UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2019 – MARZO 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

Análisis de las vulnerabilidades de las redes inalámbricas del Gad municipal del cantón Alfredo Baquerizo Moreno

EGRESADA:

Angelica Brigitte Villafuerte Bonilla

TUTOR:

ING. Ivan Ruben Ruiz Parrales

AÑO 2020

INTRODUCCIÓN

Las redes inalámbricas son muy importantes en la sociedad hoy en día y más en un mundo globalizado. "El internet permite la comunicación entre diversos países, es una red masiva usada cotidianamente." (Bravo Duarte, Chulli Paredes, & Espinoza Plaza, 2019). Por este motivo las personas buscan incorporar equipos informáticos como los routers a sus empresas, los cuales permite mantener comunicación por medio de las señales de Wi-Fi, esto permite a los usuarios estar conectados por medio de una red.

Estas redes de conexión inalámbrica son empleadas en muchos entornos, pudiendo ser estos laborales, corporativos o familiar, las mismas que pueden ofrecer un servicio no tan bueno brindando una experiencia desfavorable para quienes manejan información digital y necesitan de una conexión óptima, considerando como factor principal de este inconveniente las vulnerabilidades que pueden presentar estas redes de conexión.

El presente trabajo de investigación se basa en un análisis de las vulnerabilidades de las redes inalámbricas del Gad Municipal del Cantón Alfredo Baquerizo Moreno (Jujan), el cual se encuentra ubicado al Noroeste de la Provincia del Guayas a 60 km de Guayaquil en las calles Jaime Roldos aguilera #313 y José Domingo Delgado, con una extensión de 218 km² y una población aproximada de 25.179 habitantes.

> La misión de la institución es que el Gobierno Autónomo Descentralizado Municipal del Cantón Alfredo Baquerizo Moreno "JUJAN" contribuye a la sociedad del Cantón brindando obras y servicios públicos de buena calidad en forma equitativa respetando la biodiversidad y la diversidad cultural en consecución del buen vivir; además, trabaja con transparencia y crea espacios

para la participación protagónica de la ciudadanía en la toma de decisiones en los ámbitos sociocultural, ambiental económico y político institucional, con lo que promueve el desarrollo cantonal planificado y sustentable del cantón en el corto mediano y largo plazo. (Fernandez Torres & Solis Tobar, 2019)

Su Visión es que el Gobierno Autónomo Descentralizado Municipal del Cantón Alfredo Baquerizo Moreno "JUJAN", se constituirá en un ejemplo de desarrollo local con un personal capacitado que trabaja planificada mente basado en principios y valores como solidaridad, honestidad, responsabilidad; es una institución que realiza autogestión sostenible y eficiente; promueve la participación de la ciudadanía para la distribución eficaz y equitativa de los recursos; sus servicios son de calidad y trabaja en forma transparente; sus acciones permiten preservar el medio ambiente, la diversidad cultural, la equidad de género y generacional, convirtiéndolo en un municipio para todas y todos (Fernandez Torres & Solis Tobar, 2019)

En este estudio se utilizó la metodología de campo con la finalidad de identificar las amenazas y vulnerabilidades que afectan el funcionamiento dichas redes, mediante la técnica de observación se pudo determinas si los equipos con los que cuenta la institución cumple con las normas de seguridad especificados para redes Wifi , además se realizara un escaneo mediante la herramienta Nessus, para de esta manera determinar las vulnerabilidades e Inssider para conocer la velocidad de las redes.

Esta investigación se limitó en la realización de un estudio exhaustivo y recopilación de información , la línea de investigación es Desarrollo de Sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos y la sublínea es procesos de transmisión de datos y telecomunicaciones.

DESARROLLO

Hoy en día las redes inalámbricas han aumentado significativamente en las empresas públicas y privadas que las utilizan esta tecnología en sus operaciones y actividades diarias, estos equipos se encuentran interconectados y permiten que las computadoras, equipos móviles se encarguen de procesar la información que transita por la red.

El cantón Alfredo Baquerizo Moreno (JUJAN) es Administrado por la Alcaldesa Sra. Ángela Herrera Méndez desde el pasado 16 de Mayo del 2019, quien al asumir el cargo se encontró con irregularidades en cada uno de los departamentos de la anterior administración, las computadoras se encontraban sin discos duros, los folder sin documentos, escritorios en mal estado, departamentos con filtraciones de agua y las repisas sin ningún tipo de información sobre las gestiones realizadas , lo que ocasiono la perdida de gran cantidad de información y fue declarado en estado de emergencia debido a todas las anomalías encontradas y se tuvo la necesidad de reubicar el Municipio , por ende la nueva infraestructura evidencia un mal uso de los equipos de red y del cableado estructurado.

El Municipio cuenta con 15 Departamentos con un router en cada uno de ellos, donde laboran 200 personas hacen uso de las redes inalámbricas según (Gutierrez, 2016) “Las redes inalámbricas se llaman así para distinguirlas de las redes tradicionales por cable o las más modernas de fibra óptica.” (Venegas Vinueza , 2016) menciona que “en una red inalámbrica los datos se transmiten por el aire usando distintas tecnologías.” Estas redes son importantes para la realización de las actividades del personal que ahí trabaja, sin embargo se puede evidenciar en la ilustración 1 los equipos se encuentran

ubicados en lugares no adecuados y de fácil manipulación para todas las personas que ahí laboran ,lo que provoca que la información que se transfiere por esas redes no sea segura.

Ilustración 1:*Ubicación de los equipos de red.*

Elaborado por: Angélica Villafuerte Bonilla.

Según (Solarte Solarte, Benavides, & Enriquez Rosero, 2015) "La seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos, como electrónicos."

Adicional a esto se evidencio que en los alrededores del Gad Municipal se encuentran ubicados viviendas y edificios que poseen redes inalámbricas lo que ocasiona que el tráfico de las señales se debiliten.

Los dispositivos inalámbricos que se utilizan para la emisión de señales se describen a continuación:

Tabla 1:*Equipos de red*

Equipo	**Cantidad**	**Características**
router TP-Link	14	TL-WR741ND 150Mbps - 1 antena
Switch Tp-link	2	Switch Tp-link 16 Puertos Gigabit 10/100/1000 Tl-sg1016d

Elaborado por: *Angélica Villafuerte Bonilla*.

Las redes inalámbrica "son una tecnología que se utiliza comúnmente en el mundo de la informática para designar la conexión que se da entre nodos a través de ondas electromagnéticas sin necesidad de cables." (Pozo Bernabeu, 2019)

Este tipo de redes permite que los usuarios que se encuentren dentro del rango de cobertura puedan conectarse y tener acceso a la red según (Sánchez Peña, 2015) "Las redes inalámbricas se clasifican en los siguientes grupos"

- Redes inalámbricas de área personal (WPAN)
- Redes inalámbricas de área local (WLAN)
- Redes inalámbricas de áreas metropolitanas(WMAN)
- Redes inalámbricas de área amplia(WWAN)

Según (R, 2018) estas redes inalámbricas poseen las siguientes ventajas .

- Facilidad de la instalación
- Movilidad amplia
- Más baratas
- Sencillez
- Cantidad de dispositivos
- Redes complejas

Previo a la realización del análisis de las vulnerabilidades en las redes del Municipio se utilizó la metodología de campo según (Baena Paz, 2014) "esta metodología tiene como finalidad recoger y registrar ordenadamente los datos relativos al tema escogido como objeto de estudio, las principales técnicas que se usan son la observación y la interrogación"(pág. 11), y la metodología inductiva.

Se utilizó la técnica de la entrevista, que se realizó a la Sra. Ángela Herrera Méndez Alcaldesa del Catón quien autorizo a la encargada del departamento de sistemas la Ing. Marjorie Fructuoso brinde la información necesaria sobre el tema que se está investigando permitiendo el acceso a ciertos equipos para poder realizar el estudio y detectar las vulnerabilidades en la red como menciona (Incibe, 2017) "una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma."

Mediante la observación se pudo verificar las vulnerabilidades físicas de los routers que se encuentran en algunos de los departamentos, estos están ubicados en lugares inadecuados llenos de polvo y su configuración no brinda las seguridades necesarias.

Ilustración 2:*Uso incorrecto de los equipos de red.*

Elaborado por: Angélica Villafuerte Bonilla

En el ámbito de las redes inalámbricas , el término Wi-Fi significa acceso inalámbrico en general, perteneciente al Wi-Fi Alliance, un grupo dedicado a certificar que los productos de Wi-Fi cumplen con los estándares IEEE 802.11.

Estos estándares, como el 802.11b y 802.11ac, incluyen un conjunto de especificaciones desde los años 90 y continúa creciendo en la actualidad. Según (Shaw, 2018) "el estándar 802.11 codifica las mejoras que aumentan el rendimiento y el alcance inalámbrico, así como la disponibilidad de nuevas frecuencias."

Sin embargo las redes inalámbricas no son totalmente seguras según (Serna, 2014) estas redes pueden ser interferidas por otros dispositivos que funcionan en la misma frecuencia, podría mediar la velocidad de transmisión del sistema

En la tabla a continuación se detallan las distintas variaciones del estándar 802.11 y sus significados.

Tabla 2:*Especificaciones del estándar 802.11*

Estándar	**Especificación**
802.11a.	Según (Axtel, 2017) "El estándar 802.11funciona con conexiones de hasta 54Mbps,en un rango de 30 metros aproximadamente opera en la banda de 5GHz utiliza 8 canales no superpuestos".
802.11ac.	"Tiene un promedio de entre 2,34 y 3,47 Gbps; se mantiene el uso de la banda de los 5 GHz y el ancho de banda se incrementa en una frecuencia de los 80 MHz hasta los hasta 160 MHz." (Álvarez, 2016)
802.11ad	Según (García, 2016) "Utilizan las frecuencias de 2,4 o 5 GHz. El WiFi 802.11ad opera en la banda de los 60 GHz (entre 57 y 66 GHz).Operar en estas frecuencias tiene dos grandes ventajas: bandas muy poco saturadas, y velocidades mucho mayores".

802.11b.	Como menciona (Spedtest, 2016) "Permitía velocidades de hasta 11 Mbit/s, frente a los 2 Mbit/s del original, con una frecuencia de 2.4 GHz lo que ocasionaba mayor alcance, no estaba regulada y generaba interferencias con aparatos inalámbricos y electrónicos".
802.11g	Menciona (Carabajo, 2013) "Es el más aceptado actualmente a nivel mundial. Trasmiten en el mismo ancho de banda, los 2,4 Ghz y la diferencia básica radica en la velocidad de transferencia (teórica) que son capaces de conseguir, 54 Mbit/s".
802.11-1997	"Es el estándar original de IEEE WLAN. Fue reemplazado veintiún meses después con IEEE Std 802.11-1999. Ese documento sigue siendo el documento base y se ha complementado con ocho documentos de enmienda" (Cwnp, 2015)

Elaborado por: *Angélica Villafuerte Bonilla*.

Seguridad de las redes.

La seguridad de las redes es muy importante ya que permite adoptar medidas de prevención además de establecer políticas de control de acceso ayudando a proteger la red y supervisando las actividades que en ella se realizan

> La seguridad de la red es la práctica de prevenir y proteger contra la intrusión no autorizada en redes corporativas. La seguridad de redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. (Fruhlinger , 2018)

En las redes inalámbricas es muy importante establecer medidas de seguridad (Fruhlinger , 2018) también menciona las siguientes medidas:

Control de acceso: debe poder bloquear a usuarios y dispositivos no autorizados de su red. Los usuarios que tienen acceso autorizado a Internet solo han sido autorizados para utilizar el sitio web.

Autenticación: Una de las medidas que se pueden tomar para controlar mejor el acceso a una red WiFi es el filtrado de direcciones MAC. Esta medida, aunque poco efectiva de cara a la seguridad frente a un intruso con conocimientos de redes, todavía puede ser útil en ciertos ambientes pequeños. (Suarez Gutierrez, 2017)" La autenticación se puede dar de 2 maneras según (Familia IEEE 802.11, 2014) la modalidad empresarial El punto de acceso emplea el protocolo EAP sobre 802.1x y RADIUS para la autenticación y la modalidad domestica el mecanismo de autenticación usado es PSK. Esta modalidad no requiere de servidor de autenticación"

Técnicas y herramientas utilizadas.

Se realizó la entrevista a 5 personas de diferentes departamentos y al técnico del departamento de sistemas quienes manifestaron que debido a los inconvenientes que actualmente el Municipio tiene no se realizó la contratación del personal adecuado para la configuración de los equipos inalámbricos y fueron configurados por un pasante y desconocen si la red presente algún tipo de vulnerabilidad .

En cuanto al periodo de tiempo que cambian contraseñas de los routers manifestaron que las contraseñas no han sido cambiadas

Referente a la calidad de la red manifestaron que hay horas del día que el internet es lento y que en momentos de lluvia presenta limitaciones.

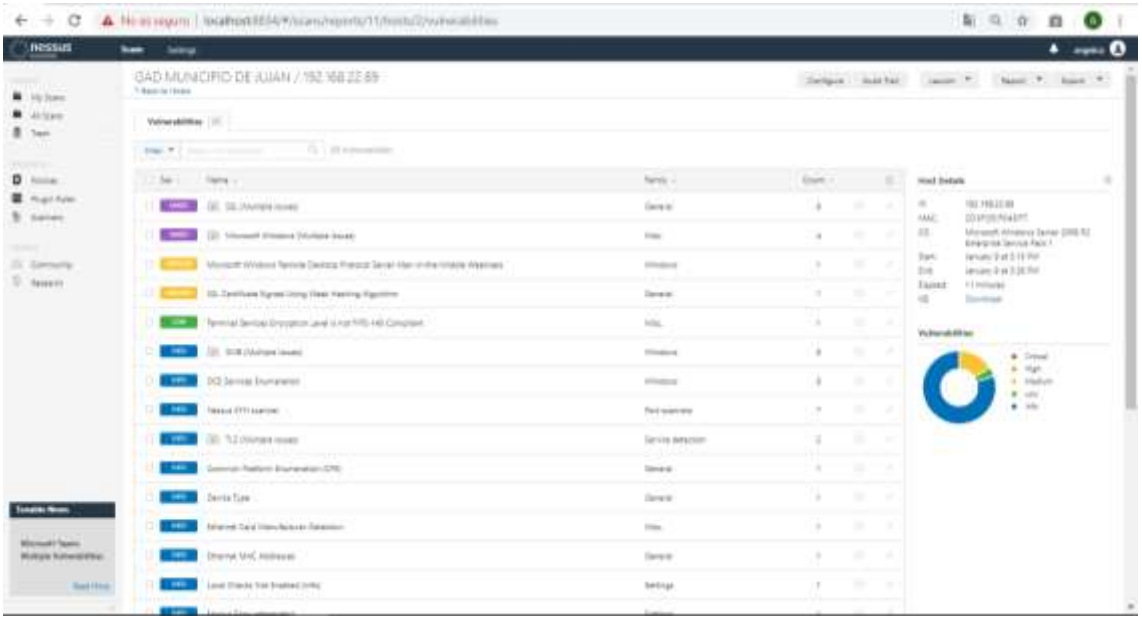
Para la elaboración del análisis de las vulnerabilidades se utilizó la herramienta nessus. Como menciona (Eworo Osa & García Ara, 2016) “nessus es un programa de escaneo de vulnerabilidades que funciona en varios sistemas operativos, es un tipo especial de proceso que se ejecuta en segundo plano y escanea el sistema, mostrando el avance e informando sobre el estado de los escaneos.”

Ilustración 3:*Inicio de sesión de nessus*

Elaborado por: Angélica Villafuerte Bonilla.

Se instaló el software nessus y se procedió a realizar el escaneo de la red.

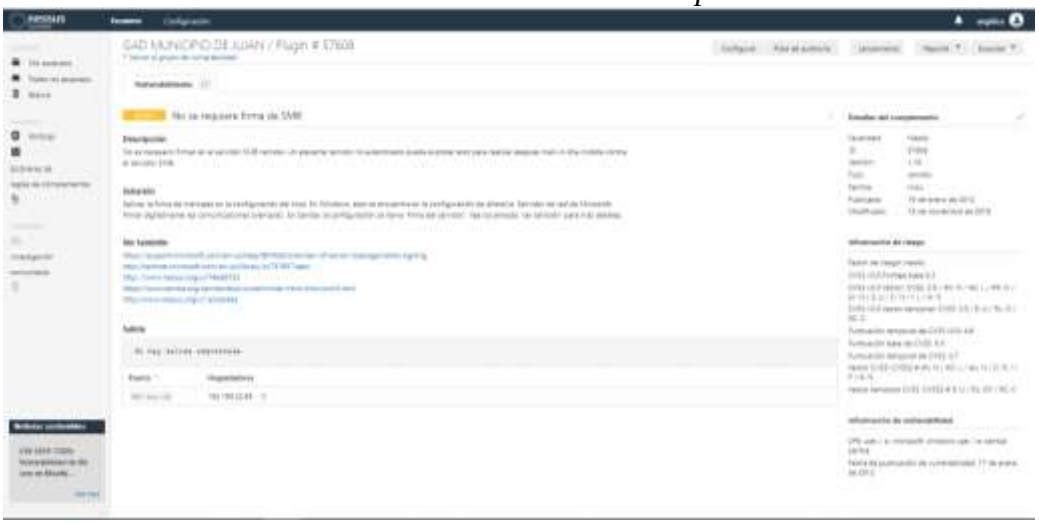
Ilustración 4:*Analisis de las vulnerabilidades con nessus*



Elaborado por: Angélica Villafuerte Bonilla.

Luego de realizarse el escaneo de las vulnerabilidades con el software nessus se realiza una comparación de los resultados obtenidos y se realiza un análisis de los niveles de gravedad que se muestran por colores.

Ilustración 5:*Vulnerabilidades de puertos.*



Elaborado por: Angélica Villafuerte Bonilla.

Se encontró una vulnerabilidad media que indicando que no es necesario firmar el servidor SMB remoto. Esto provocaría que un atacante remoto no autentificado podría realizar ataques contra el servidor SMB

Ilustración 6:*Vulnerabilidad de hombre en el medio.*

Elaborado por: Angélica Villafuerte Bonilla.

El servidor de protocolo de escritorio remoto de Windows posee una debilidad de hombre en el medio indicando que un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado permitiendo obtener cualquier información confidencial transmitida incluyendo las credenciales de autenticación.

Como menciona (Microsoft, 2017) esto puede ocurrir debido a las congestiones de red, estos mensaje de error también puede aparecer si el servidor de escritorio remoto está configurado para conexiones seguras TLS y TLS no es posible utilizar en el cliente que intenta la conexión RDP.

Ilustración 7:*Certificados no confiables.*

Elaborado por: Angélica Villafuerte Bonilla.

El certificado SSL no es confiable esto se debe a que la cadena de certificados puede contener una firma que no coincida con la información o que no se pudo verificar lo que ocasiona que los usuarios sean más difíciles de verificar su identidad y podría ser fácil de vulnerar.

Para conocer la velocidad de transmisión de la red Wi-Fi del Municipio se utilizó el programa Speedtest “es un prueba que muestra cual es la velocidad de una conexión a Internet. Estas pruebas operan completamente a través del protocolo HTTP para asegurar una máxima compatibilidad, poniendo a prueba la lactancia o Ping, la velocidad de descarga y la velocidad de subida” (Maja, 2015)

Ilustración8:*Velocidad de red*

Elaborado por: Angélica Villafuerte Bonilla.

Los resultados muestran 40 ping con una velocidad de 6.83 Mbps de descarga y 10.33 Mbps de carga evidenciando que el ancho de banda que posee la institución es bueno como indica el estándar 802.11b que se pueden transferir hasta 11 Mbps en la banda de 2,4 GHz..

lustración 9:*Analisis de la frecuencia mediante Inssider.*

Elaborado por: Angélica Villafuerte Bonilla

Con la herramienta Inssider se puede observar el SSID de app, la dirección Mac y se evidencia que la potencia de la red es de de -80 dBm a -70 dBm evidenciando que la señal de la red Wi-Fi es inestable y puede presentar congestionamientos.

Mediante la observación se pudo evidenciar que Gad del Cantón Alfredo Baquerizo Moreno no cuenta con la infraestructura tecnológica adecuada, los equipos inalámbricos que posee están en mal estado, llenos de polvo y en algunos departamentos el router está mal ubicado, personal que trabaja en el técnico del departamento de sistemas no se encuentra capacitado para la función que debe realizar por ende su trabajo lo delega a un pasante quien es el encargado de realizar las distintas configuraciones a los equipos, a continuación se detallan las vulnerabilidades encontradas en la red inalámbrica del departamento de sistemas.

Tabla 3:*Listado de vulnerabilidades*

Vulnerabilidad	**Nivel Gravedad**	**Puerto**

Servidor de protocolo de escritorio remoto de Microsoft Windows Debilidad del hombre en el medio	Medio	3389 / tcp / msrdp
Certificado SSL firmado con algoritmo de hash débil	Medio	3389 / tcp / msrdp
El nivel de cifrado de Servicios de Terminal Server no cumple con FIPS-140	Bajo	3389 / tcp / msrdp
Detección del servicio SMB de Microsoft Windows	Información	139 / tcp / smb 445 / tcp / cifs
Divulgación de información del sistema remoto de Microsoft Windows SMB NativeLanManager	Información	445 / tcp / cifs
Divulgación de información de host remoto de Windows NetBIOS / SMB	Información	137 / udp / netbios-ns
Dialectos SMB2 de Microsoft Windows compatibles (verificación remota)	Información	445 / tcp / cifs
Versiones de Microsoft Windows SMB compatibles (verificación remota)	Información	445 / tcp / cifs
El certificado SSL no se puede confiar	Medio	3389 / tcp / msrdp
Suites de cifrado SSL de resistencia media compatibles (SWEET32)	Media	3389 / tcp / msrdp

Elaborado por: *Angélica Villafuerte Bonilla*.

CONCLUSIONES.

Finalizado el trabajo de investigación se concluye que las redes inalámbricas son cada vez más comunes en las instituciones públicas por ende su seguridad es muy importante debido a la información que por ellas se envían.

- Se pudo evidenciar que las redes Wi-Fi instaladas actualmente en el Municipio del Cantón Alfredo Baquerizo Moreno no disponen de la seguridad necesaria ya que su nivel de seguridad muy bajo, lo que pone en riesgo la integridad de la información, además de no contar con los equipos de red adecuados.
- Mediante el escaneo realizado con la herramienta nessus se encontraron 25 vulnerabilidades de niveles medio y bajo.
- El ingreso a los routers es fácil debido a que la contraseña de ingreso por defecto no ha sido cambiada por lo que cualquier persona podría obtener la contraseña sin la autorización necesaria.
- Las firmas de los certificados SSL no son válidos esto se debe a que la parte inferior del certificado está firmado por una institución pública no conocida
- Se encontró vulnerabilidad de nivel medio en el servidor remoto de Windows debido a las con gestiones que se dan en la red.

RECOMENDACIONES.

Concluido el estudio de caso relacionado análisis de las vulnerabilidades de las redes inalámbricas del Gad del Cantón Alfredo Baquerizo Moreno se recomienda lo siguiente:

- El departamento de sistemas debe realizar una verificación de los equipos inalámbricos y establecer un cronograma de renovación de claves, esto permitirá establecer mayor seguridad de la información,
- Para contrarrestar la vulnerabilidad de certificado SSL es necesario generar un certificado adecuado para ese servicio ya que la firma que tiene no es confiable y el servidor puede ser víctima de ataques.
- Es necesario verificar los equipos físicos que se encuentran es mal estado y realizar el cambio de ubicación para una mejor seguridad.
- De acuerdo a los inconvenientes encontrados es necesario realizar el cambio de los equipos de red debido a que los routers TP-Link son fáciles de vulnerar por lo cual se recomienda adquirir equipos más seguros como los Cisco o Microtik.

Bibliografía

Álvarez, R. (29 de Junio de 2016). *Xataca*. Obtenido de https://www.xataka.com/perifericos/el-estandar-wi-fi-802-11ac-se-actualiza-y-nos-trae-mas-velocidad-y-mayor-ancho-de-banda

Baena Paz, G. M. (2014). *Metodología de la Investigación* (Primera ed.). Mexico: Grupo Editorial Patria. Recuperado el 30 de Diciembre de 2019, de https://books.google.com.ec/books?id=6aCEBgAAQBAJ&printsec=frontcover&dq=que+es+la+metodologia+de+campo&hl=es&sa=X&ved=0ahUKEwi4tpXk-fnmAhWCzlkKHTbSAP0Q6AEIPDAD#v=onepage&q&f=false

Carabajo, A. (10 de Mayo de 2013). *Nobbot*. Obtenido de https://www.nobbot.com/tecnologia/perdido-en-una-marana-de-siglas-y-numeros-comprende-mejor-las-diferentes-redes-wifi-para-sacarles-todo-el-provecho/

García, A. (15 de Diciembre de 2016). *Adslzone*. Obtenido de https://www.adslzone.net/2016/12/15/implica-nuevo-wifi-802-11ad-opere-60-ghz/

Gutierrez, A. (31 de Noviembre de 2016). *aboutes*. Recuperado el 28 de Diciembre de 2019, de https://www.aboutespanol.com/red-inalambrica-lo-que-necesitas-saber-3507889

López Ortiz, F. (2015). *upm.* (U. p. demadrid, Ed.) Obtenido de http://www.dit.upm.es/~david/tar/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf

Pozo Bernabeu, R. (28 de Mayo de 2019). *techclub*. Recuperado el 30 de Diciembre de 2019, de https://techclub.tajamar.es/redes-inalambricas/

Shaw, K. (3 de Febrero de 2018). *networkworld*. Recuperado el 3 de Enero de 2020, de https://www.networkworld.es/wifi/80211-estandares-de-wifi-y-velocidades

Axtel. (16 de Octubre de 2017). *Axtel*. Obtenido de http://axtelmx.custhelp.com/app/answers/detail/a_id/223/~/significado-de-ieee-802.11-a%2Fb%2Fg%2Fn-y-ac

Bravo Duarte, F. L., Chulli Paredes, J. V., & Espinoza Plaza, B. A. (Enero de 2019). *repositorio unemi*. Obtenido de http://repositorio.unemi.edu.ec/handle/123456789/4460

Cwnp. (20 de Octubre de 2015). *cwnp*. Obtenido de https://www.cwnp.com/forums/posts?postNum=304657

De Luz, S. (1 de Febrero de 2014). *computerhoy*. Obtenido de https://computerhoy.com/noticias/internet/que-es-wifi-80211ac-que-hace-tan-rapido-8789

Eworo Osa , M., & García Ara, I. (Octubre de 28 de 2016). *slideshare*. Recuperado el 4 de Enero de 2020, de https://es.slideshare.net/nananana74/presentacinnessus-66586757

Familia IEEE 802.11. (2014). *bibing*. Obtenido de http://bibing.us.es/proyectos/abreproy/11579/fichero/f.+Cap%C3%ADtulo+2+-+Familia+IEEE+802.11.pdf+

Fernandez Torres, A., & Solis Tobar, E. J. (2019). *dspace utb*. Obtenido de http://dspace.utb.edu.ec/handle/49000/5525

Fruhlinger , J. (4 de Julio de 2018). *networkworld*. Obtenido de https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red

Herrera Ramírez, E., Díaz Ramírez, A., & Calafate, C. T. (2015). *Cicomp07*. Obtenido de http://www.grc.upv.es/calafate/download/Cicomp07_Estandar80211n.pdf

Incibe. (20 de Marzo de 2017). *incibe*. Recuperado el 2 de Enero de 2020, de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Maja. (31 de Octubre de 2015). *speedtest*. Obtenido de http://speedtest.plus/speed-test/speed-test.html

Microsoft. (30 de Noviembre de 2017). *Microsoft*. Obtenido de https://support.microsoft.com/es-py/help/2493594/rdp-connection-to-remote-desktop-server-running-windows-server-2008-r2

R, J. L. (27 de Abril de 2018). *tecno*. Obtenido de https://247tecno.com/tecnologias-inalambricas-caracteristicas-y-como-funcionan/

Sánchez Peña, I. (12 de Enero de 2015). *Loyvan*. Recuperado el 2 de Enero de 2020, de https://www.loyvan.com/informatica/clases-de-redes-inalambricas/

Serna, E. (10 de Diciembre de 2014). *scielo*. Obtenido de de www.scielo.org.co: http://www.scielo.org.co/pdf/cein/v23n2/v23n2a01.pdf

Solarte Solarte, F. N., Benavides, M. d., & Enriquez Rosero, E. R. (Diciembre de 2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE*, *28*(15). Recuperado el 30 de Diciembre de 2019, de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Spedtest. (11 de Agosto de 2016). *Spedtest*. Obtenido de https://www.testdevelocidad.es/2016/08/11/conoce-cuales-todos-los-estandares-wi-fi-existen/

Suarez Gutierrez, M. (3 de Enero de 2017). *irix*. Obtenido de http://www.irix.es/blog/control-de-acceso-en-redes-inalambricas/

Venegas Vinueza , J. P. (Julio de 2016). *scribd*. Recuperado el Enero de 2020, de https://es.scribd.com/document/397135458/04-Red-115-Tesis-de-Grado

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
ESCUELA DE SISTEMAS Y TECNOLOGIAS

ANEXOS

Anexo 1: Entrevista

1. **Cree usted que la red inalámbrica presenta alguna vulnerabilidad?**

   Desconozco la información.

2. **Con que frecuencia cambian las contraseñas del /los Router's en el**

   Se ha cambiado una sola vez

3. **Considera usted que la calidad de la red inalámbrica es buena?**

   Si es buena pero cuando llueve o hace mucho viento a veces se limita.

4. **Con que frecuencia actualizan o cambian los dispositivos de conexión inalámbrica.**

Aun no se ha cambiado ningún equipo debido a la situación económica que atraviesa el municipio.

5. **Considera usted que el Municipio cuenta con personal debidamente capacitado para dar mantenimiento a los dispositivos de conexión inalámbrica**

   Si contamos con un pasante de la carrera de Analisis de Sistemas del ITSB

Entrevista realizada al técnico del departamento de sistemas

Anexo 2:Entrevista Alcaldesa

Ilustración 9:*Entrevista Alcaldesa*

Elaborado por: Angélica Villafuerte Bonilla

Anexo 3:Entrevista encargado departamento

Ilustración 10:*Entrevista Técnico departamento sistemas*

Elaborado por: Angélica Villafuerte Bonilla

Anexo 4: Configuración router

Ilustración 11:*Configuracion por defecto del router*

Elaborado por: Angélica Villafuerte Bonilla

Anexo 5: Departamento de sistemas

Ilustración 12:*Departamento Sistemas*

Elaborado por: Angélica Villafuerte Bonilla

Anexo 6: Realizacion escaneo

Ilustración 13:*Escaneo con nessus*

Elaborado por: Angélica Villafuerte Bonilla

Anexo 7:Resultados escaneo

REPORTE DE LAS VULNERABILIDADES
192.168.22.89

0	0	8	2	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information

192.168.22.89

INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	26024	PostgreSQL Server Detection
INFO	N/A	66173	RDP Screenshot
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed c
			TCP/IP Timestamps Supported
		1	TLS Version 1.0 Protocol Detection
		1	TLS Version 1.1 Protocol Detection
			Terminal Services Use SSL/TLS
			Traceroute
			Windows NetBIOS / SMB Remote Host Information Disclosure
			Windows Terminal Services Enabled