UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Trabajo de grado previo a la obtención del Título de Ingeniero en Sistemas y Computación

TRABAJO DE GRADUACIÓN

MEJORAS EN LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO APLICANDO HACKING ÉTICO.

AUTORES:

Olga Oñate

Carlos Martínez

DIRECTOR:

Mgs. Ing. Gonzalo Allauca

Riobamba – Ecuador

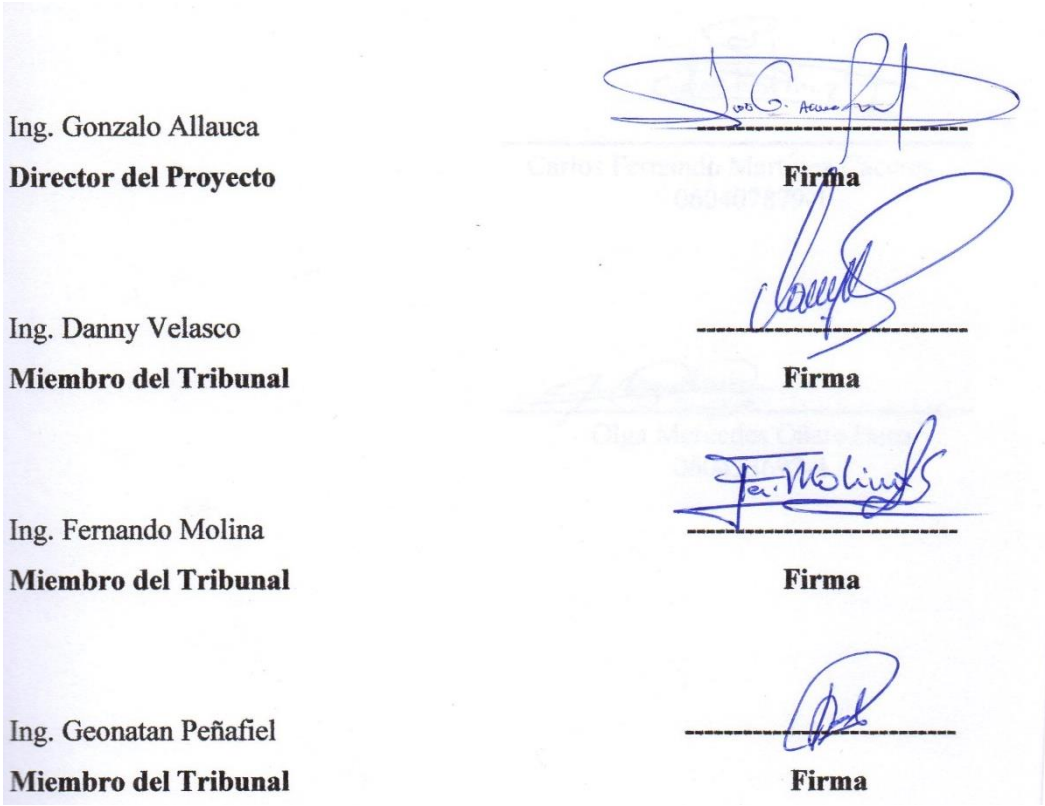
2017

Los miembros del Tribunal de Graduación del proyecto de investigación de título: Mejoras en la seguridad de la red inalámbrica de la universidad nacional de Chimborazo aplicando hacking ético.

Presentado por: Olga Mercedes Oñate Haro, Carlos Fernando Martínez Cáceres y dirigida por: Mgs. Ing. Gonzalo Allauca.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

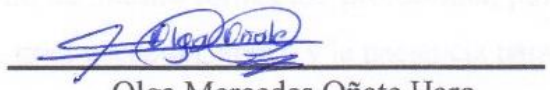


Ing. Gonzalo Allauca	----------
Director del Proyecto	**Firma**
Ing. Danny Velasco	----------
Miembro del Tribunal	**Firma**
Ing. Fernando Molina	----------
Miembro del Tribunal	**Firma**
Ing. Geonatan Peñafiel	----------
Miembro del Tribunal	**Firma**

Autoría de la investigación

"La responsabilidad del contenido de este Proyecto de Graduación, corresponde exclusivamente a: Carlos Fernando Martínez Cáceres y Olga Mercedes Oñate Haro con la dirección del Mgs. Ing. Gonzalo Allauca y el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo."

Carlos Fernando Martínez Cáceres
060407879-1



Olga Mercedes Oñate Haro
060433697-4

Agradecimiento

Agradezco por la culminación del trabajo de investigación a Dios porque ha estado conmigo a cada paso que doy, cuidándome y dándome fortaleza para continuar, pues siempre ha llenado de bendiciones mi vida, brindándome salud, fe para superar todos los obstáculos; a mis padres Nelson Oñate y Victoria Haro quienes me dieron la vida, educación, apoyo y consejos y por eso son el pilar fundamental, que con su esfuerzo y sacrificio siempre velan por sus hijos y buscan su bienestar para que seamos excelentes personas; a mis hermanos porque son el motor que me impulsa a salir adelante y luchar por alcanzar mis metas.

Un infinito agradecimiento al Ing. Gonzalo Allauca, Ing. Javier Haro e Ing. Fernando Molina por el tiempo compartido y por impulsar el desarrollo de nuestra formación profesional, por su guia, gran vocación, apoyo y la paciencia para colaborar en la factibilidad del proyecto; a la Universidad Nacional de Chimborazo, Carrera de Ingeniería Sistemas y Computación y a cada uno de sus docentes por impartir sus conocimientos y permitirme aprender de ellos.

OLGA MERCEDES OÑATE HARO

El trabajo de tesis en primer lugar me gustaría agradecer a Dios por bendecir a mis padres y hermanas que han sido un pilar fundamental para llegar a mi objetivo profesional. A la Universidad Nacional de Chimborazo por darme la oportunidad de estudiar y ser un profesional. A mi director de tesis, Ing. Gonzalo Allauca por su esfuerzo y paciencia, quien con sus conocimientos y experiencia y su motivación ha logrado en nosotros que podamos terminar nuestros estudios. También me gustaría agradecer a todos mis profesores durante mi carrera porque todos han aportado a mi formación de profesional y humano. De igual manera agradecer a mi profesor de la materia de proyectos de tesis y amigo, Ing. Fernando Molina por sus enseñanzas y consejos.

Son muchas personas que me gustaría agradecer por que han formado parte de mi vida en el camino hacia el objetivo de ser profesional a las que me gustaría agradecer su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Sin importar donde estén les agradezco de todo corazón por formar parte de mí y que dios los bendiga.

CARLOS FERNANDO MARTÍNEZ CÁCERES

Dedicatoria

Dedico este trabajo de grado a Dios por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor. A mis padres Nelson Oñate y Victoria Haro, por haberme apoyado en todo momento, por sus consejos, sus valores, el ejemplo de que con trabajo duro y constancia todo es posible; además por su esfuerzo, sacrificio y dedicación para que sus hijos sean personas de bien y profesionales; tengo para ellos mi infinito amor y agradecimiento.

A mis hermanos Angelita, Luis Miguel y Carmen por permanecer a mi lado y brindarme palabras de aliento, motivarme a seguir adelante y consejos. A mis docentes, en especial Ing. Gonzalo Allauca, Ing. Javier Haro e Ing. Fernando Molina por su gran apoyo y motivación para la culminación de nuestros estudios profesionales y para la elaboración de este trabajo de grado.

OLGA MERCEDES OÑATE HARO

Dedico este trabajo principalmente a Dios, por haberme dado vida y permitirme llegar a este momento tan importante de mi formación profesional y humana. A mi madre Lilian y mi padre Vinicio por ser mi pilar fundamental y demostrarme su cariño y apoyo incondicional a pesar de las dificultades que se presentan en el camino de la vida. A mis dos hermanas Erika y María José por hacer de mi vida una alegría a pesar de las dificultades y opiniones distintas. A mi amada enamorada Marcia por demostrarme que en la vida siempre va a ver un mejor camino. A mis dos amigos de carrera Dennys y Cristian que compartieron alegrías y tristezas durante 5 años de carrera y a mi amiga y compañera porque sin el equipo de trabajo que se conformó, no se hubiera logrado esta meta.

CARLOS FERNANDO MARTÍNEZ CÁCERES

Índice general

Índice de tablas

Índice de figuras

Resumen

La presente investigación permite realizar mejoras en la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo aplicando hacking ético, se tiene como objetivos analizar las técnicas de hacking ético aplicado a las redes inalámbricas para determinar que herramientas son apropiadas para mitigar las vulnerabilidades y desarrollar un manual políticas de seguridad adecuadas los escenarios que se está realizando en la investigación.

La metodología que se utiliza en la investigación es un estudio longitudinal, pues se obtiene datos de las vulnerabilidades de la red inalámbrica sin el uso de hacking ético y con el uso de hacking ético, teniendo como resultado un manual de políticas de seguridad, aplicable a las distintas vulnerabilidades encontradas.

Para lo cual, se analiza e identifica parámetros de medición como el promedio de equipos conectados a la red inalámbrica, número de dispositivos que se pueden ser vulnerables a un análisis de paquetes o sniffer, nivel de vulnerabilidad detectada por descubrimiento de contraseñas y/o spoofing, nivel de calidad servicio y por último el nivel de políticas de administración aplicadas.

Para realizar las mediciones pre y post sobre los escenarios de la red inalámbrica, se utilizan sistemas operativos como Kali Linux, Wifislax, Backtrack, equipos activos de red como wiresslan controller y servidor Radius.

Se utiliza T-STUDENT para la comprobación de la hipótesis obteniendo los resultados siguientes: en la red de estudiantes el número de clientes con posibilidad de ser analizados sus paquetes o sniffer bajan de 867.60 clientes a 468.20 clientes con una media de 399,400 y en la red de Docentes bajan de 522.40 clientes a 285.80 clientes con una media de 236,600.

De acuerdo a la auditoría técnica realizada y el manual de políticas de seguridad desarrollado y entregado con Acta Entrega Recepción al Administrador de Red; en base a las vulnerabilidades detectadas en la red inalámbrica de la Universidad Nacional de Chimborazo, se concluye que se podrá mejorar la seguridad en al menos un 25%.

Abstract

The present research allows to make improvements in the security of the wireless network of the Universidad Nacional de Chimborazo by applying ethical hacking. Its objective is to analyze the techniques of ethical hacking applied to the wireless networks to determine which tools are appropriate to mitigate the vulnerabilities and to develop a manual of security policies according to the scenarios that are being carried out in the research.

The methodology used in the research is a longitudinal study. Data are obtained from the vulnerabilities of the wireless network without the use of ethical hacking and with the use of ethical hacking. The outcome of this research will be a safety policy manual applicable to the different vulnerabilities that were found.

It was analyzed and identified the measurement parameters such as the average number of devices connected to the wireless network, number of devices that may be vulnerable to a packet or sniffer analysis, level of vulnerability detected by the discovery of passwords and spoofing , the level of service quality and finally the level of applied administration policies.

To perform the pre and post measurements about the wireless network scenarios. operating systems were used such as Kali Linux, Wifislax, Backtrack, active network equipment such as wiresslan controller and Radius server.

T-STUDENT was used to test the hypothesis, obtaining the following results: in the network of students, the number of clients with the possibility of being analyzed their packages or sniffer decrease from 867.60 clients to 468.20 clients with an average of 399,400. In the network of teachers the amount decrease from 522.40 clients to 285.80 clients with an average of 236,600.

According to the technical audit carried out and the security policy manual developed based on the vulnerabilities detected in the wireless network of Universidad Nacional de Chimborazo. it is concluded that security can be improved by at least 25%.

Reviewed by: Lara, Adriana
Language Center Teacher

Introducción

El mundo de la tecnología ha evolucionado simultáneamente con las vulnerabilidades y los ataques informáticos; esto no solo afecta a las grandes corporaciones sino a los usuarios de todo el mundo. Uno de los ataques cibernéticos más grandes de la historia fue a la NASA en agosto de 1999, la misma que fue atacado por Jonathan James interceptando millones de mensajes confidenciales, contraseñas y software vital para la agencia. (Rodríguez, 2013)

La seguridad es un aspecto de alta relevancia cuando se trata de redes inalámbricas siendo que cualquier individuo interno o externo de la organización podría acceder a la red sin siquiera encontrarse en las instalaciones. (Barajas b, 2004) Consientes a las faltas de seguridad en las redes inalámbricas la IEEE desarrollo una tecnología de seguridad nombrándola WEP, en la norma de las redes inalámbricas la 802.11.

Los delitos informáticos en el Ecuador van desde el fraude hasta el espionaje, los mismos que son denunciados en la fiscalía; el internet abrió el paso a estas nuevas formas de delincuencia que ponen en riesgo la información privada, la seguridad en la navegación de los usuarios y la información de las instituciones públicas y privadas. La fiscalía general del estado registro 626 denuncias por delitos informáticos en el año 2014. Desde 10 de agosto del 2014 entra en vigencia el Código Orgánico Integral penal en cual se sanciona los delitos informáticos cuyos actos se cometen con el uso de tecnología, para violentar la confidencialidad y la disponibilidad de datos personales. (Fiscalia General del Ecuador, 2015)

La red inalámbrica de la Universidad Nacional de Chimborazo ha sufrido ataques informáticos poniendo en riesgo la información que se transmite, según datos obtenidos de la encuesta aplicada a los administradores de la red del Centro de Tecnologías de la Educación.

Es importante realizar un estudio que refuerce la seguridad en la red, pues su principal objetivo es transmitir información crítica de los estudiantes, docentes y

administrativos de la universidad, es necesario evitar infiltraciones por agentes externos e internos que afecten a la información institucional.

En los últimos años, las grandes organizaciones han implementado controles para mitigar los ataques en sus redes inalámbricas, las más aplicadas con: Ajuste de políticas, actividades de concientización de la seguridad, técnicas de encriptación y habilidades de auditoria. (Ernst & Young Global, 2011)

En la universidad es necesario aplicar estrategias enfocadas a la protección de la información crítica de la institución, por este motivo se toma como guia las estrategias que están siendo aplicadas en las empresas a nivel mundial como son las políticas de seguridad en las redes inalámbricas, con la finalidad de disponer un acceso seguro a la información y los servicios que brinda.

El principal objetivo de la investigación es mejorar la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo aplicando hacking ético, el mismo que tendrá como una propuesta de solución la implementación de políticas de seguridad basadas en la auditoria de hacking ético y el desarrollo de un manual para garantizar la seguridad de la red inalámbrica.

Para elevar la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo se aplicará las fases del hacking ético, que permiten la detección de ataques y vulnerabilidades; de esta forma poder mitigarlos y elaborar un manual de políticas de seguridad para la red inalámbrica.

Con el fin de presentar una guía para el desarrollo de la investigación se esquematiza brevemente los aspectos desarrollados en cada uno de los capítulos.

En el primer capítulo se describe temas introductorios que van a ser utilizados a lo largo de la investigación, en el segundo capítulo se aplica las etapas del hacking ético, iniciando con pruebas de penetración para la detección de ataques y vulnerabilidades, en el tercer capítulo se visualizará los resultados de la evaluación

obtenidas luego de la aplicación de las fases de hacking ético, en el cuarto capítulo se finaliza este proyecto estableciendo conclusiones y recomendaciones, en el quinto capítulo se indica en qué consiste la propuesta, el plan de acción que se seguirá para cumplir los objetivos y de esta forma se desarrollará un manual de políticas de seguridad de redes inalámbrica.

Objetivos

Objetivo general

Mejorar la seguridad de la Red Inalámbrica de la Universidad Nacional de Chimborazo aplicando Hacking Ético.

Objetivos específicos

- Analizar las herramientas de Hacking Ético aplicado a las redes inalámbricas (wirelessLAN).
- Determinar las vulnerabilidades de la red inalámbrica de la Universidad Nacional de Chimborazo.
- Comprobar las medidas de seguridad realizadas en la red inalámbrica de la Universidad Nacional de Chimborazo.
- Desarrollar un manual para garantizar la seguridad de la red inalámbrica en la Universidad Nacional de Chimborazo.

Capítulo I

1. Fundamentación teórica

1.1.Seguridad en las redes inalámbricas

La utilización de las redes inalámbricas está tomando importancia debido a que brindan una gran versatilidad en cuanto a la movilidad. Se ha convertido en una excelente alternativa en áreas imposibles de brindar conectividad con el servicio cableado. (Giraldo, Giraldo, Huertas, & Camacho, 2011)

La seguridad es un aspecto de alta relevancia cuando se toca el tema de redes inalámbricas, por el motivo de que cualquier individuo externo a la organización podría acceder a la red sin ni siquiera estar en las instalaciones. (Barajas a, 2004)

Conscientes de la falta de seguridad en las redes WLAN, la IEEE público un mecanismo opcional de seguridad, nombrado Wired Equivalent Privacy (WEP) en la norma de redes inalámbricas 802.11. Es de esta manera que la IEEE emprendía una solución a la inseguridad de las rede WLAN, con este nuevo protocolo se pretendía dar la suficiente seguridad. (Barajas a, 2004)

1.1.1. Sistemas de encriptación.

La seguridad de las redes inalámbricas WI-FI han sido de suma importancia para de la Alianza Wi-Fi. (Wireless Fidelity Alliance, 2012)

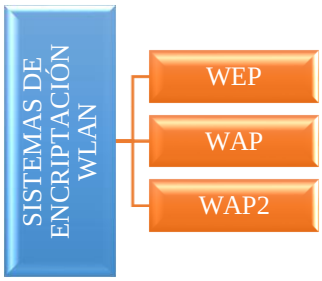


Figura 1. 1. *Tipos de sistemas de encriptación.*

Elaborado por: Los Autores

1.1.2. Mecanismos y factores de seguridad.

Existen tres mecanismos básicos para prestar servicios de seguridad.

- Información secreta como claves y contraseñas, conocida por las entidades autorizadas.
- Un conjunto de algoritmos para realizar el cifrado y descifrado.
- Un grupo de procedimientos para definir cómo usar los algoritmos.

La administración de los sistemas de seguridad comprende dos extensas secciones.

1) La política de los servicios y mecanismos para detectar las violaciones de seguridad e inicialización acciones correctivas.
2) Seguridad en la generación, localización y distribución de la información secreta para lograr acceder por entidades autorizadas. (Cisco Systems)

1.1.3. Ataques en redes WLAN.

Para asegurar una red WLAN lo primero que se debe conocer son las amenazas y ataques que puede sufrir. Existen varios métodos, pero se pueden dividir en dos grandes grupos. (Andreu b, Pellerejo, & Lesta, 2006)

1.1.3.1. ataques pasivos.

El principal objetivo del ataque es lograr obtener información. Es el primer paso para los ataques posteriores. A continuación, analizaremos los ataques más comunes a las redes WLAN. (Andreu a, Pellerejo, & Lesta, 2006)

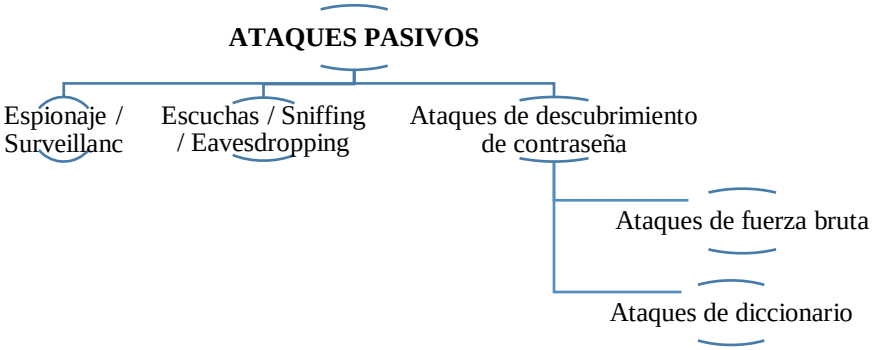


Figura 1. 2. *Ataques pasivos.*
Fuente: (Andreu a, Pellerejo, & Lesta, 2006)
Elaborado por: Los Autores

1.1.3.1.1. Escuchas / Sniffing / Eavesdropping

Muchas redes son vulnerables Eavesdropping o Sniffing que es la pasiva intercepción sin modificación de datos del tráfico de una red. La manera de realizar este tipo de ataque activo es con Packet Sniffer los cuales son programas que monitorean los paquetes que circulan por la red. Esto se puede realizar por usuarios con legitimo acceso a la red o por un pirata informático.

Un sniffer consiste en colocar a la interfaz de red de la computadora en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por

lo tanto los paquetes que son enviados por la red llegan a la tarjeta de red donde está instalado o ejecutándose el Sniffer. Este tipo de herramientas era muy utilizado por los administradores de redes, pero con el tiempo y con la explotación de este tipo de software los piratas informáticos le fueron convirtiendo en una herramienta esencial para sus ataques. Normalmente, los buenos sniffers, no son fáciles de detectar, aunque la inmensa mayoría trabaja con el protocolo TCP/IP y se les puede detectar utilizando diferentes métodos. (Goncalves, 1997)

1.1.3.2. ataques activos.

Los ataques activos implican algún tipo de modificación en el flujo de datos o la creación de falsos flujos en la trasmisión de datos. Puede consistir en dos principales objetivos: ser alguien que en realidad no es para poder obtener información o colapsar los servicios que proporciona la red. (Andreu c, Pellejero, & Lesta, 2006)

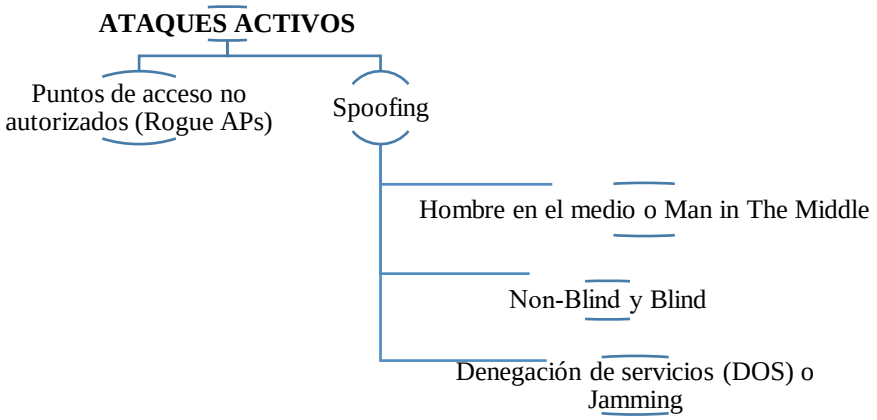


Figura 1. 3. *Ataques activos.*
Fuente: (Andreu c, Pellejero, & Lesta, 2006)
Elaborado por: Los Autores

1.1.3.2.1. Spoofing

Hace referencia a las técnicas de suplantación de identidad generalmente con uso malicioso o investigativo, esto significa que el pirata informático hace un falso origen de los paquetes haciendo que la víctima o cliente piense que está conectado a un host autorizado. Utiliza tres computadoras o host que son: Atacante, Atacado y el sistema suplantado. Para que el pirata informático pueda conseguir el objetivo del ataque necesita establecer una comunicación falsa y por otro evitar que el equipo suplantado interfiera en el ataque (Miro, 2012).

1.1.3.2.2. Hombre en el Medio (MITM)

Consiste en que el pirata informático se introduce en la comunicación entre dos equipos para que todo el tráfico pase primero por un host no autorizado, básicamente este tipo de ataque utiliza el protocolo ARP. El protocolo ARP se comunica con todos los hosts de la red enviando una solicitud para preguntar cuál es el equipo que contiene la dirección IP solicitada (Miro, 2012).

1.1.3.2.3. Denegación de Servicios (DOS) o Jamming

Un ataque de denegación de servicios no es más que un número exponencial de peticiones a una misma dirección IP, de tal manera que el servidor es incapaz de gestionar dichas peticiones y causando un error y la detención o reinicio del sistema dejando de esta manera inaccesible al resto de usuarios (Miro, 2012).

1.2.Vulnerabilidades en las redes

Las vulnerabilidades describen los métodos más utilizados incidir en ataques a la seguridad de los protocolos TCP/IP (confidencialidad, integridad y disponibilidad de los datos). Los ataques pueden ser inducidos por diferentes causas como fraude, extorsión, robo de información. Las organizaciones pueden sufrir de vulnerabilidades internas y externas, provocando fallas a los sistemas o servicios.

1.2.3. Vulnerabilidades en redes WiFi

Las vulnerabilidades de acceso más conocidas para redes wifi en acceso son wardriving; de cifrado WEP son ataques FSM, KoreK, etc.; de ataques de Man-in-the-Middle son Rogue APs; de vulnerabilidades en APs en modo "bridge"; y por último ataques de denegación de servicio. (Rios, 2011)

1.3. Políticas de seguridad informática (PSI) y su impacto en la organización

Las políticas de seguridad informática son una base para el personal en relación con el uso de los recursos y servicios informáticos de la organización y la protección de los mismos. Las PSI requieren de la disposición de todo el personal de la organización permitiendo la eficiencia de su implementación.

Para la implementación de PSI es necesario tomar en cuenta los siguientes aspectos: alcance de las políticas brindado la importancia que merece; objetivos de la política; responsabilidades por cada servicio y recurso informático; se definen las

violaciones a la política y las consecuencias de esto; asignación de responsabilidades a los usuarios de acuerdo a la información que tienen acceso.

Con las políticas de seguridad informática bien definidas en una organización, se posee un estándar de acción comunal a la hora de presentarse fallas y/o ataques en los sistemas de información, lo que permite que todos los entes de la organización contribuyan en un mismo rumbo hacia una posible mitigación o solución. (ArCERT Coordinación de Emergencia en Redes Teleinformaticas)

1.4. Hacking ético

1.4.1. Historia de hacking ético.

Las organizaciones informatizaron de procesos dentro de un sistema de información, tomando al internet como plataforma de información. Debido a intrusiones se hizo evidente la falta de un servicio profesional que imitara esos ataques o capacitara a su personal con las mismas metodologías que utilizan los intrusos. Los accesos no autorizados, vulnerabilidades y amenazas permitieron que especialistas ligados a la seguridad informática investigaran metodologías de intrusión a lo que llamaron hacking ético. (Tori, 2008)

1.4.2. Introducción al hacking ético.

"Ética significa carácter, estudia la moral, la acción humana, y verifica afirmaciones de lo correcto y lo incorrecto, mientras Hacking significa piratear y romper la seguridad de un sistema de forma ilegal." Un hacker ético es un experto en informática y sistemas, tiene profundos conocimientos sobre los sistemas operativos, hardware, electrónica, redes, telecomunicaciones, y programación en lenguajes de alto y bajo nivel. (Pacheco a & Jara, 2012)

1.4.3. Ethical hacking: impulso del futuro.

La piratería se puede dividir en 3 niveles bajos, medio y alta.

Bajo es que requieren menos cantidad de habilidad técnica y se basa más en la ingeniería social y unas pocas cosas simples como registradores de claves de hardware. Nivel medio cuenta con una buena habilidad con las herramientas desbordamientos de búfer disponible y pre compilados. Alta es una persona que puede pensar fuera de la caja y los aspectos más profundos de TCP/IP y código. (Zunzunwala & Amruta , 2010)

1.4.4. Clasificación de hacker.

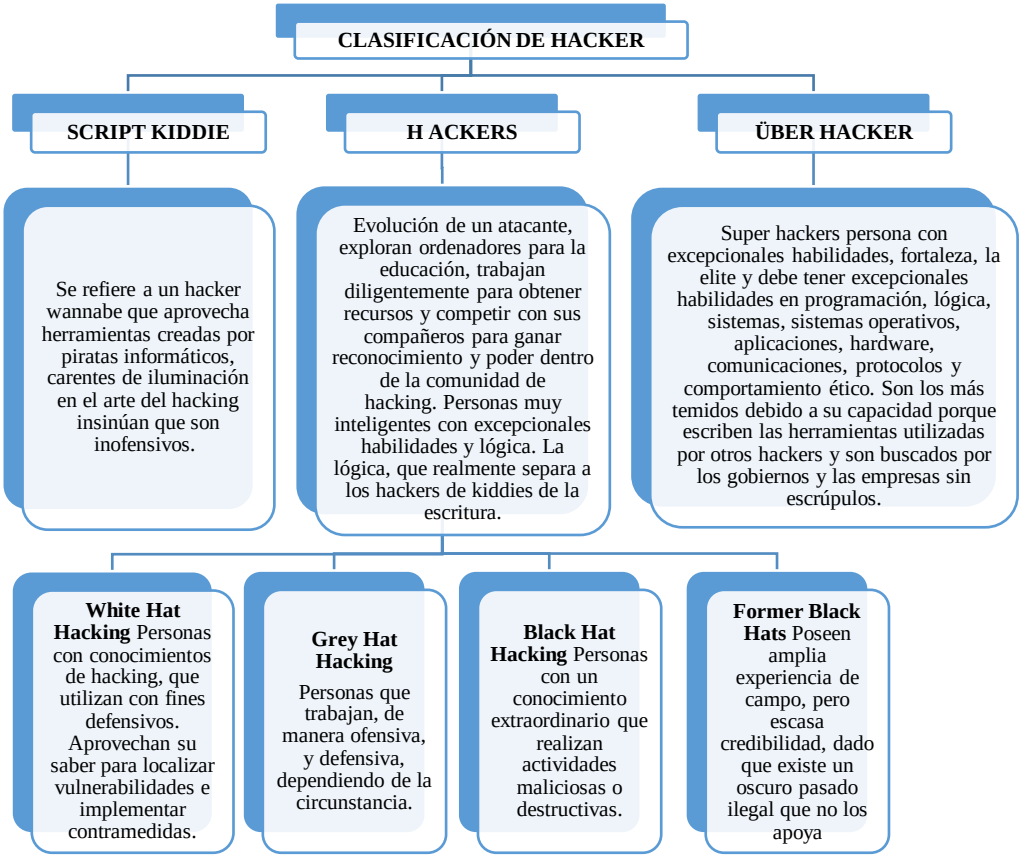


Figura 1. 4. Clasificación de tipos de Hacker.
Fuente: (Pacheco b & Jara, 2012) (TILLER, 2005)
Elaborado por: Los Autores

1.4.5. Tipos de hacking.

Hacking ético externo: Se puede realizar desde la internet sobre los equipos o infraestructura de una red pública del usuario final. **Hacking ético interno:** Se puede ejecutar en una red interna del usuario final, o como un empleado que posee el acceso a la red de la institución. (Astudillo, 2013)

1.4.6. Fases del hacking

Tanto el auditor como el cracker siguen un orden lógico de pasos al momento de ejecutar un hacking, a estos pasos agrupados se los denomina fases. Existe un consenso generalizado entre las entidades y profesionales de seguridad informática de que dichas fases son 5 en el siguiente orden:

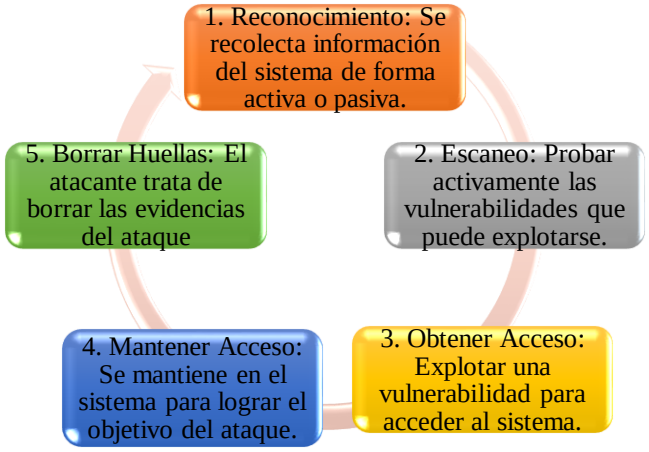


Figura 1. ***5.*** *Circulo de hacking - Pasos que sigue el cracker.*
Fuente: EC-Council (Astudillo, 2013)
Elaborado por: Los Autores

1.5.Estado del arte

A través de tiempo, los delitos informáticos hechos por hacker de sombrero negro son perjudiciales para las entidades bancarias pues generan pérdidas millonarias principalmente a vulnerabilidades en los sistemas de información, el acceso a sus bases de datos y la clonación de tarjetas de crédito bancarias. “En Cali un ejecutivo, accedía a las cuentas de los usuarios suplantando su firma y su huella. Así, retiraba dinero, desde el año 2009 hurtó a los clientes del banco $360 millones.” (Colprensa, 2015)

Los estudiantes tienen gran inclinación a vulnerar sistemas, especialmente en los primeros semestres donde experimentan con fines personales y a medida que aumentan en conocimiento, para poner a prueba sus conocimientos y/o demostrar sus destrezas con fines económicos o de aceptación en grupos de la cultura hacker. En actualidad gran cantidad de empresas aun no dedican ni el 10% de dinero a la seguridad informática, se concluye que aún falta mucha concientización del gran daño grande que se pueden sufrir si no se toma medidas para garantizar la seguridad, y como el delito más cometido en el país es la suplantación, por la facilidad de acceso. (Manchola, Suarez, & Herrera, 2016)

1.5.1. Metodología de una prueba de penetración.

Una Prueba de Penetración es el proceso utilizado para realizar una evaluación o auditoría de seguridad de alto nivel; definiendo un conjunto de reglas, prácticas, procedimientos y métodos a seguir e implementar durante la realización de

cualquier programa de auditoría en seguridad de la información. Una metodología define una hoja de ruta con ideas útiles y prácticas comprobadas, las cuales deben ser manejadas cuidadosamente para poder evaluar correctamente los sistemas de seguridad. (Quezada, 2015)

1.5.2. Tipos de pruebas de penetración.

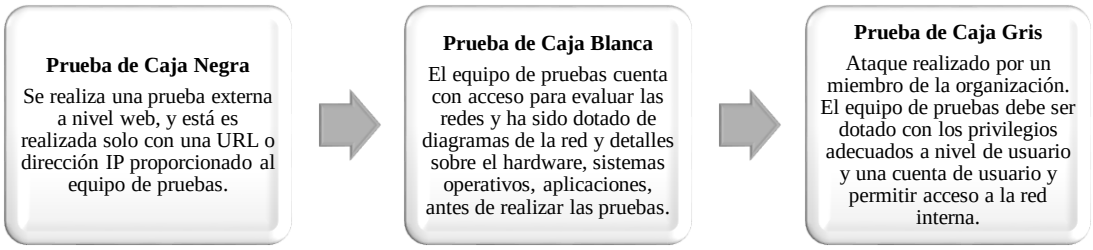


Figura 1. 6. *Tipos de pruebas de penetración.*
Fuente: (Quezada, 2015)
Elaborado por: Los Autores

Las organizaciones conjuntamente con la tecnología deben evolucionar rápidamente, esto suele afectar la infraestructura tecnológica, por ello es muy importante que los administradores conozcan los riesgos a los que se exponen sus activos de red, y la forma de combatirlos. Las pruebas propuestas brindan un excelente panorama del estado de seguridad de una WLAN, gracias al detalle y diversificación de la información resultante.

Tabla 1. 1. *Desarrollo de las pruebas de penetración.*

N°	PRUEBAS DE PENETRACIÓN	CARACTERÍSTICAS
1	IDENTIFICACIÓN DE REDES OCULTAS	Verificar si en el espectro, se encuentran SSID ocultos, con el fin de establecer si se trata de redes no autorizadas
2	FALSO PUNTO DE ACCESO INALÁMBRICO	Punto de Acceso Falso para engañar clientes y lograr que se conecten a un SSID falso
3	ROMPIMIENTO DE CONTRASEÑA	Interceptación de tráfico e inyección maliciosa del mismo para atrapar vectores de inicialización que permitan adivinar o predecir la contraseña de acceso
4	DENEGACIÓN DE SERVICIO – PRUEBA DE CONCEPTO	Inundación de peticiones que busca suspender un servicio, Prueba de Concepto para validar si la infraestructura es vulnerable
5	FALSO PUNTO DE ACCESO INALÁMBRICO+ HOMBRE EN EL MEDIO – PRUEBA DE CONCEPTO	Punto de Acceso Falso al que se conectan clientes engañados y se intercepta el tráfico –Prueba de Concepto
6	PHISHING	Falsificación de Portal de Autenticación de Acceso, para robas las credenciales de inicio de sesión
7	COBERTURA DE SEÑAL	Pruebas de Alcance Físico de la señal con antenas de diferentes potencias
8	VULNERABILIDADES	Comprobación de Vulnerabilidades en las direcciones IP Objetivo
9	GEOLOCALIZACIÓN	Utilizando un GPS de conexión USB, es posible ubicar en un mapa, las redes al alcance del objetivo
10	CODIGO MALICIOSO E INGENIERIA SOCIAL	Utilizando un código malicioso y técnicas de Ingeniería Social, es posible engañar a clientes potenciales para que se conecten a una red inalámbrica trampa

Fuente: (Gacharna, 2014)
Elaborado por: Los Autores

1.5.3. Metodologías de pruebas de seguridad.

Existen diversas metodologías open source que tratan de guiar los requerimientos de las evaluaciones en seguridad. La idea principal de utilizar una metodología durante la evaluación, es ejecutar diferentes tipos de pruebas paso a paso para poder juzgar con mucha precisión la seguridad de un sistema. (Quezada, 2015)

Las metodologías ISSAF permiten realizar un procedimiento de hacking y evaluación de riesgos éticos porque está orientado a a red inalámbrica con la ayuda de las metodologías OSSTMM y OWISAM permitiendo en la auditoria visualizar un esquema ordena de las fases y la elaboración de informe ejecutivo y técnico; pero todo este procedimiento no tiene validez si no se realiza un seguimiento y se muestra al cliente los resultados para su pronta resolución. (Bonilla, 2015)

1.5.4. Seguridad en las redes wifi.

WPA2 es la generación actual de seguridad Wi-Fi. Se basa en dos protocolos principales: Advanced Encryption Standard (AES), el protocolo de cifrado utilizado por los Estados Unidos y otros gobiernos para proteger la información confidencial y clasificada, y por la empresa para asegurar las redes WLAN y IEEE 802.1 X. WPA2 se basa en el estándar IEEE 802.11i y proporciona encriptación basada en AES de 128 bits. También proporciona autenticación mutua con Pre-Shared Key (PSK, en el modo personal) y con IEEE 802.1X / EAP (en el modo de empresa) (Wireless Fidelity Alliance, 2012).

En 2004, la Alianza Wi-Fi introdujo la certificación WPA2. En el año 2006 la certificación WPA2 se hizo obligatorio para todos los equipos Wi-Fi CERTIFIED presentado para la certificación. Además, en 2007 la Alianza Wi-Fi introdujo el programa de configuración protegida Wi-Fi para simplificar y fomentar la activación de WPA2 en las redes residenciales. (Wireless Fidelity Alliance, 2012)

Con el anexo 802.11i de la IEEE (IEEE, 2016), que fue publicado en el año 2004 se logró solventar algunos problemas de seguridad de las redes WLAN sobre todo en el ámbito de confidencialidad y la integridad, pero en el caso de la disponibilidad aun esta echo un estudio con profundidad (Labs, 2007).

Tabla 1. 2. *Descripción de protocolo WPA2.*

WPA2-Enterprise	WPA2-Personal
A cada usuario se le asigna credencial única.	Modo no administrado para la autenticación usando PSK permite el uso de una frase de contraseña introducida manualmente, lo que normalmente es compartida por los usuarios de esa red.
Servidor AAA IEEE 802.1X con el apoyo y la autenticación de la base de datos.	No requiere de un servidor de autenticación.
La clave de seguridad de datos es única para cada sesión.	La clave de seguridad de datos es única para cada sesión.

Elaborado por: Los Autores

Tabla 1. 3. *Funcionamiento de protocolo WPA2.*

¿Cómo funciona el WPA2?	
WPA2-Enterprise	**WPA2-Personal**
1. El cliente asociado al dispositivo de punto de acceso envía su identidad al servidor de autenticación.	1. Tanto el cliente como el punto de acceso verifican que dispongan de la misma PSK
2. El servidor de autenticación acepta la identidad del cliente y envía sus credenciales al dispositivo cliente.	2. La autenticación se ha completado entre el dispositivo cliente y el punto de acceso con un apretón de manos de cuatro vías
3. El dispositivo cliente identifica el servidor como uno autorizado y envía credenciales de usuario para la validación.	3. En el saludo de cuatro vías, el PSK se utiliza para generar la PTK, tanto en el dispositivo cliente y el punto de acceso
4. Una llave maestra en pares y por parejas transitorios son generados en el dispositivo cliente y en el servidor de autenticación	4. Claves de cifrado AES se derivan de las PTK para cifrar los datos intercambiados entre el dispositivo cliente y el punto de acceso
5. La autenticación se ha completado entre el dispositivo cliente y el punto de acceso con un apretón de manos de cuatro vías	
6. Claves de cifrado AES se derivan de las PTK para cifrar los datos intercambiados entre el dispositivo cliente y el punto de acceso	

Fuente: (Wireless Fidelity Alliance, 2012)
Elaborado por: Los Autores

1.5.5. Detección de intrusiones

A través del análisis del tráfico de la red se puede detectar posibles ataques que buscan alterar la disponibilidad de los servicios. Se puede utilizar herramientas de software y hardware llamadas Sistemas de Detección de Intrusiones, cuáles pueden ser divididos en dos grandes grupos dependiendo de la estrategia de análisis y de detección de dichos eventos: IDS basados en la detección de uso indebido y los que son basados en la detección de anomalías (Pfleeger, Lawrence, & Margulies, 2015).

1.5.6. Sistemas de detección de intrusiones en redes 802.11

Los sistemas inalámbricos de detección de intrusiones (WINS) está basado en un grupo de sensores y un núcleo que recepta toda la información que proporciona las áreas de cobertura de los sensores inalámbricos. La arquitectura puede ser centralizada la cual se basa en la recopilación individual mediante sensores que remiten toda la información de la 802.11 a un analizador central donde toda la información es almacenada y procesada. (Romero, Balseca, Sáenz, & Diaz, 2016)

Capítulo II

2. Metodología

La metodología a utilizar en esta investigación es un estudio longitudinal, pues se obtiene datos en distintos momentos durante un periodo determinado, con la finalidad de examinar sus variaciones en el tiempo.

Se obtiene datos del estado de los ataques de la red inalámbrica en la Universidad Nacional de Chimborazo sin aplicar métodos de hacking ético y luego de aplicar el manual de políticas de seguridad para verificar los posibles ataques y vulnerabilidades en la red inalámbrica.

Para la comprobación de la hipótesis se utiliza la prueba estadística T-Student para muestras relacionadas y un estudio longitudinal, siendo la variable fija la que nos crea dos medidas una anterior y otra después. Una variable antes de aplicar hacking ético y una después de aplicar manual de políticas de seguridad en la red inalámbrica de la Universidad Nacional de Chimborazo. Luego se toma la variable aleatoria que es la variable de comparación, que son los indicadores las variables de comparación numéricas para el estudio.

La metodología de la investigación permite identificar y filtrar por palabras clave como: “Hacking Ético”, “Seguridad en la red Inalámbrica”, "Auditoria de red inalámbrica", “Seguridad de redes wifi”,” Ethical hacking and security network”; e investigar en los diferentes motores de búsqueda, para poder recuperar información relevante que aporte significativamente a la investigación, luego de aplicar criterios de selección y exclusión.

2.1. Tipo de estudio

2.1.1. Según el objeto de estudio.

- **Investigación Aplicada**

Permite aplicar métodos y técnicas de hacking ético con el apoyo de herramientas para la detección de vulnerabilidades y ataques en la red inalámbrica.

2.1.2. Según nivel de medición y análisis de la información.

- **Investigación Descriptiva**

Se realiza un análisis sobre las vulnerabilidades y riegos que afectan la optimización de la red, así como también medir y evaluar la seguridad de la red inalámbrica con la utilización de herramientas y metodologías.

2.1.3. Según las variables.

- **Investigación Experimental**

Se realiza el estudio de la red inalámbrica de la Universidad Nacional de Chimborazo aplicando técnicas y metodologías de hacking ético con la ayuda de herramientas de software libre que permitirán comprobar la seguridad y de esta manera se podrá implementar mejoras de seguridad en la red inalámbrica y de esta manera poder comprobar la hipótesis de la investigación.

2.2.Población y muestra

En la investigación no se dispone de población y muestra porque se va a trabajar con equipos de la red inalámbrica que actualmente funcionan en la Universidad Nacional de Chimborazo**.**

2.3.Operacionalización de variables

Tabla 2. 1. *Identificación de variables.*

VARIABLE	TIPO	DEFINICIÓN CONCEPTUAL	DIMENSIÓN	INDICADOR
La aplicación de Hacking Ético	Independiente	Hacking ético es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.	Reconocimiento y Escaneo Obtener Acceso Borrar Huellas	- Analizar el promedio de equipos conectados a la red inalámbrica. - Aplicar técnicas y herramientas para la evaluación y auditoria. - Eliminar el número de técnicas aplicadas en los equipos auditados.
El grado de mejora de seguridad en la red inalámbrica de la Universidad Nacional de Chimborazo.	Dependiente	Las redes inalámbricas se te incorporando en muchos más entornos corporativos, universitarios, PYMES y en el ámbito familiar. Este tipo de redes ofrece una gran cantidad de ventajas frente a las redes guiadas. Es por lo cual es muy importante mejorar la seguridad en la red inalámbrica.	Ataques Pasivos Ataques Activos Políticas de Administración de red	- Número de dispositivos que se pueden ser vulnerables a un análisis de paquetes o sniffer. - Nivel Vulnerabilidad detectada por descubrimiento de contraseñas. - Nivel de vulnerabilidad por spoofing. - Nivel de Calidad Servicio de la red inalámbrica. - Nivel de políticas de administración que se aplican.

Elaborado por: Los Autores

2.4.Procedimientos

Se aplican las siguientes fases de hacking ético en la red inalámbrica de la Universidad para la detección de vulnerabilidades en la misma.

2.4.1. Reconocimiento.

Consiste en descubrir la mayor cantidad de información relevante de la red inalámbrica de la Universidad Nacional de Chimborazo utilizando la técnica de reconocimiento activa pues existe una interacción directa con la red inalámbrica.

2.4.2. Escaneo.

Identificar los host activos dentro de ciertos rangos de IP's y determinar si es posible escuchar datos que están siendo transmitidos por estos medios y así conocer si los hosts de la red tienen vulnerabilidades informáticas potenciales para explotar.

2.4.3. Enumeración.

Recolectar información relevante acerca de vulnerabilidades y hosts, aprovechando una debilidad en uno o más de los protocolos o servicios activos detectados previamente.

2.4.4. Explotación o hacking.

Se realizará los test de penetración a la red inalámbrica de la universidad con la que se obtendrá información más profunda para de esta manera determinar las vulnerabilidades y amenazas. Se aplicarán ataques pasivos y activos, internos y externos a la universidad para comprobar el aseguramiento de la red inalámbrica.

2.4.5. Informe.

Pasos generales para aplicar con éxito en la documentación de cualquier auditoría.

1. Desarrollar una bitácora de las actividades que se realiza a diario.
2. Capturar imágenes / video de los aspectos más relevantes.
3. Elaborar un registro de los hallazgos a lo largo de la auditoria.
4. Utilizar un software o herramientas que facilite la documentación.

2.5.Escenarios

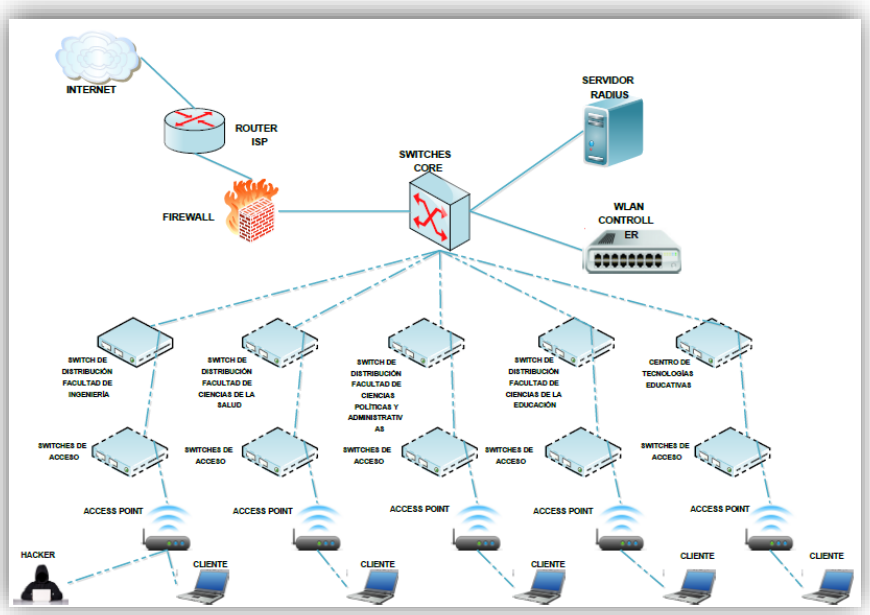


Figura 2. 1. *Topología de red donde se realizó los procedimientos de la investigación.*

Elaborado por: Los Autores

Capitulo III

3. Resultados y discusión

3.1.Análisis de herramientas

Como resultado del análisis y revisión bibliográficas de las diversas herramientas para hacking ético se establece de acuerdo los escenarios de medición propuestos las características siguientes.

Tabla 3. 1. *Análisis de herramientas de sniffer para hacking ético.*

HERRAMIENTA	LICENCIA	DESCRIPCIÓN	PLATAFORMA	APLICACIÓN	ESCENARIO
WireShark	General Public License	Se utiliza para analizar el tráfico de paquetes en una red, se apoya en una interfaz gráfica que facilita el uso.	Multiplataforma	Sniffer	Se aplica en el escenario 1, figura2.2
Microsoft Network Monitor	Licencia Gratuita	Descifra protocolos de red utilizados, captura en tiempo real el tráfico de datos.	Sistemas Operativos Microsoft Windows	Sniffer	Se aplica en el escenario 1, figura2.2
Capsa packet Sniffer	Freeware y Shareware	Captura y decodifica el tráfico de red monitoreada.	Sistemas Operativos Microsoft Windows	Sniffer	Se aplica en el escenario 1, figura2.2
InnoNWSniFfer	Licencia Gratuita	Puede escanear en vivo IP públicas y cualquier ordenador de la LAN, muestra una información muy detallada del sistema.	Linux y Microsoft Windows	Sniffer	Se aplica en el escenario 1, figura2.2
SniffPass	Licencia Gratuita	Captura contraseñas del tráfico de la red, compatible con protocolos de red POP3, IMAP4, SMTP, FTP y HTTP	Sistemas Operativos Microsoft Windows	Sniffer	Se aplica en el escenario 1, figura2.2

Elaborado por: Los Autores

Tabla 3. 2. *Análisis de herramientas de spoofing para hacking ético.*

HERRAMIENTA	LICENCIA	DESCRIPCIÓN	PLATAFORMA	APLICACIÓN	ESCENARIO
Nessus	Propietaria y GPL	Herramienta de escaneo y descubre vulnerabilidades de una red.	Multi Plataforma	Escáner de vulnerabilidad	Se aplica en el escenario 1, figura2.2
Ettercap	GNU General Public License	Es un interceptor de datos de una red, utiliza PPTP (Point to point tunneling protocol) que ayuda a establecer un ataque hombre en el medio.	Multi Plataforma	Seguridad Informática	Se aplica en el escenario 2, figura2.3
MDK3	GNU General Public License	Autenticación de denegación de servicio para bloquear Puntos de acceso de una red inalámbrica.	Linux	Denegación de Servicio	Se aplica en el escenario 2, figura2.3

Elaborado por: Los Autores

3.2.Comprobación de hipótesis

La prueba de hipótesis estadística es una regla que con base en una hipótesis nula H_0 ayuda a decidir si ésta se acepta o no. Para la verificación de la hipótesis se hará uso de la distribución t de Student en dos muestras relacionadas y porque las poblaciones son pequeñas. Con ello se da a entender que, en el primer período, las observaciones servirán de control o testigo, para conocer los cambios que se susciten después de aplicar una variable experimental. (Sarabia)

3.2.1. Planteamiento de hipótesis

H_0 = La aplicación de Hacking Ético NO permite mejorar la seguridad de las redes inalámbricas de la Universidad Nacional de Chimborazo.

H_a= La aplicación de Hacking Ético permite mejorar la seguridad de las redes inalámbricas de la Universidad Nacional de Chimborazo.

3.2.2. Nivel de significación

El valor del nivel de significación va a ser de α=0.05 = 5%

3.3.Comprobación por indicador

3.3.1. Indicador: Número de dispositivos que se pueden ser vulnerables a un análisis de paquetes o sniffer red de estudiantes.

Se aplicó un análisis de paquete de datos (sniffer) con cinco herramientas de software distintas, se realizará un estudio preliminar a la red de estudiantes y un estudio posterior a la aplicación de políticas de seguridad. (Tabla 3.1)

Tabla 3. 3 *Base de datos de clientes de la red de Estudiantes aplicando Sniffer*

Nombre Herramienta	Numero de dispositivos Antes	Numero de dispositivos Después
WireShark	898	568
Microsoft Network Monitor	877	423
Capsa packet Sniffer	841	412
InnoNWSniFfer	868	487
SniffPass	854	451

Elaborado por: Los Autores

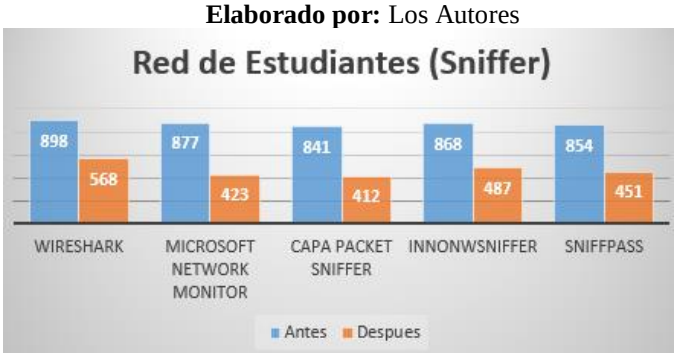


Figura 3. 1. *Base de datos de clientes de la red de Estudiantes aplicando Sniffer*
Elaborado por: Los Autores

CONCLUSIÓN:

Los datos del indicador (Número de dispositivos que se pueden ser vulnerables a un análisis de paquetes o sniffer red de Estudiantes) para la red de estudiantes provienen de una distribución **normal.**

3.3.1.1.Decisión Estadística

Una vez obtenido y verificado la normalidad de los datos obtenidos para el estudio se realizó en el software estadístico SPSS la medición la Prueba de T Student para muestras relacionadas y de esta manera se aplicará criterios para aceptar o negar las Hipótesis nula o alternativa. (Tabla 3.2)

Tabla 3. 2. *Prueba de Muestras de emparejadas para el primer indicador*

		Diferencias emparejadas					t	gl	Sig.
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Numero_Dispositivos_Estudisntes_A Numero_Dispositivos_Estudisntes_D	399,40	47,501	21,243	340,42	458,380	18,802	4	,000047
P-Valor = 0.00				**<=**		**α=0.05**			

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Elaborado por: Los Autores

3.3.1.2.Análisis e Interpretación

El número de dispositivos analizados con cinco herramientas de sniffer obtenemos un promedio de 867 clientes que se podían analizar sus paquetes que se trasmitía por la red de estudiantes previamente a la aplicación de políticas de seguridad. Se realiza el mismo estudio con las mismo cinco herramientas, pero una vez aplicada políticas de seguridad y nos dio como resultado un promedio de 468 clientes que se podía analizar sus paquetes que trasmitía por la red de estudiantes dándonos como resultado favorable que se disminuyó en un 46.03% esta vulnerabilidad de la red inalámbrica de estudiantes y con una significancia de 0,000047. No se reduce en su totalidad pues los ataques sniffer trabajan en modo pasivo, el software de detección de sniffer no es efectivo en su totalidad. Por lo cual, se establece que la **aplicación de Hacking Ético SI permite mejorar la seguridad de las redes inalámbricas de la Universidad Nacional de Chimborazo.**

3.3.2. Indicador: Número de dispositivos que se pueden ser vulnerables a un análisis de paquetes o sniffer red de docentes.

Se aplicó un análisis de paquete de datos (sniffer) con cinco herramientas de software distintas, se realizará un estudio preliminar a la red de docentes y un estudio posterior a la aplicación de políticas de seguridad. (Tabla 3.3)

Tabla 3. 3. *Base de datos de clientes de la red de Docentes aplicando Sniffer*

Nombre Herramienta	Número de dispositivos Antes	Número de dispositivos Después
WireShark	592	348
Microsoft Network Monitor	482	297
Capsa packet Sniffer	524	238
InnoNWSniFfer	517	259
SniffPass	497	287

Elaborado por: Los Autores

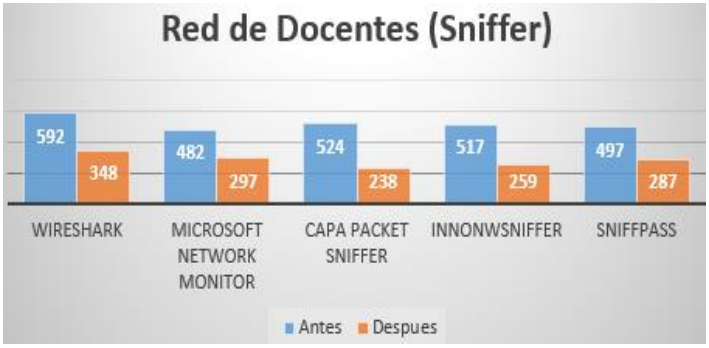


Figura 3. 2. *Base de datos de clientes de la red de Docentes aplicando Sniffer*
Elaborado por: Los Autores

CONCLUSIÓN:

Los datos del indicador (Número de dispositivos que se pueden ser vulnerables a un análisis de paquetes o sniffer red de Docentes) para la red de estudiantes provienen de una distribución **normal.**

3.3.2.1.Decisión Estadística

Una vez obtenido y verificado la normalidad de los datos obtenidos para el estudio se realizó en el software estadístico SPSS la medición la Prueba de T Student para muestras relacionadas y de esta manera se aplicará criterios para aceptar o negar las Hipótesis nula o alternativa. (Ver Tabla 3.4)

Tabla 3. 4. *Prueba de muestras emparejadas del segundo indicador*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Numero_Dispositivos_Docentes_A - Numero_Dispositivos_Docentes_D	236,600	39,759	17,781	187,232	285,968	13,306	4	,000184
P-Valor = 0.00			**<=**			**α=0.05**			

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0
Elaborado por: Los Autores

3.3.2.2. Análisis e Interpretación

El número de dispositivos analizados con cinco herramientas de sniffer obtenemos un promedio de 522 clientes que se podían analizar sus paquetes que se trasmitía por la red de docentes previamente a la aplicación de políticas de seguridad. Se realiza el mismo estudio con las cinco herramientas, pero una vez aplicada políticas de seguridad proporciona como resultado un promedio de 286 clientes que pueden analizar sus paquetes dando como resultado favorable que se disminuye en un 45.21% esta vulnerabilidad de la red inalámbrica de docentes y con una significancia de 0,000184. No se reduce en su totalidad pues los ataques sniffer trabajan en modo pasivo, el software de detección de sniffer no es efectivo en su totalidad. Por lo cual, se establece que la **aplicación de Hacking Ético SI permite mejorar la seguridad de las redes inalámbricas de la Universidad Nacional de Chimborazo.**

3.3.3. Indicador: Nivel de vulnerabilidad por spoofing para las redes estudiantes y docentes.

Se tomó 5 ataques que vulneran la seguridad de la red inalámbrica tanto de Estudiantes como Docentes y se ha realizado una escala para medir el nivel de vulnerabilidad que es de 1 a 4 Bajo, 5 a 7 Medio y de 8 a 10 Alto el nivel de vulnerabilidad. De igual manera se realizó un estudio preliminar y un estudio posterior a la aplicación de políticas de seguridad que ayudan a mitigar este tipo de vulnerabilidades. (Tabla 3.5)

Tabla 3. 5. *Nivel de vulnerabilidades de la red inalámbrica antes y después.*

Ataque	Nivel de vulnerabilidad Antes	Nivel de Vulnerabilidad Después
Hombre en el medio	8	5
Non-Blind y Blind	6	3
Denegacion de servicio (DoS)	4	4
Ingeniaria Social	9	3
Puntos de acceso no autorizado	7	4

Elaborado por: Los Autores

Figura 3. 3. *Nivel de vulnerabilidades de la red inalámbrica*
Elaborado por: Los Autores

CONCLUSIÓN:

Los datos del indicador (Nivel de vulnerabilidad por spoofing para las redes Estudiantes y Docentes) provienen de una distribución **normal**

3.3.3.1.Decisión Estadística

Una vez obtenido y verificado la normalidad de los datos obtenidos para el estudio se realizó en el software estadístico SPSS la medición la Prueba de T Student para muestras relacionadas y de esta manera se aplicará criterios para aceptar o negar las Hipótesis nula o alternativa. (Tabla 3.6)

Tabla 3. 6. *pruebas de emparejamiento del tercer indicador*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	g l	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Nivel_Vulnerabilidad_Antes - Nivel_Vulnerabilidad_Despues	3,000	2,121	,949	,366	5,634	3,162	4	,034
P-Valor = 0.034			<=			**α=0.05**			

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Elaborado por: Los Autores

3.3.3.2.Análisis e Interpretación

Se realizó un estudio con cinco ataques para medir el nivel de vulnerabilidad de la red de inalámbrica de la Universidad Nacional de Chimborazo con la cual se obtuvo un promedio de nivel de vulnerabilidad de 6.8 sobre 10 previo a la aplicación de políticas de seguridad. Una vez aplicada políticas de seguridad en la red inalámbrica se realizó los mismos ataques y como resultado se obtuvo un promedio de 3.8 sobre 10 teniendo como conclusión que se disminuyó el nivel de vulnerabilidad en un 44.11% y con una significancia de 0.034. Los ataques de spoofing no se pueden reducir en su totalidad pues el software de detección se instala en cada uno de los hosts que intervienen en la red y de igual manera se reduce en un porcentaje los ataques de ingeniería social y puntos de acceso no autorizado por el mal manejo de las políticas de seguridad. Por lo cual, se establece que la **aplicación de Hacking Ético SI permite mejorar la seguridad de las redes inalámbricas de la Universidad Nacional de Chimborazo.**

3.3.4. Indicador: Nivel de calidad servicio de la red inalámbrica para las redes estudiantes y docentes.

Se tomó las cuatro facultades y el edificio CTE para el estudio de nivel de calidad en la red inalámbrica y se ha realizado una escala para medir el nivel de vulnerabilidad que es de 1 a 4 Bajo, 5 a 7 Medio y de 8 a 10 Alto la calidad de servicio. De igual manera se realizó un estudio preliminar y un estudio posterior a la aplicación de políticas de seguridad que ayudan a mejorar la calidad de servicio en la red inalámbrica de Estudiantes y Docentes. (Tabla 3.7)

Tabla 3. 7. *Calidad de servicio de la red inalámbrica el antes y después*

Facultad	Nivel de servicio Antes	Nivel de servicio Después
Ingeniería	7,0	8,5
Ciencias de la Educación	3,5	8,4
Ciencias de la Salud	5,5	8,5
Ciencias Políticas y Administrativas	6,5	9,0
Centro de Tecnología Educativas	7,5	9,0

Elaborado por: Los Autores

Figura 3. 4. *Calidad de servicio de la red inalámbrica de antes y después*

Elaborado por: Los Autores

CONCLUSIÓN:

Los datos del indicador (Nivel de Calidad Servicio de la red inalámbrica para las redes Estudiantes y Docentes) provienen de una distribución **normal.**

3.3.4.1. Decisión Estadística

Una vez obtenido y verificado la normalidad de los datos obtenidos para el estudio se realizó en el software estadístico SPSS la medición la Prueba de T Student para muestras relacionadas y de esta manera se aplicará criterios para aceptar o negar las Hipótesis nula o alternativa. (Tabla 3.8)

Tabla 3. 8. *Prueba de muestras emparejadas del cuarto indicador*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Nivel_Servicio_Antes - Nivel_Servicio_Despues	-2,6800	1,4007	,6264	-4,4192	-,9408	-4,278	4	,013
P-Valor = 0.013			**<=**			**α=0.05**			

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Elaborado por: Los Autores

3.3.4.2.Análisis e Interpretación

Se realizará un estudio en los cuatro edificios de las facultades y en el edificio centro de tecnologías educativas para comprobar el nivel de calidad del servicio de la red inalámbrica lo cual se aplicó dos estudios uno previo a la aplicación de políticas de seguridad con el cual se obtuvo un promedio de 6 sobre 10. Una vez

aplicada políticas seguridad se realizó el estudio en los 5 edificios de la universidad y se obtiene como resultado que incrementa el nivel de servicio de la red inalámbrica con una puntuación promedio de 8.68 sobre 10 por lo cual se concluye que se incrementó el nivel de calidad 86.8% con una significancia de 0.013. El incremento de este indicador será paulatinamente una vez aplicado el manual de políticas de seguridad recomendado. Por lo cual, se establece que la **aplicación de Hacking Ético SI permite mejorar la seguridad de las redes inalámbricas de la Universidad Nacional de Chimborazo.**

3.3.5. Nivel de políticas de administración que se aplica a red inalámbrica.

Se tomó cinco criterios de políticas de seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo para el estudio de nivel de políticas administrativas en la red inalámbrica y se ha realizado una escala para medir el nivel de políticas de seguridad que es de 1 a 4 Bajo, 5 a 7 Medio y de 8 a 10 Alto. De igual manera se realizó un estudio preliminar y un estudio posterior a la aplicación de políticas de seguridad que ayudan a mejorar de las políticas de seguridad en la red inalámbrica de Estudiantes y Docentes. (Tabla 3.9)

Tabla 3.9. *Nivel de políticas de la red inalámbricas antes y después*

Tipo de políticas	Nivel de políticas antes	Nivel de políticas después
Mecanismos de identificación e autenticación	6,5	9,0
Mecanismos de separación	9,0	9,0
Mecanismos de seguridad en la comunicación	4,5	8,5
Prevención y detección de virus	4,5	9,5
Seguridad física y ambiental	9,0	9,0
Seguridad de personas	5,0	8,5

Elaborado por: Los Autores

Figura 3. 5. *Nivel de políticas de la red inalámbricas antes y después*

Elaborado por: Los Autores

CONCLUSIÓN:

Los datos del indicador (Nivel de políticas de administración que se aplica a red inalámbrica) provienen de una distribución **normal**

3.3.5.1. Decisión Estadística

Una vez obtenido y verificado la normalidad de los datos obtenidos para el estudio se realizó en el software estadístico SPSS la medición la Prueba de T Student para muestras relacionadas y de esta manera se aplicará criterios para aceptar o negar las Hipótesis nula o alternativa. (Tabla 3.10)

Tabla 3. 10. *Prueba de muestras emparejadas*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Nivel_Policas_Antes - Nivel_Policas_Despues	-2,50000	2,09762	,85635	-4,70131	-,29869	-2,919	5	,033
P-Valor = 0.033			**<=**			**α=0.05**			

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Elaborado por: Los Autores

3.3.5.2.Análisis e Interpretación

Se realizó un estudio previo a la aplicación de políticas de seguridad a nivel administrativo de la red inalámbrica y se obtuvo como promedio 6.41 sobre 10 aplicando 6 parámetros de calificación. Se realizó de la misma manera el mismo estudio, pero una vez aplicado las políticas de seguridad y se obtuvo un promedio de 8.91 sobre 10 por lo cual se concluye que aumento las políticas administrativas de la red inalámbrica de 64.1% a 89.1% con una significancia de 0.033. Por lo cual, se establece que la **aplicación de Hacking Ético SI permite mejorar la seguridad de las redes inalámbricas de la Universidad Nacional de Chimborazo.**

Capitulo IV

4. Conclusiones y recomendaciones

4.1.Conclusiones

- Luego de realizar el análisis de herramientas para hacking ético y su aplicación en los diferentes escenarios, se determina que las mejores herramientas son WireShark, Microsoft Network Monitor, Capsa packet Sniffer, InnoNWSniFfer, SniffPass, Nessus, Ettercap, MDK3, pues permiten clasificar paquetes, evitar ataques de hombre en el medio, denegación de servicio e identificación de anomalías en la red inalámbrica de la Universidad Nacional de Chimborazo.

- Luego de la aplicación de las herramientas seleccionadas para hacking ético utilizando ataques sniffer y spoofing, se determinó que el 80% de las vulnerabilidades más críticas fueron detectadas en la capa de aplicación y un 20% en la capa de transporte.

- Una vez aplicado los cálculos estadísticos de los datos obtenidos en cada uno de los indicadores propuestos antes y después de la aplicación del manual de políticas de seguridad se determina que el primer indicador disminuye en un 45.62%; el segundo indicador disminuye en un 44.11%; el tercer indicador mejora la calidad de servicio de 60% a 86.8%; el cuarto indicador aumenta el nivel de políticas de 64.1% a 89.1%, permitiendo concluir que las medidas de seguridad aplicadas si permiten mejorar la seguridad de la red inalámbrica.

- Con los resultados obtenidos en la red de estudiantes con un nivel de significancia de 0,000047 y en la red de docentes con un nivel de significancia de 0,000184 de los dispositivos vulnerados se concluye la necesidad de implementar un manual de políticas de seguridad debido a las constantes amenazas que se encuentran en la red, por ejemplo servidores distribuidos, separación de redes por Vlan’s, autenticación en la red inalámbrica, para resolver las vulnerabilidades encontradas es indispensable

instruir al personal sobre los procedimientos apropiados y aceptables y de esta manera obtener un mejor nivel de calidad de servicio en la red inalámbrica.

- De acuerdo a la auditoría técnica realizada y el manual de políticas de seguridad desarrollado en base a las vulnerabilidades detectadas en la red inalámbrica de la Universidad Nacional de Chimborazo, se concluye que se podrá mejorar la seguridad en al menos un 25%.

4.2.Recomendaciones

- Se recomienda tomar este trabajo de investigación como guía para las instituciones de nivel superior, para determinar el nivel de vulnerabilidades, para la implementación de políticas de seguridad, al realizar evaluaciones internas y generar planes de contingencia en caso de ataques informáticos.

- Para poder realizar pruebas de seguridad informática en los equipos de una red se recomienda el software Kali Linux en los Host que se utiliza para realizar la auditoria, pues es una herramienta que permite realizar auditorías informáticas, posee un abanico de herramientas todas ellas destinadas a realizar pruebas, diagnósticos y comprobaciones de aspectos importantes para evaluar la seguridad informática de los equipos destinados.

- Se recomienda a los usuarios finales de una red inalámbrica wifi mantenerse al día con las actualizaciones de su sistema operativo, firmware del Access Point, firewalls, antivirus, sistema de detección de intrusos, limpiadores de registros, además de las medidas sugeridas en esta investigación que vienen a ser preventivas, complementándolas con medidas correctivas que ayuden a la mitigación de las brechas existentes en redes inalámbricas wifi.

- Es recomendable que toda institución educativa o entidad publica que maneje una red datos corporativa, tenga un manual de políticas de seguridad que permita establecer normativas para los usuarios que hagan uso de los servicios que brinda la institución.

5. Bibliografía

TILLER, J. (2005). *The Ethical Hack A Framework for Business Value Penetration Testing.*

Andreu a, F., Pellerejo, I., & Lesta, A. (2006). *Redes WLAN Fundamentos y aplicaciones de seguridad.* Barcelona: Marcombo SA. Recuperado el 30 de Octubre de 2016

Andreu b, F., Pellerejo, I., & Lesta, A. (2006). *Redes WLAN Fundamentos y aplicaciones de seguridad.* Barcelona: MARCOMBO S.A. Recuperado el 30 de Octubre de 2016

Andreu c, F., Pellejero, I., & Lesta, A. (2006). *Redes WLAN Fundamentos y aplicaciones de seguridad.* Barcelona, España: Marcombo S.A.

ArCERT Coordinación de Emergencia en Redes Teleinformaticas. (s.f.). *Manual de Seguridad en Redes.* ArCERT, Subsecretaría de Tecnologías Informáticas, Secretaría de la Función Pública. Republica de Argentina: ArCERT. Recuperado el 10 de Febrero de 2017, de http://instituciones.sld.cu/dnspminsap/files/2013/10/Manual-de-Seguridad-de-Redes.pdf

Astudillo, K. B. (2013). HACKING ÉTICO 101. Guayaquil, Guayas, Ecuador. Recuperado el 30 de Octubre de 2016

Barajas a, S. (Junio de 2004). Protocolos de seguridad en redes inalámbricas. *Tesis de la Universidad Carlos III de Madrid*, 5. Madrid, Madrid, España. Recuperado el 30 de Octubre de 2016

Barajas b, S. (Junio de 2004). Protocolos de seguridad en redes inalámbricas. *Tesis de la Universidad Carlos III de Madrid*, 5. Madrid, Madrid, España. Recuperado el 30 de Octubre de 2016

Bonilla, J. M. (2015). *Aplicacion de hacking etico para la determinacion de amenazas, riesgos y vulnerabilidades de la red inalambrica de una institucion.* Quito. Recuperado el 30 de octubre de 2016

Cisco Systems, I. (s.f.). *Fundamentos de redes* .

Colprensa. (9 de enero de 2015). *En COlombia las cifras de delitos informaticos van en aumento millones*. Recuperado el 30 de octubre de 2016, de http://www.elpais.com.co/elpais/judicial/noticias/colombiacifras-delitos-informaticos-van-aumento

Ernst & Young Global. (2011). Seguridad de la información en un mundo sin fronteras. *Ernst & Young Global*, 6.

Fiscalia General del Ecuador. (13 de Junio de 2015). *Fiscalia General del Estado*. Obtenido de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

Gacharna, F. (2014). *Top 10 de pruebas de penetracion y hacking a redes inalmabricas.* Version 2.1. Recuperado el 30 de octubre de 2016

Giraldo, J., Giraldo, B., Huertas, C., & Camacho, J. (03 de Diciembre de 2011). Implementación de seguridad en redes inalámbricas. 4. Cali, Cali, Colombia: Corporacioón Universitaria Minuto de Dios. Recuperado el 30 de Octubre de 2016

Goncalves, M. (1997). *Firewalls Complete. Beta Book.* EE.UU.: McGraw Hill.

Grupo de Trabajo de IEEE 802.11. (s.f.). *IEEE*. Obtenido de http://grouper.ieee.org/groups/802/11/

Manchola, S., Suarez, G. C., & Herrera, O. B. (2016). Investigacion sobre el hacker y sus posibles comienzos en la comunidad estudiantil. *EATIS*, 1 - 8. Recuperado el 30 de octubre de 2016

Miro, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid.

Pacheco a, F. G., & Jara, H. (2012). Ethical Hacking 2.0. En D. S.A. (Ed.). Buenos Aires, Argentina: Fox Andina. Recuperado el 30 de Octubre de 2016

Pacheco b, F. G., & Jara, H. (2012). Ethical Hacking 2.0. En D. S.A. (Ed.). Buenoas Aires, Argentina: Fox Andina. Recuperado el 30 de Octubre de 2016

Pacheco c, F. G., & Jara, H. (2012). Ethical Hacking 2.0. Buenos Aires, Argentina: Fox Andina. Recuperado el 30 de Octubre de 2016

Pfleeger, C., Lawrence, S., & Margulies, J. (2015). Sucurity in Computing. En *Sucurity in Computing* (pág. 1043). Massachusetts: Prentice Hall.

Quezada, A. C. (2015). Hacking con Kali Linux. Lima, Peru. Recuperado el 30 de Octubre de 2016, de http://www.reydes.com/d/?q=node/2

Rios, D. (2011). SEGURIDAD EN REDES WI-FI. *Monografia de Seguridad en redes Wi-fi*, 10. Chaco, Corrientes, Argentina: Universidad Nacional del Nordeste. Recuperado el 10 de Febrero de 2017, de http://www.exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MONOGRAFIA_DE_SEGURIDAD_EN_%20REDES_WIFI.pdf

Rodríguez, K. (2013). Los ataques cibernéticos mas grandes de la historia. *PC World Mexico*.

Romero, C., Balseca, L., Sáenz, F., & Diaz, J. (2016). Estado del Arte en la deteccion de Intrusiones en las redes 802.11i. *MASKAY.*

Sarabia, J. M. (s.f.). Distribuciones multivariantes con distribuciones condicionadas t de Student. España.

Tori, C. (2008). *Hacking Etico* (Primera Edicion ed.). Rosario, Argentina: Mastroianni Impresiones. Recuperado el 30 de Octubre de 2016

Wireless Fidelity Alliance. (2012). *Wireless Fidelity Alliance*. Recuperado el 06 de Noviembre de 2016, de http://www.wi-fi.org/downloads-registered-guest/20120229_State_of_Wi-Fi_Security_09May2012_updated_cert.pdf/7600

Zunzunwala , A. A., & Amruta , K. F. (2010). Ethical Hacking. *International Journal of Computer Aplications*.

ANEXOS

ANEXOS 1: Escenarios de la metodología de la investigación.

1.1.Escenario 1: Ataques sniffer a la red inalámbrica estudiantes y docentes

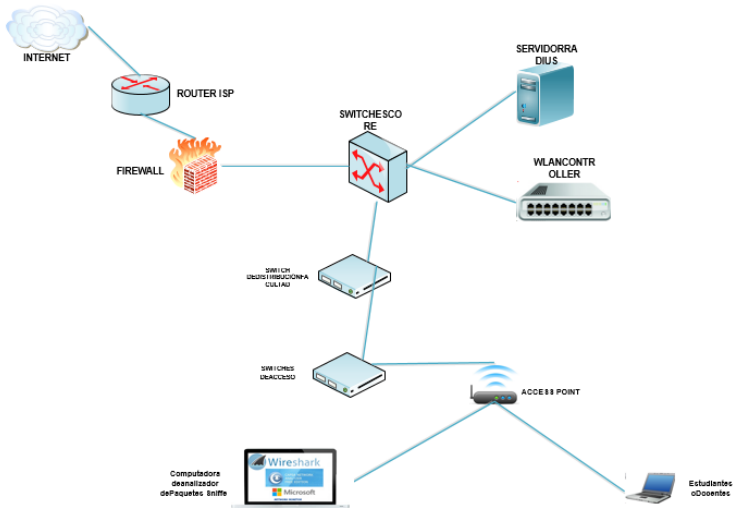


Figura 1.1. *Topología de Ataques sniffer a la red inalámbrica estudiantes y docentes*

Elaborado por: Los Autores

Con la utilización de un ordenador que estará conectada como un cliente más de la red inalámbrica, se realiza un análisis de paquetes de datos (sniffer) que se trasmiten por la red inalámbrica tanto de Estudiantes como Docentes, para ello se utiliza las siguientes herramientas WireShark, Microsoft Network Monitor, Capa Packet Sniffer, InnoNWSniFfer, SniffPass, con el objetivo de conocer si pueden ser atacados o vulnerables a ataques con el análisis de paquetes.

1.2.Escenario 2. Nivel de vulnerabilidad por spoofing a la red inalámbrica estudiantes y docentes

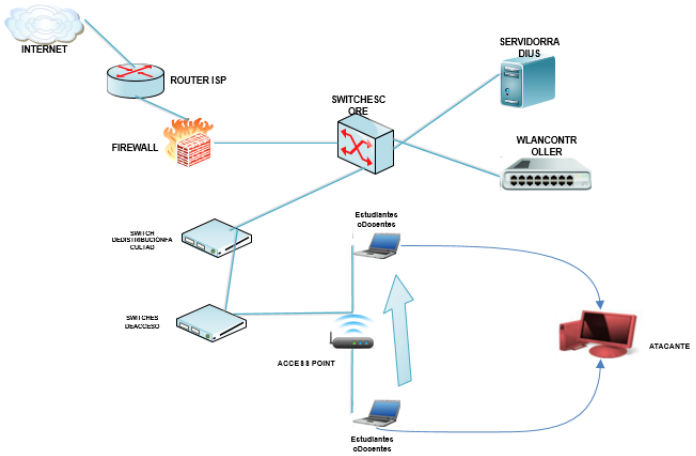


Figura 1.2. *Topología de nivel de vulnerabilidad por spoofing a la red inalámbrica estudiantes y docentes*

Elaborado por: Los Autores

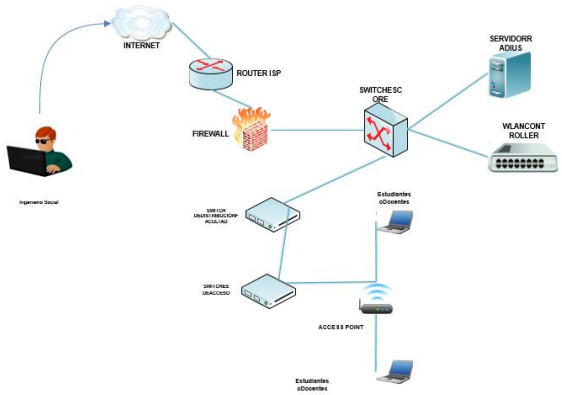


Figura 1.3. *Topología de ingeniería social a la red inalámbrica estudiantes y docentes*

Elaborado por: Los Autores

De igual forma, con la utilización de un ordenador que estará conectada como un cliente más de la red inalámbrica, se realiza los siguientes ataques de spoofing Hombre en el medio, Non-Blind y Blind, Denegación de servicio, Ingeniaría Social, Puntos de acceso no autorizado; con los cuales se obtendrá el nivel de vulnerabilidad a la que está expuesta la red inalámbrica.

1.3.Escenario 3. Nivel de calidad servicio en la red inalámbrica estudiantes y docentes.

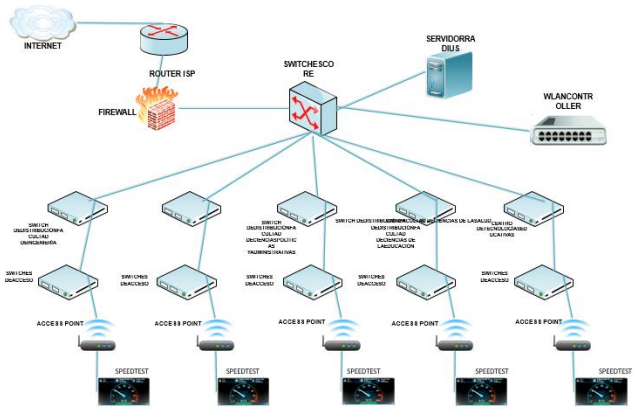


Figura 1.4. *Topología de Nivel de calidad servicio en la red inalámbrica estudiantes y docentes.*

Elaborado por: Los Autores

Se tomó las cuatro facultades Ingeniería, Ciencias de la Educación, Ciencias de la Salud, Ciencias Políticas y Administrativas y el edificio Centro de Tecnología Educativas (CTE) para el estudio de nivel de calidad en la red inalámbrica, para la medición se realizó una escala de 1 a 4 Bajo, 5 a 7 Medio y de 8 a 10 Alto la calidad de servicio, para ayudar a comprobar cuál es nivel de calidad de la red inalámbrica con la utilización de diferentes herramientas.

ANEXOS 2: Resultados de Metodología Research

Tabla 2. 1. *Desarrollo del método Research*

Query	Google scholar	IEEE	Microsoft Academic Search	Scopus	Total
“Hacking Ético”	248	18	1	6	273
“Seguridad en la red Inalámbrica”	56	11	7	5	79
"Auditoria de red inalámbrica"	2	0	1	2	5
“Seguridad de redes wifi”	2	445	2	1	450

Tabla 2. 2. *Criterios exclusión del método Research*

APLICANDO CRITERIOS DE EXCLUSION	Google scholar
"Hacking Ético" -lan -wan -man -san -herramientas privadas	8
“Seguridad en la red Inalámbrica" -lan -wan -man -san -herramientas privadas	3
"Auditoria de red inalámbrica"	2
“Seguridad de redes wifi” -lan -wan -man -san -herramientas privadas	0
APLICANDO CRITERIOS DE EXCLUSION	**IEEE**
(“Hacking Ético”) and refined by Year: 2006-2016	4
(“Seguridad en la red Inalámbrica”) and refined by Content Type: Conference Publications Books & eBooks Early Access Articles Year: 2006-2016	8
("Auditoria de red inalámbrica") and refined by Year: 2006-2016	0
(“Seguridad de redes wifi”) and refined by Content Type: Conference Publications Books & eBooks Year: 2006-2016	21
APLICANDO CRITERIOS DE EXCLUSION	**Microsoft Academic Search**
“Hacking Ético” Date Range 2006 - 2016	1
“Seguridad en la red Inalámbrica” Date Range 2006 – 2016	7
"Auditoria de red inalámbrica" Date Range 2007 – 2007	1
“Seguridad de redes wifi” Date Range 2005 – 20016	2
APLICANDO CRITERIOS DE EXCLUSION	**Scopus**
ALL (ethical hacking) AND PUBYEAR > 2005 AND (EXCLUDE (DOCTYPE , "ar OR LIMIT-TO DOCTYPE ")) AND (LIMIT-TO (LANGUAGE , "Spanish")) AND (LIMIT-TO (SUBJAREA , "ENGI"))	1
TITLE-ABS-KEY (wireless network security) AND PUBYEAR > 2005 AND (EXCLUDE (DOCTYPE , "ar OR LIMIT-TO DOCTYPE ")) AND (LIMIT-TO (LANGUAGE , "Spanish")) AND (LIMIT-TO (SUBJAREA , "ENGI")) AND (LIMIT-TO (SUBJAREA , "COMP"))	8
TITLE-ABS-KEY (audit wireless network) AND PUBYEAR > 2005 AND (EXCLUDE (DOCTYPE , "ar OR LIMIT-TO DOCTYPE ")) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "bk")) AND (LIMIT-TO (SUBJAREA , "ENGI"))	8
TITLE-ABS-KEY (wifi network security) AND PUBYEAR > 2005 AND (LIMIT-TO (LANGUAGE , "Spanish"))	1
TOTAL	**95**

Elaborado por: Los Autores

ANEXOS 3: Escaneo de Red

3.1.Wireless Network Watcher

La herramienta Wireless Network Watcher analiza la red inalámbrica y muestra la lista de todos los equipos y dispositivos que están actualmente conectados a la red y muestra: dirección IP, dirección MAC, compañía que fabricó tarjeta de red y nombre del equipo.

Herramienta Wireless Network Watcher

FECHA	HORA	RED	NUMERO USUARIOS
21/11/2016	10:04	Docentes	587
22/11/2016	10:09	Docentes	597
23/11/2016	10:06	Docentes	578
6/12/2016	17:05	Docentes	579
7/12/2016	17:21	Docentes	620
8/12/2016	0:00	Docentes	592

Red Docentes	
Promedio Mañana	587,3
Promedio Tarde	597

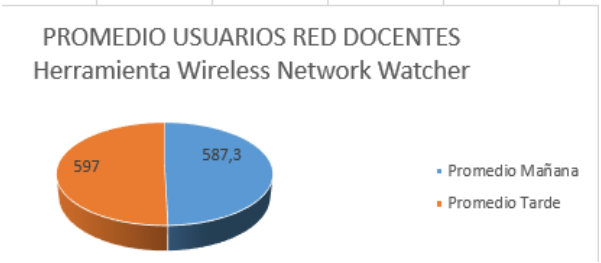


Figura 3. 1. Resultados obtenidos de la herramienta Wireless Network Watcher y representación gráfica de los resultados

Elaborado por: Los Autores

3.2.Softperfect Wifi Guard

La herramienta SoftPerfect WiFi Guard avisa si la red se utiliza sin conocimiento, se ejecuta a través de la red a intervalos establecidos e informa inmediatamente si ha encontrado cualquier dispositivo conectado nuevo, desconocido o no reconocido que podría pertenecer a un intruso.

Herramienta SoftPerfect WifiGuard

FECHA	HORA	RED	NUMERO USUARIOS
21/11/2016	10:04	Docentes	578
	16:16	Estudiantes	421
22/11/2016	10:09	Docentes	588
	10:17	Estudiantes	1050
23/11/2016	9:57	Docentes	116
	10:22	Estudiantes	1050
6/12/2016	17:08	Docentes	568
	16:50	Estudiantes	847
7/12/2016	17:42	Docentes	466
	17:55	Estudiantes	471
8/12/2016	12:01	Docentes	573
	17:23	Estudiantes	786

Red Docentes	
Promedio Mañana	427
Promedio Tarde	536
Red Estudiantes	
Promedio Mañana	1050
Promedio Tarde	631

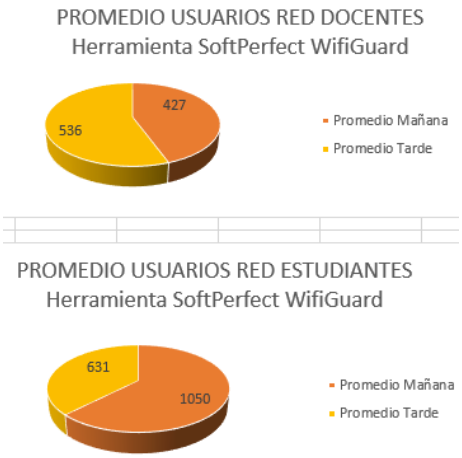


Figura 3. 2. *Resultados obtenidos de la herramienta Softperfect Wifi Guard y representaciones grafica de los resultados.*

Elaborado por: Los Autores

3.3.CISCO

Herramienta CISCO

FECHA	HORA	RED	NUMERO USUARIOS
21/11/2016	18:42	Estudiantes	594
	18:42	Docentes	347
22/11/2016	18:43	Estudiantes	591
	18:43	Docentes	350
23/11/2016	10:09	Estudiantes	1012
	10:09	Docentes	596
24/11/2016	10:18	Estudiantes	1041
	10:18	Docentes	596
6/12/2016	17:46	Estudiantes	820
	17:46	Docentes	512
7/12/2016	17:25	Estudiantes	900
	17:25	Docentes	540

Promedio Usuarios	
Red Docentes	
Promedio Mañana	596
Promedio Tarde	437
Red Estudiantes	
Promedio Mañana	1027
Promedio Tarde	726

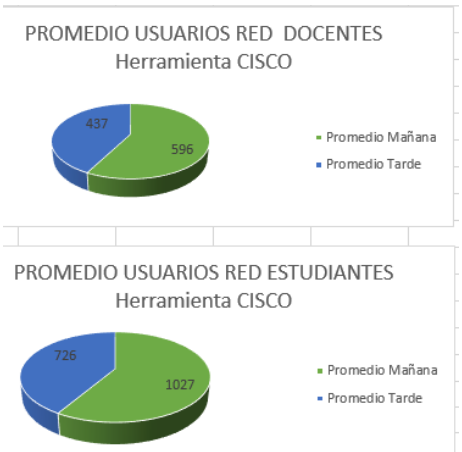


Figura 3. 3. *Resultados obtenidos de la herramienta CISCO y representaciones grafica de los resultados.*

Elaborado por: Los Autores

3.4.Nivel Vulnerabilidad Detectada Por Descubrimiento De Contraseñas.

En las pruebas de descubrimiento de contraseñas se utilizó el ataque de fuerza bruta el cual se realizó con el sistema operativo WifiSlax utilizando las herramientas GOYscript es una herramienta basada Aircrack-ng para la explotación de vulnerabilidades inalámbricas WEP, WPA y WPA2. Se realizó el ataque a las dos redes inalámbricas de la UNACH y el resultado fue negativo no se pudo obtener credenciales. La razón por la que no se pudo obtener las credencias es que la red se encuentra configurado con servidor RADIUS que es un mecanismo de autenticación y utiliza el protocolo de autenticación compatible con Microsoft PEAP. Se adjunta capturas de pantalla del intento de obtención de credenciales y documento de validación de uso de herramientas.

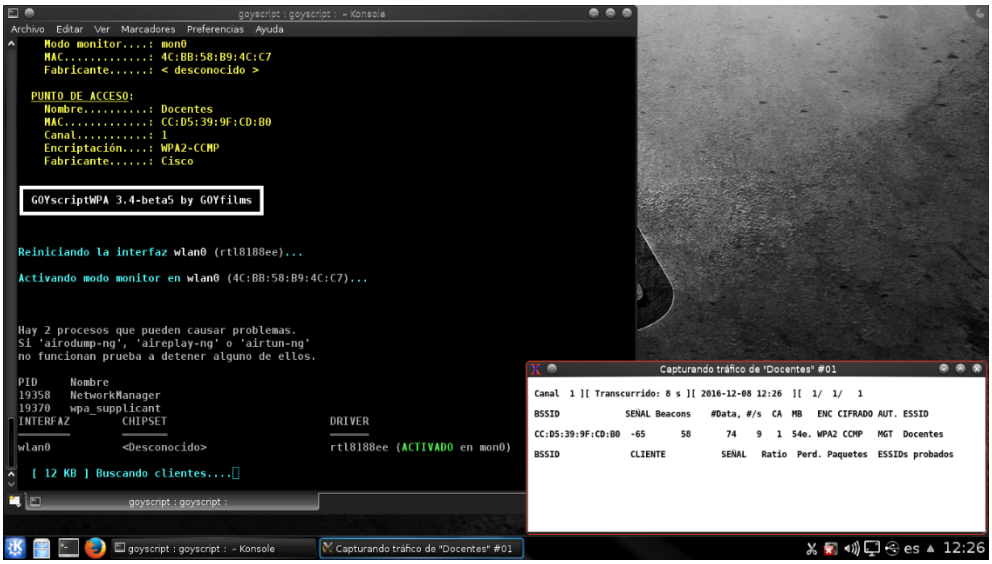


Figura 3. 4. *Resultados de ataque de fuerza bruta de la red inalámbrica.*

Elaborado por: Los Autores

3.5.Nivel de calidad servicio de la red inalámbrica.

Se ha tomado referencia los Mb/s asignados por los administradores de red que es de Estudiantes 30Mbps y Docentes 50Mbps por lo cual se procede a ser pruebas en cada facultad de ingeniería y CTE. El test de velocidad se realizará con SpeedTest que es una herramienta de análisis de velocidad de banda ancha, con servidores ubicados a nivel global, que permite a cualquiera probar su conexión a Internet.

Tabla 3.1. *Velocidad de descarga y carga a internet de la red de estudiantes con usuarios.*

Facultad	PING (Mili segundos)	Velocidad de Descarga (Megabit por segundo)	Velocidad de Carga (Megabit por segundo)
Ingeniería	13ms	5.56 Mbps	7.05 Mbps
Salud	14ms	6.86 Mbps	8.05 Mbps
Ciencias Políticas y Administrativas	14ms	5.88 Mbps	7.97 Mbps
Centro de Tecnología Educativa	19ms	11.43 Mbps	3.32 Mbps

Elaborado por: Los Autores

3.5.Centro de tecnologías educativa (CTE)

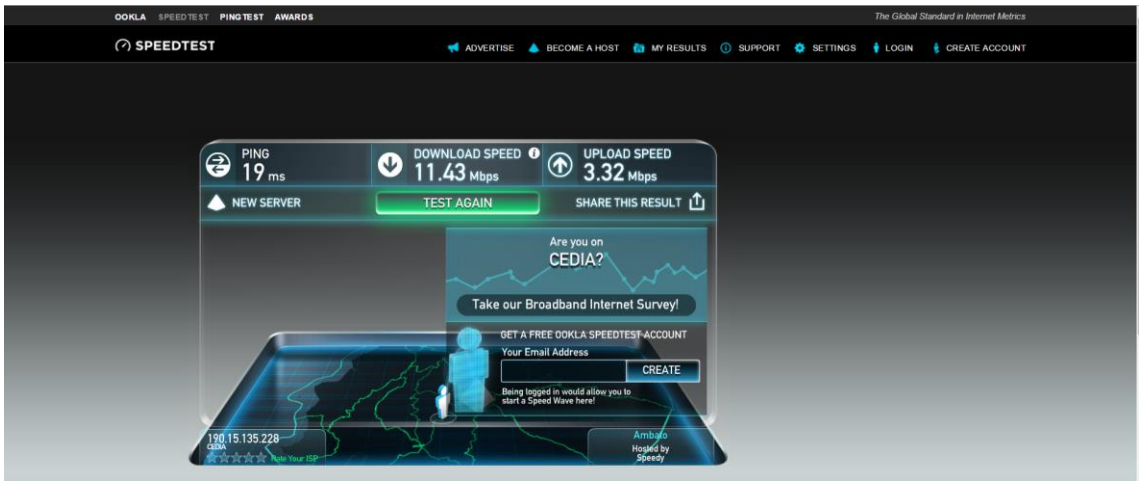


Figura 3. 5. *Análisis con la herramienta SpeedTest.*

Elaborado por: Los Autores

Tabla 3.2. *Velocidad de descarga y carga a internet de la red de estudiantes sin usuarios.*

Facultad	PING (Mili segundos)	Velocidad de Descarga (Megabit por segundo)	Velocidad de Carga (Megabit por segundo)
Ingeniería	14ms	8.98 Mbps	11.81 Mbps
Salud	15ms	9.03 Mbps	10.98 Mbps
Ciencias Políticas y Administrativas	19ms	9.08 Mbps	11.54 Mbps
Centro de Tecnología Educativa	20ms	15.51 Mbps	13.54 Mbps

Elaborado por: Los Autores

Tabla 3.3. *Velocidad de descarga y carga a internet de la red de docentes con usuarios.*

Facultad	PING (Mili segundos)	Velocidad de Descarga (Megabit por segundo)	Velocidad de Carga (Megabit por segundo)
Ingeniería	17ms	9.84 Mbps	5.75 Mbps
Salud	15ms	10.12 Mbps	6.21Mbps
Ciencias Políticas y Administrativas	19ms	8.84 Mbps	7.21 Mbps
Centro de Tecnología Educativa	18ms	9.21 Mbps	4.65 Mbps

Elaborado por: Los Autores

Tabla 3.4. *Velocidad de descarga y carga a internet de la red de docentes sin usuarios.*

Facultad	**PING (Mili segundos)**	**Velocidad de Descarga (Megabit por segundo)**	**Velocidad de Carga (Megabit por segundo)**
Ingeniería	18ms	10.28 Mbps	7.28 Mbps
Salud	19ms	12.01 Mbps	7.16 Mbps
Ciencias Políticas y Administrativas	18ms	10.58 Mbps	6.95 Mbps
Centro de Tecnología Educativa	18ms	11.09 Mbps	7.21 Mbps

Elaborado por: Los Autores

ANEXO 4: Comprobación de la hipótesis

RESULTADO DE SNIFFER DE ESTUDIANTES

Tabla 4.1. *Resumen de procesamiento de casos*

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Numero_Dispositivos_Estudisntes_A	5	71,4%	2	28,6%	7	100,0%
Numero_Dispositivos_Estudisntes_D	5	71,4%	2	28,6%	7	100,0%

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4.2. *Descriptivos*

			Estadístico
Numero_Dispositivos_Estudisntes_A	Media		867,60
	95% de intervalo de confianza para la media	Límite inferior	840,50
		Límite superior	894,70
	Media recortada al 5%		867,39
	Mediana		868,00
	Varianza		476,300
	Desviación estándar		21,824
	Mínimo		841
	Máximo		898
	Rango		57
	Rango intercuartil		40
	Asimetría		,304
	Curtosis		-,304
Numero_Dispositivos_Estudisntes_D	Media		468,20
	95% de intervalo de confianza para la media	Límite inferior	390,14
		Límite superior	546,26
	Media recortada al 5%		465,78
	Mediana		451,00
	Varianza		3952,700
	Desviación estándar		62,871
	Mínimo		412
	Máximo		568
	Rango		156
	Rango intercuartil		110
	Asimetría		1,217
	Curtosis		1,086

			Error estándar
Numero_Dispositivos_Estudisntes_A	Media		9,760
	95% de intervalo de confianza para la media	Límite inferior	
		Límite superior	
	Media recortada al 5%		
	Mediana		
	Varianza		
	Desviación estándar		
	Mínimo		
	Máximo		
	Rango		
	Rango intercuartil		
	Asimetría		,913
	Curtosis		2,000
Numero_Dispositivos_Estudisntes_D	Media		28,117
	95% de intervalo de confianza para la media	Límite inferior	
		Límite superior	
	Media recortada al 5%		
	Mediana		
	Varianza		
	Desviación estándar		
	Mínimo		
	Máximo		
	Rango		

	Rango intercuartil	
	Asimetría	,913
	Curtosis	2,000

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4.3. Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Numero_Dispositivos_Estudisntes_A	,133	5	,200*	,990	5	,981
Numero_Dispositivos_Estudisntes_D	,208	5	,200*	,898	5	,397

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

*. Esto es un límite inferior de la significación verdadera.
a. Corrección de significación de Lilliefors
Numero_Dispositivos_Estudisntes_A
Numero_Dispositivos_Estudisntes_A Gráfico de tallo y hojas

Frecuencia	Stem &	Hoja
1,00	8 .	4
4,00	8 .	5679

Ancho del tallo: 100
Cada hoja: 1 caso(s)

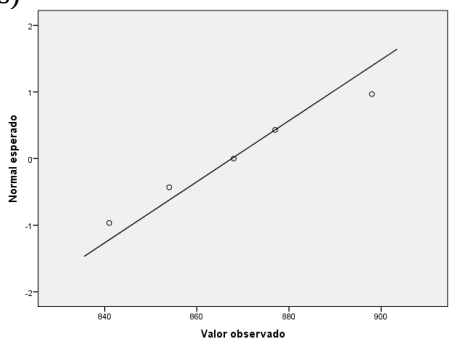


Figura 4.1.. *Q-Q normal de Número Dispositivos Estudiantes Antes*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

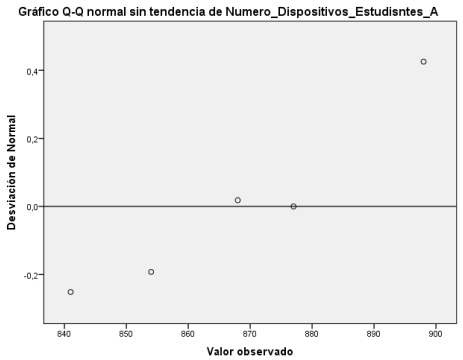


Figura 4.2. *Q-Q normal sin tendencias de Número dispositivos Estudiantes Antes*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

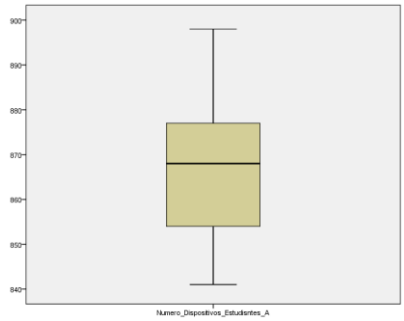


Figura 4.3. *Número dispositivos Estudiantes Antes*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Numero_Dispositivos_Estudisntes_D

Numero_Dispositivos_Estudisntes_D Gráfico de tallo y hojas

Frecuencia	Stem &	Hoja
2,00	4 .	12
2,00	4 .	58
,00	5 .	
1,00	5 .	6

Ancho del tallo: 100

Cada hoja: 1 caso(s)

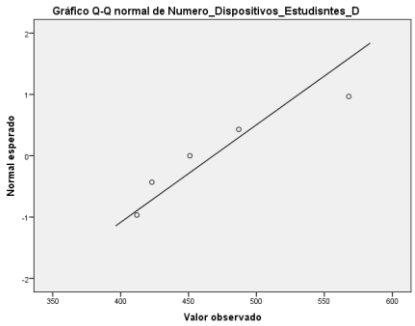


Figura 4.4. *Q-Q normal de Número Dispositivos Estudiantes Después*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

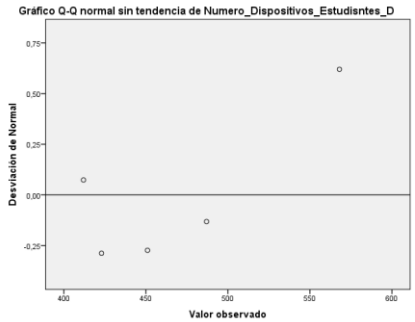


Figura 4.5. *Q-Q normal sin tendencias de Número Dispositivos Estudiantes Después*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

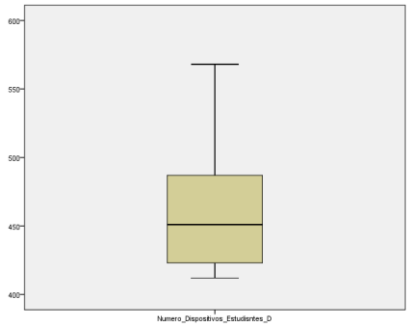


Figura 4.6. *Número dispositivos Estudiantes Después*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4.4. Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	Numero_Dispositivos_Estudisntes_A	867,60	5	21,824	9,760
	Numero_Dispositivos_Estudisntes_D	468,20	5	62,871	28,117

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4.5. Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	Numero_Dispositivos_Estudisntes_A & Numero_Dispositivos_Estudisntes_D	5	,792	,110

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4.6. Prueba de muestras emparejadas

		Diferencias emparejadas			
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior
Par 1	Numero_Dispositivos_Estudisntes_A - Numero_Dispositivos_Estudisntes_D	399,400	47,501	21,243	340,420

		Diferencias emparejadas 95% de intervalo de confianza de la diferencia Superior	t	gl	Sig. (bilateral)
Par 1	Numero_Dispositivos_Estudisntes_A - Numero_Dispositivos_Estudisntes_D	458,380	18,802	4	,000

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

RESULTADO SNIFFER DOCENTES

Tabla 4.7. Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Numero_Dispositivos_Docentes_A	5	100,0%	0	0,0%	5	100,0%
Numero_Dispositivos_Docentes_D	5	100,0%	0	0,0%	5	100,0%

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4.8.*Descriptivos*

			Estadístico
Numero_Dispositivos_Docentes_A	Media		522,40
	95% de intervalo de confianza para la media	Límite inferior	469,89
		Límite superior	574,91
	Media recortada al 5%		520,78
	Mediana		517,00
	Varianza		1788,300
	Desviación estándar		42,288
	Mínimo		482
	Máximo		592
	Rango		110
	Rango intercuartil		69
	Asimetría		1,403
	Curtosis		2,376
Numero_Dispositivos_Docentes_D	Media		285,80
	95% de intervalo de confianza para la media	Límite inferior	233,86
		Límite superior	337,74
	Media recortada al 5%		285,00
	Mediana		287,00
	Varianza		1749,700
	Desviación estándar		41,829
	Mínimo		238
	Máximo		348
	Rango		110
	Rango intercuartil		74
	Asimetría		,647
	Curtosis		,460

			Error estándar
Numero_Dispositivos_Docentes_A	Media		18,912
	95% de intervalo de confianza para la media	Límite inferior	
		Límite superior	
	Media recortada al 5%		
	Mediana		
	Varianza		
	Desviación estándar		
	Mínimo		
	Máximo		
	Rango		
	Rango intercuartil		
	Asimetría		,913
	Curtosis		2,000
Numero_Dispositivos_Docentes_D	Media		18,707
	95% de intervalo de confianza para la media	Límite inferior	
		Límite superior	
	Media recortada al 5%		
	Mediana		
	Varianza		
	Desviación estándar		
	Mínimo		
	Máximo		
	Rango		
	Rango intercuartil		
	Asimetría		,913

Curtosis	2,000

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4. 9. *Pruebas de normalidad*

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Numero_Dispositivos_Docentes_A	,285	5	,200*	,886	5	,339
Numero_Dispositivos_Docentes_D	,194	5	,200*	,967	5	,858

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Numero_Dispositivos_Docentes_A

Numero_Dispositivos_Docentes_A Gráfico de tallo y hojas

```
 Frecuencia   Stem &  Hoja
    2,00       4 .  89
    2,00       5 .  12
    1,00 Extremos    (>=592)
 Ancho del tallo:      100
 Cada hoja:       1 caso(s)
```

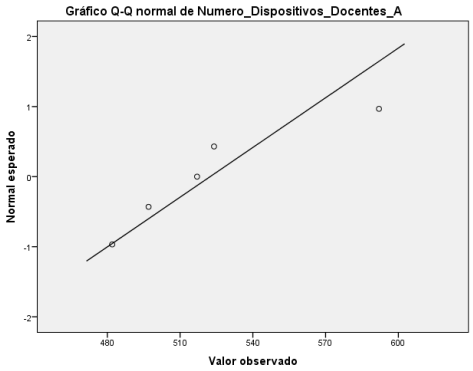


Figura 4.7. *Q-Q normal de Número Dispositivos Docentes Antes*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

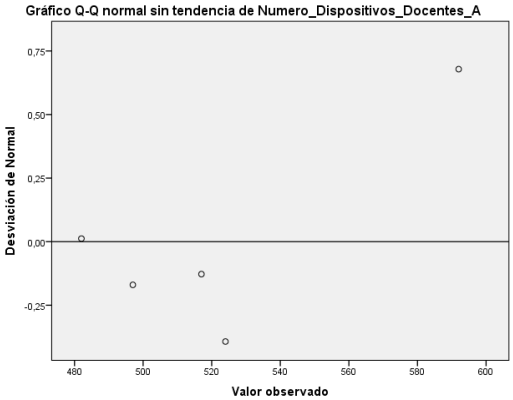


Figura 4.8. *Q-Q normal sin tendencias de Número Dispositivos Docentes Antes*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

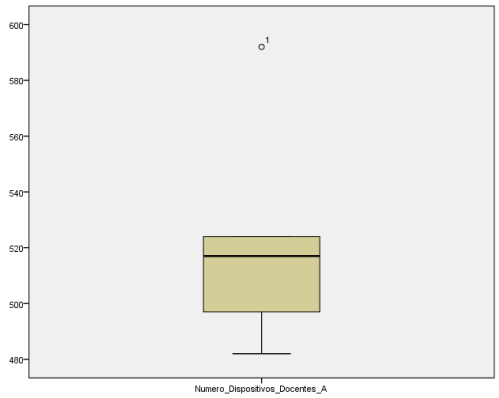


Figura 4.9. *Número Dispositivos Docentes Antes*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Numero_Dispositivos_Docentes_D

Numero_Dispositivos_Docentes_D Gráfico de tallo y hojas

Frecuencia	Stem &	Hoja
1,00	2 .	3
3,00	2 .	589
1,00	3 .	4

Ancho del tallo: 100

Cada hoja: 1 caso(s)

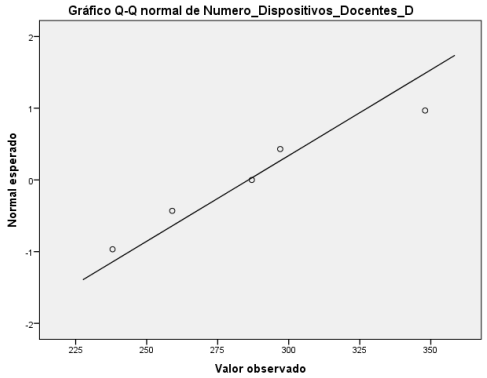


Figura 4.10. *Q-Q normal de Número Dispositivos Docentes Después*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

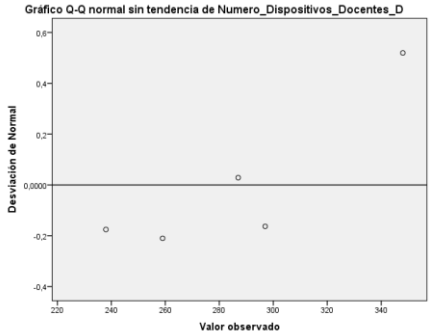


Figura 4.11. *Q-Q normal sin tendencias de Número Dispositivos Docentes Después*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

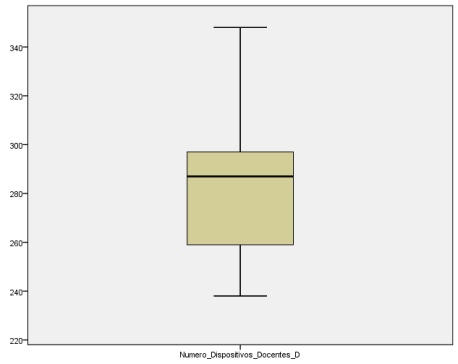


Figura 4. 12. *Número Dispositivos Docentes Después*

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4.10. *Estadísticas de muestras emparejadas*

		Media	N	Desviación estándar	Media de error estándar
Par 1	Numero_Dispositivos_Docentes_A	522,40	5	42,288	18,912
	Numero_Dispositivos_Docentes_D	285,80	5	41,829	18,707

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	Numero_Dispositivos_Docentes_A & Numero_Dispositivos_Docentes_D	5	,553	,333

Prueba de muestras emparejadas

		Diferencias emparejadas			
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior
Par 1	Numero_Dispositivos_Docentes_A - Numero_Dispositivos_Docentes_D	236,600	39,759	17,781	187,232

Prueba de muestras emparejadas

		Diferencias emparejadas 95% de intervalo de confianza de la diferencia Superior	t	gl	Sig. (bilateral)
Par 1	Numero_Dispositivos_Docentes_A - Numero_Dispositivos_Docentes_D	285,968	13,306	4	,000

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

NIVEL DE VULNERABILIDADES SPOOFING

Tabla 4.11. Descriptivos

			Estadístico
Nivel_Vulnerabilidad_Antes	Media		6,80
	95% de intervalo de confianza para la media	Límite inferior	4,41
		Límite superior	9,19
	Media recortada al 5%		6,83
	Mediana		7,00
	Varianza		3,700
	Desviación estándar		1,924
	Mínimo		4
	Máximo		9
	Rango		5
	Rango intercuartil		4
	Asimetría		-,590
	Curtosis		-,022
Nivel_Vulnerabilidad_Despues	Media		3,80
	95% de intervalo de confianza para la media	Límite inferior	2,76
		Límite superior	4,84
	Media recortada al 5%		3,78
	Mediana		4,00
	Varianza		,700
	Desviación estándar		,837
	Mínimo		3
	Máximo		5
	Rango		2
	Rango intercuartil		2
	Asimetría		,512
	Curtosis		-,612

			Error estándar
Nivel_Vulnerabilidad_Antes	Media		,860
	95% de intervalo de confianza para la media	Límite inferior	
		Límite superior	
	Media recortada al 5%		
	Mediana		
	Varianza		
	Desviación estándar		
	Mínimo		
	Máximo		
	Rango		
	Rango intercuartil		
	Asimetría		,913
	Curtosis		2,000
Nivel_Vulnerabilidad_Despues	Media		,374
	95% de intervalo de confianza para la media	Límite inferior	
		Límite superior	
	Media recortada al 5%		
	Mediana		
	Varianza		
	Desviación estándar		
	Mínimo		
	Máximo		
	Rango		
	Rango intercuartil		
	Asimetría		,913
	Curtosis		2,000

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

Tabla 4.12. Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Nivel_Vulnerabilidad_Antes	,141	5	,200*	,979	5	,928
Nivel_Vulnerabilidad_Despues	,231	5	,200*	,881	5	,314

Fuente: Herramienta IBM SPSS Statistics versión 24.0.0.0

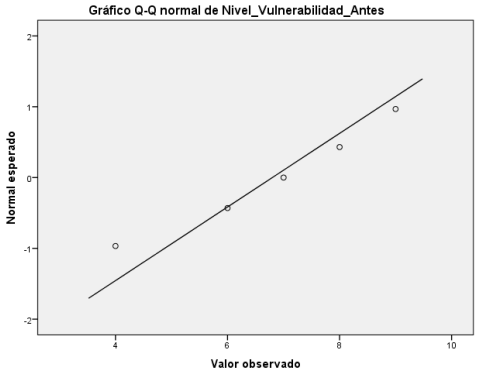
*. Esto es un límite inferior de la significación verdadera.
a. Corrección de significación de Lilliefors

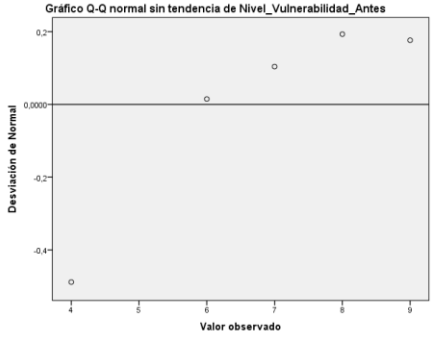
Nivel_Vulnerabilidad_Antes

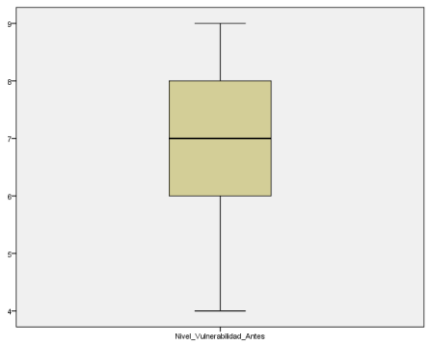
Nivel_Vulnerabilidad_Antes Gráfico de tallo y hojas

Frecuencia	Stem &	Hoja
1,00	0 .	4
4,00	0 .	6789

Ancho del tallo: 10
Cada hoja: 1 caso(s)





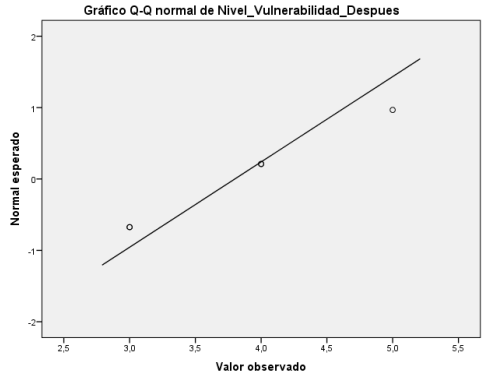


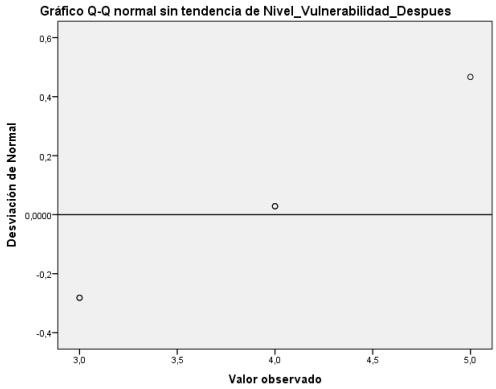
Nivel_Vulnerabilidad_Despues

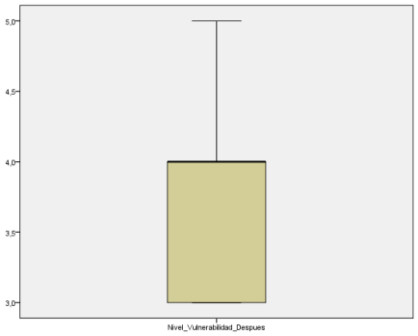
Nivel_Vulnerabilidad_Despues Gráfico de tallo y hojas

Frecuencia	Stem &	Hoja
2,00	3 .	00
2,00	4 .	00
1,00	5 .	0

Ancho del tallo: 1
Cada hoja: 1 caso(s)







Prueba T

Notas

Salida creada		13-FEB-2017 01:14:25
Comentarios		
Entrada	Datos	D:\UNACH\Decimo\Proyecto de Tesis\Tesis\Estadistica\Nivel de vulnerabilidades.sav
	Conjunto de datos activo	ConjuntoDatos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	5
Manejo de valores perdidos	Definición de perdidos	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.

Sintaxis		T-TEST PAIRS=Nivel_Vulnerabilidad_Antes WITH Nivel_Vulnerabilidad_Despues (PAIRED) /CRITERIA=CI(.9500) /MISSING=ANALYSIS.
Recursos	Tiempo de procesador	00:00:00,02
	Tiempo transcurrido	00:00:00,02

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	Nivel_Vulnerabilidad_Antes	6,80	5	1,924	,860
	Nivel_Vulnerabilidad_Despues	3,80	5	,837	,374

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	Nivel_Vulnerabilidad_Antes & Nivel_Vulnerabilidad_Despues	5	-,031	,960

Prueba de muestras emparejadas

		Diferencias emparejadas			
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior
Par 1	Nivel_Vulnerabilidad_Antes - Nivel_Vulnerabilidad_Despues	3,000	2,121	,949	,366

Prueba de muestras emparejadas

		Diferencias emparejadas 95% de intervalo de confianza de la diferencia Superior	t	gl	Sig. (bilateral)
Par 1	Nivel_Vulnerabilidad_Antes - Nivel_Vulnerabilidad_Despues	5,634	3,162	4	,034

CALIDAD DE SERVICIO

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Nivel_Servicio_Antes	5	100,0%	0	0,0%	5	100,0%
Nivel_Servicio_Despues	5	100,0%	0	0,0%	5	100,0%

Descriptivos

			Estadístico	Error estándar
Nivel_Servicio_Antes	Media		6,000	,7071
	95% de intervalo de confianza para la media	Límite inferior	4,037	
		Límite superior	7,963	
	Media recortada al 5%		6,056	
	Mediana		6,500	
	Varianza		2,500	
	Desviación estándar		1,5811	
	Mínimo		3,5	
	Máximo		7,5	
	Rango		4,0	
	Rango intercuartil		2,8	
	Asimetría		-1,186	,913
	Curtosis		1,050	2,000
Nivel_Servicio_Despues	Media		8,680	,1319
	95% de intervalo de confianza para la media	Límite inferior	8,314	
		Límite superior	9,046	
	Media recortada al 5%		8,678	
	Mediana		8,500	
	Varianza		,087	
	Desviación estándar		,2950	
	Mínimo		8,4	
	Máximo		9,0	
	Rango		,6	
	Rango intercuartil		,6	
	Asimetría		,518	,913
	Curtosis		-3,175	2,000

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Nivel_Servicio_Antes	,224	5	,200*	,912	5	,482
Nivel_Servicio_Despues	,329	5	,081	,775	5	,050

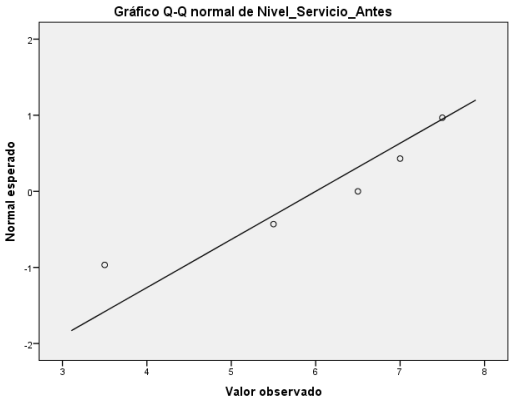
*. Esto es un límite inferior de la significación verdadera.

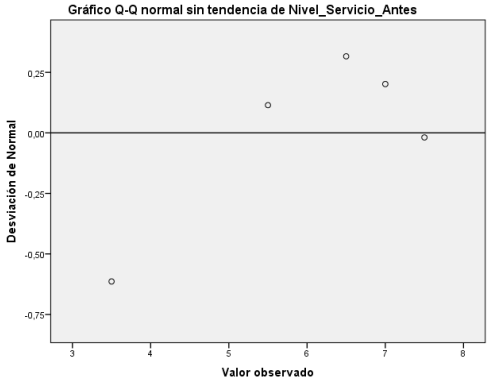
a. Corrección de significación de Lilliefors

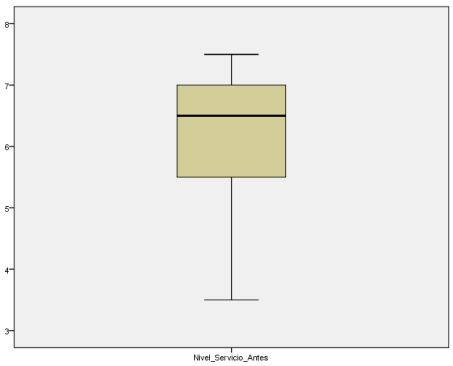
Nivel_Servicio_Antes

Nivel_Servicio_Antes Gráfico de tallo y hojas

```
 Frecuencia   Stem &  Hoja
    1,00       0 .  3
    4,00       0 .  5677
 Ancho del tallo:     10,0
 Cada hoja:       1 caso(s)
```







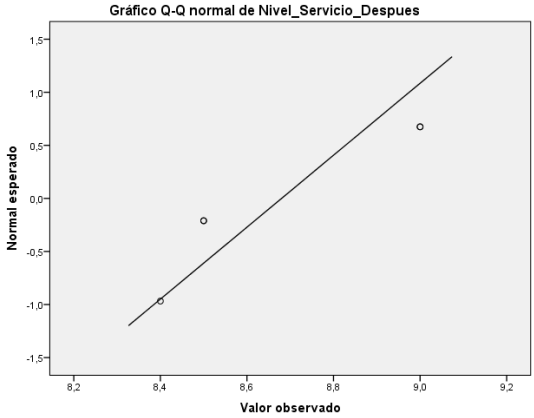
Nivel_Servicio_Despues

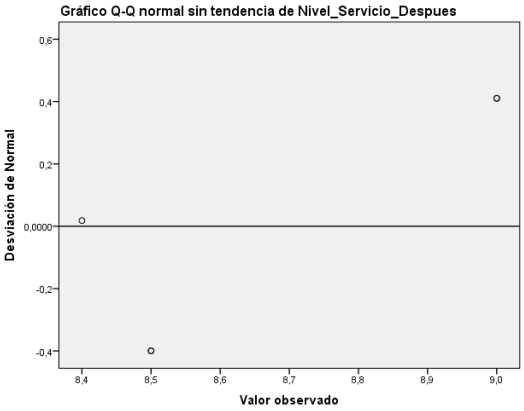
Nivel_Servicio_Despues Gráfico de tallo y hojas

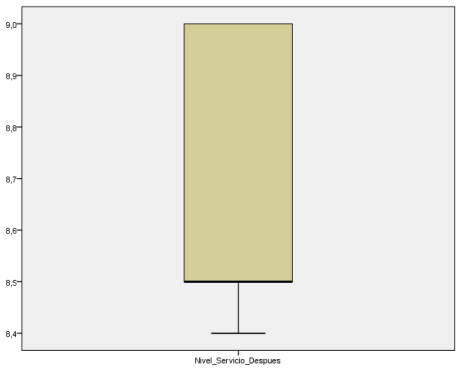
Frecuencia	Stem &	Hoja
1,00	8 .	4
2,00	8 .	55
2,00	9 .	00

Ancho del tallo: 1,0

Cada hoja: 1 caso(s)







Prueba T

Notas

Salida creada		13-FEB-2017 02:55:20
Comentarios		
Entrada	Conjunto de datos activo	ConjuntoDatos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	5
Manejo de valores perdidos	Definición de perdidos	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.

Sintaxis		T-TEST PAIRS=Nivel_Servicio_Antes WITH Nivel_Servicio_Despues (PAIRED) /CRITERIA=CI(.9500) /MISSING=ANALYSIS.
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,07

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	Nivel_Servicio_Antes	6,000	5	1,5811	,7071
	Nivel_Servicio_Despues	8,680	5	,2950	,1319

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	Nivel_Servicio_Antes & Nivel_Servicio_Despues	5	,670	,216

Prueba de muestras emparejadas

		Diferencias emparejadas			
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior
Par 1	Nivel_Servicio_Antes - Nivel_Servicio_Despues	-2,6800	1,4007	,6264	-4,4192

Prueba de muestras emparejadas

		Diferencias emparejadas 95% de intervalo de confianza de la diferencia Superior	t	gl	Sig. (bilateral)
Par 1	Nivel_Servicio_Antes - Nivel_Servicio_Despues	-,9408	-4,278	4	,013

NIVEL DE POLÍTICAS DE SEGURIDAD

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Nivel_Policas_Antes	6	85,7%	1	14,3%	7	100,0%
Nivel_Policas_Despues	6	85,7%	1	14,3%	7	100,0%

Descriptivos

			Estadístico	Error estándar
Nivel_Policas_Antes	Media		6,4167	,87003
	95% de intervalo de confianza para la media	Límite inferior	4,1802	
		Límite superior	8,6531	
	Media recortada al 5%		6,3796	
	Mediana		5,7500	
	Varianza		4,542	
	Desviación estándar		2,13112	
	Mínimo		4,50	
	Máximo		9,00	
	Rango		4,50	
	Rango intercuartil		4,50	
	Asimetría		,544	,845
	Curtosis		-2,174	1,741
Nivel_Policas_Despues	Media		8,9167	,15366
	95% de intervalo de confianza para la media	Límite inferior	8,5217	
		Límite superior	9,3117	
	Media recortada al 5%		8,9074	
	Mediana		9,0000	
	Varianza		,142	
	Desviación estándar		,37639	
	Mínimo		8,50	
	Máximo		9,50	
	Rango		1,00	
	Rango intercuartil		,63	
	Asimetría		,313	,845
	Curtosis		-,104	1,741

Pruebas de normalidad

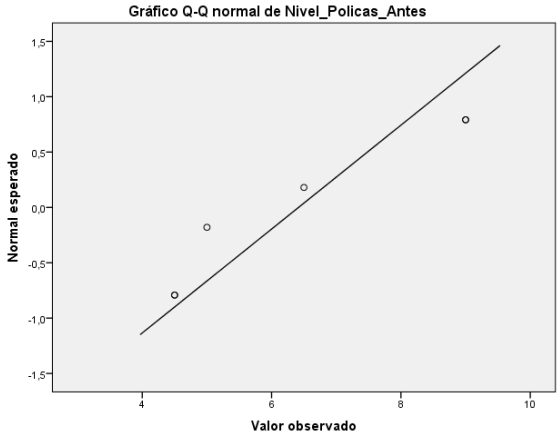
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Nivel_Policas_Antes	,247	6	,200*	,810	6	,072
Nivel_Policas_Despues	,254	6	,200*	,866	6	,212

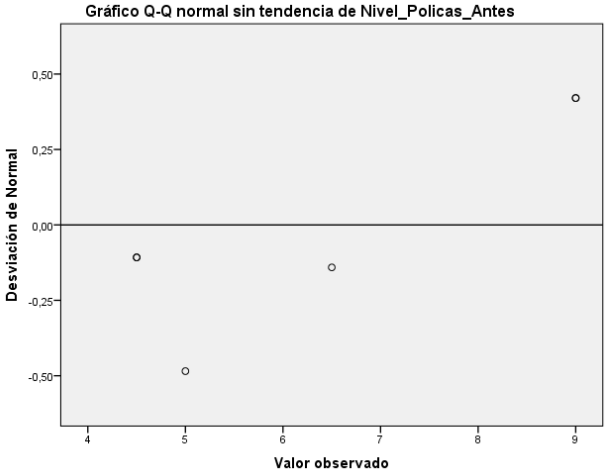
*. Esto es un límite inferior de la significación verdadera.
a. Corrección de significación de Lilliefors

Nivel_Policas_Antes

Nivel_Policas_Antes Gráfico de tallo y hojas

```
 Frecuencia   Stem &  Hoja
    2,00        0 .  44
    4,00        0 .  5699
 Ancho del tallo:     10,00
 Cada hoja:        1 caso(s)
```





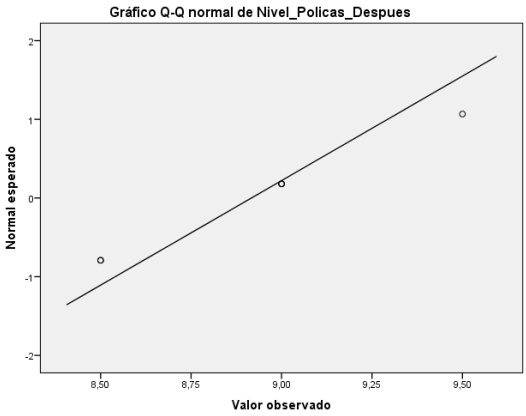
Nivel_Policas_Despues

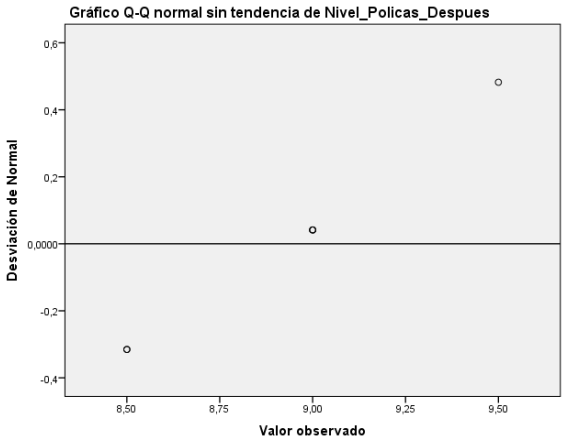
Nivel_Policas_Despues Gráfico de tallo y hojas

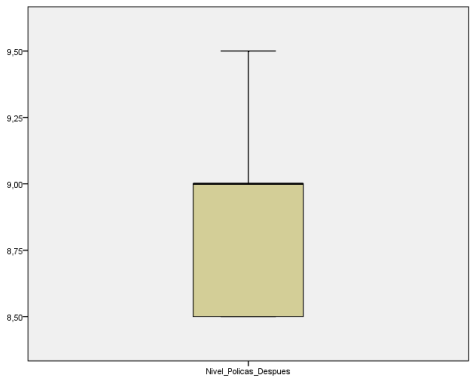
Frecuencia	Stem &	Hoja
,00	8 .	
2,00	8 .	55
3,00	9 .	000
1,00	9 .	5

Ancho del tallo: 1,00

Cada hoja: 1 caso(s)







Prueba T

Notas

Salida creada		13-FEB-2017 11:37:38
Comentarios		
Entrada	Datos	D:\UNACH\Decimo\Proyecto de Tesis\Tesis\Estadistica\Politicas.sav
	Conjunto de datos activo	ConjuntoDatos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	7
Manejo de valores perdidos	Definición de perdidos	Los valores perdidos definidos por el usuario se trata como valores perdidos.

	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST PAIRS=Nivel_Policas_Antes WITH Nivel_Policas_Despues (PAIRED) /CRITERIA=CI(.9500) /MISSING=ANALYSIS.
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,01

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	Nivel_Policas_Antes	6,4167	6	2,13112	,87003
	Nivel_Policas_Despues	8,9167	6	,37639	,15366

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	Nivel_Policas_Antes & Nivel_Policas_Despues	6	,177	,738

Prueba de muestras emparejadas

		Diferencias emparejadas			
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior
Par 1	Nivel_Policas_Antes - Nivel_Policas_Despues	-2,50000	2,09762	,85635	-4,70131

Prueba de muestras emparejadas

		Diferencias emparejadas 95% de intervalo de confianza de la diferencia Superior	t	gl	Sig. (bilateral)
Par 1	Nivel_Policas_Antes - Nivel_Policas_Despues	-,29869	-2,919	5	,033

ACTA DE ENTREGA RECEPCIÓN

MANUAL DE POLÍTICAS DE SEGURIDAD

DE LA INFORMACIÓN

En la ciudad Riobamba, a los 21 días del mes de Julio del 2017, los señores estudiantes Carlos Fernando Martínez Cáceres y Olga Mercedes Oñate Haro realizan la entrega del manual de políticas de seguridad de la información, después de realizar el proyecto de investigación con el título: **"MEJORAS EN LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO APLICANDO HACKING ÉTICO"** al Ingeniero Javier Haro Administrador de la red de la Universidad Nacional de Chimborazo, con el objeto de dejar constancia en la Entrega Recepción de conformidad del trabajo realizado.

ENTREGUE CONFORME
Carlos Martínez Cáceres

ENTREGUE CONFORME
Olga Mercedes Oñate

RECIBÍ CONFORME
Ing. Javier Haro