INNOVA Research Journal 2018, Vol 3, No. 2.1, 122-133
ISSN 2477-9024

Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador

Diagnosis of vulnerabilities in wireless networks at Ecuador

Chuquitarco Mario, Romero Mónica
Universidad Internacional SEK
Autor para correspondencia: mchuquitarcol@gmail.com.ec; monica.romero@uisek.edu.ec
Fecha de recepción: 15 de diciembre 2017 - Fecha de aceptación: 26 de febrero de 2018

Resúmen: El objetivo de la investigación fue realizar un diagnóstico de vulnerabilidades en redes inalámbricas en el Ecuador, con el fin de ayudar y proporcionar a los profesionales de tecnologías de información un recurso para mejorar la seguridad en redes wireless en empresas públicas o privadas. El estudio se realizó en la Universidad Internacional SEK con la colaboración de La Casa del Cable S.A y Bigexpert Cía. Ltda. Quito Ecuador. Se utilizó el método descriptivo, analítico-sintético acompañado de técnicas específicamente entrevistas y encuestas aplicadas a los profesionales que ayudaron en el proceso de estudio, los resultados de esta investigación reflejan que existe un alto interés con respecto a la seguridad en redes inalámbricas, por cuanto muchas empresas buscan proporcionar diferentes formas de acceso a los datos mediante el uso de nuevas tecnologías, siempre y cuando estas no afecten a la integridad, confidencialidad y disponibilidad de la información.
Palabras claves: redes inalámbricas, tecnología de la información y comunicación, seguridades.

Abstract: A The objective of the research is to diagnose vulnerabilities in wireless networks in Ecuador, in order to help and provide IT professionals with a resource for the improvement of security in wireless networks in public or private companies. This study will be carried out at the SEK International University with the collaboration of La Casa del Cable S.A and Bigexpert Cía. Ltda. Quito Ecuador. The descriptive and synthetic-analytical method, accompanied by techniques specifically interviews and surveys applied to IT professionals helped in the study process, the results of this investigation reflect that there is a high interest regarding security in wireless networks, as Many companies seek to provide different ways of accessing data through the use of new technologies, as long as this does not affect the integrity, confidentiality and availability of information.
Keywords: wireless network, information and comunications technology, security.

Introducción

La evolución de la tecnología de la información y comunicación (TIC), ha hecho que las personas tengan mayor accesibilidad a los sistemas informáticos, estos avances tecnológicos permiten que las personas tengan a su alcance cualquier tipo de información, pero todo esto ha causado que también crezca el riesgo vinculado con la seguridad.

La seguridad informática apareció debido a la necesidad de dar soporte a esas nuevas tecnologías, la infraestructura de red al ser requerida por las empresas para permitir el acceso a la información y dar movilidad a las personas, necesitan ser tratadas de manera primordial, por cuanto deben cuidar la parte vital de toda empresa, como son sus datos.

El uso de redes inalámbricas gana cada vez más usuarios y con ello el uso de herramientas y recursos tecnológicos, pero también aparecen nuevas vulnerabilidades y amenazas (García Arano, 2010). La ciberdelincuencia en el Ecuador, así como en el resto del mundo va en aumento en los últimos años (Lahora.com.ec, 2010).

Los adversarios desarrollan nuevas amenazas, debido al crecimiento del tráfico de Internet, logrando con ello que la expansión de la superficie de ataque crezca. A medida que eso sucede, los riesgos para las empresas son cada vez mayores, más de un tercio de las organizaciones que han sufrido un ataque perdió el 20 % de sus ingresos o más (Cisco, 2017).

Figura 1. Porcentaje de ingresos perdidos como resultado de un ataque
Fuente: CISCO Informe anual sobre ciberseguridad 2017

Las exigencias de seguridad de la información a creciendo en las últimas décadas motivadas principalmente por una mayor exposición de los sistemas. Antes del uso extendido de equipos para el proceso de datos, la seguridad de la información se garantizaba por medios físicos y administrativos, en la actualidad, con entornos distribuidos y descentralizados, se hace indispensable la transmisión constante de datos a través de redes públicas (Paz,

Casanova, & Gari, 2009).

El acceso a la red inalámbrica en adelante WLAN sin usar cables, hace que estas tengan problemas en cuanto a seguridad, al utilizar el aire para la transmisión de información cualquier equipo que este dentro de la cobertura de la red inalámbrica podría acceder a ella. Lo preocupante de la situación expuesta es que los administradores de la red no se dan cuenta de los riesgos que implica la mala configuración de los dispositivos de acceso inalámbrico (J Lopez., 2007).

El diagnostico de vulnerabilidades exige la identificación anticipada de riesgos, para actuar de manera preventiva y con responsabilidad, las redes inalámbricas creadas por la necesidad de proveer acceso a la información mediante dispositivos portátiles, atrajo problemas hacia el medio de transmisión, por cuanto los intrusos pueden acceder a la red libremente dando una posibilidad virtual de no ser detectados.

Es por ello, la importancia de tener comunicaciones seguras (Suárez & Resumen, 2012).La falta de un diagnóstico que permita valorar las diferentes vulnerabilidades, hace que las redes wireless sean propensas a ataques. Cualquier persona, por estar bajo la influencia de dos o más redes y a 100 metros o menos de un punto de acceso, podría conectarse a la red inalámbricas que no es la suya (Aguirre, Ordóñez, & Ureta, 2005).

¿Qué es lo que hace que las redes inalámbricas sean más vulnerables que las redes de cable?

La respuesta es sencilla: desconocimiento de las herramientas de seguridad disponibles para redes inalámbricas, lo que causa que muchas personas piensen que es más fácil "pinchar" un cable que el aire. Hoy en día existen las herramientas de seguridad, funciones y protocolos adecuados para proporcionar una protección a las LAN's inalámbricas (Saavedra Rios & informática, 2012).

La investigación de vulnerabilidades ayuda a identificar y corregir debilidades en las redes o sistemas, a proteger de ataques de intrusos y obtener información que ayude a prevenir problemas de seguridad protegiendo de esa manera los activos de una organización y/o usuario (Machado, 2012).

La seguridad mediante la identificación de vulnerabilidades a las que se encuentre expuesta la red permite mantener la información y/o recursos a salvo de eventos de hacking; logrando con ello que dichos recursos tengan la confidencialidad, autenticidad, integridad y disponibilidad en todo momento (Pazmiño Caluña, 2011).

Metodos

Diseño de la investigación

El método usado en la investigación es descriptivo, por la manera de representar los datos y las características de la población, la cual permite conocer la situación actual de las vulnerabilidades en el país.

Es de carácter analítico – sintético, por cuanto el estudio necesita un análisis por separado de cada una de las vulnerabilidades detectadas o que más impacto causan, para luego mediante el método sintético buscar factores que nos permita relacionar cada una de ellas para su posterior análisis global.

Nivel de estudio

Exploratorio: Por cuanto se busca esclarecer un diagnóstico de vulnerabilidades al momento de valorar los niveles de seguridad en redes inalámbricas. Para lo cual se buscará información bibliográfica que permita conocer los resultados de estudios similares

Experimental: El diagnóstico de vulnerabilidades en redes inalámbricas, será efectuado por parte de expertos para evaluar los resultados obtenidos en campo.

Modalidad de investigación

La metodología de investigación propuesta es: Experimental y documental.

Participantes

Para esta investigación la población objeto de estudio es de 16 empresas cada una de ellas representada por una persona vinculada a TI, estas a su vez distribuidas en dos grupos específicos:

Profesionales TI (personas encargadas en las empresas del departamento de TI) un total de 15 personas.

Jefe de Producto (Networking y Telefonía, La Casa del Cable S.A-Alcatel-Lucent Enterprise) una persona

De la muestra escogida, todos los profesionales que participarón en el estudio poseen título de tercer nivel.

Población y muestra

La población será escogida de la cartera de clientes de la empresa Ingeniería y Soluciones Tecnológicas Bigexpert Cía. Ltda, para la elaboración de las encuestas, con respecto a la entrevista se apoyará en los representantes de proveedores Alcatel-Lucent Enterprise/Casa de Cable S.A. La manera de escoger la población tiene su base en un muestreo por conveniencia, debido a la accesibilidad del investigador.

Selección instrumentos investigación

Como técnicas de la investigación se ha escogido la observación directa, la cual permite la recolección de información en sitio respecto a los diferentes estándares, configuraciones y seguridades de los diferentes equipos wireless (Educar & 2011, 2011).

Se empleará las metodologías cuantitativas para emitir criterios en términos numéricos que se evidencian en porcentajes para optimizar su comprensión que influyen en el proceso de implementación de dicha tecnología.

Validez y confiabilidad de instrumentos

Para comprobar la validez de los instrumentos según (P Baptista, Hernandez, & Juan Hernandez, 2010), "El cuestionario debe tener una correspondencia directa con los objetivos de la investigación. Es decir, las interrogantes consultarán solo aquello que se pretende conocer o medir". Para ello se realizará una prueba piloto a especialistas que tengan la experiencia o características similares a los entrevistados, con el afán de corregir alguna falla y elaborar el documento definitivo. Además, Hernández, Fernández y Baptista, (Hernández Sampieri, 2003) afirman que la consistencia de resultados al aplicar los instrumentos refleja la confiabilidad de los mismos, si las entrevistas y encuestas generadas no generan discrepancia se puede asumir que los instrumentos son válidos y confiables.

Procesamiento de datos

Se describirá las operaciones de clasificación, registro, tabulación y codificación a las que serán sometidos los datos que se obtengan. El programa informático Excel será el medio utilizado para el análisis de los datos obtenidos, vaciado de los resultados, diseño de tablas y las representaciones gráficas.

Resultados

Los resultados observados reflejan datos significativos, en la que se puede evidenciar los factores por las que el personal de TI implementa seguridades dentro de la organización.

Tabla 1: Factores que impulsan a la implantación de seguridades dentro de una organización

FACTORES
Nivel de control sobre usuarios deseado
Mejorar utilización de recursos corporativos
Mejora de procesos: evitar controles manuales
Brindar mayor comodidad a usuarios, si la implementación apunta a unificar varios sistemas de seguridad distintos

(Ej: control de acceso físico con acceso a la red informática)
Normativas tanto internas como externas, tales como disposiciones gubernamentales
Reducción de costos
Cumplimiento de estándares de calidad de organizaciones (ej: ISO)
Temor ante ataques y robo de información

Fuente: Investigador

Con respecto al impacto que tendrá el uso de las tecnologías inalámbricas en las organizaciones, se puede evidenciar que la movilidad es la tendencia para las empresas que buscan mayor productividad de sus colaboradores, pero ello conlleva a generar mayor congestión en la red inalámbrica, lo que se adiciona en puntos de vulnerabilidad.

Tabla 2: Impacto del uso de tecnologías inalámbricas en las organizaciones.

Uso de las tecnologías inalámbricas en las organizaciones	
Movilidad de usuarios	x
Nuevas tecnologías en movilidad	x
Incremento de sitios para acceso a la información	
La necesidad de contar con comunicaciones unificadas	x
Incremento de productividad en la empresa (colaboradores)	x

Fuente: Investigador

Los servicios y aplicaciones que más riesgos representan para la seguridad en la Infraestructura de TI, como parte de la entrevista; permitió evidenciar que el factor humano y los dispositivos móviles son los principales riegos, sin embargo, esto no ha impulsado a establecer un estudio sobre las vulnerabilidades enfocadas al Ecuador a diferencia con otros países.

Tabla 3: Servicios, aplicaciones, que más riesgo representan para la seguridad Infraestructura TI

Servicios/Aplicaciones	**Porcentaje**
Dispositivos móviles	20%

Datos en la nube pública	8%
Infraestructura de la nube	5%
Comportamiento del usuario (por ejemplo, hacer clic en enlaces maliciosos en el correo electrónico o los sitios web)	25%
Datos de la organización	2%
Centros de datos/Servidores	10%
Infraestructura de red	15%
Aplicaciones noviles	5%
Sistemas operativos (Windows 7, Windows 10, MacOS, etc)	10%

Fuente: Investigador

Las empresas fabricantes de tecnología dividen su mercado por áreas, por tal razón, los resultados obtenidos referente a si poseen estudios de vulnerabilidades por sector; reflejan que el área Financiera y de Comunicaciones son los más propensos a ataques. Como parte de la entrevista conocer cuáles son los ataques que más afectan a las redes inalámbricas, formo parte de esta, permitiendo establecer 4 formas de ataques que más impacto causan a la infraestructura de TI.

Tabla 4: Estudio de vulnerabilidades por sector

Sectores	Porcentaje
Educación (instituciones de educación superior)	10%
Servicios Financieros: banca, seguro	20%
Gobierno	20%
Atención médica	5%
Fabricación: no relacionada con computadoras	5%
Industria farmacéutica	7.5%
Sector minorista	7.5%
Telecomunicaciones	20%
Transporte	2%
Servicios públicos/energía	3%

Fuente: Investigador

Tabla 5: Ataques que más afectan a las redes inalámbricas en el Ecuador

Tipos de ataques	**Porcentaje**
Malware	35%
Puntos de acceso falsos	15%
Negacion de servicio	25%
Man in the Middle	25%

Fuente: Investigador

El objetivo del personal de TI es precautelar la tecnología dentro de toda empresa, pero los especialistas en muchos de los casos tienen limitaciones, lo que llevo a la siguiente pregunta; cuáles son los principales obstáculos que Alcatel-Lucent Enterprise ha encontrado al pretender implementar soluciones de seguridad, obteniendo como factor principal las restricciones de presupuesto con un 20% y con otro 20% a que la seguridad no es una prioridad de nivel ejecutivo.

Tabla 6: Principales obstáculos para implementar soluciones de seguridad

Principales obstáculos para la implantación de seguridades	Porcentaje
Restricciones de presupuesto	20%
Problemas de compatibilidad	5%
Requisitos de certificación	5%
Falta de personal capacitado	2%
Prioridades contrapuestas	10%
Carga de trabajo actual muy pesada	0%
Resistencia a comprar hasta que no se compruebe el ataque	15%
Cultura/actitud de la organización	15%
La organización no es un objetivo de gran valor para los atacantes	8%
La seguridad no es una prioridad de nivel ejecutivo	20%

Fuente: Investigador

Como parte de la investigación y de la metodología a utilizar en la obtención de resultados se procedió a encuestar al personal de TI de las empresas, los mismos que muestra un conocimiento sobre los procedimientos de seguridad para enfrentar los desafíos de seguridad con un 60 % pero contrarrestado por un 40% que no conoce dichos procedimientos;

con respecto a si las empresas han sufrido algún tipo de ataque, un 73.3% indica que sí, a diferencia del 26.7 % que demuestra lo contrario.

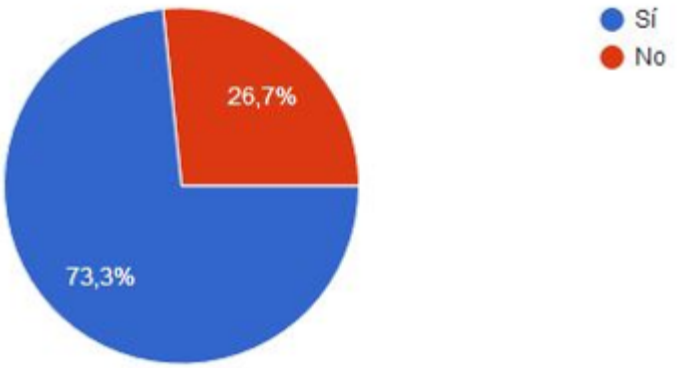

Figura 2: Resultados referente a si la infraestructura de red ha sufrido algún tipo de ataque
Fuente: Investigador

Referente al conocimiento sobre las vulnerabilidades a las que está expuesta la infraestructura de red, un 93.3 % está al tanto de las misma, sin embargo, aun sabiendo sobre las vulnerabilidades y afectación, se puede evidencia que el personal de TI no monitorea de forma activa las seguridades de su red inalámbrica, dispositivos o aplicaciones, teniendo como resultado un 53.3%. Lo que conlleva a que el nivel de afectación este entre alto y medio en la mayoría de empresa, según una de las preguntas realizadas.

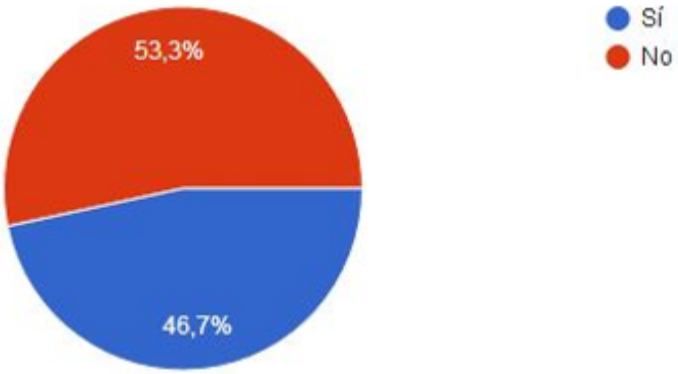

Figura 3: Resultados referente a si monitorea de forma activa las seguridades de red inalámbrica, dispositivos o aplicaciones
Fuente: Investigador

El que se realice auditorias periódicas para analizar los accesos y uso de infraestructura de red, así como el acceso a las diferentes aplicaciones, formo parte de la encueta, obteniendo un 53.3% del personal de TI que no efectúa dicho proceso.

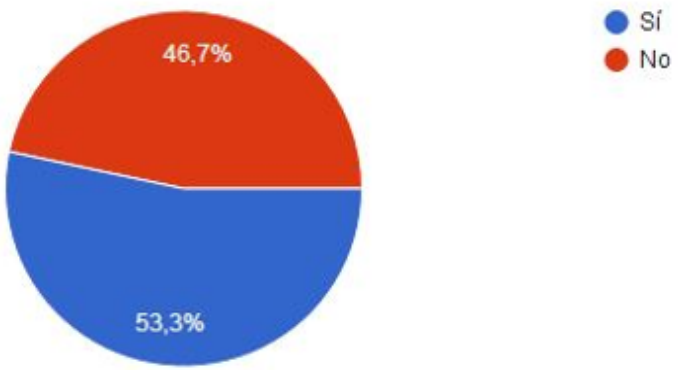

Figura 4: Resultados referente a si realizan auditorias periódicas en las que se revise los accesos y usos de la infraestructura de red y aplicaciones.
Fuente: Investigador

Si como administrador de TI, solicita a sus proveedores de red y software detalles de cómo actualizar sus productos y someterlos a pruebas de seguridad, un 53.3% lo realiza y un 46.7% no, contrarrestándose con lo referente a si hacen uso de las herramientas de seguridad provistas en los dispositivos de redes (APs), donde se puede evidenciar que un 53.8% no hace uso.

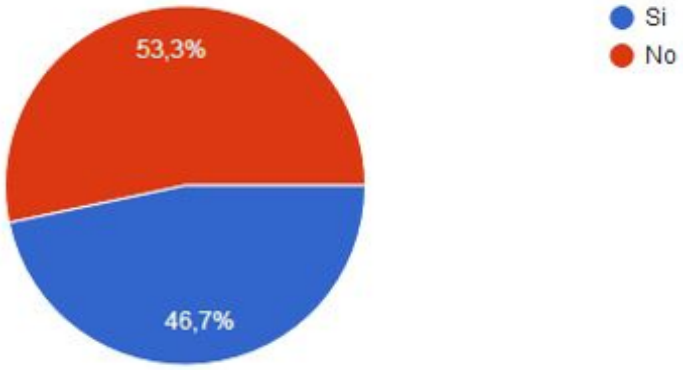

Figura 5: Resultados referente a si hace uso de las herramientas de seguridad provistas por los Fabricantes de dispositivos Wireless
Fuente: Investigador

Discusión

Los resultados obtenidos reflejan datos significativos, por cuanto el personal de TI de las empresas que hacen uso de las tecnologías inalámbricas, así como los que proveen de ellas, muestran conocimiento referente a las vulnerabilidades que puede afectar a su infraestructura WLAN.

Los profesionales de TI encargados de la infraestructura de red, así como de los proveedores de servicios y tecnología, indicaron que sería de utilidad contar con un modelo

que les permita diagnosticar las vulnerabilidades en redes inalámbricas. Se pudo determinar que las empresas buscan el empleo de nuevas tecnologías para maximizar el nivel de aceptación ante sus clientes.

Es importante señalar que en el Ecuador no existen estudios referentes a las vulnerabilidades en redes inalámbricas, que permitan tener una base para una adecuada implementación de redes Wireless en cualquier tipo de empresa; existe un trabajo similar en la Universidad Politécnica del Chimborazo, en la cual mediante el uso del manual metodológico OSSTMM y la utilización de herramientas bajo Linux identificaron las fallas de seguridad en su red inalámbrica.

Se plantea como líneas de trabajo futuro, un estudio para el diseño de un modelo para la identificación de vulnerabilidades en redes inalámbricas, así también el empleo de normas y marcos de referencia que ayuden a una adecuada administración de los servicios de TI precautelando la seguridad.

Conclusión

Las redes inalámbricas cada vez más usadas en las empresas requieren un tratamiento diferente, por cuanto brindan a más de acceso a la información, movilidad y esto hace que sean vulnerables si no se toma las respectivas medidas de seguridad.

Los profesionales de TI en su afán de implentar nuevas tecnologías se topan con obstáculos, muchos de ellos de presupueso por cuanto aun la tecnología de la información y comunicación no es vista como un factor importante para el desepeño y crecimiento de las empresas.

Las diferentes formas de ataques que se pueden presentar y que afectan al correcto funcionamiento de la infraestrutura de tecnología (redes inalámbricas) es conocida por los profesionales de TI, pero al no contar con herramientas adecuadas hace que esta continue siendo propensa a un ataque y la información sea vulnerada.

Referencias

Aboba, B., Blunk, L., Vollbrecht, J., & Carlson, J. (2004). Extensible Authentication Protocol (EAP). RFC 3748. Recuperado de https://tools.ietf.org/html/rfc3748

Aguirre, G., Ordóñez, A., & Ureta, L. (2005). Seguridad En Redes Inalámbricas. Tesis, 118. Retrieved from http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1445/LAZO_GARCIA_NUTTSY_SERVIDORES_AAA.pdf?sequence=1&isAllowed=y

Barajas, S. (2003). Protocolos de seguridad en redes inalámbricas. Recuperado de http://www.saulo.net/pub/ inv/SegWiFi-art.htm

Campbell, P., Calvert, B., Boswell, S., & Hecht, H. (2004). Security+ Guide to Network Security Fundamentals. London: Atlantic Books.

Cisco. (2017). Informe anual sobre ciberseguridad 2017.

DeKok, A. (2010). Use of Status-Server Packets in the Remote Authentication Dial In User Service (RADIUS) Protocol. RFC 5997. Recuperado de https://tools.ietf. org/html/rfc5997

DeKok, A. L., & Lior, A. (2013). Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions. RFC 6929. Recuperado de https://tools.ietf.org/html/ rfc6929

Educar, I. R. C.-T. de, & 2011, U. (2011). Elementos para el diseño de técnicas de investigación: una propuesta de definiciones y procedimientos en la investigación científica. Redalyc.org. Retrieved from http://www.redalyc.org/html/311/31121089006/

Filip, A., & Vázquez Torres, E. (2010). Seguridad en redes WiFi Eduroam. Recuperado de http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20 en%20redes%20Wifi%20Eduroam.pdf

Freier, A., Karlton, P., & P. Kocher. (2011). The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101. Recuperado de https://tools.ietf.org/html/rfc6101

García Arano, C. (2010). Impacto de la seguridad en redes inalámbricas de sensores IEEE 802.15.4, 15–49. Retrieved from http://eprints.ucm.es/11312/1/Memoria_Fin_de_Master_-_Carlos_Garc□a_Arano.pd f

García, R. R. (2011). Arquitectura para el Control de Acceso de la Red inalámbrica local de la Universidad Central "Marta Abreu" de Las Villas. Santa Clara: Universidad Central "Marta Abreu" de Las Villas.

Hernández Sampieri. (2003). Metodología de la investigación. (McGraw-Hill, Ed.). Mexico.

J Lopez. (2007). Wireless Networks LAN, 1–80.

Lahora.com.ec. (2010). Internet: vía libre a delitos : Economía : La Hora Noticias de Ecuador, sus provincias y el mundo. Retrieved February 3, 2018, from https://lahora.com.ec/noticia/1020547/internet-vc3ada-libre-a-delitos

Machado, D. V. (2012). Propuesta Metodológica para Asegurar Redes Inalámbricas y su Aplicación en la ESPOCH. Retrieved from http://dspace.espoch.edu.ec/handle/123456789/1480

P Baptista, Hernandez, & Juan Hernandez. (2010). Metodología de la investigación.

Paz, I. A. G., Casanova, Ms. D. B., & Gari, D. C. E. R. F. (2009). Universidad y sociedad. Universidad y Sociedad (Vol. 8). Retrieved from https://rus.ucf.edu.cu/index.php/rus/article/view/472

Pazmiño Caluña, A. A. (2011). Aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas WiFi. Retrieved from http://dspace.espoch.edu.ec/handle/123456789/1726

Rumale, A.S., & Chaudhari, D. N. (2011). IEEE 802.11x, and WEP, EAP,WPA / WPA2. Tech. Appl, 2 (6), pp. 1945-1950. Recuperado de http://www.ijcta.com/documents/

Saavedra Rios, G. A., & informática, I. de sistemas e. (2012). Seguridad en redes inalámbricas. reponame:Repositorio Institucional Universidad Libre. Retrieved from http://repository.unilibre.edu.co/handle/10901/4612

Suárez, M., & Resumen, G. (2012). MECANISMOS DE SEGURIDAD EN REDES INALÁMBRICAS. Retrieved from https://s3.amazonaws.com/academia.edu.documents/38082620/Mecanismos-de-Segur idad-en-Redes-InalambricasProtegido.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2 Y53UL3A&Expires=1517710467&Signature=gWotmUxID3PVF56HKMS9KyzYI5 E%3D&response-content-disposition=inline%3B file

United State of América. University of California.(2015). WEP FAQ. Recuperado de www.isaac.cs.berkeley. edu/isaac/wep-faq.html

Veizaga, W. J. B. (2013). Ethical Hacking: Hacking de Red Inalámbrica Wifi. Carrera de Informática, pp. 2-3.