# TALLER N°9: SEGURIDAD EN REDES DE COMUNICACIONES ÓPTICAS

Manosalvas Dayanna, Zuña Bryan
Facultad de Ingeniería Eléctrica y Electrónica
Escuela Politécnica Nacional
REDES DE COMUNICACIONES ÓPTICAS

dayanna.manosalvas@epn.edu.ec bryan.zuna@epn.edu.ec

***Resumen*. - El presente documento, muestra el Informe correspondiente al Taller número 9 de la Materia de Redes de Comunicaciones Ópticas sobre: *Seguridad en Redes de Comunicaciones Ópticas.* Este trabajo muestra la investigación realizada sobre los principales problemas de seguridad que enfrentan las redes ópticas, así como los mecanismos que existen para enfrentarlos.**

***Palabras Clave.* -** *Seguridad en la red, Mecanismos de protección, Ataques y Vulnerabilidades.*

## I. OBJETIVOS

- Conocer los principales problemas e inconvenientes que presentan las redes ópticas en cuanto a seguridad.
- Investigar sobre los mecanismos que existen para combatir los problemas de seguridad en las redes ópticas.

## II. INFORME

### *A.* Describa los principales problemas, inconvenientes y amenazas de seguridad en redes ópticas. Describa los problemas de seguridad en las distintas porciones de la red.

Uno de los principales problemas que siempre están presentes en los sistemas de comunicaciones son las actividades que vulneran y operan para dañar la confidencialidad, integridad y violar la seguridad de en la red y así robar datos durante la transmisión de la misma [1].
Estas amenazas que se dedican a corromper la seguridad en la red utilizan muchas manearas de ataques, como, por ejemplo:

- ***Ingeniería social:***

Busca acceder a la información por medios sociales, haciéndose pasar por un usuario legítimo o a su vez por un administrador del sistema para obtener claves ilegalmente [1].

- ***Ataques de denegación de servicio***

Este tipo de ataques están focalizados en saturar a un ordenador o una red, así los usuarios autorizados no pueden hacer uso de este medio [1].

- ***Ataques a servidores***

Se da por las vulnerabilidades en la configuración y administración del sistema, así como en sistemas operativos [1].

- ***Adivinar contraseñas***

Se dan debido a la baja complicación en la creación de contraseñas por parte de los usuarios, pues no son consideradas como seguras y por esto son fáciles de adivinar [2].

- ***Espionaje***

Es la principal causa de captura de archivos, mensajes de correo electrónico, contraseñas y además otro tipo de información de conexión a red que es lo que permite capturar todos los mensajes de usuario.
En este punto se puede escuchar o interpretar la información, pues el uso de técnicas criptográficas es lo que permite que los datos sean leídos por otras personas conforme se distribuye en la red de comunicaciones ópticas [1].

- ***Análisis de tráfico***

Con este parámetro se puede hacer referencia a la interpretación de los datos, así como el análisis de los mismos. Pues a un atacante le permite que la comunicación se de para dos entidades en un determinado momento.

Por otro lado, se tiene otro tipo de ataques que se presentan en las redes, este se trata de que la red sufre ataques activos y estos son los que buscan alterar los recursos del sistema para afectar asi su funcionamiento.

Los ataques son los principales defectos en la red que intentan borrar, añadir o modificar los datos transmitidos. Ya que por este tipo de vulneraciones se amenaza con la integridad de los datos, la autenticidad y la confidencialidad. Podemos citar algunas categorías por las cuales se dan los principales problemas en la red [1].

- **Modificación de mensajes:** Se altera, elimina o modifica el contenido del mensaje que pasa por la red.
- **Hombre en el medio:** Se intercepta las comunicaciones entre dos entidades como lo pueden ser usuario y algún sitio web. Generalmente se puede robar información personal y realizar algún fraude.
- **Amenazas persistentes avanzadas:** Es una técnica utilizada por atacantes, consiste en permanecer un largo periodo de tiempo dentro de la red de manera oculta y no autorizada con el único objetivo de robar información y así causar daños en la red u organización.

- **Repetición:** Este se trata de atacar a una transmisión de datos válida, con lo cual se retarda en forma maliciosa y provoca que se pierda información en el lado de recepción [1].

**AMENAZAS**

Como en todo sistema de comunicaciones se van a tener amenazas, y en el caso de las redes ópticas se dan estas para dañar hardware, software y a los datos [1].

Estas amenazas se pueden dar por los siguientes fenómenos

- ***Amenazas de interrupción***

Se da cuando hay un daño, perdida o falta de funcionamiento de un punto en el sistema.

- ***Amenazas de interceptación***

Se define como el acceso a la información por parte de personas no autorizadas, pues se hace uso de privilegios no adquiridos.

- ***Amenazas de modificación***

Son accesos que cambian el entorno para su beneficio y su detección es difícil según sus circunstancias.

- ***Amenazas generación***

Es la creación de nuevos objetos dentro del sistema y la detección de los mismos es más difícil. Estos son los que causan delitos de falsificación.

- ***Amenazas de atacantes***

Esta es una gran amenaza ya que estos son intrusos que tratan de obtener permisos o accesos no autorizados a información. Estos pueden estar dentro de una red como fuera de la misma y los dos tratan de robar la información, recursos y servicios del sistema, haciendo mal uso de la misma y aprovechando las vulnerabilidades de la red [1].

Estos se pueden clasificarse de la siguiente manera:

- ✓ *Aficionados:* tienen un bajo nivel de conocimiento y no causan ataques peligrosos.
- ✓ *Profesionales:* son especialistas en informática o telecomunicaciones altamente capacitados. Causan consecuencias graves en sistemas de comunicaciones y redes.

**ATAQUES Y VULNERABILIDADES EN LAS REDES**

Según la constitución de una red y sus diferentes características de diseño, configuración y operación de los sistemas con el transcurso del tiempo se han desarrollado varias técnicas sofisticadas para el robo y explotación de las redes. Nos basamos principalmente en el modelo OSI para representar los diferentes tipos de ataques que se dan tanto a nivel físico como a nivel lógico [1].

- **Ataques a la capa aplicación**

En esta capa los ataques están focalizados a la denegación del servicio, por el gran número de peticiones al servidor lo cual causa una sobrecarga y así se llega a la alteración del servicio a los usuarios que tienen acceso legítimo.

- **Ataques a la capa transporte**

En esta capa los ataques van dirigidos al correcto funcionamiento de los protocolos TCP y UDP. Es el escaneo de puertos, inundaciones UDP, DoS por sobrecarga de conexiones.

- **Ataques a la capa de red**

Es un ataque que aprovecha las vulnerabilidades de protocolo de enrutamiento, de tal forma que se introducen paquetes de actualización de rutas, y así logran manipular los caminos que va a seguir el tráfico de acuerdo con las intenciones del atacante.

- **Ataques a la capa enlace de datos**

Se encuentran los ataques relacionados con los protocolos ARP, VLAN y STPN. Se dan ya que el atacante que está conectado a un puerto de acceso en una VLAN particular, puede obtener el acceso al tráfico en otras VLAN

- **Ataques básicos en la fibra óptica**

Estos ataques se dan fundamentalmente en la línea de transmisión, en este caso la fibra óptica, que es por donde vamos a transportar la información. El ataque se puede dar por la causa de daños físicos provocados a la fibra o a sus dispositivos que pertenecen a la red, así como una simple desconexión o por daños a causa de accidentes o incendios [1].

Estas son algunas de las características de los problemas amenazas que puede sufrir nuestro sistema de comunicaciones, y se dará una breve explicación de los mecanismos con los cuales podemos incrementar la seguridad en la red.

***B.*** **Indique los mecanismos para proveer servicios de seguridad en redes de comunicaciones ópticas. Indique aspectos o consideraciones que deben ser cubiertas para que una red de comunicaciones ópticas se considere segura y/o resilente.**

A continuación, se presentan algunos de los mecanismos de protección que se utilizan para asegurar la confidencialidad y autenticación en las redes de comunicaciones ópticas para ataques pasivos y activos.

**ATAQUES PASIVOS**

- ***Confidencialidad de datos***

  La confidencialidad de datos es un aspecto importante para la seguridad de una red, ya que asegura que la información de los usuarios no sea divulgada. El cifrado de datos es una técnica que proporciona confidencialidad al usuario. El cifrado puede darse en diferentes niveles de la red para hacer que la transmisión de información sea más confiable. A continuación, se muestran algunas técnicas de cifrado para diferentes capas de la red [3].

  - **Técnicas de cifrado para capa 1**

    El cifrado a nivel de capa 1 permite tener protección para la carga útil de la red de transporte óptico. Algunos de los beneficios que se tiene con el cifrado en capa 1 son [3]:

    - ✓ *Independencia del protocolo:* el cifrado de capa 1 permite flexibilidad para posibles cambios en la red.

- ✓ *Elimina latencia:* el cifrado de capa 1 para una velocidad de 100Gbps proporciona una latencia <150ns
- ✓ *Mayor eficiencia:* ya que no requiere bits de sobrecarga.
- ✓ *Protección integral:* el cifrado de capa 1 brinda protección a toda la red ya que encripta la carga útil y el direccionamiento.

➢ **Técnicas de cifrado para capa 0**

Las técnicas de cifrado para capa 0, también conocida como capa óptica; brindan una protección de los datos directamente en el dominio óptico. El cifrado de capa cero brinda los mismos beneficios que el cifrado en capa 1 con la ventaja de que en capa 0 se cifra toda la señal óptica.

El cifrado en capa 0 para aplicaciones donde se requiere altos niveles de seguridad sin que se comprometa la velocidad de procesamiento [3].

- ***Protección mediante esteganografía óptica***

La esteganografía óptica es una técnica que permite ocultar un canal para que este no sea detectado. De esta forma se evita que el canal llegue a usuarios no deseados. Los canales ocultos a través de esteganografía son conocidos como canales sigilosos.

La esteganografía consiste en enviar los datos utilizando la emisión espontánea amplificada (ASE) que se presenta en los amplificadores EDFA. Las subportadoras ASE no son detectadas ya que presentan un espectro similar al ruido ASE del sistema. De esta manera se evita que un usuario no deseado pueda interferir en el canal.

Una de las desventajas que presenta la esteganografía es que el ASE ocupa todo el ancho de banda por lo que se limita su uso a un canal a la vez [3].

- ***Autenticación de las redes ópticas***

Otro de los aspectos importantes a tomar en cuenta en las redes es la autenticación. La interceptación de información que viaja a través de diferentes canales de las redes ópticas, puede hacerse simplemente usando un ROADM. Es por eso que la autenticación tiene el objetivo de evitar que usuarios no deseados intercepten canales a los que no tienen autorizado el acceso.

La autenticación en redes ópticas se realiza mediante el uso de códigos de acceso múltiple por división de código óptico (OCDMA). El código que se asigna a cada usuario es único y debe ser establecido tanto en el transmisor como en el receptor. De esta forma los datos codificados que se envían solo podrán decodificados por el usuario correspondiente [3].

- ***Protección ante escuchas ilegales***

La protección ante interceptaciones ilegales del canal, es un aspecto que influye en la calidad de seguridad de una red óptica. Para proveer protección ante este tipo de ataques existen diferentes mecanismos que se presentan a continuación.

➢ **Protección de las fibras ópticas utilizando interferencias en dirección opuesta**

Se sabe que los sistemas de comunicaciones ópticas en general se usan dos fibras para el tráfico bidireccional. La técnica de interferencia opuesta aprovecha esta característica, ya que consiste en enviar señales de interferencia por la fibra contraria a la que se realiza la transmisión de datos. Es así que esta señal de interferencia solo afecta a posibles escuchas ilegales del canal. La señal de interferencia puede ser ruido ASE o otra señal con la misma longitud de onda que la señal de datos [3].

**ATAQUES ACTIVOS**

- ***Planificación de la red óptica***

Es importante que durante la implementación de la red se identifiquen posibles puntos críticos para poder minimizarlos. Para mejorar la seguridad de la red los operativos pueden clasificar el servicio en tres tipos dependiendo el nivel de seguridad requerida [3].

➢ **De mejor esfuerzo:** para este tipo de servicios la planificación se basa en la cantidad de servicios que pueden resultar afectados en caso de un ataque. Para este tipo de servicios no se asignan recursos de protección.

➢ **De protección estándar:** este tipo de servicios también se planifican como servicios de mejor esfuerzo. La diferencia de este servicio es que sí se emplean recursos de protección ya sean compartidos o dedicados.

➢ **De usuarios Gold:** este tipo de servicio tiene acceso a recursos de protección Premium. Como, por ejemplo, enrutamiento por rutas de alta seguridad, y técnicas de prevención de desvío.

- ***Protección de puertos de monitoreo***

La protección de puertos de monitoreo es de suma importancia, ya que pueden ser utilizados para introducir señales de ataque a la red. En las redes ópticas las señales de ataque pueden ser introducidas utilizando las propiedades de reflectancia de los puertos. Es por eso que para brindar protección a los puertos de monitoreo sed usan aisladores ópticos o circuladores ópticos. Estos permiten que la señal de ataque sea desviada.

***C.*** **De existir, indique la normativa o estándares vigentes relacionados con los aspectos de seguridad en redes ópticas. Describa los estándares y describa los aspectos técnicos y procedimientos que consideren más relevantes.**

- ***RFC 2828***

La seguridad en redes ópticas en cuanto a la eliminación de ataques ya amenazas, trabaja siguiendo las especificaciones de la recomendación RFC 2828. Esta recomendaciÓN plantean cinco puntos importantes a tomar en cuenta para tener una red segura [4].

➢ **Autenticación:** confirmación de la identidad del usuario. Corroboración a una entidad que la información recibida proviene de un usuario verdadero.

➢ **Control de acceso:** proveer seguridad contra el uso de recursos por entidades no autorizadas.

➢ **Confidencialidad:** protección de la divulgación de los datos un usuario a entidades no autorizadas.

➢ **Integridad:** provee protección para que los datos almacenados o transmitidos no sean alterados.

➢ **No repudio:** provee protección contra usuarios que nieguen falsamente el haber enviado o recibido una determinada información.

- ***ISO 17799***

  El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre las empresas.

- ***UIT-T X.800***

  Se incluye una lista más completa de definiciones de seguridad en el compendio de definiciones de seguridad aprobadas por el UIT-T extraídas de las Recomendaciones del UIT-T [5].
  - **Control de acceso:** Estándar referente a la Gestión de claves de instituciones financieras. Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada.
  - **Amenazas fortuitas:** cabe señalar las disfunciones del sistema, los errores operativos y los problemas que plantean los programas informáticos.
  - **Imputabilidad**: Propiedad que garantiza que las acciones de una entidad puedan ser rastreadas de una manera inequívoca para imputarlas a esa entidad.
  - **Autenticación**: El término autenticación no se emplea en relación con la integridad de los datos, para ello se emplea el término integridad de datos.
  - **Intercambio de autenticación:** Mecanismo destinado a garantizar la identidad de una entidad mediante intercambio de información.
  - **Autorización**: Esta definición implica la concesión de permisos para realizar determinadas actividades (por ejemplo, acceder a datos) y su relación con determinados procesos, entidades o agentes humanos.
  - **Capacidad**: Testigo utilizado como identificador de un recurso de modo que la posesión del testigo confiera derechos de acceso a ese recurso.
  - **Criptograma**: Datos producidos mediante cifrado. El contenido semántico de los datos resultantes no está disponible
  - **Confidencialidad**: Propiedad que garantiza que la información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados.
  - **Credenciales**: Datos que se transfieren para establecer la identidad alegada de una entidad
  - **Descifrado**: Operación inversa al cifrado reversible correspondiente

- ***Otras normativas***

  Las redes ópticas operan bajo la normativa de varios estándares de seguridad los cuales se mencionan a continuación [2]:
  - **X9.17:** Estándar referente a la Gestión de claves de instituciones financieras.
  - **RFC 1321:** Estándar referente al algoritmo de mensajes MD5.
  - **RFC 1636:** Estándar referente a la arquitectura del internet.
  - **RFC 2049:** Estándar referente a las Extensiones de correo de Internet Multipropósito (MIME).
  - **RFC 2246:** Estándar referente al protocolo TLS (Transport Layer Security)
  - **RFC 2571:** Estándar referente a la arquitectura para describir Marcos de Gestión SNMP.
  - **RFC 3174:** Estándar referente a algoritmos de HASH seguro de EEUU.
  - **X.509:** Estándar IT-T referente a infraestructura de claves públicas y certificaciones.
  - **FIPS 46-3:** Estándar referente al cifrado de datos (DES)
  - **FIPS 180:** Estándar referente al HASH seguro (SHS).
  - **SP800-38:** Estándar referente a los modos de operación de cifrado de bloque.

## III. REFERENCIAS


[1] Á. J. Ordóñez Mendieta y J. A. Sigcho Poma, «Estudio de la seguridad en redes GPON,» Universidad Nacional de Loja, Loja, 2018.

[2] L. F. Abril Rincón, «SEGURIDAD Y GESTIÓN EN ARQUITECTURAS ÓPTICAS DE COMUNICACIÓN DE DATOS,» UNIVERSIDAD LIBRE PROGRAMA DE INGENIERIA DE SISTEMAS, Bogotá, 2013.

[3] D. Dahan y U. Mahlab, «Security threats and protection procedures for optical networks,» *The Institution of Engineering and Technology*, p. 16, 2017.

[4] «La arquitectura de seguridad OSI,» Dargon JAR, [En línea]. Available: https://www.dragonjar.org/la-arquitectura-de-seguridad-osi.xhtml. [Último acceso: 05 08 2021].

[5] ITU, «Seguridad de las telecomunicaciones y las tecnologías de la información,» 2009. [En línea]. Available: https://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-S.pdf. [Último acceso: 07 08 2021].