FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE VULNERABILIDADES DE LA INFRAESTRUCTURA DE RED Y DISEÑO DE LOS PRINCIPALES MECANISMOS DE SEGURIDAD PARA LA AGENCIA METROPOLITANA DE TRÁNSITO

Autor

Freddy Danilo Cuyo Semblantes

Año
2019

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE VULNERABILIDADES DE LA INFRAESTRUCTURA DE RED Y DISEÑO DE LOS PRINCIPALES MECANISMOS DE SEGURIDAD PARA LA AGENCIA METROPOLITANA DE TRÁNSITO

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar el título de Ingeniero en Redes y Telecomunicaciones.

Profesor Guía

MSc. Iván Patricio Ortiz Garcés

Autor

Freddy Danilo Cuyo Semblantes

Año

2019

DECLARACIÓN DEL PROFESOR GUIA

“Declaro haber dirigido el trabajo, Análisis de vulnerabilidades de la infraestructura de red y diseño de los principales mecanismos de seguridad para la Agencia Metropolitana de Tránsito, a través de reuniones periódicas con el estudiante Freddy Danilo Cuyo Semblantes, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Iván Patricio Ortiz Garcés
Master en Redes de Telecomunicaciones
C.C.0602356776

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, Análisis de vulnerabilidades de la infraestructura de red y diseño de los principales mecanismos de seguridad para la Agencia Metropolitana de Tránsito, del estudiante Freddy Danilo Cuyo Semblantes, en el semestre marzo 2018 - agosto 2019 segundo semestre 201920, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Milton Nepalí Román Cañizares
Master en Gerencia de Redes y Telecomunicaciones
C.C.0502163447

DECLARACIÓN DE AUTORIA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Freddy Danilo Cuyo Semblantes
C.C. 1720912714

AGRADECIMIENTOS

Agradezco a Dios por darme la fortaleza espiritual para alcanzar mis objetivos; a mi madre por el sacrificio, la compañía de cada noche de estudio; a mis maestros y tutor por impartir sus conocimientos.

DEDICATORIA

Este trabajo lo dedico: a mi hijo Mateo, a mi amada esposa Amanda Asadobay por ser los motores de inspiración, a mi madre Rosa Elena y mi hermana Jeanneth por su apoyo incondicional.

RESUMEN

El presente proyecto analiza las vulnerabilidades de la infraestructura de red y genera un documento guía con los principales mecanismos de seguridad para sean utilizados en la Agencia Metropolitana de Tránsito. Se empieza por señalar los conceptos básicos que respalda al modelo TCP/IP, como funciona, la jerarquía basada en protocolos y servicios.

Se menciona las vulnerabilidades más sobresalientes que están presentes en el modelo TCP/IP, donde alguien con un conocimiento de las estructuras de funcionamiento de protocolos podría obtener beneficios o causar fallos en el normal desarrollo de sus funciones.

Mediante el uso de herramientas, software y ciertas variables que se obtiene en los sitios web en internet se puede generar manipulación de servicio relacionadas a la transmisión, que puede resultar con el conflicto en aplicaciones Web, desactivación de servicio, lentitud en la transmisión datos y suplantación de servicio o usuarios. A través de las mismas se llega a tener un conocimiento más afondo de los vacíos existentes en el modelo TCP/IP.

El uso de herramientas, la creación una Red Privada Virtual (VPN), mecanismos como SSH y clave pública PKI permiten mimetizar la información que será transmitida a través de canales no seguros cliente/servidor, la redirección de puertos, la propuesta de métodos o equipos de seguridad que nos permitan evitar que alguien ingrese, intercepte falsifique o manipule los datos enviados por internet son el objetivo principal del presente estudio.

ABSTRACT

This project analyzes the vulnerabilities of the network infrastructure and generates a guide document with the main security mechanisms for use in the Metropolitan Transit Agency. It is about pointing out the basic concepts that respond to the TCP / IP model, how it works, the hierarchy based on protocols and services.

The most outstanding vulnerabilities that are present in the TCP / IP model are show, where knowledge of the operating structures that can be obtained in the normal development of their functions is known.

Use of tools, software and certain variables obtained in the websites and on the internet can be given service related to the transmission, which can be useful for the conflict in Web applications, deactivation of service, slowness in the transmission of data and Impersonation of service or users. Through them, you get to have a knowledge beyond the existing gaps in the TCP / IP model.

The use of tools, the creation of a Virtual Private Network (VPN), mechanisms such as SSH and the PKI public key allows minimizing the information transmitted through unsecured client / server channels, port redirection, the proposal of methods or security equipment that we cannot prevent someone from entering, intercepting or manipulating the data sent over the Internet.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Actualmente, en el Distrito Metropolitano de Quito la entidad encargada del control del Trasporte Terrestre Tránsito y Seguridad Vial es la Agencia Metropolitana de Tránsito quien asumió el 9 de agosto del 2014, la total competencia de Tránsito y Seguridad Vial. Para ejercer dichas competencias la AMT cuenta con parte de la infraestructura hardware, software y comunicaciones heredadas por la Corpaire y otra por otra parte infraestructura que sea ha venido adquiriendo según las necesidades.

Al ser una institución nueva no cuenta con un departamento dedicado a la seguridad informática, motivo por el cual la integridad de las bases de datos, las transacciones, la seguridad perimetral sean propensas a sufrir ataques internos y externos que pueden llegar a disminuir la operatividad y en el peor de los casos a tener denegación de servicio como sucedió en la Agencia Nacional de Tránsito (ANT).

La Agencia Metropolitana de Tránsito cuenta con varios aplicativos entre los principales tenemos: Sistema de Revisión Técnica Vehicular, sistema de pagos de la revisión técnica vehicular para los bancos, página web: www.amt.gob.ec, intranet Matriculación, sistema de Cita Previa, sistema de Pico y Placa, sistema de mal estacionados. Mismos que son utilizados por aproximadamente 527 administrativos, 1949 agentes de tránsito, usuarios internos y externos.

El Departamento de Infracciones posee diferentes mecanismos de sanción para las multas pecuniarias y rebaja de puntos que son los siguientes: foco rojo e invasión del carril exclusivo denominados también como foto multa se tiene un promedio de 250 infractores por día, así también con el control de velocidad o foto radar se tiene un aproximado 1200 infractores captados por día y citaciones por boletín entregadas por los agentes de tránsito es un aproximado de 750, las mismas que son ingresadas por software a la Agencia Nacional Tránsito.

La Agencia Metropolitana de Tránsito cuenta con un ancho de banda de 60MB, donde la suma del tráfico de salida y entrada es 47,07Mbps semanal, existen 356.364 sesiones que la interacción o conjunto interacciones de la ciudadanía que tiene lugar en nuestra página web durante un periodo mensual aproximadamente.

El diario el telégrafo publica acerca del *hackeo* a la Agencia Nacional de Tránsito quienes revelan que a su sistema ingresaron 99 usuarios no autorizados entre diciembre 2017 hasta enero 2018. El *hackeo* de las cuentas de funcionarios de la entidad permitió la emisión ilegal de 15.970 licencias de conducir. Además se modificaron 14.583 infracciones y se restituyeron 26.801 puntos (Diario el telégrafo, 2017).

Por esta razón, se propone realizar el análisis y diseño de la infraestructura de red para lo cual nos hemos planteado, señalar los conceptos base que respalda al modelo TCP/IP, como funciona, la jerarquía basada en protocolos y servicios.

El uso de herramientas, software y ciertas variables pueden generar manipulación de servicios relacionados a la transmisión, conflicto en aplicaciones Web, desactivación de servicio, lentitud en la transmisión datos, suplantación de servicio, usuarios y manipulación de la información en general que causan fallos en el normal desarrollo de las actividades diarias.

Levantar la información que posee la entidad para para analizarla de los principales mecanismos que se adapten a la infraestructura existente, asegurar la confiabilidad y protección a la red logrando establecer una buena comunicación mediante el uso de herramientas, equipos que nos permitan evitar que alguien ingrese, intercepte falsifique o manipule los datos.

El uso de herramientas, la creación una Red Privada Virtual (VPN), mecanismos como SSH y clave pública PKI permiten ocultar información transmitida a través de canales no seguros cliente/servidor, redirección de puertos, copia de seguridad, los sistemas criptográficos juegan un papel importante en el incremento de la seguridad de los sistemas de prevención y equipos que nos permitan evitar que alguien ingrese, intercepte, falsifique o manipule los datos enviados son el objetivo principal del presente estudio.

ALCANCE

El presente proyecto tiene como objetivo fundamental realizar el análisis de las vulnerabilidades y mostrar todas las alternativas en los tipos de seguridad de red existentes que se ajusten a las necesidades de la infraestructura de red de la Agencia Metropolitana Tránsito, este trabajo se reflejara en un informe dirigido al administrador de red.

Basándonos en los hallazgos diseñar la red TCP/IP integral y segura donde se utilizará los métodos de seguridad informática que sean capaz de mitigar dichos problemas.

En el diseño se abarca el planteamiento de la solución, fundamentos teóricos, inspección en sitio, análisis de equipos, calidad de servicio y adicionalmente optimizar la red de datos como una alternativa interesante, económicamente competitiva para brindar mejor disponibilidad del sistema actual de comunicaciones TCP/IP, con una conexión de red integral y segura con sus sucursales remotas.

JUSTIFICACIÓN

El diseño actual de la red de la Agencia Metropolitana de Tránsito está basada en la funcionalidad, es muy riesgoso transportar de un lugar a otro la información transaccional. El tráfico aproximado de salida y entrada es de

47,07 Mbps esto debido a las transacciones diarias de 1450 infracciones de foto-multas captadas en (semáforo rojo e invasión de carril exclusivo) y 750 citaciones por boletín todo esto asciende a un total de 2200 multas diarias las mismas que son ingresadas por software a la Base de Datos de la Agencia Nacional Tránsito.

El presente proyecto tiene como fundamento la construcción de un modelo seguro e integral usando las tecnologías existentes de manera que se logrará fiabilidad, disponibilidad. Proponer la adquisición de nuevos y modernos equipamientos que nos permitan ser custodios de nuestra información organizacional al configurar métodos como la redundancia, políticas de seguridad que nos proporcionan los equipos de gran capacidad como (router, firewall, switch) para tener la información asequible en todo momento.

Para la realización del análisis y diseño de una red segura es necesario conocer las características de los protocolos de comunicaciones que serán los encargados de transportar la información que desean distribuir. Se deberá también analizar los servicios que se ofrecen por medio de la red y detalles de funcionamiento para proporcionar una alta disponibilidad de base de datos.

Basándonos en lo expuesto anteriormente es de vital importancia encontrar una o varias soluciones de mecanismos para poseer una red segura e integral protegiendo los datos contra accesos no autorizados, nos ayuda a prevenir una posible corrupción durante el ciclo de vida de los mismos, con el objetivo de brindar un excelente servicio en nuestras sucursales: Jefaturas, Centros de Matriculación, Patios de Retención Vehicular, Terminales, Administración Matriz, Centros de Detención de Infractores, Departamento de Fiscalización y Operaciones.

1.1. Objetivos generales

Diseñar una infraestructura de red aplicando los principales mecanismos de seguridad y alta disponibilidad para la Agencia Metropolitana de Tránsito.

1.2. Objetivos específicos

- Realizar el levantamiento de los requerimientos técnicos de la Agencia Metropolitana de Tránsito, para investigar los métodos de seguridad actuales que se adapten a sus necesidades.

- Analizar mecanismos para la prevención, mantenimiento, operación y lo que se debe tomar en cuenta para el resguardo a través de la seguridad TCP/IP.

- Determinar el mejor método de seguridad mediante el análisis de vulnerabilidades, funcionabilidad, escalabilidad, costo-beneficio de la infraestructura.

- Diseñar la infraestructura de telecomunicaciones que permita trasmitir la información desde la Matriz AMT hacia las diferentes dependencias de una manera eficiente y eficaz bajo políticas y normas de seguridad.

2. MARCO TEÓRICO ESTRUCTURA DE FUNCIONAMIENTO DE LA RED

2.1. Historia de Ataques y Seguridad

Para entender que es la seguridad en redes debemos empezar mencionando que la red es la conexión entre dos o más computadoras través medio físico y cómo fueron sus inicios.

Desde los años 60 había pocas computadoras y el único acceso remoto a ellas era por medio de una línea telefónica local, en 1966 dos computadores fueron conectadas desde el laboratorio Lincon y Corporación de Santa Mónica por medio de un enlace discado (conexión dedicada telefónica) de 1200 bits por segundo, como se evidencia en la figura 1.

Figura 1. La primera conexión discada.
Tomado de (Soler Amaya, 2016).

En 1969 se da la primera conexión de ARPANET, en consecuencia se implementó la transmisión TCP y IP y posterior el conjunto de protocolos daría como resultado el modelo TCP/IP (González, 2016).

2.1.1. Crecimiento de las Redes

Red de área local (LAN). Un grupo de computadores que tienen una línea de conexión común en lugares pequeños y preestablecidos como cuartos o edificios.

Red de Área Metropolitana (MAN). Es una red de área geográfica extensa con alta velocidad brinda servicios de integración múltiple como es: transmisión de datos, voz, video por diferentes medios de transmisión como fibra óptica y par trenzado.

Red de área amplia (WAN). Es una red que une varias redes locales sin importar que se encuentren en un mismo lugar, una distancia de 100 a 1000 kilómetros es usado generalmente por empresas, organizaciones, ISP, etc.

Es un conjunto de equipos informáticos conectados sin la necesidad de un cable denominado (*Red Wireless*), haciendo que el usuario final pueda desplazarse de un lado a otro en una determinada área, estas redes usan ondas electromagnéticas.

Red de área personal (PAM). Red que comunica dispositivos de computación con diferentes tecnologías cercanas a una persona como puede ser: PDAs, tableros electrónicos de comunicación, computadoras portátiles, celulares, impresoras, consolas de video juegos etc.

2.1.2. Primeros Ataques a la Red

En 1970 no existían copias de seguridad, únicamente existían medidas de seguridad físicas incorrectas.

En 1972 John Draper con la ayuda de una caja azul dispositivo de generación de tonos y el silbato de un juguete de cereal de capitán Crunch, logra realizar llamadas gratis considerado como fraude telefónico.

En 1980 aparecen los primeros virus informáticos con aplicaciones maliciosas que se propagaban de computador en computador con el fin de dañar diversos funcionamientos del computador, en 1985 aparecieron los primeros caballos de Troya o troyanos mismo que se presentaban ante el usuario común como una imagen de programa de mejora de gráficos.

Posterior el virus Brain creado para atacar al sistema informático MS DOS, distribuidos en disquete (*diskette o floppy disk*- almacenamiento de datos magnético) pirateados de programas es el primer virus que logro propagarse a nivel mundial entre los años de 1986 a 1987, ya que era compatible con IBM PC.

En 1903 un mago británico Nevil Maskelyne que para demostrar las vulnerabilidades del telégrafo inalámbrico que había desarrollado Marconi transmitió un poema en lugar del mensaje original, para lograrlo había instalado un transmisor de códigos morse y repetidor de señal de 50 metros de altura.

2.1.3. Las Primeras Defensas

En 1987 aparece la comercialización de los antivirus para los computadores con el fin de contrarrestar dichos virus.

La colaboración por internet fue un detonante para muchas violaciones de seguridad al final de los 80’s. Los enrutadores (*router*- encamina paquetes a través de una red) eran las primeras defensa o cortafuegos por su característica principal de separar una red de otra.

Primera generación. - Cortafuegos de red. Se basa en un sistema realizado por los ingenieros (DEC) *Digital Equipment Corporation* permitía el filtrado de paquetes y protocolos.

Segunda generación. - Cortafuegos de estado. Es el resultado de la investigación de los Laboratorios AT&T Bell, inspección de estado de paquetes debido a que tiene el registro de todas las conexiones con esto verificaba si un paquete inicia una nueva de sesión era un paquete erróneo o de una conexión existente, ayudo a prevenir ataques de Denegación de Servicio (DOS).

Tercera generación. - Cortafuego de aplicación. Este tipo podía entender aplicaciones y protocolos, permitía detectar si un protocolo malicioso se coló a través puertos no estandarizados.

Cortafuego Visas. - El primero con un interfaz gráfico, a color e iconos, su característica principal era ser compatible con los sistemas operativos como Windows de Microsoft o MacOS de Apple, era fácil de implementar y fue patentada en 1994 por la compañía de Israel Check Point Software Teconologies como Firewall-1.

2.2. Niveles del modelo TCP/IP y vulnerabilidades

Para diseñar una infraestructura segura comenzaremos a definir los puntos vulnerables y las medidas de seguridad de una red, es necesario ver su estructura de funcionamiento. Para esto hay que basarse en el modelo TCP/IP como se detalla en la figura 2. El cual muestra de forma clara cómo viaja la información a través de la red. Este modelo es una mejora del modelo OSI, por lo tanto, el modelo TCP/IP se simplificó y replanteó la estructura de cómo los datos se trasladan a través de la red.

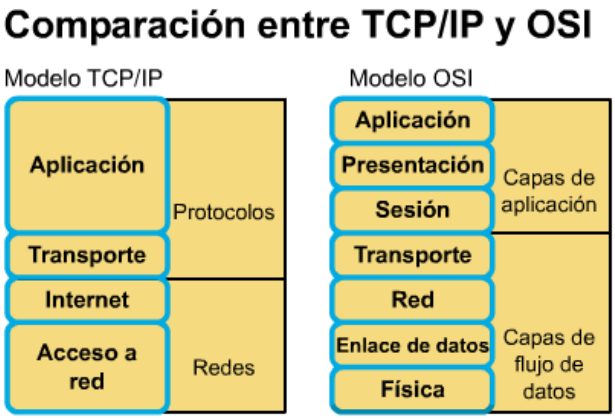


Figura 2. Modelo TCP/IP y OSI

Tomado de (Quijije Lopez, 2014)

Aquí vamos a exponer las capas del modelo TCP/IP, si bien es cierto que la mayoría de los nombres de las capas son iguales a los del modelo OSI y comparten características en común, también se pretende mostrar las falencias que existen en el modelo TCP/IP, analizando los protocolos de cada capa, es muy importe no confundir las funciones de cada modelo ya que cada una de ellas desempeñan funciones diferentes en cada modelo.

La funcionalidad de los protocolos de capa de aplicación de TCP/IP se adaptan aproximadamente a la estructura de las tres capas superiores del modelo OSI: Capas de Aplicación, Presentación y Sesión.

El principal objetivo es que a través de estos problemas poder observar como el atacante puede engañar a los usuarios que se encuentran operando en una red, ya sea deshabilitando el servicio, interrumpiendo la comunicación y manipulando la información.

La figura 3. Detalla las vulnerabilidades generales que existen en el presente modelo en cual estamos centrando el estudio.

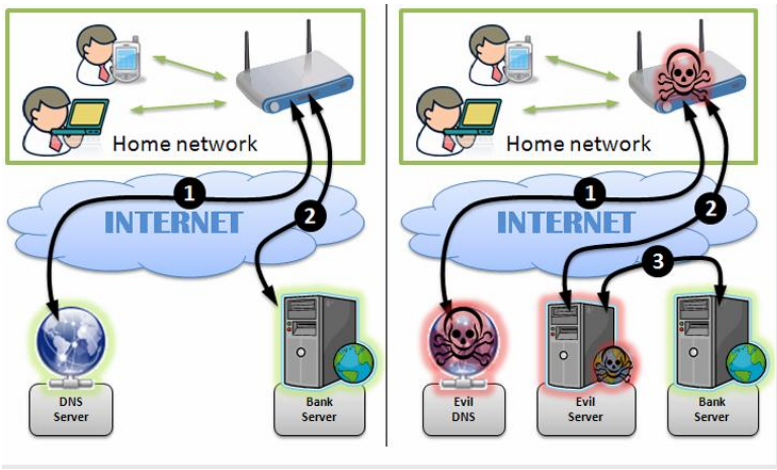


Figura 3. Vulnerabilidades a través de DNS Hijacking

Tomado de (Arg-Wireless.com.ar., 2011-2014)

2.2.1. Capa Aplicación

Maneja protocolos de alto impacto, aquí es donde los usuarios llaman a la aplicación que contiene aspectos como la codificación, control de diálogos y aspectos de presentación.

Este modelo reúne todas las características de las aplicaciones en una sola capa y se asegura que los datos que van a ser enviados estén correctamente empaquetados antes de pasar a la siguiente capa, para este envió cada programa de aplicación selecciona el tipo de transporte que va a utilizar, los cuales pueden ser flujo continuo de octetos o una secuencia de mensajes individuales.

La capa superior es la única capa de aplicación en TC/IP que puede o no utilizar las conexiones establecidas (con el modo no conectado) y permite, finalmente que los procesos realizados en distintos ordenadores puedan comunicarse entre sí (Cordoigne, 2015, pág. 128).

Es así que se puede detectar debilidades de diseño en el aspecto de la identificación y validación de los paquetes en este proceso es donde favorecen la falsificación de los mismo, ya que el atacante puede modificar a gusto esta

información, el intruso puede enviar direcciones incorrectas o recibir información de las cuentas de los usuarios a través de sus peticiones.

2.2.2. Capa Transporte

El deber esta capa es garantizar la comunicación extremo a extremo entre las aplicaciones de los usuarios mediante una conexión lógica a los puntos finales de la red más conocida como conexión punta a punta. El usuario emisor y receptor segmenta y ensambla los datos que han sido enviados por las capas superiores en un mismo flujo de datos, cumpliendo la trasmisión de datos a través del transporte de extremo a extremo.

Se suele imaginar que el internet es como una nueve donde los paquetes viajan de una forma confiable, asegurando que los datos lleguen sin errores y en orden que fueron enviados. Para esto el protocolo de transporte tiene una tarea importante que debe realizarse en el lado del receptor, enviar acuse recibo de retorno en caso de haberse perdido el paquete en el transcurso retransmite los paquetes que contenga error.

Debido a que la capa transporte aceptar datos desde diferentes programas de usuarios y enviarlos a los siguientes niveles, se tiene que añadir información adicional que incluye código de identificación de cada programa a enviar o recibir de esta manera utiliza los códigos para identificar el programa en el otro extremo al cual le pertenece basándose en su identificación.

Esta capa transmite TCP o UDP sobre datagramas IP. Las principales vulnerabilidades que podemos encontrar aquí son autenticación, integridad y confidencialidad. La denegación de servicio es el ataque más común en esta capa se ve asociada a la relación de protocolos de comunicación entre capas.

La negociación involucrada en el establecimiento de sesión existe atacantes que aprovechan las falencias en su diseño, el secuestro de sesiones TCP

establecidas anteriormente tiene como objetivo dirigirlos a otros dispositivos con fines de obtener lucro para un atacante.

2.2.3. Capa de Internet

Esta capa es la encargada de seleccionar y establecer el mejor camino entre dispositivos finales a través de la utilización de un algoritmo de ruteo para ver si el datagrama debe procesarse de manera local o debe ser transmitido. El paquete debe llevar identificación de la terminal hacia la que se debe enviar el paquete para que pueda ser receptado.

Por último, la capa Internet envía los mensajes ICMP (Protocolo de Control de Mensajes de Internet) de error y control necesarios y maneja todos los mensajes ICMP entrantes.

Los datagramas IP en esta capa son frecuentemente más afectados, debido a la información que se puede encontrar para vulnerar el sistema, la modificación de información, suplantación de mensajes, denegación de mensajes y retrasos de mensajes; se puede hacer uso de estos datos para beneficio personal mediante software espías o captura de información que circulan en la red (*sniffing*).

El principal error de esta capa es la autenticación la cual se realiza a nivel de máquina, es decir la IP es asignada por el dispositivo de red y no es a nivel de usuario. Si un sistema entrega una dirección de dispositivo errónea el receptor del otro lado no detecta la suplantación, no verifica si la dirección es real o es una dirección alterada por un atacante. Es así como un atacante puede acceder a una máquina.

A través de un método llamado la predicción de secuencias TCP, este emula la participación en una red, permite tener acceso a una red en particular y lograr robar una sesión TCP. Por otro lado, después de la captura de datos los

paquetes se pueden manipular, si modifican los datos y se reconstruyen de forma correcta los controles en las cabeceras. Si se tiene éxito, el cambio será indetectable por el receptor.

2.2.4. Capa de Red

Esta capa utiliza como protocolo principal (IP), engloba todos sus aspectos que requiere para efectuar un enlace con los medios físicos de red. Aquí podemos ver una reunión de la capa física y enlace del modelo OSI donde incluye los detalles de tecnologías (LAN y WAN).

Esta capa recepta datagramas IP para transmitirlos a una red especifica los mismos que sirven para buscar el mejor enrutamiento permitiendo que llegue a su destino final.

La figura 4. Muestra como la información viaja a través de las diferentes capas.

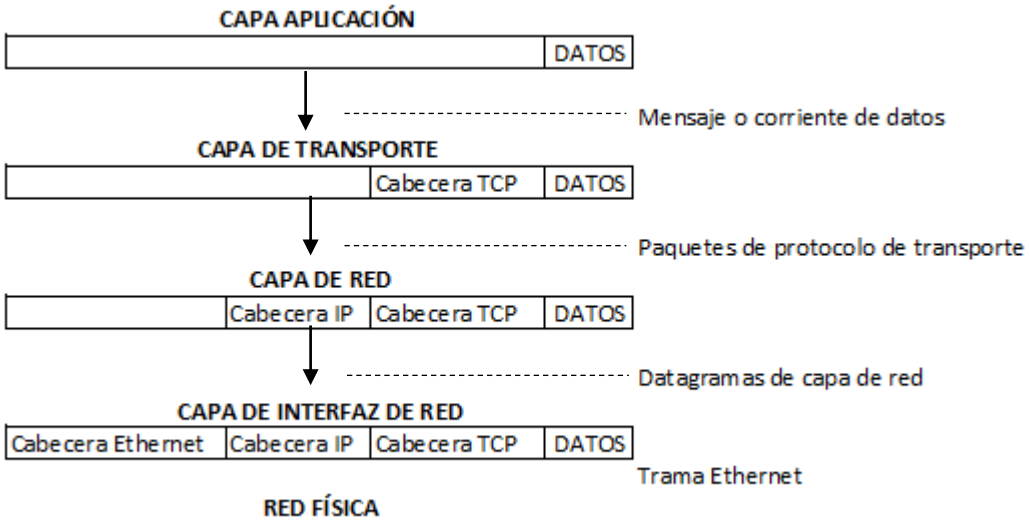


Figura 4. Flujo de información de TCP/IP
Tomado de (IBM, 2016)

Esta capa es propensa a ataques cuando alguien tiene acceso a los dispositivos de red presentes en una infraestructura de red o cuartos de

telecomunicaciones, el acceso a los equipos remotos o al cableado. Es así que tenemos los ataques que ocurren en líneas de cable, desvió de cable, hacia otros sistemas, captura de comunicación entre equipos (pinchar líneas). Estos ataques están estrechamente ligados a la accesibilidad que pudiese tener una persona o atacante.

La Tarjeta de Interface de Red posee falencias físicas como la burla de la confidencialidad, autenticación e Integridad, el descuido de estas tres condiciones representa un flanco débil en las vulnerabilidades de la capa de red.

2.3. Protocolos vulnerables relacionados con el Modelo TCP/IP

Existen muchos protocolos dentro de las capas y algunos son vulnerables como los podemos apreciar en la figura 5. Donde se exponen los más conocidos.

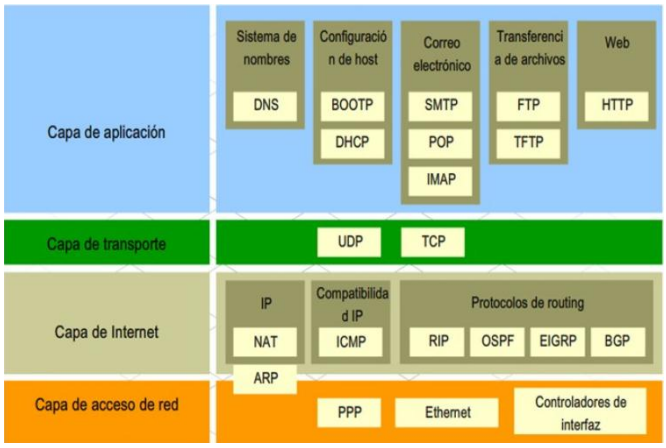


Figura 5. Modelo TCP/IP y protocolos por nivel

Tomado de (SlidePlayer.es, 2018)

La estructura mostrada es fundamental realizar el análisis ya que aquí observaremos las principales vulnerabilidades y fallos. Debido a lo mencionado se expone el detalle de las funciones de cada protocolo y sistemas que son usados para establecer la conversación entre dispositivos.

2.3.1. Ethernet

Permite la comunicación entre dos o más dispositivos conectados entre sí, también conocida como tarjeta de área local o tarjeta de interface de red (NIC-*Network Interface Card*) nos ayuda a compartir recursos entre dos o más equipos.

- Establecida en la capa red del modelo (TCP/IP).
- Comúnmente conocida como Ethernet utiliza una interface o puerto (RJ-45 *Registred Jack 45* o conector 45 registrado).
- Las tarjetas poseen un número de identificación que lo hace únicos en la red, esto es posible gracias a sus 48 bits únicos en hexadecimal nombrado dirección MAC.
- La tarjeta puede ser de conexión física o inalámbrica.

Tarjeta de interfaz de Red NIC, transforma de señales analógicas a digitales los datos enviados por los dispositivos se transmite a través de un cable de red denominado conexión física de área local. Adicional se encarga de traducir los pulsos eléctricos emitidos por el cable en señales digitas o bytes para que el segundo dispositivo pueda comprenderlos, “su papel es preparar los datos que deben transmitirse antes de enviarlos e interpretar los recibidos. Para ello contiene un transmisor y receptor” (Cordoigne, 2015, pág. 135).

2.3.2. Protocolo PPP

Conecta dos dispositivos finales, permite que múltiples protocolos de comunicaciones de red utilicen una misma línea de comunicaciones física.

Es conocido por utilizar tramas, dentro de la trama PPP el Bit de entramado es el delegado de señalar el inicio y el fin de la trama PPP.

2.3.3. Protocolo ARP

Es el encargado de resolver direcciones (ARP- *Adress Resolution Protocol*), permite conocer la dirección física de una interfaz de red actuando como intérprete y traductor de una dirección IP y los controladores de red.

2.3.4. Protocolo ICMP

Protocolo de Control Mensajes de Internet (ICMP-*Internet Control Message Protocol*) realiza control de los datagramas IP que se transmite por la red.

Es una especie de sub capa IP, que trabaja en paralelo con este protocolo. Su propósito es proporcionar el control y la interpretación de errores. Identifica ciertos eventos importantes en TCP (Cordoigne, 2015, pág. 415), como:

- Descubrimiento de router.
- Medida de los tiempos de tránsito de los grupos de paquetes de internet.
- Dirección de tramas.

2.3.5. Protocolo UDP

El protocolo data drama de usuario (UDP), se basa en el intercambio de datagramas sin haber conexión, es el que permite crear una interfaz entre la capa red y aplicación, esta es una forma de multiplexar y demultiplexar los datagramas IP enviados en la red.

2.3.6. Protocolo HTTP

Protocolo de Transferencia de Texto (HTPP- *Hyper text Markup Language*), permite transferir archivos en lenguaje de marcación de Hyper texto (HTML) entre un navegador y un servidor Web a través de una cadena nombrada como dirección de localización uniforme de recursos (URL). Es el encargado de que el formato visualizar sea entendible en una página Web el manejo correcto del texto y los diferentes elementos en multimedia permite que el usuario pueda tener una buena experiencia y sea amigable al navegar.

2.3.7. Protocolo Telnet

Permite la conexión de terminales y aplicaciones remotas por medio de red. El protocolo posee reglas sencillas que permiten la comunicación entre cliente y servidor mediante el uso de un intérprete de comandos. En la actualidad ya existe un protocolo que ofrece seguridad en la interpretación de conexiones (SSH).

2.3.8. Protocolo SMTP

Realiza transferencia simple de mensajería electrónica o correo (SMTP), permite la transferencia directa de mensajes desde un servidor de correos a otro para hacer esto debe tener la identificación, seguido del signo @ y el nombre de dominio.

2.3.9. DNS

Es el encargado de traducir el nombre del dominio a una dirección IP, es un servidor de dominio de nombres que se traduciría como un almacén de gran capacidad donde se ubican las direcciones que solicitan los usuarios. Esto puede ser asignado a las máquinas de forma dinámica o manual.

2.4. Vulnerabilidades más comunes

A los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se les denominan “Piratas Informáticos”. Y es así que tenemos los ataques más comunes generados por:

- Rastreo de tráfico
- Denegación de servicio
- Acceso no autorizado
- Manipulación de información
- Enmascaramiento
- Virus informáticos
- Físicos

2.4.1. Rastreo de tráfico

Es la captura por terceras personas de paquetes, datos y tramas que están circulando por la red, a través del resultado de esta captura se puede utilizar para realizar ataques o el ingreso a sistemas empresariales.

Mediante el uso de un analizador de tráfico de red se realiza la captura de sesiones TCP/IP, en la capa de enlace que están presentes en un medio compartido como las Redes inalámbricos y Área Local (*Ethernet*).

Los fisgones una vez en el interior de red pueden es cuchar sesiones que portan en sus líneas: números de tarjetas de crédito, nombres de usuarios, contraseñas. Esta información puede ser robada ganando acceso no autorizado a cuentas o sistemas críticos.

2.4.2. Denegación de servicio

El (DDOS) o denegación de servicio uno de los más conocidos como se muestra en la figura 6. El objetivo de este ataque es detener o apagar los servicios que quede completamente inaccesible a los usuarios legítimos de una infraestructura de computadoras colocadas en red.

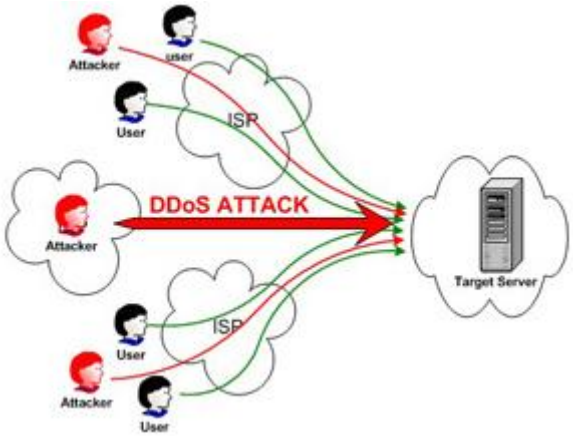


Figura 6. Esquema de denegación de servicio
Tomado de (culturacion, 2014)

2.4.3. Acceso no autorizado

Acceso de manera indebida sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o únicamente por curiosear o divertirse de su autor.

Tener el acceso como administrador o *root* dependiendo el sistema es el objetivo principal que persiguen los atacantes, para poder modificar, copiar, robar o espiar la información en la red.

2.4.4. Manipulación de información

Con la manipulación de datos, los atacantes pueden capturar, manipular y reenviar información hacia otros sistemas a través de la conexión de red. Es una derivación del ataque de contraseñas.

2.4.5. Enmascaramiento

Manipula los paquetes TCP/IP para enviar o receptar de mensajes usando la identidad de otro sin su autorización con el objetivo de falsificar la IP, el atacante se disfraza de usuario valido para acceder a los privilegios del usuario a través del uso de *spoofing*- suplantación la dirección de la red.

Como hemos visto, en el spoofing entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo y por otro evitar que el equipo suplantado interfiera en el ataque

Probablemente esto último no le sea muy difícil de conseguir: a pesar de que existen múltiples formas de dejar fuera de juego al sistema suplantado - al menos a los ojos del atacado que no son triviales (modificar rutas de red, ubicar un filtrado de paquetes entre ambos sistemas), lo más fácil en la mayoría de las ocasiones es simplemente lanzar una negación de servicio contra el sistema en cuestión.

Para el uso de este método se usa rastreo de contraseñas, modificadores de secuencia, herramienta de prueba sistemática de puertos TCP.

2.4.6. Virus informáticos

Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se pueda dar cuenta. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador. Aunque no todos son tan dañinos. Existen unos un poco más inofensivos que se caracterizan únicamente por ser molestos (Community Foundation International, 1998-2016).

Existen muchos tipos de virus, veamos a continuación en la figura 7. Los más importantes:

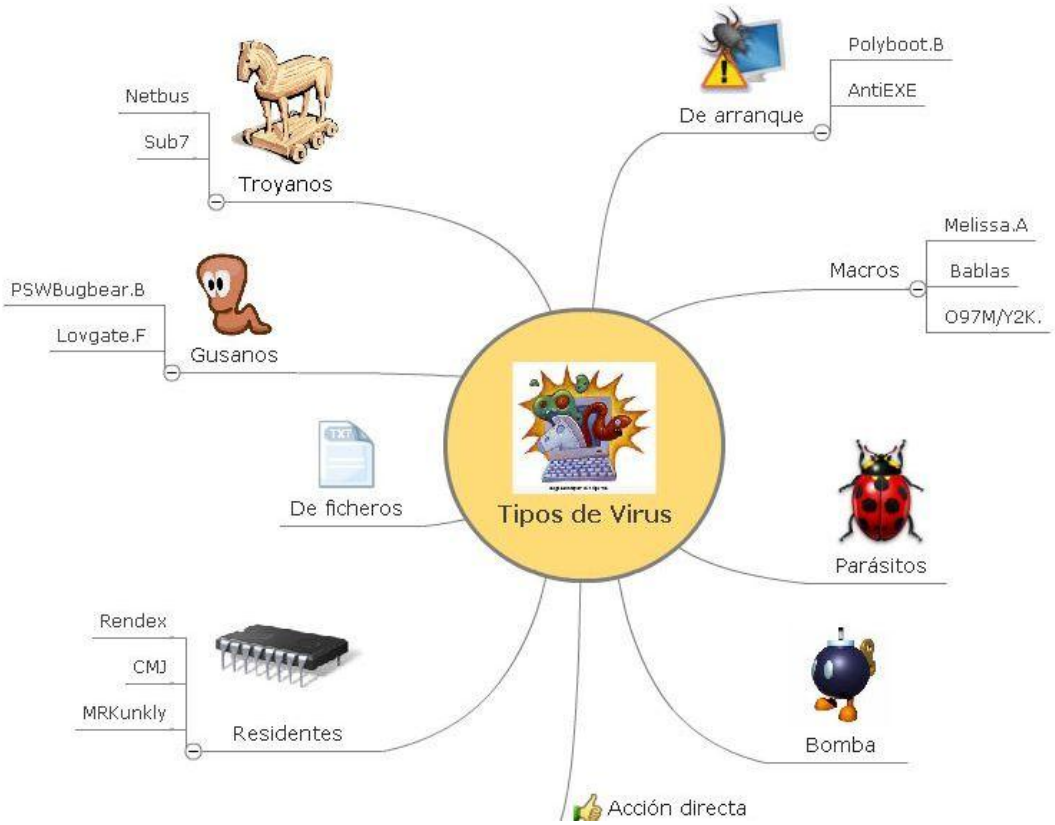


Figura 7. Tipos de virus

Tomado de (Taringa, 2012)

2.4.6.1. Tipos de virus

El principal objetivo de estos malware es ingresar al sistema como programas inofensivos y destruir información o niega el uso a los usuarios legítimos consumen ancho de banda, memoria espacio en disco (masadelante, 1999-2018).

- Virus residentes en la memoria: Este virus se oculta y residen de forma permanente en la (RAM) Memoria de Acceso Aleatorio. Desde ahí, infecta a los programas o archivos que progresivamente sean ejecutados, abiertos, cerrados, copiados, renombrados de acuerdo al uso de la máquina hasta que esta se apague (Gomez, 2018).

- Virus de sobre escritura: son aquellos que una vez infectados eliminan el contenido de un archivo de forma total o parcial, las características para detectar el ataque es que el tamaño del fichero o programa no cambia y deja funcionar, se puede eliminar perdiendo todo el archivo o desinstalando el programa.

- Virus de acción directa: Este virus por lo general se aloja en el directorio raíz, actúa cuando cumple ciertas condiciones infecta todos los archivos que se encuentren en su camino y cada vez que se instala busca una nueva ubicación para alojarse.

- Virus de sector de arranque: Este virus infecta al disco y dispositivos de almacenamiento que contengan sector o *boot* de arranque el cual les ayuda iniciar el sistema.

- Virus FAT: este virus ataca a la Tabla de Asignación de Ficheros por este motivo es considerado nocivo ya que puede impedir el acceso a pequeños archivos o grandes cadenas de directorios donde se almacenan archivos importantes para el funcionamiento del ordenador.

- Macro virus o virus de macro: Virus que infecta a los archivos creados a través de programas macros como; Doc, pps, xls y mdb estos mini programas cambian, modifican o sustituye un macro.

- Virus polimórfico: Estos virus considerados los duros de detectar debido a que su naturaleza es camuflaje esto logra gracias a que en cada ataque de infección se cifra de una forma distinta generado muchas copias e impide que los antivirus los detecte.

- Virus del tipo de secuencias de comandos web: Sitios web que contienen códigos complejos para el entretenimiento del usuario, que a su vez puede ser explotado por virus informático para realizar acciones indeseables en el ordenador (comofuncionaque.com, 2016).

2.4.7. Físicos

En general influye algunas variantes como: incendios, inundaciones, condiciones climatológicas, instalaciones eléctricas, disturbios o sabotaje que puedan afectar directamente a la infraestructura de red. Frecuentemente los ataques son por personas que usan una computadora sin autorización.

2.5. Herramientas para analizar vulnerabilidades

Un escáner de vulnerabilidades es una aplicación diseñada para realizar análisis automáticos de cualquier aplicación, sistema o red en busca de cualquier posible vulnerabilidad. Aunque estas aplicaciones no son capaces de detectar la vulnerabilidad con total precisión, sí son capaces de detectar ciertos elementos que podrían desencadenar en una vulnerabilidad, facilitando enormemente el trabajo a los investigadores e ingenieros.

2.5.1. Nmap

No podemos empezar un recopilatorio con los mejores escáneres de vulnerabilidades sin hablar de uno de los más potentes, completos y veteranos que podemos encontrar en la red: Nmap. Este software es uno de los más utilizados para buscar hosts dentro de una red, así como para buscar los puertos abiertos a través de los cuales poder conectarnos a un sistema de forma remota e incluso recoger información sobre todos los hosts de una red, como el sistema operativo que utiliza o los servicios que tiene habilitados.

2.5.2. Aircrack-ng

Las redes Wi-Fi son uno de los puntos más débiles de las empresas, y por ello es uno de los aspectos que más debemos cuidar. En este punto, Aircrack-ng es sin duda la mejor herramienta para poder a prueba la seguridad de cualquier red Wi-Fi en busca de cualquier posible vulnerabilidad que pueda permitir a cualquier usuario no autorizado hacerse con la contraseña de nuestra red.

2.5.3. Wireshark

Continuando con las auditorías de redes, Wireshark es el analizador de paquetes y protocolos por excelencia. Esta aplicación es capaz de registrar absolutamente todos los paquetes que pasan por una red, recogerlos y poder filtrarlos y ordenarlos de multitud e formas para poder analizar cómodamente todo el tráfico. Esta herramienta además es capaz de descifrar los paquetes enviados a través de los principales protocolos de conexión segura para poder analizar sin problema su contenido.

2.5.4. OpenVAS

OpenVAS es un escáner de vulnerabilidades al que podemos introducir una dirección IP y encargarle el análisis de dicho equipo, recogiendo información

sobre los servicios en funcionamiento, los puertos abiertos, fallos de configuración, posibles vulnerabilidades conocidas en el software del equipo o servidor, etc.

2.5.5. Nessus

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron.

2.6. Sistemas de gestión de la seguridad de la información

Procesos y procedimientos para llevar una buena gestión de seguridad de la información, identificando las vulnerabilidades de la información, para posterior realizar la ejecución de las estrategias de seguridad de la información, medición de resultados y mejoras sobre las estrategias, con la finalidad de lograr un excelente sistema de seguridad de la información, a continuación, se detalla gráficamente el entorno del sistema de gestión.

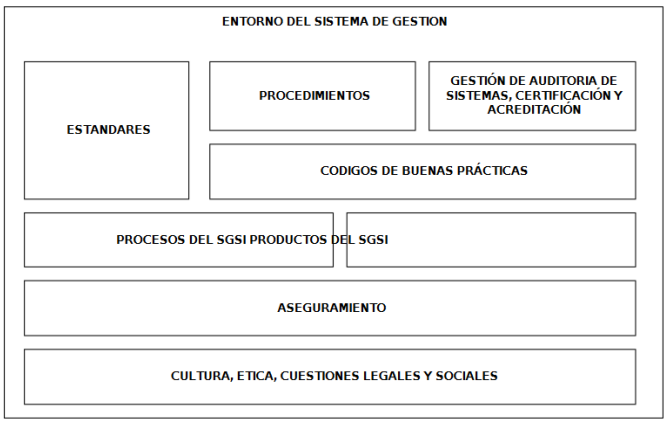


Figura 8. Aspectos a cubrir en un SGSI

Tomado de (Crespo L. E., 2005)

2.6.1. Gestión de Activos de Información

Clasificar a los activos de acuerdo a su nivel de sensibilidad, detallando claramente cómo deben ser tratados, esto se lo puede lograr realizando un inventario tanto de software como de hardware y delegando custodios para cada uno de los dispositivos con las respectivas actas de entrega-recepción con el fin de preservar su cuidado, prevención y mantenimiento de los mismos.

2.6.2. Gestión de las Comunicaciones y Operaciones

Diseñar un proyecto para el buen manejo de situaciones de riesgo de la información, para controlar el uso del sistema de seguridad se debe separa la persona que realiza las tareas gestión y las que realiza la tarea de ejecución.

Se debe contar con un programa de copias de respaldo para resguardar la información alineada a las políticas de seguridad.

3. LEVANTAMIENTO DE LA INFRAESTRUCTURA DE RED DE LA AMT

En este capítulo se pretende mostrar las falencias que existen en el modelo TCP/IP, analizando los protocolos y dispositivos de cada capa.

El atacante puede engañar a los usuarios de la Agencia Metropolitana de Tránsito que se encuentran operando su red, ya sea por medio de la deshabilitación de servicio, interrupción de la comunicación o manipulación de información.

3.1. Situación Actual Infraestructura

La Agencia Metropolitana de Tránsito centraliza sus servicios en un Centro de Datos de la Matriz con el objetivo de la información no esté dispersa y que las dependencias (Patios de retención Vehicular, Terminales Terrestres, Jefaturas Zonales, Oficinas administrativas, .etc.), se conectan a los distintos aplicativos de la institución tales como: correo institucional, usuarios active directory e internet los cuales usan los enlaces de datos como medio de trasferencia para cumplir con el normar desempeño de las actividades laborales.

Los enlaces datos e internet que utilizan a la fibra óptica como medio de transmisión guiado para integrar la información y el consumo de recursos tecnológicos, se contrata con la Corporación Nacional de Telecomunicaciones CNT-EP como proveedor único. Cabe mencionar que la infraestructura de telecomunicaciones de borde: protocolos de enrutamiento, ancho de banda, enlaces de fibra óptica, IP, es manejada por la CNT.

Figura 9. Se evidencian los principales equipos de comunicación en el centro de datos Matriz de la Agencia Metropolitana de Tránsito y la conexión de sus dependencias.

La Matriz de la Agencia Metropolitana de Tránsito, posee cuartos de equipos ubicados en cada uno de los pisos, los mismos que son conectados a un Centro de Datos principal a través de cableado vertical o (*backbone.* -Columna Vertebral).

La infraestructura de switch de acceso para cada piso es de la marca Cisco modelo SG300- 52MP-K9NA de 48 puertos con excepción de la planta baja que cuenta un modelo SG300- 28MP-K9NA de 24 puertos, para el Data Center poseen varios modelos, pero una sola marca que es la de Cisco, es por ello que es necesario buscar soluciones basadas en la marca mencionada.

En los Centros de matriculación pertenecientes a la Agencia Metropolitana de Tránsito ubicados en diferentes sitios del Distrito Metropolitano de Quito, poseen infraestructura de similares características como se puede evidenciar son: ocho switches de 24 puertos marca cisco modelo SG300- 28MP-K9NA y dos switches de 48 puertos modelo SG300- 52MP-K9NA.

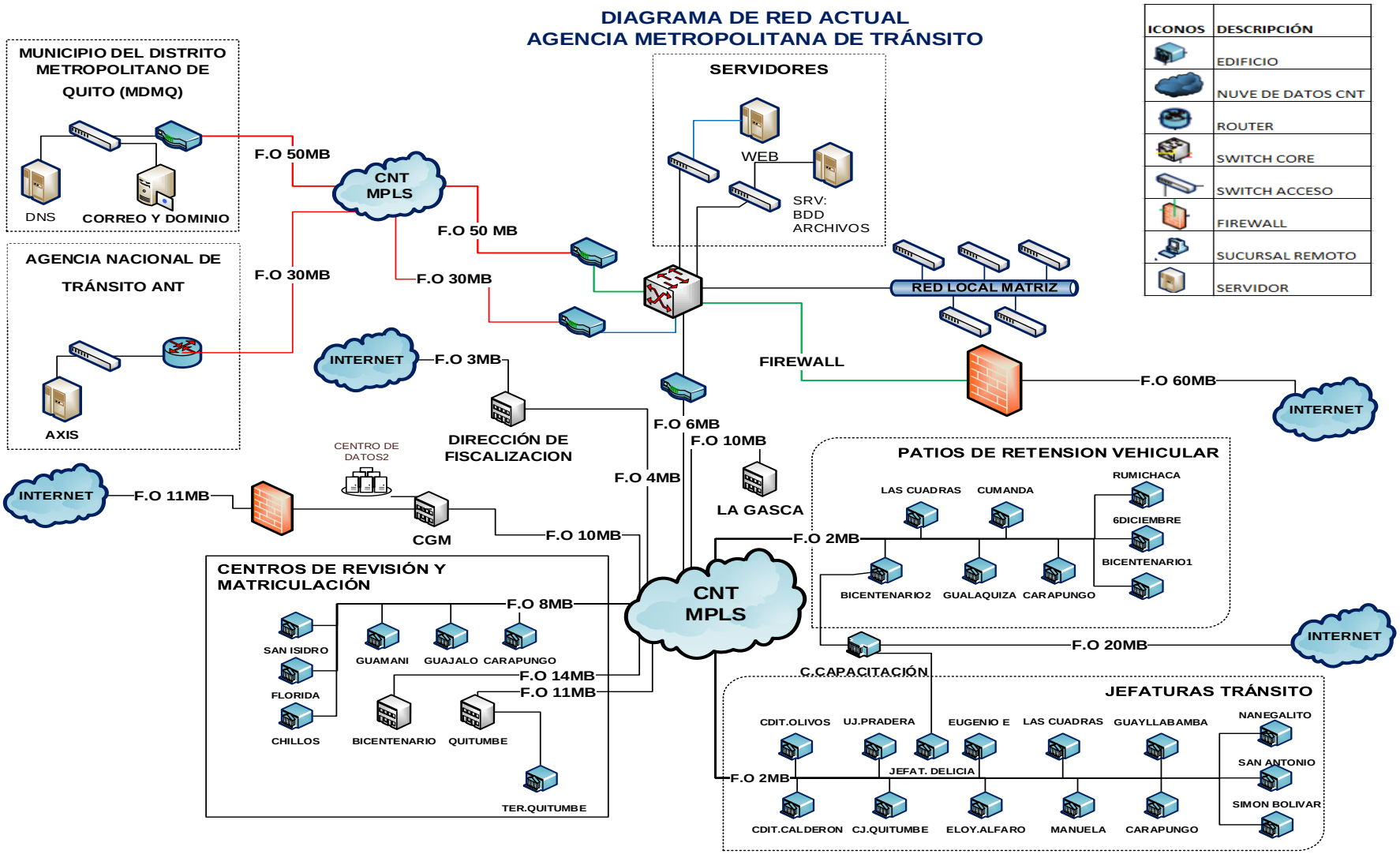


Figura 9. Centro de datos y sus dependencias

3.2. Inventario tecnológico por áreas de la AMT

Para entregar un servicio de calidad a la ciudadanía es importante contar con una infraestructura integra y segura, en la actualidad aún posee dispositivos de comunicación que han sido heredados de la Ex Corpaire, La Agencia Metropolitana de Tránsito por ser una entidad pública paulatinamente ha realizado procesos de adquisición de los equipos según la asignación de presupuesto de cada año, en consecuencia, de esto la actualización tecnología ha seguido a paso lento.

3.2.1. Coordinación de Servicios Ciudadanos

Área encargada de ayudar y guiar a la ciudadanía con trámites en materia de tránsito como son: emisión de salvo conductos (permisos de circulación), multas por medios electrónicos, pagos de infracciones, etc.

En esta área se usa el siguiente software: AS 400, End4sys, Socrit, Avaya Aura, Contac Center, sistemas de turneros.

Tabla 1. Inventario servicios ciudadanos

EQUIPO	CANTIDAD	PUERTOS	UNIDADES
Rack de Pared Abierto	1	N/A	9u
Switch. SG300-28MP-K9NA	1	24Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	3	24	1u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u

3.2.2. Coordinación Administrativa Financiera

El personal que labora en esta área es la encargada de revisar y realizar los diferentes pagos, procesos financieros que tiene la empresa, manejan gran cantidad de información digital ya que todo proceso tiene que ser archivado, adicional utilizan una herramienta de pago e ingreso de bienes llamado SI PARI

que está en red y tiene conexión con el Municipio de Quito a través de un enlace datos.

Tabla 2. Inventario coordinación administrativa Financiera

Rack de Pared Cerrado	1	N/A	12u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	3	24	1u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u

3.2.3. Coordinación de Registro de Infracciones

En esta área se realiza el ingreso de infracciones de tránsito ya sean estas emitidas por boletas físicas y medios electrónicos que se convierten en datos para enviarlos mediante software a la Agencia Nacional de Tránsito (ANT), se usa la plataforma AXIS.

Tabla 3. Inventario Coordinación de Registro de Infracciones

Rack de Pared Cerrado	1	N/A	12u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	2	24	2u
Organizador de Cable Horizontal	2	N/A	2u
PDU	1	8	1u

3.2.4. Coordinación de Seguridad Vial e Ingeniería de Tránsito

Esta área se encarga de capacitar a peatones, conductores y ciclistas sobre seguridad vial, análisis de las zonas con mayor índice de accidentabilidad, realizar estudios técnicos en zonas escolares, corredores viales y sectores con presencia masiva de peatones y conductores. Todo esto con el objetivo de evitar más accidentes en las vías.

Aquí se genera archivos grandes de planos de calles, información de capacitaciones, informes de estados de vías que va a un servidor local de almacenamiento, usan el programa: Arcgis, etc.

Tabla 4. Inventario Coordinación de Seguridad Vial e Ingeniería

Rack de Pared Cerrado	1	N/A	6u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	4	24	4u
Organizador de Cable Horizontal	1	N/A	2u
PDU	1	8	1u

3.2.5. Coordinación Asesoría Legal

Área encargada de ejercer la defensa y el patrocinio judicial de los funcionarios públicos en el ejercicio de sus funciones y en beneficio de la Agencia Metropolitana tránsito, a fin de garantizar los derechos consagrados en la Constitución de la República del Ecuador y demás normativa legal vigente, se usa la plataforma de la Fiscalía General del Estado (FGE).

Tabla 5. Inventario Coordinación Asesoría Legal

Rack de Pared Cerrado	1	N/A	9u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	3	24	3u
Organizador de Cable Horizontal	2	N/A	2u
PDU	1	8	1u

3.2.6. Coordinación de Comunicación Social

Área encargada de comunicación social y estratégica, analizan los mejores métodos para llegar a las personas con campañas de concientización, analizan o discuten los fenómenos sociales relacionados con la información y la comunicación, buscando los medios de difusión masivos más efectivos parar dar a conocer el trabajo que realiza la Agencia Metropolitana de Tránsito.

Esta área utiliza las redes sociales como son Facebook, YouTube WhatsApp, Twitter, etc. Con la finalidad de ver la opinión de la ciudadanía y buscar comunicar una solución u orientación, lo cual demanda la utilización de recursos de red e internet para lograr su objetivo.

Tabla 6. Inventario Coordinación de Comunicación Social

Rack de Pared Cerrado	1	N/A	12u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	2	24	2u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u

3.2.7. Panificación y Compras Públicas

Área encargada de analizar y brindar apoyo en las propuestas de los proyectos de cada unidad requirentes, además de una asesoría legal según los reglamentos vigentes del sistema de contratación pública. usan la plataforma SOCE, SERCOP, módulo USHAY.

Tabla 7. Inventario Panificación y Compras Públicas

Rack de Pared Cerrado	1	N/A	12u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Router Wifi	1	5	N/A
Patch Panel	1	24	1u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u

3.2.8. Coordinación General

Es el área encargada de múltiples funciones como controlar todas las coordinaciones y direcciones de La Agencia Metropolitana Tránsito, representar a la entidad frente a terceros y coordinar todos los recursos a través del

proceso de aprobación, planeamiento, organización y dirección a fin de lograr objetivos establecidos en la planeación anual.

Tabla 8. Inventario Coordinación General

Rack de Pared Cerrado	1	N/A	6u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Router Wifi	1	5	N/A
Patch Panel	1	24	1u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u

3.2.9. Inventario tecnológico consolidado

Tabla1. Se realizó un levantamiento de la infraestructura física en cada coordinación para analizar los equipos y capacidades.

Tabla 9. Consolidado de equipos

Servicios Ciudadanos			
EQUIPO	**CANTIDAD**	**PUERTOS**	**UNIDADES**
Rack de Pared Abierto	1	N/A	9u
Switch. SG300-28MP-K9NA	1	24Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	3	24	1u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u
Coordinación Administrativa Financiera			
Rack de Pared Cerrado	1	N/A	12u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	3	24	1u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u
Coordinación de Registro de Infracciones			
Rack de Pared Cerrado	1	N/A	12u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	2	24	2u
Organizador de Cable Horizontal	2	N/A	2u
PDU	1	8	1u
Coordinación de Seguridad Vial e Ingeniería			
Rack de Pared Cerrado	1	N/A	6u

Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	4	24	4u
Organizador de Cable Horizontal	1	N/A	2u
PDU	1	8	1u
Coordinación Asesoría Legal			
Rack de Pared Cerrado	1	N/A	9u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	3	24	3u
Organizador de Cable Horizontal	2	N/A	2u
PDU	1	8	1u
Coordinación de Comunicación Social			
Rack de Pared Cerrado	1	N/A	12u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Patch Panel	2	24	2u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u
Panificación y Compras Públicas			
Rack de Pared Cerrado	1	N/A	12u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Router Wifi	1	5	N/A
Patch Panel	1	24	1u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u
Coordinación General			
Rack de Pared Cerrado	1	N/A	6u
Switch. SG300-52MP-K9NA	1	48Gigae+2Gigae+2Gigae o SFP	1u
Router Wifi	1	5	N/A
Patch Panel	1	24	1u
Organizador de Cable Horizontal	1	N/A	1u
PDU	1	8	1u

3.2.10.Centro de Datos

La Agencia Metropolitana de Tránsito cuenta con un centro de datos donde se encuentra instalado su infraestructura de red, servidores, equipos de telecomunicaciones, sistema de enfriamiento, etc., mismos que se encuentran bajo la operación y Coordinación de Tecnología de la Información (TIC´s). A continuación, se detallan los equipos existentes:

Tabla2. Se puede observar los equipos, modelos y marcas que maneja la entidad para el respectivo almacenamiento y publicación de servicios, están ubicados en distintos racks desde el 01 hasta el rack 05, no se cuenta con una adecuada etiquetación y organización de equipos.

Tabla 10. Infraestructura Rack1

Nº	NOMBRE	MARCA	MODELO
1	SYSTEM STORAGE	IBM	3,57E+45
2	POWER 7	IBM	8202E4B
3	EXPANSION STORAGE	IBM	-
4	RACK36 UR	IBM	41V0416

Tabla 11. Infraestructura Rack2

Nº	NOMBRE	MARCA	MODELO
1	SERVIDOR ORACLE - SO: ORACLE LINUX SRV	-	CSE-811
2	SERVIDOR DELL POWER EDGE - SO: CENTOS 6,6_GNOME_2,28	DELL	R720XD
3	SERVIDOR DELL POWER EDGE	DELL	R720XD
4	SERVIDOR DELL POWER EDGE	DELL	R720XD
5	SERVIDOR SYSTEM X320 M2 - SO: W2_SRVR_2008_R2	SYSTEM	X3200M2
6	SERVIDOR DELL POWER EDGE	DELL	POWER EDGE R530
7	SERVIDOR DELL POWER EDGE	DELL	POWER EDGE R530
8	MICRO SERVER G8	HP	PROLLANT
9	SERVIDOR HP - SERVIDOR BOSS	HP	PROLIANT DL360P G8
10	POWER EDGE	DELL	R410

Tabla 12. Infraestructura Rack3

Nº	NOMBRE	MARCA	MODELO
1	RACK	-	-
2	SWITCH CORE	CISCO	WS-C4507R+E
3	SWITCH 48 PUERTOS	CISCO	SG300
4	PATCH PANEL 24	R&M	
5	PATCH PANEL 24	R&M	
6	PATCH PANEL 24	PANDUIT	
7	PATCH PANEL 24	PANDUIT	
8	PATCH PANEL 25	PANDUIT	
9	ROUTERS PROVEEDORES	CISCO	

Tabla 13. Infraestructura Rack4

Nº	NOMBRE	MARCA	MODELO
1	IBM SERVER	IBM	BLADE CENTER
2	EXPANSION 0595	IBM	FC0595
3	POWER6_IMB	IBM	8203-E4A
4	IBM	IBM	DS3512
5	ESERVER X SERIES 336	IBM	7310-CR3
6	SLR TAPE IBM - TAPE 520	IBM	SLR 60
7	CONSOLA IBM	IBM	SK-8840
8	SYSTEM STORAGE ULTRIUM 4.TS 3580. IMB	IBM	3580-L43/S43
9	SWITCH 3COM	3COM	3C16794
10	IBM CONSOLE SWITCH	IBM	1735-HC1
11	ESERVER I5 - I SERIES 520	IBM	39J5590
12	TYPE 9406-520	IBM	9406-520
13	IBM RIGHT	IBM	2PH87365
14	IBM RIGHT	IBM	-
15	SYSTEM STORAGE - TS3100	IBM	3573L2U
16	SYSTEM X3550 SRV-127	IBM	7978B1U
17	FIREWALL FORTIGATE 900D	FORTINET	900D
18	SWITCH CISCO 48 PUERTOS	CISCO	S300
19	IBM BREAKER SWITCH	IBM	9306-RTP
20	IBM TOMA 220V	IBM	9306-RTP
21	IBM TOMA 220V	IBM	9306-RTP
22	RACK	-	-

Tabla 14. Infraestructura Rack5

N°	EQUIPO	MARCA	PRODUCTO/MODELO
1	SERVIDOR POWER 8 S.O: IBM V6R1M0	IBM	8286-41A
2	CONSOLA HMC	IBM	7042-CR8
3	FLEX SISTEM ENTERPRISE CHASIS	IBM	8721A1U
4	IBM FLEX SYSTEM X240 COMPUTE NODE, XEON 6C E5-2630V2 80W 2.6GHZ/1600MHZ/15MB, 8GB, O/BAY 2.5IN SAS (SERVIDORES TIPO CUCHILLA 1)	IBM	8737B4U
5	IBM FLEX SYSTEM X240 COMPUTE NODE, XEON 6C E5-2630V2 80W 2.6GHZ/1600MHZ/15MB, 8GB, O/BAY 2.5IN SAS (SERVIDORES TIPO CUCHILLA 2)	IBM	8737B4U
6	IBM FLEX SYSTEM X240 COMPUTE NODE, XEON 6C E5-2630V2 80W 2.6GHZ/1600MHZ/15MB, 8GB, O/BAY 2.5IN SAS (SERVIDORES TIPO CUCHILLA 3)	IBM	8737B4U

7	TAPE LIBRARY (LIBRERÍA DE CINTAS)	IBM	3573-L2U
8	IBM CONSOLA DE ADMINISTRACIÓN IBM	IBM	17238BX
9	IBM STORWIZE V3700 SFF DUAL CONTROL ENCLOSURE (SISTEMA DE ALMACENAMIENTO DE DISCOS)	IBM	2072-24C
10	SWITCH NEXUS 5548 UP CHASIS 32 10GBE PORTS 2 PS 2 FANS	CISCO	NEXUS 5548
11	SWITCH CISCO CATALYST 3650 24 PORT POE 4X1G UPLINK IP BASE	CISCO	CATALYST 3650
12	FIREWALL HARDWARE PLUS 24X7 FORTICARE AND FORTIGUARD UTM BUNDLE	FORTINET	1000C

3.2.11.Sistema de Climatización

Debido a la naturaleza del cuarto de equipos y el espacio reducido la Agencia Metropolita de Transito no cuenta un sistema de enfriamiento de precisión solo posee un sistema de climatización como de detalla a continuación:

- Un aire acondicionado EVERWELL de 60 KBTU.
- Un aire acondicionado LG de 18.000 BTUs.

3.2.12.Sistema de Alimentación Ininterrumpida (Ups)

El sistema de energía regulada es una herencia de la ex-Corpaire este dispositivo tiene 10 años aproximados de uso, es necesario realizar el respectivo informe técnico e iniciar el proceso de baja de UPS.

- UPS MGE SYSTEMS de 30 KVA.
- Tomas eléctricas de 220V y 110 V.
- Tablero de distribución.

Esta infraestructura es de suma importancia para el buen funcionamiento de la Agencia Metropolitana de tránsito, y con el objetivo de prolongar la vida útil de todos equipos pertenecientes a esta institución y tener disponibilidad las 24 horas del día, y los 365 días del año, los sistemas y aplicativos.

3.3. Principales Vulnerabilidades de la Red

En la actualidad existen varios tipos de vulnerabilidades que dependiendo el tipo se aplicará la solución, puesto que existen distintas soluciones. Se puede mencionar los tipos de vulnerabilidades que son:

3.3.1. Entidades y sitios vulnerados

La investigación de la ANT reveló que al sistema ingresaron 99 usuarios no autorizados entre diciembre 2017 hasta enero 2018. El *hackeo* de las cuentas de funcionarios de la entidad permitió la emisión ilegal de 15.970 licencias de conducir. Además, se modificaron 14.583 infracciones y se restituyeron 26.801 puntos (Diario el telégrafo, 2017).

El 10 de abril de 2018. Un grupo de hackers habría borrado el videoclip musical “Despacito”, de Luis Fonsi, de su cuenta de YouTube y habría puesto en su lugar durante unas horas una imagen de los ladrones de la serie de Antena 3 La casa de Papel y habrían escrito *Free Palestine* (en español: Palestina Libre) debajo de los vídeos, de forma que no se podía ver ni escuchar el tema más visto de esta plataforma, que acumula más de 5.000 millones de reproducciones.

Muchos de los ataques son basados en los errores fundamentales de sistemas, afectando a los enrutadores y protocolos que se usan para transmitir o recibir cualquier dato saliente sin saber cuál es su propósito en la red.

En internet y las redes de todo el mundo se generan nuevos ataques según investigaciones en menos de 10 horas un hacker puede ingresar a un sistema en algunos casos tan solo les basta una hora y en la mayoría de los casos no son detectados por las infraestructuras empresariales. Cada hora se genera un nuevo virus o ataques distintos, por esta razón es posible acercarse a un nivel de seguridad alto, pero no totalmente absoluto.

3.3.2. Políticas de seguridad

Las políticas de seguridad en una entidad son para establecer parámetros formales de conexión entre usuarios internos y externos, identificar y resguardar los puntos de protección, implementar la arquitectura y topología de red, con el fin de mejorar el sistema de seguridad informática y gestión de la AMT.

3.3.3. Lista de dispositivos vulnerables

La primera acción que se debe tomar en cuenta para el desarrollo de políticas de seguridad es contar con una lista donde refleje los elementos a proteger. Los aspectos a considerar son los siguientes:

3.3.3.1. Datos

Los datos en línea, almacenados fuera de línea, durante la ejecución, almacenado, bases de datos, cuando se transmite sobre los medios físicos de comunicación. No existe el respaldo al 100% de los datos o configuraciones de equipos.

3.3.3.2. Dispositivos

Enrutadores, conmutadores, servidores de acceso remoto, máquinas virtuales, computadoras, tarjetas, terminales, impresoras, unidades de almacenamiento, líneas de comunicación.

3.3.3.3. Programas

La Agencia Metropolitana tiene un aproximado de veinte aplicativos que sirven para la extracción de datos y proceso de los mismos, con el fin de brindar un servicio eficiente y eficaz a la ciudadanía.

Tenemos: el historial de revisión, cita previa, formulario de capacitación de seguridad vial, aplicativos taxis, zona azul, aplicativo de patios, exonerados, movilidad mal parqueado, movilidad pico y placa, operativos revisión técnica vehicular, web service AMT, creación de órdenes de pagos, calificación de taxis por web, aplicativo móvil de taxis, aplicativos de reportes y administradores de patios.

Además de los programas existentes y las utilidades de cada uno de ellos, se cuenta con programas como: el PRTG, sistemas operativos win7, programas de comunicaciones entre otros aplicativos.

3.3.3.4. Personas

No existen mecanismos o procesos de control de acceso, para el personal externo que utilizan servicios locales, debido a la falta de control los funcionarios son propensos a ser víctimas de ataques maliciosos y en el peor de los casos que un dispositivo tecnológico sea hurtado, lo cual pondría en peligro la base de datos ya que esta utiliza una conexión mediante telemetría a los aplicativos de Agencia Metropolitana de Tránsito.

3.3.3.5. Documentación

La Agencia Metropolitana de Tránsito al poseer la responsabilidad de controlar la seguridad vial y sancionar amparados en los artículos vigentes que están establecidos en el COIP en el capítulo de Tránsito, es importante identificar de quien se debe proteger estos documentos y vigilar la custodia de los mismos.

3.3.4. No existen establecidas responsabilidades

En La Agencia Metropolitana de Tránsito no está definido quien puede realizar y quien no una determinada actividad o función, es importante señalar las

responsabilidades y procesos de cada participante en la red según el cargo que desempeñe en esta entidad pública.

3.3.5. Conexiones remotas en dispositivos

La Agencia Metropolitana de Tránsito utiliza el acceso remoto en soporte al usuario en las dependencias alejadas y para conectar dispositivos que están en la vía para realizar operativos vehiculares, control de velocidad con radares todo esto a través de internet o Telemetría. El acceso remoto consiste en acceder a una computadora a través de otra diferente. De este modo, las acciones que se llevan a cabo en una computadora también se ejecutan en la otra.

3.3.5.1. Enlaces de internet a través de módem

La Agencia Metropolita de Tránsito a través de Proveedores de Servicio de Internet (ISP), en este caso el proveedor es CNT-EP (Corporación Nacional de Telecomunicaciones Empresa Pública) generalmente entrega una dirección IP pública para el acceso a internet mediante esta pueden enviar paquetes de cualquier dirección IP, cuando se quiere el ingreso para que varias máquinas a través de un enlace.

3.3.5.2. Acceso a servidores

Se tiene servidores que necesitan ser ingresados desde el exterior o *internet* hacía una red local o *intranet, c*on frecuencia esto se da cuando tenemos una sola dirección IP pública, si se sobrepone el destino de los paquetes que ingresan esto es posible.

3.3.5.3. Traducción de Direcciones de Red Solapamiento

Es el más común ya que es usado para entregar el acceso a servicios institucionales, a los Centros de Matriculación que no están dentro de los estándares de red del Municipio del Distrito Metropolitano de Quito (MDMQ), su funcionamiento consiste asignar una sola IP del grupo de IP´s de la red estándar para permitir el acceso a telefonía, internet y correo a varias direcciones IP´s privadas de la red 192.168.0.0.

3.4. Análisis de Configuración

Aquí se buscará chequear las configuraciones existentes en los dispositivos de red y detectar falencias en su operación o configuración, si se están cumpliendo los parámetros de seguridad ya que se ha detectado que un 50% de fallos en los dispositivos es por la mala manipulación o el desconociendo de usuarios internos de la red porque no están sujetos a procesos internos de uso de dispositivos informáticos.

3.4.1. Conmutador de acceso

En la matriz de la Agencia Metropolitana de Tránsito existen 08 switch de acceso que corresponden a los distintos departamentos de la agencia donde están conectados los dispositivos terminales como computadoras, impresoras, biométricos, puntos de acceso, turneros, teléfonos IP, etc.

Figura 10. El switch de acceso SW1-P7 del Área de Comunicación Social tomado como referencia se ha detectado que no posee restricciones de seguridad de ningún tipo en los 48 puertos.

```
interface gigabitethernet2
spanning-tree portfast
switchport mode access
!
interface gigabitethernet45
spanning-tree portfast
switchport mode access
switchport access vlan x
!
interface gigabitethernet51
!
interface gigabitethernet52
 ip dhcp snooping trust
 switchport trunk allowed vlan add A,B,C,D


SW1-P7#show ports security GigabitEthernet 45

Port        status      Learning     Action     Maximum   Trap     Frequency
---------  ---------  ------------ ----------- --------- --------  ----------
gi45       Disabled       Lock              -         1         -          -

SW1-P7#show ports security GigabitEthernet 52

Port        status      Learning     Action     Maximum   Trap     Frequency
---------  ---------  ------------ ----------- --------- --------  ----------
gi52       Disabled       Lock              -         1         -          -
```

Figura 10. Configuración puertos

Según lo mostrado en la figura 9., este descuido de seguridad puede generar inconvenientes en la red ya que al no existir restricción en el puerto cualquier persona puede usar cable de red y conectar un dispositivo para tener el acceso a nuestra infraestructura.

Con el fin de agregar dispositivos a la red, se ha detectado que los usuarios conecten router wifi, switch o conmutador en puertos que fueron habilitados para una estación de trabajo, esto causa reducción en el rendimiento de la capacidad de la red por que se generan loop lógicos que provocan perdida en la disponibilidad de red.

3.4.2. Conmutador de distribución

Después de analizar la configuración de los switches o conmutadores de distribución se puede concluir que estos dos equipos no está realizando esta función, esta capa debe proveer ruteo, filtrado, acceso a la red WAN y determinar que paquetes deben llegar al switch Core. Además, definir cuál es la forma más rápida de responder a los requerimientos de red.

Los equipos están actuando como switch de acceso conectados directamente al conmutado de Core para proveer de la conexión a un grupo de servidores IMB y conexión al firewall.

3.4.3. Conmutador de núcleo

En el análisis de la configuración se encontró que los puertos no tienen protección que limite la comunicación con equipos ajenos, (los mismos que se resaltaran de color amarillo), otro de los inconvenientes es el uso del conmutador de núcleo como un switch de distribución es importante dividir estas funciones en otro switch, para que el switch de núcleo se encargue de conmutar el tráfico a mayor velocidad y pueda llevar grandes cantidades de información de manera confiable con esto se mejorará el factor latencia y la velocidad.

```
SWCORE-SM#sh run
Building configuration...

Current configuration : 19028 bytes
!
! Last configuration change at 23:15:48 UTC Sun Nov
4 2018 by admin
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!


hostname SWCORE-SM
!
boot-start-marker
boot system bootflash:cat4500es8-
universal.SPA.03.09.00.E.152-5.E.bin


boot-end-marker
!
!
vrf definition mgmtVrf
 !
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
!
enable secret
!
username admin privilege 15 password 0
no aaa new-model
clock timezone UTC -8 0
hw-module module 1 mode 1
hw-module module 2 mode 1
!
ip domain-name
!
vtp mode transparent
!
power redundancy-mode redundant
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
redundancy
 mode sso
 main-cpu
  auto-sync startup-config
!
vlan internal allocation policy ascending
!
vlan
 name DMDTM
!
vlan
 name AMT
!
vlan
 name FIX-CRTV
!
vlan
 name TELCO-Rapipagos
!
vlan
 name CNT-Fotomultas
!
vlan
 name CNT-ANT
!
```

```
vlan
 name CNT-CMV
!
vlan
 name CNT-DMI
!
vlan
 name TELCO-PACIFICO
!
vlan
 name LAN2.VALDERRAMA
!
vlan
 name Management
!
vlan
!
interface Loopback1
 ip address ...255.255.255.0
!
interface FastEthernet1
 vrf forwarding mgmtVrf
 no ip address
 speed auto
 duplex auto
!
interface TenGigabitEthernet1/1
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet1/2
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet1/3
 description backup DMI
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet1/4
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet1/5
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet1/6
 description CONEXION-DMI_AMT
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet1/7
 switchport access vlan
!
interface TenGigabitEthernet1/8
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet1/9
 switchport mode access
!
interface TenGigabitEthernet1/10
!
interface TenGigabitEthernet1/11
 description SRV-WEB-ALCO
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet1/12
 description Conexion con Fotomultas
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/13
!
interface GigabitEthernet1/14
!
interface GigabitEthernet1/15
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/16
 description conexion NAT CGM-AMT-ANT
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/17
 description Conexion-Axis Cloud
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/18
!
interface GigabitEthernet1/19
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/20
 description Freddy Cuyo
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/21
 description WIRELESS-ALCO
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/22
 description SRV-ORACLE-LINUX-ALCO
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/23
 switchport access vlan
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/24
 description Enlace_ANT
 switchport trunk allowed vlan ,
 switchport mode trunk
 shutdown
!
interface GigabitEthernet1/25
 description AXIS-CLOUD
 switchport trunk allowed vlan
 switchport mode trunk
!
interface GigabitEthernet1/26
!
interface GigabitEthernet1/27
!
interface GigabitEthernet1/28
!
interface GigabitEthernet1/29
!
interface GigabitEthernet1/30
!
interface GigabitEthernet1/31
!
interface GigabitEthernet1/32
 description SWR-Dominio
!
interface GigabitEthernet1/33
!
```

```
interface GigabitEthernet1/34
!
interface GigabitEthernet1/35
!
interface GigabitEthernet1/36
!
interface GigabitEthernet1/37
!
interface GigabitEthernet1/38
 description CMV_Quitumbe
 switchport trunk allowed vlan -
 switchport mode trunk
!
interface GigabitEthernet1/39
 description Alchodetectores
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/40
!
interface GigabitEthernet1/41
!
interface GigabitEthernet1/42
!
interface GigabitEthernet1/43
 !
interface GigabitEthernet1/44
 description Conexion Bnk-pacifico
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/45
!
interface GigabitEthernet1/46
!
interface GigabitEthernet1/47
 description POWER6 T3-LINK5
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet1/48
!
interface TenGigabitEthernet2/1

 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet2/2

 switchport access vlan
!
interface TenGigabitEthernet2/3
!
interface TenGigabitEthernet2/4
!
interface TenGigabitEthernet2/5
!
interface TenGigabitEthernet2/6
!
interface TenGigabitEthernet2/7
!
interface TenGigabitEthernet2/8
!
interface TenGigabitEthernet2/9
!
interface TenGigabitEthernet2/10
!
interface TenGigabitEthernet2/11
!
interface TenGigabitEthernet2/12
 description ENLACE TRONCAL SW1.P1
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/13
 description ENLACE TRONCAL SW1.P2
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/14
 description ENLACE TRONCAL SW2.P2
 switchport mode trunk
 switchport nonegotiate
 ip dhcp snooping trust
!
interface GigabitEthernet2/15
 description ENLACE TRONCAL SW3.P2
 switchport trunk native vlan
 switchport mode trunk
 ip arp inspection trust
 speed 1000
 duplex full
 ip dhcp snooping trust
!
interface GigabitEthernet2/16
 description ENLACE TRONCAL SW4.P2
 switchport trunk native vlan
 switchport mode trunk
 ip arp inspection trust
 speed 1000
 duplex full
 ip dhcp snooping trust
!
interface GigabitEthernet2/17
 description ENLACE TRONCAL SW5.P2
 switchport trunk native vlan
 switchport mode trunk
 ip arp inspection trust
 speed 1000
 duplex full
 ip dhcp snooping trust
!
interface GigabitEthernet2/18
 description ENLACE TRONCAL SW1.P3
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/19
 description ENLACE TRONCAL SW1.P4
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/20
 description ENLACE TRONCAL SW1.P5
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/21
 description ENLACE TRONCAL SW1.P6
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/22
 description ENLACE TRONCAL SW1.P7
```

```
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/23
 description ENLACE TRONCAL SW1.P9
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/24
 description ENLACE TRONCAL SW1.P11
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet2/25
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/26
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/27
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/28
 switchport mode access
!
interface GigabitEthernet2/29
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/30
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/31
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/32
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/33
 switchport mode access
!
interface GigabitEthernet2/34
 description Monitoreo
 switchport mode access
!
interface GigabitEthernet2/35
!
interface GigabitEthernet2/36
!
interface GigabitEthernet2/37
!
interface GigabitEthernet2/38
!
interface GigabitEthernet2/39
!
interface GigabitEthernet2/40
!
interface GigabitEthernet2/41
!
interface GigabitEthernet2/42
!
interface GigabitEthernet2/43
 description BiciQuito
!
interface GigabitEthernet2/44
 description groman-p
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/45
 description VOZ-19 Pruebas
 switchport access vlan
 switchport mode access
!
interface GigabitEthernet2/46
 description AZAMBONINO
 switchport access vlan
 switchport mode access
 switchport port-security maximum 4
!
interface GigabitEthernet2/47
!
interface GigabitEthernet2/48
 description PC-srv-Ruben
 switchport access vlan
 switchport mode access
!
interface TenGigabitEthernet3/1
!
interface TenGigabitEthernet3/2
!
interface TenGigabitEthernet3/3
!
interface TenGigabitEthernet3/4
!
interface TenGigabitEthernet3/5
!
interface TenGigabitEthernet3/6
!
interface TenGigabitEthernet3/7
!
interface TenGigabitEthernet3/8
!
interface TenGigabitEthernet4/1
!
interface TenGigabitEthernet4/2
!
interface TenGigabitEthernet4/3
!
interface TenGigabitEthernet4/4
!
interface TenGigabitEthernet4/5
!
interface TenGigabitEthernet4/6
!
interface TenGigabitEthernet4/7
!
interface TenGigabitEthernet4/8
!
interface Vlan
 description Red Local
 ip address 192...255.255.255.0
!
interface Vlan
 description GW-DMDTM
 ip address 172...255.255.255.0
!
interface Vlan
 description GW-AMT
 ip address 172...255.255.255.0
!
interface Vlan
 description ENLACE-AMT-CRTV
 ip address 10.100.200.9 255.255.255.248
```

```
!
interface Vlan
 description CONEXION-WAN-R-ANT
 ip address 192...255.255.255.248 secondary
 ip address 192...255.255.255.0
 no ip redirects
!
interface Vlan
 description CONEXION CA-CNT_R1941
 ip address 192...255.255.255.0
!
interface Vlan
 description CONEXION-DMI
 ip address 172...255.255.255.0
 ip access-group Vlan7-Block-dhcp in
 no ip redirects
!
interface Vlan
 description GW-BCO-PACIFICO
 ip address 10...255.255.255.248
!
interface Vlan
 description LAN2-VAL
 ip address 172...255.255.255.0
!
interface Vlan
 ip address 192...255.255.255.0
!
interface Vlan
 ip address 192...255.255.255.0
```

Analizando esta parte de la configuración se puede evidenciar la excesiva creación de rutas estáticas en total son 94 líneas de código (señaladas con resaltador amarillo), que se muestra a continuación del párrafo. Este tipo de errores representa para el conmutador el uso de recursos y procesamiento innecesario que se puede mejorar con otro tipo de solución de enrutamiento.

```
ip forward-protocol nd
ip http server
ip route 0.0.0.0 0.0.0.0 172...
ip route 10...255.255.255.255 192...
ip route 10...255.255.255.255 192...name WEBSERVICE-SRI-ANT
ip route 10...255.255.255.255 10...
ip route 10...255.255.255.255 10...name SRV-bnk-Pacifico
ip route 10...255.255.255.0 192...name CA-rANT-CTE
ip route 10...255.255.255.0 192...name ALEGRO-GPRS
ip route 10...255.255.255.0 192...name AMT-CNT-movil-HH
ip route 10...255.255.255.0 192...name AMT-CNT-movil-HH2
ip route 10...255.255.255.0 192...name AMT-CNT-movil-HH3
ip route 10...255.255.255.0 192...name CHIPS-AMT-AS400
ip route 10...255.255.255.0 192...name CHIPS2-AMT-AS400
ip route 10...255.255.255.0 192...name CA-rANT-CTE
ip route 10...255.255.255.255 192...name ServerCTE
ip route 10...255.255.255.0 172...name AMT-AXISCLOUD-NAT
ip route 162...255.255.255.252 192...name ALEGRO-W1
ip route 172...255.240.0.0 172...
ip route 172...255.255.255.0 192...name PRUEBAS-ICAM
ip route 172...255.255.255.255 172...name TT-Quitumbe
ip route 172...255.255.252.0 192...name Servidor-SitCom-rANT
ip route 172...255.255.252.0 192...name Segunda-Red-ANT
ip route 172...255.255.255.0 192...name Red-DMI
ip route 172...255.255.255.0 172...name Red-Municipio-Alcaldia
ip route 172...255.255.255.0 192...name AXIS-LAN1-ANT
ip route 172...255.255.255.255 172...name TT-Carcelen
ip route 172...255.255.255.0 192...name MAT-FLORIDA-CNT
ip route 172...255.255.255.0 192...name MAT-GUAMANI
ip route 172...255.255.255.0 192...name MAT-SAN-ISIDRO-CNT
ip route 172...255.255.255.0 192...name MAT-CHILLOS-CNT
```

ip route 172...255.255.255.0 192...name MAT-CARAPUNGO-CNT
ip route 172...255.255.255.0 192...name MAT-GUAJALO-CNT
ip route 172...255.255.255.0 172...name MAT-Quitumbe
ip route 172... 255.255.255.0 192...name MAT-Aeropuerto
ip route 172...255.255.255.0 192...name AMT-LA-GASCA
ip route 172...255.255.255.192 192...name CR-NANEGALITO
ip route 172...255.255.255.192 192...name JZ.SIMON-BOLIVAR
ip route 172...255.255.255.192 192...name JzManuelas
ip route 172...255.255.255.192 192...name JzEloyA
ip route 172...255.255.255.192 192...name CR-SAN.ANTONIO
ip route 172...255.255.255.0 192...name PrvBicentenario2
ip route 172...255.255.255.192 192...name FlAgQuitumbe
ip route 172...255.255.255.192 192...name S18_Dop.Transporte
ip route 172...255.255.255.192 192...name S18_BiciQuito
ip route 172...255.255.255.192 192...name S15_PRV.6DICMB-CEDROS
ip route 172...255.255.255.192 192...name S15_PRV.GUALAQZ
ip route 172...255.255.255.192 192...name S15_PRV.MATD-ALVARZ
ip route 172...255.255.255.192 192...name S15_PRV.RUMICHAC
ip route 172...255.255.255.192 192...name S15_TER.RIOCOCA
ip route 172...255.255.255.192 192...name S15_PRV.Gral_RUMINIAH
ip route 172...255.255.255.192 192...name S15_PRV.LA-Y
ip route 172...255.255.255.192 192...name S15_TER.QUITUMBE
ip route 172...255.255.255.192 192...name S15_TER.CARCELEN
ip route 172...255.255.255.192 192...name S15_TER.OFELIA
ip route 172...255.255.255.192 192...name S15_TER.MARIN
ip route 172...255.255.255.192 192...name S15_PRV-CARAPUNGO
ip route 172...255.255.255.192 192...name S15_PRV.GUAMANI
ip route 172...255.255.255.192 192...name S15_CA.PRADERA
ip route 172...255.255.255.192 192...name S15_CDC.CALDERON
ip route 172...255.255.255.192 192...name S15_TROB.M_AMBROSI
ip route 172...255.255.255.192 192...name S15_J.EUG-ESPEJO
ip route 172...255.255.255.192 192...name S15_JEFARUTA-PENDIENT
ip route 172...255.255.255.192 192...name S15_J.CHILLOS
ip route 172...255.255.255.192 192...name CR-GUAYLLAMBA
ip route 172...255.255.255.0 192...name S16_FiscT-PUBLICO
ip route 172...255.255.255.0 192...name S16_DO-FotoMulta
ip route 172...255.255.255.0 192...name S16_LAN2-tQuitumbe
ip route 172...255.255.255.0 192...name AXIS-LAN2-AMT
ip route 172...255.255.255.0 192...name LAN2-CGM
ip route 172...255.255.255.0 192...name S15_CDI.OLIVOS
ip route 172...255.255.0.0 172...
ip route 172...255.255.255.255 192...name Router-DMI-Access
ip route 172...255.255.255.252 192...name ALEGRO-W2
ip route 192...255.255.255.0 172...name AMT-AXISCLOUD2
ip route 192...255.255.255.0 172...name AMT-AXISCLOUD
ip route 192...255.255.255.0 192...name red-FotoMultas
ip route 192...255.255.255.0 192...name correo_ant
ip route 192...255.255.255.0 192...name red-ope-fotomultas
ip route 192...255.255.255.0 192...name MAT-GUAJALO-rCNT
ip route 192...255.255.255.0 192...name MAT-CHILLOS-rCNT
ip route 192...255.255.255.0 192...name MAT-SAN-ISIDRO-rCNT
ip route 192...255.255.255.0 192...name MAT-FLORIDA-rCNT
ip route 192...255.255.255.0 192...name MAT-CARAPUNGO-rCNT
ip route 192...255.255.255.0 192...name Mat-Guamani
ip route 192...255.255.255.0 192...name CGM-CNT-AMZ

```
ip route 192...255.255.255.0 10...name CRTV-GUAMANI-FIX
ip route 192...255.255.255.0 10...name CRTV-SANISIDRO-FIX
ip route 192...255.255.255.0 10...name CRTV-CHILLOS-FIX
ip route 192...255.255.255.0 10...name CRTV-CARAPUNGO-FIX
ip route 192...255.255.255.0 10...name CRTV-GUAJALO-FIX
ip route 192...255.255.255.0 10...name CRTV-FLORIDA-FIX
ip route 192...255.255.255.255 192...name SRV-Rapipagos3
ip route 192...255.255.255.255 192...name SRV-Rapipagos
ip route 192...255.255.255.255 192...name SRV-Rapipagos2
ip route 192...255.255.255.0 192...name Vradar

ip access-list extended Vlan-Block-dhcp
 deny   ip host 172...any
 permit ip any any
ip access-list extended acceso-fixCRTV-Power
 permit ip ...0 0.0.0.255 host 172...
 permit ip ...0 0.0.0.255 host 172...
 permit ip ...0 0.0.0.255 host 172...
 permit ip ...0 0.0.0.255 host 172...
 permit ip ...0 0.0.0.255 host 172...
 permit ip ...0 0.0.0.255 host 172...
!
ip sla enable reaction-alerts
!
snmp-server community public RO
!
banner login ^CC
^C
!
line con 0
 privilege level 15
 password
 logging synchronous
 login
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 password
 logging synchronous
 login local
line vty 5 15
 privilege level 15
 password
 logging synchronous
 login local
 no exec
!
end
SWCORE-SM#
```

3.5. Resumen de los hallazgos

Se realiza la agrupación de acuerdo a su afinidad o relación para identificar y resumir todas falencias que existen en los distintos participantes o usuarios de red que tiene la Agencia Metropolitana de Transito y en algunos casos la administración es compartida con el Municipio del Distrito Metropolitano Quito.

3.5.1. Usuarios

Los usuarios de perfiles de navegación o los operadores técnicos de sistemas y equipos informáticos tienen descuidos que pueden perjudicar a la entidad por el mal uso de los mismos.

La Tabla 15. Muestra algunos de los usuarios de los diferentes programas que presentan problemas en su operación diaria.

Tabla 15. Tipos de usuarios de red vulnerables

Usuarios	Localidad	Vulnerabilidades	
		Física	Lógica
Perfil active	Matriz AMT	Se debe adquirir o configurar un servidor de correo	La administración de usuarios no es permitida a nuestros técnicos.
Perfil PRG	Matriz AMT	Se debe migrar de la PC a un servidor o máquina virtual	No hay perfiles de operadores. No existe cronograma de respaldos.
Usuario, switch y router	Matriz y dependencia de la AMT	No existe una base de datos segura para almacenar usuarios y contraseñas	No hay perfiles de operadores. No existe cronograma de respaldos.
Claves usuarios	Matriz y dependencia de la AMT	Anotan las claves en sitios visibles al público	Las claves no son fuertes. Se comparten las claves. Anotan las claves en lugares visibles

3.5.2. Equipos de comunicaciones

Estos equipos tienen la responsabilidad de tener disponible la conexión entre usuarios de la Agencia Metropolita de Tránsito y las dependencias desconcentradas de la AMT, si cualquiera de estos equipos pierde conectividad dependiendo de la capa en la que se encuentre, se reflejara en la cantidad de usuarios afectados.

La Tabla 16. Se ha escogido las vulnerabilidades más relevantes que afectan a la operatividad directa de los dispositivos de red.

Tabla 16. Equipos y vulnerabilidad

Equipos	Localidad	Vulnerabilidades		
		Física	Enlace	Red
Switch Principal	Matriz AMT	No tiene organizado las conexiones. El rack no está cerrado.	No existe una segmentar por VLAN	La vlan1 está activada y difundida en todos los puertos
Router de la red	Matriz AMT	No ha realizado mantenimiento El rack no está cerrado. Existen muchos routers.	No se sabe que configuración sirve se debe depurar configuración. Los routers de borde no pertenecen a la AMT.	Las contraseñas para el acceso no pertenecen a la AMT
Switch de armario	Matriz AMT	No se ha coordinado realizar mantenimientos	No existe seguridad en los puertos	No tiene seguridad en los puertos
Servidores	Matriz AMT	No se ha ejecutado mantenimiento	Existen máquinas virtuales con Windows XP. No se sabe cuál está operativo o en funcionamiento.	No tiene un método de prevención de intrusos Tienen puertos abiertos
Firewall Fortinet	Matriz AMT	No tiene identificación de puertos. El rack no está cerrado.	Verificar políticas y proxy	Existen puertos abiertos

Servidores DNS	Matriz MDMQ	No posee administración física	No existe administración de las configuraciones en la AMT	La conexión hacia el servidor es a través de MPSL de CNT con rutas estáticas
Servidores DHCP	Matriz MDMQ	No posee administración física	No existe administración de las configuraciones en la AMT	Las contraseñas para el acceso no pertenecen a la AMT
Servidor de correo electrónico	Matriz MDMQ	No posee administración física	No existe administración de las configuraciones en la AMT	La conexión hacia el servidor es a través de MPSL de CNT con rutas estáticas
Servidor de active	Matriz MDMQ	No posee administración física	No existe administración de las configuraciones en la AMT	La conexión hacia el servidor es a través de MPSL de CNT con rutas estáticas
Computadoras	Matriz y dependencias de la AMT	No existen mantenimientos programados	Falta licencias de programas Antivirus configurado con reglas de conexión.	No se tiene un registro de las Mac address

3.5.3. Sucursales

Estos lugares remotos como jefaturas y circuitos son encargados de realizar documentos llamados partes de accidentes de tránsito, estos archivos son importantes ya que brinda la información delicada en la apertura de procesos en el caso de existir acciones legales en los accidentes, los mismos que a través de la red son almacenados en la Matriz y en algunos casos de forma local, además todas las sucursales utilizan los servicios institucionales correo e internet. Todas las dependencias se conectan por medio de enlaces de datos por fibra óptica hacia la Matriz.

La Tabla 17. Recolecta las debilidades que se presentan en la infraestructura de algunas dependencias, por ello es importante la adquisición de equipos para ayudar a la protección de accesos no deseados.

Tabla 17. Vulnerabilidades de las sucursales

Dependencia	Localidad	Vulnerabilidades	
		Físicas	Lógicas
Jefatura Zonal Eloy Alfaro	Eloy Alfaro	Los Equipos no tiene protección de rack cerrado. No existe switch Capa 2 para usar como switch de acceso. No existe ventilación No existe mantenimiento	No existe el equipo adecuado para la configuración de restringir puertos
Jefatura Zonal Eugenio Espejo	Eugenio Espejo		
Jefatura Zonal Manuela Sáenz	Manuela Sáenz		
Jefatura Zonal Calderón	Calderón		
Circuito Rural San Antonio	San Antonio		
Circuito Rural Simón Bolívar	Simón Bolívar		
Circuito Rural Guayllabamba	Guayllabamba		
Los Olivos	Cipreses		
Transportes AMT	Ponciano		
Trolebús	Manuel Ambrosi		
Patios de Retención Vehicular Las Cuadras	Frente a parque Fundeportes		
Patios de Retención Vehicular Cumanda	Parque Cumandá		
Patios de Retención Vehicular Rumichaca	Frente al parque las Cuadras		
Patios de Retención Vehicular Gualaquiza	Cabecera norte parque Bicentenario		
Patios de Retención Vehicular 6 de Diciembre	Galo plaza y 6 de diciembre		
Patios de Retención Vehicular Carapungo	Vía Marianitas		
Terminal Rio Coca	Micro Terminal terrestre Rio Coca		
Terminal Marín	Micro terminal terrestre El Playón		
Centro de Gestión de la Movilidad CGM	Instalaciones de la EPMMOP	No existe accesos en horarios fuera de oficina	No existen seguridades de puerto en los switch. No existe VLAN de monitoreo

3.5.4. Servicios

Los servicios que son usados por la Agencia Metropolitana de Tránsito en su mayoría son administrados por la Dirección Metropolitana de Informática del Municipio de Quito - DMI esto se debe a que la AMT no tiene infraestructura

física para alojar servicios. En los primeros años de operaciones laborales de la AMT estos servicios eran considerados como algo secundario.

Pero a medida que la institución fue creciendo: en número de contrataciones de personal, las funciones adquiridas para el control de tránsito, la creación de nuevos aplicativo y apertura de más dependencias.

Es una necesidad el poder administrar todos estos servicios y brindar operatividad en las actividades laborales. En casos de servicios puntuales como son el correo electrónico, DNS, DHCP y active directory. Se podría mejorar tiempos de respuesta en los incidentes dependiendo la complejidad.

La Tabla 18. Reúne los servicios básicos para que la Agencia Metropolitana de Tránsito pueda trabajar con normalidad y los errores de programación que afectan directamente a la seguridad de base de datos.

Tabla 18. Vulnerabilidad en servicios

Servicios	**Localidad**	**Vulnerabilidades**	
		Física	**Lógica**
Servicio DNS	Matriz MDMQ	No existe un servidor físico que pertenezca a la AMT	No existe administración de la AMT. No se puede brindar pronta atención a incidentes referente al servidor.
Servicio DHCP	Matriz AMT	No existe un servidor físico que pertenezca a la AMT	No existe administración de la AMT. No se puede brindar pronta atención rápida a incidentes referente al servidor. Entrega IP´s repetidas
Servicio de correo electrónico	Matriz MDMQ	No existe un servidor físico que pertenezca a la AMT	No existe administración de la AMT. El servidor se desconecta

Servicio de active	Matriz AMT	No existe un servidor físico que pertenezca a la AMT	No existe administración de la AMT. No se puede asignar los perfiles a los usuarios
Bases de datos	Matriz AMT	No existen mantenimientos periódicos	No se ha depurado y encriptado las contraseñas usuarios administrador en programas que usan la base de datos
Programas	Matriz AMT	No existe mantenimientos periódicos	No existe un estándar definido del software. No se ha puesto en práctica códigos o procedimientos de programación seguridad. No posee licenciamiento actualizado
Servicio antivirus	Matriz AMT	No existe mantenimientos periódicos	Falta configurar las reglas en cada dispositivo. No se agregado todas las nuevas Redes a los grupos de confianza
Servicio Axis	Matriz ANT	No existe un servidor de supervivencia local en el caso de que el servidor en la ANT falle	Se desconecta con mucha frecuencia Posee intermitencia

Basándose en los hallazgos se puede concluir que la seguridad que se ha implementado desde la adquisición de competencias del control de tránsito y seguridad vial haciende a tan solo el 60%, ya que existe vulnerabilidad, aunque se vean como descuidos pequeños o falta de equipos esto representa un crecimiento exponencial en la inseguridad en una entidad pública como es La Agencia Metropolitana de Tránsito.

3.6. Herramienta de análisis

¿Por qué hacer un análisis de vulnerabilidades?

Para evaluar riegos y proporcionar orientación para los controles de seguridad en los diferentes equipos, servidores, servicios, aplicativos etc.

Para el análisis de vulnerabilidades en la Agencia Metropolitana de Transito se utilizó el programa Nessus, el cual es un escáner de vulnerabilidades herramienta de seguridad en redes y ayuda a prevenir eficientemente los ataques de red detecta debilidades y errores de configuración.

Con el análisis se pretende mostrar que dispositivos requieren de una intervención en cuanto a las vulnerabilidades encontradas se determinará los métodos de mitigación para las debilidades de seguridad.

3.6.1. Análisis de switch Core

Cuadro total de vulnerabilidades de servidor de archivos y equipos de telecomunicaciones. Cada color tiene un significado: rojo = crítico, naranja = alta, amarillo=medio, verde=baja y azul= informativo.

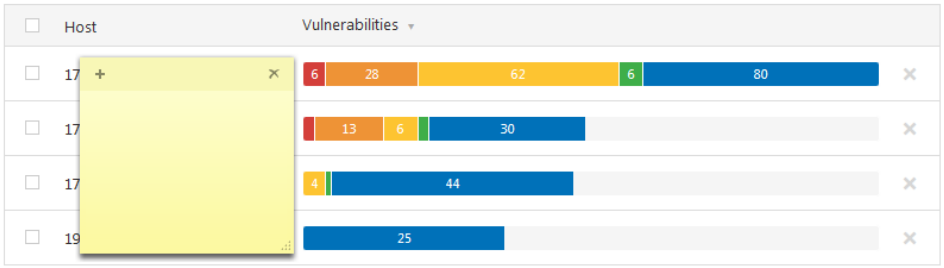


Figura 11. Resultado de análisis
Tomado de (Nessus, 2019)

3.6.1.1. Cisco IOS XE Cluster Management Protocol Gestión de opciones de Telnet

De acuerdo con su versión y configuración auto informadas, el software Cisco IOS XE que se ejecuta en el dispositivo remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subsistema del Protocolo de administración de clústeres (CMP), debido al manejo inadecuado de las opciones de Telnet específicas de CMP.

Un atacante remoto no autenticado puede hurtar información, esto estableciendo una sesión con opciones de telnet específicas de CMP con formato incorrecto, para ejecutar código arbitrario.

3.6.1.2. Validación del certificado Smart Call Home de Cisco IOS e IOS XE Software

Según su versión auto informada, el software Cisco IOS XE se ve afectado por la siguiente vulnerabilidad

Una vulnerabilidad en la característica Cisco Smart Call Home del software Cisco IOS e IOS XE podría permitir que un atacante remoto no autenticado obtenga acceso de lectura no autorizado a datos confidenciales mediante un certificado no válido. La vulnerabilidad se debe a que el software afectado no procesa la validación del certificado. Un atacante podría aprovechar esta vulnerabilidad al proporcionar un certificado elaborado a un dispositivo afectado.

Una explotación exitosa podría permitir al atacante realizar ataques de intermediarios para descifrar información confidencial sobre las conexiones de los usuarios al software afectado (CVE-2019-1757).

3.6.1.3. Cisco IOS DHCP Vulnerabilidades múltiples

De acuerdo con su versión auto informada, el software Cisco IOS que se ejecuta en el dispositivo remoto se ve afectado por múltiples vulnerabilidades de denegación de servicio, en la implementación del cliente DHCP cuando se analizan los paquetes DHCP. Un atacante remoto no autenticado puede explotar estos problemas, a través de paquetes DHCP especialmente diseñados, para hacer que el dispositivo se vuelva a cargar.

3.6.1.4. Vulnerabilidad de pérdida de información en el protocolo del enrutador Hot Standby

Una vulnerabilidad en el subsistema de Protocolo de enrutador Hot Standby (HSRP) del software Cisco IOS e IOS XE podría permitir que un atacante adyacente no autenticado reciba información potencialmente sensible de un dispositivo afectado. La vulnerabilidad se debe a una inicialización de memoria insuficiente. Un atacante podría aprovechar esta vulnerabilidad si recibe tráfico HSRPv2 de un miembro HSRP adyacente. Una explotación exitosa podría permitir al atacante recibir información potencialmente sensible del dispositivo adyacente.

4. ANÁLISIS DE LOS MÉTODOS PARA PREVENIR LAS VULNERABILIDADES DE LA RED TCP/IP

Es muy importante saber que proteger implica mucha responsabilidad, conectarnos al mundo del internet sin temor a ser atacado y para lograr esto es necesario el estudio y definición de los aspectos que se debe tomar en cuenta a la hora de planear la seguridad de red, análisis de riesgos, identificación de recursos y amenazas, planes de contingencia nos llevarán a un ambiente seguro.

4.1. Seguridad de las Redes de Datos

Proviene del latín *securitas*, que a su vez deriva de *securus* (sin cuidado, sin precaución, sin temor a preocuparse), es referente a la característica de seguro, es decir, realza el enfoque en algo donde no se registra peligroso, amenazas, daños ni riegos. En términos generales, la seguridad se considera como el estado de bienestar que percibe y disfruta algo o alguien (Borghello C. , 2009).

La red es un área potencial a la exposición de riesgos. Por lo general, define el perímetro real de seguridad, en consecuencia, los atacantes suelen dirigirse a la red como punto de partida para acceder a otros activos de tecnologías de información (TI).

La seguridad de red consiste en defender los recursos relacionados a la infraestructura de red frente a amenazas. La seguridad emplea contramedidas físicas y de software para proteger la infraestructura de red contra el acceso no autorizado, el uso inadecuado, la modificación y la destrucción (Hewlett Packard Enterprise Development LP, 2018).

Basándonos en lo expuesto. La seguridad de red hace referencia a políticas, prácticas y tecnología que evitan los ataques a las redes de las organizaciones y a los recursos de sistemas informáticos accesibles de la red.

4.2. Esquema de seguridad

La seguridad se divide en varios campos de los cuales tomaremos los más sobresalientes.

- Seguridad Física. - Se refiere a la protección física de los dispositivos que actúan en una red.

- Seguridad Personal. - Mecanismos de protección, políticas de seguridad para los usuarios de red.

- Seguridad Lógica. - consiste en colocar barreras y procedimientos que resguarden el acceso a los datos y solo sea usada por la persona autorizada.

- En Redes. - Es el evitar que terceras personas puedan tener accesos no autorizados, causar daño o interrupciones costosas. Sin importar el medio de transmisión que brinde la conexión.

- Seguridad de sistemas de informática. - Seguridad de los sistemas de transmisión de datos.

  · Privacidad

    Seguridad física o mecanismos de prevención y detección, para la protección de los recursos de red, ejemplo (enrutador, *switch*-conmutador, servidores, máquinas).

Autenticación. Es confirmar y determinar la identidad de un individuo mediante la presentación de sus credenciales.

- Integridad.

  La encriptación, permite y garantiza que los datos transmitidos lleguen a su destino sin sufrir robo o modificación, los más comunes tenemos: Certificados digitales, VPN, SSH, DES, AES.

- Disponibilidad

  Donde se expone cuanto tiempo un servicio está activo, cabe mencionar este punto es el favorito por los atacantes, por el desprestigio y pérdida económica que representa la denegación de un servicio.

  IDS sistema de detección de intrusos (*intrusión detection system).*

- Administración.

  Se refiere la forma en que el administrador de red debe resguardar los datos de acceso con el manejo de políticas a usuarios, alertas generadas por los sistemas, las mismas que son muchas de las veces ignoradas.

4.3. Sistema de detección de intrusos (IDS)

Un sistema de detección de intrusos (o IDS por sus siglas en inglés *Intrusion Detection System*) Es un proceso o dispositivo capaz analizar las actividades del sistema y de la red cuando existen entradas no autorizadas y/o actividades maliciosas esto lo realiza a través de un software diseñado específicamente para detectar actividades inusuales (clavei, 2018).

Existen dos tipos de sistemas de detección de intrusos la figura 12 clasifica en grupos dependiendo el tipo de evento que monitorean.

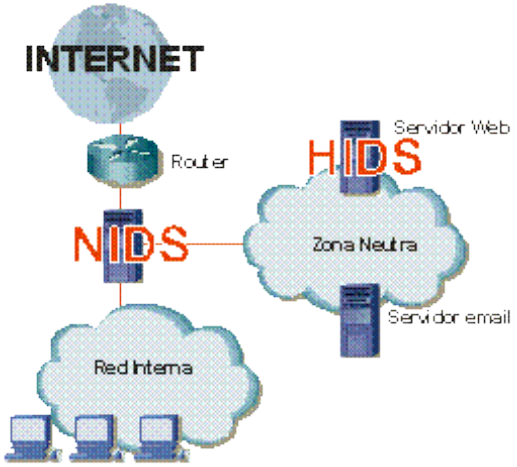


Figura 12. Sistemas de detección de intrusos

Tomado de (Adminso, 2014)

4.3.1. Sistema de detección de intrusos de red (N-IDS)

El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo “invisible” en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques (Sanchez Avila, 2015).

También se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado adentro de la red.

4.3.2. Sistema de detección de intrusos en el host (H-IDS)

Su software cubre una amplia gama de sistemas operativos por el mismo hecho de encontrarse en los hosts como Windows, Solaris, Linux, HP-UX, Aix etc.

El H-IDS actúa como un daemon o servicio estándar en el sistema de un host. Tradicionalmente.

El H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura paquetes de la red que se introducen o salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer) (Sanchez Avila, 2015).

4.4. Como funciona un IDS

Los principales métodos utilizados por N-IDS para informar y bloquear intrusiones son:

Reconfiguración de dispositivos externos firewalls o ACL en routers: Comando enviado por el N-IDS a un dispositivo externo como un filtro de paquetes o un firewall para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta en el encabezado del paquete (Yu & Tesai, 2011, pág. 51).

Envío de una trampa SNMP a un hipervisor externo: Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa como HP Open View Tivoli, Cabletron, Spectrum, etc.

Envío de un correo electrónico a uno o más usuarios: Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.

Registro del ataque: Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.

Almacenamiento de paquetes sospechosos: Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.

Apertura de una aplicación: Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora).

Envío de un “ResetKill“: Se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válido para técnicas de intrusión que utilizan el protocolo de transporte TCP).

Notificación visual de una alerta: Se muestra una alerta en una o más de las consolas de administración.

4.5. Prevenir desvíos de información o ataques

Es importante evitar desviaciones de información para esto es necesario las actualizaciones de los sistemas de cada uno de los equipos que conforman la red de comunicación de una entidad.

La implementación de contraseñas fuertes es la primera barrera de protección para nuestra información personal y empresarial, no podemos darnos el lujo de usar una contraseña muy fácil o muy común, seguir estos pasos para construir una contraseña fuerte (Paus, 2016).

- Seleccionar una palabra.
- Agregar y cambiar minúsculas por mayúsculas.
- Reemplazar una o varias vocales por números
- Agregar caracteres especiales.
- Aumentar la longitud de la contraseña a por lo menos diez caracteres o más.
- Seleccionar una frase entera y aplicar los puntos anteriores.

Ejemplo:
Frase normal: dragon ball super gogeta vs broly 2019
Contraseña fuerte: “Dr4g0n B4ll Sup3r Gog3t4 Vs Br0ly! 2019”

El cifrado de información en la trasmisión de la información evita que un posible atacante atrape y entienda los datos informáticos en un sistema de red.

La información que enviamos y recibimos es vulnerable cuando se transmite, ya que puede ser interpretada si los datos no están cifrados. En estos casos, es recomendable utilizar protocolos seguros (por ejemplo, HTTPS o SSH) cuando se realizan conexiones o se utiliza algún servicio en Internet (Mendoza, 2014).

Adicional a esto, las herramientas que cifran el texto antes de ser enviado o los archivos, son de gran utilidad. En caso de que los datos sean interceptados, es necesario contar con la clave con la cual se cifró para poder acceder a la información.

Las 8 herramientas de cifrado de información (Capacity Academy, 2016):
DiskCryptor, VeraCrypt, OpenStego, OpenPuff, GNUGPG, OpenSSH, OpenSSL, TOR.

4.5.1. Mecanismos de identificación y autenticación

Permiten identificar de forma única entidades del sistema y la autenticación se trata de comprobar que la entidad es quien dice ser. Antes de determinar cualquier restricción a los accesos se debe implementar una Matriz de accesos. Tener definido claramente todas las condiciones de accesos a la red, se debe cuestionar:

¿Quién puede ingresar a la Red?, ¿Qué días?, ¿En qué horarios?, ¿A qué programas?, ¿A qué archivos?, etc.

4.5.1.1. Identificación

Es la capacidad exclusiva de un usuario cuando se da a conocer en un sistema o aplicación el mismo que debe estar registrado en dicho sistema, es el paso previo a la a autenticación (IBM, 2018).

4.5.1.2. Autenticación

Es el proceso en cual un sistema o aplicación verifica la identificación de un usuario registrado en su base de datos.

Lo que debe tomar en cuenta para reforzar la autenticación:

- Medidas de seguridad en cuanto al tratamiento de las claves o passwords.
- Handshacking.
- Control Físico complementario.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas (Borghello C. , 2009):

- Algo que solamente el individuo conoce: por ejemplo, una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- Algo que la persona posee: por ejemplo, una tarjeta magnética.

- Algo que el individuo es y que lo identifica unívocamente: por ejemplo, las huellas digitales o la voz.

- Algo que el individuo es capaz de hacer: por ejemplo, los patrones de escritura

Los accesos deben ser siempre restringidos y con la máxima limitación, por regla general hay que recordar “Lo que no está expresamente autorizado está prohibido".

4.5.2. Mecanismos de control de acceso

En cualquier sistema informático, especialmente si es multiusuario, el control de acceso sobre usuarios y recursos del mismo es un pilar fundamental para su seguridad. Por ello, es de gran importancia contar con mecanismos que proporcionen una apropiada segregación de privilegios y permisos de usuario, así como de la administración de los mismos y de los elementos relacionados (Lopez, 2014).

Los objetos de un sistema de red deben estar protegidos mediante mecanismos de control de acceso que establezcan los tipos de acceso al objeto por parte de cualquier entidad del sistema.

- Control de acceso discrecional (Discretionary Access control, DAC)
- Control de acceso basado en roles (Role Base Access Control, RBAC)
- Control de acceso obligatorio (Mandatory Access Control, MAC)

4.5.3. Mecanismos de separación

Separar los dispositivos por capas o en la parte lógica separa la configuración de una red es importante para controlar el acceso de una red a otra.

La segmentación de red puede ser compleja, pero los fundamentos son sencillos. En pocas palabras, es el proceso de agrupar lógicamente activos de

red, recursos y aplicaciones, junto a las zonas compartimentadas que no tienen relaciones de confianza entre sí (Blaustein, 2014).

Hay que tener en cuenta las siguientes consideraciones antes de la segmentación: Obtener visibilidad del tráfico, los usuarios y los activos, proteger las comunicaciones y recursos en ambas solicitudes entrantes/ salientes, implementar controles granulares de tráfico, los usuarios y los activos, establecer una política de denegación predeterminada en todas las conexiones entre segmentos.

Mediante la configuración de listas de control de acceso y configuración segmentada de VLAN´s, se puede separar en los dispositivos de telecomunicación de la capa 3.

Si se realiza la implementación de redes inalámbricas estas no podrán conectar a la red por cable, ya que se debe restringir por políticas de seguridad en los equipos de capa 3.

4.5.4. Mecanismos de seguridad en las comunicaciones

La protección de la información, integridad y privacidad cuando viaja por la red es especialmente importante, es necesario aplicar protocolos seguros que cifraran el tráfico por la red.

4.5.4.1. Políticas de seguridad

Las políticas de seguridad en una entidad son para establecer parámetros de conexión entre usuarios internos y externos, identificar los puntos de protección, como implementar la arquitectura y topología de red.

Una política de seguridad es el conjunto leyes, reglas y prácticas que deben gobernar una organización, a través de ella se transmite protegiendo la

información sensible. Con este documento se pretende crear y dar el primer paso para que sea implementada una barrera eficiente de protección (López A. , 2015, pág. 21).

Es muy importante contar con políticas de seguridad que resguarden los recursos informáticos sobre todo definir claramente el valor, que tan importantes son los recursos e información que se tienen en la red corporativa.

Una política de seguridad informática es una forma de comunicación protegida con los usuarios y los gerentes de una organización. Las políticas de seguridad informática (PSI), establecen los paramentos de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

Una política no se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que deseamos proteger y el porqué de la protección.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

4.5.4.2. Características principales de políticas de seguridad

Una política de seguridad es desarrollada de acuerdo a las necesidades, los servicios que va a proyectar y los recursos a los que se va a proteger en fin todo lo que represente un activo importante para el normal desarrollo de las funciones laborales de la organización.

Por lo antes mencionado las políticas deben poseer las siguientes características fundamentales.

Tabla 19. Características fundamentales PSI

DISPONIBILIDAD	Es necesario garantizar que los recursos del sistema se encuentren disponibles cuando el usuario necesite de ellos.
UTILIDAD	Los recursos del sistema y la información manejada en el mismo deben ser útil para alguna función.
INTEGRIDAD	La información del sistema debe estar disponible tal y como se almaceno por una persona autorizada.
AUTENTICIDAD	El sistema debe ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
CONFIDENCIALIDAD	La información solo debe estar disponible para agentes autorizados, especialmente su propietario.
POSESION	Los propietarios de un sistema deben ser capaces de controlarlo en todo momento, perder este bien a favor de un usuario no autorizado compromete la seguridad del sistema hacia el resto de los usuarios.

Tomado de (Javier & Nava, 2014)

4.5.4.3. Porque utilizar políticas de seguridad

Son muchos los motivos para implantar seguridad en una organización, pero sin embargo mencionamos la más relevante, permite dar el valor que corresponde a la información.

- Ayuda prevenir incidentes de seguridad.
- Ayuda a la restauración cuando un incidente ocurre.
- Sirve de sustento frente a requerimientos legales.
- Se desarrolla estrategias de protección.
- Emite reglas para los usuarios de la red.
- Aporta a la efectiva protección de la organización.

- Culturiza a los participantes en el uso de servicios de red y enseña el valor real que para ellos debe representar.
- Planeación estrategia de la infraestructura de red en el interior de la organización.

4.5.5. Sistema de prevención de intrusos (IPS)

Un sistema de prevención de intrusos (o IPS por sus siglas en inglés *Intrusion Prevention System*) son dispositivos ubicados en puntos clave de una red interna, los mismos que analizan en forma permanente el tráfico buscando patrón conocidos, almacenados en una base de datos para ejecutar acciones a tiempo y combatir actividades potencialmente maliciosas (Panda, 2019).

Los protocolos analizados son IP, ICMP, TCP y UDP; y el administrador puede configurar el bloqueo automático de las intrusiones detectadas, además de especificar valores límite y umbral para cada regla, que reducirán los falsos positivos.

El IPS fue creado con la intensión de ser una alternativa complementaria a otras herramientas de seguridad en redes, tales como un firewall o un IDS, por lo que muchas de sus características son heredadas de estos dos elementos, complementadas con un comportamiento proactivo ante ataques y amenazas (Infotecs, 2019).

Los IPS se clasifican en dos grupos diferentes por método de detección y por otro lado basados en tecnología

Métodos de detección

IPS basado en firmas o signaturas: cuentan con una base de datos de “firmas”, en la cual se reflejan patrones conocidos de ataques a la seguridad de un dispositivo o una red. Esta información se adhiere al dispositivo que realizará la

detección para que así, mediante una búsqueda de coincidencias, se pueda establecer si existe o no un posible ataque y reaccionar en consecuencia.

IPS basado en anomalías: también conocido como basado en “perfil”, esta funcionalidad intenta identificar un comportamiento diferente que se desvíe de lo que, de alguna forma, se ha predefinido como una “actuación normal” de un dispositivo o una red. Para garantizar este comportamiento se hace uso de un potente análisis estadístico de indicadores de tráfico.

IPS basado en políticas: se requiere que se declaren muy específicamente las políticas de seguridad. El IPS reconoce el tráfico definido por el perfil establecido, permitiendo o descartando paquetes de datos, por lo que su manera de actuar ocurre de forma muy similar al funcionamiento de un firewall.

IPS basados en detección por Honey Pot (Pote de Miel): funciona usando un equipo configurado para que, a primera vista, parezca ser vulnerable e interesante para un ataque, de forma tal que al ocurrir estos, se deja evidencia de la forma de actuar, con lo cual posteriormente se pueden implementar políticas de seguridad.

4.5.5.1. Basados a su tecnología

IPS basado en host: monitorea las características de un dispositivo de un abonado de la red en particular. Entre las características que analiza se encuentran: el tráfico de red cableada o inalámbrica, registros del sistema, acceso de los usuarios, ejecución de procesos y modificaciones de archivos.

Actúa solo sobre el host en el cual trabaja. Este tipo de IPS se emplea con frecuencia en la protección de servidores y dispositivos con aplicaciones de servicios ininterrumpidos.

IPS basado en red: se realiza el monitoreo sobre el tráfico que fluye a través de segmentos particulares analizando protocolos de red de transporte y de aplicación para identificar actividades sospechosas.

Analiza en tiempo real los paquetes de datos del tráfico (cableado o inalámbrico), en busca de patrones que puedan suponer algún tipo de ataque. Una solución recomendada para la detección de intrusos que proceden de redes no fiables, es que el sistema IPS resida junto con el firewall en el mismo dispositivo.

4.5.6. Identificación de dispositivos a proteger

La primera acción que se debe tomar en cuenta para el desarrollo de políticas de seguridad es contar con una lista donde se indique los elementos específicos a proteger. Los aspectos a considerar son los siguientes:

Tabla 20. Equipos según su nivel de riesgo

Sistema	Descripción	Nivel de riesgos	Tipos de usuarios
Switches ATM	Dispositivo del núcleo de red	Alto	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Todos los otros para usar como transporte
Routeres de la red	Dispositivo de distribución de red	Alto	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Todos los otros para usar como transporte
Switches de armario	Dispositivo de red de acceso	Medio	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Todos los otros para usar como transporte
ISDN o servidores de marcación rápida	Dispositivo de red de acceso	Medio	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Socios y usuarios con privilegios para el acceso especial

Firewall	Dispositivo de red de acceso	Alto	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Todos los otros para usar como transporte
DN y servidores DHCP	Aplicaciones de Red	Medio	Administradores para configuración; Usuarios con privilegios y generales para el uso
Servidor externo de correo electrónico	Aplicación de red	Bajo	Administradores para configuración; Todos los otros para el transporte del correo entre Internet y el servidor de correo interno
Servidor interno de correo electrónico	Aplicación de red	Medio	Administradores para configuración; El resto de los usuarios internos para el uso
Bases de datos Oracle	Aplicación de red	Moderado o alto	Administradores para la administración del sistema; Usuarios con privilegios para las actualizaciones de los datos; Usuarios generales para el acceso de datos; Todos los otros para el acceso a los datos parciales

Tomado de (cisco, 2005)

4.5.6.1. Datos

Datos a proteger en línea, almacenados fuera de línea, durante la ejecución, almacenado, respaldos, bases de datos, cuando se transmite sobre los medios físicos de comunicación.

4.5.6.2. Dispositivos

Enrutadores, conmutadores, servidores de acceso remoto, máquinas virtuales, computadoras, tarjetas, teclados, terminales, impresoras, unidades de almacenamiento, líneas de comunicación.

4.5.6.3. Programas

Programas fuentes, programas objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

4.5.6.4. Personas

Usuarios, personal externo con uso de servicios locales.

4.5.6.5. Documentación

Documentos de programas, contraseñas, dispositivos, procedimientos de administración local.

4.5.7. Socialización a los usuarios

Quien esté a cargo del área de seguridad informática o en su defecto administrador de red, deberá notificar a todo el personal que se vincule con la DTI, el detalle de las obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas, guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información.

De igual forma, será responsable de la notificación y socialización de la presente política y de los cambios o actualizaciones que en ella se produzcan a todo el personal, a través de la suscripción de los acuerdos de confidencialidad y de labores de capacitación continua en materia de seguridad según los lineamientos establecidos por el Área de Seguridad de la Información de la Entidad.

Para crear una política de seguridad de red efectiva es necesario encontrar un balance entre la protección y la productividad.

Implantar una política de seguridad de red efectiva es un esfuerzo colectivo y como tal se deben proveer los medios para que los usuarios participen activamente en la definición de la misma y hagan aportes de lo que ellos mismo perciben de su interacción con la red.

4.6. Detectar el desvió de información

Aprovechar las herramientas de monitoreo de seguridad de red para ayudar a detectar las desviaciones y si producen, violaciones o intentos de violación de seguridad del sistema de red proceder a detener dichos intentos.

El tradicional firewall de red. Los firewalls de una sola función hace mucho tiempo se transformaron en plataformas de gestión unificada de amenazas (UTM), que combinan firewall, IPS, VPN, gateway web y capacidades antimalware. Sin embargo, incluso las UTM tienden a centrarse en la inspección del tráfico de red. Cuando se examina la carga útil de una aplicación, es por una razón específica, como bloquear una dirección URL que está en la lista negra, algún tipo de contenido o un malware reconocido (Phifer & TechTarget, 2018).

La gestión de movilidad empresarial (EMM), se puede utilizar para evaluar rutinariamente la integridad de los dispositivos móviles.

Las tecnologías de gestión de eventos e información de seguridad (SIEM), agregación y normalización de eventos producidos por sistemas y aplicaciones de conexión que necesitan estar conectados a la red empresarial.
Los sistemas de detección de brechas (BDS), para aplicar análisis de big data a la información monitorizada, haciendo perfiles de patrones de comportamiento de usuarios y dispositivos para detectar brechas y facilitar la investigación interactiva.

4.6.1. Sistema Cortafuego informático (Firewall)

A finales de los 80, cuando la Red no era más que un inocente retoño que daba sus primeros pasos, algunos de sus usuarios ya habían descubierto que podían hacer travesuras en los ordenadores ajenos infiltrándose a través de su conexión a Internet.

Si traducimos la palabra firewall, la traducción más cercana que encontramos en internet es la de un cortafuego.

Firewall: Es un sistema informático simple o compuesto que actúa en defensa de nuestro sistema, se sitúa entre dos o más redes con la intención de hacer cumplir unas determinadas directivas de seguridad sobre la comunicación entre ellas brindando una conexión segura entre dos o más sistemas informáticos.
Los propósitos de un firewall son:

- Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- Prevenir los ataques.
- Restringir los permisos de los usuarios a puntos cuidadosamente controlados.

Un Firewall es vulnerable, él no protege de la gente que está dentro de la red interna, Lo que nos indica que un Firewall no puede estar solo, este debe ir acompañado de políticas estrictas de funcionamiento y reglas marcadas para que el Firewall sea funcional, de otra manera se está construyendo un sistema de seguridad sin bases sólidas. El Firewall trabaja mejor si se complementa con una defensa interna.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través de los cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

También es frecuente conectar el cortafuego a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un firewall correctamente configurado se puede denominar cortafuego de defensa, ya que es el primero en actuar cuando existen amenazas, cualquier ataque desde el exterior el firewall los detecta y mitiga con sus políticas.

Detrás de esta línea de defensa llamada firewall, generalmente se encuentran grupos de servidores, equipos del usuario. Los usuarios comúnmente lo ven como una puerta de acceso al internet, pero tenemos un sin número de dispositivos ejecutando servicios propios de una red local, ejemplo servidores de archivos, servidores de impresoras, códigos web o bases de datos, información financiera que de alguna forma requieren el acceso a Internet, pero que nadie más la tengo o puede manipular

El propósito del Firewall es hacer cumplir ciertas directivas de seguridad. Estas directivas reflejan las decisiones que se han tomado sobre qué servicios deben ofrecer o ser accesibles a los equipos y usuarios remotos en sitios específicos, además que servicios serán solo locales de la red. Todas las directivas de seguridad están relacionadas con el control de acceso y uso autenticado de servicios privados o protegidos.

Pero en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

4.6.1.1. Filtrado de Paquetes

En este apartado veremos algunas denominaciones como se conoce al firewall esto depende del mecanismo que se use para implementarlo, la capa del modelo TCP/IP, las arquitecturas y el uso de enrutamiento. Los más comunes son:

- Firewall de filtrado de paquetes
- Pasarela de aplicación, también llamada de Firewall de host explorado
- Pasarela de circuito de nivel de aplicación, también llamada Firewall Proxy

Firewall de filtrado de paquetes, es un firewall primitivo que se suele implementar dentro de un sistema operativo para redes que no requieren mucha protección y funcionan en las capas de transportes y red IP. Se basa en el aprovechamiento de la capacidad de algunos routers (sreening routers), para hacer un enrutado selectivo, es decir, para bloquear o permitir el tránsito de paquetes mediante listas de control de acceso en función de ciertas características de las tramas, de forma que el router actué como pasarela de toda la red (Lucas, 2003).

Pasarela de aplicación, es un sistema de hardware/software para conectar dos redes entre sí y para que funcionen como una interfaz entre diferentes protocolos de red. El tráfico de red nunca pasa a través de la máquina de aplicación directamente, cuando un usuario remoto contacta la pasarela, ésta examina su solicitud. Si dicha solicitud coincide con las reglas que el administrador de red ha configurado, la pasarela crea una conexión entre las dos redes. Por lo tanto, la información no se transmite directamente, sino que

se traduce para garantizar una continuidad entre los dos protocolos (ccm, 2008).

El sistema ofrece seguridad adicional, ya que toda la información se inspecciona minuciosamente y en ocasiones se guarda en un registro de eventos. Este sistema debe tener una aplicación de este tipo disponible para cada servicio, es decir para (FTP, HTTP, Telnet, etc.)

Firewall proxy, es una aplicación que actúa como intermediario entre un sistema local y un remoto, cada aplicación Proxy aparece ante el servidor como el programa cliente, y ante el cliente como el servidor real, los programas clientes especiales, o programas de cliente configurados especialmente, se conectan al servidor en vez de a un servidor remoto, donde ambos extremos de una conexión están obligados a realizar la sesión a través del proxy. Lo hacen creando y ejecutando un proceso en el firewall que refleja un servicio como si se estuviera ejecutando en el host final.

4.6.1.2. Como es su Funcionamiento

El filtrado de paquetes puede permitir o denegar el acceso según las direcciones IP de destino o los puertos, o ambos. UDP y TCP de la capa de transporte, los indicadores de conexión TCP, los tipos de mensajes ICMP del nivel de red y en si el paquete es entrante o saliente de acuerdo a lista de políticas establecidas por el administrador de red. Se pueden poner en vigor distintas políticas al definir múltiples conjuntos de reglas de filtrado de paquetes (Borghello C. , 2010).

Estas reglas definen explícitamente los paquetes que van a pasar y los que no a través de la interfaz de red. Las reglas del Firewall usan el encabezado de los paquetes para decidir si enrutar a su destino, eliminar el paquete o bloquear un paquete y devolver una condición de error a la máquina emisora múltiples conjuntos de reglas de filtrado de paquetes

La idea principal es que el usuario debe controlar con mucho cuidado lo que sucede entre Internet y la máquina que se ha conectado directamente a Internet.
Sobre la interfaz externa a Internet, el usuario filtrará individualmente lo que procede del exterior y lo que sale de la máquina de forma tan precisa y explicita como sea posible.

Esto suena pesado y extenuante para el sistema, y lo es, pero no es un mecanismo de seguridad infalible, esto es una parte del problema solamente, es otro obstáculo a ser solventado en el esquema de seguridad. No todos los protocolos de comunicación de aplicación se prestan para el filtrado de paquetes.

La capa de red no tiene la capacidad de verificar que máquina es quien o lo que dice ser. La única información de identificación disponible en este nivel es la información del encabezado donde se proporciona la dirección IP del origen y del destino, campos que pueden modificarse fácilmente, además ni la capa de transporte ni la capa de red pueden verificar si los datos de las aplicaciones son correctos.

Sin embargo, el nivel de paquete permite un control más preciso y sencillo sobre el acceso directo a un puerto, el contenido del paquete y los protocolos de comunicación correctos que se pueden establecer fácilmente o de forma adecuada, en niveles superiores.

4.6.1.3. Directivas

Es típico de una cadena de reglas de cortafuegos no cubre explícitamente todas las condiciones posibles. Por esta razón, las reglas de cortafuegos siempre deben tener una directiva especificada por defecto, que consiste en una sola acción (*accept, reject o drop*).

Rechazar o denegar. - Esta directiva de negar todo el tráfico a menos que una regla de aprobación lo permita, es la principal recomendación a la hora de implementar un firewall seguro, para ayudar a impedir ataques que puedan utilizar otros puertos, la recomendación es bloquear toda comunicación no solicitada de Internet. Rechazo global, con excepciones de regla de aprobación (lista de elementos aprobados), esto significa que se debe comprender el protocolo de comunicación para cada servicio y luego habilitar según las necesidades de la empresa o usuario especifico (Microsoft, 2017).

El mecanismo del Firewall ofrece la opción de rechazar o denegar los paquetes, términos en los cuales existe una diferencia, y es que cuando se rechaza un paquete, el paquete se descarta y se devuelve un mensaje de error protocolo de control de mensajes de Internet (ICMP) al remitente. Cuando se deniega un paquete, simplemente se descarta este sin ningún tipo de notificación al remitente.

Aceptar. - Esta directiva provee una fácil configuración de un firewall, pero el aceptar todo significa brindar acceso ilimitado lo cual nos lleva estar en constante vigilancia y prever todo tipo de acceso que se quiera deshabilitar, el problema principal será que no se restringirá ningún acceso considerado como peligroso hasta que sea demasiado tarde, en resumen, iniciar programando el firewall como acceso total con lleva a tener más trabajo, mayor dificultad y propenso a errores.

La opción denegar es entonces la mejor casi en todos los casos, hay tres razones para esto:

El consumo del tráfico de red aumenta, no hay necesidad de notificar origen del paquete ya que la mayoría es de origen malicioso.

4.7. Estándares de Seguridad ISO

Es importante mencionar las normas para el desarrollo de seguridad, ya que se toma un modelo de referencia de la organización de normas internacionales (OSI) *Iternational Organization for Standardization* que ofrecen varios consejos dirigidos a productos y servicios.

4.7.1. Estándar

La norma 17799 después de un mejoramiento constante, logra publicar una nueva versión de manera formal, estos pasos logran lanzarlo muy rápidamente y convertirse en una norma ISO es decir un estándar Internacional.

La norma ISO/ICE 27001 que antes se llamaba 17799, cuando se habla de seguridad informática lo primero que se nos viene a la cabeza es la norma ISO27001 ya que es muy relevante porque toma como base los riesgos a los que se enfrenta la organización, tiene como objetivo principal establecer, implantar, mantener y mejorar de forma continua la seguridad de la información de las organizaciones.

La norma ISO/IEC 27002 establece un catálogo de buenas prácticas que determina, desde la experiencia una serie de objetivos de control que han estado en constante evolución y es así que la versión más reciente es la ISO/IEC 27002:2017 en que basaremos nuestro estudio referencial en seguridad informática.

4.7.1.1. Estándares de seguridad ISO 17799

Origen Bristish Standard BS 7799-1 publicado en el año 1995, denominado también como ISO 270002; estándar para la seguridad de la información publicado en el año 2000 como ISO 17799 por la Organización Internacional de Estandarización y la Comisión Electrónica Nacional; con el título de*: Information*

technology - Security techniques - Code of practice for information security management; (Marín, 2006).

Sus actualizaciones se publicaron en el año 2005, este estándar realizar recomendaciones sobre las buenas prácticas en cuanto a la gestión de seguridad de la información con el fin de que instalen sistemas de seguridad en cada una de las diferentes instituciones ya sean publica o privadas, guardando siempre la confidencialidad, integridad y la disponibilidad; la publicación del año 2005 incluye: (ISO, 2011).

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Gestión de Activos de Información.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de las Comunicaciones y Operaciones.
- Control de Accesos.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes en la Seguridad de la Información.
- Gestión de Continuidad del Negocio.
- Cumplimiento.

4.7.1.2. Planeación de la Continuidad del Negocio

Los objetivos son: Contrarrestar las interrupciones de las actividades productivas críticas del negocio. Evitar fallas mayores o desastres.

Se debe contar con un plan de contingencias en caso de riesgos con el fin de mermar las interrupciones en los servicios, se debe realizar pruebas necesarias y actualización de procedimientos cuando existan cambios en el sistema o cuando existan pruebas de evaluación de fallos.

4.7.1.3. Sistemas de Control de Acceso

- Controlar el acceso a la información.
- Prevenir los accesos no autorizados a sistemas de información.
- Garantizar la protección de servicios de red.
- Prevenir los accesos no autorizados a las computadoras.
- Detectar actividades no autorizadas.
- Garantizar la seguridad de la información cuando se utilice cómputo móvil o remoto.

4.7.1.4. Desarrollo y Mantenimiento de Sistemas

Asegurarse que la seguridad del sistema está construida dentro de la aplicación para prevenir pérdidas, abusos, modificaciones de los datos. Debe de proteger la confidencialidad, autenticidad e integridad de la información. Los proyectos informáticos y sus actividades de soporte deberán de ser conducidos de forma segura.

Se utilizaran técnicas de cifrado para obtener confiabilidad e integridad de la información, evaluación de riesgos y en el entorno de producción se debe llevar un estricto control sobre el software del sistema, bibliotecas del código fuente ya que estos poseen información delicada, en el entorno de mantenimiento se identificará todos los cambios que realice en las diferentes aplicaciones, y todo los cambios, actualizaciones deberán ser correctamente documentados y verificados en concordancia a las normas de seguridad.

4.7.1.5. Seguridad Física y Ambiental

El objetivo de esta sección es prevenir el acceso no autorizado a las instalaciones para prevenir pérdida, robo, daño de los bienes y evitar la interrupción de las actividades productivas. Prevenir el robo de información y de los procesos de la empresa.

Delimitar las zonas de mayor vulnerabilidad de acuerdo a su nivel de prioridad y con acceso únicamente para personal autorizado, diseñar una infraestructura para resguardar la información de cualquier tipo de amenazas ya sean éstas causadas por personas o por la naturaleza.

También se recomienda crear políticas de escritorios sin papeles con el fin de evitar el hurto o destrucción de la información.

4.7.1.6. Cumplimiento

Evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.

Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.

Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoria del proceso.

Se deberá respetar estrictamente la Ley Orgánica de Producción de Datos, Ley de servicios de la sociedad de Información, Ley de firma electrónica, marco legal, políticas de seguridad.
Las políticas de seguridad deben estar en constante monitoreo y actualización en caso de ser pertinente y necesario.

4.7.1.7. Seguridad del Personal

Objetivo: Reducir el riesgo de error humano, robo, fraude, abuso de la información, sistemas y equipos. Asegurarse que el personal esté consciente de las amenazas de la información y sus implicaciones. Deberán de apoyar la política corporativa de seguridad en contra de accidentes y fallas. A la vez deberán de aprender de estos incidentes.

Se debe empezar por realizar una buena selección del personal que trabajara en una determinada institución ya sea de forma temporal o por contrato, por medio de contratos detallando todas las responsabilidades y función que va desempeñar, y poner en conocimiento de todo el personal tanto de forma verbal como escrita las políticas de seguridad vigentes, también se dará a conocer las estrategias de rápida reacción ante incidentes que puedan reaccionar los usuarios.

4.7.1.8. Seguridad de la Organización

Elaboración de políticas de seguridad partiendo de tres puntos indispensables: cuando la seguridad de la información está a cargo de la institución, cuando la seguridad de la información está a cargo de terceros, cuando la seguridad de la información está a cargo de externalizados.

En el primer caso se deber conformar un comité y un responsable directo el mismo que delegará responsabilidades para gestionar, controlar, supervisar el seguimiento de las políticas de seguridad, realizar mesas de trabajo con representantes de las diferentes áreas ajenas a las de tecnología. Los otros puntos de contratación a terceros y externalizados deberán ser realizados por medio de contratos debidamente revisados por el departamento jurídico.

Los objetivos de esta sección son:

- Administrar la seguridad de la información dentro de la compañía.

- Mantener la seguridad de las instalaciones de procesamiento de la información y los activos informáticos ingresados por terceros, (proveedores, clientes, etc.)

- Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información es ejecutada por terceros (Subcontratados).

4.7.1.9. Administración de las operaciones y equipo de cómputo

Objetivos:

- Asegurar la correcta operación de las instalaciones de procesamiento.
- Minimizar el riesgo de fallas en el sistema.
- Proteger la integridad del software y la información.
- Mantener la integridad y disponibilidad del procesamiento de la información y comunicaciones.
- Asegurar la protección de la información en la red y de la infraestructura que la soporta.
- Prevenir el daño a los activos y procesos críticos del negocio.
- Prevenir la pérdida, modificación o mal uso de la información intercambiada entre empresas.

4.7.1.10. Políticas de Seguridad de la Información

Objetivo: Proveer la directriz y el soporte de la dirección general de la empresa para la seguridad de la información.

Elaboración de políticas de seguridad de la información por parte del departamento de tecnología y demás departamentos de apoyo; para posterior ser analizado, revisado y aprobado previamente por los directivos de una determinada institución.

Dichas políticas deberán detallar claramente y de fácil compresión los objetivos de la seguridad de la información, indicar los responsables de la gestión de la información.

4.7.1.11. Control de Accesos

Se debe deli militar de manera documentada los derechos y responsabilidades de cada usuario para tener acceso a ciertos sitios acorde a la función que desempeña, verificar y actualizar periódicamente los accesos a usuarios conforme a su función que desempeñada.

Se diseñará un medio adecuado para la asignación de contraseñas siendo estas: huellas, candados software, y su difusión del buen uso y manejo de contraseñas para todos los usuarios.

Mediante una aplicación se debe grabar todos los ingresos con éxito y sin éxito dentro de un sistema de información con el fin de recopilar evidencia para ser analizada posteriormente de posibles amenazas.

5. PRINCIPALES MÉTODOS PARA PREVENIR LAS VULNERABILIDADES Y DISEÑO DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES

En este capítulo se va a determinar soluciones de seguridad para prevenir los posibles ataques a la red, colocando bases de confianza en orden jerárquico desde los usuarios hasta cúspide de la implementación de una infraestructura de red. Es decir que todos los dispositivos conectados a la red incluidos los usuarios o personas puedan tener protección a problemas que se presente, ya sea por la intromisión de atacantes con intenciones de espionaje o sabotaje.

En base al levantamiento realizado en la Agencia Metropolitana de Transito y los hallazgos realizados con lo que respecta las vulnerabilidades en general que posee la institución, se tomarán las más relevantes para brindar una solución se eficiente que puede implicar la implementación de métodos de seguridad en varios equipos existentes y por adquirir.

5.1. Desarrollo de políticas de seguridad

El objetivo del desarrollo de políticas de seguridad de red es definir procesos para prevenir y responder a problemas de seguridad frente a la evolución de las comunicaciones a través de internet.

Es el desarrollo de planes y procesos que protejan los recursos de red contra corrupción y fuga de datos por ello es importante mencionar lo siguiente:

- Implantar métodos para proteger sus bienes de una manera económica y oportuna.
- Determinar los objetivos y directrices de la organización.
- Establecer que recursos se quieren proteger y su importancia.
- Definir de quien se necesita proteger los recursos.

- Identificación de posibles amenazas.
- La política de seguridad debe estar acorde con otras políticas, reglas, regulaciones o leyes ya existentes en la organización.
- Identificación de los recursos disponibles.
- Verificar paródicamente la política de seguridad de red para ver si los objetivos y circunstancias han cambiado.

5.1.1.1. Análisis de riesgos

Este análisis involucra la respuesta a las siguientes preguntas importantes:

¿Qué voy a proteger?

Se identifica que la AMT debe enfocarse en la protección de los siguientes elementos: servidores, equipos de telecomunicaciones y usuarios de red.

¿Contra quién?

Contra los atacantes externos e internos que tengan la intensión de hurtar la información institucional

¿Cómo lo voy a hacer?

Con el análisis de los métodos de seguridad y tomando como referencia el modelo de IPS que es un método eficaz para proteger la red LAN y perimetral de la Agencia Metropolitana de Tránsito.

Es el proceso donde clasificamos el nivel de afectación que involucra decisiones costo beneficio para lo cual tenemos los siguientes riesgos:

- Denegación de servicio.
- Acceso no autorizado.
- Fuga de información sensible.
- El objetivo de este proceso es el análisis costo beneficio frente a la importancia de los recursos.

5.1.1.2. Definición de política de uso

Es importante señalar las responsabilidades y procesos de cada participante en la red. Otros factores a analizar es realizarse las siguientes preguntas de responsabilidad:

¿Cuáles son los derechos y responsabilidades de los administradores del sistema?

Mantenimiento y administración del sistema basados en métodos de seguridad

¿Quién puede tener privilegios para la administración del sistema?
El administrador de infraestructura y redes el Ing. Carlos Tituaña

¿A quién se le permite el uso de los recursos?
Solo a personal técnico autorizado por el Coordinador de Tecnología de la información

¿Cuál es el uso apropiado para los recursos?
Optimizar la transmisión de datos a través de una red segura e integra

¿Quién está autorizado para garantizar acceso y aprobar el uso de recursos?
El Ing. Cristian Gavilanes actual Coordinador de la Tecnología

¿Cuáles son los derechos y responsabilidades de los usuarios?
Los derechos que tiene el usuario es de gozar de un conexión fiable y sin interrupciones.

Tienen la responsabilidad salvaguardar la información empresarial obedeciendo las políticas de seguridad que se establecerán.

- ¿Qué es información altamente sensible?

Toda información que sea referente datos vehiculares y registro de sanciones

Revisión de políticas

En cualquier dispositivo de red existen rastreadores o archivos log con el objetivo de informar actividades del dispositivo, esto nos ayuda mucho a la hora de determinar si hay una violación a las políticas de seguridad, el examen del historial de registros (logs), son el paso inicial para determinar el uso no autorizado de cualquier sistema, para esto se puede realizar las siguientes acciones:

- Se puede detectar anomalías o comportamientos irregulares comparando las listas de usuarios actualmente conectados con listas históricas.

- Examinar las facilidades de log del sistema para chequear mensajes de error inusuales de los programas del sistema operativo como intentos fallidos recurrentes de conexión a un usuario o programas que requieren autenticación.

5.2. Políticas de seguridad para manejo de usuarios

De acuerdo con el levantamiento se pudo notar que los usuarios de la Agencia Metropolitana de Tránsito exponían sus claves en lugares visibles y entregaban sus contraseñas a otras personas esto generalmente pasa en los Centros de Matriculación.

Basándonos en lo detectado el área de soporte estará a cargo de entregar las contraseñas mediante un proceso formal de gestión de contraseñas con las siguientes recomendaciones:

- Las contraseñas no se deben escribir en papel, ni en archivos sin cifrar.
- En los navegadores web o aplicaciones, no activar recordar contraseña.
- En ningún caso enviar por correo.

- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas con otros usuarios o compañeros.
- Cambia tu contraseña si sospechas que alguien la tiene para evitar el mal uso.
- Seleccionar contraseñas que no sean fáciles de adivinar aplicar método aprendido Capitulo2.
- Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres predefinido.
- Cambia tus contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, número de cedula, nombre de familia etc.
- No utilizar contraseña con variables (amt1, amt2, amt3 etc.)

5.3. Encriptación de información

Para entender que es la encriptación debemos decir que es una manera de codificar la información para protegerla frente a terceros como se muestra en la figura 13. El proceso de encriptación.

La encriptación de la informática se hace cada vez más necesaria debido al aumento de los robos de claves de tarjetas de crédito, número de cuentas corrientes, y en general toda la información que viaja por la red, etc.

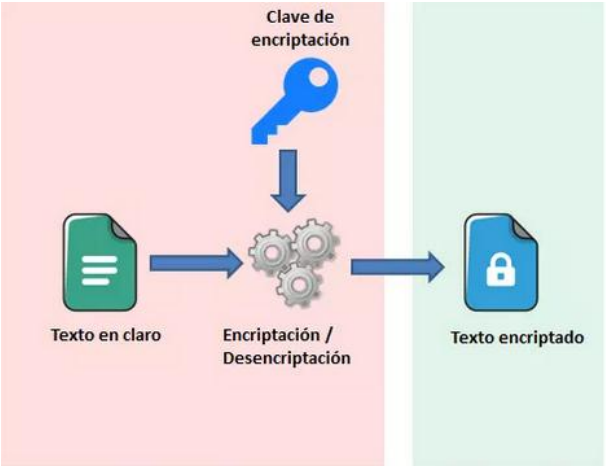


Figura 13. Encriptación de información

Tomado de (Acosta, 2016)

5.3.1. Protocolo SSH

El Protocolo *Secure SHell (SSH), permite* (cisco, 2018)[OBJ].,Es así como recoge los datos que el cliente quiere enviar y los reenvía por un canal seguro, donde al otro lado del canal se recogen los datos y se reenvían al servidor conveniente. En la figura 14. Se puede ver un esquema general del uso de SSH:

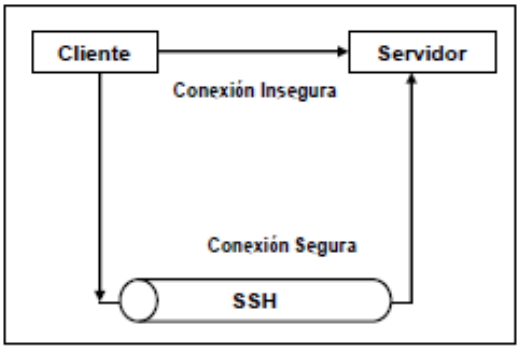


Figura 14. Diagrama ssh

Tomado de Visio

5.3.1.1. Transporte

El protocolo de capa de transporte se encarga del establecimiento de la conexión de transporte como se puede ver en la figura 15 muestra la autentificación del servidor y del intercambio de claves, y de las peticiones de servicio de los demás protocolos hacia el protocolo SSH.

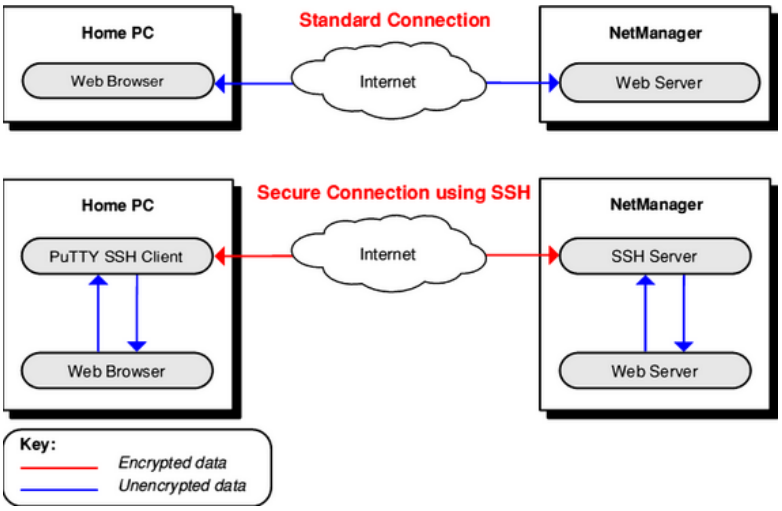


Figura 15. Diagrama con y sin SSH
Tomado de (Solvetic Sistemas, 2017)

Es así es como el cliente se conecta al servidor mediante el protocolo TCP. El servidor debe estar escuchando peticiones de conexión en el puerto asignado al servicio SSH (puerto 22 estándar para protocolo TCP) que desea adquirir el cliente, para así establecer la conexión segura como se muestra en la figura 16

Posterior a esta conexión el cliente y servidor proceden al intercambio de claves, donde cada parte envía un mensaje que contiene una cadena de 16 bytes aleatorios llamada Cookie (Fragmento de información), y las listas de algoritmos soportados por orden de preferencia, siendo primero los algoritmos de intercambio de claves.

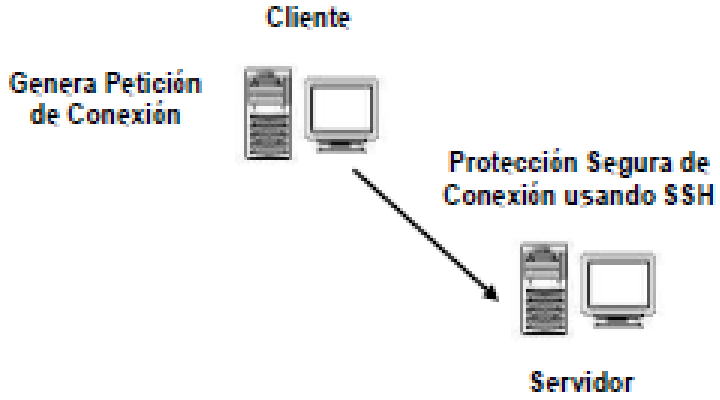


Figura 16. Uso SSH

Tomado de Visio

5.3.1.2. Autenticación de Usuario

En SSH se pueden ver diferentes tipos de autenticación de usuarios los que serán detallados a continuación:

Autenticación nula: El servidor permite que el usuario acceda directamente, sin ninguna comprobación, al servicio solicitado. Un ejemplo sería el acceso a un servicio anónimo.

Autenticación de listas de acceso: Es muy similar a la autenticación anterior, pero el servidor verifica que el sistema cliente sea efectivamente quien dice ser para evitar los ataques de falsificación de dirección.

Autenticación basada en contraseña: El servidor permite el acceso si el usuario da una contraseña correcta.

Autenticación basada en clave pública: En lugar de dar una contraseña, el usuario se autentica demostrando que posee la clave privada correspondiente a una clave pública reconocida por el servidor.

5.3.2. Protocolo SFTP

En la Agencia Metropolitana de Tránsito existen aplicativos que todavía usan el FTP como método de transmisión de archivos, el SFTP es un protocolo de transferencia de archivos SSH por omisión Cuyas siglas en ingles son: (*SSH File Transfer Protocol*), este protocolo permite varias actividades sobre archivos en modo remoto es por esto que se debe precautelar la información (Gisbert Vercher, 2015, pág. 43).

La figura 17. Se muestra cómo actúa el protocolo cifrando la información que está siendo trasmitida.

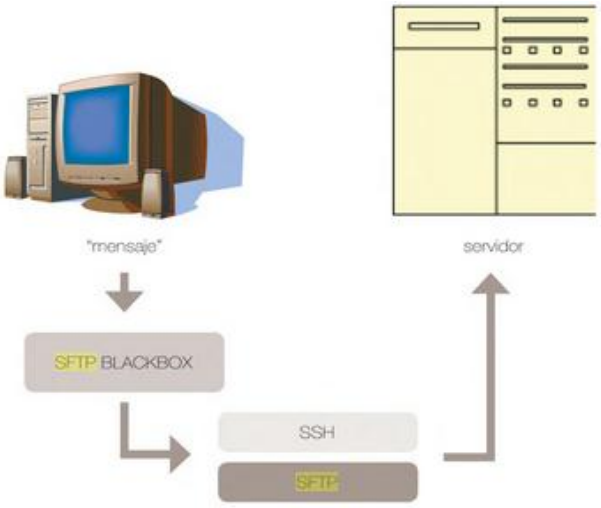


Figura 17. Funcionamiento de SFTP
Tomado de (Gisbert Vercher, 2015)

La principal ventaja que obtenemos al utilizar SFTP es la posibilidad de aprovechar una conexión segura para transferir archivos tanto en el sistema local y remoto.

La Agencia Metropolita de Tránsito usará el SFTP para enviar la información de forma cifrada evitando que sea propenso al ataque de hombre en la mitad. Para solventar esos y muchos inconvenientes que el FTP ocasionaba se propone la siguiente solución.

5.3.3. Implementando SFTP

Servidor de transferencia segura de datos (SFTP), para Windows 10 de forma simple y sin varios pasos de configuración:

SolarWinds SFTP/SCP Server, se procede a instalar de forma sencilla siguiendo los siguientes pasos:

Una vez instalada la aplicación se debe dar click en next y abrir el aplicativo como se puede ver en la figura 18. Pantalla SolarWinds:

Figura 18. Pantalla principal

5.3.3.1. Pestaña general

Se configuran los parámetros desde la pestaña general que se puede ver en la Figura 19. Esta se ubica en la esquina superior izquierda del programa.

Service status Stopped, esto indica que el servicio se encuentra detenido, si se selecciona File/Configure.- se debe iniciar la configuración para que SFTP funcione.

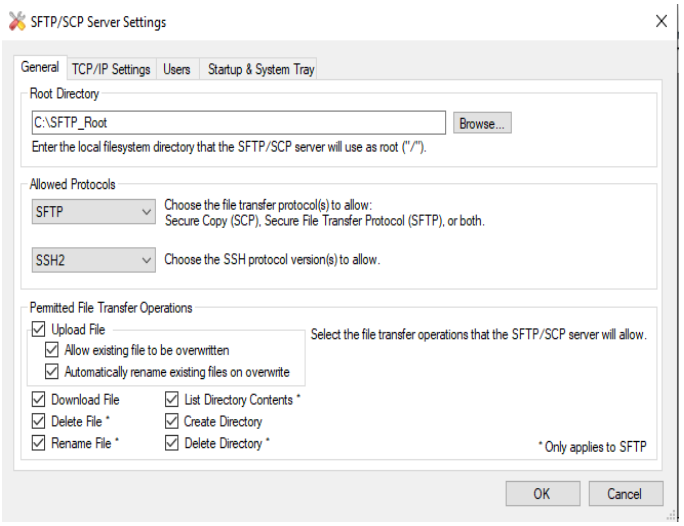


Figura 19. Ventana de configuración

Root Directory. - Esta opción indica dónde va a estar ubicada o alojada la aplicación SolarWinds SFTP/ SCP server.

Allowed Protocols. - Aquí se debe elegir en la primera opción SFTP en la segunda opción se debe elegir SSH2.

Permited File Transfer Operations. - En esta opción se debe activar todos los checks buttons.

5.3.3.2. Pestaña TCP/IP SETTINGS

En la opción TCP/IP Settings, se cambiará al puerto 27 es el único cambio que se realizará en esta opción.

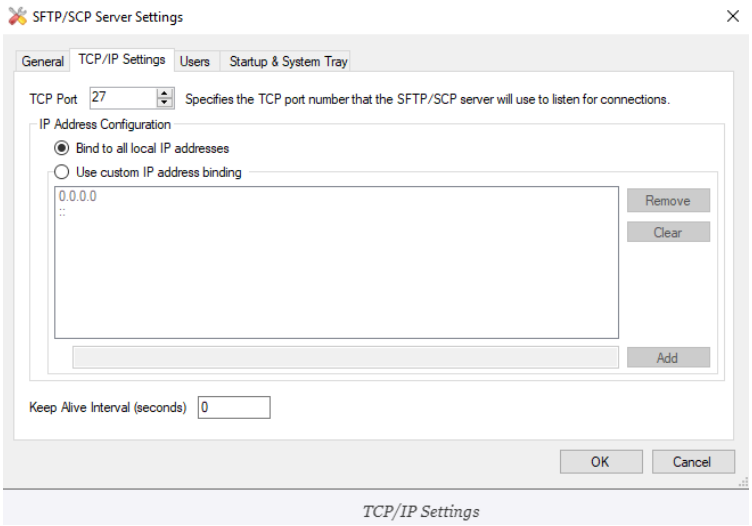


Figura 20. Habilitación de TCP

5.3.3.3. Pestaña users

En esta opción User se debe crear un usuario para poder ingresar al servicio SFTP, también es indispensable designar las credenciales de un usuario determinado al cliente FTP que se esté utilizando

Para crear un nuevo usuario se debe elegir New User y especificar el nombre del usuario y la contraseña respectiva.

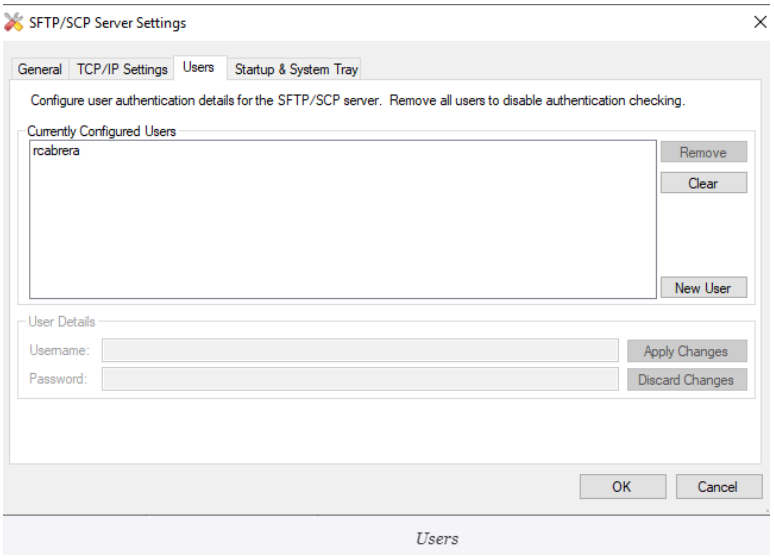


Figura 21. Creación de usuario

5.3.3.4. Startup & System Tray

No se realizarán ningún cambio en esta pantalla, se dejará las configuraciones por defecto.

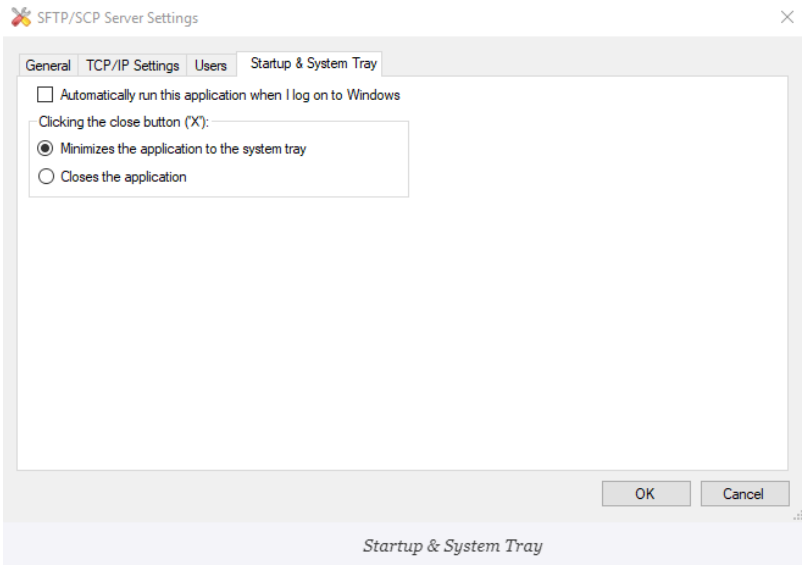


Figura 22. Configuración por defecto elige la opción OK.

Para levantar el servicio debemos elegir la opción START que se encuentra ubicada en la barra de estado de la pantalla principal de SolarWinds SFTP/ SCP Server.

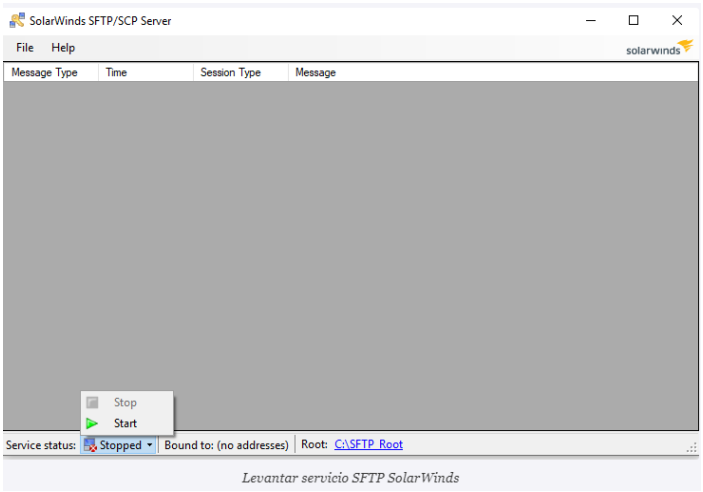


Figura 23. Iniciando el servicio

Al finalizar la configuración se debe iniciar SolarWinds SFTP/ SCP Server como administrador.

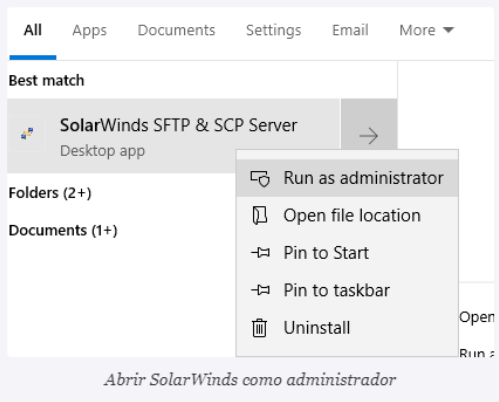


Figura 24. Ejecutar como administrador

El programa SolarWinds SFTP/SCP Server, ejecutado como administrador, se visualiza en la siguiente pantalla, pero ya no es necesario ingresar a configuraciones ya que se guarda automáticamente.

Figura 25. Pantalla del programa

5.3.3.5. Comprobación de la conexión SFTP con filezilla

La comprobación se realiza desde un cliente en este caso se va a usar Filezilla, para lo cual se realiza de la siguiente manera:

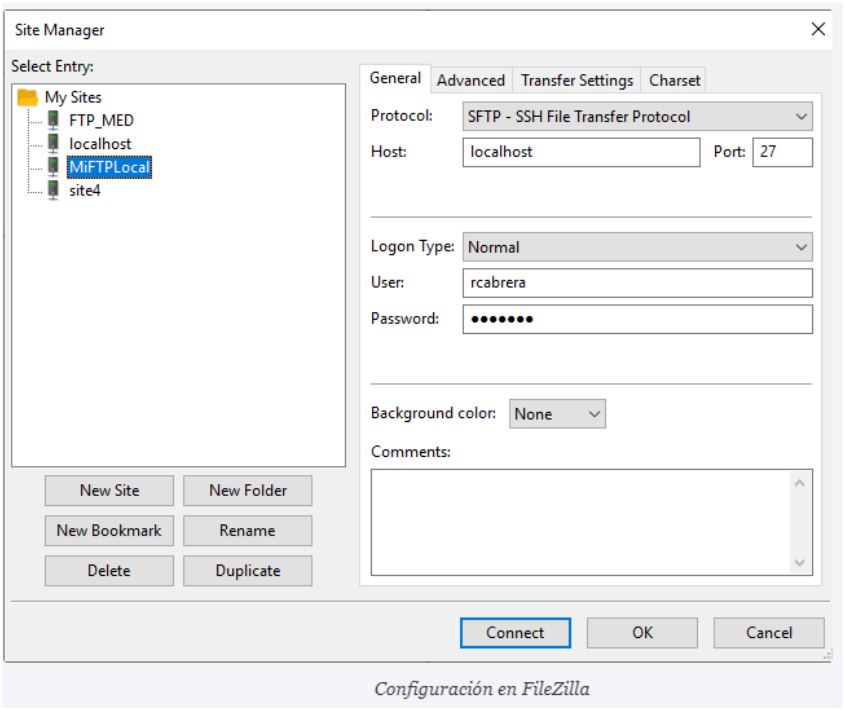
Protocolo. - se debe seleccionar SFTP.

Host. - se debe seleccionar localhost, es porque el servicio es FTP se encuentra en esa máquina.

Puerto. - se elige el puerto 27 igual como se había configurado en el programa SolarWinds SFTP/SCP Server.

Logon Type. - se debe elegir normal.

Usuario y contraseña. - se especifica las credenciales que se configuraron en programa SolarWinds SFTP/SCP Server.



Configuración en FileZilla

Figura 26. Ingreso de credenciales

En esta ventana no es necesario cambiar ninguna opción, posterior se debe seleccionar Connect, donde se establece de forma exitosa el programa SolarWinds SFTP/SCP Server, posterior se visualizará en la consola de SFTP de la siguiente manera:

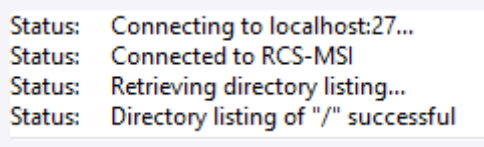


Figura 27. Estado de la conexión

5.3.3.6. Características Principales SFTP

Es que sólo usa un canal de comunicación, envía y recibe los mensajes en binario (y no en formato texto como hace FTP). Además, otorga protección contra el rastreo de contraseñas y ataques de los intermediarios. Protege la integridad de los datos mediante el cifrado, funciones criptográficas, y autenticación tanto del servidor como del usuario (latinoamericahosting, 2018).

5.4. Redes Virtuales Privadas (VPN)

Debido al crecimiento de las redes, los servicios al alcance de todos, La Agencia Metropolitana de Tránsito (AMT) y usuarios tienen otro punto de vista a la hora de implementar la interconexión de redes privadas de datos. Actualmente, estas redes privadas y la infraestructura de Internet están operando en paralelo. Sin embargo, todas las ventajas y beneficios ofrecidos a los proveedores de servicio y a los usuarios finales, está provocando que converjan en el concepto de red privada virtual (VPN).

5.4.1. Motivos para el uso de VPN

La Agencia Metropolitana de Tránsito tiene cuatro motivos por los cuales se debe elegir como un método de seguridad implementar VPN para las conexiones remotas que los funcionarios necesitan como se puede evidenciar en los siguientes puntos.

5.4.1.1. La movilidad geográfica de puestos de trabajo

Está llevando a las redes privadas de AMT a una situación ingestionable. Los usuarios necesitan conexiones que les permitan el acceso desde cualquier lugar del mundo. Esto se debe en la mayoría de los casos a los soportes de sistemas que usa la Institución como AS400, Socrit, End4sys entre otros. Estas circunstancias van en aumentado drásticamente el número de "oficinas remotas".

5.4.1.2. La necesidad de interactuar en línea

La AMT y sus proveedores están añadiendo un nuevo nivel de complejidad, en el cual muchas redes privadas deben tratarse de una forma independiente para su correcta integración y aislamiento respecto al resto. Para salvaguarda información importante como lo es la base de datos de vehículos e infracciones

5.4.1.3. El deseo de consolidar y simplificar la interfaz de usuario

Esto se ha convertido en un imperativo de negocio para los atacantes, dado que los usuarios son incapaces de defenderse frente a las nuevas aplicaciones del mundo digital se ven expuestos.

5.4.1.4. El alto coste para implementar y mantener redes privadas

Está llevando a éstas a una situación insostenible. Las líneas de larga distancia, así como los servicios conmutados, representan una serie de necesidades y costos innecesarios para la Agencia Metropolitana de Tránsito.

Existen cuatro razones de importancia que se llevan como institución municipal al uso de la VPN como una solución de seguridad y para esto en la Agencia Metropolitana de Tránsito, debe utilizar los equipos que se tiene disponible como lo es la marca fortigate, equipos que si se configuran con los parámetros

correctos nos ofrece dos tipos de VPN las cuales vamos a detallar a continuación.

Para ambos tipos de VPN usted crea configuraciones de Fase 1 y Fase 2. Ambos tipos se manejan en la capa de seguridad de inspección de estado, asumiendo que no hay IPS o AV.

5.4.2. Quienes puede usar VPN

En La Agencia Metropolitana de Tránsito, resultará muy útil el cifrado de la información desde el inicio del túnel VPN contar con protección mientras los datos viajan a través del internet hasta llegar al destino.

Se debe entregar explícitamente al personal encargado del soporte de software crítico.

Proveedores de servicios que este ubicado en otro país, y que bajo oficio escrito se solicite a la coordinación de Tecnología el acceso a la red.

Las solicitudes de permisos serán canalizadas a través del envió de la petición formal por cualquier medio hacia la máxima autoridad en la Coordinación de Tecnología de la Información, donde se asignará a través del aplicativo web mesa de ayuda un ticket que se asignará al administrador de red quien ejecutará la creación y entrega del acceso a la VPN.

5.5. Sistema de Prevención De Intrusos – IPS

Los sistemas de prevención de intrusos son una evolución de los IDS, son aquellos que permiten monitorear, detectar y reportar el mal uso de los recursos de una red de computadores con la diferencia que los IPS permiten adicionalmente prevenir los ataques de los intrusos. Los IPS realizan análisis más completos del uso de la red adoptando un enfoque preventivo

interviniendo activamente en caso de que en la red existan paquetes maliciosos o dañinos.

Además, necesita de configuraciones más complejas dependiendo de las políticas que maneje la empresa. A continuación, en la Figura 28, se presenta un diagrama de flujo general de un Sistema de Prevención de Intrusos:

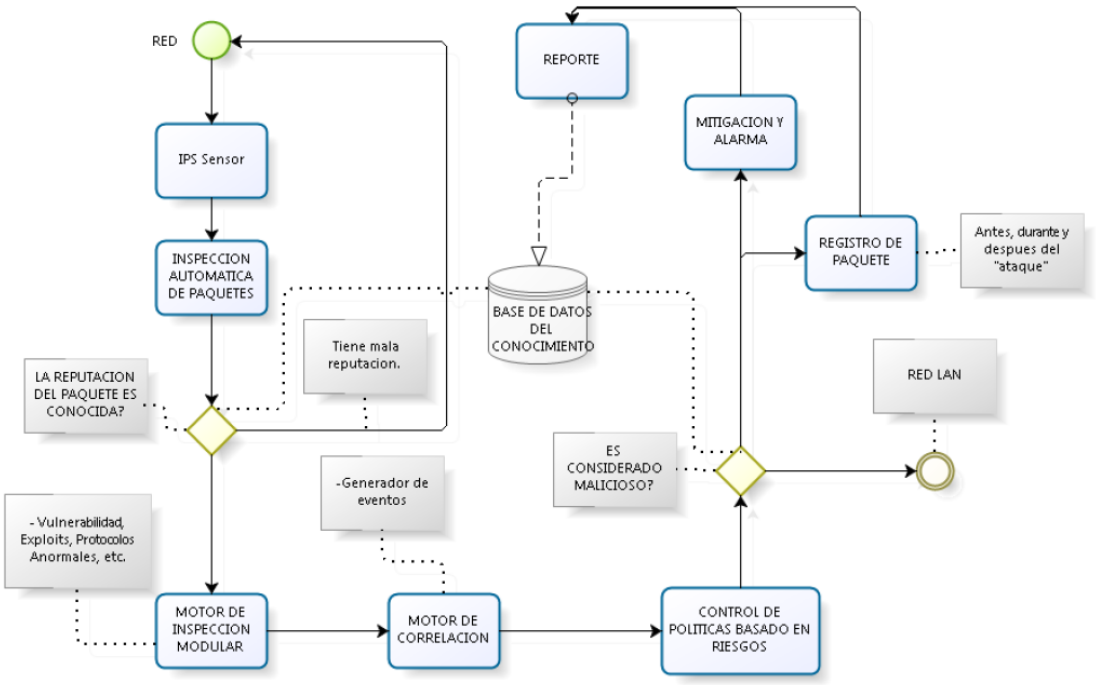


Figura 28. Diagrama Flujo de un Sistema de Prevención de Intrusos Tomado Programa Visio

5.6. Firewall e IDPS

Tanto los IDPS como los firewalls son herramientas creadas para utilizarse en conjunto y ambas permiten proteger la información en tiempo real, los IDPS son un complemento para los firewalls brinda mayor seguridad a los equipos. Los firewalls se encargan de bloquear a nivel de puertos y protocolos estando atento a los ataques de intrusos que se pueden dar desde el exterior, pero no a los ataques que se ejecutan en la red interna. Los IDPS buscan ataques en el propio firewall ya que existen ataques que no son controlados por los firewalls.

5.6.1. Uso de los IDPS

Los IDPS se encargan del control de las políticas de seguridad, Los IDPS son un complemento para los firewall, Los IDPS bloquean el paso de código maligno que no fue detectado por el firewall, Los IDPS llevan un registro de logs de las amenazas detectadas, Comprender frecuencia y naturaleza de los ataques, Impedir que usuario violen las políticas establecidas por la institución, Educar a los administradores de sistemas.

5.6.2. Diseño Propuesto

Luego de analizar la situación actual de la Oficina de Sistemas e Informática, se propondrá algunos cambios en el diseño de red.

Se debe implementar Sistemas de Prevención de Intrusos para la Red de la Agencia Metropolitana de Tránsito, el primero se colocará antes del firewall y de toda la red a proteger, esta configuración permitirá hacer frente a los ataques provenientes fuera de la red de la institución (desde la nube), el segundo se ubicará antes de la red de la (data center institucional), el cual permitirá prevenir todos los ataques que pueden originarse desde dentro de ella hacia los servidores.

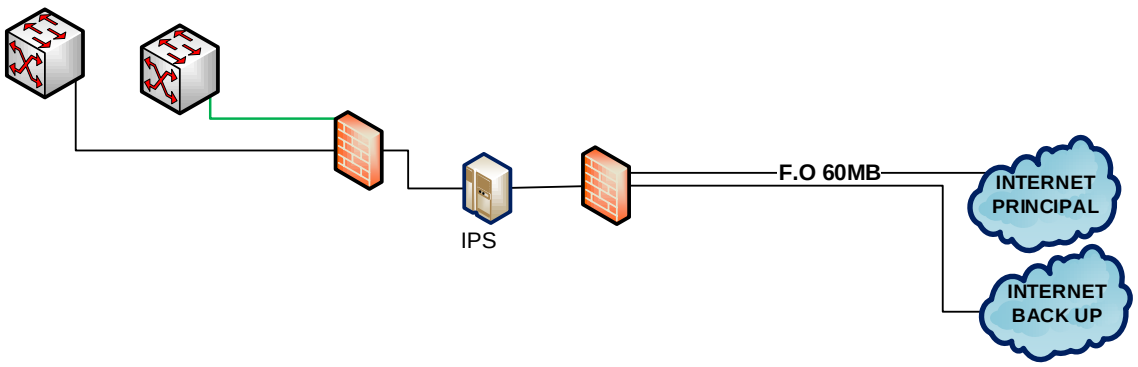


Figura 29. Propuesta para la topología de la red

Tomado del programa Visio

5.7. Redundancia y Alta disponibilidad de la Red

La Agencia Metropolitana de Tránsito debe proporciona acceso a la red para los grupos operativos de trabajo y los usuarios en general que consumen bases de datos de vehículos e infracciones para consultas en línea y así brindar a la ciudadanía un servicio de calidad frente a sus requerimientos en la competencia de Tránsito.

Para lograr este objetivo es necesario contar con un diseño jerárquico en la infraestructura de red que cumpla su función en base a un modelo de capas como se expone a continuación.

Un diseño típico de red LAN jerárquica de campus empresarial incluye la capa de acceso, la capa de distribución y la capa de núcleo. En las redes empresariales más pequeñas, puede ser más práctica una jerarquía de “núcleo contraído”, en la que las funciones de capa de distribución y de capa de núcleo se implementan en un único dispositivo. Los beneficios de una red jerárquica incluyen la escalabilidad, la redundancia, el rendimiento y la capacidad de mantenimiento.

Cuando se analiza el diseño de red, es útil categorizar las redes según la cantidad de dispositivos que se atienden:

- Red pequeña: proporciona servicios para hasta 200 dispositivos.
- Red mediana: proporciona servicios para 200 a 1000 dispositivos.
- Red grande: proporciona servicios para más de 1000 dispositivos.

5.7.1. Razones básicas para establecer infraestructura de red jerarquizada

Compartir de Base de Datos: debido a que se manejan información de vehículos se ha implementado un sistema de gestión de bases de datos para

permitir a los usuarios dentro de la empresa acceder a los archivos en diferentes sucursales.

Compartir recursos de red: Para optimizar equipos, la red proporciona un enlace de comunicación. Entre los recursos de red que se requiere compartir son las impresoras, dispositivos de almacenamiento y los recursos de comunicación.

Compartir programas y archivos: Estos programas y archivos que requiere la empresa, se guardan en un Servidor de Archivos, al cual los usuarios dentro de la red pueden acceder. La compra de licencias de software dentro de un servidor representa un ahorro significativo para la empresa, en vez de adquirir el software para cada equipo.

Separar las diferentes áreas: La red proporciona la creación de varios grupos, dependiendo de la función y estructura de la empresa, permitiéndole operar y acceder a la información de acuerdo al área de trabajo.

Correo electrónico: Para facilitar la comunicación entre cada usuario y asignar espacio de almacenamiento de correos se debe implementar un servidor Microsoft Exchange en la cual se incluirá calendarios, agenda de citas, reuniones, programación de tareas, recordatorios entre otros servicios.

5.7.2. Parámetros de seguridad general para dispositivos de telecomunicaciones

Implementar parámetros básicos de seguridad para el acceso a la interfaz de line de comandos (CLI o en ingles *Command Line*) la configuración estas medidas de seguridad es aplicado en router y switch.

5.7.2.1. Formato de nombre del dispositivo

La Tabla 21. Muestra los nombres de equipos de acceso que varían dependiendo al número de: piso, switch y departamento en los que vayan a ser implementados, este etiquetado es como una norma de seguridad para saber dónde están ubicados los equipos de comunicación.

Tabla 21. Formato de nombres

EQUIPO	DEPARTAMENTO	NOMBRE SWITCH
Switches de Acceso	Coordinación Servicios Ciudadanos	SW1.PB.CSC
	Coordinación de Registro de Infracciones	SW1.P1.CRI
	Coordinación Panificación y Compras Públicas	
	Coordinación de Talento Humano	SW1.P2.CTH
	Coordinación de Asuntos Internos	
	Coordinación de Seguridad Vial e Ingeniería de Tránsito	SW1.P3.CSVIT
	Coordinación Administrativa Financiera	SW1.P4.CAF
	Coordinación Asesoría Legal	SW1.P5.CAL
	Coordinación Tecnología de la información	SW1.P6.CTI
	Coordinación de Comunicación Social	SW1.P7.CG
	Coordinación General	

5.7.2.2. Establecer contraseñas de acceso.

Una contraseña segura es una contraseña que otras personas no pueden determinar fácilmente adivinándola o utilizando programas automáticos

Sugerencias para la creación de una contraseña segura: Debe incluir números, utilice una combinación de letras mayúsculas y minúsculas, Incluya caracteres especiales cualquiera de los siguientes (- * ? ! @ # $ / () {} = . , ; :), la contraseña debe tener una longitud mayor o igual a 8 caracteres, no debe tener espacios en blanco.

5.7.2.3. Deshabilitar el acceso http

Configurar un switch para eliminar el estado de servidor http por razones de seguridad. Ya que este protocolo es vulnerable como se evidencio en el marco teórico.

5.7.2.4. Determinar LAN virtual en el switch

Con la asignación de VLANS se logra segmentar el tráfico la VLAN, acrónimo de *virtual LAN* (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en una única red física.

Para organizar el tráfico de la información es necesario agrupar las VLAN de acuerdo a las areas de trabajo como se propone en la Tabla 22, también se agrega VLAN de gestión y seguridad a lista.

Tabla 22. Asignación de VLAN

DEPARTAMENTO	NÚMERO VLAN	NOMBRE VLAN
Coordinación Servicios Ciudadanos	100	V_CSC
Coordinación de Registro de Infracciones	110	V_CRI
Coordinación Panificación y Compras Públicas		V_CPyCP
Coordinación de Talento Humano	120	V_CTH
Coordinación de Asuntos Internos		V_CAI
Coordinación de Seguridad Vial e Ingeniería de Tránsito	130	V_CSVIT
Coordinación Administrativa Financiera	140	V_CAF
Coordinación Asesoría Legal	150	V_CAL
Coordinación Tecnología de la información	160	V_CTI
Coordinación de Comunicación Social	170	V_CCS
Coordinación General		V_CG
Vlan de Administración	200	V_ADMIN
Van de Servidores	201	V_SRV
Vlan de Voz	202	V_VOZ
Vlan de Agujeró Negro	300	V_BH

5.7.2.5. VLAN de aguajero negro

Los switches Cisco tienen una configuración de fábrica en la cual las VLAN predeterminadas se preconfiguran para admitir diversos tipos de medios y protocolos. La VLAN Ethernet predeterminada es la VLAN 1.

Por seguridad, se recomienda configurar todos los puertos de todos los switches para que se asocien a VLAN, pero diferente de la VLAN 1. Generalmente, esto se logra configurando todos los puertos sin utilizar en una VLAN de agujero negro que no se use para nada en la red. También se recomienda desactivar los puertos de switch sin utilizar para evitar el acceso no autorizado (cisco, 2018).

5.7.2.6. Asignar puertos del switch a la VLAN monitoreo

Quizá es una de las funciones más necesarias, pero menos utilizada en las redes donde se necesita analizar o monitorear el tráfico que por ella viaja. Tener un sistema de monitoreo en una red, por muy pequeña que sea, ayuda sin duda a tomar mejores decisiones respecto al funcionamiento, ampliación o modificación de la red ya que contando con información real, datos históricos e indicadores en tiempo real es posible precisar detalladamente lo que se necesita sin incurrir en gastos exagerados

El VTP reduce la administración en una red de switch. Al configurar una VLAN nueva en un servidor VTP, se distribuye la VLAN a través de todos los switches del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes.

5.7.2.7. Seguridad de puerto

Se limita el número de *MAC Address* seguras a uno y asigna un solo *MAC Address*, el puesto de trabajo asociado a ese puerto se asegura el ancho de banda completo del puerto.

Especifica una interfaz para configurar, y entra en el modo de configuración de la interfaz.

interface GigabitEthernet1/0/1

Se Habilita la interfaz como una interfaz Ethernet de una sola VLAN no etiquetada. Un puerto de acceso puede transportar tráfico en una sola VLAN. De forma predeterminada, un puerto de acceso transporta tráfico para VLAN1; con el siguiente comando configurado el puerto de acceso transporta tráfico para una VLAN diferente.

switchport mode access

Especificamos el número de VLAN para la cual este puerto de acceso transportará tráfico por ejemplo la VLAN 41 transportará datos.

switchport access vlan ”número de vlan”

Habilita la seguridad del puerto en la interfaz del switch.

switchport port-security

Cuando la dirección MAC de una estación intente acceder al puerto y esta diferente del *Mac Address* segura identificada se da una violación de seguridad

Establece el número máximo de direcciones MAC seguras para la interfaz. El rango es de 1 a 3072; el valor predeterminado es 1, en nuestro caso estamos configurando el acceso un máximo de dos MAC.

switchport port-security maximum 2

Se configura el tiempo de antigüedad y / o el tipo de antigüedad para la seguridad del puerto y se configura un tipo de acción para el puerto.

switchport port-security aging time 5
switchport port-security aging type inactivity

Permite que el puerto entre en un estado de envió (*Forwarding*) inmediatamente, pasando por alto los estados escucha (*Listening)* y aprendizaje *(Learning*).

spanning-tree portfast

Previene que un puerto. Unidad de datos de protocolo puente *Bridge Protocol Data Unit (BPDUs).* Si el puerto recibe un BPDU, el puerto es colocado en un estado de error-disabled como una manera de proteger el puerto.

spanning-tree bpduguard enable

La Agencia Metropolitana Tránsito debe implementar la propuesta de configuración para todos los puertos del switch en la capa de acceso siendo este el primer método para evitar que un atacante sin autorización pueda colarse a la red. Esta configuración se puede evidenciar en el siguiente resumen de comandos a implementar.

interface range g0/3-20
no shut down
switchport mode access

switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 2
switchport port-security aging time 5
switchport port-security aging type inactivity
spanning-tree bpduguard enable
switchport port-security violation shutdown

5.7.2.8. Deshabilitar los puertos que no se utilicen.

Como medida de seguridad se debe deshabilitar los puertos que no estén activos y solo será activado por el administrador de red para evitar que personas con criterio informático puedan infiltrarse a la red LAN.

5.7.3. Habilitar los parámetros de calidad de servicio

Calidad de Servicio, por sus siglas en inglés QoS (Quality of Service), es una de las características que debe tener una red convergente moderna bien diseñada (junto con Seguridad, escalabilidad y tolerancia a fallas) debido a que las aplicaciones y servicios que requieren los usuarios finales necesitan de la transmisión de voz y video en vivo con un buen nivel de QoE (Quality of Experience).

Pero la congestión en la red, la demanda excesiva de ancho de banda que generan dichas al ejecutarse simultáneamente aplicativos de voz y video es necesario mecanismos de control de tráfico y no degradar la experiencia del usuario

Cuando el volumen del tráfico supera la capacidad de la red, los dispositivos empiezan a "encolar" el tráfico en una memoria intermedia (búfers) hasta que la información pueda ser procesada y despachada. Es obvio que este encolamiento de paquetes provoca retardos en la red.

En este caso específico la VLAN de la calidad de servicio (*QoS*), se debe habilitar para el transporte de tráfico de voz que es generado por la plataforma de telefonía IP Avaya.

5.7.3.1. Cálculo de Ancho de Banda

G=256 Kbps (ancho de banda "garantizado" por usuario)
C=400 personas (Estimamos que 400 personas de la oficina estarán conectadas simultáneamente a Internet).

*AB = G * C*
*AB = 400 * 256 Kbps =* ***102400 Kbps.***

Recordemos que, 1 mega equivale a 1000 Kbps para la conversión de kilobit/segundo a megabit/segundo.

Es decir, 102 Mbps a Internet para una compañía de 527 empleados donde se estiman que navegan 400 personas simultáneamente.

5.7.3.2. Características del tráfico empresarial moderno

El tráfico de voz tiene un comportamiento predictivo y constante, es tolerante a pérdidas pequeñas de datos, además no consume todos los recursos de la red (benigno), no obstante, es muy sensible al retardo y mucho más al jitter. La voz emplea UDP en la capa de transporte por lo que no admite retransmisiones, lo que implica que debe tener prioridad sobre el resto de tráfico.

Tráfico de Video: Comparando el tráfico de video con el de voz, el primero resulta ser impredecible, inconsistente y no constante. A diferencia de la voz, el video es menos tolerante a la pérdida de datos.

Tráfico de Datos: Los datos empresariales que no son ni voz, ni video pueden tener comportamiento predictivo o no y pueden ser muy consumidores de recursos o no, todo depende del tipo de aplicación que esté corriendo en la red, pero, a diferencia de Voz y Video es insensible al retardo (se debe considerar si los datos son interactivos o no para ello) e insensible a la pérdida de paquetes debido a sus mecanismos de retransmisión por TCP.

5.7.3.3. Enlaces Backup

Enlace de datos, es el medio de conexión entre dos sitios distantes con el propósito de transmitir y recibir información. Que consisten en un transmisor y un receptor y el circuito de telecomunicación de datos de interconexión.

La Agencia Metropolitana de Tránsito actualmente cuenta con una infraestructura de fibra óptica que consta de 100 enlaces de datos y 04 enlaces de internet. Dentro de estos enlaces existen sucursales que manejan una prioridad alta con referencia al número de usuarios que se atiende y la cantidad de información.

Como se puede evidenciar en la Tabla 23. Son doce enlaces de datos de los centros de revisión técnica vehicular y enlaces principales que no cuentan con enlaces BackUp.

Tabla 23 Enlaces de Datos

N°	DEPENDENCIA
1	CENTRO DE REVISIÓN TÉCNICA VEHICULAR FLORIDA
2	CENTRO DE REVISIÓN TÉCNICA VEHICULAR DE GUAMANÍ
3	CENTRO DE REVISIÓN TÉCNICA VEHICULAR SAN ISIDRO
4	CENTRO DE REVISIÓN TÉCNICA VEHICULAR LOS CHILLOS
5	CENTRO DE REVISIÓN TÉCNICA VEHICULAR CARAPUNGO
6	CENTRO DE REVISIÓN TÉCNICA VEHICULAR GUAJALÓ
7	CENTRO DE MATRICULACIÓN TERMINAL QUITUMBE
8	CENTRO DE MATRICULACIÓN VEHICULAR BICENTENARIO
9	MATRIZ AMT TELEGRAFO PRINCIPAL
10	SISTEMA AXIS HACIA EL EDIFICIO MATRIZ DE AMT
11	AMT INTERCONEXIÓN (GPRS)
12	MATRIZ TELEGRAFO BACK UP DATOS

Los enlaces de internet son utilizados para publicar servicios web y aplicativos de tránsito como se puede ver en la Tabla 24, son cuatro en total con diferentes anchos de banda según la necesidad de cada sucursal.

Tabla 24 Enlaces de Internet

N°	DEPENDENCIA
1	MATRIZ AMT TELÉGRAFO INTERNET
2	CENTRO DE CAPACITACIÓN
3	COORDINACIÓN DE FISCALIZACIÓN
4	CENTRO DE GESTION DE LA MOVILIDAD

Teniendo en cuenta que se matriculan un aproximado 137 vehículos diarios en ocho centros de revisión y matriculación. La Agencia Metropolitana de Tránsito no puede verse afectada por interrupciones en el servicio por fallas en los enlaces datos o internet.

La Institución en base al modelo propuesto priorizará el brindar un mejor servicio a la ciudadanía con alta disponibilidad y para lograr este objetivo se debe financiar dieciséis enlaces para obtener redundancia en los enlaces de internet y datos.

5.7.4. Capa de acceso

En un entorno o áreas LAN de AMT, la capa de acceso debe otorgar acceso a la red para las terminales o estaciones de trabajo. En el entorno WAN, puede proporcionar acceso a la red empresarial para los trabajadores a distancia o los sitios remotos a través de conexiones WAN.

Como se muestra en la Figura 30. La capa de acceso para la red de una pequeña empresa, por lo general, incorpora switches de capa 2 y puntos de acceso que proporcionan conectividad entre las estaciones de trabajo y los servidores.

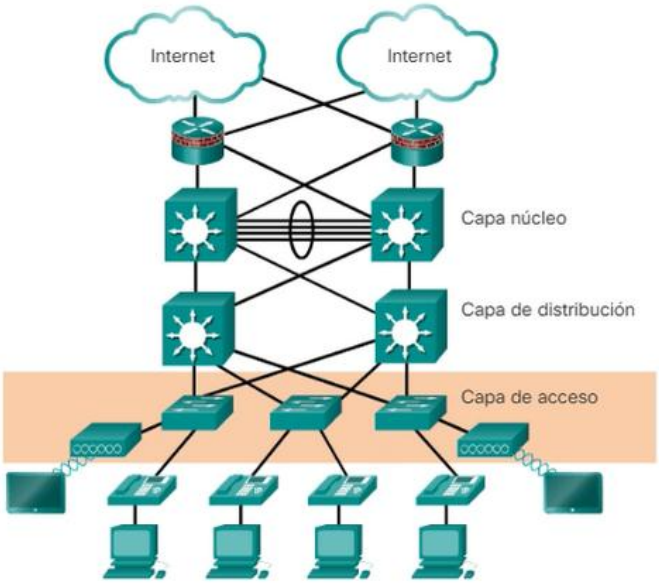


Figura 30 Capa de acceso

Tomado de (Walton, 2018)

Como se pude observar en el diseño los switches de acceso son la primera barrera desde los usuarios internos hacia los datos empresariales es importante mencionar que se deben tomar precauciones que son las siguientes: deben ser switch de capa 2, alta disponibilidad, seguridad del puerto, clasificación y marcación de QoS, y límites de confianza, inspección del protocolo de resolución de direcciones (ARP), listas de control de acceso virtual (VACL), árbol de expansión, alimentación por ethernet y VLAN auxiliares para VoIP.

La institución posee actualmente switches Cisco small business serie SG-300 de 24 y 48 puertos para el edificio matriz según la necesidad de usuarios de cada piso y el resto están instalados en sus principales sucursales como son centros de matriculación y oficinas administrativas.

En el levantamiento realizado se pudo detectar que los puertos no tienen configuración de seguridad, la configuración en la capa de acceso que se propone se basa en seguridad de puertos y alta disponibilidad para los switch en las oficinas del edificio matriz.

Se propone la compra del siguiente switch: Catalyst 9200 48-port PoE+, Network Essentials, transceiver GLC-SX-MMD 1000BaseSX SFP, Patch Cord Fibra Óptica Multimodo Duplex Lc-lc 3 M. Om3 Aqua. Para la plataforma de capa de acceso y distribuirlos en los 8 pisos del edificio matriz.

Para el ejemplo se realizará la configuración del switch perteneciente a la Coordinación de Servicios Ciudadanos, la siguiente configuración será igual para los ocho equipos con algunas excepciones en las IP´s y VLAN´s.

5.7.5. Capa de Distribución

En la actualidad la Agencia Metropolitana de Tránsito no posee un switch multicapa o router que maneje los grupos de trabajo o ruteo de VLAN, redundancia y balanceo de carga no se puede ofrecer disponibilidad en caso de fallos como se puede evidenciar en la Figura 31.

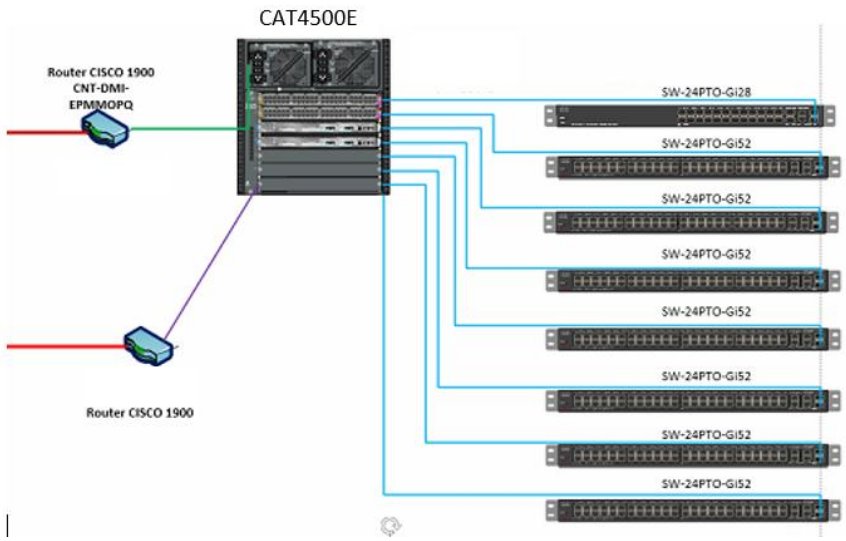


Figura 31. Esquema Actual

Un switch de capa de distribución puede proporcionar servicios ascendentes para muchos switches de capa de acceso. Para segmentar los grupos de trabajo y aislar los problemas de la red en un entorno de campus, se utiliza un switch multicapa o un router.

En la Figura 32. La capa de distribución es el límite entre los dominios de capa 2 y la red enrutada de capa 3

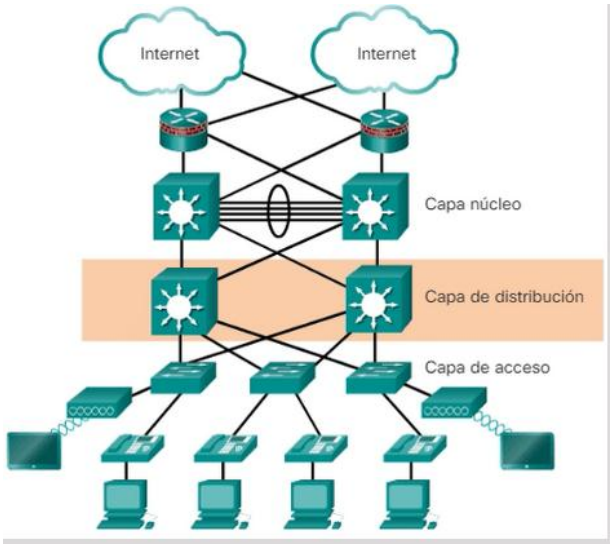


Figura 32. Capa de distribución

Tomado de (Walton, 2018)

La capa de distribución permitir lo siguiente: Agregación de enlaces LAN o WAN, seguridad basada en políticas en forma de listas de control de acceso (ACL) y filtrado, servicios de routing entre redes LAN y VLAN, y entre dominios de routing (p. ej., EIGRP a OSPF), redundancia y balanceo de carga, un límite para la agregación y la sumarización de rutas que se configura en las interfaces hacia la capa de núcleo.

El switch que se propone para la capa de distribución es Cisco Catalyst de la serie 4500 E, con un módulo de (8 Port Cisco Catalyst 4500 E 8 GE SFP Network Module C4500-NM-8-10) y transceiver SFP (CISCO GLC-SX-MMD= 1000BASE-SX SFP).

5.7.5.1. Activar el enrutamiento capa 3

Los switch traen habilitado la capa 2 por defecto, cambiarnos al modo routing debemos ingresar el siguiente comando para habilitar el modo ruteo o switch multicapa.

ip routing

El Switch de Distribución se configura para convertirse en un Root Bridge primario para los VLAN de datos 20,30,31,60,80,90,201,202 usando el comando primary VLAN de 10,30,100 raíces del atravesar-árbol Distribution1(config)#, y el Root Bridge secundario para los VLA N 20 de la Voz, 40, 200

spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree backbonefast
spanning-tree vlan 20,30,31,60,80,90,201,202 priority 8192
spanning-tree vlan 40,41,50,70, 91,200,300 priority 16384

5.7.6. Capa de núcleo

La capa núcleo debe tener una alta disponibilidad y debe ser redundante. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto, debe poder enviar grandes cantidades de datos rápidamente.

La capa de núcleo consta de dispositivos de red de alta velocidad. Estos están diseñados para conmutar paquetes lo más rápido posible e interconectar varios componentes de campus, como módulos de distribución, módulos de servicio, el centro de datos y el perímetro de la WAN.

Como se muestra en la Figura 33. La capa de núcleo es muy importante para la interconectividad entre los dispositivos de capa de distribución; por ejemplo, interconecta el bloque de distribución al perímetro de la WAN y de Internet.

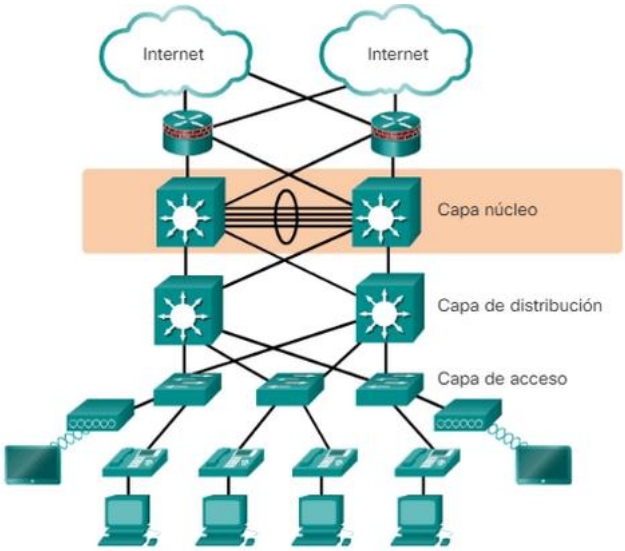


Figura 33. Capa de núcleo
Tomado de (Walton, 2018)

Las consideraciones que deben tomar en cuenta de la capa de núcleo y así lograr un correcto desempeño son: proporcionar switching de alta velocidad (es decir, un transporte rápido), proporcionar confiabilidad y tolerancia a fallas, lograr la escalabilidad, evitar la manipulación de paquetes que implica una gran exigencia para la CPU, la inspección, la clasificación de la calidad de servicio (QoS).

5.7.6.1. Redundancia EtherChannel- LACP

EtherChannel es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet.

5.7.6.2. Habilitar HSRP

Técnicamente, el HSRP envía un mensaje de saludo a la dirección de multidifusión 224.0.0.2 (todos los routers de la red) usando el puerto 1985 UDP para contactar con otros routers habilitados en el HSRP y establecer las prioridades: el router primario, con la prioridad más alta, funcionará como un router virtual.

5.7.7. Esquema de red jerarquizada propuesta

En la siguiente figura se expone gráficamente como debería estar estructurada la red de la agencia metropolitana de transito acoplado a un mecanismo de seguridad y alta disponibilidad.

EQUIPO	DEPARTAMENTO	NOMBRE POR PISO	EQUIPOS
Switch de Acceso	Coordinación Servicios Ciudadanos	SW1.PB.CSC	
	Coordinación de Registro de Infracciones	SW1.P1.CRI	
	Coordinación Panificación y Compras Públicas		
	Coordinación de Talento Humano	SW1.P2.CTH	
	Coordinación de Asuntos Internos		
	Coordinación de Seguridad Vial e Ingeniería de Tránsito	SW1.P3.CSVIT	
	Coordinación Administrativa Financiera	SW1.P4.CAF	
	Coordinación Asesoría Legal	SW1.P5.CAL	
	Coordinación Tecnología de la información	SW1.P6.CTI	
	Coordinación de Comunicación Social	SW1.P7.CG	
	Coordinación General		

Figura 34. Nombres y equipos por piso

Tomado de Excel

ICONOS	DESCRIPCIÓN
	EDIFICIO
	NUVE DE DATOS CNT
	ROUTER
	SWITCH CORE
	SWITCH ACCESO
	FIREWALL
	SUCURSAL REMOTO
	SERVIDOR

Figura 35. Identificación de iconos utilizados en el esquema

Tomado de Excel

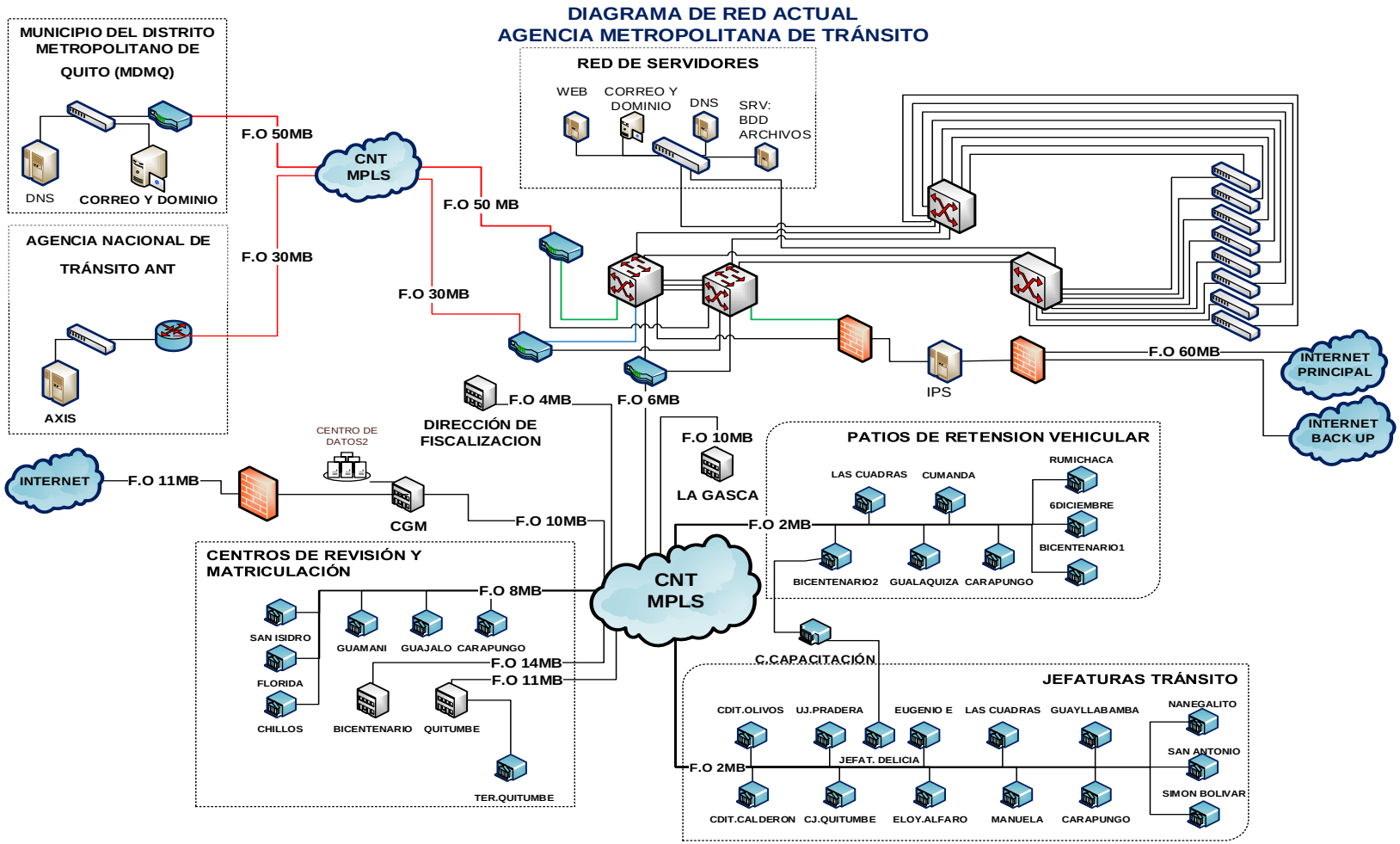


Figura 36. Esquema propuesto para la AMT

Tomado de programa Visio

5.8. Documentación de red mediante esquemas

Es una manera de analizar, mentalizar y organizar todos los contenidos, es la expresión gráfica de un resumen de un texto el cual se encarga de expresar gráficamente y jerarquizar diversas ideas sobre un contenido para que sea entendible tras una simple observación (concepto, 2017).

Un diagrama de red es la representación visual de una red de dispositivos que son parte de las telecomunicaciones y cómo interactúan entre sí. Ejemplo: enrutador, cortafuego, conmutadores como se muestra en la Figura 37. El esquema de una red LAN.

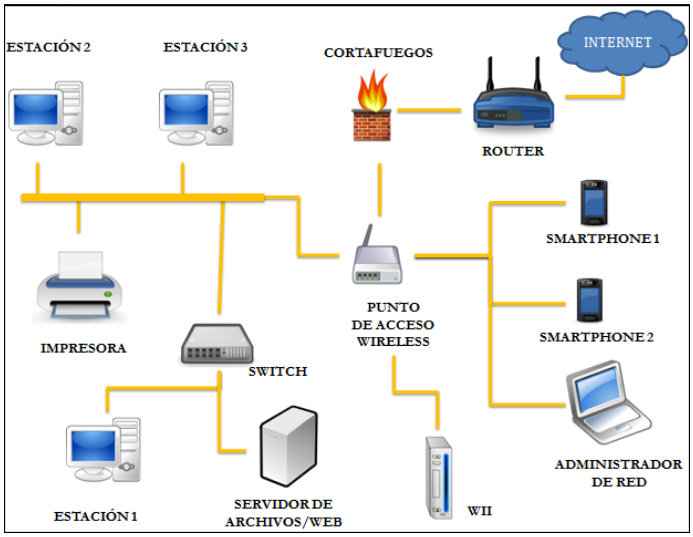


Figura 37. Esquema red LAN

Tomado de (Ruiz, 2015)

Dependiendo de la función que va a desempeñar un esquema de red varían los detalles específicos como la IP de una máquina en una red LAN o solo mostrar un panorama amplio como edificios o nodo centralizado en una red MAN.

5.8.1. Tipos de esquema de red

Esquema lógico. - Es un método para documentar la forma en que los datos viajan a través de la red, incluye entrada, procesamiento y salida. Por lo general consta que se detalla en la figura 38. Los siguientes elementos son los principales: subredes (incluidas direcciones, máscaras y nombre de VLAN), enrutadores, cortafuegos, y protocolos de enrutamiento.

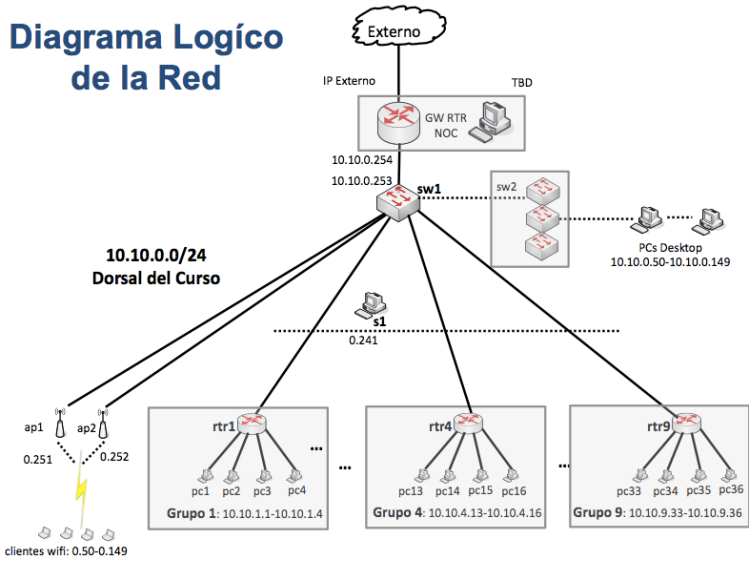


Figura 38. Esquema Lógico

Tomado de (nsrc.org, 2012)

Según el modelo (OSI), los diagramas de red lógicos se relacionan con la información que contiene la capa 3 (L3). Esta capa muestra lo fundamental de la gestión del reenvió de paquetes a través de enrutadores intermedios. La capa 2 (L2) es la conexión de datos entre los nodos cercanos, capa 1 solo es el diseño físico.

Esquema físico. - Es la ubicación específica de los componentes de red, incluye cables y hardware. Usualmente muestra la red física en plano de plantas confinadas a cuartos y edificios.

Los esquemas de red que posee del edificio matriz de La Agencia Metropolitana de Tránsito, no cuentan con descripción por áreas, identificación de VLANS, conexión unifilar del cableado estructurado, IP de los equipos principales que engloba un esquema lógico.

La propuesta como una política de seguridad en referencia a los esquemas de red es que se debe implementar un servidor de archivos virtuales donde se registre las versiones de cada uno y se pueda detectar fácilmente daños físicos o desconexión esta actividad se deberá realizar una vez al año en cada una de las dependencias de la AMT.

6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Con el levantamiento de requerimientos técnicos ejecutados en la Agencia Metropolitana de Tránsito tanto en hardware como en software se consigue determinar qué existen varias falencias de seguridad informática como: equipos tecnológicos que ya no están vigentes o actualizados, no existe control de acceso de usuarios internos y externos, no cuenta con una eficaz configuración de los dispositivos tecnológicos.

En el levantamiento se detectó claves expuestas, falta de políticas de seguridad informática donde el funcionario de la Agencia Metropolitana de Tránsito pueda tener una guía referencial del manejo y fortalecimiento de la clave para el acceso a sistemas críticos de la Institución.

Los equipos tecnológicos que han sido adquiridos por un proceso de contratación luego de finalizado el periodo de garantía técnica, no se ha seguido con un mantenimiento periódico para conservar el tiempo de vida útil que ofrecen los manuales del fabricante.

Mediante investigación se determinó que el Protocolo TCP/IP tiene falencias, un ejemplo de ello es FTP, TELNET son protocolos que ya no se encuentran vigentes y no transportan la información cifrada, lento en redes con volumen de tráfico medio bajo.

El personal de la Agencia Metropolitana de Tránsito no tiene una cultura de seguridad informática, iniciando desde sus altos ejecutivos hasta el personal que labora en la misma, tanto es así que se ha detectado que colocan adhesivos de las claves en la parte inferior de la pantalla o en los teclados.

La mayoría de los switches de la capa 2 de acceso en análisis realizado de un 100% de ellos, un 90% tiene habilitado la VLAN1 y las configuraciones de puertos de fábrica los cuales exponen el acceso no autorizado.

En el protocolo TCP/Capa transporte/datagramas IP, las principales vulnerabilidades son autenticación, integridad y confidencialidad. La denegación de servicio es el ataque más común en esta capa se ve asociada a la relación de protocolos de comunicación entre capas.

Las conexiones remotas son realizadas con software que ofrece el internet y no se está dando el uso adecuado a las funciones que posee el firewall actual.

Se ha detectado la ausencia de un equipo adicional de seguridad, es importante la presencia de un equipo IPSEG que actué en la capa de red y en la capa transporte para comunicar diferentes puntos de red de forma segura.

Con el fin de reducir al mínimo la pérdida de la alimentación principal de un enlace de Datos o de Internet, el método que produce mayor reducción de pérdidas es el balanceo de carga ya que se tiene en fases con sobrecarga.

Si la Agencia Metropolitana de Tránsito reduce las pérdidas o tiempo fuera de servicio, incide en forma directa en el mejoramiento de la calidad y eficiencia de los sistemas administrativos y a su vez la eficaz técnica para el control de las mismas.

6.2. Recomendaciones

Implementación de políticas de seguridad informática en la AMT con la finalidad de garantizar la seguridad física y magnética de la información de esta entidad pública; adquisición de equipos tecnológicos actualizados.

Se recomienda no usar FTP, TELNET en la Agencia Metropolitana de Tránsito ya que son protocolos antiguos y poseen varias desventajas al momento de competir con las nuevas tecnologías, además de ello remiten información no cifrada.

Socializar a todo el personal que labora en la Agencia Metropolitana de Tránsito sobre los riegos a los que esta propensa la Institución en caso de no acatar las políticas de seguridad informática, concientizando el compromiso del personal hacia la Institución a fin de crecer y mantenerse competitiva brindando servicio de calidad a la ciudadana.

Realizar un mantenimiento adecuado (preventivo y correctivo), de todos los equipos tecnológicos de la Agencia Metropolitana de Tránsito de forma continua según corresponda.

Luego de realizar estudios de campo en la Agencia Metropolitana de Tránsito se establece que lo más adecuado es implementación de protocolos seguros y se recomienda trabajar con TCP/IP usando el protocolo SFTP y complementando con el protocolo SSH con el fin de alcanzar comunicaciones seguras entre dos o más sistemas.

La implementación de un modelo jerárquico por capas donde se sugiere marcas de Switches, así como también tipos de configuraciones que ayudarán alcanzar una comunicación eficiente y eficaz con las diferentes dependencias, cumpliendo las políticas seguridad informática.

7. REFERENCIAS

Acosta, D. (2016). Usar la encriptacion minimizar entorno pci dss. Recuperado el 16 de febrero de 2018, de https://www.pcihispano.com/usar-la-encriptacion-minimizar-entorno-cumplimiento-pci-dss/

Adminso. (2014). *IDS*-Administración de Sistemas Operativos. Recuperado el 20 de julio de 2019, de http://www.adminso.es/index.php/Archivo:Imagen111.gif

Alcoba, J. L. (2011). *NAT* que es y como funciona. Recuperado el 24 de agosto de 2018, de https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona

Arg-Wireless.com.ar. (2011-2014). *Wireless*. Recuperado el 05 de febrero de 2018, de http://arg-wireless.com.ar/index.php?topic=1459.0

Blaustein, L. (2014). Cómo ayuda la segmentación de la red a proteger la red empresarial? Recuperado el 25 de noviembre de 2018, de https://searchdatacenter.techtarget.com/es/consejo/Como-ayuda-la-segmentacion-de-la-red-a-proteger-la-red-empresarial

Borghello , C. (2009). Seguridad Lógica - Identificación y Autentificación. Recuperado el 01 de enero de 2018, de https://www.segu-info.com.ar/logica/identificacion.htm

Borghello, C. (2010). Filtrado de paquetes. Recuperado el 01 de enero de 2018, de https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node232.html

branded content. (2014). Qué es y cómo funciona la NAT. Recuperado el 07 de mayo de 2018, de https://www.xataka.com/vodafoneadslafondo/que-es-y-como-funciona-la-nat

Brodbeck, C. (2016). Seguridad perimetral. Recuperado el 07 de Brodbeck, Cassio de 2018, de https://ostec.blog/es/seguridad-perimetral/proxy-transparente-beneficios-limitaciones

Capacity Academy. (2016). 8 Mejores Herramientas Para Cifrado De Información. Recuperado el 06 de febrero de 2018, de

http://blog.capacityacademy.com/2014/10/20/las-8-mejores-herramientas-de-cifrado-de-informacion/

Castellano, L. (2015). Sistemas Operativos. Recuperado el 01 de Febrero de 2018, de https://lcsistemasoperativos.wordpress.com/tag/cliente-servidor/

Castillo, L. (2016). *DTyOC*. Recuperado el 09 de Octubre de 2018, de https://dtyoc.com/2016/10/03/sistemas-operativos-moviles/

Ccm. (2008). Equipos de red - Pasarelas. Recuperado el 16 de octubre de 2018, de https://es.ccm.net/contents/294-equipos-de-red-pasarelas

Cisco. (2005). políticas de seguridad. Recuperado el 27 de Octubre de 2018, de cisco: https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/13601-secpol.html

Cisco. (2018). *Cisco Net Acad*. Recuperado el 20 de enero de 2019, de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/3.3.2.1/3.3.2.1.html

Cisco. (2018). Configuración *SSH* en las líneas equipo teleescritor con la opción de menú en el servidor terminal. Recuperado el 25 de septiembre de 2019, de https://www.cisco.com/c/es_mx/support/docs/security-vpn/secure-shell-ssh/212142-Configure-SSH-on-Tty-Lines-with-Menu-Opt.html

Clavei. (2018). Concepto de *IDS* - Ciberseguridad. Recuperado el 08 de julio de 2019, de https://www.clavei.es/blog/que-es-un-ids-o-intrusion-detection-system/

Community Foundation International. (1998-2016). GCFAprendeLibre. Recuperado el 22 de marzo de 2018, de https://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1.do

Comofuncionaque.com. (2016). Como funciona que. Recuperado el 13 de Abril de 2017, de http://comofuncionaque.com/tipos-de-virus-informaticos/

Concepto. (2017). Concepto de. Recuperado el 12 de diciembre de 2018, de http://concepto.de/esquema/

Cordoigne, J. (2015). Redes informáticas. Barcelona: Ediciones ENI.

Crespo, A. (2017). Ataques fuerza bruta. Recuperado el 20 de Octubre de 2018, de https://www.redeszone.net/2017/10/20/ataques-fuerza-bruta-debo-saber-puedo-protegerme/

Crespo, L. E. (2005). La Norma *ISO/IEC*. Recuperado el 02 de enero de 2018, de https://www.researchgate.net/publication/232252356_La_Norma_ISOIEC_17799_como_base_para_Gestionar_la_Seguridad_de_la_Informacion

Culturación. (2014). Qué es una denegación de servicio. Recuperado el 01 de abril de 2018, de http://culturacion.com/que-es-una-denegacion-de-servicio/

Diario el telégrafo. (2017). El Telégrafo. Recuperado el 02 de diciembre de 2018, de https://www.eltelegrafo.com.ec/noticias/judicial/12/los-hackers-emitieron-15-970-licencias-de-conducir-fraudulentas

Ediziones/Portaltic. (2017). Que es y para que sirve el servidor proxy. Recuperado el 03 de Abril de 2018, de http://www.europapress.es/portaltic/internet/noticia-sirve-servidor-proxy-20170403085932.html

Gisbert Vercher, B. (2015). Administración y auditoría de los servicios web. En B. Gisbert Vercher, Administración y auditoría de los servicios web (pág. 630). Editorial Elearning, S.L.

Golftheman. (2009). *Operating system placement*. Recuperado el 15 de Noviembre de 2018, de https://commons.wikimedia.org/wiki/File:Operating_system_placement-es.svg

Gomez, E. (2018). Tipos virus informaticos. Recuperado el 03 de junio de 2019, de https://tiposde.eu/tipos-virus-informaticos/

González, G. A. (2016). definicionabc tecnologia *arpanet*. Recuperado el 06 de Julio de 2018, de https://www.definicionabc.com/tecnologia/arpanet.php

Hewlett Packard Enterprise Development LP. (2018). *Hewlett Packard Enterprise*. Recuperado el 20 de octubre de 2019, de https://www.hpe.com/mx/es/what-is/network-security.html

IBM. (2016). Protocolos *TCP/IP*. Recuperado el 11 de enero de 2018, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.networkcomm/tcpip_protocols.htm

IBM. (2018). Identificación y autenticación -ibm. Recuperado el 23 de mayo de 2019, de https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.htm

informatica-hoy. (2007-2016). Informatica Hoy. Recuperado el 15 de junio de 2018, de https://www.informatica-hoy.com.ar/aprender-informatica/Que-es-el-sistema-operativo.php

Infotecs. (2019). IPS-Sistema de Prevención de Intrusos. Recuperado el 09 de julio de 2019, de https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html

ISO, N. (2011). Normas *ISO*. Recuperado el 20 de Agosto de 2018, de http://iso-actual.blogspot.com/p/isoiec-17799.html

Javier, & Nava. (2014). políticas se seguridad. Recuperado el 22 de mayo de 2018, de http://www.spi1.nisu.org/recop/al01/javier/part4.html

Latinoamericahosting. (2018). *FTP, SFTP y FTPS*: conociendo los diferentes protocolos para la transferencia de archivos. Recuperado el 17 de junio de 2019, de https://www.latinoamericahosting.com.co/ftp-sftp-y-ftps/

Lopez, A. (2014). Mecanismos básicos de control de acceso. Recuperado el 11 de noviembre de 2018, de https://www.incibe-cert.es/blog/control-acceso

López, A. (2015). Seguridad informática. España: Editex.

López, J. (2017). Los programas mas vulnerables que deberias actualizar. Recuperado el 15 de Mayo de 2018, de https://blogthinkbig.com/los-programas-mas-vulnerables-que-deberias-actualizar-lo-antes-posible

Lucas. (2003). Cortafuegos de filtrado de paquetes. Recuperado el 01 de enero de 2018, de https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node236.html

Marbelis. (2013). Archivo Virus. Recuperado el 16 de Febreo de 2018, de https://www.ecured.cu/Archivo:Virus.png

Marín, G. B. (2006). Directrices del Plan Director de Seguridad. Recuperado el 29 de mayo de 2018, de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=22&cad=rja&uact=8&ved=2ahUKEwjS1cinj6TjAhXxp1kKHUB3BjQ4FBAWMAF6BAgEEAI&url=https%3A%2F%2Fadministracionelectronica.gob.es%2Fpae_Home%2Fdam%2Fjcr%3A7e936665-10f7-4c30-a05d-67819d70423d%2Fdirectr

Masadelante. (1999-2018). Que es un troyano informatico. Recuperado el 19 de enero de 2019, de Que es un troyano informatico: http://www.masadelante.com/faqs/que-es-un-troyano

Mendoza, M. Á. (2014). 7 Consejos para cifrar tu información. Recuperado el 19 de Septiembre de 2018, de https://www.welivesecurity.com/la-es/2014/09/19/7-consejos-cifrar-tu-informacion/

Microsoft. (2017). Directrices para el bloqueo-supporte microsoft. Recuperado el 17 de enero de 2018, de https://support.microsoft.com/es-ec/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic

Nessus. (2019). Resultado Analisis. Recuperado el 20 de julio de 2019

Network Startup Resource Center.org. (2012). *NSRC*. Recuperado el 26 de enero de 2019, de https://nsrc.org/workshops/2012/walc-gestion/wiki/DiagramaLogico

Nsrc.org. (2012). *SNRC*. Recuperado el 09 de agosto de 2018, de https://nsrc.org/workshops/2012/walc-gestion/wiki/DiagramaLogico

Ok Hosting. (2016). que es un proxy. Recuperado el 12 de mayo de 2018, de https://okhosting.com/blog/que-es-un-proxy/

Panda. (2019). *IPS*-prevenga. Recuperado el 09 de julio de 2019, de https://www.pandasecurity.com/spain/enterprise/solutions/security-appliances/ips.htm

Paus, L. (2016). Cómo crear una contraseña fuerte en un minuto y proteger tu identidad digital. Recuperado el 06 de mayo de 2018, de https://www.welivesecurity.com/la-es/2016/05/06/crear-contrasena-fuerte-un-minuto/

Phifer, L., & TechTarget, S. (2018). Revise su empresa con herramientas de monitoreo de seguridad de red. Recuperado el 21 de julio de 2019, de https://searchdatacenter.techtarget.com/es/cronica/Revise-su-empresa-con-herramientas-de-monitoreo-de-seguridad-de-red

Pinto, M. (2014). Al fin *EEES* sistemas. Recuperado el 26 de Abril de 2018, de http://www.mariapinto.es/alfineees/sistemas/que.htm

Quijije Lopez, J. H. (2014). Laboratorio de hardware modelo *OSI Y TCP/IP*. Recuperado el 13 de agosto de 2018, de http://info2bachi.blogspot.com/2014/08/modelo-osi-y-tcpip.html

Rojas, A. (2013). Tele-Informatica. Recuperado el 01 de Febrero de 2018, de http://telei.blogspot.com/p/redes-tcpip-tcpip-y-sus-funciones-es-un.html

Ruiz, L. (2015). Red de Computadores y Elementos. Recuperado el 04 de Junio de 2018, de http://galicinformatica.blogspot.com/2015/06/de-una-red-de-computadores-una-red-de.html

Sanchez Avila, G. J. (2015). Tipos de sistemas de detección de intrusos. Recuperado el 09 de julio de 2019, de https://seguridadenredesgjsa.wordpress.com/firewall-y-otros-medios-de-defensa/idsips/

SlidePlayer.es. (2018). *slaplayer*. Recuperado el 22 de febrero de 2019, de http://slideplayer.es/slide/5551376/

Soler Amaya, S. (2016). Historia de redes de datos. Recuperado el 14 de Abril de 2018, de http://silviasoleramaya.blogspot.com/2016/04/enlace-discado.html

Solvetic Sistemas. (2017). Cómo crear y configurar túnel *SSH* en *Linux*. Recuperado el 20 de junio de 2018, de https://www.solvetic.com/tutoriales/article/3991-como-crear-configurar-tunel-ssh-en-linux/

Taringa. (2012). Tipos de virus informaticos y sus efectos. Recuperado el 04 de noviembre de 2018, de https://www.taringa.net/posts/info/15188786/Tipos-de-virus-informaticos-y-sus-efectos.html

Vialfa, C. (2017). Servidor *Proxy*. Recuperado el 04 de Diciembre de 2018, de https://es.ccm.net/contents/297-servidor-proxy-y-servidor-proxy-inverso

Walton, A. (2018). Diseño Jerárquico de Redes. Recuperado el 12 de julio de 2019, de https://ccnadesdecero.es/diseno-jerarquico-de-redes/

Yu, Z., & Tesai, J. (2011). *Intrusion Detection*: A Machine Learning Approach. Chicago: Imperial College Press.

Zoé, S. (2012). Sistema operativo. Recuperado el 10 de enero de 2018, de http://eq2-sistemasoperativos.blogspot.com/2012/04/14-clasificacion-de-los-sistemas.html

8. ANEXOS

Anexo 1

Cotización

Cotización de los implementos necesarios que contiene la propuesta de seguridad y alta disponibilidad para la Agencia Metropolitana de Tránsito a las siguientes empresas proveedoras:

Formato de cotización TELCOMBAS

TELCOMBAS
CONSULTORIA EN TELECOMUNICACIONES

PROPUESTA No:	GG-1506
OFERTA PARA:	AGENCIA METROPOLITANA DE TRANSITO
ATENCION:	SR. FREDDY CUYO
FECHA:	24 de junio de 2019
ASUNTO:	SWITCHES DE CORE Y ACCESO
Condiciones de Comercialización	
Precios:	Precios descritos en Dólares, no contienen I.V.A.
Forma de Pago:	ANTICIPO: 70%. CONTRA ENTREGA DEL EQUIPAMIENTO: 30% RESTANTE
Plazo de Entrega:	50 DIAS APROXIMADAMENTE
Validez de la Oferta:	8 días calendario

NRO PARTE	DESCRIPCION	QTY	V. UNITARIO	V. TOTAL
C9606R-48Y24C-BN-A	Catalyst 9600 Series 6 slot, 1xSup, 2xLC , DNA-A LIC	1	$ 95.285,71	$ 95.285,71
CON-SNTP-C9606R-4	SNTC-24X7X4 Catalyst 9600 Series	1	$ 37.328,45	$ 37.328,45
C9600-NW-A	Cisco Catalyst 9600 Network Advantage License	1	$ -	$ -
S9600UK9-1611	Cisco Catalyst 9600 XE 16.11 UNIVERSAL	1	$ -	$ -
C9600-CAMPUS-CORE	Catalyst 9600 Campus Core Deployment; For Tracking Only	1	$ -	$ -
C9606-FAN	Cisco Catalyst 9600 Series C9606 Chassis Fan Tray	1	$ -	$ -
C9606-SLOT-BLANK	Cisco Catalyst 9600 Series Blank for Chassis Module Slot	3	$ -	$ -
C9606-PWR-BLANK	Cisco Catalyst 9600 Series Blank for Power Supply Slot	1	$ -	$ -
C9600-DNA-A	Cisco Catalyst 9600 DNA Advantage Term License	1	$ -	$ -
C9600-DNA-A-3Y	Cisco Catalyst 9600 DNA Advantage 3 Year License	1	$ 25.892,86	$ 25.892,86
C9600-LC-48YL	Cisco Catalyst 9600 Series 48-Port 25GE/10GE/1GE	1	$ -	$ -
C9600-SUP-1	Cisco Catalyst 9600 Series Supervisor 1 Module	1	$ -	$ -
C9K-F2-SSD-960GB	Cisco Catalyst 9600 Series 960GB SSD Storage	1	$ 7.767,86	$ 7.767,86
C9600-LC-24C	Cisco Catalyst 9600 Series 24-Port 40GE/12-Port 100GE	1	$ -	$ -
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply	3	$ -	$ -
CAB-TA-NA	North America AC Type A Power Cable	3	$ -	$ -
C9200-24P-E	Catalyst 9200 24-port PoE+, Network Essentials	8	$ 3.190,00	$ 25.520,00
CON-SNT-C920024P	SNTC-8X5XNBD Catalyst 9200 24-port PoE+, Network Esse	8	$ 756,24	$ 6.049,92
C9200-NW-E-24	C9200 Network Essentials, 24-port license	8	$ -	$ -
C9200-NM-4X	Catalyst 9200 4 x 10G Network Module	8	$ 2.071,43	$ 16.571,43

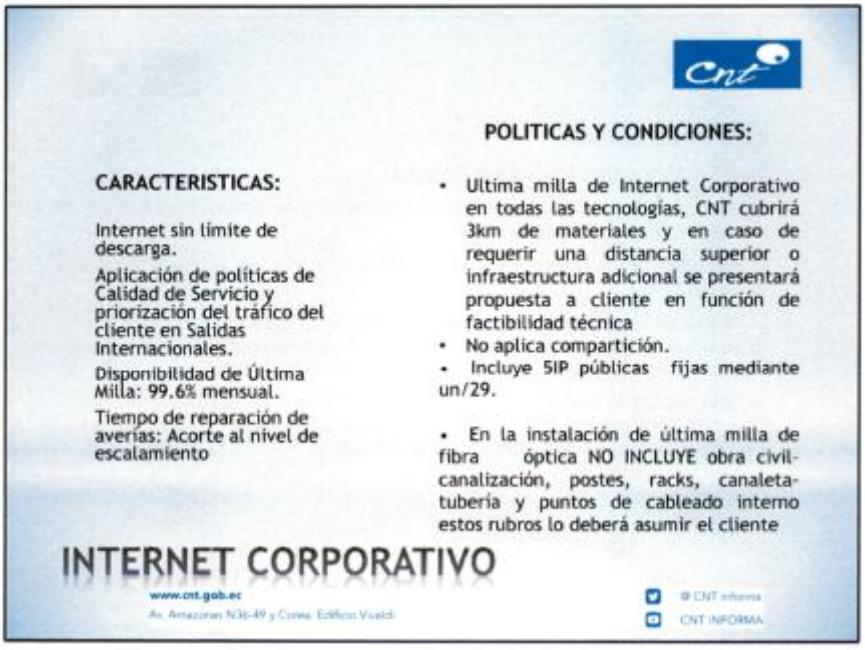
CAB-TA-NA	North America AC Type A Power Cable	8	$ -	$ -
PWR-C5-BLANK	Config 5 Power Supply Blank	8	$ -	$ -
C9200-DNA-E-24	C9200 Cisco DNA Essentials, 24-Port Term Licenses	8	$ -	$ -
C9200-DNA-E-24-3Y	C9200 Cisco DNA Essentials, 24-Port, 3 Year Term License	8	$ 631,79	$ 5.054,29
GLC-SX-MMD=	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	32	$ 517,86	$ 16.571,43
TOTAL SIN IVA		**236.041,94$**		

Notas:

* Todos los pedidos luego puesta la orden de compra, son irrevocables.
* La implementación de Servicios cubre estrictamente los alcances de este proyecto y da por sobreentendido que el contratante dispone de condiciones logicas y fisicas adecuadas para el despliegue de la solución.
* En caso de que la entrega de productos o servicios relacionados a este producto sufran retrasos, ya sea debido a problemas relacionados directamente a la marca o a temas externos a responsabilidad de Telcombas(Aduana, embarcadota, falta de stock

Corporación Nacional de Telecomunicaciones CNT-EP

Tarifario para enlaces datos e internet entregado por la CNT donde constan lo siguiente: Tipo de transmisión, disponibilidad, valor de inscripción, costo de enlaces principal y back up por cantidad de megas.



POLITICAS Y CONDICIONES

SERVCIOS SUPLEMENTARIOS DE INTERNET Y ENLACE DE DATOS	DETALLE	TARIFA
Traslados por CU	Previa verificación de permanencia del servicio mínimo 1 año - Valores por FO a cargar en el caso que no cumpla	$ 31,20
Traslados por FO	Previa verificación de permanencia del servicio mínimo 1 año - Valores por FO a cargar en el caso que no cumpla	$ 62,40
Ips Publicas Adicionales	Servicio mensual fijo	/28 (16 Ips) $8,00 /27 (32 Ips) $16,00 /26 (64 Ips) $32,00
Servicio de Upgrade por FO	A través de solicitud firmada por el cliente	En base al tarifario
Servicio de Donwgrade POR FO	A través de solicitud firmada por el cliente	En base al tarifario

Para traslados- Aplica la política comercial tanto de internet o enlace de datos
Los valores indicados son mas impuestos.

INTERNET CORPORATIVO- ENLACE DE DATOS

BACKUP DE ULTIMA

POLITICAS Y CONDICIONES MA MILLA

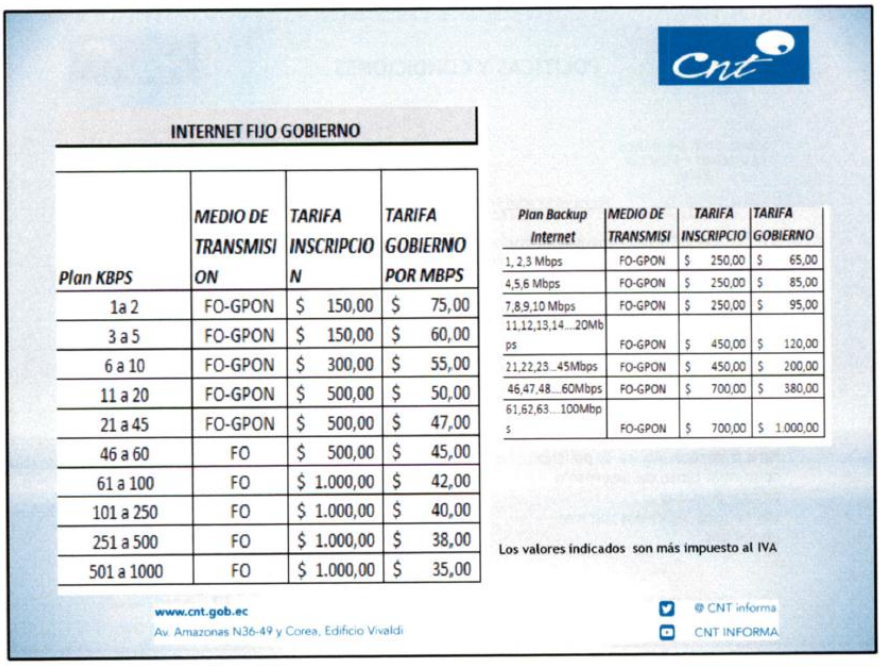
La disponibilidad de los servicios de Conectividad Corp.(Datos/Internet) con un Backup de Última Milla es de 99,8%.

El Backup tiene un esquema Activo-Pasivo (Enlace principal activo, enlace de backup pasivo

El backup debe ser instalado previa factibilidad técnica y en el caso de requerir un equipo adiciona la indicado en este esquema Activo-pasivo, tendrá un costo adicional a las tarifas de Backup de Internet Corporativa

Se debe aplicar la política de los 3Km de Fibra Óptica, en la cual no incluye obra civil-canalización, postes, racks, canaleta-tubería y puntos de cableado interno estos rubros lo deberá asumir el cliente

INTERNET CORPORATIVO



INTERNET FIJO GOBIERNO

Plan KBPS	MEDIO DE TRANSMISION	TARIFA INSCRIPCION	TARIFA GOBIERNO POR MBPS
1a 2	FO-GPON	$ 150,00	$ 75,00
3 a 5	FO-GPON	$ 150,00	$ 60,00
6 a 10	FO-GPON	$ 300,00	$ 55,00
11 a 20	FO-GPON	$ 500,00	$ 50,00
21 a 45	FO-GPON	$ 500,00	$ 47,00
46 a 60	FO	$ 500,00	$ 45,00
61 a 100	FO	$ 1.000,00	$ 42,00
101 a 250	FO	$ 1.000,00	$ 40,00
251 a 500	FO	$ 1.000,00	$ 38,00
501 a 1000	FO	$ 1.000,00	$ 35,00

Plan Backup Internet	MEDIO DE TRANSMISI	TARIFA INSCRIPCIO	TARIFA GOBIERNO
1, 2,3 Mbps	FO-GPON	$ 250,00	$ 65,00
4,5,6 Mbps	FO-GPON	$ 250,00	$ 85,00
7,8,9,10 Mbps	FO-GPON	$ 250,00	$ 95,00
11,12,13,14....20Mbps	FO-GPON	$ 450,00	$ 120,00
21,22,23...45Mbps	FO-GPON	$ 450,00	$ 200,00
46,47,48...60Mbps	FO-GPON	$ 700,00	$ 380,00
61,62,63...100Mbps	FO-GPON	$ 700,00	$ 1.000,00

Los valores indicados son más impuesto al IVA

www.cnt.gob.ec
Av. Amazonas N36-49 y Corea, Edificio Vivaldi

@ CNT informa
CNT INFORMA

Tarifas CNT de internet

Tomado de cotización CNT

RESPONSABILIDADES DEL CLIENTE:

- El cliente debe disponer de la acometida interna y energía regulada y asegurada(110Vaco-45Vdc)para la conexión de los equipos de la CNT.
- El cliente es responsable de obtener todos los permisos necesarios parar realizar trabajos de instalación reparación dentro de suspremisas.
- La instalación de infraestructura, ductería u otros dentro de las instalaciones del cliente, requiere de la previa aceptación de los costos adicionales que ello involucra
- Ultima milla enlaces de datos en todas las tecnologías, CNT cubrirá 3km de materiales y en caso de requerir una distancia superior o infraestructura adicional se presentará propuesta a cliente en función de factibilidad técnica.
- Disponibilidad de Última Milla: **99.6% mensual.**
- Aplican la política de instalación de FO PTP vigentes para Datos Interurbanos a partir de planes mayores e igual a 1 Mbps, previa factibilidad técnica.
- En la instalación de última milla de fibra óptica **NO INCLUYE** obra civil -canalización, postes, racks, canaleta -tubería y puntos de cableado interno estos rubros lo deberá asumir el cliente.

ENLACES DE DATOS LOCALES/NACIONALES

www.cnt.gob.ec
Av. Amazonas N36-49 y Corea, Edificio Vivaldi

@ CNT informa
CNT INFORMA

TARIFAS PARA ACCESOS LOCALES (PICHINCHA)

Servicios de Transmisión de Datos

ENLACE DE DATOS DISPONIBILIDAD 99,6%

VALOR DE INSCRIPCION	TX-DISPONIBILIDAD 99,6%	Megas Totales	Megas en unidades	Valores Actuales 2018	Valores Nuevos 2019
$ 120,00	FO	1.024	1	$ 67,00	$ 66,00
$ 120,00	FO	2.000	2	$ 100,00	$ 99,00
$ 150,00	FO	3.000	3	$ 114,00	$ 113,00
$ 160,00	FO	4.000	4	$ 139,00	$ 133,44
$ 160,00	FO	5.000	5	$ 206,00	$ 197,76
$ 230,00	FO	6.000	6	$ 225,00	$ 216,00
$ 230,00	FO	7.000	7	$ 248,00	$ 238,08
$ 230,00	FO	8.000	8	$ 271,00	$ 260,16
$ 230,00	FO	9.000	9	$ 305,00	$ 292,80
$ 230,00	FO	10.000	10	$ 329,00	$ 315,84
$ 230,00	FO	11.000	11	$ 357,00	$ 342,72
$ 230,00	FO	12.000	12	$ 384,00	$ 368,64
$ 230,00	FO	13.000	13	$ 412,00	$ 395,52
$ 230,00	FO	14.000	14	$ 439,00	$ 421,44
$ 230,00	FO	15.000	15	$ 467,00	$ 448,32
$ 230,00	FO	16.000	16	$ 494,00	$ 474,24
$ 230,00	FO	17.000	17	$ 522,00	$ 501,12
$ 230,00	FO	18.000	18	$ 550,00	$ 528,00
$ 230,00	FO	19.000	19	$ 577,00	$ 553,92
$ 230,00	FO	20.000	20	$ 649,00	$ 623,04
$ 230,00	FO	21.000	21	$ 677,00	$ 649,92
$ 230,00	FO	25.000	25	$ 787,00	$ 755,52
$ 300,00	FO	30.000	30	$ 856,00	$ 821,76
$ 300,00	FO	34.000	34	$ 937,00	$ 899,52
$ 300,00	FO	35.000	35	$ 961,00	$ 922,56
$ 300,00	FO	40.000	40	$ 1.081,00	$ 1.037,76
$ 300,00	FO	45.000	45	$ 1.168,00	$ 1.121,28
$ 450,00	FO	46.000	46	$ 1.192,00	$ 1.144,32
$ 450,00	FO	50.000	50	$ 1.288,00	$ 1.236,48
$ 450,00	FO	100.000	100	$ 2.393,00	$ 2.297,28
$ 800,00	FO	101.000	101	$ 2.413,00	$ 2.316,48
$ 800,00	FO	150.000	150	$ 3.428,00	$ 3.290,88
$ 1.000,00	FO	151.000	151	$ 3.448,00	$ 3.310,08

Cotización de enlaces de datos

Tomado de la cotización CNT

Backup-enlace de datos

Plan MBPS	MEDIO DE TRANSMISION	TARIFA GOBIERNO MENSUAL
1 a 20	FO-GPON	$ 35,00
21 a 30	FO-GPON	$ 55,00
31-45	FO-GPON	$ 55,00
46-100	FO-GPON	$ 115,00
101-150	FO-GPON	$ 145,00
151-1000	FO-GPON	$ 900,00

Traslados por FO-GPON	Costo Renovación $ 62,40

Traslados Por Cobre	Costo Renovación $ 31,20

Los valores indicados son más impuesto al IVA

Nota.- Para los BACKUP ACTIVO -ACTIVO se considera la tarifa del enlace principal 99,6%

Si el cliente requiere la disponibilidad de enlace de 99,8% se debe adicionar el valor del backup de tarifa mensual

ENLACE DE DATOS CAPACIDADES MENORES A 1MB

Capacidad (Kbps)	INSCRIPCIONES	% Disponibilidad	2018
128	100	99,60%	33
256	100	99,60%	32
512	100	99,60%	38

Nota.- Para los servicios con las capacidades menores a 1Mega se debe considerar el medio de transmisión es por cobre . Por fibra mínimo es 1MB.

Los valores indicados son más impuesto al IVA

ENLACES TEMPORALES

Para la implementación de enlaces temporales es previa factibilidad técnica y cotización en base a lo solicitado por el cliente.

En el caso que el cliente requiere el servicio de enlaces y no exista fibra en el lugar de instalación se informara el resultado de la factibilidad y costos de implementación.

NOTA IMPORTANTE:

- Los valores establecidos en este tarifario son en base al giro del negocio que mantiene MDWQ y sus dependencias.
- Para los servicios de conectividad se ha establecido las tarifas de acuerdo a las capacidades que son servicios ya existentes.
- Para servicios vigentes como DCV se mantiene el costo
- Para el servicio de hosting se mantiene el costo
- Para servicios nuevos de tecnologia TICS y que están dentro del portafolio de productos que maneja la CNT no se establece precio final en vista que esta sujeto a factibilidad tecnica y el dimensionamiento de recursos que solicite el cliente, se entregara la información previo requerimiento y cotización.
- Cualquier modificacion sobre enlaces ya implementados está sujeto a una factibilidad técnica.

"La Corporación Nacional de Telecomunicaciones CNT EP marca el paso en el crecimiento del desarrollo de tecnologías de la información y comunicación, incorporando estrategias que permita hacer negocios de conectividad, Cloud entre otros, enfrentar nuevos desafíos de las organizaciones es nuestro compromiso"

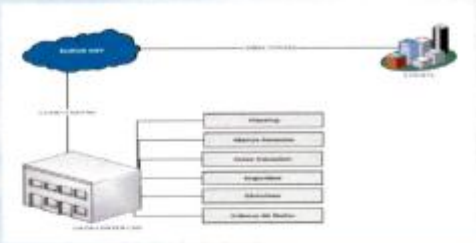
Elaborado por : Tania Cacuango-Analista de Mantenimiento de cuentas CNT EP

Revisado por : Juan Maldonado-Jefe Postventa y Backoffice Corporativa Sierra - Oriente (e)

Aprobado por: Ing. Santiago Rivera-Gerente de Negocios Corporativos y Gubernamentales

www.cnt.gob.ec
Av. Amazonas N36-49 y Corea, Edificio Vivaldi
@ CNT informa
CNT INFORMA

SERVICIOS TICS
DATA CENTER FISICO



Infraestructura de punta destinada a proveer espacio físico para la ubicación de equipos informáticos del cliente en condiciones óptimas para su funcionamiento

Nota.- Costos previa factibilidad técnica y oferta comercial vigente.

BENEFICIOS

- Disponibilidad de la infraestructura adecuada en poco tiempo.
- Seguridad de la información con alta disponibilidad y confiabilidad
- Eliminación del riesgo de pérdida de competitividad por obsolescencia tecnológica
- Flexibilidad y rápida escalabilidad

Esquema de Infraestructura como Servicio (IAAS).
El servicio da Data Center Virtual permite a un cliente contratar una computadora virtual (en la nube) la cual puede ser utilizada para correr aplicaciones propias de la operación de su negocio en lugar de comprar servidores físicos que involucran una fuerte inversión inicial y altos costos de operación, mantenimiento y licenciamiento (incluido el recurso humano

BENEFICIOS

Seguridad de la información con alta disponibilidad y confiabilidad.

Alta velocidad de lectura y escritura de datos.

Orientado a los clientes del servicio Data Center Virtual de los perfiles Gold y Silver que cuentan con un plan de crecimiento de grandes capacidades en memoria, procesamiento y almacenamiento

El cliente actualmente debe contar con umbrales de consumo mínimos de los recursos de memoria, procesamiento y almacenamiento

* DATA CENTER VIRTUAL

Anexo 2

Especificaciones Técnicas

Especificaciones Técnicas de dispositivos

La Tabla 9 enumera las especificaciones físicas del chasis Cisco Catalyst 9606.

Descripción	Presupuesto
SKU	C9606R
Dimensiones (Alto x ancho x profundidad)	35,43 x 44,2 x 40,9 cm 13.95 x 17.4 x 16.1 pulg.
Unidades de bastidor (RU)	8
Peso del chasis con 2 fuentes de alimentación (CA) y bandeja de ventilador	31,31 kg (69.03 lb)
Voltaje de entrada	CA: 90 V a 264 V, 47 a 63 Hz CA DC: -40V a -72V
Temperatura de funcionamiento	-5 ° a 45 ° C (23 ° a 113 ° F) hasta 6000 pies -5 ° a 40 ° C (23 ° a 104 ° F) hasta 10,000 pies
Temperatura de almacenamiento	-40 ° a 75 ° C (40 ° a 167 ° F)
Humedad relativa, funcionamiento y no funcionamiento, sin condensación.	10% a 95%, sin condensación
Altitud	-60 a 3000 m (-197 a 9843 pies)
Tiempo medio entre fallos (MTBF) (horas)	Chasis C9606R: 4,113,900 Bandeja de ventilador C9606: 452,570
Peso del chasis (sin bandeja de ventilador, sin PSU)	25,36 kg (55,90 libras)
Peso de la bandeja del ventilador	3,56 kg (7,85 libras)
Peso de las PSU individuales	Fuente de alimentación de CA: 1,2 kg (2,65 lb) DC PSU: 1.28 kg (2.82 lb)

Fuente de alimentación

Las fuentes de alimentación Cisco Catalyst 9600 Series admiten dos modos de operación.

Modo combinado

En modo combinado, la potencia disponible para todo el chasis es igual a la suma de la potencia de salida de todas las fuentes de alimentación multiplicada por la relación de participación. Las unidades de suministro de energía adicionales funcionan a ~ 90% de su capacidad En modo combinado, las fuentes de alimentación deben ser de igual potencia. Las fuentes de alimentación pueden ser mixtas de CA y CC, siempre que el voltaje de entrada de CA sea de 220V. La Tabla 7 muestra la potencia de salida para una, dos, tres y cuatro unidades de suministro de energía.

P = potencia de salida de una fuente de alimentación

Potencia total en modo combinado = P + (N-1) * P * (relación de distribución)

N = 1, 2, 3 o 4

Tabla 10. Potencia de salida en modo combinado

Voltaje de entrada	1 fuente de alimentación	2 PSU	3 PSU	4 PSU
110V	1050W	2040W	3030W	4020W
220V	2000W	3940W	5880W	7820W

Modo redundante N + 1

El chasis Cisco Catalyst 9600 Series también admite redundancia N + 1, con N circuitos de entrada independientes y protege contra la falla de uno (+1) de los circuitos durante una falla de la PSU. Las unidades de suministro de energía adicionales funcionan a ~ 90% de su capacidad. En modo redundante, las fuentes de alimentación deben ser de igual potencia. Las fuentes de alimentación pueden ser mixtas de CA y CC, siempre que el voltaje de entrada de CA sea de 220V. La Tabla 11 muestra la potencia de salida con dos, tres y cuatro PSU.

Tabla 11. Potencia de salida en modo N + 1

Voltaje de entrada	2 PSU	3 PSU	4 PSU
110V	1050W	2040W	3030W
220V	2000W	3940W	5880W

Tabla 12. Especificaciones de la fuente de alimentación

Característica de fuente de alimentación	C9600-PWR-2KWAC	C9600-PWR-2KWDC
Potencia máxima	2000W	2000W
Rango de voltaje de entrada y frecuencia	90VAC a 140VAC y 180VAC a 264VAC 47 a 63 Hz	-40VDC a -72VDC
Eficiencia de la fuente de alimentación	94% (típico)	92% (típico)
Corriente de entrada	CA 10.5A máx. A 115VCA (1050W) 7.8 A máx. A 230VCA (2000W)	DC 40A máx. A -48VDC (cuando se carga la fuente de alimentación completa)
Clasificaciones de salida	12V principal a 167A	12V principal a 167A
Tiempo de espera de salida	AC = 20 ms mínimo para el sistema	AC = 5 ms mínimo para el sistema
Receptáculos de entrada de alimentación	AC IEC 60320 C16	Amphenol C10-638976-000
Clasificación del cable de alimentación	AC 15A	DC 70A

Bandeja de ventilador

Cada conmutador Cisco Catalyst 9600 Series utiliza una única bandeja de ventilador útil para enfriamiento. Se puede acceder opcionalmente a los interruptores desde la parte posterior para una gestión flexible de los cables. El chasis está optimizado para armarios empresariales, con flujo de aire de lado a lado. Todas las bandejas de ventiladores están compuestas por múltiples ventiladores controlados independientemente. Si falla un solo ventilador, el sistema continuará funcionando sin una degradación significativa en el enfriamiento. Las velocidades del ventilador cambian dinámicamente para compensar la falla del ventilador. Los ventiladores Cisco Catalyst 9600 Series tienen un sensor barométrico, que permite curvas de velocidad del ventilador más lentas a altitudes más bajas. Los ventiladores también tienen un ajuste fino de modulación de ancho de pulso (PWM) individual para reducir la variabilidad en las revoluciones por minuto (rpm) del ventilador en condiciones de aceleración. El ruido acústico medido en un entorno de prueba formal de NEBS es 77.7 Lwad (dB). El chasis está diseñado para acomodar la operación sin ventilador de hasta 90 segundos para permitir la capacidad de servicio.

Cumplimiento de normas regulatorias

La Tabla 15 enumera el cumplimiento de los estándares reglamentarios para los switches Cisco Catalyst 9600 Series.

Tabla 15. Información de seguridad y cumplimiento (TBD)

Descripción	Especificación
Certificaciones de seguridad	C9606R •• IEC 60950-1 más Am1, Am2, Am9, Am10, Am11, Am12 y todas las desviaciones y diferencias •• AS / NZS 60950.1.2011 •• CAN / CSA-C22.2 No. 60950-1-07 •• GB 4943-95 •• EN 60950-1; 2006 más Am1, Am 2, Am9, Am10, Am11, Am12 y todas las desviaciones y diferencias •• NOM-019-SCFI-1998 •• UL 60950-1, segunda edición
Cumplimiento de EMI y EMC	47 CFR Parte 15 Clase A CNS13438: 2006 Clase A EN 300386 V1.6.1 EN61000-3-2: 2014 EN61000-3-3: 2013 ICES-003 Edición 6: 2016 Clase A KN 32: 2015 Clase A TCVN 7189: 2009 Clase A EN 55032: 2012 / AC: 2013 Clase A EN 55032: 2015 Clase A CISPR 32 Edition 2 Clase A V-2 / 2015.04 Clase A V-3 / 2015.04 Clase A CISPR24: 2010 + A1: 2015 EN 300386 V1.6.1 EN55024: 2010 + A1: 2015 KN35: 2015 TCVN 7317: 2003

Especificaciones Técnicas Catalyst 4500 E

La Tabla 6 enumera las especificaciones físicas.

Tabla 6. Especificaciones físicas del chasis Cisco Catalyst 4500 Series

Especificación	WS-C4503-E	WS-C4506-E	WS-C4507R + E	WS-C4510R + E
Dimensiones (H x W x D)	12.25 x 17.31 x 12.50 pulg. (31.12 x 43.97 x 31.70 cm)	17,38 x 17,31 x 12,50 pulgadas (44,13 x 43,97 x 31,70 cm)	19,19 x 17,31 x 12,50 pulgadas (48,74 x 43,97 x 31,70 cm)	24,35 x 17,31 x 12,50 pulgadas (61,84 x 43,97 x 31,70 cm)
Unidades de rack (RU)	7RU	10RU	11RU	14RU
Peso del chasis (con bandeja de ventilador)	32,25 libras (14,63 kg)	40.50 lb (18.37 kg)	44,50 libras (20,19 kg)	54,50 libras (24,73 kg)
Montaje	19 y 23 pulg. compatible con bastidor (hardware de guía de cable y bastidor de 19 pulgadas incluido)	19 y 23 pulg. compatible con bastidor (hardware de guía de cable y bastidor de 19 pulgadas incluido)	19 y 23 pulg. compatible con bastidor (hardware de guía de cable y bastidor de 19 pulgadas incluido)	19 y 23 pulg. compatible con bastidor (hardware de guía de cable y bastidor de 19 pulgadas incluido)

Indicadores de suministro de energía e interfaces

- LED de fallo de salida (por unidad): ROJO
- Entrada OK LED (por entrada): verde
- Ventilador OK LED (por entrada): verde

Las tablas 7 y 8 describen la especificación de la fuente de alimentación.

Tabla 7. Especificaciones de la fuente de alimentación de la serie Cisco Catalyst 4500E (solo datos)

Fuente de alimentación	1000W AC	1400 W de CA	Entrada triple de 1400 W CC
PoE integrado	No (solo datos)	No (solo datos)	No (solo datos)
Corriente de entrada (nominal)	12 A a 100 V CA, 5 A a 240 V CA	16 A a 100 V CA, 7 A a 240 V CA	Dos -48 VDC a 15A; Uno -48 VDC a 12.5A
Corriente de salida (datos)	• • 12V a 83.4A • • 3.3V a 12.2A	• • 12V a 113.4A • • 3.3V a 12.2A	• • 12V a 1360W • • 3.3V a 40W
Modo redundante de potencia de salida (datos)	1000W + 40W	1360W + 40W	1400W + 40W
Modo combinado de potencia de salida (datos)	1667W	2473W	-
Disipación de calor	943 BTU por hora	1048 BTU por hora	1048 BTU por hora
Tiempo de espera	20 ms	20 ms	8 ms
Intercambiables en caliente	Sí	Sí	Sí

Cumplimiento de normas regulatorias

La Tabla 9 enumera el cumplimiento de los estándares reglamentarios de las Cisco Catalyst 4500 y 4500E Series.

Tabla 9. Cumplimiento de normas regulatorias

Especificación	Estándar
Cumplimiento normativo	Marcado CE
La seguridad	• UL 60950 • CAN / CSA-C22.2 No. 60950 • EN 60950 • IEC 60950 • TS 001 • AS / NZS 3260
EMC	• FCC Parte 15 (CFR 47) Clase A • ICES-003 Clase A • EN55022 Clase A • CISPR22 Clase A • AS / NZS 3548 Clase A • VCCI clase A • EN 50121-4 • EN 55022 • EN 55024 • EN 61000-6-1 • EN 50082-1 • EN 61000-3-2 • EN 61000-3-3 • ETS 300 386
Industria EMC, seguridad y estándares ambientales	• NEBS Nivel 3 • ETS 300 019 Clase de almacenamiento 1.1 • ETS 300 019 Transporte Clase 2.3 • ETS 300 019 Uso estacionario Clase 3.1 • ETS 300 386
Telecomunicaciones (E1)	• CTR 13/12 • CTR 4 • ACA TS016
Telecomunicaciones (T1)	• FCC Parte 68 • Canadá CS-03 • JATE Green Book
Conformidad con la RoHS	ROHS5

Información de potencia y MTBF

La Tabla 10 proporciona información de potencia y tiempo medio entre fallas (MTBF) para diferentes chasis.

Tabla 10. Información de potencia y MTBF

Numero de parte	Potencia nominal máxima (W)	MTBF nominal (horas)
WS-C4503-E	60 60	1,064,279
WS-C4506-E	120	710,119
WS-C4507R + E	135	248,630
WS-C4510R + E	200	179,714

Nota: Todos los números de potencia que se muestran en la Tabla 10 son valores máximos recomendados para la planificación de la potencia de la instalación y la capacidad de enfriamiento. Estas cifras no son indicativas del consumo de energía real durante la operación. El consumo de energía típico es aproximadamente un 20 por ciento más bajo que el valor máximo mostrado.

Tabla 8. Especificaciones de la fuente de alimentación de la serie Cisco Catalyst 4500E (datos y PoE)

Fuente de alimentación	CA de 1300 W	2800W AC	4200W AC	6000 AC	9000 AC	1400W DC con módulo de entrada de energía (PEM)
PoE integrado	Sí (hasta 800W)	Sí (hasta 1400 W)	Sí (hasta 3855W)	Sí (hasta 4800W)	Sí (hasta 7500W)	Hasta 7500 W (menos la potencia consumida por los datos) cuando se conecta directamente a una planta de CC o 2 estantes de alimentación de CA externos
Corriente de entrada (nominal)	•• 16A a 100 VAC •• 7A a 240 VCA	•• 16A a 200 VAC	•• Dos 12A a 100 VAC O •• Dos 12A a 200 VAC	•• Dos 12A a 100 VAC O •• Dos 16A a 200 VAC	•• Tres 12A a 100 VCA O •• Tres 16A a 200 VAC	•• 31 A a -60 V CC (solo datos) •• 180A a -48 VCC (PoE)
Corriente de salida (datos)	•• 12V a 84.7A •• 3.3V a 12.5A	•• 12V a 113.3A •• 3.3V en 12.5A	•• 12V a 115.3A •• 3.3V a 12.5A	•• 12V a 186.9A •• 3.3V a 12.5A	•• 12V a 163.3A •• 3.3V a 12.5A	•• 12V a 120A •• 3.3V a 12.5A
Corriente de salida (PoE)	-50V a 16.7A	-50V a 28A	-50V a 77.1A (200V) -50V a 38A (100V)	-50V a 100.0A (200V) -50V a 38.5A (120V)	-50V a 150.0A (200V) -50V a 50.0A (120V)	140 A a -48 / -60 V CC
Modo redundante de potencia de salida (datos)	1000W + 40W	1360W + 40W	1383W + 40W	2200W + 40W	1960W + 40W	1360W + 40W
Modo redundante de potencia de salida (PoE)	800 W máximo por fuente de alimentación	1400 W máximo por fuente de alimentación	•• 3700W (220V) •• 1850W (110V)	•• 4800W (220V) •• 1850W (110V)	•• 7500W (220V) •• 2500W (110V)	Hasta 7500 W (menos la potencia consumida para datos)
Modo combinado de potencia de salida (datos)	1667W	2473W	2766W	4400W	3920W	-
Modo combinado de potencia de salida (PoE)	1333W	2333W	6700W (220V) 3360W (110V)	8700W (220V) 3360W (110V)	14,400 W (220 V) 4150W (110V)	3800W (100V)
Disipación de calor	1568 BTU / hora	2387 BTU / hora	3580 BTU / hora	2720 BTU / hora	3010 BTU / hora	Solo datos: 1591 BTU por hora Datos y voz: 2905 BTU por hora.
Tiempo de espera	20 ms	20 ms	20 ms	20 ms	20 ms	4 ms
Intercambiables en caliente	Sí	Sí	Sí	Sí	Sí	Sí

Notas adicionales para las tablas 7 y 8:

- •• La potencia de salida es por fuente de alimentación a menos que se indique lo contrario.
- •• Los números de disipación de calor representan las pérdidas de conversión de energía de la fuente de alimentación en funcionamiento.
- •• La cantidad de dispositivos de alimentación compatibles depende de la configuración del cliente.

Especificaciones Técnicas Catalyst 9200-48P-E

Especificaciones rápidas

La Tabla 1 muestra las especificaciones rápidas.

Modelo	C9200-48P-E
Los enlaces descendentes suman un total de 10/100/1000 o [illegible] puertos	[illegible] puertos
Configuración de enlace ascendente	Opciones de enlace ascendente modulares
Fuente de alimentación de CA primaria predeterminada	PWR-C5-1KWAC
Aficionados	FRU redundante
Software	Network Essentials
Ancho de banda de apilamiento	160 Gbps
DRACMA	4 GB
Destello	4 GB
Capacidad de conmutación	176 Gbps
Tasa de reenvío	261,9 Mpps
Dimensiones del chasis	1.73 x 17.5 x 13.8 pulgadas 4,4 x 44,5 x 35,0 cm
Peso	5,5 kilogramos

detalles del producto

La serie Catalyst 9200 proporciona estos aspectos destacados:

- Hasta 48 puertos de capacidad completa de Power over Ethernet Plus (PoE +)
- Resiliencia con unidades reemplazables en campo (FRU) y fuente de alimentación redundante, ventiladores y enlaces ascendentes modulares
- Opciones de enlace descendente flexibles con datos o PoE +
- Eficiencia operativa con apilamiento de plano posterior opcional, que admite el ancho de banda de apilamiento de hasta 160 Gbps
- UADP 2.0 Mini con CPU integrada ofrece a los clientes una escala optimizada con una mejor estructura de costos
- Seguridad mejorada con cifrado MACsec AES-128, segmentación basada en políticas y sistemas confiables
- Capacidades de capa 3, que incluyen OSPF, EIGRP, ISIS, RIP y acceso enrutado
- Monitoreo avanzado de red usando NetFlow completamente flexible
- Acceso definido por software de Cisco (SD-Access):
  - Operaciones e implementación simplificadas con automatización basada en políticas desde el borde hasta la nube administrado con Cisco Identity Services Engine (ISE)
  - Garantía de red y tiempo de resolución mejorado a través de Cisco DNA Center ™
- Plug and Play (PnP) habilitado: una oferta simple, segura, unificada e integrada para facilitar la implementación de nuevas sucursales o campus o actualizaciones de dispositivos en un red existente
- Cisco IOS XE: un sistema operativo basado en licencias comunes para la familia de productos empresariales Cisco Catalyst 9000 con soporte para modelo-

programabilidad impulsada y telemetría de transmisión

● ASIC con canalización programable y capacidades de micro-motor, junto con asignación configurable basada en plantilla de Capa 2 y Capa 3 reenvío, listas de control de acceso (ACL) y entradas de calidad de servicio (QoS)

Productos soportados

La Tabla 2 muestra los productos compatibles recomendados.

Módulos de red

Número de producto	Descripción del producto
C9200-NM-4G	Catalyst 9200 Módulo de red 4 x 1GE
C9200-NM-4X	Módulo de red Catalyst 9200 4 x 10GE, repuesto
C9200-NM-EN BLANCO	Módulo de red Catalyst 9200 BLANK

Kit y cables StackWise-80 y StackWise-160

Número de producto	Descripción del producto
C9200-STACK-KIT =	Repuesto de kit de pila C9200
C9200L-STACK-KIT =	Kit de pila C9200L de repuesto
STACK-T4-50CM	Cable de apilamiento tipo 3 de 50 cm
STACK-T4-1M	Cable de apilamiento 1M tipo 3
STACK-T4-3M	Cable de apilamiento 3M tipo 3

Licencias blandas

Número de producto	Descripción del producto
C9200-DNA-P-48	Término Premier C9200 DNA, 48 puertos: Incluye licencias a plazo para DNA Advantage, 25 ISE Base y 25 ISE Plus Puntos finales, 25 flujos Stealthwatch (incluyendo Virtual Flow Collector y Management Console). Requiere compra por separado del dispositivo ISE / ISE VM y el dispositivo DNA Center
C9200-DNA-P-48 -3Y	C9200 DNA Premier, 48 puertos, plazo de 3 años - DNA, 25 ISE PLS e ISE BASE, 25 SWATCH
C9200-DNA-P-48 -5Y	C9200 DNA Premier, 48 puertos, plazo de 5 años - DNA, 25 ISE PLS e ISE BASE, 25 SWATCH
C9200-DNA-P-48 -7Y	C9200 DNA Premier, 48 puertos, plazo de 7 años - DNA, 25 ISE PLS e ISE BASE, 25 SWATCH

Fuentes de alimentación

Número de producto	Descripción del producto
PWR-C5-1KWAC / 2 =	Fuente de alimentación de 1000WAC de repuesto

Comparar con artículos similares

La tabla 3 muestra la comparación.

Modelo	Descripción
C9200-48T-A	Conmutador de datos Catalyst 9200 de 48 puertos, ventaja de red
C9200-48T-E	Catalyst 9200 Switch de datos de 48 puertos, Network Essentials
C9200-48P-A	Conmutador PoE + Catalyst 9200 de 48 puertos, ventaja de red
C9200-48P-E	Catalyst 9200 Switch PoE + de 48 puertos, Network Essentials

Obtener mas informacion

¿Tiene alguna pregunta sobre el Cisco C9200-48P-E?

Especificaciones C9200-48P-E

C9200-48P-E Specification	
Downlinks total 10/100/1000 or PoE+ copper ports	48 ports full PoE+
Uplink configuration	Modular uplink options
Default primary AC power supply	PWR-C5-1KWAC
Fans	FRU redundant
Software	Network Essentials
Chassis Dimensions	1.73 x 17.5 x 13.8 in 4.4 x 44.5 x 35.0 cm
Weight	5.5 Kg
Virtual Networks	4
Stacking bandwidth	160 Gbps
Total number of MAC addresses	32,000
Total number of IPv4 routes (ARP plus learned routes)	14,000 (10,000 direct routes and 4,000 indirect routes)
IPv4 routing entries	4,000
IPv6 routing entries	2,000
Multicast routing scale	1,000
QoS scale entries	1,000
ACL scale entries	1,600
Packet buffer per SKU	6 MB buffers for 24- or 48-port Gigabit Ethernet models
Flexible NetFlow (FNF) entries	16,000 flows on 24- and 48-port Gigabit Ethernet models
DRAM	4 GB
Flash	4 GB
VLAN IDs	4096
Total Switched Virtual Interfaces (SVIs)	1000
Jumbo frames	9198 bytes
Wireless bandwidth per switch	Up to 48 Gbps on 24-port and 48-port Gigabit Ethernet model
Switching capacity	176 Gbps
Forwarding rate	261.9 Mpps
Mean time between failures (hours)	375,570