
**UNIVERSIDAD TÉCNICA DE BABAHOYO**

**FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA**

**PROCESO DE TITULACIÓN**

**OCTUBRE 2017 – MARZO 2018**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA**

**PRUEBA PRÁCTICA**

**INGENIERIA EN SISTEMAS**

**PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS**

**Comentado [U1]:** Esta frase se complementa con las palabras:
Ingeniero en Sistemas
Ingeniero Comercial
Ingeniero en Contabilidad y Auditoría
Tecnólogo en Electricidad
Si es de género femenino cambiar por Ingeniera o Tecnóloga

**TEMA:**

**ESTUDIO DE LAS VULNERABILIDADES Y AMENAZAS EN LA RED DE DATOS DE LA FACULTAD DE CIENCIAS DE LA SALUD DE LA UTB**

**EGRESADO:**

**Comentado [U2]:** Si es de género femenino aumentar la A.

**CINTHYA CAROLINA PILCO QUISPE**

**TUTOR:**

**Comentado [U3]:** Si es de género femenino aumentar la A.

**ING. JOFFRE LEON ACURIO**

**AÑO 2018**

## INTRODUCCIÓN

En la actualidad las ciencias informáticas y en de forma específica la industria de la computación y las telecomunicaciones han revolucionado todos los posibles escenarios de trabajo, educación, capacitación, televisión, telefonía, aviación, automotriz, telemática y la salud; manteniendo un alto impacto en todos los segmentos de la población humana.

Es así como la aparición de las redes de datos ha logrado colaborar con la evolución de todas las disciplinas y ambientes antes mencionados, se evidencia la participación de una fuerza de trabajo tomado del termino en inglés *Task Force (FT)*, la misma que indica sobre el trabajo ejercido sobre una operación o misión de manera concreta.

Por ello se pretender aportar a través de este documento un caso de estudio en el cual se describa las vulnerabilidades y amenazas en la red de datos de la *Facultad de Ciencias de la Salud (FCCSS) de la Universidad Técnica de Babahoyo (UTB)*; al mismo tiempo se representará un estado de simulación con los datos recopilados por medio de la técnica de investigación basado en la observación directa In Situ.

Con los resultados obtenidos se elaborará un análisis con alto contenido técnico en el cual se verifican los niveles de seguridad de la red de datos de la *Facultad de Ciencias de la Salud (FCCSS);* para ello sera necesaria la utilización de software afín al área de estudio con el afán de adquirir una radiografía de los sistemas de comunicaciones y sus métodos empleados para la detección de vulnerabilidades en la red de datos; se verifica el nivel de penetración en la comunidad estudiantil, docente y administrativa,

tratando de potencializar la infraestructura y la tecnología de la información (IT) existente con un nuevo modelo de red orientado al escalamiento del medio y nivel físico, enrutamiento y señalización de tráfico, multiplexación y tamaño de ventanas de comunicación, acceso múltiple y convergente al nodo principal, redes y troncales, transmisión digital y redes WiFi.

En base a lo expuesto también se abordará un factor de mucho interés como lo es la interconexión de las redes de datos con el nodo principal con el objetivo de mejorar y afianzar el rol protagónico que tienen el intercambio, almacenamiento y procesamiento de la información, por ende, se realizara la discusión sobre los tipos de redes de datos ya sean de difusión o redes punto a punto.

## DESARROLLO

Hoy en día son varias las instituciones que usan más de un computador en sus operaciones y rutinas diarias, las misma que a su vez se encuentran interconectadas a un mecanismo que dota al ecosistema cibernético la mayor velocidad posible en sus distintas formas de comunicación entre los extremos de la red.

La red generalmente permite que las computadoras, equipos móviles y demás artefactos electrodoméstico dejen de ser una isla de información y se encarguen de procesar todo el volumen de datos que transita por la red tal como lo indica la siguiente ilustración.

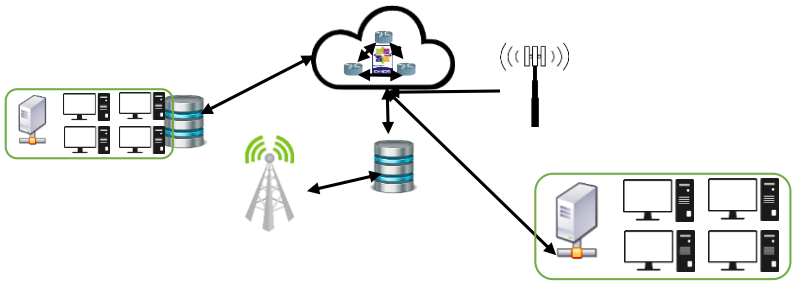

*Gráfico 1 Esquema de red tradicional, integración de redes de datos, redes Wifi, repositorios y sistemas de almacenamiento distribuido.*

Fuente: Cinthya Pilco

El escenario planteado corresponde a la red de datos de la *Facultad de Ciencias de la Salud (FCCSS)* de la *Universidad Técnica de Babahoyo (UTB)*; es así que casi todas las unidades académicas de la UTB al igual que todas las personas que estudian y trabajan en ella, dependen de alguna manera de la *Tecnología de la Información (IT*) como una herramienta esencial para los objetivos propuestos en cada una de sus actividades

propuestas diariamente, debido a esta razón la mayor parte de los usuarios deben enfrentar una amplia gama de amenazas, y vulnerabilidades asociada al entorno informático que es objeto de esta investigación.

La seguridad de la información por lo general se convierte en un punto neurálgico en todo escenario de infraestructura ya sea voz, dato y video; por ello se considera que la información es el recuso más valioso en la red, debido a este proceso se define que la seguridad debe ser el punto principal en esta investigación ya que se pretende aportar con un caso de estudio en el cual se esboza un modelo de gestión para la calidad y seguridad de la información. (Tarazona, 2017)

Junto con el crecimiento de la red de datos de la unidad académica objeto de estudio surge la necesidad de la administración de todos los componentes que se encuentran presentes en la infraestructura alámbrica e inalámbrica, para el efecto se incluyen las tareas del diseño coordinación e integración de hardware y software, así como el recurso humano necesario para la supervisión de los procesos.

Configurar, analizar, evaluar, monitorear, controlar y testear la red de datos en conjunto con todos los recursos con el objeto de obtener mayor calidad en los servicios requeridos, es necesario que la red cuente con los mecanismo y políticas que hagan posible la obtención de los resultados esperados (Joskowicz, 2015)

Desde el punto de vista local e institucional, las tareas de administración de la red se basan en la obtención de forma predecible y consistente de la *Calidad de Servicio (QoS),* así como la *Calidad de Experiencia del Usuario (QoE)* en forma adecuada a las

necesidades con un bajo impacto económico para la entidad a la que presta servicio la red de comunicaciones (Socrates, 2014)

Para la realización de este estudio es necesario realizar la detección de las diferentes fallas que actualmente se encuentran presentes en la red de datos de la Facultad de Ciencias de la Salud, posteriormente se deben aislar y como paso final corregirlas en el menor tiempo posible y al menor costo, una práctica recomendable es la continua mejora en los niveles de seguridad de la red, esto se logra a través de las configuraciones en los equipos en la Capa de Core, Capa de Distribución y Capa de Acceso .

Se evidencia que la administración de la red de datos de la unidad académica antes mencionada se encuentra construida con un sistema de cableado estructurado en categoría 6 y se encuentra desplegada por todo el edificio de la facultad, sin embargo, se evidencia que no existe un centro de cómputo en las inmediaciones o instalaciones de la misma, lo cual imposibilita realizar un correcto diagnóstico de la red.

Se procedió a establecer los mecanismos de monitoreo en la red con la instalación de un programa informático que se encarga de registrar todo tipo de información que fluye en la red de datos, así como las actividades que realizan cada equipo directamente conectada a la misma; este software toma el nombre técnico de Sniffer o su nombre comercial Wireshark. (Tanenbaum, 2014)

En la figura 1 se muestra una captura del trafico obtenido en el proceso de estudio y análisis de amenazas y vulnerabilidades de la red de datos de la facultad de ciencias de la salud.

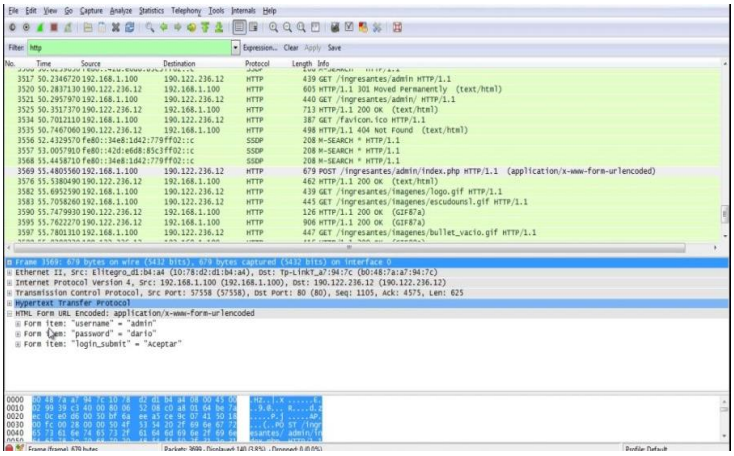

*Gráfico 2 Análisis de Tráfico y escaneo de la Red de Datos.*

Fuente: Cinthya Pilco

De acuerdo con la figura anterior se observa una captura del tráfico de la red en la cual se detecta una comunicación que apunta hacia una dirección IP fuera del rango de direccionamiento, razón por la cual se realiza pruebas de tipo pruebas y error de testeo con relación al *Protocolo de Resolución de Direcciones (ARP)*, el cual permite obtener datos de respuesta de la dirección IP de destino hacia donde apunta la comunicación entrante. (802.3-2015, 2015)

Producto de ello se evidencia que la comunicación en estado de sospecha se trata de una conexión no autorizada para resolver la interfaz de los servicios de redes sociales y sitio con información nociva como es el caso de pornografía.

Se detecta que el usuario se ha conectado de una dirección (192.168.X.X) hacia los servidores 157.240.14.35 https://www.facebook.com y también hacia los servicios establecidos en la siguiente dirección 46.4.95.165 http://umbrellacorp.forumfree.it a

través de una herramienta informática que actúa en capa 7 del modelo *Open System Interconnection (OSI)* con el nombre de UltraSurf.

Esta herramienta una vez instalada provoca la presencia de un proxy de manera virtual en la red de datos alojándose de forma local en el equipo anfitrión con el objetivo de sustituir el direccionamiento IP y enmascarándolo de tal forma que se aplica el concepto de navegación anónima y es así como se logra evadir las políticas establecidas por el administrador de red en forma general. (IEEE, 2013)

Es así que se logra detectar como se entabla una comunicación no autorizada entre el servidor remoto y un equipo local de la red, en el siguiente grafico se demuestra como por medio del enmascaramiento de protocolos se obtiene resultado de peticiones de usuarios y contraseñas así como credenciales del servidor principal de comunicaciones; el encapsulamiento se lo realza con la ayuda del *Protocolo de control de transmisión (TCP)*, *User Datagram Protocol (UDP)* y *Protocolo de Transporte en Tiempo Real (RTP)* (ISO/IEC, 2013)

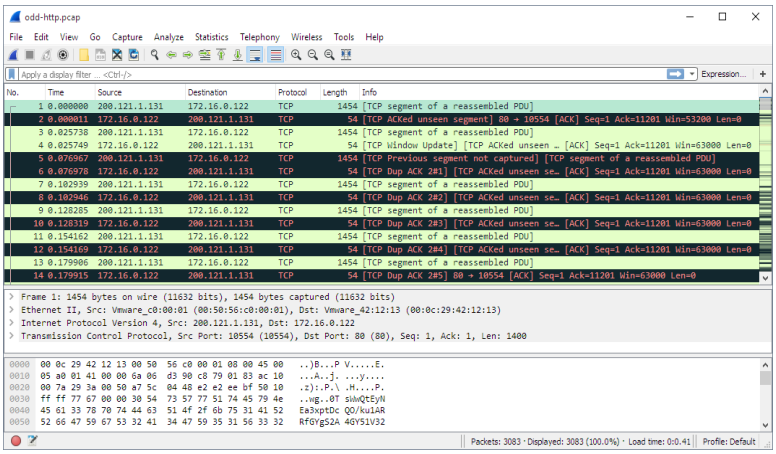


*Gráfico 3 Encapsulación de tráfico por TCP, UDP, RTP*

Fuente: Cinthya Pilco

**GESTIÓN DE FALLAS.**

Una de las funciones de la administración de la red de datos es poder detectar y resolver en tiempo real cada una de las anomalías que se lleguen a suscitar en el medio o en cualquiera de las instancias dentro del reducto de la infraestructura de comunicación; este propósito se basa en el aseguramiento de la información. (Francisco F. Pardo Barro, 2013)

La gestión se inicia en el instante que se genera una alarma ya sea de forma automática o reportada por cualquier usuario de la red de datos, es necesario disponer de un sistema que se encargue del seguimiento y monitoreo de incidencias a fin de que las notificaciones alerten a los encargados del control y resolución de inconvenientes. (Vicente Aceituno Canal, 2014)

Por ello se procedió a hacer una prueba de error con los datos obtenidos con el Sniffer y se detecta posteriormente varias anomalías en la cual existen comunicaciones provenientes desde otros segmentos de red con la finalidad de establecer enlaces de tipo *punto a punto (P2P)*, para el efecto se utiliza un agente de red con el nombre de Zenmap

En la siguiente gráfica 4 se muestra detalles de lo anteriormente explicado.

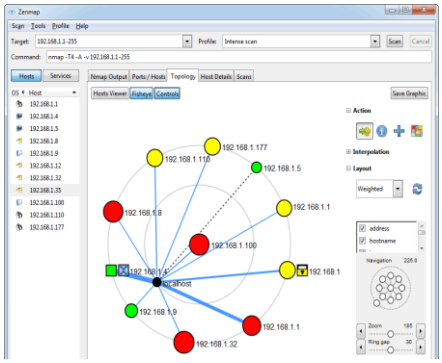


*Gráfico 4 Detección de comunicaciones p2p entre equipos de varios segmentos de red*

Fuente: Cinthya Pilco

## GESTIÓN DE DESEMPEÑO

La gestión del desempeño de las redes de datos tiene como objetivo asegurar el funcionamiento y la escalabilidad de las redes con *la calidad de servicio (QoS)* deseada, el principal propósito de utilizar y establecer un QoS en la red de datos es evitar el congestionamiento que produce el tráfico de la red y este factor va de la mano con el establecimiento y asignación del ancho de banda entre los distintos enlaces de comunicaciones internas y externas. (Stone, 2014)

Este objetivo es necesario en todo ambiente de red ya que provee de los mecanismos relacionados al desempeño y rendimiento de la red, la principal causa que motiva este aspecto es garantizar la disponibilidad del servicio en general sin importar el novel de convergencia en las comunicaciones internas o externas. (Acosta, 2013)

Se ha detectado que el canal de comunicación a menudo se suele saturar, pero esto es debido a que no existen políticas que normen y regularicen este aspecto muy importante para el aseguramiento de la calidad.

## GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información es un tema de concierne a todas las personas que trabajan o se encuentran inmersas de una u otra forma en el área de rede de datos, el principal objetivo de cumplir con los mecanismos y políticas mandatorios es el respeto al marco de definir permisos de acceso, control de identificación, configuraciones de autenticación entre usuario y equipo de cómputo, establecimiento de una entidad controladora de dominio institucional y demás elementos que forman parte activa de una barrera de protección que cumple con evitar intrusiones de posibles ataques dirigidos y no dirigidos a la red de datos. (Spencer, 2014)

Los controles son definido previo a un análisis del escenario a ser administrado, así también de define una planificación de cobertura en relación con el parque informático y la cantidad de usuarios que va a soportar la red de datos (Chavarria, 2015)

## GESTIÓN DE RED

La gestión de red se basa en la administración de todos los aspectos relacionados con la estructura jerárquica en todo lo referente a las comunicaciones de la infraestructura de red, la principal característica de la gestión de red es la clasificación de funciones que se deben realizar y ejecutar según el nivel de prioridad y responsabilidad del administrador de red. (Dekker, 2013)

Si bien es cierto la gestión de redes es más que un concepto amplio que abarca todos los enfoques técnico-prácticos que engloban políticas y procedimientos que intervienen en un planteamiento de servicios con alto grado de eficiencia; por lo tanto, se considera que es la suma de actividades orientadas a mantener una red eficiente con la mayor disponibilidad.

Un aspecto clave que requiere fundamentalmente de toda la atención del administrador de red es la complejidad de los tiempos de respuesta entre las diferentes transacciones que se ejecutan a diario en una red de comunicaciones.

**AMENAZAS Y VULNERABILIDADES**

Entre las amenazas detectadas en la red de datos de la Facultad de Ciencias de la Salud se definen las siguientes:

- Administración de diferentes plataformas de *Sistemas Operativos (OS)* se evidencia que todos los equipos no cuentan con licenciamiento y el 100% de los equipos están con problemas de vulnerabilidad debido a la aplicación de llaves fraudulentas. (García, 2014)
- No existe un Servidor de Nombre de Dominio (DNS), razón por la cual no se evidencia la presencia de un ente regulador de acciones sobre la estructura de los equipos informáticos, actualmente cualquier persona puede instalar cualquier tipo de aplicaciones y no hay ningún nivel de seguridad que impida las instalaciones no autorizadas.
- No existe un administrador de red de datos en la facultad, la persona que se encuentra encargada de los laboratorios no cumple con los requisitos mínimos para desempeñar el cargo.
- No existe un plan de contingencia para su activación frente a cualquier anomalía suscitada en la red de datos de la unidad académica.

- No existe un plan de mantenimiento que se aplique al mejoramiento preventivo o correctivo
- La red informática de la facultad no cuenta con los mecanismos de seguridad ya que fue fácil instalar un supresor de políticas y realizar pruebas en el sitio.

## CONCLUSIÓN

La Facultad de Ciencias de la Salud debe contar con un departamento técnico que sea capaz de absorber las múltiples incidencias que se generan a diario en la red debido a la carencia de políticas y mecanismos para el control de la red de datos.

Los servicios están soportados por un equipo de alta gama cuya función se basa en el control de actividades en capa 2 y capa 3 del modelo *Open System Interconnection (OSI),* el equipo en mención es de la marca SOPHO modelo Astaro, la fortaleza de esta herramienta se basa en el control perimetral de todas la comunicaciones, cabe indicar que el SOPHOS se encuentra gestionando la red desde el cuarto de máquinas en la dirección de sistemas, sin embargo, la línea de defensa no es lo suficientemente robusta ya que los niveles de incidencia en los laboratorios no han mermado.

Es necesario que se aplique de manera urgente una política de protocolos y funciones especialmente diseñados para la cobertura en la gestión de red basado en *Simple Network Management Protocol (SNMP),* con este proceso el administrador de red podrá detectar, aislar y monitorear las fallas e incidencias en cualquier extremo de la red sin afectar el rendimiento de las comunicaciones.

La red de datos en la Facultad de Ciencias de la Salud es muy permisiva y potencialmente vulnerable, la red ha soportada varios escenarios de ataques a la seguridad de la información y no hay un elemento local que identifique y actúe en primera instancia contra la amenaza.

La forma de comunicación entre los elementos de la red de datos es algo accidentada ya que los equipos de capa 2 no cuentan con las características para enrutar el tráfico de la red local hacia la red de internet, se evidencia un cuello de botella en la compuerta primaria del equipo local hacia la puerta de enlace del router principal.

# BIBLIOGRAFÍA


802.3-2015, I. (2015). EEE Standard for Information technology--Telecommu nications and information exchange between systems--Local and metropolitan area networ ks--Specific requirements--Part 3: Carrier Sense Multiple Access with Collision Detect ion (CS. IEEE .

Acosta, S. (2013). Redes Coporativas. Universidad de León España, 32.

Chavarria. (2015). Controles de la red de datos, aspectos en el análisis de Vulnerabilidad. Seguridad de la Información, 98.

Dekker, M. (2013). Security of the Internet . New York Security Network, 83.

Francisco F. Pardo Barro. (2013). Amenazas, vulnerabilidades y contramedidas. Tecnologías de la Información, DET, Universidad de Vigo , 63.

García, A. G. (2014). Sistemas de detección de intrusiones . Programa de Doctorado en Tecnologías de la Informac ión, DET, Universidad de Vigo , 101.

IEEE. (2013). IEEE Standard for Information technology— Tele communications and information exchange between systems— Local and metropolitan are a networks— Specific requirements . IEEE, 35.

ISO/IEC. (2013). ISO/IEC 17799:2000: Information technology -- Code of practice for information security management . Information technology, 67.

Joskowicz, J. (2015). REDES CORPORATIVAS . Instituto de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de la República DE Uruguay, 73.

Socrates, H. &. (2014). Coexistencia entre QoS & QoE, práctica para mejorar la calidad de la Red. Prentice Hall PTR. 2014, 74-75.

Spencer, C. (2014). Security Manager of Network Data. Security Manager, 77.

Stone, O. H. (2014). Performance Manager. Netwoking & Security, 83.

Tanenbaum, A. S. (2014). Redes de Computadoras (Tercera edición, ISBN 9 68-880-958-6) . Prentince Hall Hispanoamericana, 1997 , 82.

Tarazona, C. (2017). AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. HEIN ONLINE, AMENANZAS INFORMÁTIAS Y SEGURIDAD DE LA INFORMACIÓN., 137.

Vicente Aceituno Canal. (2014). La rentabilidad de las medidas de seguridad d e la información . Security, 68.