ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ANÁLISIS DE LA APLICACIÓN DEL PROTOCOLO DE SEGURIDAD SSL CON UNA HERRAMIENTA OPENSOURCE EN REDES DE TRANSMISIÓN DE DATOS ORIENTADAS A TELE PRESENCIA Y TELEMETRÍA.

JUAN GABRIEL PEÑAFIEL SIGUENCIA

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SISTEMAS DE TELECOMUNICACIONES

Riobamba – Ecuador

Mayo 2021

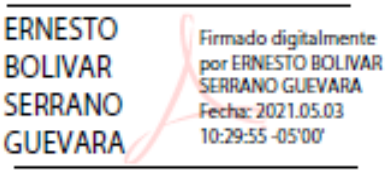
ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

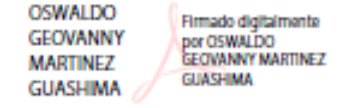
El **Trabajo de Titulación Modalidad Proyectos de Investigación y Desarrollo**, titulado: **"ANÁLISIS DE LA APLICACIÓN DEL PROTOCOLO DE SEGURIDAD SSL CON UNA HERRAMIENTA OPENSOURCE EN REDES DE TRANSMISIÓN DE DATOS ORIENTADAS A TELE PRESENCIA Y TELEMETRÍA",** de responsabilidad del señor Juan Gabriel Peñafiel Siguencia, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

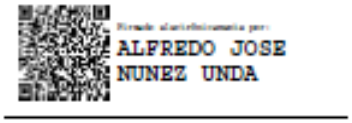
Ing. Jorge Luis Paucar Samaniego MSc
PRESIDENTE



Ing. Ernesto Bolívar Serrano Guevara MSc.
DIRECTOR DEL TRABAJO
DE TITULACIÓN



Ing. Oswaldo Geovanny Martinez Guashima MSc.
MIEMBRO DE TRIBUNAL

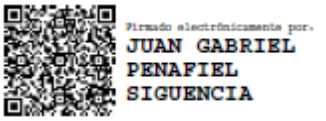


Ing. Alfredo José Nuñez Unda MSc.
MIEMBRO DE TRIBUNAL

Riobamba, mayo 2021

DERECHOS INTELECTUALES

Yo, Juan Gabriel Peñafiel Siguencia, soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.



Juan Gabriel Peñafiel Siguencia

No. Cédula: 0302309729

DECLARACIÓN DE AUTENTICIDAD

Yo, Juan Gabriel Peñafiel Siguencia declaro que el presente Trabajo de Titulación, modalidad Proyectos de Investigación y Desarrollo, es de mí autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Juan Gabriel Peñafiel Siguencia

No. Cédula: 0302309729

DEDICATORIA

Dedico este trabajo de titulación a mis abuelos y familia quienes son mi fuente de inspiración y fortaleza para buscar mi superación personal; a mi madre por su apoyo incondicional; a mi hermano, mis amigos a por sus ánimos y aliento para cumplir mis metas.

Juan Gabriel

AGRADECIMIENTO

Agradezco a Dios por haberme permitido logra una meta trazada y con sacrificio cumplirla, mis tutores y coordinadores en especial a los Ingenieros Ernesto Serrano y Oswaldo Martínez por ser un guía en este trabajo de titulación, quien de una manera acertada, coherente y profesional brindó sus conocimientos para concretar el desarrollo de la presente investigación.

A todas aquellas personas que de alguna manera me brindaron su apoyo en el desarrollo del proyecto de titulación y poder culminarlo.

Juan Gabriel

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

LISTA DE ABREVIATURAS

AES	Advanced Encryption Standard
AIX	Advanced Interactive eXecutive
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Goverment
CA	Certificado de Confianza
CMS	Content Management System
C2C	Consumer to Consumer
CSS	Cascading Style Sheets
CTRS	Telepresencia Cisco Servidor de Grabación
DSA	Direct Selling Association
FTP	File Transfer Protocol
FSF	Free Software Foundation
GLPI	Gestionnaire Libre de Parc Informatique
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines
IMAP	Internet Message Access Protocol
IT	Tecnología de la Información
ITU	International Telecommunication Union
NNTP	Network News Transport Protocol
OCS	Open Computer and Software
POP	Post Office Protocol
RSA	Rivest, Shamir y Adleman
SIP	Session Initiation Protocol
SMTP	Protocolo para Transferencia Simple de Correo
SSL	Secure Socket Layer
TELNET	Telecommunication Network
TCP	Transmission Control Protocol
TCS	Telepresencia Cisco Servidor de Contenidos
TIC	Tecnologías de la Información y la Comunicación
WCM	Web Content Management
3DES	Triple Data Encryption Standard

RESUMEN

En la actualidad las aplicaciones y tecnologías como la computación distribuida, voz y vídeo sobre IP requieren de una comunicación eficiente, segura y óptima entre distintos puntos remotos. El objetivo de esta investigación es diseñar un prototipo que integre el protocolo SSL con una herramienta Opensource incrementando la seguridad sin causar efectos negativos en las redes que será utilizadas para telepresencia y telemetría.

Es un estudio cuasi-experimental, con una investigación descriptiva, recolectando información de las debilidades de las diferentes herramientas. También es una investigación exploratoria y descriptiva, nos sirve para definir la herramienta Opensource a utilizar, midiendo de características y resultados para la definición del prototipo.

Utilizando el método científico experimental, hipotético deductivo para obtener diferentes conocimientos, y análisis y síntesis. Contando como diferentes fuetes de información primarias y secundarias además de técnicas e instrumentos como Sniffing, denegación de servicios, y observación de fichas.

Analizados los resultados de las pruebas en ambos escenarios se concluye que aplicar el protocolo de seguridad SSL no afecta negativamente en las redes de comunicación de datos.

Como propuesta se desarrolla una guía para la implementación de comunicaciones seguras para la transmisión de datos en redes orientadas a telepresencia y telemetría, incluyendo todas las consideraciones que se debe aplicar en los escenarios reales producto de las pruebas realizadas.

Palabras Clave: <PROTOCOLO SSL>, <TELEMETRÍA>, <TELEPRESENCIA>, <SEGURIDAD DE REDES>, <TRANSMISIÓN DE DATOS>, <OPENSOURCE>, <RENDIMIENTO>, <REDES>.

ABSTRACT

Currently, applications and technologies such as distributed computing, voice and video over IP require efficient, secure and optimal communication between different remote points. The objective of this research is to design a prototype that integrates the SSL protocol with an Opensource tool, increasing security without causing negative effects on the networks that will be used for telepresence and telemetry. It is a quasi-experimental study, with a descriptive investigation, collecting information on the weaknesses of the different tools. It is also an exploratory and descriptive research, it helps us to define the Opensource tool to use, measuring characteristics and results for the definition of the prototype. Using the experimental, hypothetical deductive scientific method to obtain different knowledge, and analysis and synthesis. Counting as different sources of primary and secondary information as well as techniques and instruments such as Sniffing, denial of services, and observation of files. After analyzing the results of the tests in both scenarios, it is concluded that applying the SSL security protocol does not negatively affect data communication networks. As a proposal, a guide was developed for the implementation of secure communications for the transmission of data in networks oriented to telepresence and telemetry, including all the considerations that must be applied in real scenarios as a result of the tests carried out.

Keywords: <SSL PROTOCOL>, <TELEMETRY>, <TELEPRESENCE>, <NETWORK SECURITY>, <DATA TRANSMISSION>, <OPENSOURCE>, <PERFORMANCE>, <NETWORKS>.

CAPÍTULO I

1. INTRODUCCIÓN

En la actualidad los sistemas de telemetría permiten vigilar diferentes infraestructuras como suministros de agua, niveles de agua entre otras; permitiendo hacer medidas correctivas mediante actuadores remotos, poniendo a disposición del centro central toda la información recolectada del estado de la infraestructura y tomar medidas de los acontecimientos suscitados. En la transmisión de datos existen diversas soluciones que dependen de aspectos económicos, extensión de la infraestructura, acceso al lugar, etc., a controlar o monitorizar; una solución que se puede dar es líneas alquiladas, sistemas de radio convencionales, entre otros.

Telepresencia es un sistema de videoconferencia que permite la conexión entre dos o más sedes que se pueden conectar a miles de kilómetros de distancia, permitiendo establecer una comunicación bidireccionales directa, fluida, flexible con niveles de calidad sorprendentes, permitiendo ver y escuchar al interlocutor con gran calidad de audio y video; a su vez posee componente de inmersión que evita los desplazamientos innecesarios de los interesados, ahorra tiempos improductivos, acelera los procesos de decisión y mejora la comunicación.

Además, no sólo se mantiene una comunicación oral y gestual, sino que al mismo tiempo se pueden compartir la visualización simultánea del interlocutor con una imagen de la pantalla de un ordenador donde realizar presentaciones.

En los últimos años se ha visto como las redes de comunicaciones han formado parte de la vida cotidiana y forman parte de la población para ser utilizadas por la mayoría de los ciudadanos y empresas, utilizándose para actividades como compra electrónica hasta el control logístico en puertos y aeropuertos internacionales. Este incremento en el uso de las redes de comunicación ha tenido múltiples consecuencias, pudiendo destacar entre ellas el aumento de la cantidad y la importancia de la información. En algunos casos encontramos que la información que fluyen por estas redes, requiere de algún tipo de protección en su tránsito, mediante servicios de confidencialidad, autenticación.

Existen diversas actividades delictivas que se presentan de muchas formas desde actualizaciones de estafas, engaños, suplantaciones de identidad esto se produce por información personal recabada de la víctima, debido al incremento de la información en la red se debe realizar medidas de seguridad y se pueden clasificar en medidas de protección a equipos o dispositivos instalando algún tipo de software o hardware que se encargan de proporcionar las herramientas necesarias.

En los últimos años múltiples protocolos de seguridad se han estandarizado, de manera que las

especificaciones de los mecanismos para proteger la información. Algunos de estos estándares se encuentran ampliamente integrados con las herramientas de comunicaciones en la actualidad.

1.1. Planteamiento del problema

Con varias implementaciones de tecnologías de telepresencia con grandes firmas en redes como CISCO, notamos que esta rama de las comunicaciones avanza a pasos agigantados por lo cual el acceso y la utilización se esta tecnología ya no solo está en entornos de red especializados para estos fines, sino que se encuentran adaptando redes de uso regular a las necesidades de la telepresencia para la utilización y mediana explotación de la misma, por lo cual los problemas regulares de las redes domésticas se convierten en problemas para la red orientada a la telepresencia.

Por otro lado, cabe mencionar a IPV6 como un punto trascendental a tener en cuenta en esta tecnología, teniendo 2 frentes a discusión, el punto positivo nos especifica que al ser matemáticamente 340.282.366.920.938.463.463.374.607.431.768.211.456 de direcciones posibilitan tener millones de direcciones para cada persona del mundo lo cual dejaría a la tecnología NAT fuera de uso, misma que es un gran causante de una baja en el rendimiento al comunicar una red privada (red interna de hogar/empresa) con una red pública (internet) (Cisco, 2016), mejorando así automáticamente el rendimiento de las comunicaciones, en este caso de la telepresencia.

Como punto negativo tenemos el ritmo lento con el que el mundo se está actualizando a la IPV6 basado en los costos que esto implica, con datos recolectados por la empresa GOOGLE sobre la expansión de IPV6 a nivel mundial, se puede observar que apenas un 28% de tráfico es generado en IPV6.

En cuanto al funcionamiento, como se mencionó anteriormente, las redes más utilizadas para este trabajo son las redes domésticas al igual que la IPV4, motivo por el cual, los problemas como la intercepción de tráfico en la red, así como la falsificación de sitios se vuelven problemas a tener en cuenta en las redes de telepresencia, dado que a diferencia de una simple comunicación por video, en una sesión de telepresencia se pueden tratar casos médicos o de alta importancia, en los cuales la manipulación de los datos podría tener consecuencias inclusive fatales.

En este contexto se hace evidente que en una red orientada a telepresencia es imprescindible contar con 2 factores primordiales como seguridad y rendimiento, en lo cual se basará este estudio.

1.2. Justificación

Dada la creciente demanda de integración global en cuanto a la participación de personas en procesos específicos como medicina o reuniones de negocios, le industria de la telepresencia ha tenido un desarrollo acelerado en los últimos años (Ñacato, 2014), no obstante la tecnología para la implementación de la misma no ha logrado avanzar con la misma velocidad, dado que a lo largo del tiempo este avance se ha visto continuamente limitado por la infraestructura disponible así como empañado por problemas legales entre las empresas como Microsoft y Apple por las tecnologías desarrolladas con este fin (Salvador, 2007).

Otra rama en que actualmente se encuentra difundiendo la telepresencia es en la medicina, haciendo posible la intervención de personal especializado desde una ubicación geográfica remota, dentro de la cual en la rama de cirugía existe especial interés, mismo que se ha visto interrumpido por la velocidad de las conexiones así como especialmente por la seguridad de las mismas (Luevano, 2013), dado que alguna interrupción en un momento determinado podría tener consecuencias incluso fatales en muchos casos.

Una ciencia moderna como la robótica también basa significativos proyectos sobre la telepresencia, tal es el ejemplo del robot "Curiosity" de la NASA, el cual permite tomar imágenes de su actividad en Marte e interactuar con su entorno de manera remota (Reyes, 2014), en el cual, un fallo determinaría la pérdida de la inversión realizada en la construcción así como el envío del robot.

En cuanto al protocolo SSL se ha determinado que a través de su conexión criptográfica mejora sustancialmente la seguridad de una comunicación apoyado en la autenticación mutua que provee basada en claves públicas, sin embargo, este proceso involucra la inversión de recursos hardware durante el proceso, lo cual podría influir de manera negativa en el rendimiento de las redes, especialmente cuando se desea que estas sean en tiempo real.

Por cuanto la presente investigación pretende utilizar el protocolo SSL para mejorar la seguridad de las redes para telemetría sin influenciar negativamente en el rendimiento de la red.

1.3. Objetivos

1.3.1. Objetivo general

Diseñar un prototipo que integre el protocolo SSL con una herramienta Opensource para incrementar la seguridad sin afectar negativamente el rendimiento de las redes utilizadas para telepresencia y telemetría.

1.3.2. Objetivos específicos

- Analizar herramientas Opensource para implementación del protocolo SSL para seleccionar uno a utilizar en los ambientes de pruebas.
- Implementar un ambiente de pruebas de similares características a los estudiados en el estado del arte para el uso de telepresencia en el cual determinar vulnerabilidades en seguridad y rendimiento.
- Implementar el protocolo SSL en el ambiente de pruebas para compararlo con su versión inicial.
- Empleando la metodología PPDIOO, definir el prototipo de red y configuraciones a implementar basado en los resultados obtenidos sobre seguridad y rendimiento del ambiente inicial y el ambiente de pruebas en el que se implementó el protocolo SSL.

1.4. Hipótesis

1.4.1. Hipótesis general

La implementación del protocolo SSL con una herramienta Opensource en una red para telepresencia, conlleva una mejora en la seguridad sin afectar negativamente el rendimiento de las redes utilizadas para telepresencia.

1.4.2. Hipótesis Específicas

- La elaboración del sustento teórico y conceptual fundamenta la investigación.
- La implementación de una red para telepresencia permite la identificación de problemas habituales en cuanto a seguridad.

La implementación del protocolo SSL con una herramienta Open Source en redes para telepresencia, conlleva una disminución en los problemas detectados y su incidencia.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Telemetría

2.1.1. Definición

Telemetría es una técnica automatizada de las comunicaciones que permite la recopilación y medición de datos realizados en lugares remotos y de transmisión para vigilancia; utiliza transmisión inalámbrica, aunque fue original de los sistemas de transmisión utilizados por cable. Los usos más importantes de telemetría han sido la recopilación de datos del clima, supervisión de plantas de generación de energía y hacer el seguimiento de vuelos espaciales tripulados y no tripulados.(Bedoya, 2013)

Los sistemas que utilizan esta tecnología tienen ventaja sobre el control y supervisión del funcionamiento, así como el envío de información recolectada por el sistema hacia la estación receptora para su debido análisis y estudio (Labastida, 2014, p. 31)

Los sistemas telemétricos tienen como función realizar las mediciones en diferentes puntos remotos para luego hacer trasmisiones a un puesto de control. El equipo de telemetría este compuesto por sensores que miden una magnitud física (calor, presión, caudal, temperatura, etc.) y la transforman en señales eléctricas (analógicas o digitales) para su posterior envió y tratamiento. (García, 2008, p. 25).

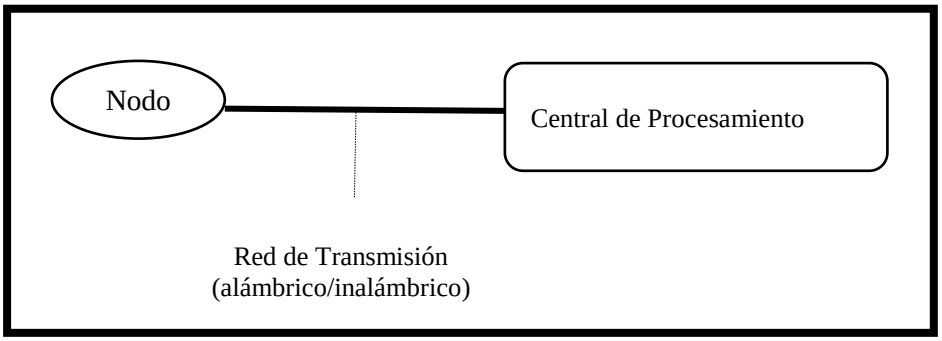


Figura 1-2: Diagrama de un proceso Telemétrico
Fuente: (García, 2008, p. 25)

2.1.2. Partes de un sistema de telemetría

Los elementos que intervienen el sistema de Telemetría varían dependiendo del lugar donde están utilizados, por lo general están formados por los nodos (su función es realizar las mediciones de las variables físicas) en un centro de control y monitoreo (García, 2008, p. 16).

2.1.3.1. Los elementos del sistema de Telemetría

- Sensores
- Sistemas de comunicaciones de datos
- Sistema de procesamiento y almacenamiento
- Acoplamiento de la señal proveniente del sensor
- Receptores (García, 2008, p. 16)

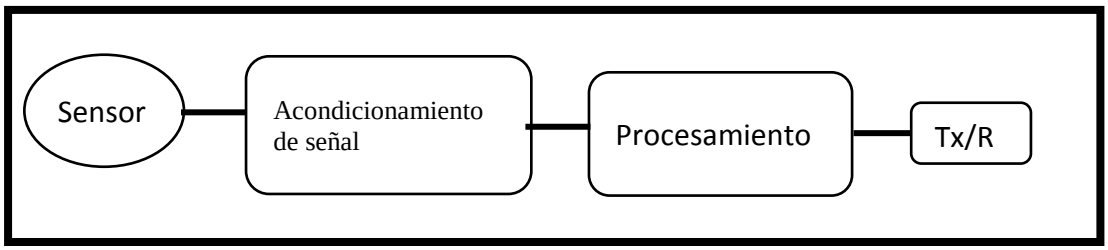


Figura 2-2: Diagrama de bloques de un nodo

Fuente: (García,2008, p. 16)

Cada una de las partes están acopladas de manera específica, si una de ellas falla el sistema se altera en sus principales funciones.

Descripción de las funciones del sistema de Telemetría:

- **Sensores. –** Se produce la señal eléctrica de la medición de alguna magnitud física (temperatura, presión, etc.); este sensor no altera la propiedad censada, esto depende del sensor y su tecnología, requiere de un proceso de acondicionamiento de la señal que es realizado por lo general por un amplificador.
- **Tx / Rx. –** Aquí se realiza el proceso de trasmisión y recepción de datos, enviando los datos a la central provenientes del sensor después de ser tratados.
- **Procesamiento. –** Se reciben las señales provenientes del proceso de control automático para ser trasmitido, almacenado esto depende de las necesidades del sistema implementado. (García Manuel, 2008, p. 16)

- **Acoplamiento de la señal. –** Las señales generadoa por los sensores esta dado en los milivoltios o microamperios, esto dificulta su acople al sistema de almacenamiento, por lo general su adecuación es la parte fundamental para el funcionamiento de los nodos. (García Manuel, 2008, p. 16)

2.1.3.2. Magnitudes

Las magnitudes a ser medidas son físicas, químicas como se menciona a continuación:

- Temperatura
- Humedad
- Caudal
- Presión
- Velocidad
- Aceleración
- Luminancia
- PH
- Densidad
- Colores (Valencia, 2011)

2.1.4. Esquemas del Sistema Telemétrico

En estos sistemas se hacen la medición de varias variables en los nodos distantes de la estación central, por lo general se realiza un sistema de multiplexación.

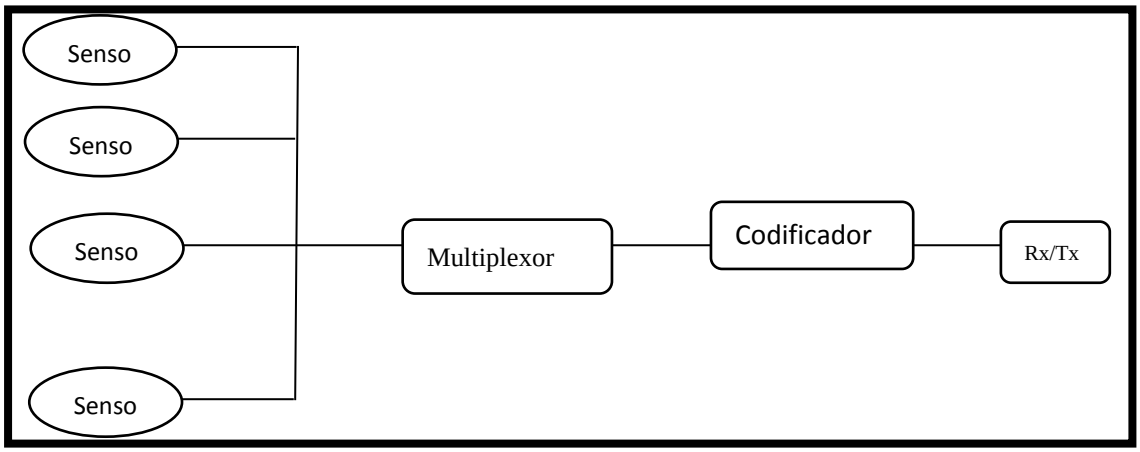


Figura 3-2: Diagrama de bloques de un sistema de multiplexación del sistema telemétrico
Fuente: (García, 2008, p. 17)

- Si la distancia de los nodos a la estación central es muy amplia se debe utilizar amplificadores para evitar la atenuación de la señal.
- Cuando los sensores están a una distancia muy amplia se les debe considerar como nodos independientes como se muestra en la figura 4-2.

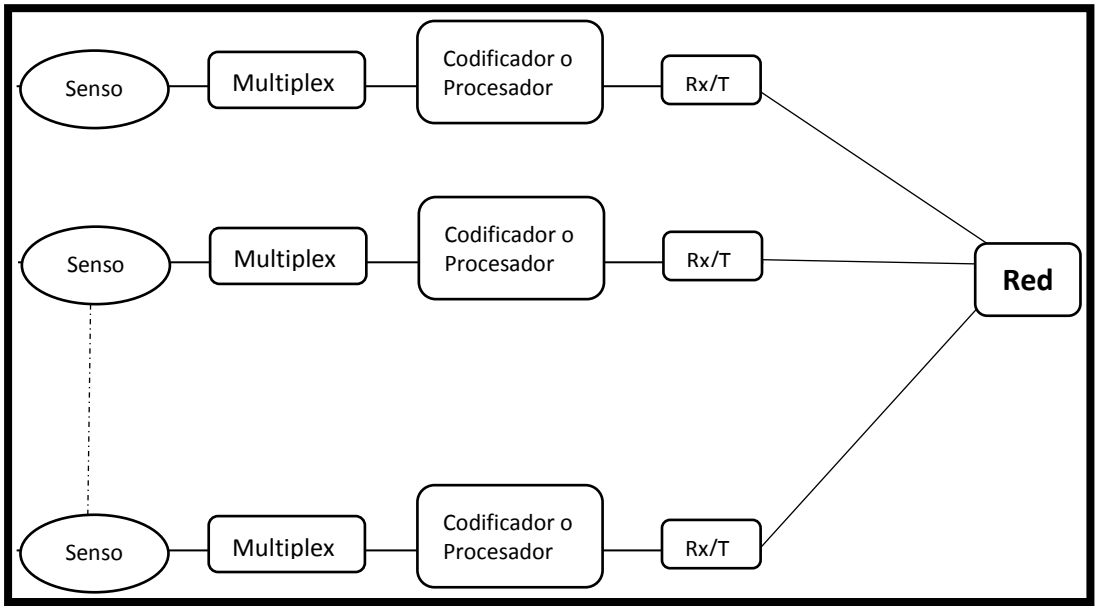


Figura 4-2: Red de nodos

Fuente: (García, 2008, p. 17)

Los sistemas de telemetría están formados por estructuras diferentes esto depende del sector donde se aplique y está formado por medición, procesamiento y trasmisión.

2.1.5. Enlaces de los Sistemas de Telemetría

Para la comunicación de los sistemas de telemetría se usan medios guiados (cobre, cable de par trenza, etc.) y me medios no guiados (onde de frecuencia).

- **Medios Guiados. –** La distancia máxima entre los nodos deben ser 100m y se utiliza cable de par trenzado, una de las ventajas es la economía. Actualmente lo más utilizado es la fibra óptica como medio guiado con mayor inmunidad al ruido eléctrico y no tiene límite de distancia.

- **Medios No Guiados. -** Se utiliza para la movilidad de los sistemas o de los nodos, la mayor ventaja en la comunicación que proporciona este medio es el enlace entre nodos que están separados por grandes distancias y donde la diversidad topográfica es muy irregular y de muy poco acceso.

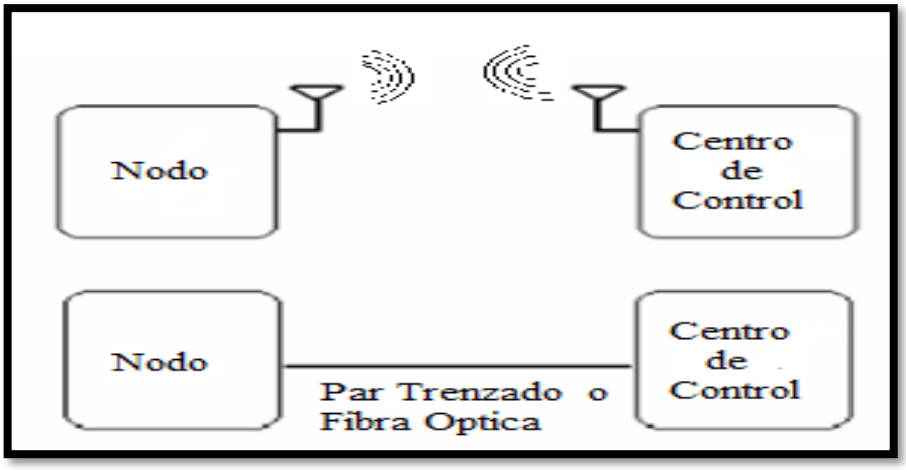


Figura 5-2: Diagrama de bloques de un sistema de telemetría dependiendo del medio de comunicación
Fuente: (García, 2008, p. 18)

2.1.5.1. Enlaces por Ondas Electromagnéticas y Espectro Radioeléctrico

En el espectro radioeléctrico se encuentran todas las radiaciones de origen electromagnético que existen en la naturaleza y están divididas en regiones dependiendo del rango de frecuencias donde se propagan.

La división del espectro radioeléctrico está basada en bandas de frecuencias que va desde los 30 KHz hasta 300 GHz como se muestra en la figura

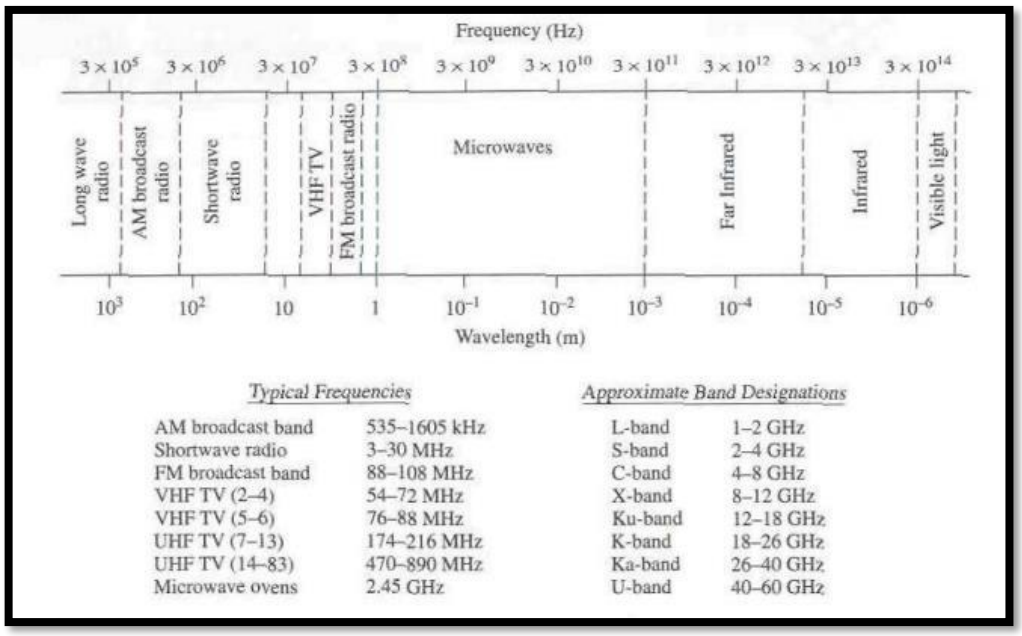


Figura 6-2: División del espectro radioeléctrico
Fuente: (Labastida,2014, p. 32)

Las frecuencias utilizadas en las telecomunicaciones según la ITU (Internacional Telecommunication Union):

Tabla 1-2: Las frecuencias utilizadas en las telecomunicaciones

Frecuencia	Valor	Nombre
Very Low Frecuency	9 KHz a 30 KHz	Radio a larga distancia
Low Frecuency	30 KHz a 300 KHz	Radiodifusión Naval
Medium Frecuency	300 KHz a 3 MHz	Radiodifusión AM y Comunicación Aeronáutica
High Frecuency	3 MHz a 30 MHz	Radiodifusión
Very High Frecuency	30 MHz a 300 MHz	Red de servicio de radio
Ultra High Frecuency	300 MHz a 3 GHz	Difusión de TV
Super High Frecuency	3 GHz a 30 GHz	Radar
Extremely High Frecuency	30 GHz a 300 GHZ	Acceso Inalámbrico de banda ancha

Fuente: (Labastida Paulina,2014, p. 32)

2.1.5.2. Microondas

Esta tecnología ocupa canales de 30 GHz a 45 GHz y poseen un gran ancho de banda disponible para los usuarios finales y los operadores de redes de telecomunicaciones; también están sujetas a dificultades del medio físico, estados meteorológicos, atenuaciones o ecos. Requiere una línea de vista sin obstáculos para un buen desempeño.

- Bajo costo en la utilización de enlaces terrestres.
- Portabilidad y flexibilidad de reconfiguración
- Amplio ancho de banda para la trasmisión de datos multimedia
- Requerimiento indispensable de línea de vista
- Susceptible al ambiente ya que se puede provocar distorsión o perdida de la señal
- Requerimientos de permiso de licencia Restricciones a la colocación de torres repetidoras dependiendo de la zona. (Labastida, 2014, p. 32)

2.2. Telepresencia

2.2.1. Definición de telepresencia

Este protocolo es muy utilizado por la mayoría de las empresas pequeñas, medianas y grandes, la que permite integrar señales de voz, datos y videos, que aprovecha de manera eficiente al ancho de banda, permitiendo lograr comunicaciones de voz y video de alta definición y calidad en tiempo real.(Angulo, 2014, p. 5)

Permite mantener una mejor fiabilidad, calidad de servicio (QoS), bloqueos a hackers logrando mayor seguridad y confiabilidad; también se puede incrementar aplicaciones de uso intensivo de ancho de banda, tales como videoconferencia de alta definición. Por ejemplo, si se realizará videoconferencias en alta calidad la transmisión no sufrirá inconvenientes en los puntos donde se conectan a telepresencia, y depende de las necesidades de los usuarios. Esto incluye puntos terminales envolventes, multifunción, personales y móviles. (Angulo, 2014, p. 5)

- Servicios administrados y alojados
- TelePresence entre empresas
- Servicios de valor agregado
- Salas públicas

2.2.2. Características de telepresencia

Los sistemas de telepresencia poseen una arquitectura de red inteligente que incorpora funciones innovadoras de seguridad, servicio y confiabilidad para conectarse dentro de una misma organización o entre distintas organizaciones, para eso usa tecnología IP estándar y funciona en una red integrada de voz, video y datos. (García et all, 2008, p.39)

Ofrecen comunicaciones de voz y video de alta calidad y en tiempo real como, por ejemplo: oficinas centrales, sucursales y oficinas remotas; son confiables y seguras, operan con calidad de servicio incluso sobre conexiones con ancho de banda limitado, o conexiones de Internet de banda ancha de alta velocidad. (García et all, 2008, p.39)

Este sistema incorpora cámaras y pantallas, iluminación, altavoces, micrófonos y capacidad de proyección para las salas de mayor tamaño. Las salas de Telepresencia pueden utilizar ya sea muebles diseñados especialmente para el sistema o mesas y sillas existentes. (García et all, 2008, p.39)

La interfaz de usuario sencilla e intuitiva elimina tareas y costos operativos para que pueda concentrarse en la comunicación y no en la tecnología.

- **Telefonía IP**. - Estos sistemas usan teléfonos y capacidades de administración de llamadas basadas en IP para simplificar el inicio de llamadas., esto se logra por la interfaz telefónica en vez de un control remoto complicado, los usuarios no necesitan capacitación. (García et all, 2008, p.39)
- **Servicios. –** Permite proporcionar sencillas aplicaciones de programación, administración, facturación, seguimiento de las actividades del sistema y la presentación de los servicios en tiempo real.
- **Groupware**. - La integración con soluciones de groupware empresarial (tales como Microsoft, Outlook y Lotus Notes) facilita la programación de reuniones y el acceso a salas y recursos. (García et all, 2008, p.39)

2.2.3. Generalidades de las soluciones de telepresencia

Este sistema utiliza audio de alta calidad y video de gran realismo a baja latencia en un entorno especialmente adaptado, es una experiencia muy buena como estar realmente en la misma sala con los demás participantes. (García et all, 2008, p.37-38)

Estos sistemas cuentan con colaboración innovadoras, fáciles de usar, entorno atractivo, arquitectura confiable y seguro.

Los estándares y tecnologías utilizados son:

- Codificadores/ Decodificadores y Cámaras de alta definición con resoluciones de 720p y 1080p. (García et all, 2008, p.37-38)
- Protocolo SIP (Session Initiation Protocol)
- Acondicionamiento ambiental óptimo para proporcionar audio y video de la mejor calidad.
- Funciones de cifrado de medios
- Señales sin latencia detectable en la llamada de telepresencia del usuario
- Códecs de video H.264 o H265 que ofrece mayor calidad con baja velocidad de transferencia.
- Codificador de audio con retardo bajo (AACLD) de banda ancha. (García et all, 2008, p.38)
- Grabación de video de alta definición para proporcionar mensajes dinámicos
- Interoperabilidad con sistemas de videoconferencia basados en estándares H.323 con alta definición.
- Audio espacial multicanal con cancelación de eco y filtros de interferencia(García et all, 2008, p.39)

2.2.4. Arquitectura de telepresencia

La arquitectura de este sistema incluye dispositivos a nivel de infraestructura de red, terminales, servidores, aplicaciones y recursos de hardware y/o software, de acuerdo a los requerimientos y necesidades, permitirá que éste disfrute de una la experiencia de audio, video de alta calidad.

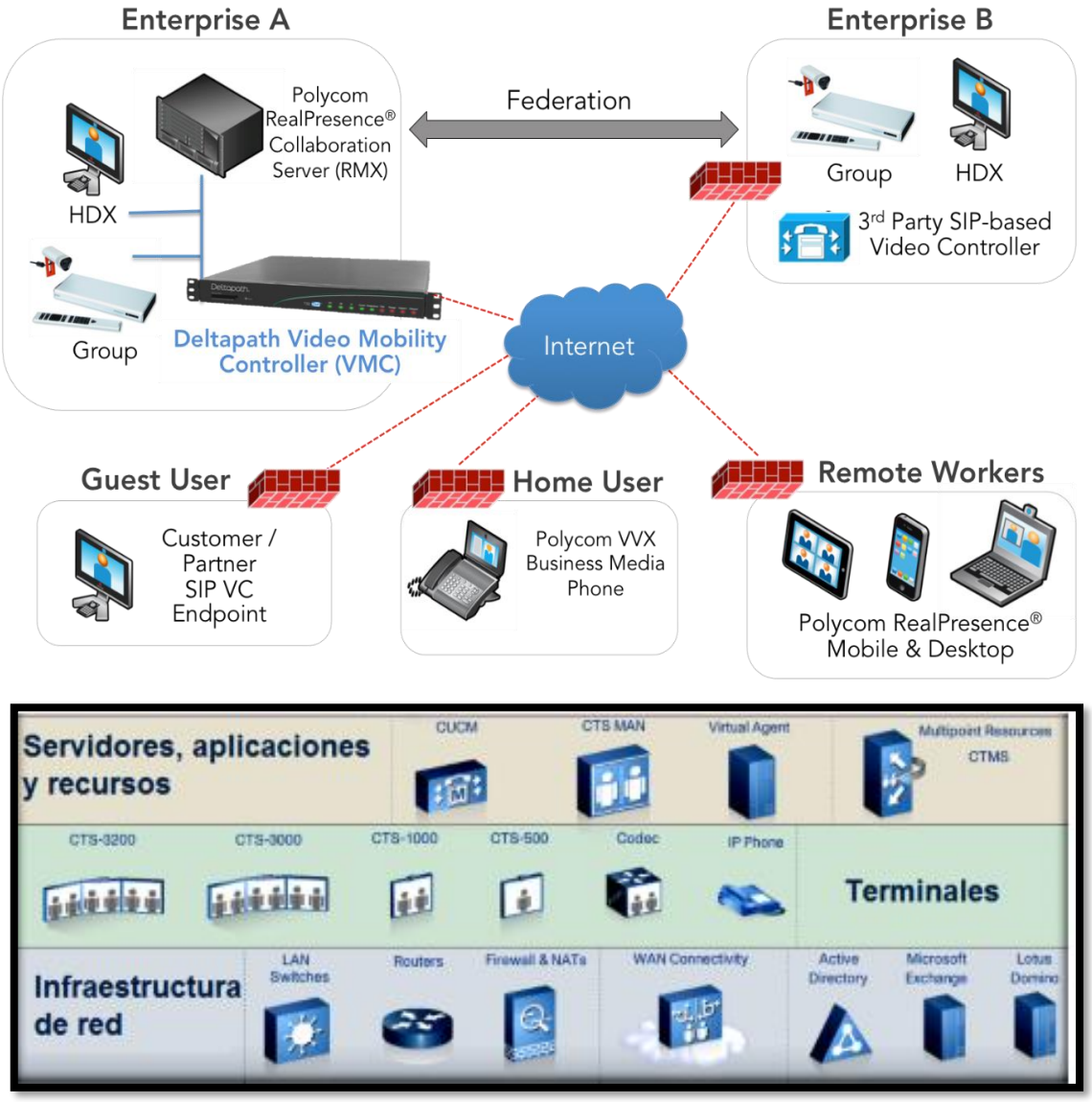


Figura 7-2: Elementos usados en la Arquitectura
Fuente: (García et all, 2008 p.37)

La arquitectura utiliza un centro de Telepresencia Server encargado de interconectar los distintos dispositivos que hacen parte de la infraestructura.

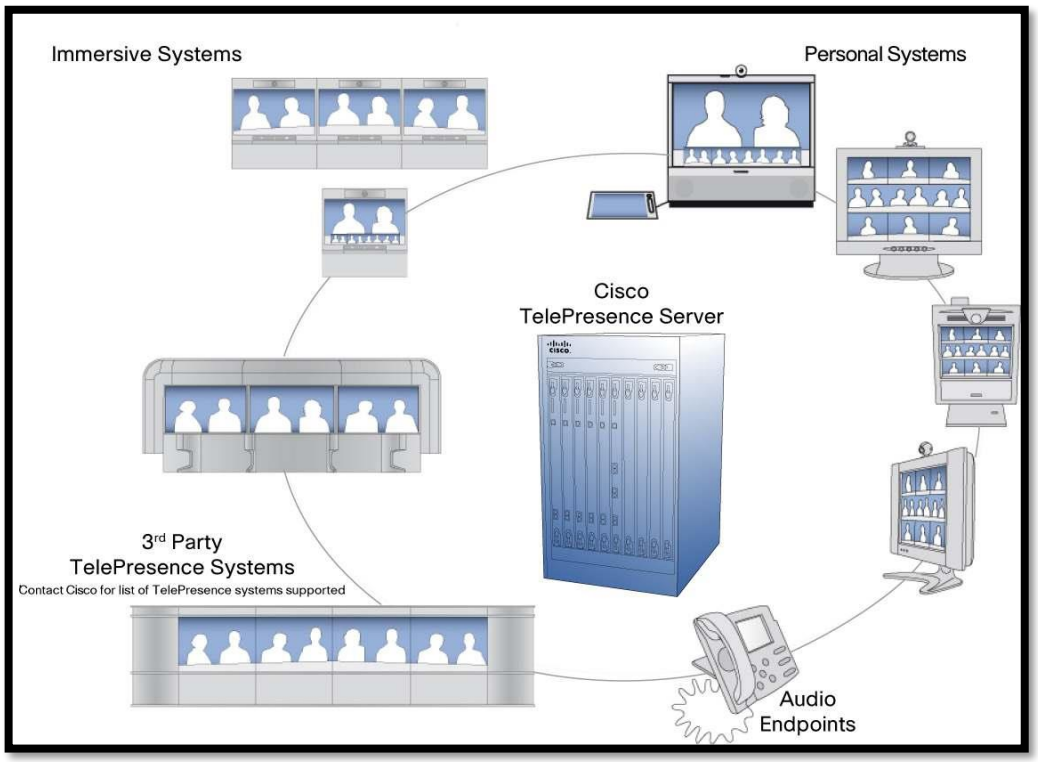


Figura 8-2: Modelo de la Telepresencia Server

Fuente: (García et all, 2008 p.39)

Tabla 2-2: Características de los elementos de Telepresencia

Elemento	Característica	Funciones
Servidor de Telepresencia	• Interoperabilidad de Telepresencia con • múltiples proveedores. • Es compatible con terminales de videoconferencia de los principales fabricantes y basada en estándares de la industria. • Reconoce el tipo de sistema a unirse a una Conferencia. • Proporciona a los participantes la mejor vista posible para sus sistemas • Proporciona una interfaz de administración fácil de usar y versátil.	• Soporta sistemas de Telepresencia individuales y de múltiples pantallas. • El servidor interconecta terminales HD y SD. • Resoluciones de vídeo de alta definición. • Puertos de sonido de banda ancha adicionales • Ancho de banda por la pantalla hasta 4 Mbps • AES • Hasta 1080p30 y 720 p 60 cuadros por segundo (fps)
Matriz de Video	• Posee 8 entradas (2 x HDMI, 3 x HDMI/VGA, 1 x entrada analógica, 2 x entrada digital). • La flexibilidad multi-formato que garantiza la	• Permite el enrutamiento de video, audio y procesamiento de las señales de control.

	conectividad entre dispositivos analógicos y digitales. • Son compatibles con estándares vigentes.	
Monitores	• Pantalla LED • 60″ y 19″ • Resolución: 1920 x 1080 • Interfaces HDMI • Interface Ethernet • DVI Audio In • Digital Audio Out	• Permite la visualización de los diferentes contenidos.
Transmisores de Audio y Video	• Contaran con entradas de video, VGA para compatibilidad con equipos. • Salidas análogas y una entrada HDMI. • Debe soportar estandares: H.263, H.263+, H.264. H.265.	• Se trasmitirá desde transmisores DM 8G+ para audio y video. • Seleccionara de forma automática entradas de audio y video.
Audio y Parlantes	• Puede ser un sistema estéreo para mayor intangibilidad.	• Esto debe ofrecer los niveles de sonido apropiados para las conferencias.
Iluminación	• Este sistema será de manera autónoma y por medio de sensores. • Reguladores de luces acorde a cada caso o uso.	• Permite el control de los circuitos de manera independiente.
Sistema y Pantalla de Control	• El sistema de control está formado por la matriz de video y mezclador de audio. • Las salas tendrán una pantalla de control táctil.	• Permitirá el acceso a reuniones, contactos, directorios y contenidos de las conferencias. • Gestiona llamadas.

Fuente: (García et all, 2008, p.39)

2.2.5. Arquitectura de Video en Telepresencia

Está formado por cinco categorías como:

- Endpoints (Puntos finales o terminales)
- Video Services (Servidor de video)
- Video Network Services (Servicio de red de video)
- Management (Gestión o manejo)
- Network (Red) (Angulo, 2014, p.7)

Las categorías proporcionan diferentes dispositivos con funciones específicas para despliegue de video. (Angulo, 2014, p.7)

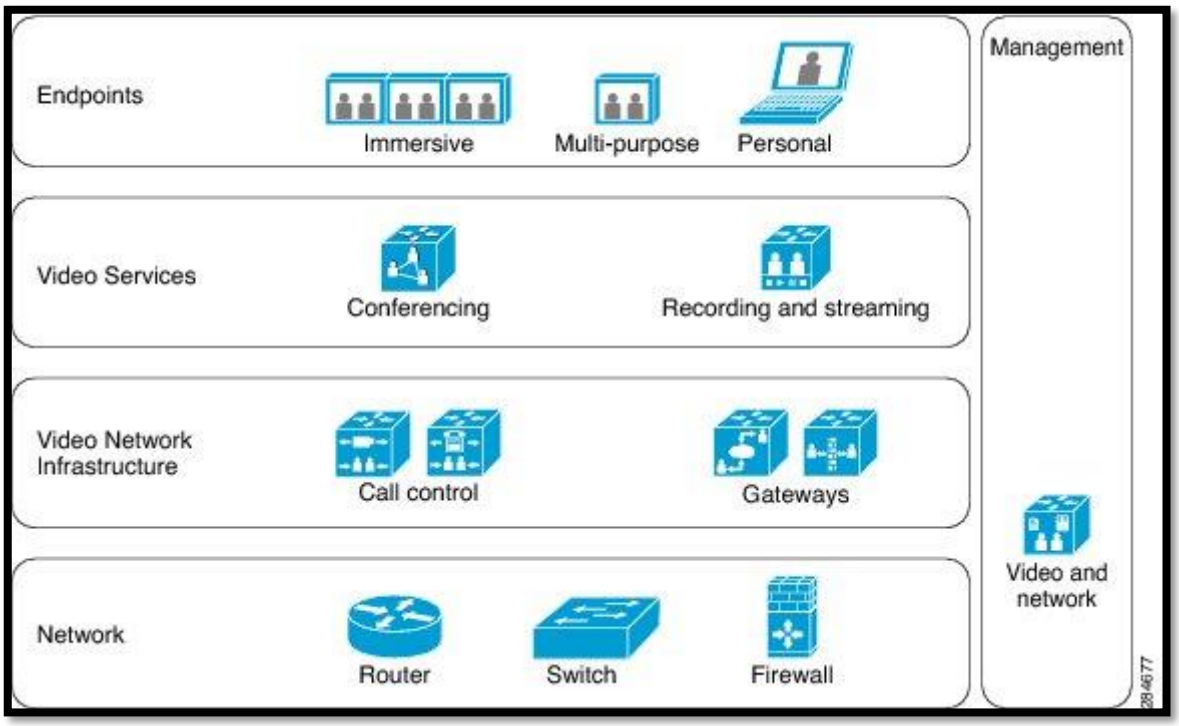


Figura 9-2: Arquitectura de video
Fuente: (Angulo 2014, p.7)

2.2.5.1. Endpoints

Están constituidos por una pantalla de micrófonos, altavoces, videos y procesamiento de audios (codecs); todos estos elementos se conectan en un solo dispositivo como los teléfonos, sistemas multipantallas. Cada terminal video es compatible con múltiples resoluciones y no admiten el mismo ajusto de resolución; la resolución más utilizada es de 1080p a 30 fotogramas por segundos (Fps), (Angulo, 2014, p.7).

Las terminales de video tienen un conjunto de funciones que consisten en la capacidad de enviar y recibir audio y video, enviar y recibir contenido compartido, esto depende de las características avanzadas tales como conferencia integrada o la capacidad para soportar video adicional y fuentes de audio pueden estar disponibles en el momento de la transmisión, (Angulo, 2014, p.7).

Las resoluciones más altas consumen más ancho de banda de la red y los clientes optan por limitar las resoluciones más altas basadas en el tipo de terminal o tipo de usuario.

Figura 10-2: Clases de video

Fuente: (Angulo, 2014, p.8)

2.2.6. Servicio de video para telepresencia

Servicios de video consiste en dos subcategorías:

2.2.6.1. Conferencia

Permiten que tres o más dispositivos de video y conferencia participen en una reunión en el mismo tiempo, y puedan proporcionar una gestión de los recursos permitiendo que los puertos sean más eficientes. Algunos dispositivos de conferencia soportan conmutación y transcodificación de entradas de audio y video sin necesidad de manipular los medios de comunicación del mismo video.(Angulo, 2014, p.10)

Las plataformas de conmutación de video cambian de un extremo a otro y requieren el uso de todos los terminales de video para el envío y recepción de las resoluciones. La resolución es rentable y escalable para la implementación de terminales de video y no requieren funciones de video avanzadas. (Angulo, 2014, p.10)

La transcodificación es l codificación y decodificación de flujos de video entre puntos finales (terminales), también permite establecer una lista máxima de flexibilidad en conferencias y largometrajes, en la siguiente tabla se puede observar las plataformas que soportan conmutación y transcodificación.

Tabla 3-2: Plataformas que soportan conmutación y transcodificación

Plataforma de Conferencia	Conmutación (Switching)	Transcodificación (Transcoding)
Cisco TelePresence Multipoint Switch	SI	NO
Cisco TelePresence Server	NO	YES
Cisco TelePresence MCU4000 Series and MSE 8000 series	NO	YES
Cisco Integrated Services Router (ISR) G2	NO	YES

Fuente: (Angulo, 2014, p.10)

2.2.6.2. Transmisión y grabación

Los dispositivos de trasmisión y grabación dan la posibilidad de reproducir, grabar y transmitir mensajes, grabaciones que puede ser escuchada por un gran número de usuarios, los dispositivos que se encuentran en el mercado son los siguientes:

- **Telepresencia Cisco Servidor de Contenidos (TCS). –** Está disponible como una aplicación que proporciona grabación en vivo, transmisión y reproducción de las reuniones de video. Las trasmisiones en vivo y grabaciones se pueden apreciar los estándares Quick Time, RealPlayer y Windows Media Player.

- **Telepresencia Cisco Servidor de Grabación (CTRS). –** Está basado en plataformas que proporcionan el modo de estudio, grabación de eventos y reproducción de sistemas de Telepresencia.

2.2.7. Característica telepresencia y videoconferencia

- Las dos proporcionan reuniones virtuales.
- Clasifican que cualquier unidad de videoconferencia compatible con video de alta definición, como un producto de Telepresencia.

- Un sistema de Videoconferencia de alta definición puede ser parecida a una experiencia de Telepresencia, permitiendo que diferentes proveedores utilicen códecs de alta definición que hacen parte de un sistema de Telepresencia.
- La telepresencia es un conjunto de varias tecnologías incluyendo audio y video permitiendo que los usuarios formen parte de una misma sala, lo que no permite hacerla videoconferencia.(García, 2008, p. 33-34)

2.2.8. Diferencias entre telepresencia y videoconferencia

Tabla 4-2: Diferencias entre Telepresencia y Videoconferencia

	Telepresencia	**Videoconferencia**
Calidad	• Video y Audio de alta calidad. • Usan cámaras especializadas ubicadas en sitios estratégicos. • Las cámaras poseen un foco fijo y optimizado. • Pantallas Integradas que proporcionan imágenes vividas y realistas. • El audio nítido, realista con códec de banda ancha. • Los micrófonos y altavoces están estratégicamente ubicados en la sala. • La iluminación, acústica son requerimientos necesarios para las salas de Telepresencia.	• En la actualidad proporcionan calidad de video y audio con muchos sistemas de alta definición en el video y banda ancha para el audio. • Se adaptaron sistema para la flexibilidad y adaptabilidad. • Estos sistemas utilizan cámaras de pan-tilt-zoom para salas. • Para este sistema se puede integrar pantallas grandes proyectores para salas mucho más grandes. • En estos sistemas utilizan micrófonos para mesas en salas de conferencias.

Simplicidad	• Estos sistemas están diseñados con interfaces simplificadas, sencillas (teléfonos IP) que son utilizados en todos los sistemas. • Son inflexibles y carecen de muchas características que proporcionan los sistemas de videoconferencia. • Los primeros sistemas proporcionaban funciones básicas. • En la actualidad el sistema de telepresencia es sencillos y fácil de agregar conjuntos funcionales implementados por las nuevas tecnologías.	• La complejidad y la inconsistencia de las diferentes interfaces hacen la baja utilización de este sistema. • Para este sistema se utilizan controles remotos para reuniones, cámaras de foco, compartir documentos entre otros. • Usan paneles táctiles en salas de gran tamaño. • Algunas empresas utilizan personal encargado de planificar, iniciar y gestionar reuniones para las videoconferencias.
Ancho de banda	• Para este sistema el uso de ancho de banda es muy grande. • La telepresencia ha implementado algoritmos de comprensión basadas en los estándares para la reducción del consumo del ancho de banda. • La resolución utilizada es de 1,5 Mbps a 3 Mbps. • Algunos de estos sistemas utilizan tres pantallas de video al mismo tiempo. •	• Este sistema de videoconferencia de alta calidad utiliza el mismo ancho de banda que la telepresencia. • Lo que más abarca en este sistema es la codificación de video y audio. • Este sistema habilita las resoluciones más bajas de audio y video para reducir el consumo de ancho de banda. • La resolución utilizada es de 720p y consume entre 2Mbps a 4Mbps

Fuente: (García, 2008, p. 37)

2.3. Protocolo de seguridad SSL

2.3.1. Definición

Este protocolo de cifrado fue diseñado para proporcionar comunicaciones seguras y transferencia de datos en internet, permitiendo a los clientes autenticar la identidad de servidores mediante la verificación de sus certificados digitales X.509 y rechaza conexiones si el certificado del servidor no es emitido por una autoridad de certificados de confianza (CA). El protocolo SSL de

encriptación del tráfico HTTP es utilizado entre sitios web y los navegadores, pero también es utilizado por otras aplicaciones como mensajería instantánea y las transferencias de correo electrónico.(Granda et all, 2017, p. 21)

Es un protocolo criptográfico que proporciona comunicaciones seguras en la red, se basa en el proceso de cifrado de clave pública estableciendo un canal de comunicación seguro entres dos equipos o terminales después de una fase de autenticación, esta comunicación se realiza mediante mensajes entre el servidor y el cliente. (Alonso, 2013, p.11)

SSL es el protocolo más utilizado para la autenticación de sitios web, proporcionando privacidad e integridad entre dos o más aplicaciones; está formado por dos capas, la capa interior es conocida como (SSL Record Protocol), este puede funcionar sobre una capa de trasporte confiable y a su vez se encarga de la encapsulación de varios protocolos de capas superiores. (Cornejo, 2010, p. 11)

Se encuentra en la capa de transporte de pila TCP/IP baja la capa de aplicación, es decir debajo de los protocolos HTTP, FTP, SMTP, etc. Este es independiente del protocolo utilizado por lo tanto se puede realizar transacciones a través de HTTP, FTP, POP e IMAP cifrado con el sistema SSL. (AlonsoJesús, 2013, p.11)

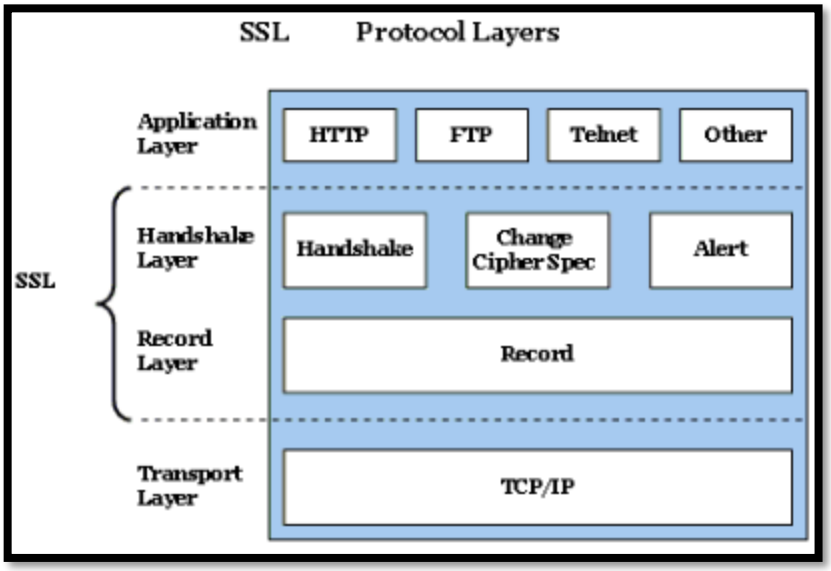


Figura 11-2: SSL en modelo TCP/IP

Fuente: (Alonso, 2013, p.11)

2.3.2. Características de SSL

SSL proporciona mecanismos para establecer una comunicación de manera segura entre cliente y servidor.

- Cifrado de datos: toda la información transferida, aunque caigan en manos de atacantes será indescifrable, garantizando la confidencialidad. (Guaigua, 2007, p. 48)

- Autenticación de Servidores: el usuario se asegura de la identidad del servidor al que se conecta y al que se envía información personal y confidencial.
- Integridad de mensajes: permite detectar modificaciones intencionadas o accidentales en la información mientras viaja por internet.
- Autenticación del cliente: permite conocer al servidor la identidad del usuario, con el fin de decidir si se puede acceder a ciertas eras que están restringidas. (Guaigua, 2007, p. 48)

2.3.3. Capa del estándar SSL

- SSL Record Layer
- SSL Handshake Layer

SSL Record Layer: Esta se utiliza para encapsular varios tipos de protocolos de mayor nivel, proporcionando comunicación segura; tomando mensajes y los codifica con algoritmos de encriptación de manera simétrica. (Granda, 2017, p. 24)

SSL Handshake Layer: Esta parte es la fase de negociación de los algoritmos, donde se hacen la autenticación del servidor generando el secreto compartido. El alert protocol gestiona la sesión SSL, los mensajes de error y las advertencias. (Granda, 2017, p. 24)

2.3.4. Comunicación SSL

Con el uso del protocolo SSL se establece una comunicación muy segura con los siguientes pasos:

1. Se realiza una solicitud de seguridad (SSL Handshake), donde se establecen los parámetros.
2. Se estable la comunicación segura y verificación periódicas se garantiza que la comunicación es segura para la transmisión de la información y datos.
3. Después de completar la transacción, se termina la comunicación SSL. (Grandaine, 2017, p. 24)

2.3.5. Funcionamiento de SSL

Este protocolo se introduce como una capa adicional en el modelo jerárquico OSI, ocupando un espacio entre la capa de aplicación y de transporte de manera independiente. Esto quiere decir que se utiliza para la encriptación de información entre navegador y servidor web, y la encriptación de información de cualquier aplicación como IMAP, FTP, TELNET, etc. También utiliza algoritmos comprimidos de 214 bytes los mismos que solo se pueden ser reensamblados por el receptor. (Granda, 2017, p. 23 - 24)

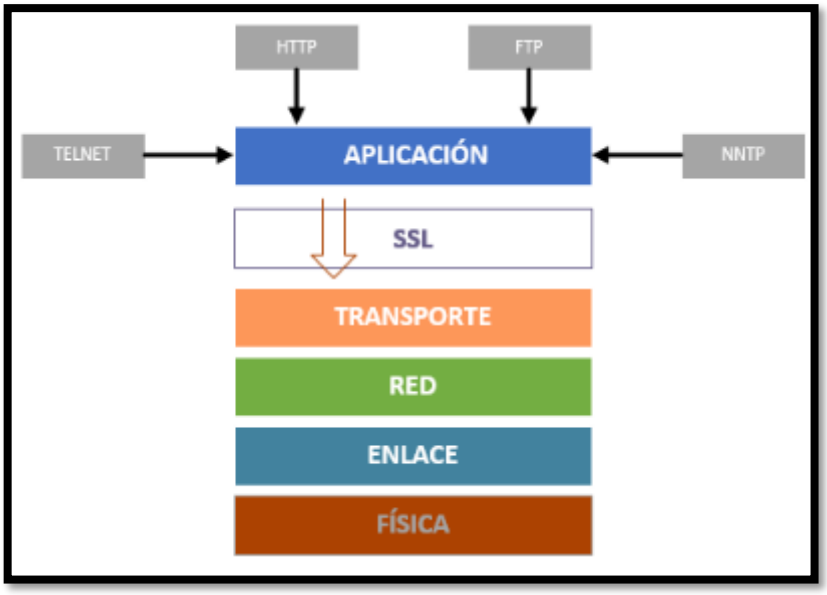


Figura 12-2: Protocolo SSL en OSI

Fuente: (Granda, p. 24)

El protocolo negocia entre el cliente y el servidor los algoritmos que se utilizarán en la comunicación como (3DES, IDEA, AES, RSA, DiffieHellman, DSA, SHA-2, etc.). Después realizará el intercambio de claves y la autenticación basada en certificados digitales, utilizando una validación mediante una infraestructura de clave pública PKI cuando es necesario, finalmente el cifrado del tráfico basado en criptografía simétrica genera una clave de sesión para la comunicación en función de los parámetros negociados. Esta clave facilitará el cifrado de los datos. (Alonso, 2013, p. 13 - 14)

La criptografía asimétrica sólo se utiliza en el intercambio de claves y en el firmado, después de concluir la negociación comienza la conexión segura. Esta negociación entre el cliente y el servidor está basa en el intercambio de mensajes, cada mensaje posee un campo (content_type) donde se especifica el protocolo de nivel superior utilizado. Estos mensajes pueden ser comprimidos, cifrados y empaquetados con un Message Authentication Code (MAC). (Alonso, 2013, p. 13 - 14)

2.3.5.1. Simmple Handshake

El servidor se autentica con entrega de su certificado y el cliente no:

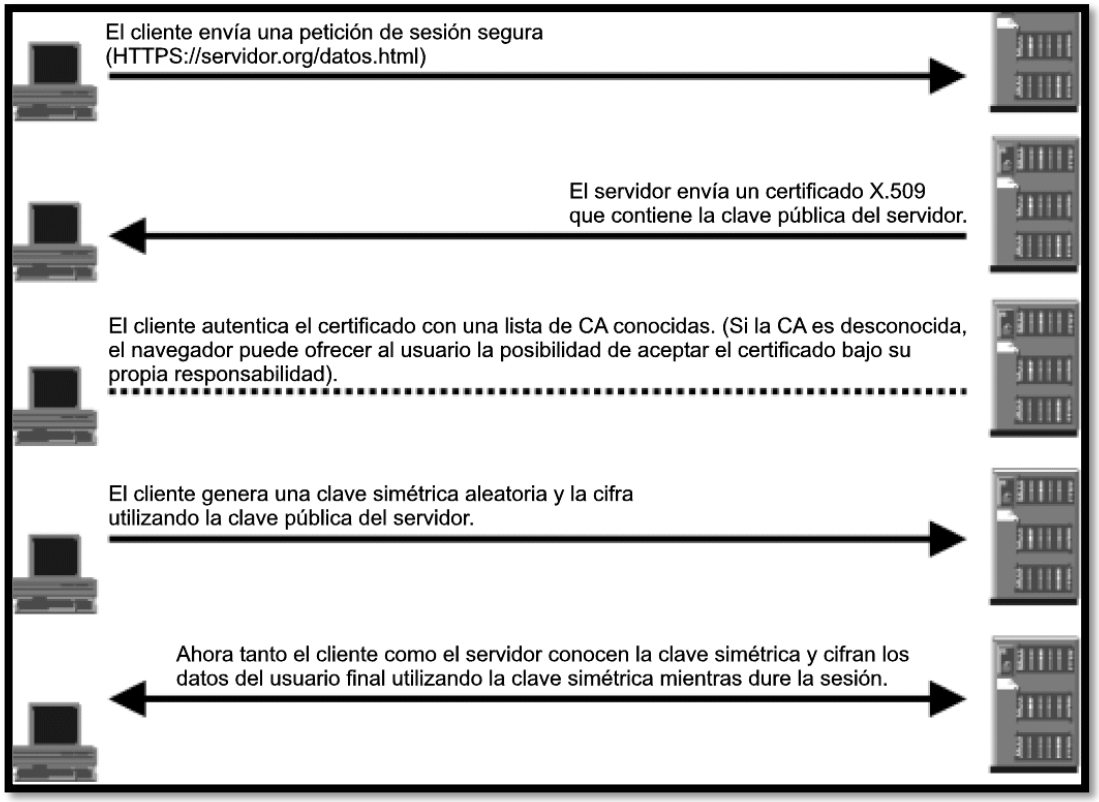


Figura 13-2: Funcionamiento SSL
Fuente: (Alonso, 2013, p. 13 - 14)

Pasos para el funcionamiento

- El cliente inicia la comunicación enviando un mensaje "Client Hello" donde especifica una lista de cifrados (Cipher Suites), métodos de compresión y la versión del protocolo SSL más alta permitida. También se envían bytes aleatorios que será usados más tarde (challege de Cliente). (Alonso, 2013, p. 13 - 14)

- El servidor responde con un mensaje "Server Hello" donde se indican los parámetros elegidos por el servidor a partir de las opciones ofertadas por el cliente. Se envía el ID de sesión, versión, compresión y un número aleatorio que se usará con el cliente en la creación de la clave simétrica.
- Una vez establecidos los parámetros de la conexión, el servidor ofrece su certificado (Normalmente X.509) a través de un mensaje llamado "Certificate" puede enviarse la clave pública o hacerlo en el paso siguiente. (Alonso, 2013, p. 13 - 14)
- Este mensaje se envía sólo si el anterior mensaje no incluye clave pública para el cifrado escogido, con este mensaje el servidor ofrece cifrado asimétrico entre cliente y servidor la clave pública firmada con la clave del Certificado. De esta forma se separa la autenticación (paso

anterior, certificate) del cifrado. Lo más común es que el Certificado sea un certificado de autenticación de servidor que incluya la clave pública de cifrado

- El servidor da por concluida su fase de negociación asimétrica. (Alonso, 2013, p. 13 - 14)
- El cliente tras haber comprobado y validado el certificado, genera el premaster secret que será el elemento secreto compartido que junto a otros datos intercambiados previamente darán lugar a un mismo master secret en la parte servidor y en el cliente y que será la clave simétrica utilizada para cifrar los datos. El premaster secret es cifrado con la clave pública del servidor y enviada. De este modo sabemos que solo el servidor legítimo puede descifrarlo y generar el master secret de la sesión.
- Con este mensaje el cliente informa que los sucesivos datos estarán cifrados con el cifrado acordado.
- El cliente da por finalizada su handshake. (Alonso, 2013, p. 13 - 14)
- El mensaje que finaliza el Handshake incluye un hash de todos los mensajes de handshake que garantiza la integridad de la comunicación.
- El servidor tras checkear que todo ha ido correctamente (en base al hashing MAC), descifra con su clave privada el premaster secret enviado por el cliente en el paso 6 y genera el master secret del mismo modo que el cliente. En este momento cliente y servidor han logrado establecer una clave simétrica y acordado un cifrado. Con este mensaje el servidor indica que sus mensajes desde este momento se cifran.
- El servidor finaliza el handshake. (Alonso, 2013, p. 14)

2.3.6. Aplicaciones de SSL

SSL fue diseñado para la protección de cualquier aplicación basada en protocolo de transporte como TCP, algunas de estas aplicaciones son:

- **HTTPS:** Es el protocolo más utilizado para la navegación web segura.
- **NNTPS:** Permite el acceso seguro al servicio de News. Utiliza puertos propios de TCP 443 para HTPPS y 563 para NNTPS. Para la utilización innecesarias de nuevos puertos se usan aplicaciones como:
- **TELNET:** usan la opción de autenticación (RFC 1416)
- **FTP:** usan las extensiones de seguridad (RFC 2228)
- **SMTP:** usa extensiones para SSL (RFC 2487)
- **PO3 e IMAP:** usa comandos específicos para SSL (RFC 2595) (Alonso, 2013, p. 15)

2.3.7. Ataques en SSL

Los protocolos SSL fueron diseñados para resistir los siguientes ataques:

- **Lectura de los paquetes enviados por el cliente y servidor. -** Utilizando el protocolo SSL los datos se envían cifrados por lo que un ataque de utilice sniffer para leer los paquetes se enfrentan al problema de romper el cifrado. (Alonso, 2013, p. 18)
- **Suplantación de servidor o cliente. –** Cuando se realiza la autenticación del servidor o cliente, el certificado digital debe estar firmado por la CA para verificar la identidad del propietario. Un posible ataque seria hacer que la CA firme un certificado no legítimo.
- **Alteración de los paquetes. –** Un ataque puede modificar los paquetes para que lleguen a su destino con un contenido diferente del original. Por lo general el receptor detectara que el paquete viene alterado ya que a MAC esta alterada. (Alonso, 2013, p. 18)
- **Repetición, eliminación de paquetes. -** Aunque un atacante intentara enviar un paquete correcto que ya fue enviado o eliminar algún paquete haciendo que no llegue a su destino por lo general será detectado por el receptor mediante los códigos MAC. (Alonso, 2013, p. 13 - 18)

2.3.8. Criptografía en SSL

SSL se basa en la implementación conjunta de dos criptografías, simétrica y asimétrica, certificados y firmas digitales para establecer un medio seguro de comunicación mediante el internet.

Tabla 5-2: Clases de Criptografía

Clases	Detalles
Criptografía Simétrica	Es el motor principal para la encriptación de información aprovechando la rapidez operacional, adicionando códigos de autenticación de mensajes garantizando la integridad de los datos.
Criptografía Asimétrica	Es usada para intercambiar claves simétricas de manera segura para la confidencialidad en el transporte de información.
Criptografía de llaves publicas	Se crean dos llaves únicas repartidas entre cada participante del transporte de información, funcionando de manera dual, la una clave cierra la información mientras que la otra clave abre, de esta manera cualquier extraño que intente acceder a la información no podrá hacerlo porque no posee la clave de desencriptación.
Certificado Digital	Este documento es publicado y concedido por un Autoridad de Certificación (CA), este incluye información clave de individuo o compañía

	solicitante del documento como ejemplo: nombre de la compañía, clave pública, número de serie, fecha de expiración, firma de la CA y cualquier información que sea solicitada.

Fuente: (Granda, 2017, p. 40)

2.3.9. Versiones del protocolo SSL

Tabla 6-2: Versiones del Protocolo SSL

Versión	Descripción	Soporte para el Navegador
SSL v2.0	Primer protocolo SSL para el cual existen implementaciones	○ NS Navigator 1.x/2.x ○ MS IE 3.x ○ Lynx/2.8+OpenSSL
SSL v3.0	Revisiones preventivas para ataques específicos a la seguridad, añade encriptadores no-RSA y soporte para series de certificados.	○ NSnavigator 2.x/3.x/4.x/5.x/6.x/7.x ○ MS IE 3.x/4.x/5.x/6.x ○ Lynx/2.8+OpenSSL
TLS v1.0	Revisión del SSL 3,.0 que se hace desde la capa MAC hasta la capa HMC, añade bloques de relleno para los encriptadores de bloques, estandarizaciones de mensajes y con más mensajes de alerta.	○ Lynx/2.8+OpenSSL

Fuente: (Caisaguano, 2003, p. 24)

2.4. Herramientas open source para SSL

2.4.1. Definición de Open Source

Open Source o código abierto es el software desarrollado y distribuido de manera libre, que permite crear software de alta calidad para el propietario; es importante diferencia el código fuente del código libre que se distribuye libremente.(Velasco, 2017, p. 8)

Este tipo de herramientas son muy recomendadas y de más preferidas en lugar que una de propietario, ya que tienen detrás a una gran comunidad de desarrolladores brindando su apoyo indicando que son seguros y estables, incluso estos desarrolladores a su vez trabajan para brindar mejoras a las herramientas libres. (Granda, 2017, p. 41)

Una herramienta open source permite hacer uso de ella de 4 maneras:

- Permite usar el programa, con cualquier propósito.
- Posee una libertad de estudio del funcionamiento del programa, y adaptarlo a las necesidades. El acceso al código fuente es una condición previa para esto. (Granda Katherine del Pilar, 2017, p. 42)
- Se puede distribuir copia, con lo que puedes ayudar a tu vecino.
- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. El acceso al código fuente es un requerimiento previo para esto. (Granda Katherine del Pilar, 2017, p. 42)

2.4.1.1. Tipos de Software

Existen diferentes tipos de software Open Source:

- Sistemas Operativos
- Antivirus
- Herramientas Ofimáticas
- Lenguaje de Programación
- Navegadores Web
- Clientes de Correo Electrónico
- Sistemas de Monitoreo de Redes

2.4.2. Características de la Herramienta de Open Source

De acuerdo a diferentes autores la herramienta Open Source poseen las siguientes características:

- **Flexibilidad:** Por tener su código fuente disponible los desarrolladores pueden aprender, modificar los diferentes programas a su manera y realizar tareas específicas, permitiendo mejorar la calidad del programa. (Armijos Christian, 2015, p. 21)
- **Fiabilidad y Seguridad:** Cuando varios programadores están al mismo tiempo mirando se detectan errores que se corrigen con anterioridad, por lo que el producto es confiable y efectivo.
- **Rapidez de Desarrollo**: Las actualizaciones y ajusten se llevan a cabo por medio de una comunicación constante mediante el internet.
- **Relación con el usuario:** De acuerdo con los usuarios se puede definir las necesidades y por consecuencia crear un producto específico para cada uno de ellos. (Armijos, 2015, p. 21)

2.4.3. Herramientas Open Spurce

- E-commerce
- CMS
- Sistemas de Tickets
- Sistema Colaborativo
- Sistema de Inventario

2.4.3.1. E-commerce o Comercio Electrónico

Permite qué los clientes accedan de manera simple y desde cualquier parte del mundo a los productos, servicios que ofrece una empresa. Este ofrece la distribución, venta, compra, marketing de la información de productos o servicios mediante la internet. (Armijos, 2015, p. 21)

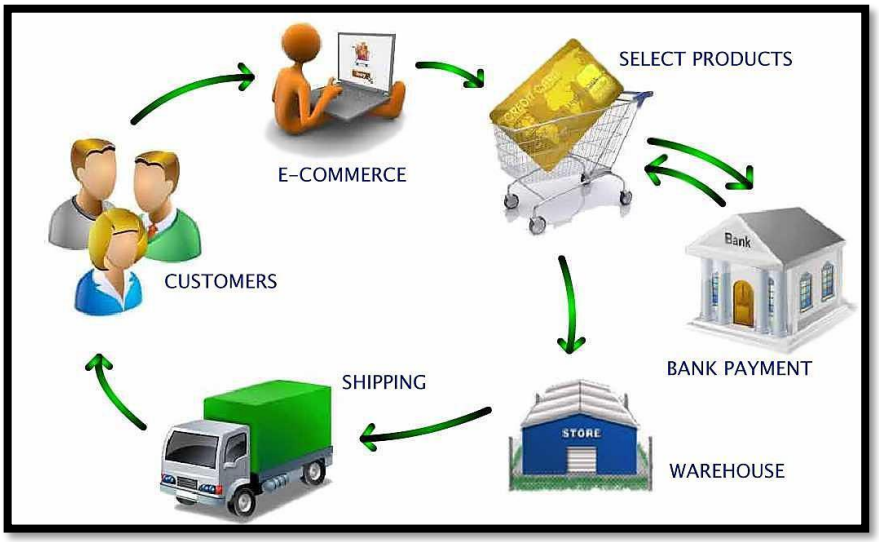


Figura 14-2: Comercio Electrónico

Fuente: (Armijos, 2015, p. 21)

Tipos de Comercio Electrónico

- B2C (Business-to-Consumer): Empresas que venden al público en general.
- B2B (Business-to-Business): Empresas haciendo negocio entre ellas
- B2G (Business-to-Government): Empresas que venden a instituciones de gobierno
- C2C (Consumer-to-Consumer): Plataforma de la cual los consumidores compran y venden entre ellos. (Armijos, 2015, p. 21)

Ventajas del Comercio Electrónico

- Expandir la base de clientes al entrar al mercado más amplio
- Horario de venta las 24 horas del día, los siete días de la semana, 365 días del año.
- Crear ventajas competitivas
- Reducir costos de producción, capital, administración.
- Mejora la comunicación entre clientes con efectivas campañas publicitarias. (Armijos, 2015, p. 22 - 23)

Implementación de un E-commerce

Tabla 7-2: Factores que se aplican para el desarrollo de E.commerce

Factores	Detalles
Fullfilment/ Distribución	Se realiza las consultas, ordenes, empaquetados, preparación para la distribución, asignación de ordenes de compras, manejo de almacén, actualización y manejo de inventario.
Merchandising	Aquí se hace la actualización de catálogos, precios, promociones y paquetes.
Comercial/ Marketing	Se realiza un análisis de la información de los clientes para mantener una comunicación personalizada, desarrollo de políticas, lineamiento para ventas, promociones, descuentos, devoluciones, etc.
Estrategia	Se desarrolla la estrategia general del negocio, lineamientos de negocio y oferta de valor al cliente; también permite definir mercados para ser abordados.
Finanzas	Se realiza los reportes de ventas, devoluciones, cancelaciones, cierres diarios, semanales, mensuales y cancelaciones. También se hace los informes trimestrales y anuales.
Tecnologías Informáticas	Se realiza la evaluación y selección de la plataforma, mantenimiento, actualización de la información, ver el correcto funcionamiento de la plataforma.
Atención al Cliente	Se atienden las solicitudes, quejas, dudas, reclamos que realizan los clientes.

Fuente: (Armijos, 2015, p. 23)

2.4.3.2. CMS (Content Management Systems)

Sistemas de gestión de contenidos es un software que se usa para facilitar la gestión de webs en la internet o intranet. Algunos usuarios utilizan CMS para la elaboración y gestión de sus webs personales para una mejor dinámica, este resultado es mejor comparado con las webs que poseen las empresas las que poseen paginas estáticas que no aportan ningún valor añadido. (Armijos, 2015, p. 24)

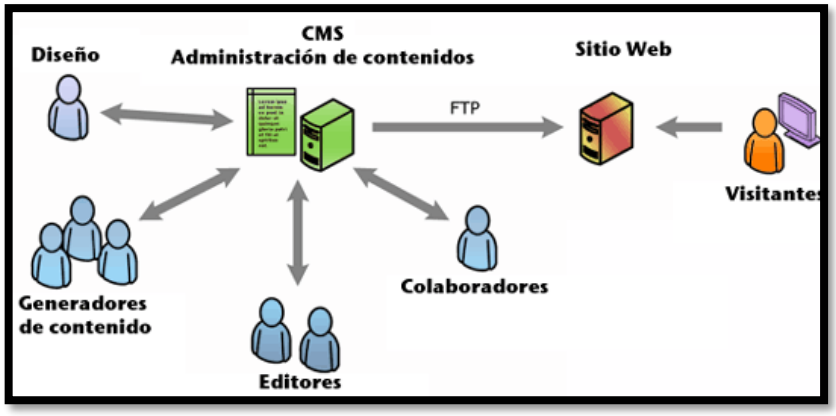


Figura 15-2: Sistema de Gestión de Contenidos

Fuente: (Armijos, 2015, p. 21)

Herramientas de un CMS

Wordpress: permite a creación de blogs en PHP y de manera gratuita.

Mambo: esta creado en PHP muy fácil de utilizar, tiene características como editores de contenidos WYSIWYG, noticias, banners, administración de enlaces, estadísticas, contenido de base de datos, 2º idiomas, módulos, componentes, etc.

Typo3: es de uso profesional muy fácil de usar, poseen características como editores de contenido WYSIWYG, noticias, banners, administración de enlaces, estadísticas, archivo de contenidos, 20 idiomas, módulos, componentes, etc.

Joomla: esta creado en PHP, es una mejora de Mambo. (Armijos, 2015, p. 27)

Ventajas de CMS

Tabla 8-2: Ventajas de CMS

Factores	Detalles
Nuevas funciones en la Web	Permite la revisión de millones de páginas y la generación del código. El sistema puede crecer y adaptarse a las necesidades futuras.
Mantenimiento de Páginas	Permite hacer la distribución de trabajos de creación, edición y mantenimiento con permisos de acceso a diferentes áreas. Se hace las gestiones de los metadatos de cada documento.
Reutilización de objetos	Permite la recuperación y reutilización de páginas, documentos de cualquier objeto publicado.

Páginas Interactivas	Las páginas dinámicas se generan según las peticiones de cada usuario.
Control de Acceso	Controlar el acceso no solo consiste en permitir la entrada a la web, sino se debe gestionar los diferentes permisos para cada área de la web de manera individual o grupal.

Fuente: (Armijos, 2015, p. 27)

2.4.3.3. Sistemas de Tickets

Un ticket es un tipo de consulta, sugerencia, mejoras al producto adquirido, reclamos, pedidos, asesoramiento que el usuario solicita esta comunicación se hace cliente - administrador.

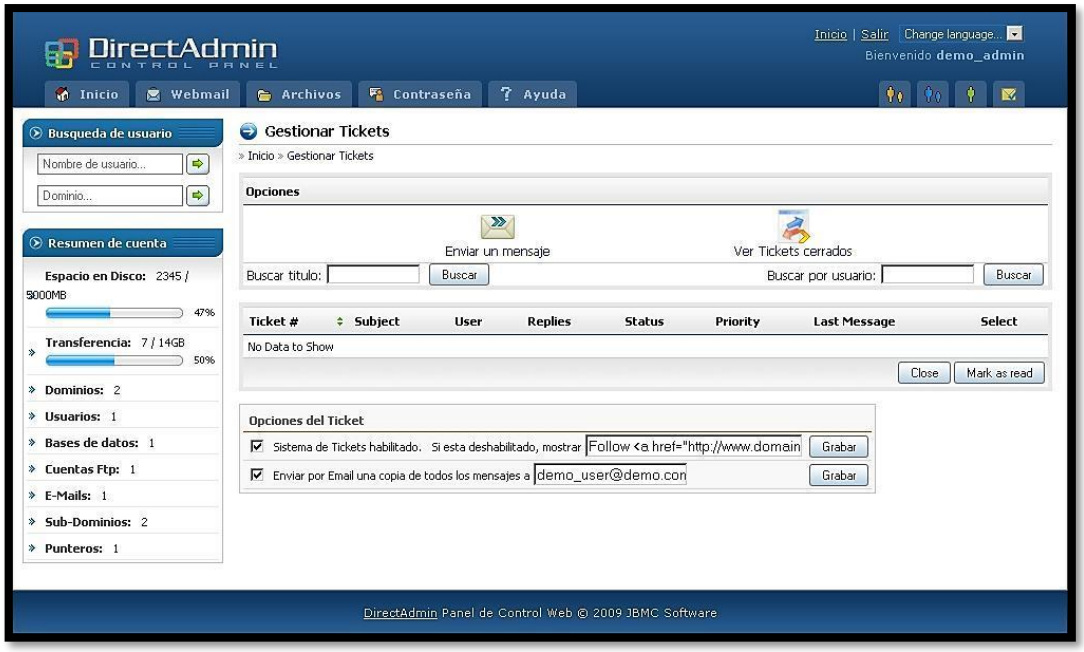


Figura 16-2: Sistema de Ticket
Fuente: (Armijos,2015, p. 28)

Beneficios del Sistema de Ticket

Solicita y registra tickets (pedidos) en cualquier momento

Mediante este sistema el cliente estará informado de las fechas que debe realizar los abonos mensuales de los productos adquiridos. (Armijos, 2015, p. 29)

Posee una herramienta de ayuda que le permite encontrar respuesta a una variedad de consultas.

Permite acceder a preguntas frecuentes con las cuales podrá solucionar los problemas que enfrentan los usuarios. (Armijos, 2015, p. 29)

2.4.3.4. Sistema Colaborativo

Son sistemas que soportan grupos de personas involucradas en una tarea común con un interfaz y aplicaciones corporativas; permitiendo que compartan los diferentes recursos como documentos, hojas de cálculo, y toda la información que el cliente necesite o que se quiera publicar en la Web. (Armijos, 2015, p. 29)

Las características más importantes son:

- Posee un ambiente de colaboración donde se percibe el trabajo grupal se lleva a cabo.
- Mantiene la información en un solo sitio común para todos los miembros.
- Interactuar con otros usuarios, de forma escrita, voz o video. (Armijos, 2015, p. 30- 31)

Los sistemas de colaboración nacieron de la necesidad de realizar actividades que requieren trabajar en grupo. Es así como se crearon softwares orientados a la colaboración, los Groupware y Workflow.

Groupware

Este sistema permite que un grupo de personas trabajen en conjunto en una tarea definida, su característica principal es un ambiente de colaboración, con la información en un solo lugar, y que se pueda interactuar con los usuarios. (Armijos, 2015, p.32)
Pueden ser sincrónico, es decir que se envían mensajes en tiempo real, como en sesiones de chat o pizarras compartidas, o de manera asíncrona, como es el caso de los blogs y correos electrónicos.

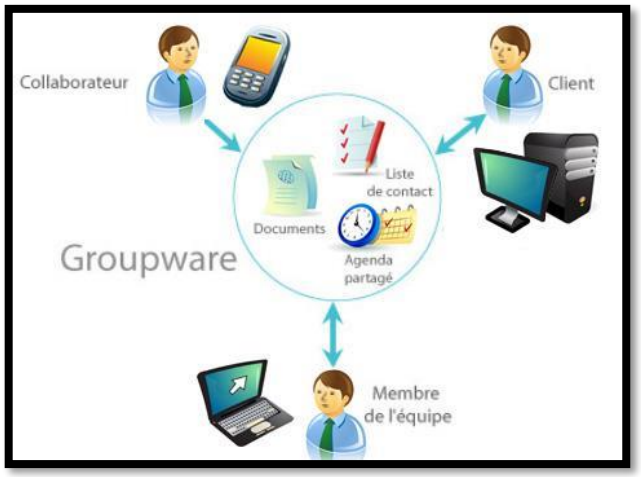


Figura 17-2: Groupware
Fuente: (Armijos, 2015, p. 32)

Workflow

Son sistemas que automatizan e integran los procesos de negocios de una empresa, de acuerdo a determinadas estrategia; una de sus actividades puede ser asignar tareas, avisar de tareas pendientes, automatizar secuencias de negocios y optimizarlas, entre otras. (Armijos, 2015, p. 33)

La principal diferencia de un workflow de un groupware es que el primero no necesariamente implica colaboración de otras personas, sino que se puede utilizar de forma individual.

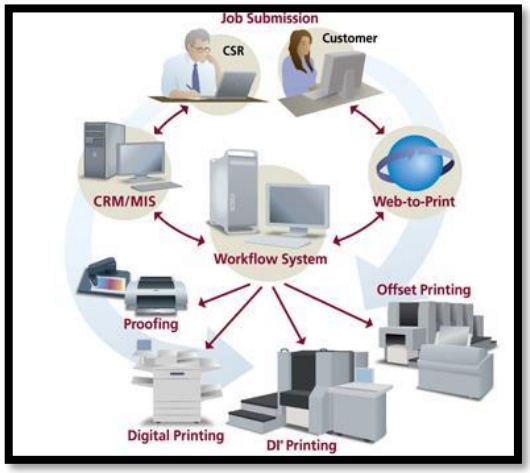


Figura 18-2: WORKFLOW
Fuente: (Armijos, 2015, p. 33)

2.4.3.5. Sistema de Inventarios

Existe un conjunto de herramientas gratuitas que permiten tener un inventario exhaustivo de los componentes del ordenador (procesador, RAM, disco, etc.) y programas (licencias, etc.) instalados en los ordenadores de la red, en Linux o Windows. (Armijos, 2015, p. 33)

- OCS Inventory (Open Computer and Software Inventory)
- GLPI (Gestión Libre de Parque Informático)

OCS (Open Computer and Software Inventory)

Es una herramienta multiplataforma que permite realizar inventario de los equipos de una red, permitiendo recolectar la información diariamente de los recursos de hardware y tiene una aplicación cliente - servidor, soportando casi todas las plataformas disponibles en el mercado, tales como Linux, Windows, Mac os, Sun, IBM, AIX. (Armijos, 2015, p. 34)

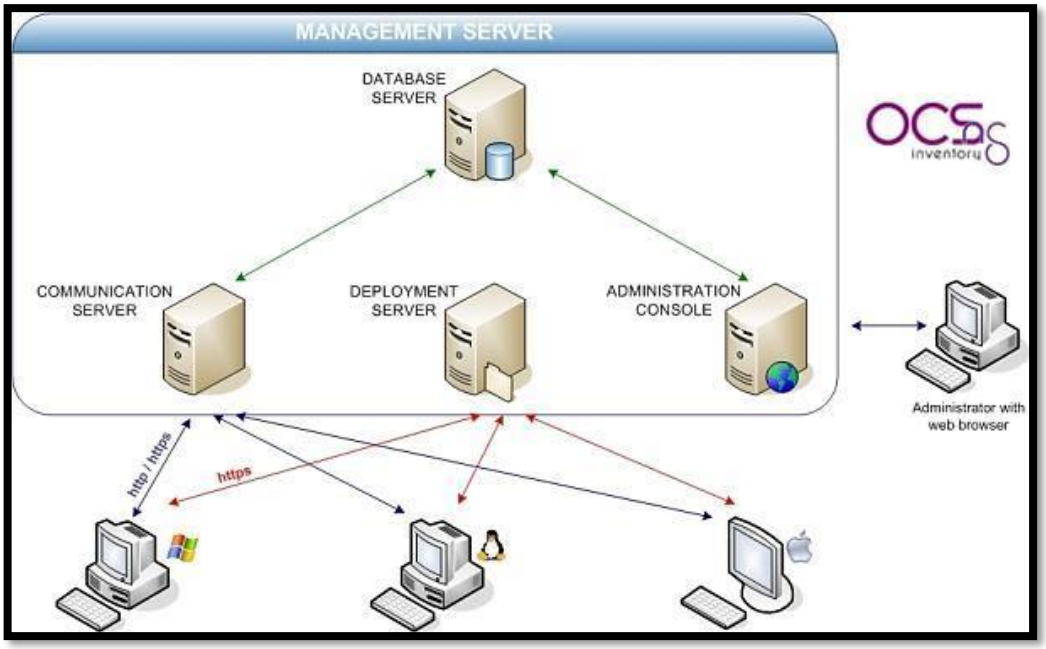


Figura 19-2: Arquitectura de Comunicación OCS
Fuente: (Armijos, 2015, p. 34)

Características de OCS

- Posee filtro de búsqueda: por cantidad de memoria, sistemas operativos.
- Ingreso de campos personalizados
- Organización de los datos por los campos definidos
- Son compatibles con GLPI para inventarios automatizados. (Armijos, 2015, p. 34)

Elementos de OCS

- Servidor de base de datos: Aquí se guarda toda la información del inventario y soporta MySQL 4.1.
- Servidor de Comunicaciones: Se encarga de la comunicación HTTP del servidor con los agentes. (Armijos, 2015, p. 35)
- Consola Administrativa: Permite a los administradores consultar la base de datos del servidor utilizando un navegador favorito.
- Servidor de Despliegue: Almacena toda la información de implementación de paquetes.

Funcionamiento de OCS

Este se basa en los estándares vigentes, diálogos entre equipos clientes – servidor basados en HTTP y con formatos XML. (Armijos, 2015, p. 35)

El servidor utiliza Apache, MySQL y Perl; es una multiplataforma y su rendimiento es muy bueno.

- GNU/ Linux (Ubuntu, Debian, Suse, RedHat, Gentoo, Knoppix, Slackware, Mandriva, Fedora y Centos).
- Windows (95, 98 NT4, 2000, XP, Server 2003, Vista, 7).
- Mac OS X. (Armijos Christian, 2015, p. 35)

Interfaz de Web está escrita en PHP ofreciendo los siguientes complementos:

- Consulta de Inventario
- Gestión de derechos de usuario
- Interfaz de desglose servicio (Help Desk)

GLPI (Gestión Libre de Parque Informático)

Permite la administración de recursos informáticos; esta aplicación está basada en Web escrita en PHP, que permite registrar y administrar los inventarios del hardware y el software de una empresa, optimizando el trabajo de los técnicos gracias a su diseño coherente. (Armijos, 2015, p. 36)
Las principales funciones de GLPI son:

- Inventario de los equipos: incluyen componentes de hardware como discos duros, y otros componentes de hardware.
- Inventario de periféricos: están asociados a los equipos, como monitores, ratones, teclados o altavoces, impresoras, etc.
- Inventario de red: donde se establecen todos los criterios de conexión de los equipos, IP, dirección MAC de la tarjeta de red, VLAN's configuradas. (Armijos, 2015, p. 36)

Ventajas de GLPI

- Reducción del esfuerzo en el mantenimiento de la información.
- Permite consultar mucha información del parque informático en un único repositorio.
- Tener una vista de la situación actual del inventario incluidas sus interconexiones. (Armijos, 2015, p. 36)

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Diseño de la investigación

Dada la naturaleza del estudio, este se define como Cuasi-Experimental, dado que el ambiente de pruebas, así como el tráfico a analizar, no son generados de manera aleatoria, sino previamente definidos por el investigador, además se manipula una variable independiente y evaluación de su correspondiente efecto en la variable dependiente.
Su validez se alcanza a medida que se logren capturar paquetes entendibles, así como estresar la red o sus miembros a niveles que los dejen inoperables, esto para medir la seguridad y el rendimiento correspondientemente.

3.2. Tipo de Investigación

En la investigación se considera que el tipo de estudio que se va a realizar es una investigación descriptiva y aplicada, dado que se realizará recolección de datos basados en el conocimiento previo para el levantamiento de la información relacionada a las vulnerabilidades explotadas por las diferentes herramientas.
Por la naturaleza investigativa y experimental del proceso se define a este estudio como un compendio de diferentes métodos y técnicas a través de las cuales se conseguirán tanto las bases teóricas de fundamento, así como las métricas de resultados.

3.2.1. Estudio Exploratorio

Los estudios exploratorios sirven para familiarizarse con fenómenos relativamente desconocidos, obtener información sobre la posibilidad de llevar a cabo una investigación más completa sobre un contexto particular, investigar problemas de comportamiento humano que consideren cruciales los profesionales de determinada área, identificar conceptos o variables promisorias, establecer prioridad para investigaciones futuras, o sugerir afirmaciones o postulados. Este tipo de estudio será fundamental en las fases iniciales del estudio, específicamente en el proceso de recolección de información y decisión de la herramienta Opensource a implementar.

3.2.2. Estudio Descriptivo

Así como los estudios exploratorios se interesan fundamentalmente en descubrir y prefigurar, los descriptivos se centran en recolectar datos que muestren un evento, una comunidad, un fenómeno, hecho, contexto o situación que ocurre (para los investigadores cuantitativos medir con la mayor precisión posible). Este estudio se utilizará específicamente en la fase de medición de características y resultados para la definición del prototipo.

3.3. Metodología de la investigación

Los métodos de investigación científica a utilizar siguen los siguientes pasos:

1. Consulta en base a documentos (Registros, Internet, bibliografía científica, investigaciones realizadas en el país y estadísticas oficiales).
2. Experimentación: Se recrearán distintas circunstancias en un ambiente controlado para la ejecución de pruebas, las cuales proveerán los resultados para la toma de decisiones y la definición del prototipo.
3. Análisis de la información.
4. Observación de campo: se harán distintas mediciones a los fenómenos recreados para la toma de decisiones.

3.3.1. Método Científico

Conocido como el método experimental de prueba y error, será de utilidad para la selección de herramientas como de configuraciones a implementar en el ambiente de pruebas, así como para la selección y uso de las herramientas de prueba de seguridad de la red. Se ha realizado las siguientes consideraciones para esta investigación:

- Se plantea el experimento en base a la existencia de 2 servidores para telepresencia implementados de manera diferente.
- Se orienta hacia el cumplimiento estricto de los objetivos para garantizar el alcance de la investigación.
- Se plantea una hipótesis relacionada y enfocada a la solución del problema.
- Se realiza la recolección de datos, y se observa el comportamiento del ambiente de pruebas en las condiciones iniciales.
- Se consultan las recomendaciones más actuales y confiables sobre mejores prácticas en redes para brindar mayor seguridad al prototipo.

- Se realiza la recolección de datos, y se observa el comportamiento del ambiente de pruebas en las condiciones mejoradas para comprobar que no se pierde rendimiento.
- Se realiza la prueba de la hipótesis con los resultados obtenidos.
- Se elaboran las conclusiones y recomendaciones, producto de la investigación realizada.

3.3.2. Método Hipotético – Deductivo

Debido a que se partirá del conocimiento general y los casos de prueba existentes para trabajar con nuestro caso de pruebas particular y específico, considerando que existe material suficiente sobre temas principales como la seguridad en redes y limitada información sobre los ataques a servidores de telepresencia

3.3.3. Método de Análisis y Síntesis

Este método será utilizado para la revisión del estado del arte de las redes para telepresencia, además para la toma de decisiones, así como la obtención de información sobre los datos medidos.

a) Fuentes

Dentro de las fuentes de obtención de información utilizadas en la presente investigación se mencionan:

Primaria:

Información original obtenida por el investigador en el ambiente de pruebas implantado, con el fin de contrastar la hipótesis.

Secundaria:

- Artículos publicados en revistas científicas.
- Trabajos de investigación publicados a nivel nacional e internacional con temas afines al investigado.
- Páginas de internet que brinden información confiable y especializada.
- Libros especializados en la biblioteca y electrónicos.
- Revistas electrónicas.

b) Técnicas e instrumentos de investigación

En el presente proyecto se utilizarán:

- Sniffing: wireshark
- Sniffing: Netcat
- Denegación de Servicios: Loiq

- Observación: ficha de observación

3.4. Recursos técnicos

Tabla 1-3: Recursos Técnicos

RECURSO	CARACTERÍSTICA	DESCRIPCIÓN
Servidor Virtual para Telepresencia	Procesador de 2 núcleos con 4 gb de RAM	Servidor Virtual dedicado a mantener el sistema de telepresencia sin SSL
Servidor Virtual para Telepresencia	Procesador de 2 núcleos con 4 gb de RAM	Servidor Virtual dedicado a mantener el sistema de telepresencia utilizando SSL
Router Huawei	Modelo hg8245	Router ADSL / Frontera
Router Mikrotik Home AP lite	Router mikrotik con herramientas para el monitoreo y pruebas de la red	Router utilizado para generar y medir información relacionada a las pruebas
Laptop DELL	Procesador Intel core I7 con 16 gb de Ram	Equipo destinado a ser el atacante, mediante el uso de máquinas virtuales se pretende incrementar la concurrencia
Debian 8	Versión de 64 bits con Escritorio de GNOME	Sistema Operativo Libre utilizado en los servidores virtuales
Wireshark	Versión 2.4.2 para Linux Ubuntu 64 bits	Analizador de Protocolos de Red
Linux Ubuntu 16.04	Versión 16.04 64 bits LTS	Sistema Operativo Libre utilizado en las máquinas atacantes, así como en el hospedero de las mismas
SNORT	IDPS para Centos 7	Sistema de Detención y Prevención de Intrusiones
VirtualBox	Versión 5.2 para Ubuntu 64bits	Software de Virtualización de Sistemas Operativos
Janus	Front End para uso del protocolo WEBRTC en comunicaciones	Base seleccionada como librerías para la creación de los ambientes de pruebas de las funcionalidades de WEBRTC orientadas a telepresencia

Fuente: (Peñafiel, 2019)

CAPÍTULO IV

4. PRUEBAS Y RESULTADOS

4.1. Desarrollo

Existen ataques que comprometen la integridad de la información, suplantación de identidad mediante un ataque de tipo hombre de en medio y de negación de servicios al descubrir la IP del servidor y el puerto, por lo cual se propone establecer un túnel entre cliente – servidor, a través del puerto 3306 o cualquier otro establecido para la interconexión.

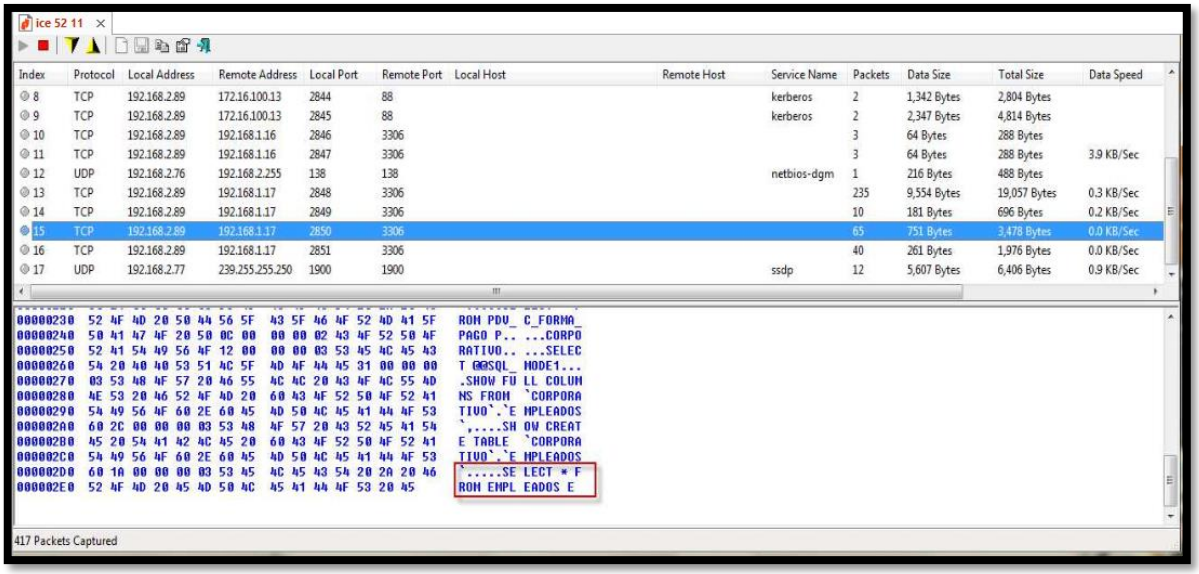


Figura 1-4: Puerto habilitado para la interconexión

Fuente: (Peñafiel, 2019)

El túnel se establece para la comunicación cliente – servidor por el puerto 3306, esto quiere decir que el túnel re direcciona el servicio en la configuración por default a un localhost, cuando se realeza la conexión, esto se realiza indicando el IP del servidor y el puerto.

En este punto se observa que se debe proponer políticas de seguridad, una de estas tiene que ver con el acceso que se puede restringir por IP o por segmentos de red, existe la configuración que acepte todo tipo de conexión, esto implica que mediante la configuración toda solicitud y respuesta viaja en texto plano. La implementación de los túneles tiene como objetivos establecer características de seguridad de acceso a los usuarios de manera remota en los equipos, además proporciona la característica de cifrar la información para que viaje por la red, esto agrega un tipo de seguridad.

Los túneles se establecieron utilizando protocolos SSH v2.0 y el SSL v2.0, la razón principal es que permite al tunneling cifrar la información, trabajar con TCP, la conexión para este proyecto se realizó mediante identificación de usuario y contraseña, permitiendo el uso de certificados digitales para evitar la intervención del usuario.

El funcionamiento es simple, para la comunicación se establece utilizando PortForwarding primero local y luego remoto esto quiere decir que el equipo cliente la conexión se realiza de forma local (localhost) por el puerto 3306. La respuesta tiene que ver con el re direccionamiento del servidor, esta característica es posible utilizar con los protocolos SSH y SSL.

Para establecer el túnel, primero se identifica los puertos, su funcionamiento es básico cuando se hace la petición por el puerto 3306, que esta redireccionado al puerto 22 para el protocolo SSL.

Una vez que la información fue re direccionada inician los mecanismos de autenticación y cifrado, una vez establecida la sesión, se cifra la información para que viaje por el túnel, cuando llega al equipo servidor, la información es descifrada y re enviada al puerto 3306 para que el servciio realice el procesamiento de la solicitud; de igual manera la respuesta de la solicitud es re direccionada al puerto, en donde será cifrada y enviada al cliente, esta secuencia se repite para cada solicitud.

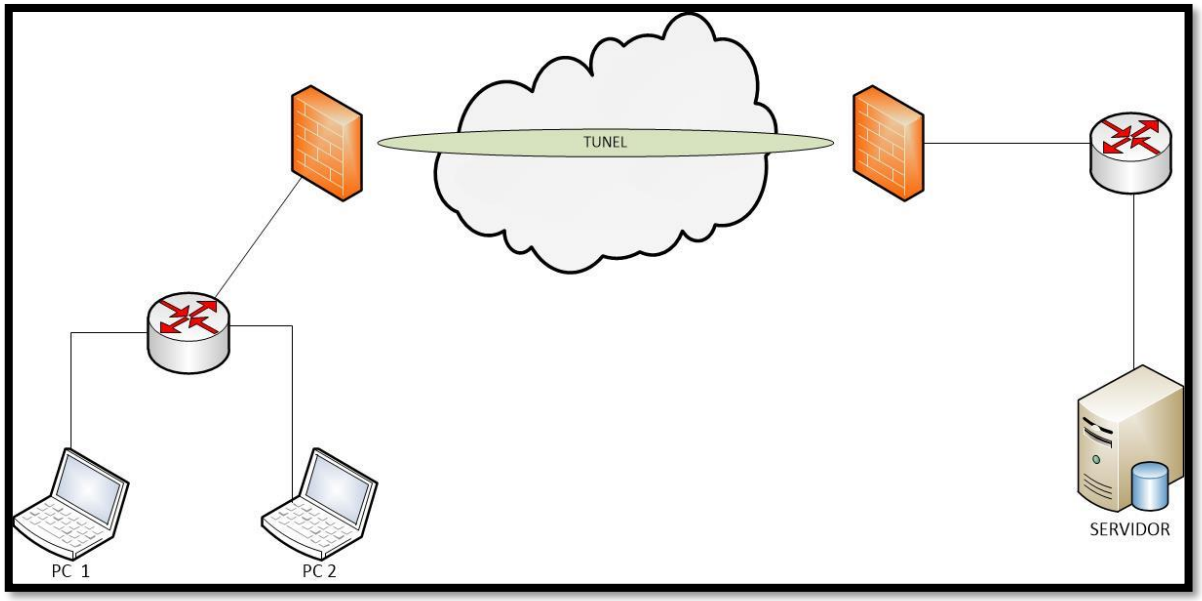


Figura 2-4: Escenario de Pruebas

Fuente: (Peñafiel, 2019)

Al tener los túneles se realizaron pruebas de petición al servidor, para la captura de datos en cada túnel y sin túnel con el fin de examinar la información, de esta manera se establece el escenario de pruebas para la obtención de datos que se van a examinar.

4.1.1. Túnel con SSL

La idea de crear un túnel es crear un envoltorio de datos o paquetes de un protocolo inseguro dentro de los paquetes de otro cifrado. Aquí se puede observar como stunnel es un envoltorio SSL que se utiliza para cubrir varias aplicaciones con estos túneles SSL cifrados.

Open SSL ha llevado a la creación de Stunnel una de las herramientas de seguridad más versátiles y útiles en el repertorio de software de código abierto, permitiendo hacer el cifrado de las conexiones enmascaramiento virtual de cualquier servicio de puerto simple TCP, esto refiere a los servicios que están escuchando las conexiones de un solo puerto sin utilizar puertos adicionales para otras funciones.

Stunnel se apoya en Open SSl para todas sus funciones de cifrado, por lo tanto, para utilizar Stunnel, primero se debe instalar Open SSL en cada Host donde se desee utilizarlo, para la implementación del túnel se lo hace con el protocolo SSL, se lo hace con la herramienta stunnel cuya distribución está disponible para las diferentes versiones de Windows y Linux; la configuración se la realiza en dos partes a una es el servidor y la otra el cliente.

4.1.1.1. Configuración del Servidor

Se debe recordar que el equipo servidor es un sistema Linux con una distribución Ubuntu 10.10, se debe de abrir una terminal para la instalación de stunnel4 ingresando el siguiente comando:

$ apt – get install stunnel

Después se debe otorgar permisos de lectura a stunnel.pem que es el certificado que se instala por default stunnel, que solo se recomienda para hacer pruebas y no se utilizara otro certificado.

/etc/ stunnel# apt-get install stunnel14

/etc/ stunnel# chmod 0400 stunnel14

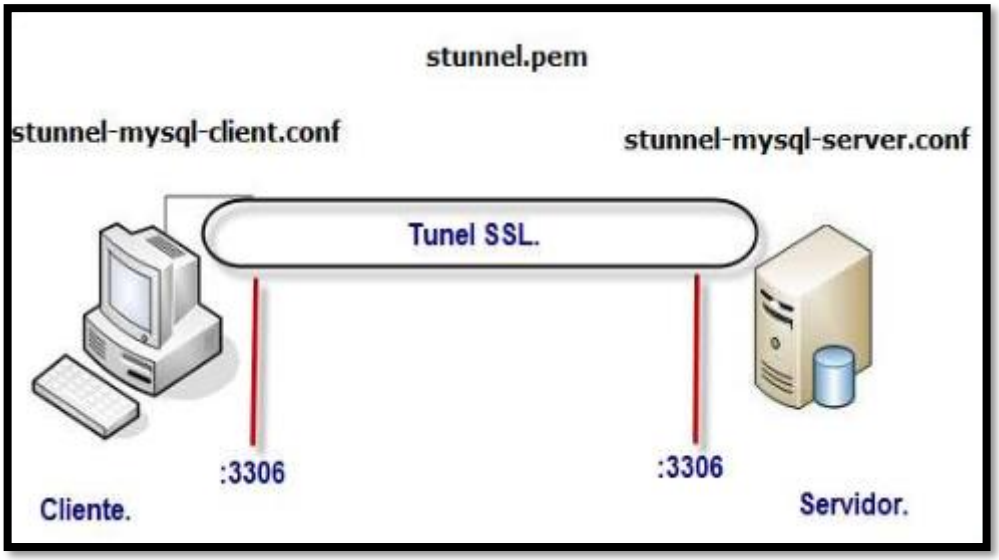


Figura 3-4: Esquema de la configuración para el túnel SSL

Fuente: (Peñafiel, 2019)

En las versiones de Stunnel (versiones 4) acepta todas las configuraciones desde la línea de comandos, utiliza un archivo de configuración, stunnel.conf, la localización de este archivo de configuración es lo único que se puede especificar con los parámetros del comando en línea, para lo cual se crea un archivo de configuración para iniciar el túnel:

vi stunnel – mysql – server. conf

dentro de este archivo, se debe especificar la ruta en donde se encuentra el certificado, además de establecer los puertos de conexión, para este trabajo se utiliza el certificado que instala por default el stunnel, este certificado lo recomiendan tan solo para realizar pruebas, razón por el cual lo utilizaremos, si se necesita mayor seguridad se debe utilizar un certificado más seguro, para fines prácticos y demostrativos no se detallan las características de este certificado, tan solo se utiliza los siguiente.

stunnel – mysql – server.conf

cert = / etc / stunnel / stunnel.pem

chroot = / var / run / stunnel.pem/

pid = / stunnel.pid

setuid = nobody

setgid = nobody

Para la configuración de los puertos en donde se va a establecer el túnel se utilizó el puerto 3307 local va a ver el lugar por donde se va a establecer el tunnel SSL, con esta configuración se coloca el puerto 3307 del servidor a la escucha, con lo cual toda solicitud que llegue a este puerto lo va a redireccionar al puerto 3306 del mismo equipo.

[mysql]

accept = 3307

connect = 127.0.0.1:3306

Con esto se finaliza la configuración del archivo para establecer de túnel del lado del servidor quedando con la siguiente estructura.

stunnel – mysql – server.conf

cert = / etc / stunnel / stunel.pem

chroot = / var / run / stunnel4/

pid = / stunnel.pid

#setuid = nobody

#setgid = nobody

[mysql]

accept = 3307

connect = 127.0.0.1:3306

Luego se establecen los permisos para la ejecución al archivo de configuracion stunnel-mysql-server.conf

Establecer permisos: / etc / stunnel # chmod 755 stunnel-mysql-server.conf

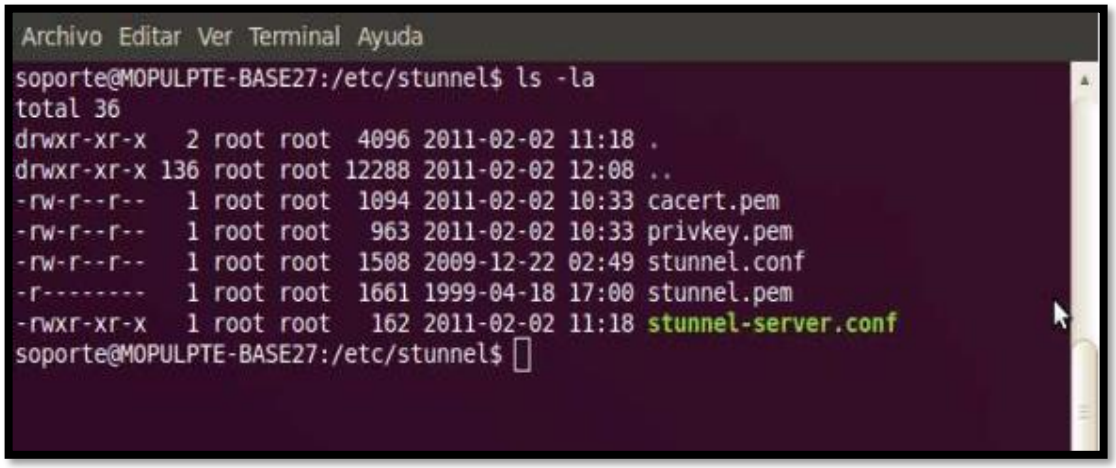


Figura 4-4: Stunnel-server-conf
Fuente: (Peñafiel, 2019)

Para realizar una verificación al archivo de configuración creado, hay que ejecutar el stunnel, pasando como argumento el archivo de configuración, si todo está bien no indica error, de forma contraria se debe analizar la alerta para encontrar el error.

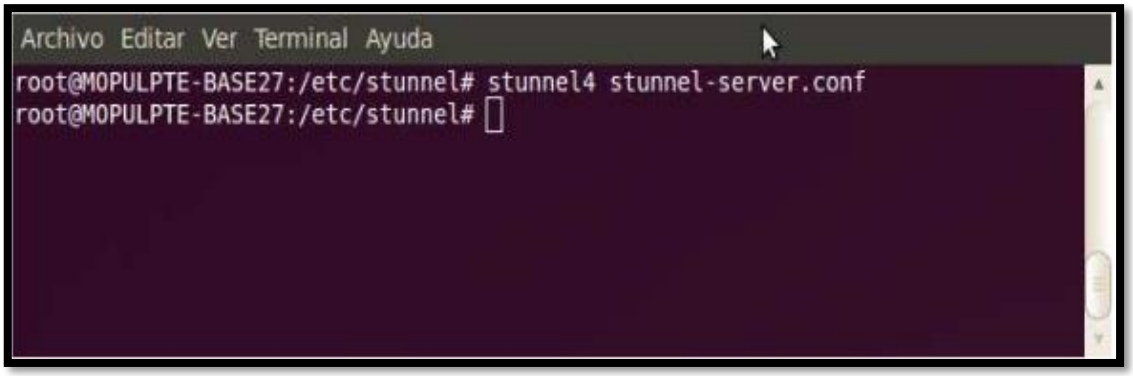


Figura 5-4: Establecimiento del túnel SSL
Realizado por: (Peñafiel, 2019)

Se verifica que el puerto configurado en este caso el 3307, que escucha las solicitudes, este paso es necesario realizarlo para verificar que el puerto está abierto a la espera de peticiones, si no se realiza este proceso, al tratar de establecer el túnel, no se podrá asegurar que la conexión se realice con éxito, si indicara un error y no se realizó la verificación del puerto, será más fácil deducir el origen del error como se muestra en la figura y para verificar la conexión se ejecuta la siguiente instrucción:

/ etc / stunnel # netstat – pln grep: 3307

La salida debe de mandar algo similar:

tcp 0 0.0.0.0:3307 0.0.0.0: listen 2847/ stunnel4

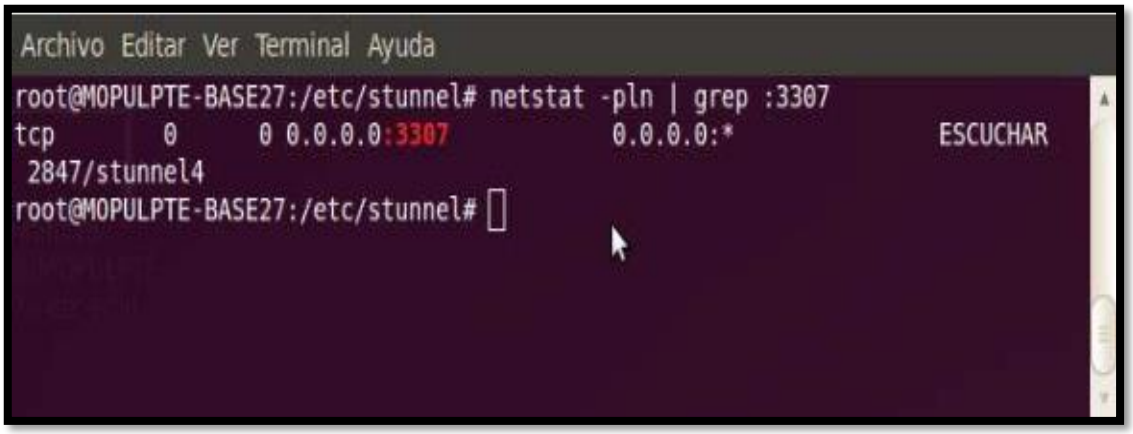


Figura 6-4: Comprobación de puerto en equipo Servidor
Fuente: (Peñafiel, 2019)

Con esta verificación se concluye la configuración de stunnel del lado del servidor.

4.1.2. Configuración en el Cliente

La configuración para el cliente se la hizo de la siguiente manera; se instalo el stunnel en su versión para Windows, agregando las librerías (libeay32.dl, libssl32) en la carpeta en donde se instaló el stunnel.

Instalar el: stunnel-4.34-installer.exe

Agregar a la carpeta de stunnel (C:\ Program Files\ stunnel) las siguientes librerias dll

- Libeay32.dll
- Libssl32

Ahora se crea un archivo de configuración, para establecer el túnel, tomando la estructura del archivo por default que instala el stunnel, el punto importante aquí es:

[mysql]

Accept = 127.0.0.1:3306

Connect = 192.168.2.163:3307

Aquí se indica que el servidor con la IP x.x.x.x que escucha el puerto 3307, va a ser la conexión para todas las peticiones que se realicen al localhost por el puerto 3306, de esta manera toda petición realizada a través del puerto 3306 del equipo local, será redireccionado al equipo remoto con IP x.x.x.x hacia el puerto local 3307. Así toda petición que se realice desde el equipo cliente al puerto local 3306 será dirigida a la dirección x.x.x.x por el puerto 3307, para de esta forma simular que la petición fue realizada de forma local.

De esta manera el archivo de configuración del lado del cliente queda con la siguiente estructura:

Stunnel – mysql – client.conf

Sample stunnel configuration file for securing Mysql (client side)

socket = r: TCP_NODELAY = 1

Provide the full path to your certificate – key pair file cert = stunnel.pem

lock the process into a chroot jail

chroot = / usr / local / var / run /stunnel /

and créate the PID file in this jail

pid = / stunnel.pid

change the IUD and GID of the process for security reasons

setuid = nobody

setgid = nobody

enable client mode

Client = yes

Configure our secured Mysql client

[mysql]

Accept = 127.0.0.1:3306

Connect = 192.168.2.163:3307

Para establecer el túnel se ejecuta el stunnel con archivo de configuración creado como argumento; iniciando el establecimiento del túnel de forma automática, la autenticación la realiza a través del certificado especificado en cada archivo de configuración, tanto del cliente como del servidor, para de esta forma establecer el túnel como se muestra en la figura:

Se ejecuta la instrucción en una consola ms – dos: stunnel.exe stunnel_mysql-client.conf

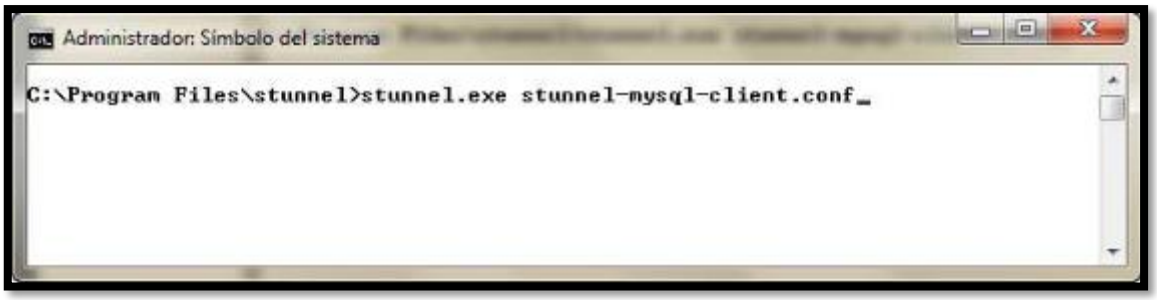


Figura 7-4: Establecimiento del túnel SSL en el cliente

Fuente: (Peñafiel, 2019)

Se verifica que se ejecute el servicio de stunnel debido a que, en el paso anterior, no se visualiza ningún mensaje a excepción de que haya ocurrido un error al establecer el túnel.

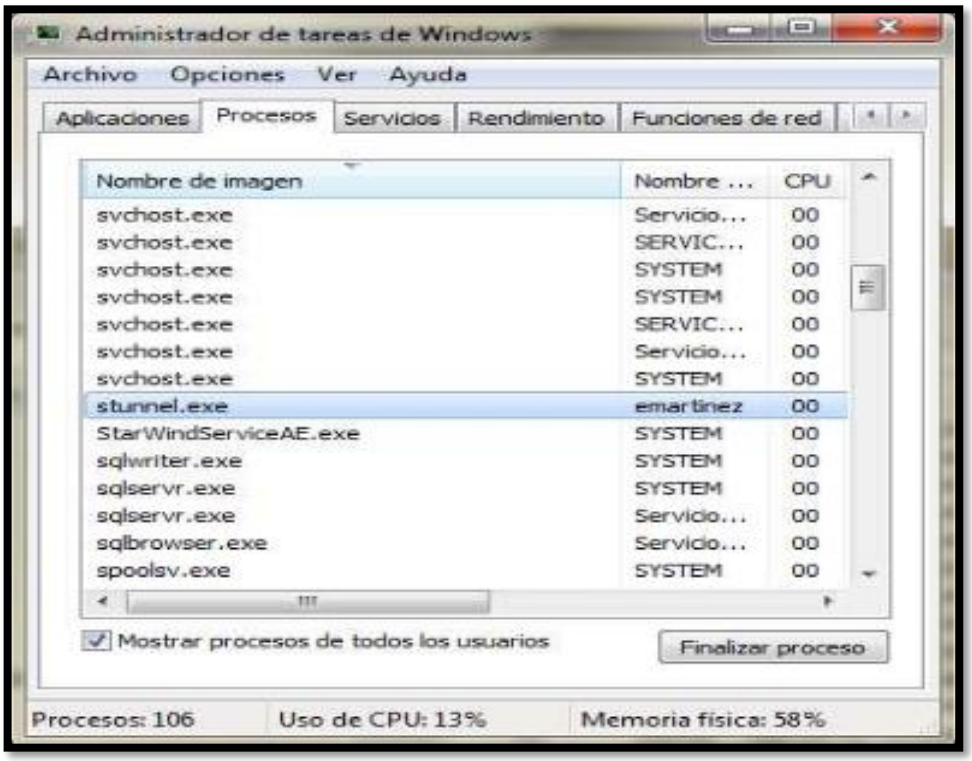


Figura 8-4: Verificación del servidor stunnel en el cliente

Fuente: (Peñafiel, 2019)

Se realiza un aprueba de conexión Telnet de forma local al puerto 3306, para verificar que la respuesta sea devuelta para el servidor de datos, que viajara por el túnel. La respuesta espera será el nombre predeterminado.

Figura 9-4: Prueba de Conexión del túnel SSL en el cliente
Fuente: (Peñafiel, 2019)

Si se establece la conexión, entonces el servidor envía su respuesta a la solicitud realizada.

Figura 10-4: Respuesta del servidor utilizando el túnel SSL en el cliente
Fuente: (Peñafiel, 2019)

Después de haber verificado la conexión se puede realizar una conexión al servidor por el puerto 3306 de forma local 127.0.0.1.

Figura 11-4: Establecimiento del túnel SSL en el cliente

Fuente: (Peñafiel, 2019)

Al entrar en el servidor de manera local se hace una consulta para que la solicitud y la respuesta viajen por el túnel SSL, y que estos datos estén cifrados, de esta manera el sistema posee una seguridad en la integridad de la información que viaja por el túnel.

Finalmente se ha establecido que el túnel SSL a través de la herramienta stunnek, la conexión se ha establecido, debido a que el archivo de configuración del cliente se indica que sea aceptado todas las conexiones solicitadas vía localhost al puerto 3306, esto puede generar un error en primera instancia.

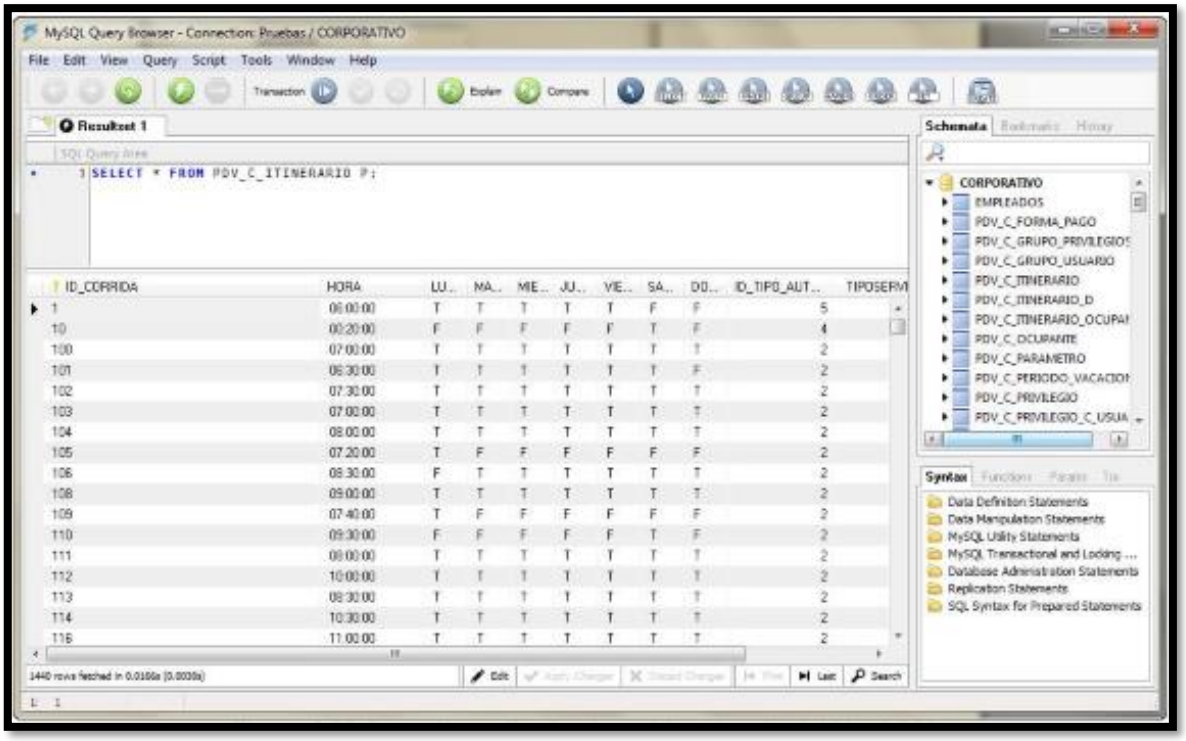


Figura 12-4: Consulta realizada al servidor a través del túnel SSL

Fuente: (Peñafiel, 2019)

Stunnel realiza un trabajo después de haber aceptado las solicitudes entonces establece una sesión con el servidor por el puerto 3307, aquí se realiza todo el mecanismo de autenticación utilizado por SSL, es decir, utiliza los protocolos de establecimiento de sesión, además valida el certificado utilizando una vez aceptados, entonces, la autenticación a finalizado, y con ello se inicia la sesión de SSL, mediante la cual viajara los datos de forma cifrada.

Del lado del servidor, la configuración establece el aceptado de lo que proviene del puerto 3307, y toda esta información una vez que ha llegado al servidor es descifrada, recordar que el cliente cifro los datos antes de enviarlos, entonces una vez que los descifro los redirecciona al puerto 3306, que es el servidor de datos, así que el servidor procesa la solicitud y se vuelve a realizar nuevamente el regreso de forma inversa, con esto la información viaja a través del túnel de forma cifrada y se ha establecido una conexión remota hacia un servidor.

Con el establecimiento del túnel la información ya no viaja en texto plano, y con ello está en funcionamiento en sistema de seguridad, que ayuda a la integridad de datos se mantengan y no sea expuesta a ataques, además la autenticación también se ve fortalecida. Lo primero se realiza la autenticación en el servidor con la diferencia de que ahora toda esta autenticación está cifrada.

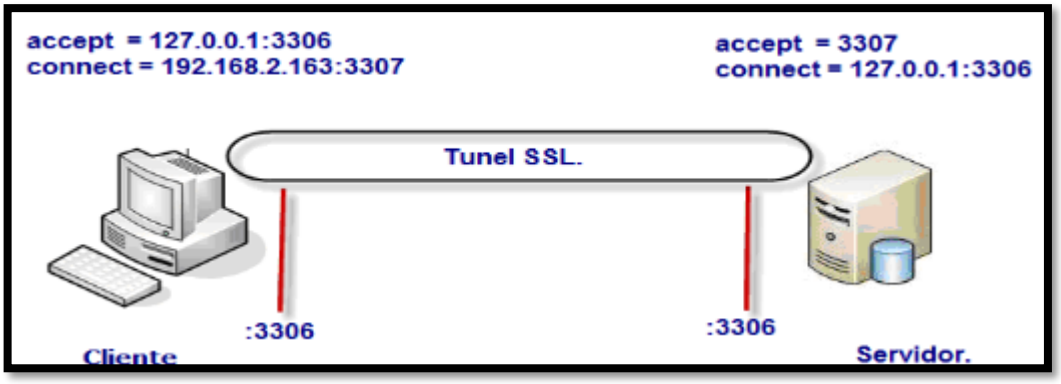


Figura 13-4: Escenario de prueba para el túnel SSL

Fuente: (Peñafiel, 2019)

De esta manera la información no es expuesta y menos puede ser interceptada para sufrir ataques, si en algún momento se pudiera obtener la información, está en primera instancia seria dirigida al servidor, entonces el que sufre las consecuencias es el sistema operativo. Con ellos se puede mantener la integridad hasta cierto punto la disponibilidad de la información.

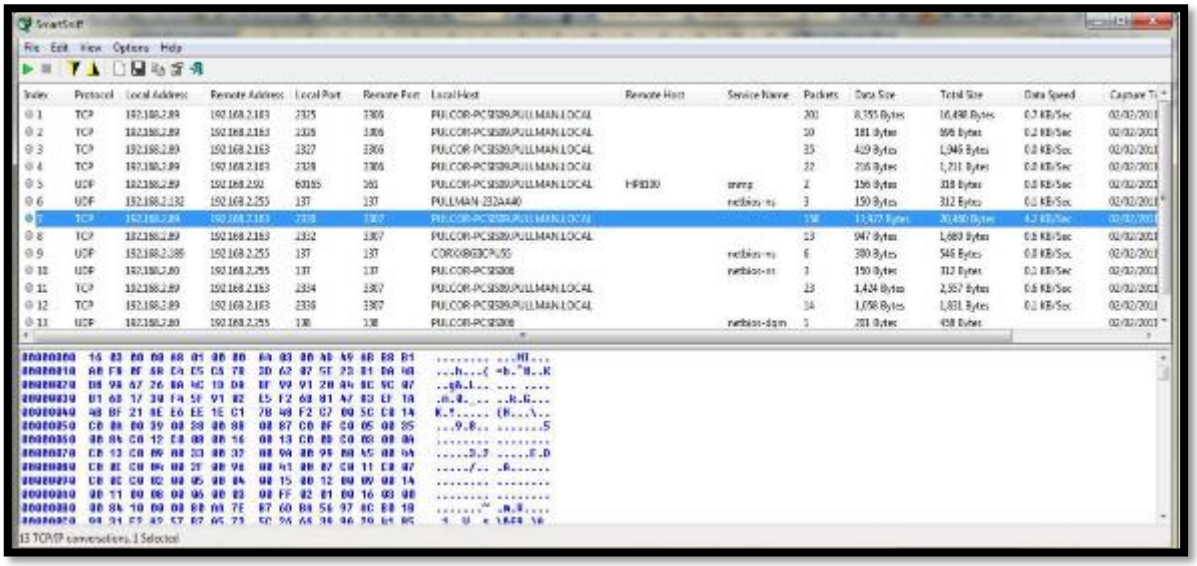


Figura 14-4: Captura de datos en el túnel SSL

Fuente: (Peñafiel, 2019)

El stunnel puede encapsular conexiones TCP de y hacia puertos arbitrarios entre un servidor y un cliente, se puede redirigir un puerto local a uno remoto en donde está corriendo el demonio stunnel al cual a su vez redirige ese puerto a uno estándar donde esta escuchado algún servicio.

Después de haber configurado el túnel para el protocolo se realizaron solicitudes de petición de información al servidor, para obtener un conjunto de datos necesarios para realizar la comparativa de características entre los túneles.

El tema de vulnerabilidad es importante porque no se puede crear un sistema de seguridad de la información, completamente seguro al grado de garantizar que el sistema y la gestión puntual de las políticas no va a sufrir algún ataque sin verse afectado. Para eso hay que detectar las vulnerabilidades de un sistema para poder minimizar el riesgo de un ataque que las consecuencias sean mínimas y aceptables.

La finalidad del establecimiento del túnel aumenta la seguridad para mantener la integridad de la información, sin dejar de lado que también poseen vulnerabilidades, pero el beneficio es mayor ya que la información no está a disposición de cualquier proceso que puede interceptar la comunicación, con esto se pretende minimizar el riesgo de ver comprometida la integridad y disponibilidad, y como ningún sistema es seguro se deben emplear protocolos para dar solución a esos inconvenientes.

Las pruebas contempladas, son un análisis de velocidad, una prueba para el rendimiento y finalmente exponer los casos de seguridad emitidos por un CERT en este caso el SSI (Subdirección de Seguridad de la Información) / UNAM-CERT de la Dirección – General de Computo y de Tecnologías de Información y Comunicación, UNAM.

Con los resultados de estas pruebas, se puede conocer el comportamiento que tiene cada túnel en relación a los tiempos de respuesta y el rendimiento del equipo al establecer los túneles, características que dan una idea general.

4.2. Velocidad

La prueba de velocidad, es solicitar información al servidor de datos, utilizando sentencias predeterminadas, que han sido obtenidas de procedimientos almacenados escritos para la base de datos que se está utilizando, en este punto el lector puede determinar sus propias sentencias para su base de datos, dejando axial, un análisis para medir el rendimiento de los túneles para una tarea definida.

La recopilación de la información se realizó de la siguiente forma se establece conexión con el servidor mediante el túnel, luego se hace las peticiones, esta consulta es ejecutada y muestra los resultados de la sentencia, esta herramienta despliega toda la información, así como los tiempos que han transcurrido al ejecutar la sentencia, estos tiempos de ejecución son los que se han utilizado como se muestra en la tabla

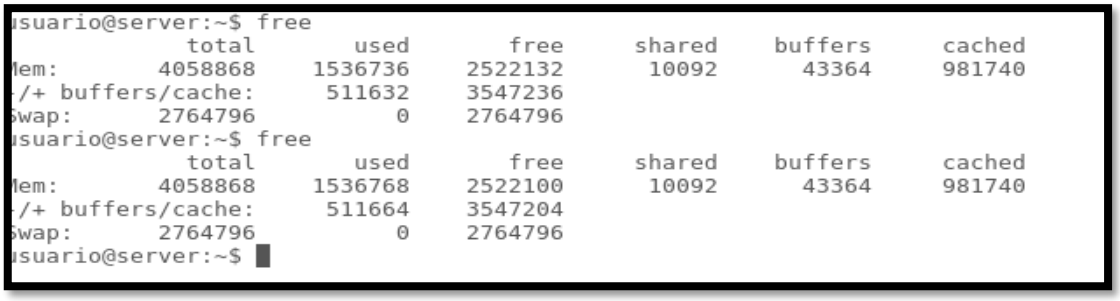


Figura 15-4: Captura de tiempo de respuesta sin túnel videoconferencia
Fuente: (Peñafiel Juan Gabriel, 2019)

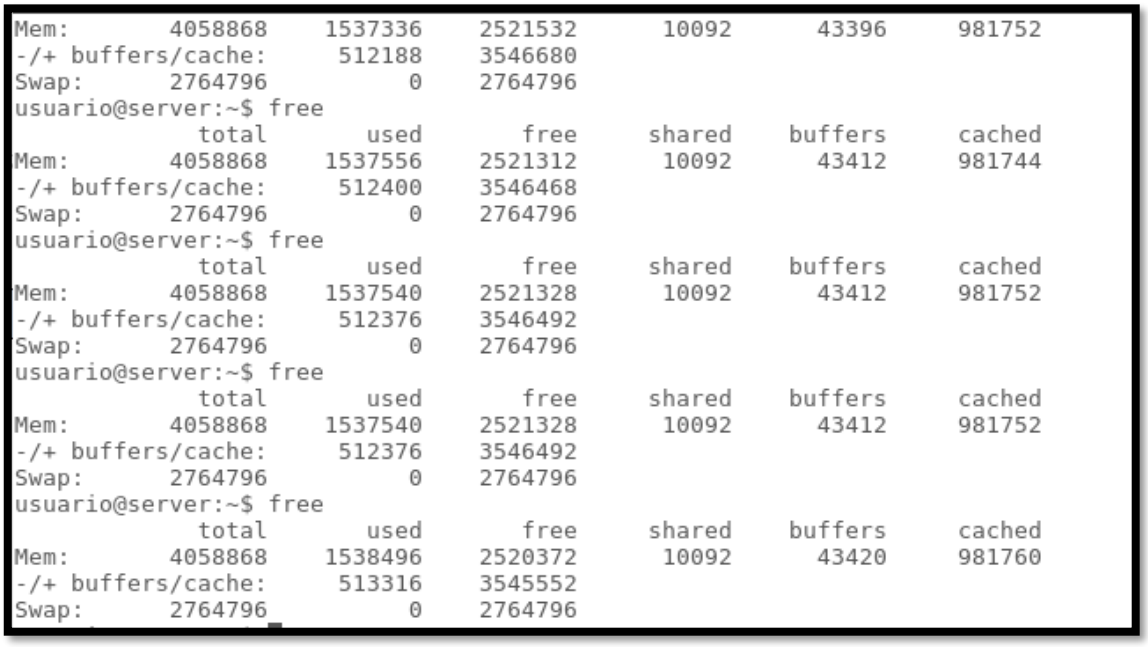


Figura 16-4: Captura del tiempo de respuesta con túnel SSL en video conferencia
Fuente: (Peñafiel, 2019)

Tabla 1-4: Resultados de las Peticiones al Servidor

	Sin Túnel	Túnel SSL
1	1051 rows fetched in 0.0147s	1051 rows fetched in 0.0137s
2	1578 rows fetched in 0.0056s	1578 rows fetched in 0.0057s
3	1623 rows fetched in 0.0075s	1623 rows fetched in 0.0077s
4	3001 rows fetched in 0.0213s	3001 rows fetched in 0.0221s
5	8068 rows fetched in 0.0218s	8068 rows fetched in 0.0258s
6	2015 rows fetched in 0.0063s	2015 rows fetched in 0.0067s
7	3043 rows fetched in 0.0093s	3043 rows fetched in 0.0097s
8	3580 rows fetched in 0.0131s	3580 rows fetched in 0.0138s
9	1 rows fetched in 0.0013s	1 rows fetched in 0.0012s
10	2015 rows fetched in 0.0064s	2015 rows fetched in 0.0067s

Fuente: (Peñafiel, 2019)

Para realizar la comparativa de velocidades, se toma como punto de partida el tiempo que marca hacia una petición realizada sin el establecimiento de un túnel. Cada sentencia se ejecutó de igual manera para cada túnel establecido, los tiempos emitidos por la herramienta, son los datos utilizados para la realización gráfica.

Los tiempos obtenidos se grafican para poder tener una interpretación visual del comportamiento de peticiones realizadas al servidor se determina el tiempo de respuesta ya que estos datos viajan por el túnel, con esto se pretende mostrar cual es más rápido y seguro.

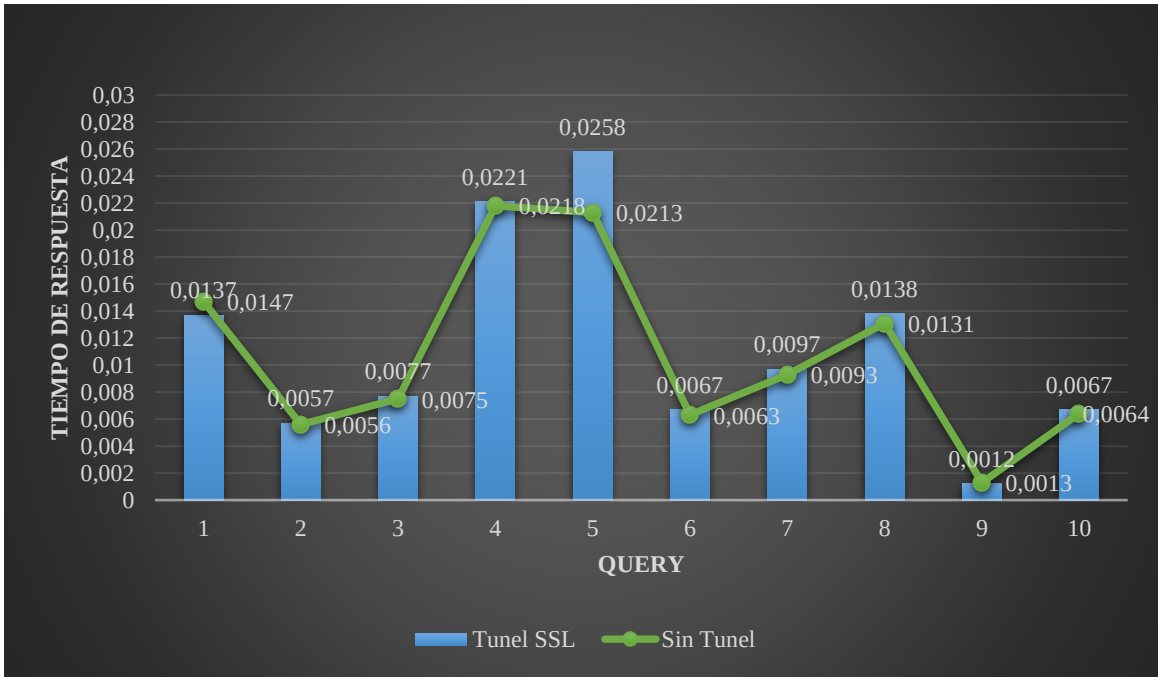


Gráfico 1-4: Resultados de las Peticiones al Servidor

Fuente: (Peñafiel, 2019)

De acuerdo al planteamiento de seguridad que se desea establecer, es decir si se necesita velocidad se debe utilizar un túnel SSL, pero no es muy robusto en un sistema de autenticación al no utilizar un certificado avalado por el CA. Por otro lado, si se necesita mayor control de seguridad en los accesos, entonces se debe utilizar un certificado, que se obtiene de una CA, y que además se transfiere el riego a una autoridad para garantizar la integridad de los datos o información, utilizando un túnel SSL.

4.3. Rendimiento

La prueba de rendimiento consiste en medir el uso y establecer el túnel para luego hacer consultas al servidor, durante un periodo de tiempo se mide el tráfico que ocasiona la telepresencia,

telemetría al enviar datos, audio y video; de acuerdo al dato obtenido se realizara la comparativa de los túneles y sin túneles para de esta manera obtener el dato de comparación.

Esta prueba tiene como finalidad determinar los recursos que utiliza el procesador para la transmisión de datos y poder establecer los túneles al iniciar el cifrado y descifrado; una vez establecido los túneles y que los datos estén viajando, cada vez se envía una solicitud al servidor el equipo del cliente para cifrar la información y la prepara para enviarla por el túnel, cada vez que el servidor envía una respuesta se tiene que descifrar, esto requiere un procesamiento muy grande.

Para medir el rendimiento sin el establecimiento del túnel, se realiza una solicitud al servidor y se obtiene la información contenida en la figura siguiente, la cual indica que el uso medio del CPU es del 0.28 y utiliza el 46% del total del CPU.

Figura 17-4: Uso de CPU sin túnel

Fuente: (Peñafiel, 2019)

Para medir el rendimiento a través del túnel SSL, se realiza una solicitud al servidor y se obtiene la información contenida en la figura siguiente, la cual indica que el uso medio del CPU es del 3.30 y utiliza el 44% del total del CPU.

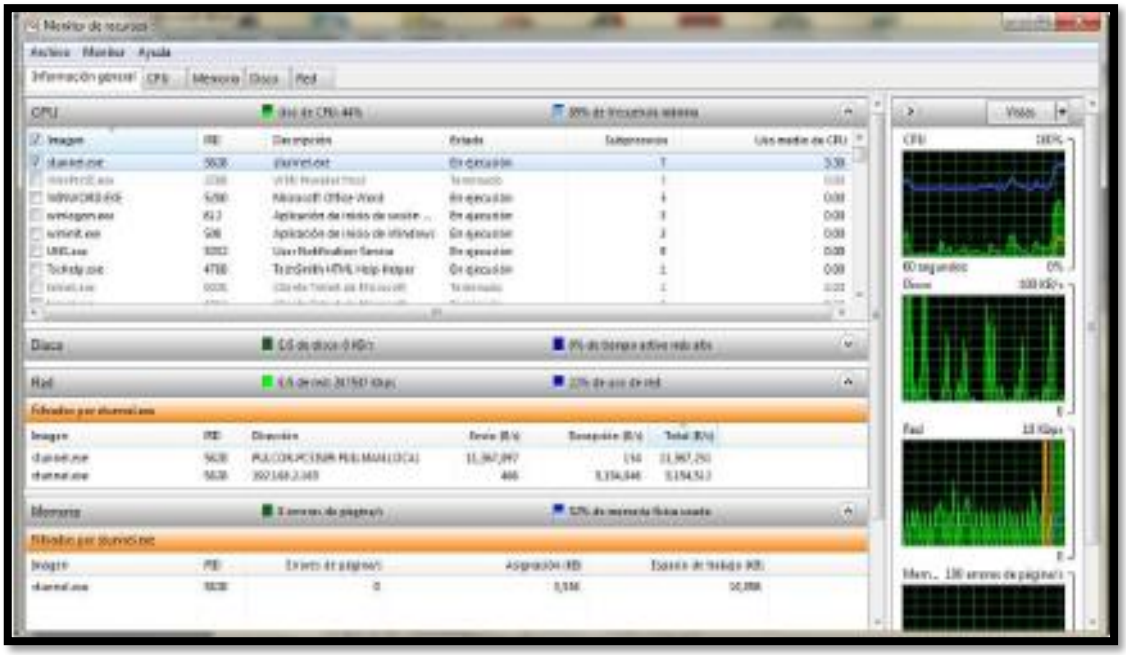


Figura 18-4: Uso de CPU con túnel SSL en video conferencia

Realizado por: (Peñafiel, 2019)

Con la obtención de los datos en la videoconferencia se construye la tabla siguiente, donde se ha ordenado primero el tiempo medio de la CPU, para finalizar con el uso del CPU y con esto se finaliza la prueba de rendimiento, cabe indicar que estas pruebas fueron realizadas en un equipo HP Compaq 8000 Elite Small Form Factor con procesador Intel Core (TM) duo 3. 00GHz con 2GB en ram.

Con los datos obtenidos en la tabla se obtienen que sin el establecimiento del túnel la petición realizada hacia el servidor requiere del 23% del CPU y que el uso medio es del 3.10, esto indica sin duda alguna que el rendimiento es mejor sin un túnel, pero carece de medidas de seguridad, ya que la información está viajando de manera plana elevando el riesgo de ver comprometida la integridad y la disponibilidad de datos.

Tabla 2-4: Resultados de la mediación de uso de CPU

	Sin Túnel	**Túnel SSL**
Uso del CPU 2 usuarios	23%	44%
Uso del CPU 3 usuarios	23,5%	45%
Uso del CPU 4 usuarios	28%	47%
Uso del CPU 6 usuarios	32%	48,5%
Uso del CPU 8 usuarios	35%	50%

Fuente: (Peñafiel, 2019)

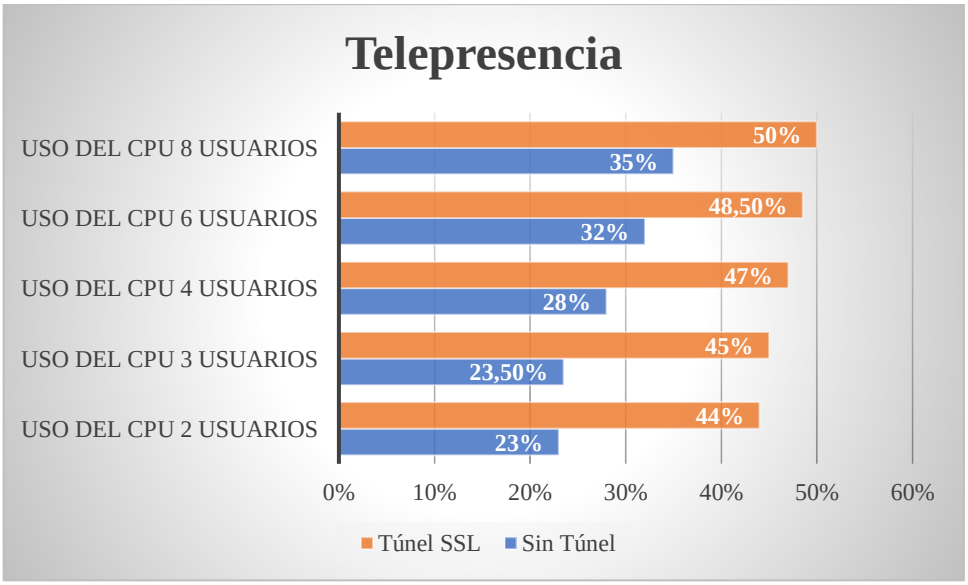


Gráfico 2-4: Resultados de medición de uso de CPU

Fuente: (Peñafiel, 2019)

En el túnel SSL la información obtenida muestra que el uso medio es de 3.30, mayor en relación a sin túnel y en cuanto al uso del CPU es del 44%, con esta información obtenida se da a conocer que el procesamiento es utilizado en gran medida para cifrar la información, pero la ventaja que proporciona SSL es el certificado que podemos utilizar, es decir un CA.

El certificado CA agrega mayor seguridad en el túnel SSL ya que garantiza la integridad de la información de esta manera se crea un estricto control de seguridad.

4.4. Vulnerabilidad

La vulnerabilidad de un sistema surge por errores individuales en un componente sin embargo en la actualidad siguen apareciendo nuevas vulnerabilidades de las interacciones entre varios componentes de un sistema de red como es la telepresencia (videoconferencia), para reducir los riegos de seguridad por las vulnerabilidades de software y de protocolo, se realiza un esfuerzo para la identificación de estas vulnerabilidades mediante el protocolo que se está utilizando.

Para esta parte de las vulnerabilidades se dividió en dos partes la una identificar y reducir el número de nuevas vulnerabilidades, se puede evidenciar la gran importancia de desarrollar mecanismos de autoprotección contra los diferentes ataques los cuales deben pasar por una fase de identificación de los riesgos potenciales a los que están expuestos, luego a una fase de análisis de las debilidades para posteriormente definir acciones de mejora y defensa así como planes de mitigación ante sucesos indeseados.

Para conocer las vulnerabilidades de cada protocolo, se ha realiza una consulta ante la SSI (Subdirección de Seguridad de la Información) / UNAM-CERT de la Dirección General de

Cómputo y de Tecnologías de Información y Comunicación, UNAM que es punto de encuentro al cual puede acudir la comunidad de cómputo para obtener información, asesoramiento y servicios de seguridad; así como para intercambiar experiencias.
Los reportes aquí representados son:

- **Boletín de Seguridad UNAM-CERT 2004-004: Múltiples vulnerabilidades en Open SSL**

OpenSSL implementa los protocolos Secure Sockets Layer (SSL) y Transport Layer Securuty (TLS) que incluyen bibliotecas criptográficas de propósito general. SSL es comúnmente usada para proporcionar servicio de autenticación, encriptación, integridad y no repudio para aplicaciones de red como HTTP, IMAP, POP3, STP y LDAP. Es ampliamente utilizado entre diversas plataformas y sistemas.

CONCLUSIONES

- Luego del estudio realizado en esta tesis en donde se propone el análisis de la aplicación de seguridad SSL y de diseñar el prototipo incluyendo seguridad en la comunicación se concluye que dicha aplicación no afecta negativamente al rendimiento de la red y el servidor.
- Para la protección de los datos se plantea un sistema robusto de seguridad basado en opensource que contempla varios aspectos en la comunicación de tal forma que minimicen los efectos de un ataque o vulnerabilidad en el sistema.
- La información es un activo que llega a tener gran relevancia para la protección de los sistemas de telepresencia en la cual se gestiona sistemas de seguridad para no comprometer la integridad de la información que circula en la red.
- El túnel desarrollado y presentado cubren características de seguridad para la autenticación y envío de información (datos, audio y video), proporcionando un canal de comunicación seguro, esta seguridad está fundamentada en el tratamiento de la información con el cifrad, ya no viaja en texto plano y ahora resulta difícil interpretarlos, con eso se garantiza la integridad de los datos.
- Existen elementos necesarios para poder establecer un túnel de comunicaciones seguro, sus principales características que lo convierten en un sistema seguro, conocer estos aspectos ayuda para detectar principalmente las vulnerabilidades que puede tener el sistema.
- El protocolo utilizado para este proyecto permite mejorar la seguridad de red, este como todo protocolo tiene mecanismo para ayudar a la seguridad, pero al utilizarlos también se está agregando vulnerabilidades propias del protocolo.

El túnel SSL es más rápido y la seguridad es buena y puede agregar más recursos de seguridad, estos recursos pueden ser el manejo de un Certificado (CA) o el uso de claves para el establecimiento de la sesión.

RECOMENDACIONES

- Se recomienda que a futuro se tenga una infraestructura de red LAN y WAN robusta, para la implementación de un equipo de video conferencia SX20, Gestionador de reuniones CISCO TMA, los equipos VCS y el servidor de telepresencia inmersa que permita tener más de 5 conferencias al mismo tiempo.
- A partir de la definición de conceptos y entendimiento de la solución se procedió a realizar el estudio de la situación actual de la red de ESPOCH y se recomienda como primera fase realizar la interconexión entre todas las facultades haciendo el edificio principal CISCO donde se ubicar el Data Center.
- Se recomienda para todo tráfico de datos aplicar el protocolo de seguridad SSL para proteger la comunicación entre el servidor y el cliente, ya que los sistemas por defecto presentan vulnerabilidades.

BIBLIOGRAFÍA

Alonso Rodríguez Antonio Jesús Caro. (2013). *Man In The Middle Attacks On SSL/TLS*. (tesis) (Maestría). Cataluña: Universidad Obertá de Catalunya. Universidad Rovida I Virgili. Universidad Autónoma de Barcelona. Recuperado de http://index-of.co.uk/Sslstrip/acaroalTFM0113memoria.pdf

Angulo Maketa Luis Fernando. (2014). *Estudio Y Diseño Para La Implementación De Una Solución De Telepresencia Inmersiva Dirigida Al Personal Docente Y Estudiantil Para La Universidad Estatal De Guayaquil*. (tesis) (Grado). Guayaquil, Ecuador: Universidad Católica de Santiago de Guayaquil. Facultad de Educación Técnica para el Desarrollo. Ingeniería en Telecomunicaciones. Recuperado de http://repositorio.ucsg.edu.ec/bitstream/3317/1810/1/T-UCSG-PRE-TEC-ITEL-49.pdf

Armijos Cedeño Christian Javier. (2015). *Implementación De Herramienta Open Source Para La Gestión De Inventario Del Parque Informático En CNEL EP*. (tesis) (Grado). Guayaquil, Ecuador: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Ingeniería en Sistemas Computacionales. Recuperado de http://repositorio.ug.edu.ec/bitstream/redug/6657/1/TesisCompleta-546-2015.pdf

Bedoya Giraldo Yeferson, & Salazar Giraldo Cristian Felipe, & Muñoz Lozano Jhon Fredy. (2013). *Implementación, Control Y Monitoreo De Un Sistema De Seguridad Vehicular Por Redes GSM/GPRS*. (tesis) (Grado). Pereira, Colombia: Universidad Tecnológica de Pereira. Facultad de Tecnológica. Ingeniería en Mecatrónica. Recuperado de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4350/6298B412.pdf?sequence=1

Caisaguano Changotasig Anita Margoth. (2003). *Implementación De Un Servidor Web SSL (Secure Socket Layer) Con Encriptación A 128 Bits Bajo Plataforma Linux En Petroecuador*. (tesis) (Grado). Cotopaxi, Ecuador: Universidad Técnica de Cotopaxi. Carrera de Ciencias de la Ingeniería y Aplicadas. Especialidad de Ingeniería en Informática y Sistemas. Recuperado de http://repositorio.utc.edu.ec/bitstream/27000/474/1/T-UTC-1038.pdf

Cisco. (2016). *CISCO SPARK*. Recuperado de https://www.ciscospark.com/

Cornejo Ortega Ángel Danilo, & **Tintín Suquilanda Jorge Luis.** (2010). *Diseño, Construcción e Implementación de un Sistema De Telemetría Utilizando Tecnología GSM: Para el Monitoreo de los Parámetros de Temperatura, Presión de Aceite, Velocidad de Giro del*

Motor y Velocidad de Desplazamiento de un Vehículo Chevrolet Optra, 2008. (Tesis) (Grado). Cuenca, Ecuador: Universidad Politécnica Salesiana sede Cuenca. Facultad de Ingenierías. Ingeniería Mecánica Automotriz. Recuperado de https://dspace.ups.edu.ec/bitstream/123456789/1114/23/UPS-CT001987.pdf

García Patiño Manuel Ricardo, & Suarez Fajardo Didier Alexander. (2008). *Módulo De Telemetría Inalámbrico Para El Monitoreo De Señales De Presión, Temperatura Y Nivel*. (tesis) (Grado). Bucaramanga: Universidad Pontificia Bolivariana. Facultad de Ingeniería Electrónica. Recuperado de https://repository.upb.edu.co/bitstream/handle/20.500.11912/293/digital_15947.pdf?sequence=1&isAllowed=y

Granda Katherine del Pilar, & Saquicela Parra Luis Gustavo. (2017). *Análisis De Vulnerabilidades Del Protocolo SSL/TLS En Las Páginas Web Gubernamentales Del Ecuador Mas Usadas En La Carrera De Ingeniería En Networking Y Telecomunicaciones*. (tesis) (Grado). Guayaquil, Ecuador: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Ingeniería en Networking y Telecomunicaciones. recuperado de http://repositorio.ug.edu.ec/bitstream/redug/24303/1/B-CINT-PTG-N.234.%20Granda%20Katheryn%20Del%20Pilar.Saquicela%20Parra%20Luis%20Gustavo.pdf

Guaigua Guanopatin Sinthia Elizabeth. (2007). *Certificados digitales para autoridades militares de la Fuerza Terrestre*. (tesis) (Grado). Sangolquí, Quito, Ecuador: Escuela Politécnica del Ejército. Departamento de Ciencias de la Computación. Ingeniería de Sistemas e Informática. Recuperado de https://repositorio.espe.edu.ec/bitstream/21000/2531/1/T-ESPE-021811.pdf

Labastida Lara Paulina. (2014). *Propuesta De Adquisición De Datos Y Telemetría Para Primer Efecto Del Proceso De Desalación Med-Le*. (tesis) (Grado). Universitaria, México: Universidad Nacional Autónoma de México. Facultad de Ingeniería. Recuperado de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/5472/TESIS_PROPUESTA_DE.pdf?sequence=1

Luevano E, & López de Lara. E. (2013). *Uso de Dispositivo Móvil de Telepresencia en la Educación a Nivel Universitario.* Buenos Aires, Argentina: Congreso Iberoamericano de Ciencia, Tecnología, Innovación y Educación. Recuperado de Uso de Dispositivo Móvil de Telepresencia en la Educación a Nivel Universitario.

Ñacato Estrella Diego Ramiro. (2014). *Diseño e Implementación De Sistemas De Tele operación para Controlar un Robot Humanoide Mediante un Sensor KINECT* .(tesis) (Grado). Riobamba, Chimborazo, Ecuador: Escuela Superior Politécnica de Chimborazo. Facultad de Informática y Electrónica. Escuela de Ingeniería Electrónica en Control y Redes Industriales. Recuperado de http://dspace.espoch.edu.ec/handle/123456789/3622

R**eyes Diaz Dailos.** (2014). *TFG - Robot Android Y Telepresencia*. (tesis) (Grado). La Laguna: Universidad de la Laguna. Departamento de Ingeniería de Sistemas y Automática y Arquitectura de Computadoras. Escuela Técnica Superior de Ingeniería Informática. Recuperado de https://riull.ull.es/xmlui/bitstream/handle/915/633/TFG%20-%20Robot%20Android%20y%20Telepresencia.pdf?sequence=1&isAllowed=y.

Salvador Salvador Gustavo Adolfo. (2007). *Implementación de un Sistema Piloto de Tele-Presencia (Video Conferencia) para Banda Ancha*. (tesis) (Maestría). Quito, Ecuador: Escuela Politécnica Nacional. Escuela de Posgrado en Ingeniería y Ciencias. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/8403/3/CD-0728.pdf

Valencia Vargas Susana Elizabeth. (2011). *Sistemas De Comunicación Para La Transmisión De Datos Del Sistema De Telemetría En La Propiedad De La Sra. Jaqueline García, Ubicada En La Parroquia San Antonio Del Cantón Montalvo, Provincia De Los Ríos*. (tesis) (Maestría). Ambato, Ecuador: Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Centro de Estudios de Posgrado. Recuperado de http://repositorio.uta.edu.ec/bitstream/123456789/25/1/t592mrt.pdf

Velasco Briones Carlos Ángel, & Cagua Ordoñez Gianella Stephania. (2017**)**. *Implementación De Un Sistema De Monitoreo De Redes Utilizando Herramientas Open Source Y Proveer Servicios De Directorios A Través De Active Directory En La Facultad De Filosofía, Letras Y Ciencias De La Educación De La Universidad De Guayaquil*. (tesis) (Grado). Guayaquil, Ecuador: Universidad Politécnica Salesiana sede Guayaquil. Carrera Ingeniería de Sistemas Recuperado de http://repositorio.utc.edu.ec/bitstream/27000/474/1/T-UTC-1038.pdf

ANEXOS

ANEXO A: TIEMPO DE RESPUESTA

```
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537336    2521532      10092      43396     981752
-/+ buffers/cache:     512188    3546680
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537336    2521532      10092      43396     981752
-/+ buffers/cache:     512188    3546680
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537336    2521532      10092      43396     981752
-/+ buffers/cache:     512188    3546680
Swap:      2764796          0    2764796
```

```
Mem:       4058868    1537336    2521532      10092      43396     981752
-/+ buffers/cache:     512188    3546680
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537556    2521312      10092      43412     981744
-/+ buffers/cache:     512400    3546468
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537540    2521328      10092      43412     981752
-/+ buffers/cache:     512376    3546492
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537540    2521328      10092      43412     981752
-/+ buffers/cache:     512376    3546492
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1538496    2520372      10092      43420     981760
-/+ buffers/cache:     513316    3545552
Swap:      2764796          0    2764796
```

ANEXO B: RED ESTABILIZADA PARA EL TIEMPO DE RESPUESTA

```
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537636    2521232      10092      43444     981760
-/+ buffers/cache:     512432    3546436
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537636    2521232      10092      43444     981760
-/+ buffers/cache:     512432    3546436
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537748    2521120      10092      43444     981760
-/+ buffers/cache:     512544    3546324
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537648    2521220      10092      43444     981760
-/+ buffers/cache:     512444    3546424
Swap:      2764796          0    2764796
usuario@server:~$ free
             total       used       free     shared    buffers     cached
Mem:       4058868    1537624    2521244      10092      43444     981760
-/+ buffers/cache:     512420    3546448
Swap:      2764796          0    2764796
```

ANEXO C: ESTABLECIMIENTO DE VIDEOCONFERENCIA