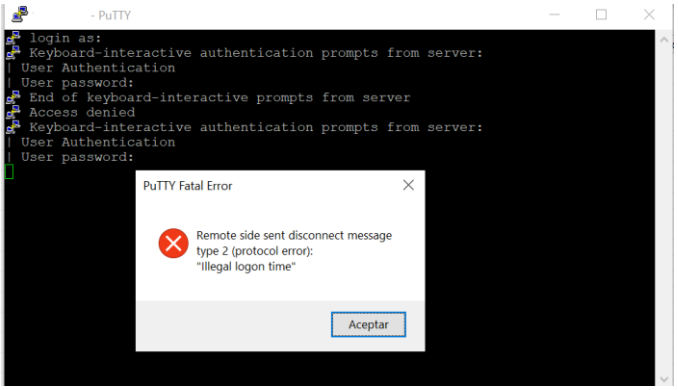
Fuente: Kali Linux nmap.

No se pudo verificar los puertos disponibles, desde la red de abonados, mostrando una eficiente seguridad, así mismos se trató de forzar el ingreso al equipo en un horario no permitido, utilizando un usuario y contraseña facilitado por un técnico de la empresa y con la autorización

del administrador de la red, al momento de ingresar se verifica que el acceso está denegado por estar fuera de tiempo establecido como se muestra en la figura 14.

Figura 14

Prueba acceso OLT fuera de horario de trabajo



Fuente: Investigador.

5.3.3. Pruebas ONT.

En los abonados se utiliza una ONT (Optical Network Termination) tipo Bridget modelo HG8310M, en marca Huawei, el mismo realiza la validación de autentificación con la OLT (Optical Line Terminal), y se implementa después de la roseta y después de la ONT se utiliza un Router WIFI como se muestra en la figura 15.

Figura 15

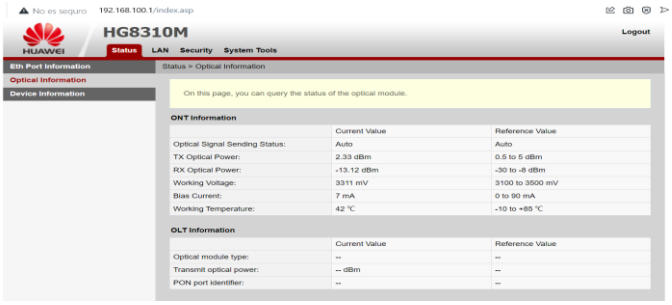
Equipos Instalados en los abonados ONT, Router WIFI y roseta de fusión FO

Fuente: Investigador.

Al tener una ONT que no asigna DHCP (Dynamic Host configuration Protocol), se dificulta ubicar la IP de acceso WEB, por lo que se opta en forzar el reseteo de fábrica al dispositivo, de esta manera se pudo ingresar al equipo el cual tenía los valores de fábrica, como se muestra en la gráfica 16.

Figura 16

ONT Bridget



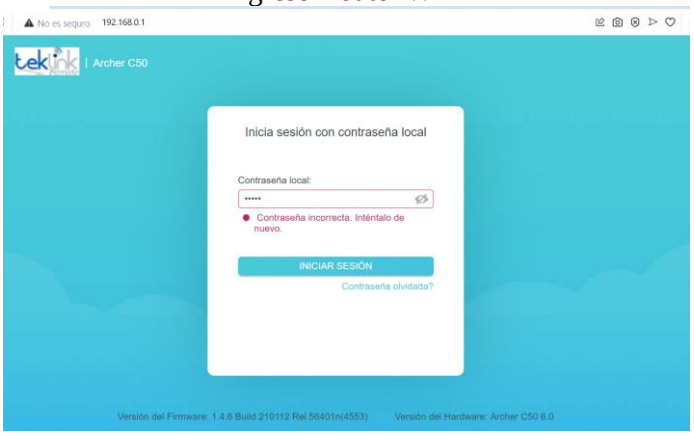
Fuente: ONT Bridget HG8310M.

Con el equipo reseteado se pudo verificar que, el equipo si se autentifica con la OLT (Optical Line Terminal), pero al no tener la IP autorizada no da ningún servicio y tampoco se puede acceder a la red GPON, con esto se probó la eficiencia en cuanto a seguridad del dispositivo.

5.3.4. Pruebas Router WIFI.

En los abonados se utiliza modelos TP-LINK con una plantilla predeterminada, para las pruebas nos dirigimos a un abonado, se conectó a través del puerto LAN un computador y se procede a vulnerar la seguridad del equipo con claves por defecto y varias combinaciones sin poder ingresar, luego se procede a forzar el reseteo el equipo, el equipo se resetea con valores establecidos por la plantilla de la empresa y en sí no se puede ingresar a la configuración del equipo mostrando siempre la siguiente pantalla (Ver figura 17).

Figura 17
Ingreso Router WIFI



Fuente: Router Tp-link C50.

Como se muestra en la gráfica 17, el equipo se resetea con datos de la empresa incluyendo el logo, con esta seguridad la empresa garantiza que solo personal técnico pueda manipular los equipos, previniendo la manipulación y posibles ataques a la red.

5.3.5. Pruebas ODN

Se inició identificando la red de distribución óptica (ODN) implementada en la infraestructura de la red GPON de la empresa TEKLINK CIA. LTDA., la misma se encuentra desplegada en la zona urbana del cantón Catamayo, en la tabla 5 se detalla los elementos implementados.

Tabla 5
Elementos ODN

Elemento	Descripción
Distribuidor de fibra óptica ODF	Está ubicado en el nodo principal con una capacidad de 48 hilos.
Fibra óptica 48 hilos	Es utilizada una fibra ADSS con un SPAM de 120 metros en marca FIBERHOME, y se utiliza como troncal principal, con un recorrido de 8 km.
Fibra óptica 12 hilos	Es utilizada una fibra ADSS con un SPAM de 80 metros en marca Nexus, y se utiliza para distribución desde las mangas a las NAPS, con un recorrido total de 20 km.
Fibra óptica 2 hilos	Es utilizada una fibra DROP con un SPAM de 80 metros en marca Nexus, y se utiliza desde las cajas NAPS hasta la roseta de abonado.
Manga tipo domo 96H	Se tiene implementado en la troncal principal, 7 mangas de fusión para 96H, se utilizan para la distribución de las cajas NAP, su certificación es IP69.

Caja distribución NAP	Estas cajas de punto de acceso esta ubicadas en los postes de energía eléctrica, la empresa cuenta con un total de 128 en toda su red, su certificación es IP65.
Splitter 1x2	Son utilizados para dividir la señal óptica de 1 entrada 2 salidas, y están ubicados en las NAPS
Splitter 1x4	Son utilizados para dividir la señal óptica de 1 entrada 4 salidas, y están ubicados en las mangas.
Splitter 1x8	Son utilizados para dividir la señal óptica de 1 entrada 8 salidas, y están ubicados en las NAPS de 8 puertos.
Splitter 1x16	Son utilizados para dividir la señal óptica de 1 entrada 16 salidas, y están ubicados en las NAPS de 16 puertos.
Roseta	Esta instalado en los abonados como punto de fusión de última milla.

Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

Una vez identificando la red de distribución óptica (ODN), se procede a realizar pruebas de vulnerabilidad, se inicia desde la cabecera como se muestra en la gráfica 18, la cual cuenta con personal en sitio.

Figura 18

Ingreso data center

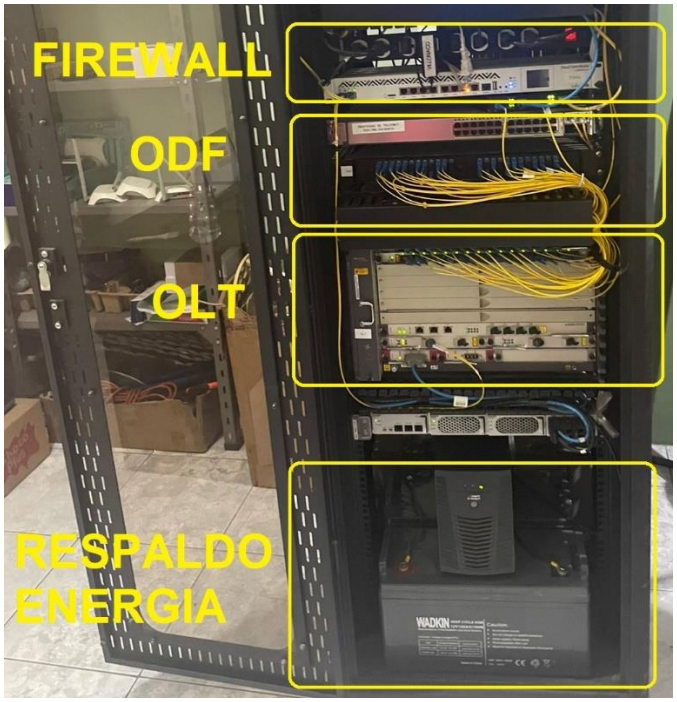
Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

Para el ingreso se debe llenar una bitácora la cual consta de datos personales del visitante, hora de inicio y fin, firma y responsable, adicional se observa que el sitio cuenta con cámaras de seguridad y el acceso está restringido por el administrador de la red y una secretaria en sitio, para

el acceso al ODF (distribuidor de fibra óptica) es necesario abrir un rack que tiene llave y no se permite la manipulación a personal externo como se muestra en la figura 19.

Figura 19

Rack cabecera ODN



Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

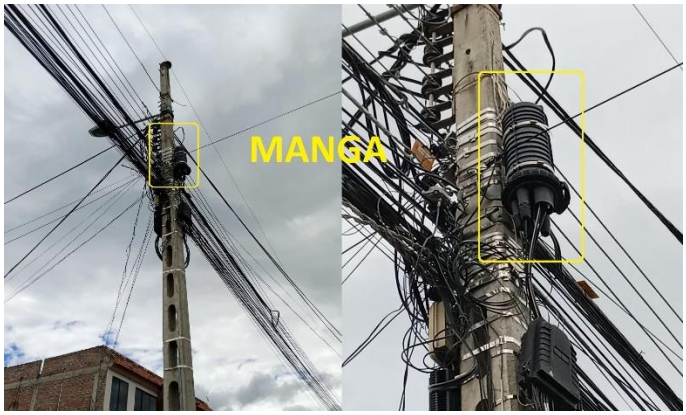
Con esta prueba se valida la política de seguridad en el data center y ODF (distribuidor de fibra óptica), cumpliendo con los objetivos de las políticas implementadas.

Para las pruebas de seguridad en la red de distribución óptica (ODN), se inició con la fibra implementada, se delimitó la FO en la troncal principal al ser de mayor incidencia, esta FO es ADSS de 48H y 12H con estándar G.652.D, donde se tiene tendido tramos de 4km y de 2km, con una pérdida de 0,22 dB/km, se verificó que es relativamente fácil crear micro curvas de la FO, por el fácil acceso a los postes de energía eléctrica. Adicional se observa que, al utilizar postes compartidos con otros proveedores, se puede generar cortes de FO o atenuaciones por mala manipulación.

Dentro de esta prueba se observó las mangas implementadas, al tener todo el despliegue aéreo se observa que las mismas se encuentran adosadas a los postes de energía como se muestra en la figura 20.

Figura 20

Manga tipo domo red ODN

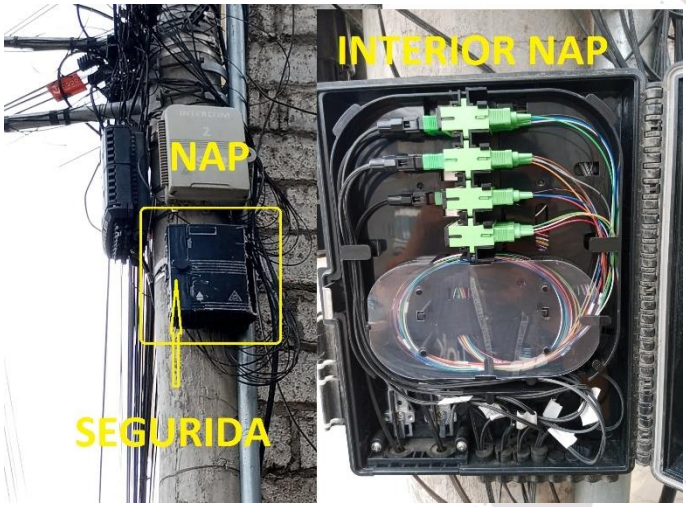


Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

Estas mangas son utilizadas para la implantación de los splitters 1x4 y 1x2, estos divisores ópticos pasivos generan una pérdida de 3dB a 6 dB, asimismo la implementación de NAPS (puntos de acceso a la red), permite distribuir la señal a los diferentes abonados, como se muestra en la figura 21.

Figura 21

NAP



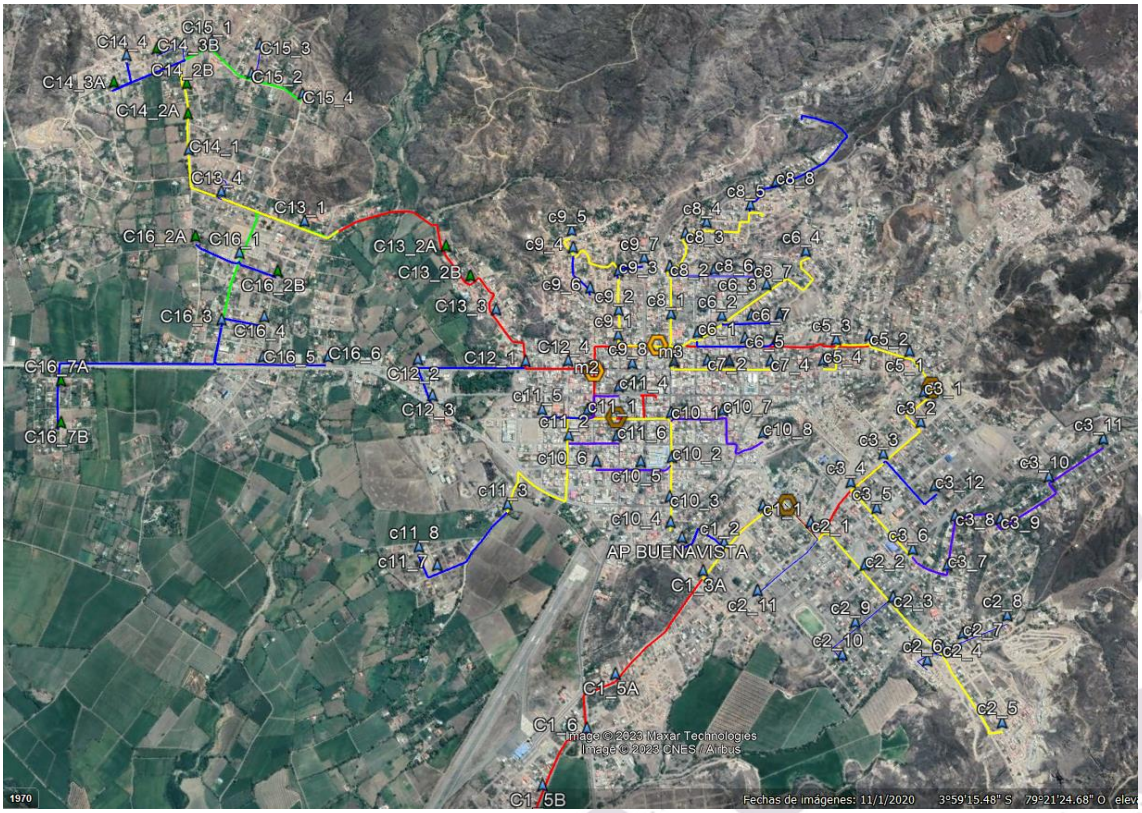
Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

Estas NAPS están instaladas en los postes de energía eléctrica, las mismas tienen splitters de 1x8 y 1x16 y tienen implementados conectores SC/APC (Subscriber Connector/ Angled Physical Contact), con el fin de ayudar al técnico a través de conectores mecánicos, cada FO(Fibra Óptica) que ingresa a la NAP (Network Access Point) se encuentra etiquetada con nomenclaturas preestablecidas por la empresa, la potencia en las mismas oscila de -14.5 a -20 dB, esta variación depende del número de empalmes, distancia y splitters utilizados, se verifica que las NAP tienen una cerradura la cual se abre con una llave individual dependiendo del modelo, se pudo validar la seguridad de las cajas forzando la seguridad sin tener un resultado positivo, lo que hace seguro el acceso a las NAPS.

Se confirma con el administrador de la red, que la implementación de la red GPON es de 2 años, es decir es casi nueva y la calidad es óptima, se verifica que la implementación está en buenas condiciones y operativa, en la figura 22 se muestra la implementación de la red GPON en la zona urbana del cantón Catamayo.

Figura 22

Distribución red GPON



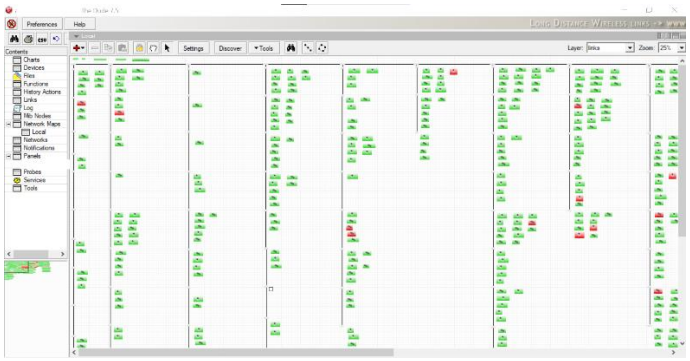
Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

5.3.6. Pruebas de monitoreo

Para el monitoreo de la red se utiliza una herramienta llamada THE DUDE, la cual trabaja a través de los protocolos que se muestran en la figura 23, esta aplicación toma los datos de funcionamiento de los equipos remotos y ofrece estadísticas gráficas y logs detallados, permitiendo al administrador de red analizar el comportamiento de toda la red GPON.

Figura 23

Sistema de monitoreo de la red GPON



Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

Con esta herramienta implementada en el firewall, los técnicos pueden tomar decisiones en relación a la conectividad de los abonados, adicional utilizan herramientas de campo como el OTDR que es un reflectómetro óptico en el dominio del tiempo que permite reparar FO de abonados y de la red troncal, así también utilizan herramientas de verificación de potencia o luz que ayudan a solucionar los incidentes de la red GPON.

5.4. Propuestas de seguridad de la red GPON

Culminada la recolección de la información y analizando cada uno de los elementos implementados en la red GPON de la empresa TEKLINK CIA. LTDA., se propone:

Implementar medidas para detectar y prevenir posibles intrusiones en la red, incluyendo la implementación de un sistema de detección y prevención de intrusiones (IDS / IPS), mejorando la monitorización constante de la red y la evaluación de posibles riesgos.

Realizar una auditoría de seguridad, esta puede ser anualmente para evaluar la efectividad de las políticas de seguridad y detectar posibles amenazas y vulnerabilidades en la red GPON.

Implementar un anillo troncal de distribución con fibra de 48 hilos como backup de la ODN (Red de Distribución Óptica) entre las mangas principales y el ODF (Optical Distribution Frame).

Capacitar a los abonados acerca de los ataques phishing para evitar los intentos de engaño a los usuarios, impidiendo que revelen información personal o confidencial, como contraseñas o información de tarjetas de crédito.

Implementar un canal virtual que envíe alertas a los usuarios, sobre posibles fallas en el servicio ocasionadas por terceros o fallas técnicas de la red GPON.

Construir espacios de capacitación periódicas, dirigidas a los técnicos y personal administrativo, con temas de seguridad informática, vulnerabilidades y amenazas, ciber amenazas, ciber ataque, hackers.

Diseñar una política preventiva de amenazas fortuitas, que establezcan soluciones rápidas y enfocadas en los servicios ofrecidos por parte de la empresa.

Implementar un sistema de monitoreo en la OLT (Optical Line Terminal), donde se reflejen todos los eventos de la red pasiva, para mejorar la respuesta a vulnerabilidades y amenazas dentro de la red GPON.

5.5. Metodología utilizada

Se utilizo una metodología de análisis de datos partiendo del punto de vista de la seguridad, utilizando como marco de referencia los estándares y protocolos de seguridad mencionados en el marco teórico, se inició detallando la infraestructura implementada en la red GPON de la empresa TEKLINK CIA. LTDA., para posteriormente analizar sus políticas de seguridad ante amenazas y vulnerabilidades asociadas a la red GPON. Dentro de la fase de pruebas se validó las políticas de seguridad, pudiendo proponer soluciones para mitigar riesgos encontrados.

6. Resultados

La identificación de cada uno de los dispositivos implementados en la red GPON (Red Óptica Pasiva con Capacidad de Gigabit) de la empresa TEKLINK CIA. LTDA., se verificó a través del estudio de la topología implementada y comprobando el funcionamiento de los mismos.

Dentro de la red de distribución (ODN), la principal vulnerabilidad analizada es el corte de fibra óptica, este se puede producir por accidentes de tránsito, manipulación de la fibra o eventos naturales, para mitigar esta amenaza se utiliza un constante mantenimiento y en conjunto con el monitoreo de la red GPON, se minimiza las incidencias, los puntos críticos detectados en la red pasiva son las mangas, cajas NAP (Network Access Point), rosetas y ODF (Optical Distribution Frame), estos puntos cuentan con seguridad que para un atacante le complicaría su objetivo.

Para detectar un ONT (Optical Network Termination) intrusa la OLT (Optical Line Terminal) genera un mensaje, que indica el número de serie y el puerto donde está conectado el equipo atacante, si en la OLT no se agrega al equipo, este no puede acceder a la red, adicional la empresa como norma de seguridad genera un IP estática por cada ONT, es decir que un atacante tiene que vulnerar una doble autentificación para ingresar a la red GPON.

El monitoreo de la red es fundamental ante los ataques, es por tal motivo que la empresa tiene implementado mensajes automáticos en el firewall, que alertan a través de correo electrónico incidencias como caídas de servicio, acceso de usuarios al sistema y control de abonados.

Se corroboró las políticas de seguridad implementadas por parte de la empresa TEKLINK CIA. LTDA., a través de pruebas de forzado y ataques a la seguridad.

Se inició con un ataque a la capa de aplicación, esta prueba se realizó escaneando el firewall, desde la red GPON y también desde el exterior a través de la dirección IP pública, donde se pudo verificar que los puertos abiertos tienen restricciones y su acceso es limitado.

En la capa de trasporte se escaneó los puertos de toda la red GPON, donde se observa que hay puertos abiertos que la empresa utiliza para la administración de abonados, monitoreo de los equipos y configuraciones específicas, estos puertos son monitoreados y validados por el personal de la empresa.

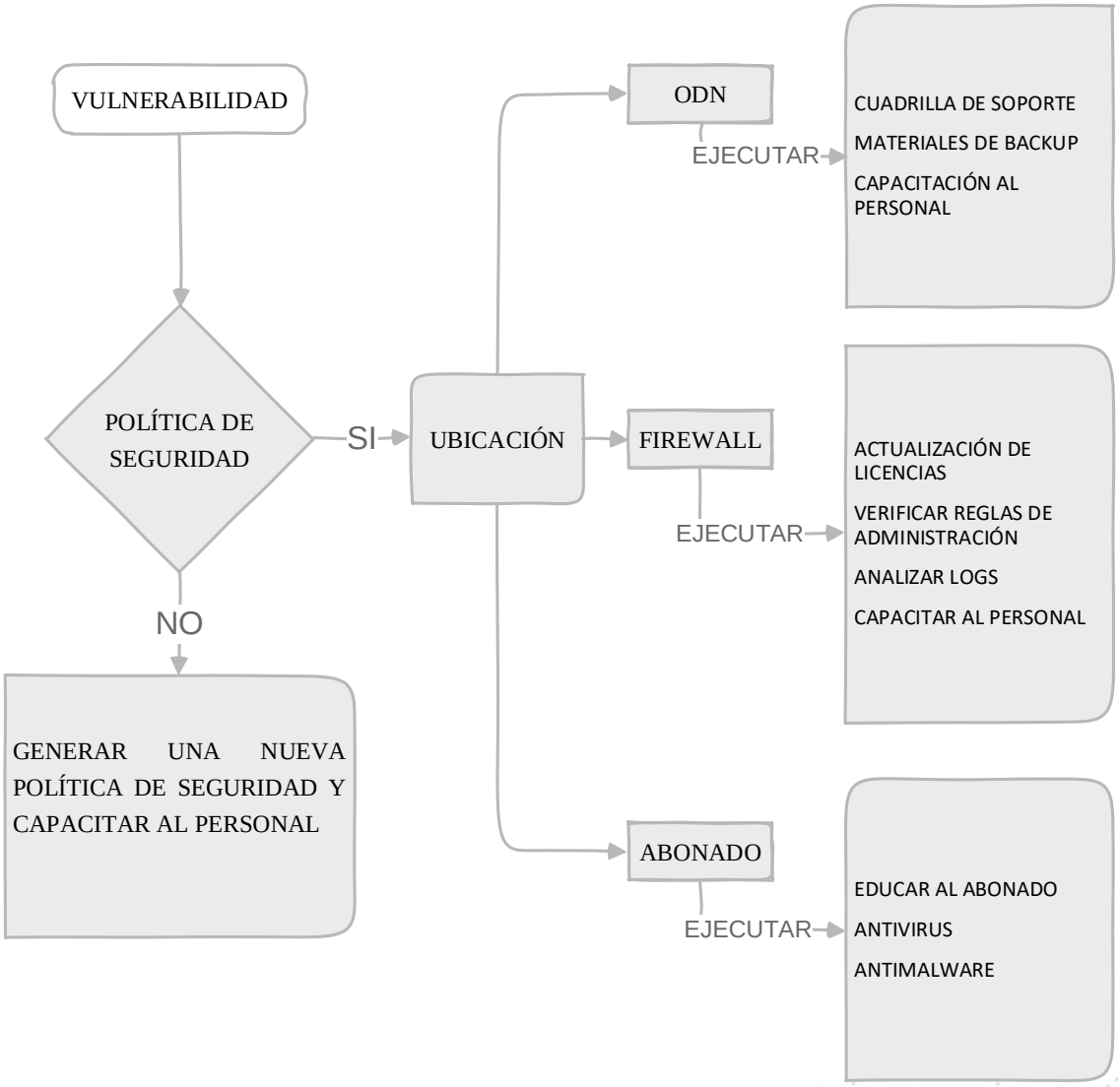
En la capa de enlace de datos se validó el uso de VLANS (Virtual Local Area Network), la empresa tiene como política de seguridad la implementación de redes virtuales para el monitoreo y administración de la red GPON, estas redes virtuales tienen restricciones y son validadas por el firewall, el uso de contraseñas seguras está a cargo del administrador de red y un constante cambio de las mismas las cuales tienen combinaciones de letras minúsculas, mayúsculas, números y caracteres especiales.

Después de analizar las vulnerabilidades y amenazas de la red GPON, se han propuesto políticas de seguridad adicionales para mejorar la seguridad y optimizar el rendimiento del ancho de banda prestado a los abonados. Estas políticas ayudarán a proteger la red contra posibles ataques y garantizarán que los usuarios tengan un servicio de alta calidad y confiable.

Para una mejor compresión en la figura 24, se explica el proceso de las vulnerabilidades identificando si tiene una política de seguridad, la ubicación de la incidencia y la acción a ejecutar.

Figura 24

Diagrama de flujo vulnerabilidades



Fuente: Tomado de la empresa TEKLINK CIA. LTDA.

7. Discusión

La seguridad de una red GPON en una tarea en la que se debe estar a la vanguardia, implementado actualizaciones que mejoren el rendimiento, con los resultados obtenidos al analizar las vulnerabilidades y amenazas de la red GPON de la empresa TEKLINK CIA. LTDA., se cumplió con los objetivos planteados.

Al analizar la infraestructura de la red GPON de la empresa TEKLINK CIA. LTDA., se pudo determinar que la implementación de la red se encuentra en la zona urbana del cantón Catamayo, cuenta con una ODN que le permite trasmitir grandes capacidades y así ofertar servicios de alta velocidad a sus abonados.

La implementación de la red GPON tiene 2 años de implementación, y se corroboró que los elementos desplegados cumplen con los estándares de seguridad y robustez.

Se realizó pruebas de vulnerabilidades y amenazas de la red GPON, las cuales incluyeron diferentes escenarios, se validó la seguridad de la red desde el área externa como interna, se utilizó diferentes técnicas que nos permitieron determinar las vulnerabilidades y amenazas.

Estas pruebas fueron focalizadas para cada elemento de la red GPON, se realizaron ataques a las capas de implementación, de trasporte y de datos, estos ataques validaron las políticas de seguridad implementadas por la empresa, en las cuales se pudo observar que están delimitadas por áreas de afectación, al tener políticas de seguridad la empresa puede brindar un servicio adecuado y de calidad a sus abonados, permitiendo fortalecer los puntos críticos.

Al culminar las pruebas se propone recomendaciones y soluciones para mejorar la seguridad de la red GPON de la empresa TEKLINK CIA. LTDA., con el objetivo de mejorar la seguridad de la información de los abonados y de la compañía.

Dentro de estas recomendaciones el pilar fundamental es la capacitación, tanto para los clientes y trabajadores de la empresa, es necesario educar y capacitar para evitar ataques maliciosos, asimismo tener políticas claras que ayuden a determinar la ubicación del problema y así ejecutar una respuesta adecuada en la zona amenazada.

8. Conclusiones

Mientras el mercado del servicio de internet siga creciendo, es necesario tener políticas de seguridad claras que ayuden a fortalecer la confiabilidad del ISP, y ante las amenazas, los clientes puedan estar más protegidos.

La red GPON implementada cumple con los estándares de seguridad y calidad, lo que permite ofrecer servicios de alta velocidad a los clientes de la empresa TEKLINK CIA. LTDA.

Se deme tomar en cuenta las políticas de seguridad antes de implementar una red GPON, esto ayudará a mejorar el desempeño y la capacidad de la red, optimizando los recursos.

Las pruebas efectuadas para determinar las vulnerabilidades y amenazas de la red GPON, comprobaron que las políticas de seguridad implementadas son eficaces, pero es necesario actualizarlas periódicamente.

El monitoreo de una red GPON, es fundamental, ayuda a determinar los puntos críticos y tomar medidas de seguridad, con un monitoreo oportuno se puede prevenir posibles ataques, el monitoreo en tiempo real ayuda a optimizar los recursos de la empresa.

La importancia de capacitar al personal sobre seguridad informática, en conjunto con los abonados, es muy necesaria puesto que los atacantes están en constante búsqueda de las vulnerabilidades de la red.

9. Recomendaciones

Implementar medidas para detectar y prevenir posibles intrusiones en la red, incluyendo la implementación de un sistema de detección y prevención de intrusiones (IDS / IPS), mejorando la monitorización constante de la red y la evaluación de posibles riesgos.

Realizar una auditoría de seguridad, esta puede ser anualmente para evaluar la efectividad de las políticas de seguridad y detectar posibles amenazas y vulnerabilidades en la red GPON.

Capacitar a los abonados acerca de los ataques phishing, para evitar los intentos de engañar a los usuarios, impidiendo que revelen información personal o confidencial, como contraseñas o información de tarjetas de crédito.

Implementar un canal virtual que envíe alertas a los usuarios, sobre posibles fallas en el servicio ocasionadas por terceros o fallas técnicas de la red GPON.

10. Referencias bibliográficas

Agencia de regulación y control de las telecomunicaciones ARCOTEL, (2020), Boletín estadístico N° 2020-01, https://www.arcotel.gob.ec/wp-content/uploads/2015/01/boletin-febrero-2020-.pdf

Goh T., Lee K. L., (2014), An overview of next generation PON technologies, IEEE Communications Surveys & Tutorials, vol. 16, no. 1

Revista Espacios (2019), Red óptica pasiva para proveer de Internet a la ciudad de Riobamba – Ecuador, N40 p12

Aguilera Purificación, (2011). Redes seguras, https://books.google.com.pe/books?id=15PTAwAAQBAJ

Romero C. Martha I., Figueroa M. Grace L., Vera N. Denisse S., Álava C. José E., Parrales A. Galo R., Álava M. Christian J., Murillo Q. Ángel L., Castillo M. Miriam A., (2018, octubre), Introducción a la seguridad informática y el análisis de vulnerabilidades.

Bancal D., Ebel F, Vicogne F., Fortunato G., Berneart J., Hennecar J., Clarhaut J., Shalkwijk L., Raul R., Cracfer R., Lasson S., (2022, diciembre), Seguridad informática, Ethical Hacking, 5ta edición.

Solomongo Ceh, (2022, febrero), Análisis de vulnerabilidades, riesgos y amenazas, hacking ético, Spanish Edition.

Celene Milanés B., Liber Galbán R., Nadia J. Olaya C., (2017), Amenazas riesgos y desastres.

11. Anexos

Anexo 1 Certificado de la empresa TEKLINK CIA. LTDA.

teklink Networks

Loja: Bernardo Valdivieso 193-32 e Imbabura
072 586671 - 0987489651
Catamayo: Bolívar y Av. Catamayo y 1ero. De Mayo
0962038560
teklinknetworks@gmail.com

Catamayo, 17 de abril de 2023

CERTIFICADO

La empresa TEKLINK NETWORKS CIA. LTDA., certifica a través de su gerente general, VIVIANA ESTEFANIA SUAREZ CAMPOVERDE, que el ing. PABLO ALEXANDER SANMARTIN VASQUEZ con CI: 1104261076, entrego propuestas para mejorar la seguridad de la red GPON implementada en la ciudad de Catamayo, relacionado al trabajo de investigación "ANÁLISIS DE VULNERABILIDADES Y AMENAZAS DE LA RED GPON DEL ISP TEKLINK CIA. LTDA.", previa a la obtención del título de Magíster en Telecomunicaciones.

1104632425 VIVIANA ESTEFANIA SUAREZ CAMPOVERDE
Firmado digitalmente por 1104632425 VIVIANA ESTEFANIA SUAREZ CAMPOVERDE
Fecha: 2023.04.17 17:41:59 -05'00'

Ing. Viviana Suárez Campoverde
GERENTE
TEKLINK NETWORKS CIA. LTDA.

Anexo 2 Certificado traducción de resumen

CERTIFICATION OF TRANSLATION ACCURACY

An instance of a certificate of translation sample follows.

I, Andres Roberto Baldassari C. declare that I am fluent in the English and Spanish languages, and that the translation of this ABSTRACT, related to SANMARTÍN VÁSQUEZ PABLO ALEXANDER, the original of which is in the Spanish language, truly reflects the content, meaning and style of the original text and constitutes in every respect a correct and true translation of the original document.

TRANSLATORS QUALIFICATIONS

Universidad Central del Ecuador - Bachelor in Arts in English Teaching.

Pontificia Universidad Católica – Master in Applied Linguistics English – Spanish

Certified Translator – Senescyt register

Universidad Central del Ecuador – Autorized translator

Andres Baldassari C. does not vouch for the authenticity of the aforementioned copy of the document or statements contained therein.

Andres Baldassari C. and his associates are not liable for any action/losses taken by the holder of this translation.

ANDRES ROBERTO BALDASSARI CAZQUETE

Andrés Baldassari MA.App.Lng
Certified Translator – Senescyt - MDT-3104-CCL-259519
Phone: (593) 098 7030 511
Email: andresbaldassari@hotmail.com

CERTIFICADO DE TRADUCCIÓN

Andrés Baldassari
MA.App.Lng

CERTIFICO:

Haber realizado la traducción de español a inglés del resumen de la tesis titulada: "ANÁLISIS DE VULNERABILIDADES Y AMENAZAS DE LA RED GPON DEL ISP TEKLINK CIA. LTDA.", de autoría PABLO ALEXANDER SANMARTÍN VÁSQUEZ con cédula de identidad Nro. 1104261076, egresado de la facultad de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, trabajo que se encuentra bajo la dirección del Ing. Andy Vega León, Mg. Sc. previo a la obtención del título de Magíster en Telecomunicaciones.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado hacer uso del presente en lo que creyere conveniente.

ANDRES ROBERTO BALDASSARI CASQUETE

Quito, 18 de abril de 2023

Andrés Baldassari MA.App.Lng
Certified Translator – Senescyt - MDT-3104-CCL-259519
Celular: (593) 098 7030 511
Email: andresbaldassari@hotmail.com