# UNIVERSIDAD TÉCNICA DE BABAHOYO

**FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA**

**PROCESO DE TITULACIÓN**

**MAYO 2019 - SEPTIEMBRE 2019**

**EXAMEN COMPLEXIVO O FIN DE CARRERA**

**PRUEBA PRÁCTICA**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE:**

**INGENIERÍA EN SISTEMA**

**TEMA:**

DIAGNÓSTICO DE LAS VULNERABILIDADES DE LA RED PARA PROPONER SOLUCIONES DE SEGURIDAD DE LA CTE DE BABAHOYO


**EGRESADO:**

MONTERO JONATHAN

**TUTOR:**

Ing. JOSÉ MEJÍA VITERI, MSc.


**BABAHOYO – LOS RÍOS – ECUADOR**

**2019**

# INTRODUCCIÓN

En el mundo contemporáneo, las diferentes instituciones que existen en el medio ya sean de índole pública o privada utilizan las redes informáticas para cumplir actividades como la comunicación interna o el establecimiento de metas planeados, por tal razón, las empresas establecen redes internas con el objetivo de facilitar y agilizar funciones que son consideradas de gran responsabilidad y con peso sustancial de información, por tal motivo, las redes tienen como función principal crear bases de datos que eviten el uso de espacio innecesario y la vez permita llevar un control sistematizado de las funciones de la organización.

La Comisión de Tránsito del Ecuador que está establecida en la ciudad de Babahoyo cumple con la función de regular y realizar el control de las actividades que prestan servicios de transporte, que de alguna u otra forma busca el modo de preservar la seguridad vial dentro de la ciudad, a través, de la ejecución de programas de capacitación, aplicación de sanciones monetarias, entre otros, basados en las leyes de transito establecidas en el país, por tal razón, esta institución fue creada a partir de la necesidad de salvaguardar la vida de las personas en las vías del país, ya que estas funciones las realizaban anteriormente la policía nacional y no las ejecutaban de la mejor manera.

La situación problemática que presenta la institución objeto de estudio es en el diagnóstico de la vulnerabilidad de la red debido a que presenta debilidades en su sistema de operaciones tales como de seguridad de confiabilidad, de amenazas por virus, entre otras, además, no cuenta con una estructura física adecuada por lo que se ocasiona fallos o interrupción en la red, lo que causa que los proceso se retrasen, además no tiene a su

disposición herramientas informáticas, que permita evaluar y verificar posibles ataque a la seguridad del sistema ante algún posible malware o cualquier situación exógena a la que este expuesta.

El caso de estudio está estrechamente relacionado con la línea de investigación de la carrera de ingeniería en sistema denominada como Desarrollo de Sistemas de la Información de la Facultad de Administración Finanzas e Informática debido a que se desarrolla un diagnóstico exhaustivo de la vulnerabilidad de la red de la institución objeto de estudio, es decir, se trata de identificar cuáles son las causas y consecuencias de persistir la problemática existente.

El presente trabajo investigativo tiene como objetivo fundamental efectuar un diagnóstico de la vulnerabilidad de la red de la Comisión de Tránsito de Babahoyo y a la vez proponer soluciones de seguridad de la misma, por tal razón, esta investigación se justifica bajo perspectiva profesional, académica y laboral debido a que son de suma importancia en garantizar la seguridad y protección integral de los habitantes fluminenses, por tal circunstancia se espera que sirva de análisis sustancial para aquellos individuos que interpreten el sustento del presente caso de estudio.

Cabe recalcar que la metodología utilizada en el presente trabajo fue el tipo de investigación descriptiva el cual consiste en efectuar una descripción detallada y exhaustiva de múltiples aspectos de una situación en particular, para cual se utilizó el método deductivo que se basa en analizar minuciosamente hechos en particular de una situación en común, por tal motivo se aplicó la técnica de encuesta que mediante la ejecución de un

cuestionario de preguntas permitió recolectar la información necesaria que sirve de sustento en la elaboración y desarrollo del presente trabajo investigativo.

## DESARROLLO

La Comisión de Tránsito del Ecuador ubicada en las calles Segunda entre la calle “k” y calle “L” del cantón Babahoyo provincia de Los Ríos, es una institución dedicada a garantizar la seguridad de los ciudadanos fluminenses, a través, de mecanismos de control y vigilancia que regulen el trasporte terrestre y seguridad vial de las personas mediante la actuación efectiva de los agentes del orden aplicando la ley, normas, procedimientos y políticas de manera eficiente que permita satisfacer las expectativas del usuario y comunidad en general, además, la profesión de agente transito le aportará al crecimiento profesional y personal de cada uno de los que conforman la institución objeto de estudio.

Es necesario mencionar que esta noble institución tiene metas y objetivos propuestos para ejecutarlas en periodo de tiempo relativamente corto en beneficio a la comunidad fluminense, es por ello que tiene como misión la planificación, organización, dirección, control y regularización de la gestión del transporte, seguridad vial, tránsito dentro del territorio local y nacional, a la vez toma de decisiones que coadyuven a la preservación del medio ambiente de las aéreas que rodea la ciudad y de aporte sustancial para que contribuyan al desarrollo del país en el ámbito en que se desenvuelve.

Ahora bien, la situación problemática que se evidencia en la Comisión de Tránsito del Ecuador ubicada en la ciudad de Babahoyo es la vulnerabilidad que presenta su red local, debido a que cuenta con ciertas debilidades de seguridad en la estructura y diseño de su sistema o simplemente un error de software o bugs, aunque, en la actualidad no existe un

sistema que garantice un 100% de seguridad, pero si programas que de alguna u otra forma están diseñados específicamente para proteger la defensa integral de la información de las instituciones de amenazas frecuentes que violentan la seguridad de un sistema.

Para el autor (Ortiz, 2014) menciona que "La defensa integral de los sistemas informáticos esta diseñados para protégelos de amenazas que implican un riesgo en el software mediante el uso de varios niveles de seguridad que evitan la penetración fácil de un intruso" (p. 36), por tal razón, los fallos o interrupciones que tiene el sistema de red ocasiona que los procesos se retrasen o no se resuelvan en el tiempo esperado, debido a que su políticas de seguridad son deficientes y la debilidades existente en sus protocolos de red provocan que no se satisfagan las necesidades y expectativas de la ciudadanía en general de forma eficiente y eficaz.

La topología de la red de la Comisión de Tránsito es deficiente por una mala distribución de los nodos que según el autor (Peinado & González, 2014) "Se determina como nodo informático cada uno de los equipos informáticos que se conectan a la red, es decir cuando los equipos de cómputo se interconectan entre sí, forma un nodo central" (p. 9)

Aspecto que provoca que el internet sea lento, pues su estructura básicamente cuenta con un solo punto de salida a internet con IP fija, además, el mantenimiento del cableado de la red no se la efectúa de la mejor manera posible debido a que no existen recursos monetarios o una partida presupuestaria asignada específicamente a efectivizar procedimientos de cuidado a los equipos informáticos que hacen posible la comunicación sistemática entre agentes que son necesarios para proponer soluciones de seguridad.

Además, la seguridad de la infraestructura de la institución objeto de estudio cuenta con un solo segmento en la red lo que impide que el tráfico de información se encamine a algunos servidores en específico al no encontrarse dividida en secciones tales como: de defensa, de perímetros, autentificación, gestión, control y estaciones de trabajo que permiten identificar con facilidad los riesgos o amenazas que podrían infiltrase en la red, al efectuar un diagnósticos de los computadores que posee la institución se encontró que no tienen a su disposición un sistema de detección de intrusos basado en Hots, que les permita detectar e identificar anomalías que representarían un riesgo potencial a futuro.

Cabe mencionar, que las vulnerabilidades de una red se pueden clasificar en varios aspectos y dentro del presente trabajo investigativo se analizarán la vulnerabilidad de red por medio de hardware, en donde se reconocerá e identificará el estado de los dispositivo físicos y lógicos con lo que dispone la institución para el correcto funcionar de su programa, y por software establecer la vulnerabilidad de programas, debilidad en diseño de protocolos, posible errores de programas y la posibilidad de existencia de puertas traseras en sistema.

Para analizar las vulnerabilidades y amenazas de la Comisión de Tránsito de la ciudad de Babahoyo, se tomó como referencia la ISO 27005 sobre la seguridad informática, la cual nos permite identificar en el contexto organizacional de la institución analizada, parámetros relacionados con la temática estudiada como el diseño inadecuado de red a través de un patch core, que según los autores (Khanh, Wagner, & Küng, 2016) "El Patch Core son los cables que conectan la red y las computadoras o sistemas electrónicos informáticos el cual está hecho de un material de plástico en el exterior y cobre en el interior" (p. 80).por ello,

se describe las determinación de amenazas y vulnerabilidades mediante una tabla, **Véase en anexo # 5**

Como se observó en la tabla Nº1 del anexo 2 se busca determinar cuáles son las vulnerabilidades y amenazas que presente la red de la institución, de manera descriptiva lo que da una idea clara del estado en que se encuentra los activos tangibles e intangibles a disposición para efectuar sus actividades en beneficio de la población, ahora bien, las debilidades y amenazas que están expuestos los activos informáticos también se las conoce como agujeros de seguridad que son los causantes de fallos de sistemas.

Una vez evidenciado los recursos tangibles e intangibles informáticos de la organización se procesa a diagnosticar la red, basado en el diagnóstico de estándar de la ISO 27005 para evaluar la seguridad de las redes informáticas, que según (Pandini, 2015) "Se centra en realizar buenas prácticas de gestión de seguridad de los sistemas de información que permite la oportunidad de tomar acciones correctivas de los puntos débiles de un software que garantice la seguridad de la información que cualquier institución sea esta público o privada" (p. 33). Por tal razón, se efectúa una lista de los activos físicos y lógicos que posee el organismo objeto de estudio con los responsables del óptimo funcionar de los mismos, **Véase en anexo # 5, tabla Nº2.**

En la cual se muestran los activos que dispone la institución para realizar sus diferentes procedimientos los cuales se observa que los responsables del optimo funcionar del software informático son individuos externos a la organización, razón por la cual, a continuación se procede a desarrollar una valoración de activos según la dependencia, su

funcionalidad, confidencialidad, integridad y disponibilidad de acuerdo a las normas ISO 27005 que son de aporte sustancial en proporcionar parámetros de evaluación de gestión de riesgo con eficacia y eficiencia.

En el anexo # 5, en la tabla Nº3 se determina cuáles serán los parámetros de análisis para efectuar una valorización de activos según la dependencia, funcionamiento, y demás parámetros objeto de estudio, los cuales serán de gran utilidad para realizar una objetiva ponderación de activos, tal como, se muestra en el **anexo # 5, tabla Nº4.**

Una vez, realizada la valoración de los activos basada en la norma ISO 27005 utilizada para establecer un efectivo sistema de gestión informática se puede determinar que el presente estudio demuestra que existen ciertos parámetros observables debido a que pueden estar expuestos a posibles amenazas y vulnerabilidades de su diseño y estructura informática, por tal, razón en el **anexo # 5, tabla Nº5** se muestra la probabilidad de ocurrencia de amenazas de las mismas que servirán como aspecto de interpretación y ponderación del estado de los sistemas.

A continuación, tomando como referencias las ejemplificaciones de amenazas y vulnerabilidades de la ISO 27005 sobre la seguridad informática, se han detectado vulnerabilidades de los activos informáticos de la Comisión de Tránsito del Ecuador. **Véase anexo # 5, tabla Nº6**

Las principales vulnerabilidades de la institución estudiada se deben a problemas de sistemas de cableados, inadecuado mantenimiento de switches, pc, portátiles, inadecuadas instalaciones eléctricas y una administración inapropiada de la red, donde no existe un personal encargado de diagnosticar la red y evitar espionajes remotos, congestionamiento,

manejo inadecuado de contraseñas y el deterioro de los activos informáticos de la organización. Para ello, se muestra los criterios de evaluación de riesgo según se grado o nivel de riesgo que presentare los activos. **Véase en anexo # 5, tabla Nº 7.**

Ahora bien, la parte medular de la investigación recae en el anexo # 5, tabla Nº 8 - 9 en donde se pretende evidenciar la vulnerabilidad y amenazas que tiene los activos que dispone la institución según el nivel de riesgo que presenta.

De acuerdo a la investigación realizada se puede determinar que la infraestructura informática de la Comisión de Tránsito presenta vulnerabilidad y amenazas de riesgo considerablemente altas, razón por la cual se observa que no cuenta con un diseño eficiente de su parte física y lógica y al no tomar acciones correctivas en tiempo y espacio mínimos podría causar el declive de las funcionalidad tecnológica de los mismos causando dificultades en su procedimientos y la respectiva perdida de información.

A continuación, de acuerdo al diagnóstico efectuado con el programa Network Inventory el cual recoge toda la información relevante de todos los dispositivos de la red para evaluar su estado actual, a través de estadísticas en este caso el análisis efectuado a la red de la Comisión de Tránsito que presenta. **Véase en anexo # 5, figura Nº 1.**

Al observar el diagnóstico realizado a la red para identificar posibles anomalías o causas que presenta, en este caso se puede apreciar el detalle de la vulnerabilidad que presenta el sistema informático en donde se puede conocer ciertos parámetros de amenazas en los controles de protección de la red como, es el caso del antivirus el cual no presenta su detalle actual, es decir, si está vigente o no, además, permite determinar cuál es el tipo de

procesador que posee la maquina principal de la organización y de toda la estructura de la red.

Por otra parte, la institución objeto de estudio no cuenta con una herramienta básica que le permita corregir los errores y falencias que presenta la red como es el caso de Network Inventory que según los autores (Romero & Figueroa, 2018) menciona que es un "Programa que permite efectuar un análisis integral de la estructura informática de diversos sistemas operativos mediante la realización de un escaneo que permitan conocer cuáles son los agujeros de seguridad que están expuesto a un ataque o intruso informático" (p. 47) motivo por el cual el no contar con un sistema que permita conocer la situación del sistema informático no se podrán efectuar los procedimientos de la mejor manera posible debido a que se podrían encontrar controles de acceso no deseados en la red.

Otra de las problemáticas que se pueden detectar es la falta de monitoreo de la red dentro de la Comisión de Transito de la ciudad de Babahoyo, puesto que como es conocimiento de todos, los programas y procesos debe de ser controlado por una persona capacitada en el área informática, si este no es revisado de manera constante presentará fallas e inconvenientes para la institución, por tal razón, se da a conocer que no existe el personal encargado de evaluar la estructura de la red, según la autora (Navarro, 2014) "La estructura de red es analizar las necesidades de un lugar específico, en el cual se determina los equipos que estarán interconectados por la red, el acceso a internet, entre otros aspectos que son necesarios para alcanzar el rendimiento informático óptimo que se espera de la Red LAN" (p. 2)

Según el autor (Ariganello, 2016) sobre las redes informáticas menciona que "El monitoreo de las redes está a cargo de un administrador de sistemas quien ejecuta un sinnúmero de procedimientos a seguir en la búsqueda de intrusos que sean considerado sustancialmente un riesgo para los usuarios finales en tiempos finitos" (p. 38), situación que no ocurre en la institución objeto de estudio debido a que la administración no evalúa constantemente las fallas que podrían presentar los servidores o la infraestructura de la red de la institución.

Por ello, al no realizarse el monitoreo de la red continuamente no se puede tomar en consideración cuáles son sus principales amenazas, en relación a las amenazas más común que pueden afectar la función de este sistema informático, que según el autor (Asimane, 2016) "Es una máquina virtual que a través del sistema operativo permite el almacenamiento y procesamiento de datos por medio de software, hardware y el individuo que hace uso de ella" (p. 100), por tal razón, se considera la filtración de información al sistema informático, mediante, de la creación de puertas traseras por personal que ya no está laborando, la falta de conocimiento de los usuarios de este sistema es otra de las falencias que se presentan en esta red, la gran mayoría de los colaboradores de esta institución no poseen ni las habilidades ni los conocimientos informáticos para manejar todo los procedimientos y cuidados que incluye este proceso.

Para ello, se efectúa un análisis del sistema de un servidor distinto en cual nos muestra la capacidad de almacenamiento del equipo de acuerdo a sus comparticiones disco local C, D.

**Véase en anexo # 5, figura Nº 2**

De acuerdo a la figura se puede identificar que la capacidad de almacenamiento del disco local C está al límite situación que causa lentitud al sistema operativo que puede traer consecuencias irreversibles al sistema que contenga, pues puede provocar la pérdida de información permanente, causando graves daños a la organización y representando un vulnerabilidad lógica del sistema, debido a la ineficiente administración e instalación de programas en un ordenador sin evaluar su capacidad de almacenamiento y procesadores que posea.

Por otra parte, la no aplicación de las políticas de seguridad es la principal falencia que existe dentro de esta institución y por la cual la red se encuentra en un estado de fácil vulneración, dentro de las organizaciones públicas se guarda un recelo de información y más si son datos de seguridad de la ciudadanía.

La Comisión de Tránsito en el diseño de su red cuenta con las conexiones de varios dispositivos, entre pc, portátiles, entre otros, los mismos que no cuentan con una protección adecuada de los archivos que en ellos reposan, por lo que cuando de forma inconsciente se instalan programas o abren links inapropiados puede afectar al sistema operativo y la red, debido a que existen muchos programas sin licencias legales o producen la instalación de virus que pueden eliminar la información; lo narrado ocurre porque los dispositivos que se conectan a la red no cuenta con software de seguridad ante la presencia de malwares. Según (Rascagneres, 2016)“El malware es un software informático que en español se traduce como software malicioso que detecta los posibles tipos de virus que pueden afectar los equipos de cómputo”. (p. 154)

Otra falencia que se puede determinar en la red de esta institución es la mala configuración que se realizó al momento de su programación porque fueron colocados ficheros que no son ejecutados de la manera correcta, también se puede evidenciar errores de diseño y de ejecución puesto que en la mayoría de las ocasiones que los usuarios pretenden utilizar la red esta les arroja un mensaje de error, generando así que los diferentes procesos que se elaboran a cabo dentro de esta institución no estén llevados bajo este sistema. Según el autor (Bezet Torres & Bonnet, 2016) (p. 89)

En este estudio se manifiesta que no existe un plan de contingencia eficiente que minimice los daños ocasionados en la institución que permitan detectar a tiempo las vulnerabilidades de la infraestructura del diseño de la red, por ejemplo, necesitan de una copia fuera de la dirección informática para mantener a salvo la información almacenada. Según el Sistema de Gestión Seguridad y Salud en el Trabajo (2015) "El plan de contingencia consiste en tener una preparación basada en las posibles vulneraciones de una actividad en específico que genere algún tipo de pérdida económica de una empresa u organización, este plan consiste en métodos y estrategias para cubrir las actividades afectadas." (p. 5)

En la comisión de tránsito no existe un área de informática ni un profesional para que atiende los problemas relacionados con la red, por tal razón no se implementan monitoreos, salvo el caso de problemas informáticos, donde tienen que realizar el llamado de personas con competencia en la rama de la informática, razón por la cual no detectan las posibles vulnerabilidades relacionadas con amenazas externas; puesto que la institución carece de protección al perímetro por la falta de software cortafuegos basados en host y proteger los servidores de las redes.

Los problemas relacionados con la vulnerabilidades de la red en ocasiones se debe a la ineficiente inspección de limpieza en las instalaciones en la Comisión de Tránsito, debido a que los equipos instalados por los proveedores de internet están colocados de manera compacta por lo que en un ligero movimiento pueden sufrir alguna caída o ser desconectados, afectando la funcionalidad de la conexión del internet, también se encuentran ubicados en el suelo rodeados de un entorno desorganizado, lo que provoca un desgaste pronto del cableado estructurado. ***Véase en Anexo Nº 6***

Según Mora Pérez, (2017) "Los mecanismos de seguridad son una técnica que se utiliza para implementar un servicio y está diseñado prevenir alguna amenaza de seguridad" (p.386). En la Comisión de Tránsito la falta de mecanismos de seguridad representa una situación de vulnerabilidad en el control del acceso al sistema informático debido a que no tienen instalado un programa de antivirus adecuado, sin embargo existe debilidad en el diseño protocolario utilizado en la red, es decir no implementan técnicas que sirvan de protección de seguridad basada en red, para minimizar riesgos de confiabilidad provocando situaciones que puedan afectar a la integridad de la institución.

De acuerdo con el autor Baca, (2016) la seguridad informática consiste en:" Disciplinas basadas en políticas, normas internas y externas de la institución, se encarga de proteger la integridad y privacidad de los datos almacenados controlando cualquier tipo de amenazas, riesgos lógicos y físicos a los que están expuestos los sistemas informáticos"(p.12) en la institución de la Comisión de Transito no se centran en controlar el acceso de las redes, no tienen un diseño apropiado para tratar problemas en el entorno de seguridad perimetral evadiendo aquellos mecanismos de protección con enfoques en la construcción de firewalls, exponiendo la autenticidad y confidencialidad de la información.

Dentro del diagnóstico de la Red que se encuentra en la Comisión de Tránsito del Ecuador en Babahoyo se detectan en una de las redes convergente fallas en la capa core o capa de núcleo, que de acuerdo al autor Cocero &García (2017) "La capa core es aquella que permite el respaldo y distribución de datos", se verifica que el backbone, es decir la estructura principal de diseño jerárquico de la red puede presentar problemas al momento de la conectividad con los diferentes dispositivos, que por vulnerabilidades de la red en determinados momentos limita la capacidad de transmitir datos a una velocidad adecuada, situaciones que afectan las actividades del personal administrativo, impidiendo que las funciones que desempeñen sean cumplidas con efectividad.

Por otra parte los routers de velocidad de acuerdo a el autor (Gómez Montes, 2017) "Son aquellos que proporcionan una serie de asistencias dentro de la capa de núcleo de la red LAN, los cuales dependerán de las necesidades y entre las acciones más comunes suministran los cambios de velocidad de los datos y se toleran las fallas que se puedan presentar" (p. 82), pero el dispositivo implementado en las instalaciones lleva varios años de función y las personas encargadas del mantenimiento de los equipos no han realizado el cambio pertinente del router instalado, por lo tanto es un factor condicionante de la falla detectada en la capa core de la Comisión de Tránsito.

La calidad de servicio que proporcione la capa de núcleo en la distribución de los datos a los demás distribuidores que se encuentran en las instalaciones de la Comisión de Tránsito es baja, debido al desinterés de los administradores para la renovación de equipos obsoletos que dificultan la disminución de fallas de la capa de núcleo porque uno de sus componentes no se encuentra en el estado pertinente para su funcionamiento.

# CONCLUSIONES

La red local de la Comisión de Tránsito presenta vulnerabilidades relacionadas con la conservación y mantenimiento que se les da a los equipos informáticos, debido a que presentan sistemas operativos antiguos, lo cual representa aspectos vulnerables que ocasionan el congestionamiento de la red, y el retraso de las actividades internas de la organización.

No existe la realización de monitoreo constantes de la red para identificar potenciales vulnerabilidades relacionadas con la combinación de caracteres en contraseñas, y la presencia de malware que afecten la gestión de archivos que reposa en la base de datos de la institución, que si bien mediante el diagnóstico de la red realizado por medio del programa Network Inventory.

La institución analizada no cuenta con un área informática dedicada a realizar evaluaciones periódicas que ayuden a identificar aspectos vulnerables que eviten el congestionamiento de la red o la presencia de amenazas externas, lo que ha ocasionado que en ocasiones tenga que contratar de forma ocasional a profesionales del área de informática para solucionar problemas en el diseño de red de la institución.

La actualización de los sistemas operativos de los equipos informáticos, navegadores, claves de usuarios y que el personal de la institución adopte políticas de seguridad en cuanto a la administración del área local que evite el congestionamiento de la misma o problemas de conectividad.

# REFERENCIAS BIBLIOGRÁFICAS


Ariganello, E. (2016). *Redes Cisco instalación y administración de Hadware y Software.* Madrid: Ediciones RA-MA.

Asimane, A. (2016). *Servicios RDS de Windows Server.* Barcelona: Ediciones ENI.

Baca Urbina, G. (2016). *Introduccion a la seguridad informatica.* Mexico: Ebook.

Bezet Torres, J., & Bonnet, N. (2016). *Windows Server Infraestructura de Red.* Barcelona: Ediciones ENI.

Cocero Matesanz , D., & García Garralón, M. (2017). *Informática aplicada: herramientas digitales para la investigación y el tratamiento de la información en humanidades.* Madrid: UNED - Universidad Nacional de Educación a Distancia.

Gómez Montes, A. (2017). *Estrategias de Internet.* Bogotá: ECOE Ediciones.

Khanh, T., Wagner, R., & Küng, J. (2016). *Future Data and Security Engineering.* Vietnam: Springer.

Mora Perez, P. (2017). *UF1347 Instalacion y configuracion de los nodos de interconexion de redes.* España: Elearning S.L.

Navarro, R. (2014). *Diseño de Sistemas en redes de área local.* Madrid: Paraninfo.

Ortiz, A. (2014). *Seguridad de la información.* Guatemala: Editorial Sancarlos de Guatemala.

Pandini, W. (2015). *ISO 27002.* MADRID : Editorial RA-Ma .

Peinado, M., & González, C. (2014). *Instalación y configuración de los nodos de una red de área local.* Madrid: Paraninfo.

Rascagneres, R. (2016). *Seguridad Informática y Malwares.* Barcelona: ENI Ediciones.

Romero, M., & Figueroa, G. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Madrid: Editorial Área de Innovacion y Desarrollo.

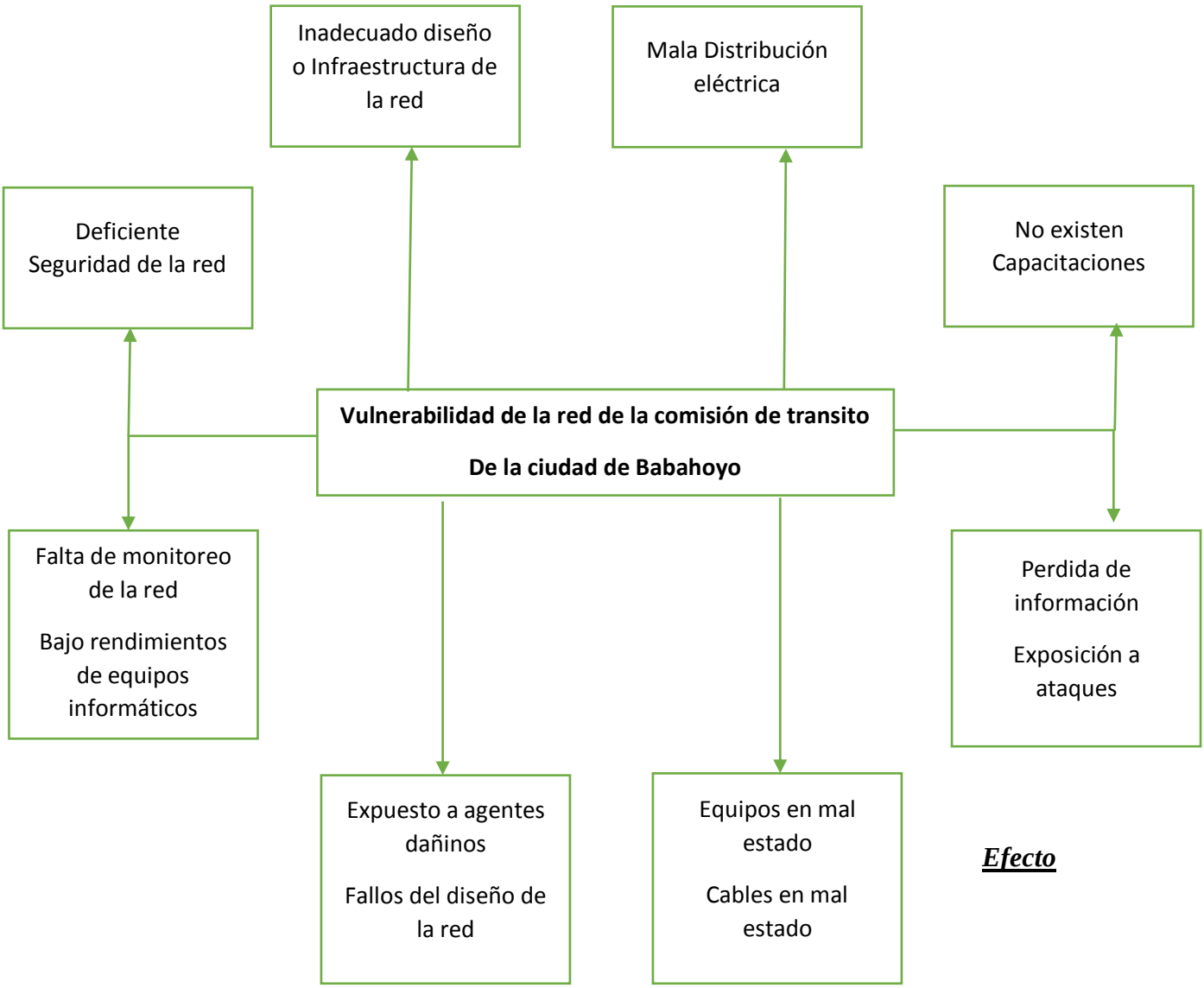
Sistema de Gestión Seguridad y Salud en el Trabajo. (2015). Plan de contingencia. *Plan de contingencias instituto distrital de recreacion y deporte Bogota D.c*, 1-124.

# Anexos

**ANEXO 1**

Árbol de problemas

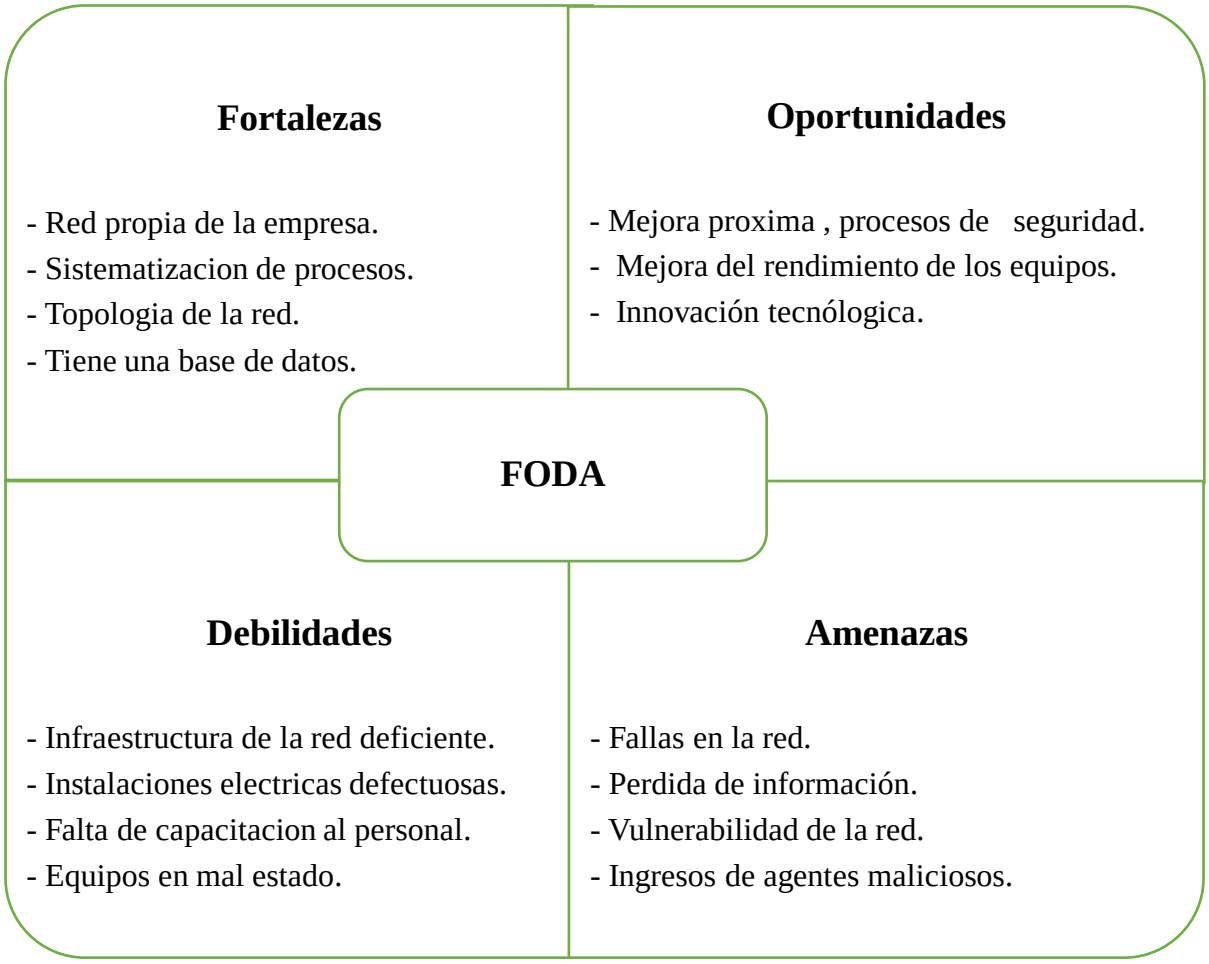
***Causas***




***Efecto***

**ANEXO 2**

Análisis FODA



UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZA E INFORMÁTICA

ESCUELA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS

**ANEXO 3**

Cuestionario de preguntas dirigidas al personal de la Comisión de Tránsito

1. **¿Dentro de esta institución existe internet de manera permanente?**

   Si ( )

   No ( )

2. **¿Conoce usted las políticas de seguridad de la red que se utiliza en esta institución?**

   Si ( )

   No ( )

3. **¿Posee usted el conocimiento necesario para el manejo de esta red?**

   Si ( )

   No ( )

4. **¿Existe el personal específico para el mantenimiento y cuidado de la red?**

   Si ( )

   No ( )

5. **¿El equipo tecnológico cuenta con aire acondicionado?**

   Si ( )

   No ( )

6. **¿Dentro de esta institución se utiliza firewall para proteger el ataque cibernético o de virus?**

   Si ( )

   No ( )

7. **¿Esta institución contrata personal externo para evaluación de la red?**

   Si ( )

   No ( )

8. **¿Considera usted que existe la confidencialidad de datos en la red de la Comisión de Transito?**

   Si ( )

   No ( )

   Desconoce ( )

9. **¿Conoce usted sobre la existencia de un plan de contingencia si llegase a ocurrir algún altercado en la red o en los equipos tecnológicos?**

   Si ( )

   No ( )

10. **¿Conoce usted si existe un programa que se dedique al diagnóstico de la red?**

    Si ( )

    No ( )

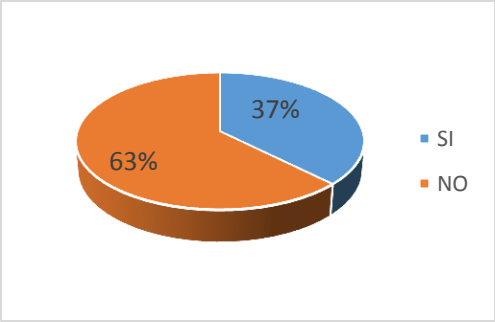
## ANEXOS # 4

## ANÁLISIS DE RESULTADOS

A continuación, se presenta los resultados obtenidos de las encuestas realizadas en la Comisión de Transito del Ecuador del cantón de Babahoyo para conocer cuáles son las vulnerabilidades de la red.

**¿Dentro de esta institución existe internet de manera permanente?**

| | Frecuencia | Porcentaje Válido | Porcentaje Acumulado |
|---|---|---|---|
| **SI** | 3 | 38% | 38% |
| **NO** | 5 | 63% | 100% |
| **TOTAL** | **8** | **100%** | |

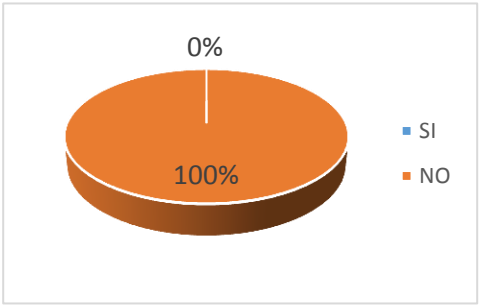



**Análisis:**

El personal que labora en la institución responde con un 63% que el internet de la institución no es constante, lo cual evidencia problemáticas en la red y lo cual ocasiona retrasos en los procesos que se llevan a cabo en la institución y con un 38% el personal responde de forma positiva.

**¿Conoce usted las políticas de seguridad de la red que se utiliza en esta institución?**

| | Frecuencia | Porcentaje Válido | Porcentaje Acumulado |
|---|---|---|---|
| **SI** | 0 | 0% | 0% |
| **NO** | 8 | 100% | 100% |
| **TOTAL** | **8** | **100%** | |

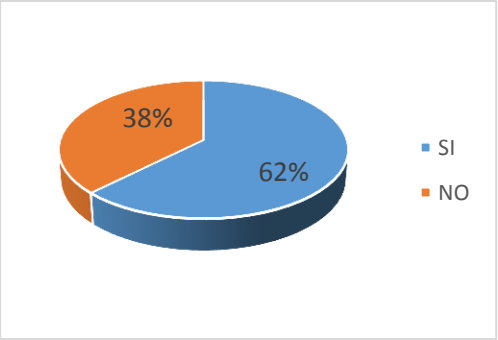



**Análisis:**

La totalidad del personal que labora en la institución manifiesta que no tiene conocimiento de las políticas de seguridad que son implementadas para que la red no sea vulnerada, lo cual proporciona un panorama de desconocimiento del manejo de herramientas técnicas para solucionar los posibles inconvenientes que se puedan presentar con respecto a la red de la institución.

**¿Posee usted el conocimiento necesario para el manejo de esta red?**

| | Frecuencia | Porcentaje Válido | Porcentaje Acumulado |
|---|---|---|---|
| **SI** | 5 | 63% | 63% |
| **NO** | 3 | 38% | 100% |
| **TOTAL** | **8** | **100%** | |

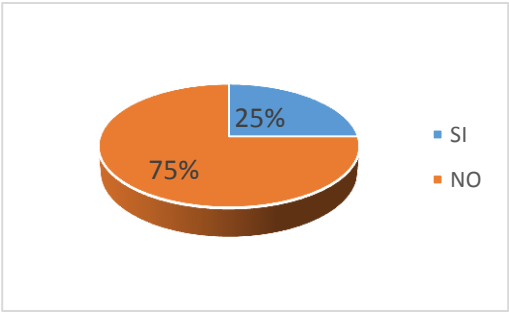



**Análisis:**

Los trabajadores de la Comisión de Tránsito del Ecuador, expresa con un 62% que, si es necesario poseer conocimientos básicos acerca del funcionamiento de la red, mientras que el 38% opina que no lo es, pero los conocimientos acerca de los protocolos básicos, permite a los colaboradores accionar esfuerzos, con respecto a una situación solicitada.

**¿Existe el personal específico para el mantenimiento y cuidado de la red?**

| | Frecuencia | Porcentaje Válido | Porcentaje Acumulado |
|---|---|---|---|
| **SI** | 2 | 25% | 25% |
| **NO** | 6 | 75% | 100% |
| **TOTAL** | **8** | **100%** | |

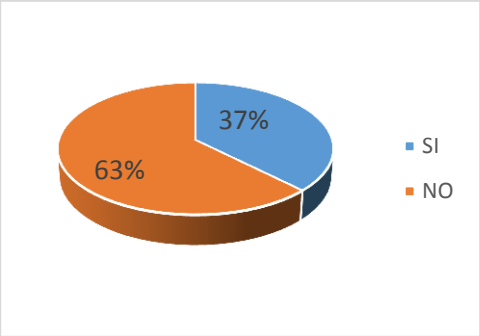



**Análisis:**

El personal no tiene conocimiento si existe un personal específico para el manejo y mantenimiento de la red con un 75%, mientras que el 25% siendo esta la parte administrativa comenta que se contrata un servicio particular para resolver los inconvenientes que se presentan con las conexiones de la institución.

**¿Dentro de esta institución se utiliza firewall para proteger el ataque cibernético o de virus?**

| | Frecuencia | Porcentaje Válido | Porcentaje Acumulado |
|---|---|---|---|
| **SI** | 3 | 38% | 38% |
| **NO** | 5 | 63% | 100% |
| **TOTAL** | **8** | **100%** | |




**Análisis:**

El personal comenta que los equipos de la institución no cuentan con firewall para la protección y seguridad de la información con un 63%, mientras que el 37% comenta que sus equipos si cuentan con firewall porque es necesario para mantener la información segura, ya que son los encargados de realizar trámites importantes para los usuarios del cantón.

## ANEXO # 5

**Tabla Nº1:** *Determinación de amenazas y vulnerabilidades según la ISO 27005*

| TIPOS | EJEMPLIFICACIÓN EN VULNERABILIDADES | EJEMPLOS DE AMENAZAS |
|---|---|---|

| | | |
|---|---|---|
| HARDWARE | Mantenimiento inadecuado | No cumplimiento del mantenimiento |
| | Exposición de polvo, humedad y suciedad | Deterioro de equipos |
| | Débil control de cambio de configuración | Inadecuado Uso |
| | Almacenaje sin la debida protección | Robo o pérdida de documento |
| SOFTWRE | Deficiente pruebas de software | Violación de derechos |
| | Configuración incorrecta de parámetros | Falla en el uso |
| | Gestión de contraseñas | Falsificación |
| | Software Nuevos | Inadecuado funcionar del software |
| | Débil respaldo de información | Manejo del software |
| | Descarga sin control de software | Manejo del software |
| RED | Líneas de comunicación no protegidas | Escucha subrepticia |
| | Sistema de cableados deficiente | Fallas de equipo de telecomunicaciones |
| | Congestionamiento de la red | Saturación del sistema |
| | Diseño inseguro de la red | Espionaje automático |
| | Punto único de falla | Fallas de equipo de telecomunicaciones |
| | Conexiones de red sin protección | Uso no autorizado |
| PERSONAL | Ausencia de personal | Disponibilidad del personal de informática |
| | Débiles políticas de seguridad | Uso no autorizado de los equipos |
| | Inadecuado uso del software y hardware | Usos erróneos |
| | Trabajo no monitoreado del personal de limpieza | Hurto de información |
| | No se realizan capacitaciones de seguridad | Usos erróneos |
| Lugar | Usos inadecuados la infraestructura física | Destrucción de los equipos |
| | Posibles inundaciones | Inundación |
| | Fluido eléctrico inestable | Pérdida de suministro de energía |
| | Falta de protección física | Robo de equipos |

**Fuente:** Norma ISO 27005

**Tabla Nº2:** *Activos de la Comisión de Tránsito del Ecuador – Babahoyo*

| ACTIVOS | RESPONSABLES |
|---|---|
| Router de red | Personal externo de informática |
| Switches de CTE | Personal externo de informática |
| Firewall | Personal externo de informática |
| Sistema de cableado | Personal externo de informática |
| Portátiles | Personal externo de informática |
| PC de escritorios | Personal externo de informática |

| | |
|---|---|
| Sistemas Operativos | Personal externo de informática |
| Correo Electrónico | Personal externo de informática |
| Quipux | Personal externo de informática |
| Servidor interno de correo electrónico | Personal externo de informática |
| Sistema eléctrico | Personal externo de informática |

**Fuente:** Norma ISO 27005

**Tabla Nº3:** *Valoración de los activos que dispone la Comisión de Tránsito*

| **Parámetros / valoración** | | **Dependencia** | **Funcionalidad** | **Confidencialidad, disponibilidad e integridad** |
|---|---|---|---|---|
| 1 | Muy Bajo | No guardan relación entre equipos para gestionar un proceso de servicio. | Capacidad de equipos informáticos limitadas | La no optimatización y disponibilidad de la configuración de programas y gestión de archivos pueden causar afectaciones irrelevantes a la realización de un proceso de servicio. |
| 2 | Bajo | Escasos equipos dependen entre sí, de para gestionar un proceso de servicio. | Capacidad de equipos informáticos limitadas | La no optimatización y disponibilidad de la configuración de programas y gestión de archivos pueden causar afectaciones a la realización de un proceso de servicio. |
| 3 | Medio | Una cantidad mínima de equipos dependen de para gestionar un proceso de servicio. | Capacidad de equipos informáticos limitadas | La no optimatización y disponibilidad de la configuración de programas y gestión de archivos pueden causar afectaciones a la realización de un proceso de servicio. |
| 4 | Alto | Un sinnúmero de equipos dependen para gestionar un proceso de servicio. | Capacidad de equipos informáticos limitadas | La no optimatización y disponibilidad de la configuración de programas y gestión de archivos pueden causar afectaciones a la realización de un proceso de servicio. |
| 5 | Criterio | Todos los equipos dependen entre sí, para gestionar un proceso de servicio. | Capacidad de equipos informáticos limitadas | La no optimatización y disponibilidad de la configuración de programas y gestión de archivos pueden causar afectaciones a la realización de un proceso de servicio. |

**Fuente:** Norma ISO 27005

**Tabla Nº4:** *Valoración de los activos que dispone la Comisión de Tránsito*

| **Activos de soporte** | **Funcionalidad** | **Confidencialidad** | **Disponibilidad** | **Integridad** | **Promedio** |
|---|---|---|---|---|---|
| Router de red | Disponen de configuración de la red de la Comisión de Tránsito | 4 | 4 | 4 | 4 |
| Switches de CTE | Encargados de controlar la conectividad de los equipos disponibles | 2 | 4 | 2 | 3 |
| Firewall | Controla el acceso a la red | 2 | 4 | 2 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | de un computador. | | | | |
| Sistema de cableado | Permite entrelazar la conectividad entre dispositivos. | 2 | 2 | 2 | 2 |
| Portátiles | Permite interactuar con los servicios y acceso de red que dispone la institución | 5 | 4 | 4 | 5 |
| PC de escritorios | Permite interactuar con los servicios y acceso de red que dispone la institución | 4 | 4 | 4 | 4 |
| Sistemas Operativos | Permita la ejecución de programas y acceder a ejecutar tareas | 4 | 4 | 4 | 4 |
| Correo Electrónico | Permite recibir y enviar archivos | 3 | 3 | 2 | 3 |
| Quipux | Permite la gestión documental | 3 | 2 | 3 | 3 |
| Servidor interno de correo electrónico | Equipo que envía, recibe y almacena correos para los usuarios | 3 | 3 | 2 | 3 |
| Sistema eléctrico | Provee de energía eléctrica a los equipos | 2 | 3 | 4 | 3 |

**Fuente:** Norma ISO 27005

**Tabla Nº5:** *Probabilidad de que ocurra amenazas en la red que dispone la Institución*

| Aspecto | Valoración | Descripción |
|---|---|---|
| 1 | Baja | Son aquellas amenazas que presentan vulnerabilidad mínima |
| 2 | Medio | Son aquellas amenazas que presentan frecuencia de vulnerabilidad estándar. |
| 3 | Alta | Son aquellas amenazas que presentan frecuencia de vulnerabilidad estándar. |

**Fuente:** Norma ISO 27005

**Tabla Nº6:** *Vulnerabilidades y Amenazas detectadas de la CTE Babahoyo.*

| Activo | Amenaza | Vulnerabilidad | Probabilidad que ocurra la amenaza | Facilidad de explotación |
|---|---|---|---|---|
| **Router de red** | Débil mantenimiento | Deterioro del equipo, problemas de conectividad | Alta | Media |
| | Uso inadecuado del equipo | Conexiones externas sin protección | Media | Media |

| | | | | |
|---|---|---|---|---|
| | Hurto de información | Información de la CTE sin respaldo ni protección | Alta | Media |
| | Escucha subreceptiva | Líneas de comunicación que no cuentan con protección | Baja | Baja |
| | Espionaje | Diseño de red inadecuado | Alta | Media |
| **Switches de CTE** | No se realiza mantenimiento | Mantenimiento insuficiente | Alta | Alta |
| | Uso inadecuado | Equipos Viejos | Alta | Media |
| | Suministro de energía inapropiado | Modificaciones de tensión | Medio | Bajo |
| **Sistema de cableado** | No se realiza mantenimiento | Mantenimiento insuficiente | Alta | Baja |
| | Uso inadecuado | Infraestructura inapropiada | Media | Baja |
| **Portátiles** | No se realiza mantenimiento | Mantenimiento insuficiente | Alta | Alta |
| | Robo de información | Información sin protección o respaldo | Alta | Media |
| **PC de escritorios** | No se realiza mantenimiento | Mantenimiento insuficiente | Alta | Alta |
| | Robo de información | Información sin protección o respaldo | Alta | Media |
| | Instalación de software | Virus, malware, troyanos. | Alta | Alta |
| **Sistemas Operativos** | Uso erróneo | Configuración incorrecta de los parámetros, insuficiencia de políticas de seguridad | Alta | Baja |
| | Falsificación de los derechos | Contraseñas sencillas y fáciles de hackear | Alta | Media |
| | Manejo inapropiado del software | No existen copias de respaldo | Alta | Alta |
| | Uso inadecuado del equipo | Manteamiento insuficiente | Alta | Alta |
| **Quipux** | Violación de derechos | No se terminado o cierra la sesión y se abandona el lugar de trabajo | Media | Media |
| **Sistema eléctrico** | No se realizan mantenimiento | Instalaciones inadecuadas, ausencia de conmutadores, Fallos eléctricos | Alta | Alta |
| **Administrador de Red** | Débil mantenimiento | No existe personal de informática en al CTE Babahoyo | Alta | Alta |

**Elaborado por:** Jonathan Montero, (2019)

**Tabla Nº7:** *Evaluación del riesgo (activos) de la CTE Babahoyo.*

| | **Probabilidad de que ocurra** | **Baja** | | | **Media** | | | **Alta** | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Facilidad de explotación** | **Baja** | **Media** | **Alta** | **Baja** | **Media** | **Alta** | **Baja** | **Media** | **Alta** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Valorización de equipos | 1 | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| | 2 | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| | 3 | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| | 4 | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| | 5 | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

**Fuente:** Norma ISO 27005

**Tabla Nª 8:** *Cálculo de riesgo sobre los equipos de la CTE Babahoyo*

| Activo | Amenaza | Vulnerabilidad | Valoración de equipos | Probabilidad que ocurra la amenaza | Facilidad de explotación | Riesgo |
|---|---|---|---|---|---|---|
| **Router de red** | Débil mantenimiento | Deterioro del equipo, problemas de conectividad | 4 | Alta | Media | **7** |
| | Uso inadecuado del equipo | Conexiones externas sin protección | 4 | Media | Media | **6** |
| | Hurto de información | Información de la CTE sin respaldo ni protección | 4 | Alta | Media | **7** |
| | Escucha subreceptiva | Líneas de comunicación que no cuentan con protección | 4 | Baja | Baja | 4 |
| | Espionaje | Diseño de red inadecuado | 4 | Alta | Media | **7** |
| **Switches de CTE** | No se realiza mantenimiento | Mantenimiento insuficiente | 3 | Alta | Alta | 8 |
| | Uso inadecuado | Equipos Viejos | 3 | Alta | Media | **7** |
| | Suministro de energía inapropiado | Modificaciones de tensión | 3 | Medio | Bajo | 5 |
| **Sistema de cableado** | No se realiza mantenimiento | Mantenimiento insuficiente | 2 | Alta | Baja | **6** |
| | Uso inadecuado | Infraestructura inapropiada | 2 | Media | Baja | 5 |
| **Portátiles** | No se realiza mantenimiento | Mantenimiento insuficiente | 5 | Alta | Alta | 8 |
| | Robo de información | Información sin protección o respaldo | 5 | Alta | Media | **7** |
| **PC de escritorios** | No se realiza mantenimiento | Mantenimiento insuficiente | 4 | Alta | Alta | 8 |
| | Robo de información | Información sin protección o respaldo | 4 | Alta | Media | **7** |
| | Instalación de software | Virus, malware, troyanos. | 4 | Alta | Alta | 8 |
| **Sistemas Operativos** | Uso erróneo | Configuración incorrecta de los parámetros, insuficiencia de políticas de seguridad | 4 | Alta | Baja | **7** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Falsificación de los derechos | Contraseñas sencillas y fáciles de hackear | 4 | Alta | Media | **7** |
| | Manejo inapropiado del software | No existen copias de respaldo | 4 | Alta | Alta | 8 |
| | Uso inadecuado del equipo | Manteamiento insuficiente | 4 | Alta | Alta | 8 |
| **Quipux** | Violación de derechos | No se terminado o cierra la sesión y se abandona el lugar de trabajo | 3 | Media | Media | 6 |
| **Sistema eléctrico** | No se realizan mantenimiento | Instalaciones inadecuadas, ausencia de conmutadores, Fallos eléctricos | 3 | Alta | Alta | 8 |
| **Administrador de Red** | Débil mantenimiento | No existe personal de informática en al CTE Babahoyo | 3 | Alta | Alta | 8 |

**Elaborado por:** Jonathan Montero, (2019)

**Tabla Nª 8:** índice de *riesgo según su nivel sobre los equipos de la CTE Babahoyo*

| Parámetro | Índice de riesgo | Descripción de acciones y riesgos |
|---|---|---|
| 8 | Alto | Se requiere tomar acciones correctivas en corto plazo con atención prioritaria de la administración de turno |
| **6-7** | Medio- Alto | Se requiere efectuar una vigilancia alta a través de planes y reportes a los encargados de las unidades |
| 4-5 | Medio | Tomar acciones correctivas a cargo de individuos especializados en el manejo de inconvenientes en tiempo óptimos. |
| 2-3 | Medio Bajo | El riesgo es razonable y los procedimientos de control son normales |
| 0-1 | Bajo | La administración de los activos efectuados es aceptable. |

**Fuente:** Norma ISO 27005

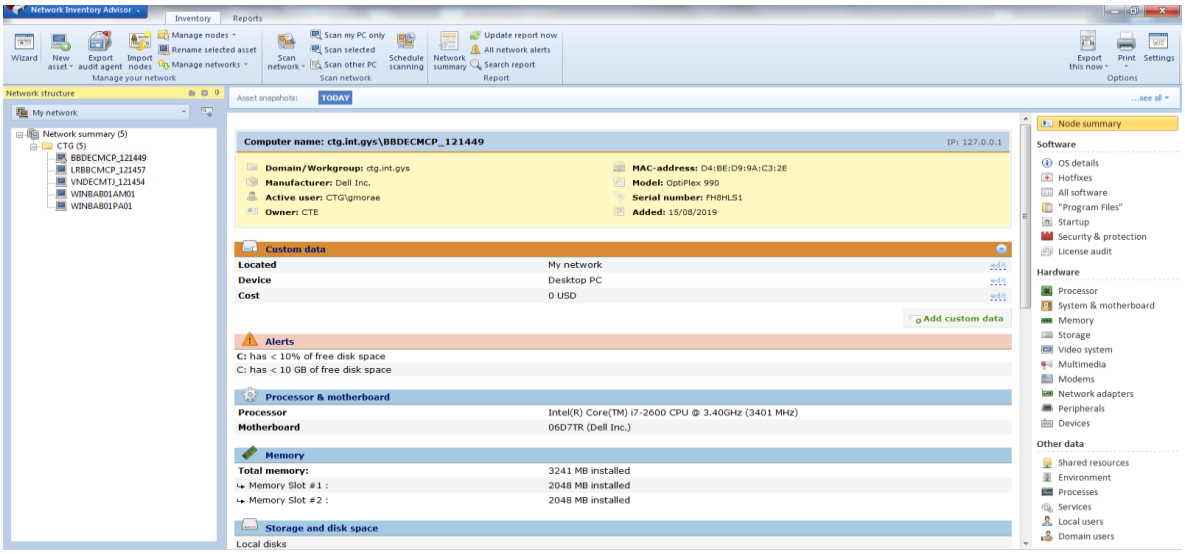



***Figura # 1.*** Escaneo de la red de la Comisión de Tránsito
Fuente: Network Inventory, (2019)

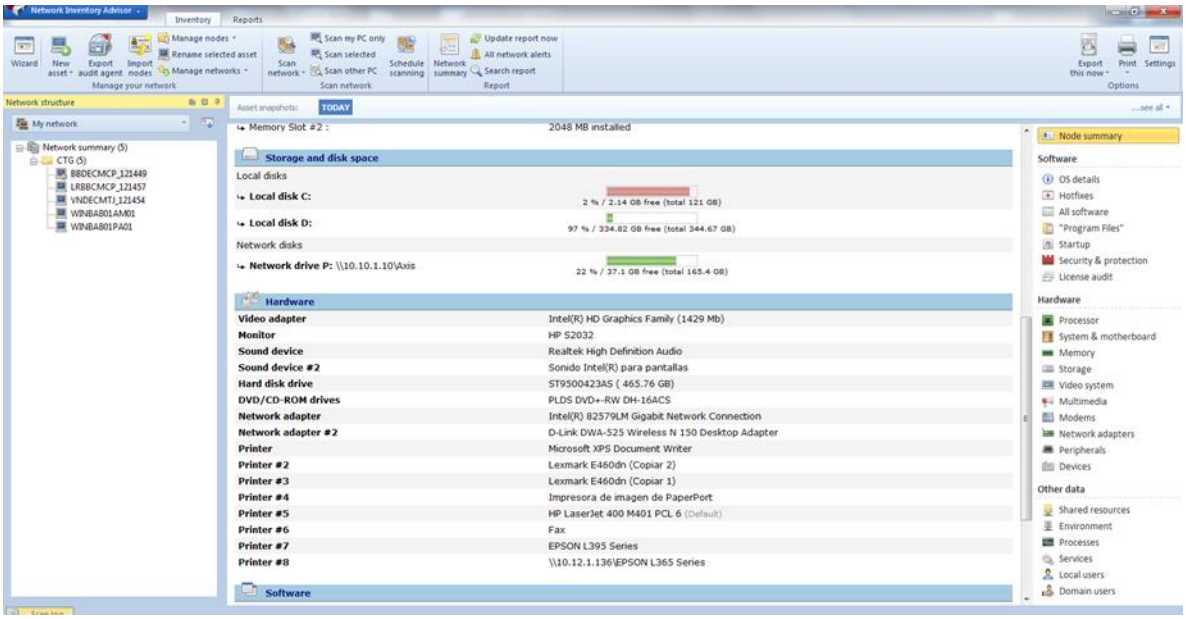
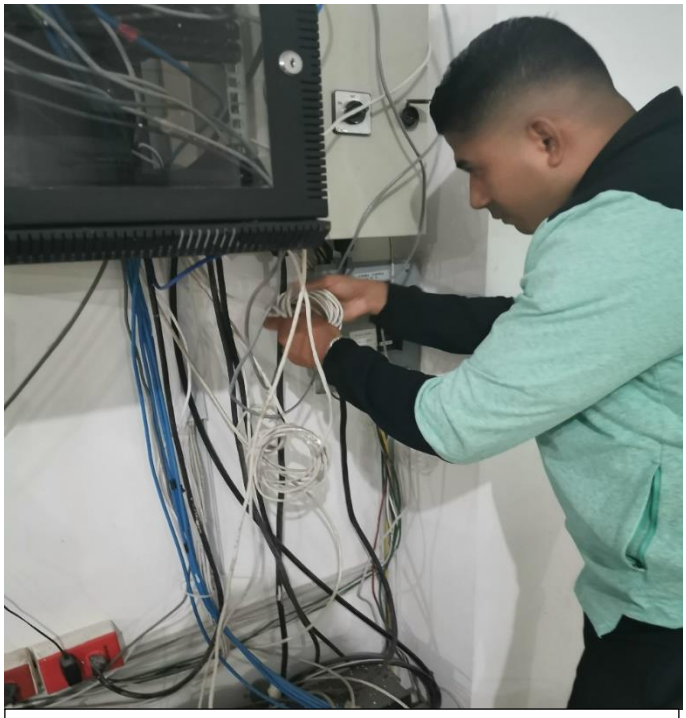



***Figura 4.*** Análisis del sistema

Fuente: Network Inventory, (2019)

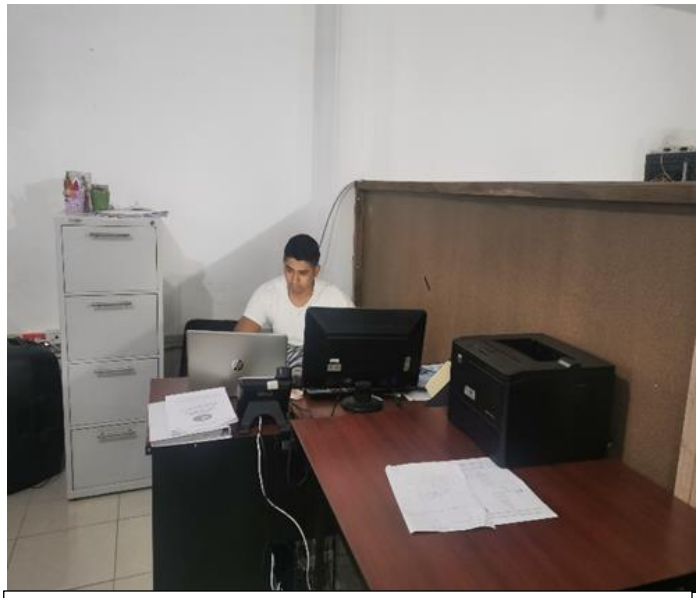
**ANEXO 6**

Imágenes del diagnóstico de la red y su estructura



Diagnóstico de la red donde se puede observar que no cuentan con un eficiente sistema de cableado de la red que dispone la institución

De acuerdo al análisis efectuado se detectaron instalaciones eléctricas defectuosas que representan un peligro sustancial para la organización



Diagnóstico de la red de la Comisión de Tránsito