UNIVERSIDAD DEL SURESTE: DE LA FRONTERA COMALAPA.

DOCENTE: Lic. Ervin Silvestre Castillo.

ASIGNATURA: Taller de elaboración de tesis.

ALUMNO: Ramiro Gerardo Resendíz Valdéz.

CUATRIMESTRE: Noveno (9no).

CARRERA: Ingeniería en sistemas computacionales.

GRUPO: ISC13SDC0220-A.

UNIDAD: Primera (1ra).

TRABAJO: Capítulo 4 de la tesis.

FECHA DE ENTREGA: 16/Mayo/2023.

CAPÍTULO 1: PLANTEAMIENTO DEL PROBLEMA

“PROTOCOLO EN REDES INFORMÁTICAS”

1.1. DESCRIPCIÓN DEL PROBLEMA

(Navas, 2017) Explica:

Wi-Fi es un conjunto de especificaciones para las redes de área local inalámbricas (WLAN), basadas en el estándar IEEE 802.11. El nombre de Wi-Fi es tenido como una abreviatura del término inglés “Wireless Fidelity”, aunque Wi-Fi Alliance, la entidad responsable principalmente por el licenciamiento de productos basados en la tecnología, nunca haya afirmado tal conclusión.

Es común encontrar el nombre Wi-Fi escrito como “wi-fi”, “Wi-fi” o incluso “wifi”. Todas estas denominaciones se refieren a la misma tecnología. Con la tecnología Wi-Fi, es posible implementar redes que conectan ordenadores y otros dispositivos (smartphones, tablets, consolas de videojuegos, impresoras, etcétera) que están próximos geográficamente. Estas redes no requieren el uso de cables, ya que efectúan la transmisión de datos por medio de radiofrecuencia. Este esquema ofrece varias ventajas, entre ellas: permite al usuario utilizar la red en cualquier punto dentro de los límites de alcance de la transmisión, posibilita la inserción rápida de otros equipos y dispositivos de la red, evita que las paredes o estructuras de la propiedad inmobiliaria sean de plástico o adaptadas para el paso de cables.

La flexibilidad del Wi-Fi es tan grande que se hizo viable la implementación de redes que hacen uso de esta tecnología en los más variados lugares,

principalmente por el hecho de que las ventajas mencionadas en el párrafo anterior muchas veces resultan en disminución de costos. Así, es común encontrar redes Wi-Fi disponibles en hoteles, aeropuertos, carreteras, bares, restaurantes, centros comerciales, escuelas, universidades, oficinas, hospitales, y muchos más sitios. Para utilizar estas redes, solo es necesario que el usuario tenga un ordenador portátil, smartphone o cualquier dispositivo compatible con Wi-Fi. Actualmente cualquier empresa tiene que hacer frente a una mayor demanda de accesos inalámbricos, ya sea por parte clientes, proveedores o empleados.

Desafortunadamente, también los hackers continúan intentando lograr acceder dentro de las redes. Para proteger una red inalámbrica, primero hay que conocer las principales amenazas a las que se ven afectadas y que ponen en riesgo la seguridad del usuario. Cada vez tenemos más dispositivos conectados a Internet de forma inalámbrica. Si pensamos en cómo navegábamos hace unos años, seguro que la mayoría de nosotros utilizaba un ordenador conectado por cable al router. Sin embargo, esto ha cambiado en los últimos tiempos.

Las redes inalámbricas han ganado peso poco a poco. Hoy utilizamos más equipos conectados sin cables a Internet. La cuestión es que esto también puede traer algunos problemas. En esta investigacion vamos a hablar de cuáles son los principales problemas del Wi-Fi y qué hacer para solucionarlos. En la actualidad las redes Wi-Fi tienen un gran peso en la sociedad. Podemos encontrar puntos de acceso por muchas partes y que nos ofrecen la posibilidad de navegar desde nuestros dispositivos móviles casi en cualquier lugar.

El auge de lo que conocemos como el Internet de las casas también ha ayudado a que las conexiones sin cables sigan creciendo. Son muchos los aparatos que tenemos conectados en nuestro hogar. Necesitamos que

nuestros routers Wi-Fi funcionen correctamente. A veces hay problemas con el Wi-Fi, fallos que hacen que no funcione correctamente o que la velocidad de Internet no sea la adecuada. Vamos a detallar cuáles son los principales. También daremos recomendaciones para mejorar la velocidad y que funcione mejor.

Las redes inalámbricas son mucho más sensibles que el cableado, esto significa que vamos a tener más problemas de estabilidad, velocidad e incluso tener que soportar cortes continuos. Esto no siempre ocurre; lógicamente todo dependerá de nuestros dispositivos, la configuración que tengamos o cómo sea la conexión. No obstante, a veces surgen problemas que conviene corregir.

Uno de los problemas más importantes a la hora de conectarnos de forma inalámbrica es tener una mayor latencia. Es algo que puede lastrar el buen funcionamiento para algunos usuarios. Hablamos de por ejemplo a la hora de realizar vídeo llamadas o jugar por Internet. Siempre que lo comparemos con una conexión cableada, en este sentido va a salir perdiendo el Wi-Fi, tomándolo como un punto negativo. Esto puede afectar a la hora de llevar a cabo determinadas acciones, como hemos indicado. Debemos evitar que esto ocurra y lograr que el ping sea lo más bajo posible.

La velocidad de Internet también puede verse mermada si nos conectamos de forma inalámbrica. Es algo que está presente en los usuarios que utilizan este medio para navegar por Internet. Siempre que hagamos un test de velocidad en un mismo equipo conectado por cable o a través de Wi-Fi habrá diferencias. Puede ser mayor o menor en función de determinados factores, como por ejemplo qué dispositivo estemos utilizando, la distancia con el router o si usamos amplificador de señal o no. Hay determinados equipos que pueden ayudar a que la pérdida de velocidad sea lo mínimo posible.

Los problemas de seguridad son sin duda uno de los problemas del Wi-Fi más comunes y es un factor muy importante para los usuarios, pero no siempre está presente cuando navegamos de forma inalámbrica. Nuestro router puede ser atacado por intrusos que busquen la manera de robar la clave de acceso y entrar en nuestra conexión. Lo mismo ocurre cuando nos conectamos a una red inalámbrica ajena.; allí también tendríamos problemas de seguridad. No sabemos realmente quién puede estar detrás de la conexión y si ese Wi-Fi ha podido ser creado con el único objetivo de robar información personal.

Para evitar estos problemas viene bien hacer uso de una VPN que pueda cifrar la conexión. La cobertura no es la que nos gustaría y esto es otra cuestión muy influyente dentro del tema, Especialmente en cuanto nos alejamos un poco del router o nos conectamos desde un lugar donde no está optimizado. Es cierto que existen dispositivos que pueden ayudarnos, como sistemas Mesh, repetidores o PLC, pero no siempre funcionan correctamente o no siempre ayudan realmente a mejorar la cobertura como nos gustaría.

Por último, algo que también ocurre es la pérdida de inestabilidad y cortes. No es lo mismo una conexión cableada que a través del Wi-Fi. La fiabilidad no es la misma y también pueden venir problemas.

(Quero, 2013) Menciona:

Siempre conviene saber qué tipos de vulnerabilidad en una red existen. El mundo (Wireless), como la gente suele llamarlo, ha desencadenado una lucha entre desarrolladores y usuarios acerca de la vulnerabilidad de las redes inalámbricas. Todos queremos WiFi gratis y no está mal usar una red de acceso libre de vez en cuando, pero ten cuidado, porque podrías exponer

tu información bancaria. No todas las redes WiFi gratuitas son creadas con el afán de dañar la privacidad de los usuarios, sin embargo, existen personas malintencionadas y con el conocimiento suficiente para aprovechar una de las vulnerabilidades de este tipo de conexiones y los riesgos y amenazas en las redes inalámbricas públicas. La razón por la que los datos pueden ser vulnerados en una red de acceso libre es que este tipo de conexiones no cifran la información, y, por esta causa, si se tiene una conexión WiFi en casa, se debe emplear seguridad WPA o WPA2.

Este tipo de seguridad no solamente protege a la red de intrusos, sino que también cifra todos los datos enviados a través de ésta, como cuentas bancarias, contraseñas, nombres, números telefónicos, etc. Según Think Big, estas redes predominan en restaurantes, aeropuertos o sitios públicos como parques o bibliotecas, existen brechas de seguridad que deben ser tomadas en cuenta. Otro problema muy importante es que hay muchos routers desactualizados. Cualquier dispositivo puede sufrir vulnerabilidades, pero esos fallos suelen ser corregidos por los propios fabricantes a través de parches y actualizaciones. Pero claro, si no instalamos esas nuevas versiones no podremos corregirlos. Ahí está el problema, ya que estamos rodeados de routers que pueden llevar incluso años sin actualizar. Por otra parte, un punto también esencial es el tipo de cifrado que estemos utilizando. Hoy en día los más fuertes y fiables son WPA-2 y WPA-3. Sin embargo, muchos usuarios, especialmente aquellos que tienen routers más antiguos, siguen utilizando algunos cifrados obsoletos e inseguros, como podría ser el WEP. Es muy importante evitar esto, ya que podría habilitar la entrada de intrusos.

1.2 FORMULACIÓN DEL PROBLEMA

1. ¿Qué son los cifrados de redes wifi?

2. ¿Cuáles son los riesgos de conectarse a una red pública?

3. ¿Conocen los estudiantes de la Universidad del Sureste los riesgos de no tener una red wifi segura?

4. ¿Identifican los estudiantes de la Universidad del sureste las páginas de dudosa procedencia?

5. ¿Saben los estudiantes de la Universidad del Sureste los riesgos de no cambiar la configuración predeterminada del modem?

6. ¿Por qué las redes públicas son un punto de acceso de robo de información más fácil de manipular?

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Crear estrategias educativas para mejorar la seguridad las redes informáticas en los hogares de los estudiantes de la Universidad del Sureste.

1.3.2. OBJETIVOS ESPECÍFICOS

- Proporcionar información de manera simple y entendible sobre los riesgos de conectarse a una red wifi.
- Aportar el conocimiento básico a los estudiantes de la Universidad del Sureste sobre cómo cambiar la configuración de su modem.
- Informar a los estudiantes de la Universidad del Sureste el riesgo que conlleva conectarse a una red pública y lo vulnerable que somos al robo de información.
- Explicar a los estudiantes de la Universidad del Sureste las diferencias de una red de hogar (privada) a una red pública.
- Listar los detalles de una página segura de navegar para que las personas no tengan ningún riesgo de navegar en ellas.
- Enseñar a los estudiantes de la Universidad del Sureste a identificar paginas de dudosa procedencia.

1.4. HIPÓTESIS

Entre más información tengan los estudiantes de la Universidad del Sureste sobre las medidas de seguridad en las redes informáticas, menos riesgo de hackeo tendrán.

1.5 JUSTIFICACIÓN

(Jurado, 2023) Menciona:

Una red inalámbrica es insegura de manera predeterminada. Esto significa que está abierta a todos y cualquier persona dentro del área de cobertura del punto de acceso puede potencialmente escuchar las comunicaciones que se envían en la red. En el caso de un individuo, la amenaza no es grande ya que los datos raramente son confidenciales, a menos que se trate de datos personales. Sin embargo, si se trata de una compañía, esto puede plantear un problema serio.

Este tipo de ataques, conocidos como Man in the Middle u Hombre en el medio ocurren cuando un hacker se aprovecha de la falta de mecanismos de seguridad en una red Wi-Fí pública para establecer su equipo como intermediario entre los datos que comparte tu ordenador o smartphone con la red WiFi a la que estás conectado. Así, podrá acceder a tus contraseñas o datos bancarios si entras a sitios para hacer compras en línea o ver tu estado de cuenta. También podrá interceptar tus contraseñas, algo especialmente peligroso si te conectas desde un ordenador de trabajo a cualquier red WiFi Pública. Como también está la variable de intrusión de datos, la instalación de un punto de acceso en una red local permite que cualquier estación acceda a la red conectada y también a Internet, si la red local está conectada a ella.

Es por esto que una red inalámbrica insegura les ofrece a los hackers la puerta de acceso perfecta a la red interna de una compañía u organización. En las redes públicas, este tipo de ataques puede aparecer en forma de redes sin contraseña que tienen un nombre similar al establecimiento en el que te encuentras. A simple vista, parecen un buen punto para conectarte desde donde estás; sin embargo, estarás compartiendo tus datos

directamente con una persona malintencionada. Además de permitirle al hacker robar o destruir información de la red y de darle acceso a Internet gratuito, la red inalámbrica también puede inducirlo a llevar a cabo ataques cibernéticos.

Como no existe manera de identificar al hacker en una red, puede que se responsabilice del ataque a la compañía que instaló la red inalámbrica. También existe la problemática llamada interferencia radial y denegación del servicio que son básicamente las ondas radiales son muy sensibles a la interferencia. Por ello una señal se puede interferir fácilmente con una transmisión de radio que tenga una frecuencia cercana a la utilizada por la red inalámbrica. Hasta un simple horno de microondas puede hacer que una red inalámbrica se vuelva completamente inoperable si se está usando dentro del rango del punto de acceso.

El método de acceso a la red del estándar 802.11 se basa en el protocolo CSMA/CA, que consiste en esperar hasta que la red este libre antes de transmitir las tramas de datos. Una vez que se establece la conexión, una estación se debe vincular a un punto de acceso para poder enviarle paquetes. Debido a que los métodos para acceder a la red y asociarse a ella son conocidos, un hacker puede fácilmente enviar paquetes a una estación solicitándole que se desvincule de una red.

El envío de información para afectar una red inalámbrica se conoce como ataque de denegación de servicio. Asimismo, conectarse a redes inalámbricas consume energía. Incluso cuando los dispositivos inalámbricos periféricos tengan características de ahorro de energía, un hacker puede llegar a enviar suficientes datos cifrados a un equipo como para sobrecargarlo.

Muchos periféricos portátiles, como los PDA y ordenadores portátiles, tienen una duración limitada de batería. Por lo tanto, un hacker puede llegar a provocar un consumo de energía excesivo que deje al dispositivo inutilizable durante un tiempo. Esto se denomina ataque de agotamiento de batería.

Actualmente cualquier empresa tiene que hacer frente a una mayor demanda de accesos inalámbricos, ya sea por parte clientes, proveedores o empleados. Desafortunadamente, también los hackers continúan intentando lograr acceder dentro de las redes. Para proteger una red inalámbrica, primero hay que conocer las principales amenazas a las que se ven afectadas y que ponen en riesgo la seguridad del usuario. Las reúne WatchGuard con motivo del lanzamiento de un nuevo punto de acceso inalámbrico para empresas.

Los usuarios que son víctimas de un Rogue AP son susceptibles de verse afectados por código malicioso, que a menudo pasa desapercibidos. La colocación de malware consiste en que los usuarios que se unen a una red inalámbrica de invitados son susceptibles de, sin saberlo, llevarse malware no deseado de algún vecino con malas intenciones. Una táctica común utilizada por los hackers es colocar una puerta trasera en la red, lo que les permite regresar más tarde para robar datos confidenciales. Los ataques móviles, tales como Stagefright de Android, se propagan de un usuario a otro, incluso sin que la "víctima cero" lo sepa.

En la actualidad hay muchas formas de ser víctima de un ataque cibernético con el simple hecho de conectarse a cualquier tipo de red inalámbrica estas expuesto a cualquier tipo de amenazas y virus, por eso hemos decididos estudiar este tema para comprender aún más como es el uso de las redes inalámbricas todos los tipos de vulnerabilidades y cómo es que estos se roban la información de los usuarios para así poder brindar la ayuda e

información a las personas que menos tiene conocimientos en redes informáticas para qué así ellos puedan estar o tener un poco más de seguridad la conectarse a una red inalámbrica y navegar usando dicha red.

1.6 DELIMITACIÓN DEL ESTUDIO

(Jurado, 2023) Explica:

En el mundo actual, dominado por la tecnología y las redes informáticas, es fundamental saber qué es seguridad informática y poder utilizarla eficazmente. Los sistemas, archivos importantes, datos y otras cosas virtuales importantes están en riesgo si no hay seguridad para protegerlos. Tanto si se trata de una empresa de TI (Acrónimo de Tecnologías de la Información) como si no lo es, todas ellas deben estar protegidas por igual. Con la mejora de la nueva tecnología en seguridad informática, los atacantes tampoco se quedan atrás. Están utilizando cada vez mejores técnicas de hacking y se dirigen a los puntos débiles de muchas empresas.

La seguridad informática, es un proceso de protección de datos sensibles, redes y aplicaciones de software contra un posible ataque cibernético. Los ataques cibernéticos pueden ser considerados como una explotación de recursos, acceso no autorizado a los sistemas, ataques de rescate para encriptar datos y extraer dinero.

El uso de redes inalámbricas no está exento de riesgos de ataques cibernéticos o hackeos, especialmente cuando nos conectamos a redes WiFi públicas. En el ámbito empresarial esto puede tener consecuencias graves, como el robo de información, mientras que en las redes personales puede darse la duplicación de identidad y el fraude.

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. La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red.

La macro localización: es en la cuidad de Frontera Comalapa que está ubicada en los puntos fronterizos de Chiapas y Guatemala perteneciente a unas de las localidades de la ciudad de Comitán de Domínguez, una ciudad muy transitada por el paso de fronteras.

Frontera, es un adjetivo refiriéndose al límite que hace con la República de Guatemala y el término Comalapa proviene de la voz náhuatl: Comalapan En el agua de los comales, que deriva de las voces: Comalli, comal; Atl, agua; y -Pan, adverbio de lugar. Pero también se considera que su nombre se debe al recuerdo de la extinta San Juan Comalapa, y está sobre el paraje Cushú, que se encontraba cerca de Tecpan, Guatemala; es decir en la frontera.

La localidad de Frontera Comalapa está situada en el Municipio de Frontera Comalapa (en el Estado de Chiapas). Hay 21,727 habitantes. Es el pueblo más poblado en la posición número 1 de todo el municipio. Frontera Comalapa está a 645 metros de altitud.

La Micro localización: será en el instituto universitario de “Universidad del Sureste, campus Frontera Comalapa” que está ubicado en barrio la lima en la carretera internacional en libramiento de la ciudad de Comalapa aquí será donde obtendremos la mayor parte de nuestra investigación.

CAPÍTULO 2: MARCO DE REFERENCIA

"PROTOCOLO EN REDES INFORMÁTICAS"

2.1 MARCO FILOSOFICO-ANTROPOLOGICO

Desde los años 70 se vienen haciendo experimentos para lograr la conexión entre dispositivos de manera inalámbrica, pero fue en 1979 cuando la gente de IBM publicó los resultados de sus experimentos de conexión inalámbrica mediante infrarrojos en una fábrica suiza, este estudio se consideró como el punto de partida de las redes inalámbricas.

De ahí en adelante los estudios realizados en este campo fueron hechos utilizando altas frecuencias y fue cuando el FCC asignó las bandas IMS de 902 – 928 MHz, 2,4– 2,4835 GHz y 5,725 – 5,850 GHz a las redes inalámbricas basadas en Spread Spectrum. Al hacerse la asignación de bandas de frecuencias, se vio favorecida la actividad en las empresas, ya cuando se tuvo este respaldo las redes inalámbricas empezaron a llegar a otros lados diferentes de los laboratorios, e iniciaron el camino hacia el mercado.

Entre 1985 y 1990 se realizaron trabajos de investigación más que todo orientados a la parte de desarrollo, hasta que en el año de 1991 se publicaron trabajos referentes a redes inalámbricas operativas cuya velocidad era un poco mayor de 1Mbps, el cual era el mínimo establecido por la IEEE 802 para que la red sea considerada una LAN.

Las ondas de radio fueron usadas de otra forma para crear lo que se conoce como Bluetooth que eran ondas de radio corta, la ventaja de estos dispositivos es que requieren de poca energía para su funcionamiento. A

pesar de que estas redes inalámbricas simplificaban la vida cotidiana siempre estaba presente la restricción de la distancia, para resolver esto se creó un nuevo estándar de conexión también usando ondas de radio llamado WiMAX el cual permite la operatividad a grandes distancias (50 - 60 Km) y altas velocidades de transmisión de datos (superiores a 20Mbps).

Redes Inalámbricas Hoy Día

Actualmente las redes inalámbricas juegan un papel importante en el día a día de las personas, debido al creciente mercado de computadoras portátiles la necesidad de conectarse no solo a internet sino también estar en red con otras personas sin necesidad de cables ha ido aumentando debido a que muchos dependen de esto para realizar las actividades de su vida cotidiana (revisar el correo electrónico, buscar información para informes u otras asignaciones), ya que se puede dar el caso de que la actividad que las personas realizan no sea dentro de una oficina sino que le demande el estar desplazándose de un lugar a otro y para eso necesitan el acceso a internet de una forma sencilla y sin la necesidad de estar conectados mediante un cable.

En sus inicios, las redes inalámbricas eran de difícil acceso para todo el mundo por el alto costo que representaba el instalar un punto de acceso a la red, pero gracias a la evolución que ha ido teniendo la tecnología en el campo de dispositivos para facilitar la conexión inalámbrica ahora es común encontrar acceso a redes inalámbricas en lugares claves y de forma gratuita.

Hoy en día, las redes inalámbricas son usadas en todas partes y hacen parte vital de la estructura de comunicaciones e informática de una empresa u organización, lo que se busca con ellas no es reemplazar las redes cableadas, sino que son utilizadas como complemento de estas ya que hay

lugares en donde estas no pueden tener acceso y debido a la facilidad de instalación de dispositivos para la conexión a la red los cuales ya funcionan con PoE.

Otra aplicación de las redes inalámbricas es cuando se presenta el caso de la reconfiguración la topología de la red sin añadir costos adicionales, esta es una solución muy usada en entornos cuyo cambio es constante y los cuales necesitan de una estructura de red flexible que pueda adaptarse a los cambios que se vayan presentando.

El protocolo de conectividad inalámbrica WiFi no se encuentra estático y ya presenta una nueva versión que la IEEE ha liberado con la denominación 802.11n la cual trae consigo la solución a una de las desventajas más grande de la tecnología WiFi y es el aumento de la velocidad de conexión inalámbrica a una velocidad de 300 Mbps con un alcance 70 metros interior, lo que hace más óptima y eficaz la conexión, si la comparamos con la velocidad de conexión del estándar 802.11g establecido en 54 Mbps

Las principales características promocionales del 802.11n son:

- MIMO (Multi-In, Multi-Out) generando canales de tráfico simultáneos entre las diferentes antenas de los productos 802.11n.
- Canales de 20 y 40 Hz, los cuales permiten el incremento de la velocidad.
- El uso de las bandas de 2,4 y 5 GHz simultáneamente, con esto se disminuirán los problemas ocasionados por las interferencias en la banda 2,4 GHz, y optimizara el uso de las bandas.

Tipos de tecnología Wi-Fi:

Tecnología Wi-Fi	Banda de frecuencia	Máximo de ancho de banda o velocidad de datos
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	**2,4 GHz, 5 GHz, 2,4 o 5 GHz (seleccionable), o 2,4 y 5 GHz (concurrente)**	450 Mbps

2.2. Antecedentes de la investigación.

Con las siguientes tesis que se presentaran a continuación nosotros reforzaremos más nuestro conocimiento y bases sobre las redes informáticas, con el fin de poder crear o investigar mejor el tema y comprenderlo para poder tener un trabajo de investigación más sofisticado y estructurado.

“Tesis de referencia”.

1. Nombre de la tesis: Redes inalámbricas.

Autores: Miguel Andrés Maturana, Andrés Alonso Rodríguez.

Año: 2003.

Objetivo: Introducir al conocimiento de conceptos de WLAN, su administración y su aplicación en las técnicas de acceso celulares, mediante una documentación escrita, que permita, a personas, no solo con

conocimientos previos, sino también a “principiantes” vincularse a este desarrollo tecnológico actual.

Hipótesis: En la facultad de Sistemas de la CUTB se conoce poco de este hecho, pero la idea de búsqueda de información de los sistemas inalámbricos, esta. Y como no está descrito como tal, serviría de mucha ayuda para la universidad y su desarrollo hacia el futuro la realización de este documento.

Discusión: Para ofrecer mejor adecuación al estudiante, en su forma de investigar, consultar y realizar sus tareas, muchas escuelas se agregan a la red mundial de computadoras, por supuesto, la Internet, ayuda en la enseñanza del estudiante. Las WLAN entran en acción debido al bajo costo de inversión en comparación con las redes alámbricas. Un estudio muestra que en las 11.000 escuelas de Estados Unidos de pre-escolar a secundaria, gastan 6.200 millones de dólares al año en tecnología, incluyendo Software y Hardware; de estos, aproximadamente 500 millones son invertidos en tecnología móvil cada año del 2001 al 2002, y se espera que siga aumentando, e incluso las escuelas de menos recursos rurales y urbanas buscan financiamiento para disminuir la brecha del conocimiento por medio de esta tecnología.

Resultados: La solución al primer problema, supuso que los organismos más relevantes en materia de Telecomunicaciones se pusieran de acuerdo para definir y plantear una solución tanto para la unificación de todos los estándares de comunicación vía radio como para la creación de un nuevo sistema que soportase un mayor ancho de banda con calidad digital.

2. Nombre de la tesis: “Operación y manejo de una red inalámbrica en la compañía FMI Internacional”.

Autor: Iván Montiel Dávila.

Año: 2006.

Objetivo: Describir la importancia de hacer uso de la tecnología en favor de la industria, las ventajas de esta en cuanto a desarrollo y funcionalidad y dar a conocer como es que influyó de manera particular en una compañía tan grande a nivel internacional.

Hipótesis: El desarrollo de este trabajo es muy importante, ya que, dado el proyecto que se realizó en esta compañía, se pueden dar a conocer alternativas para otras compañías dedicadas al mismo trabajo o a diferentes, puesto que un equipo de cómputo y la gran diversidad de programas y paquetes que existen están para cumplir con las expectativas de cualquier negocio y de la industria en general.

Discusión: Las redes son cada vez más indispensables, ya no pertenecen a un grupo selecto de personas. Actualmente la mayoría de los países del mundo están conectados a una red que los une. Este capítulo se enfocará a describir la compañía como tal, su historia, sus actividades principales, sus objetivos y lo más importante, el por qué es una de las compañías más importantes en Estados Unidos en cuanto a distribución y por qué se ha esforzado a través de los años en implementar nuevas tecnologías de comunicación y transporte para bien de sus clientes.

Resultados: Las redes inalámbricas son cada vez más indispensables, ya no pertenecen a un grupo selecto de personas. Como conclusiones finales de éste proyecto, hay que mencionar puntos muy importantes como: Que cualquiera que sea el proyecto de mejorar la calidad en servicios y rendimiento de la industria en general, es muy importante el no tener miedo al cambio de implantar nuevas tecnologías y de querer estar entre los mejores haciendo uso de nuevas herramientas de información.

3. Nombre de la tesis: Análisis de la seguridad en redes.

Autor: Roberto Amado Gimenez.

Año: 2008.

Objetivos: Es por ello que el objetivo de este proyecto se centra en el estudio general del estado de esta tecnología y sus herramientas de protección, estudiando el nivel de seguridad alcanzable, los métodos de ataque y soluciones para evitar las intrusiones. Se realizará un repaso por los diferentes métodos de cifrado, las herramientas de ataque más populares y los métodos de protección utilizados.

Hipótesis: supone uno de los estándares de comunicación por radiofrecuencia más utilizados y populares para redes de área local. No es extraño que dispositivos como ordenadores portátiles, PDA's, consolas de videojuegos, móviles o incluso maquinaria industrial hagan uso de este estándar como solución inalámbrica para interconectar y transferir cualquier

tipo de información, datos, voz o video. Como ejemplo de ello, basta con realizar una búsqueda mediante su ordenador portátil de las redes inalámbricas disponibles en su entorno, para darse cuenta de la gran acogida que esta tecnología ha tenido en la sociedad.

Discusión: Todo apunta a que el crecimiento y despliegue de este tipo de redes seguirá aumentando en los próximos años. Encuestas realizadas por la Asociación para la Investigación de los Medios de Comunicación (AIMC) reflejan que el 52 % de los usuarios de Internet en 2007 obtuvo acceso a la red de redes a través de este tipo de tecnología, frente al 43% del año anterior. Pero no solo los usuarios domésticos adquieren productos de la norma, instituciones, PYMEs y grandes compañías cada vez más hacen uso del estándar esta tecnología como solución de comunicación inalámbrica.

Resultados: Por lo tanto y como conclusiones obtenidas tras el análisis realizado, si no se utiliza cifrado de datos , se debe activar un protocolo de seguridad robusto como WPA o WPA2 siendo este último más aconsejable. En el caso de que el dispositivo no permita habilitar los protocolos anteriores, se sugiere la utilización de WEP extremando la seguridad en el entorno aplicado, complementando el uso del protocolo con otras medidas de seguridad como: segmentación de la red , aislamiento de la subred inalámbrica del resto de la red, utilización de firewalls, etc. Estas sugerencias de seguridad son fruto en parte, de la experiencia laboral del autor del proyecto tras numerosas auditorias de seguridad inalámbrica y test de penetración, realizadas a importantes compañías, de sectores tan diversos como industrias textiles, ingeniería electrónica, ferroviarias o de automoción. Obteniendo la posibilidad de penetrar, en la mayor parte de los casos, hasta el segmento de servidores corporativos simplemente sentado en el perímetro exterior de la compañía auditada.

2.3 Marco teórico.

2.3.1: Con base a la temática de estudio y a los antecedentes evidenciados con respecto el problema generado por usar redes inalámbricas de conexión a internet obsoletas o con protocolos inseguros; mientras que desde 1969 se da por fecha de inicio a la creación de los primeros pinos de lo que conocemos hoy como internet y que en su inicio fue nombrado ARPAnet1, seguidos de toda la evolución desde ser una red únicamente con fines militares a volverse finalmente una tecnología al alcance de millones de usuarios para hacer búsquedas en línea y ejecutar tareas de diferentes tipos. En 1997 se lanzó públicamente lo que se conoce hoy como wifi al mundo y según la memoria colectiva no es sino hasta aproximadamente el año 2005 o 2006 en que las redes inalámbricas de conexión a internet llegan a todo el continente latinoamericano; simplemente con esa observación podemos darnos cuenta de que en materia de tecnologías, dispositivos y seguridad informática nuestro país no ha sido pionero y ha tardado en ponerse a la vanguardia en estos asuntos. Es por ello por lo que no es sorprendente darse cuenta de que en diferentes sectores de la ciudad capital puedan encontrarse dispositivos de conexión inalámbrica obsoletos o con protocolos inseguros; cuando aún existen zonas apartadas de la ciudad en donde no llega la conexión o el servicio es paupérrimo on ello podemos ver que es muy importante que expertos en seguridad informática analicen minuciosamente las causas por los cuales pueden estarse efectuando dichos ciberataques. A pesar de que existen técnicas muy avanzadas para la ejecución de malware y ciberataques, en muchos casos se tiende a olvidar los puntos claves y se dan por obvias tareas tan sencillas como solicitar a un ISP la actualización de su hardware. Es muy importante recordar que no sólo basta con una seguridad perimetral o por capas en las compañías, sino que sin la concientización del usuario final que se conecta desde su casa a raíz de la pandemia, se está generando una brecha de seguridad muy extensa dando por hecho que el usuario tiene sus tecnologías y dispositivos actualizados cuando no se le ha

dado la capacitación y advertencia sobre el uso de estos. Aunque el WarDriving no esté catalogado como un ataque un delito ya que su funcionalidad en sí misma es recolección de datos en forma pasiva, sí existen.

(Jiménez Bonilla & Leaño Suárez, 2011) Mencionan:

2.3.2: A la hora de comparar las redes inalámbricas con las redes de alambicas encontramos que existen ciertos puntos en contra de las redes inalámbricas, los principales inconvenientes son: Velocidad13: Las redes inalámbricas Wi-Fi14 trabajan a 11 Mbps, pero existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi; mientras que las redes cableadas ya llegaron hace unos cuantos años a los 100 Mbps. Seguridad15: Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Muchas redes Wi-Fi sufren accesos no debidos, gracias a la inexperiencia de quienes las instalaron y no configuraron correctamente los parámetros de seguridad, trayendo esto como consecuencia, que cualquier persona con dispositivos de menor jerarquía, como por ejemplo Palms, PDA o pequeños dispositivos portátiles, solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Propensión a interferencias: Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GHz; Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Esto trae como consecuencia que no se cuente con una frecuencia completamente limpia para que la red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros

equipos, menor será el rendimiento de la red. Aclarando que, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan.

2.3.2.1: La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido. Incertidumbre tecnológica. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi. Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se acredite esta nueva tecnología, se deje de utilizar la actual. Los productos que salen al mercado están marcados por las necesidades del cliente y, aunque existan incógnitas o dudas con respecto al uso de los que ya están comercializados, los fabricantes no querrán perder el impulso que ha impuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales.

2.3.2.2: Una pérdida de disponibilidad en una red inalámbrica puede ser causada por dos factores, o interferencia o inundación de datos. La interferencia ocurre cuando un atacante deliberadamente transmite una señal electromagnética que satura las señales de los dispositivos inalámbricos. También puede haber interferencia accidental, causada por otros dispositivos que usan la misma frecuencia, como teléfonos inalámbricos o un horno microondas, la interferencia tiene como consecuencia una interrupción o una pérdida completa de la comunicación, porque la señal no puede ser transmitida correctamente. Un atacante también puede causar una pérdida en la disponibilidad al provocar una inundación de datos, este tipo de ataque ocurre cuando se transmiten una gran cantidad de paquetes de datos a un punto de acceso u otro dispositivo inalámbrico, teniendo como consecuencia que el dispositivo no pueda responder a todos los paquetes y no tenga una operación normal. Puede

haber una inundación de paquetes no intencional, si un usuario monopoliza la capacidad de la red por ejemplo descargando archivos muy grandes. En este tipo de ataque la red puede degradar su rendimiento o incluso fallar completamente. Tanto en las redes cableadas como en las redes inalámbricas, la integridad de los datos, es algo que normalmente se le deja a las aplicaciones en niveles superiores para que lo verifiquen, pocas veces se hace un control de integridad en niveles inferiores o se hace usando herramientas que pueden ser vulnerables. Las redes inalámbricas 802.11 usan el mecanismo de integridad CRC32, este mecanismo es vulnerable porque se pueden modificar bits sin ser detectados por el CRC32. Esto puede llegar a extremos hipotéticos en los que un atacante pueda modificar un mensaje de correo electrónico sin ser detectado. Para proteger la integridad se recomienda usar 802.11i, que utiliza códigos de integridad del mensaje, estos códigos se cifran y no es posible modificar los datos transmitidos, sin que sea detectado algún cambio en los mismos. Un ataque posible en las redes inalámbricas es el de hombre en el medio, en este ataque, un atacante con un equipo básico se hace pasar por un PA legítimo, mientras restringe la disponibilidad o emite su señal más fuertemente que el PA legítimo, de esta forma, las ESTs se conectaran al PA del atacante, este PA recibe los datos de autenticación y simultáneamente puede autenticarse al PA original, actuando como un puente transparente entre las partes, de esta forma el atacante puede recolectar todos los datos que se transmitan, modificarlos, retardarlos, extraviarlos, sin ser detectado, y efectivamente creando pérdida de autenticidad en la información tanto para la EST como para el PA legítimo, puesto que las dos partes si no están bien protegidas no tienen forma de detectar fácilmente este ataque. Todo este ataque se facilita en las redes que usan una conexión anterior a una RSNA, en una RSNA, la autenticidad se protege luego de crear la asociación entre las partes, exigiendo una autenticación mutua, de esta forma el ataque de hombre en el medio no puede ser realizado, a menos de que el atacante tenga los medios para suplantar los certificados y métodos usados para

garantizar la autenticidad de las partes. Y Debido a que las redes inalámbricas utilizan un medio abierto, el cuidado que se debe tener con la confidencialidad de la información debe ser mayor al que se tiene en otros tipos de transmisiones y es más sensible que en una red cableada Un atacante que se ubique dentro del radio de alcance de un PA, puede escuchar pasivamente la información que se transmite, sin levantar sospechas, mientras monitorea el tráfico que flota en el aire, puede ver información sensible, como nombres de redes y claves, datos de la configuración de la red e incluso analizando solamente la cantidad de tráfico transmitida en un periodo de tiempo deducir si se está transmitiendo una videoconferencia o una conversación por chat. Este riesgo de ser escuchado sin ser detectado, se debe a que las señales de IEEE 802.11 pueden viajar más allá del radio de servicio previsto, permitiendo que un atacante pueda monitorear la información, incluso si no utiliza una antena especial para ello. Monitorear el tráfico de una red inalámbrica es sencillo, si se usa una herramienta como un analizador de protocolos o sniffer, esta herramienta permite que alguien pueda recibir el tráfico inalámbrico de las redes que se encuentran a su alcance y es posible porque la mayoría de las redes inalámbricas no están debidamente protegidas o están protegidas con protocolos no seguros, que le permiten a un atacante tener acceso a los datos que se transmiten sin mayor dificultad. Para proteger la confidencialidad es necesario evitar protocolos poco seguros como WEP y en lo posible usar el estándar IEEE 802.11i en la versión para hogar o empresa dependiendo del caso. Hasta ahora no existe un método algebraico para descifrar la clave que se usa en los casos de CCMP y TKIP, aunque se recomienda CCMP por usar un algoritmo más fuerte, solo se tienen noticias de ataques basados en diccionario, por lo tanto sigue siendo muy importante seleccionar una contraseña lo suficientemente larga y compleja como para que un ataque de diccionario no sea viable. ¿Qué es un ataque de diccionario? Es un método por el cual, se recorre una serie de palabras o combinaciones de letras, números y símbolos, con el fin de

usarlos como palabra clave y generar un texto conocido cifrado, si el resultado que se obtiene es igual a algún texto que se encontraba cifrado, se ha encontrado la llave usada, si es diferente se continua la búsqueda, es posible generar o descargar de internet estos diccionarios, pero no son eficaces ante una contraseña cuidadosamente seleccionada.

(García, 2022) Expresa:

2.3.3: Actualmente las conexiones inalámbricas, específicamente las conexiones definidas en la IEEE 802.11x o popularmente conocidas como redes Wifi, se han convertido en parte esencial de las comunicaciones en múltiples entornos. Es así como se encuentran redes Wifi en restaurantes, bibliotecas, aeropuertos, bancos y muchos lugares más; sin embargo, no se puede hablar de conexiones sin involucrar a los dispositivos de los usuarios finales donde hoy en día prácticamente todo puede estar conectado a la red; el Internet de las Cosas (IoT) como nueva tecnología de interconexión de dispositivos ha hecho que la vida cotidiana esté interconectada con múltiples servicios. Hoy en día es prácticamente imposible imaginar un mundo sin conexiones a la red ya que sería muy difícil, por no decir imposible realizar muchas de las actividades que hacen que el mundo se mueva hoy en día; por ejemplo, piense que sin los servicios de red muchas operaciones bancarias no se podría realizar o por ejemplo no sería tan fácil llevar el funcionamiento de las empresas debido a la pandemia por COVID-19 que obligó a que todo el mundo se incluyera en el teletrabajo y la oficina en casa para seguir trabajando y mantener las operaciones globales. Aunque las tecnologías Wifi no son nuevas para nadie, ya que se han implementado desde hace más de 30 años gracias a la creación del IEEE802.11, la evolución de estas redes ha traído consigo cambios relacionados con sus mecanismos de seguridad desde que se vulneró el protocolo WEP, de ahí el lanzamiento de WPA, WPA2 y otras versiones que

finalmente se liberaron sin ser completadas y siguieron desplegando vulnerabilidades en todas las infraestructuras donde se utilizan las redes Wifi.

2.3.3.1: Una red Wifi con contraseña no es garantía de seguridad; así se ha demostrado en múltiples pruebas de concepto en donde un ciberdelincuente podría comprometer fácilmente la seguridad de una red y por tanto toda la información que circula por ella. Por otro lado, las redes Wifi están vinculadas a otros dispositivos de red que tienen conectados múltiples dispositivos no inalámbricos como servidores, impresoras, redes VoIP en el caso de entornos corporativos y dispositivos como televisores, sistemas de CCTV, alarmas y otros en entornos domésticos. Por todo ello, existen múltiples técnicas de recopilación de información sobre objetivos inalámbricos para muchos ciberataques; sin embargo, es posible hacer uso de estas técnicas para hacer una revisión de las configuraciones más comunes y de las implementaciones erróneas de las redes Wifi con el fin de proporcionar metodologías de mitigación y recomendaciones para los usuarios que hacen uso de este tipo de redes prestadas o públicas. Desde la invención del WiFi se han venido exponiendo al público diferentes tipos de protocolos de seguridad para proteger las conexiones. Los protocolos de seguridad de las redes inalámbricas son aquellos con los cuales se logra proteger, cifrar los datos y el tráfico que viajan por la red mientras estamos conectados a una red inalámbrica. Desde 1997 hasta la actualidad se han publicado 4 protocolos diferentes en los que encontramos WEP, WPA, WPA2 y WPA3 cada uno con distintas características y cualidades, pero con la particularidad que su desarrollo no fue lo suficientemente profundo como para garantizar que ningún ciberdelincuente pueda acceder a ella. La primera norma IEEE para el Wi-Fi se publicó en 1997 y se conoce como IEEE 802.11. Tenía grandes deficiencias, ya que el rendimiento máximo era de 2 Mbps. En 1999 se introdujeron dos modificaciones en la norma original.

802.11a funcionaba en la banda de 5 GHz y utilizaba OFDM, mientras que 802.11b seguía en la banda de 2,4 GHz y utilizaba DSSS. La OFDM se ha adoptado en el ámbito de la Wi-Fi, con estándares como 802.11a, 802.11n y 802.11ac, entre otros. También se ha elegido para el estándar de telecomunicaciones celulares LTE / LTE-A, y además ha sido adoptado por otros estándares como WiMAX y muchos más. La multiplexación por división de frecuencias ortogonales también se ha adoptado para una serie de estándares de radiodifusión, desde la radio digital DAB hasta los estándares de difusión de vídeo digital, DVB. También se ha adoptado para otros sistemas de radiodifusión, como la Radio Digital Mundial, que se utiliza para las bandas de onda corta y media larga. Aunque la multiplexación por división de frecuencias ortogonales (OFDM) es más complicada que las formas anteriores de formato de señal, ofrece algunas ventajas claras en términos de transmisión de datos, especialmente cuando se necesitan altas velocidades de datos junto con anchos de banda relativamente amplios.

2.3.3.2: Cuando se presenta una pérdida de confidencialidad, potencialmente se pierde posesión exclusiva sobre la información, porque una vez que la confidencialidad ha sido comprometida un atacante puede descifrar todos los datos que se transmiten, leer correos electrónicos, reproducir conversaciones por voz IP, replicar la sesión de navegación web que se esté llevando a cabo, capturar contraseñas y archivos que se transmitan. La pérdida de posesión es potencial porque puede que el atacante guarde toda la información sin revisar su contenido, es ese caso el atacante no ha vulnerado efectivamente la posesión de la información a menos de que elimine los datos originales, en un proceso destructivo de recaudo de datos. Pero además de la pérdida de posesión causada por una pérdida de confidencialidad, también existe el caso en que efectivamente se pierde posesión sobre los dispositivos, un computador portátil, un organizador personal o un PA, además de la información que pueden

contener estos dispositivos se pierde la configuración de la WLAN, comprometiendo otros niveles de seguridad, con un organizador personal un atacante puede acceder a una red, haciéndose pasar por un usuario autorizado, o con los datos que se encuentran en un PA puede descifrar la clave usada por la red inalámbrica y luego intentar usarla. La pérdida de posesión física de los equipos se puede prevenir con alarmas o seguridad física, pero luego de que se pierda la posesión es importante informar sobre la pérdida, para que se niegue el acceso a ese dispositivo y se cambien las claves de red que estén en uso, incluso además de verificar la clave es importante verificar la identidad del usuario. De esta forma aunque se presente una pérdida de posesión, se mitigan futuras pérdidas potenciales. También es importante tener un proceso al momento de retirar dispositivos de la red, botarlos inmediatamente es una mala idea, tanto para puntos de acceso, como para computadores. El estándar 802.11i introduce el concepto de redes con seguridad robusta, en inglés Robust Security Network (RSN), una RSN es una red inalámbrica que solo permite la creación de asociaciones a redes con seguridad robusta, en inglés Robust Security Network Asociations (RSNA). Una RSNA es una conexión lógica entre dos dispositivos 802.11 que se establece a través del esquema de manejo de claves 802.11i, este esquema se llama apretón de manos de cuatro tiempos, que es un protocolo que valida que ambos dispositivos compartan una llave maestra par, en inglés Pairwise Master Key (PMK), que las llaves temporales se sincronicen y confirma la selección y configuración de los protocolos de confidencialidad e integridad. Los dispositivos obtienen la PMK de dos formas, o la PMK está configurada en cada uno, si es así, se llama llave pre-compartida, en inglés Pre-Shared Key (PSK), o se obtuvo como efecto de una autenticación exitosa contra un servidor de autenticación usando el protocolo EAP que es un componente de la especificación 802.1X que sirve para controlar el acceso. Hay dos componentes en la definición de 802.1X que son usados para la creación de RSNAs, los servidores de autenticación y el control de acceso de 802.1X,

el estándar IEEE 802.1X provee un marco de operación para el control de acceso que permiten la existencia de un servicio centralizado de autenticación mutua.

2.3.3.3: Este estándar originalmente fue diseñado para redes cableadas y prevenir el acceso a usuarios no autorizados en ambientes abiertos, como un campus universitario, 802.1X permite bloquear a los usuarios hasta que estos se autentiquen correctamente, de esta forma se controla el acceso a los recursos de la WLAN. La figura-8 muestra una vista conceptual de IEEE 802.1X, presentando todos los componentes fundamentales de 802.11i: varias EST, un PA y un servidor de autenticación, las estaciones buscan ser autenticadas y se denominan suplicantes y el PA es el que facilita la autenticación por esto se denomina el autenticador. Solamente hasta que haya una autenticación exitosa entre la EST y el servidor de autenticación, las comunicaciones de la EST son desbloqueadas por el PA, como el PA está en la frontera entre la red inalámbrica y la red cableada, esto evita que una EST no autenticada acceda a la red cableada. La técnica usada para bloquear las comunicaciones se conoce como control de acceso basada en el puerto. IEEE 802.1X puede distinguir los flujos de datos de paquetes de autenticación y paquetes normales de datos, solamente deja pasar los paquetes de autenticación por un puerto no controlado del PA, los demás paquetes pasan por un puerto controlado que puede bloquear el acceso. 802.11i extiende estas capacidades para que el PA bloquee la comunicación hasta que las claves estén debidamente utilizadas. Es así que 802.11i solamente permite que un PA no autorizado pueda solo ver datos de autenticación que ya están cifrados.

(Buettrich & Escudero Pascua, 2007) Expresan:

2.3.4: La topología de una red define la distribución física y lógica de la conexión entre sus nodos. Dependiendo del propósito y naturaleza de una red, una topología puede ser más apropiada que otra. Antes de decidir la topología de su red, usted debe tener claramente definidos los puntos siguientes:

- ¿La red debe ser escalable o se debe diseñar sólo para algunos nodos?
- ¿La eficiencia de los costos es más importante que la confiabilidad y la redundancia?
- ¿Qué rango de cobertura se requiere?
- ¿Para cúantos nodos?
- ¿Cómo es el terreno del sitio en donde se implementará?

2.3.4.1: Todas estas preguntas y muchas más, deben ser consideradas en el proceso de diseño de la topología de una red cableada o inalámbrica. Los cinco puntos principales a recordar de esta unidad se pueden resumir como sigue: 1. La mayoría de las implementaciones de redes inalámbricas están basadas en: Topología de estrella, árbol, línea (repetidores). 2. Una implementación típica de red inalámbrica incluye:

- Puntos de acceso y/o enrutadores.
- Clientes inalámbricos (computadores portátiles, PDA, equipos de vigilancia, teléfonos inalámbricos de VoIP). 3. La implementación se puede realizar de dos modos: ad hoc o infraestructura. 4. La configuración básica incluye: Modo, Identificador de la red, Canal, IP (para características de gestión y enrutamiento) y dirección(es) MAC (opcional). 5. Muchas de las implementaciones inalámbricas se basan en más de una topología.

Luego de la ratificación del estándar 802.11i en 2004, IEEE 802.11 comienza a ofrecer dos clases generales de capacidades en seguridad para

las WLAN, la primera clase, es la seguridad anterior a RSN, que incluye las capacidades originalmente ideadas para el estándar IEEE 802.11: autenticación basada en sistema abierto o por clave compartida para validar la identidad de la estación inalámbrica y WEP para proteger la confidencialidad del tráfico. La segunda clase de seguridad incluye mecanismos para crear RSN. Una RSN incluye mejoras en la seguridad para afrontar todas las debilidades conocidas de WEP y provee una protección robusta para el enlace inalámbrico, incluyendo integridad de datos y confidencialidad. [3] La figura-9 presenta una taxonomía de alto nivel de los mecanismos anteriores a RSN y de RSN. 802.11i define dos protocolos RSNA para la confidencialidad e integridad de datos. Protocolo de integridad de llave temporal, en inglés Temporal Key Integrity Protocol (TKIP) y Protocolo de modo contrario con cifrado en bloque encadenando MAC, en inglés Counter Mode with Cypher Block Chaining MAC Protocol (CCMP). TKIP fue creado para permitir que los dispositivos existentes pudieran afrontar las debilidades de WEP. TKIP puede ser implementado a través de una actualización de software, sin requerir cambios en el hardware en los PA o en las ESTs. Sin embargo TKIP usa RC4 (el mismo cifrado de WEP) y el código de integridad de mensaje Michael MIC, que tienen debilidades conocidas. Por esto TKIP no es la mejor alternativa cuando se requiere la mejor protección, en esos casos es mejor usar CCMP. Pero CCMP es un protocolo que computacionalmente es más exigente y no se puede implementar en dispositivos anteriores a RSN. Es obligatorio que todos los dispositivos que soporten RSNA implementen CCMP, TKIP es opcional. TKIP TKIP es un protocolo de cifrado que amplía el protocolo WEP en hardware anterior a RSN sin causar una degradación significativa en el desempeño. TKIP ofrece las siguientes características de seguridad para WLAN 802.11. Protección de la confidencialidad usando el algoritmo de cifrado RC4. Protección contra varios tipos de ataques contra la integridad de los datos, usando un algoritmo que genera un código de integridad para los mensajes (MIC). Prevención del reenvio de paquetes de datos, por

medio de una técnica que secuencia los paquetes. Uso de una nueva llave con cada paquete de datos, para prevenir ataques como Fluhrer-Mantin-Shamir (ataque FMS) que es uno de los principales ataques que compromete la confidencialidad en WEP. Implementación de medidas cuando una EST o un PA encuentra un paquete de datos con un error MIC, lo cual es un indicador fuerte de que un ataque puede estar ocurriendo. Al igual que TKIP, CCMP fue diseñado para afrontar las debilidades que tiene WEP, con la diferencia de que CCMP fue diseñado sin pensar que fuera compatible con los dispositivos anteriores a RSN. Se considera que CCMP es la solución a largo plazo para la creación de RSNs para WLANs. CCMP se basa en CCM que es un modo autenticado genérico de cifrado en bloque de AES (AES es un estándar de cifrado usado mundialmente y de uso obligatorio en las agencias de gobierno de los Estados Unidos, en inglés Advanced Encryption Standard). CCMP protege la integridad de los datos transmitidos y también de los encabezados del paquete de datos usando una TK de 128 bits para proteger el canal. CCMP tiene las siguientes características de seguridad: Una sola llave criptográfica para manejar la confidencialidad y la integridad de los datos, así se minimiza la complejidad y se maximiza el desempeño. Protección de la integridad del encabezado del paquete de datos y de los datos, además de la confidencialidad de los datos. Computación de algunos parámetros antes de recibir los paquetes y así posibilitar una comparación rápida cuando lleguen, lo que reduce la latencia. Computacionalmente liviano, lo que permite que pueda ser implementado en software o en hardware. Poca sobrecarga relacionada con la seguridad de los paquetes. No hay problemas por patentes pendientes o existentes.

(TUQUERES, 2019) Explica:

2.3.5: Con el objeto de efectuar una comparación entre las tecnologías inalámbricas descritas, tomando en cuenta sus características, ventajas y desventajas, en los siguientes numerales se realizará un análisis por pares de tecnologías ZigBee y Z-Wave son dos de los principales protocolos inalámbricos utilizados en los productos de los edificios inteligentes mediante WPAN. En tal sentido es necesario analizar ambas tecnologías para determinar los aspectos necesarios que guíen la elección de una u otra tecnología. Una de las fortalezas y debilidades de ZigBee es su protocolo abierto, aspecto beneficioso ya que el código puede ser verificado, sin embargo y en contraposición, al tener un protocolo abierto existe la posibilidad de modificar el código para que se ajuste a necesidades particulares. A diferencia de ZigBee, Z-Wave es un estándar cerrado, propiedad de Silicon Labs, al ser un sistema cerrado, generalmente el protocolo no es susceptible de cambios. Z-Wave agrega seguridad adicional al requerir que cada dispositivo use una ID única para comunicarse con su hub, lo que permite una fácil identificación. Por lo expuesto, se puede concluir que en el caso de que el usuario requiera seguridad, los sistemas cerrados serían la opción recomendada, aspecto por el cual Z-Wave estaría sobre ZigBee. Por otra parte, tanto Z-Wave como ZigBee crean una red de malla entre los diferentes dispositivos que tiene en los edificios inteligentes. Sin embargo, una ventaja distintiva para Z-Wave es lo lejos que pueden estar estos dispositivos. Z-Wave puede conectar dispositivos a una distancia de 160 metros, mientras que ZigBee alcanza el máximo a unos 20 metros. Por lo citado, en base a la longitud del edificio inteligente, Z-Wave es una buena opción para la comunicación en lugares muy amplios sin realizar un gasto excesivo.

2.4 Marco conceptual.

- SSID: Es el nombre de la red, todos los paquetes de información que se envían o reciben llevan esta información.
- WEP: El protocolo WEP es el sistema de cifrado para redes wifi más simple y lo implementan prácticamente todos los dispositivos, Se considera inseguro, ya que existen vulnerabilidades que provocan que se pueda saltar fácilmente, y se considera obsoleto.
- WPA: Sistema posterior a WEP que mejora notablemente la encriptación de WEP.
- EL PROTOCOLO WPA: utiliza un cifrado más fuerte que hace que sea más robusto, aunque no todos los dispositivos ni los sistemas operativos lo soportan. La versión definitiva es WPA2
- WPA2: Sistema de cifrado, evolución del WPA, con contraseña de 128 bits, se considera el más robusto actualmente, aunque no todos los dispositivos lo implementan.
- IP: Una dirección formada por una serie de números que identifica a nuestro equipo de forma unívoca dentro de una red.
- MAC: Es un valor que los fabricantes asignan a cada componente de una red, y que los identifica de manera unívoca, es como el DNI del dispositivo. Tienen dirección MAC las tarjetas de red, los routers, los USB wifi...todos los dispositivos que puedan tener una IP.
- DHCP: Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos de dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente.
- AP: Del inglés Access Point, o punto de acceso. El punto de acceso corresponde a un transmisor-receptor de redes inalámbricas, o "estación base", que puede conectar una red LAN cableada a uno o varios dispositivos inalámbricos. Los puntos de acceso también se pueden conectar en puente entre sí.

- AD-HOC: Configuración del equipo cliente que ofrece conectividad independiente entre dispositivos dentro de una red LAN inalámbrica. Como alternativa, los ordenadores se pueden comunicar entre sí a través de un punto de acceso.
- CLAVE DE CODIFICACION: Una serie de letras y números que permite codificar datos y después decodificarlos de forma que se puedan compartir de manera segura entre los miembros de una red. Los usuarios de WEP utilizan una clave de codificación que codifica automáticamente los datos salientes. Esta misma clave le permite al ordenador receptor decodificar automáticamente la información para que se la pueda leer.
- CLIENTE: Una aplicación instalada en un ordenador o dispositivo conectado a una red que solicita servicios (archivos, impresión) de otro miembro de la red.
- DNS: Del inglés Domain Name System (Service o Server), también llamado Sistema (servicio o servidor) de nombres de dominio. El DNS es un programa que traduce los URL en direcciones IP ingresando a una base de datos ubicada en una serie de servidores Internet. Este programa funciona en segundo plano para que el usuario pueda navegar por Internet utilizando direcciones alfabéticas en vez de una serie de números. El servidor DNS convierte un nombre como misitioweb.com en una serie de números como 107.22.55.26. Cada sitio Web tiene su propia dirección IP en Internet.
- DSL: Del inglés Digital Sebscriber Lines, o Línea de cliente digital. Diferentes protocolos de tecnología para la transmisión de datos, voz y vídeo de alta velocidad mediante cables telefónicos comunes de cobre de par trenzado.
- ENRUTADOR: Punto de acceso o dispositivo que envía datos desde una red de área local (LAN) o red de área amplia (WAN) a otra. El enrutador monitorea y controla el flujo de datos, y envía información

a través de la ruta más eficiente en función del tráfico, el costo, la velocidad, las conexiones, etc.

- llNFRAESTRUCTURA: Modo de acceso que proporciona conexión a un punto de acceso. En comparación con el modo Ad-hoc, en el que los ordenadores se comunican directamente entre sí, los clientes configurados en el modo Infraestructura pasan datos a través de un punto de acceso central. El punto de acceso no sólo controla el tráfico de la red inalámbrica del entorno inmediato, sino que, además, proporciona comunicación con la red cableada.
- NOMBRE DE LA RED: Identifica la red inalámbrica para todos los componentes compartidos. Durante el proceso de instalación de la mayoría de las redes inalámbricas, el usuario debe introducir el nombre de la red o SSID. Al configurar el ordenador, el grupo de trabajo o la red cableada, se utilizan diferentes nombres de red.
- PUENTE: Producto que conecta una red LAN con otra red de área local que utilice el mismo protocolo (por ejemplo, inalámbrico, Ethernet o token ring). Por lo general, los puentes inalámbricos se utilizan para conectar edificios o escuelas en un campus.
- SSL: Del inglés Secure Sockets Layer, o nivel de sockets seguro. Programa de codificación que normalmente utilizan los sitios de banca y venta electrónica y que protege la integridad financiera de las transacciones.
- TCP/IP: Tecnología tras Internet y las comunicaciones entre ordenadores en una red.
- WI-FI: Del inglés Wireless Fidelity, o Fidelidad inalámbrica. Término creado por Wi-Fi Alliance que se utiliza para describir redes inalámbricas estándar tipo 802.11. Los productos que Wi-Fi Alliance haya probado y certificado como "Wi-Fi" pueden operar entre sí incluso si son de marca diferente.
- CERTIFICADO DIGITAL: También llamado certificado de clave pública o certificado de identidad. En criptografía de clave pública,

certifica que una clave pública pertenece a la entidad que envía los datos cifrados o firmados digitalmente con esa clave. Los certificados digitales son emitidos por una autoridad de certificación y contienen la clave pública del emisor, más una firma digital que verifica que el certificado es auténtico y que la clave pertenece al emisor.

- CIFRADO: Método de seguridad que vuelve la información ilegible a quien no tenga la clave para descifrarla. Se utiliza generalmente para proteger las compras y otras transacciones de Internet. Cuando un sitio web indica que es "seguro", generalmente se refiere a que los datos que se envían y se reciben están cifrados.
- CIFRADO SIMÉTRICO: Método de cifrado que utiliza la misma clave secreta para cifrar y descifrar
- mensajes.
- AUTENTIFICACIÓN FUERTE: Basada en la utilización de técnicas de criptografía asimétrica y en el uso de certificados electrónicos. También suele referirse a la combinación de algo que el usuario posee (por ejemplo, una tarjeta electrónica) con algo que conoce (como un código PIN).
- AUTENTIFICACIÓN SIMPLE: Basada en mecanismos tradicionales de usuario y contraseña.
- CLAVE PRIVADA: En el cifrado asimétrico, clave no publicada usada para descifrar mensajes cifrados con una clave pública correspondiente.
- CLAVE PÚBLICA: En el cifrado asimétrico, clave que se pone a disposición de cualquier usuario que desee enviar un mensaje cifrado al propietario de la clave. El propietario de la clave pública usa su clave privada para descifrar los mensajes.
- ATAQUES DE NEGACIÓN DE SERVICIO DoS.: Ataque a una computadora o red que provoca una saturación en el ancho de banda o una sobrecarga en los recursos hasta que los servicios de la computadora o la red dejan de estar disponibles para los clientes. La

negación de servicio también puede deberse a un código malicioso que simplemente desconecta los recursos.

- FIRMA DIGITAL: Utilizada en la criptografía de clave pública para validar la integridad de los datos cifrados y confirmar tanto la identidad del titular del certificado digital como la autenticidad del certificado.
- INGENIERÍA SOCIAL: Método de engaño a los usuarios para que divulguen información privada. La ingeniería social saca partido de nuestra tendencia natural de confiar en el otro, en vez de utilizar solo medios tecnológicos para robar información. Generalmente asociado con phishing, pharming, spam y otras estafas basadas en Internet.
- PHISHING: Intento de engañar a los usuarios para que divulguen información personal, como números de documentos de identidad y contraseñas. El phishing generalmente utiliza correo electrónico o mensajes instantáneos que parecen legítimos, en combinación con sitios web falsos a fin de realizar solicitudes fraudulentas de información (es decir, salir a “pescar” datos). Consulte también ingeniería social.
- PHARMING: Intento de defraudar navegantes de Internet a través del secuestro del nombre de dominio de un sitio web, o URL, y el redireccionamiento de los usuarios a un sitio web falso donde se realizan solicitudes fraudulentas de información. Consulte también falsificación de URL. Punto de acceso Wi-Fi Área física donde se puede usar un dispositivo con Wi-Fi para conectarse a Internet mediante una red inalámbrica pública. Si bien algunos puntos de acceso no poseen medidas de seguridad instaladas, otros usan WEP o WPA para asegurar las transmisiones.
- 802.11 O IEEE 802.11x: Serie de estándares convencionales para las comunicaciones de red inalámbrica. Existen diferentes versiones o modulaciones de 802.11. Los más conocidos son 802.11b y

802.11g. Los estándares 802.11 también definen los protocolos de seguridad que incluyen WEP, WPA y WPA2.

- HIJACKING: Se denomina hijacking a las técnicas informáticas que se utilizan para adueñarse o "secuestrar" páginas web, conexiones de internet, dominios, IPs, etc.
- ATAQUES DE FUERZA BRUTA: Este tipo de ataques consiste en intentar todas las contraseñas posibles según el sistema. Este método siempre logra encontrar la contraseña pues la prueba todas. La dificultad está en la cantidad de caracteres posibles de utilizar en la contraseña.
- AP (Access Point): Punto de acceso inalámbrico. El dispositivo que proporciona el acceso inalámbrico a la red a los usuarios finales.
- DMZ: (Demilitarized Zone): También conocida como red perimetral. Una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. En ella se permiten conexiones desde ambas redes, pero la red DMZ solo puede establecer comunicaciones con la red externa, siendo la interna inaccesible para los equipos dentro de la red DMZ.
- LEAP: (Lightweight Extensible Authentication Protocol): Versión ligera del protocolo de autenticación extensible. Es el más sencillo de los protocolos de autenticación extensible utilizados en las redes inalámbricas.

CAPÌTULO IV: RESULTADOS

4.1 RESULTADOS DE LA IMPLEMENTACION DEL MARCO METODOLOGICO.

El día viernes 09 de junio del año en curso 2023 se realizó la aplicación de las encuestas y fichas de observaciones a las personas previstas de acuerdo a la muestra establecida. La muestra utilizada fue de 15 personas que se encontraban disponibles en la universidad del sureste de la cuidad de Frontera Comalapa, Chiapas.

La encuesta se llevó a cabo en un promedio de 5 horas por parte de los tesistas profesionales de Ingeniería en sistemas computacionales del 9° cuatrimestre, modalidad ejecutiva de la Universidad del Sureste, Campus de la Frontera.

Cabe destacar que el proceso de investigación se llevó a cabo de manera satisfactoria obteniendo los resultados de la participación deseada.

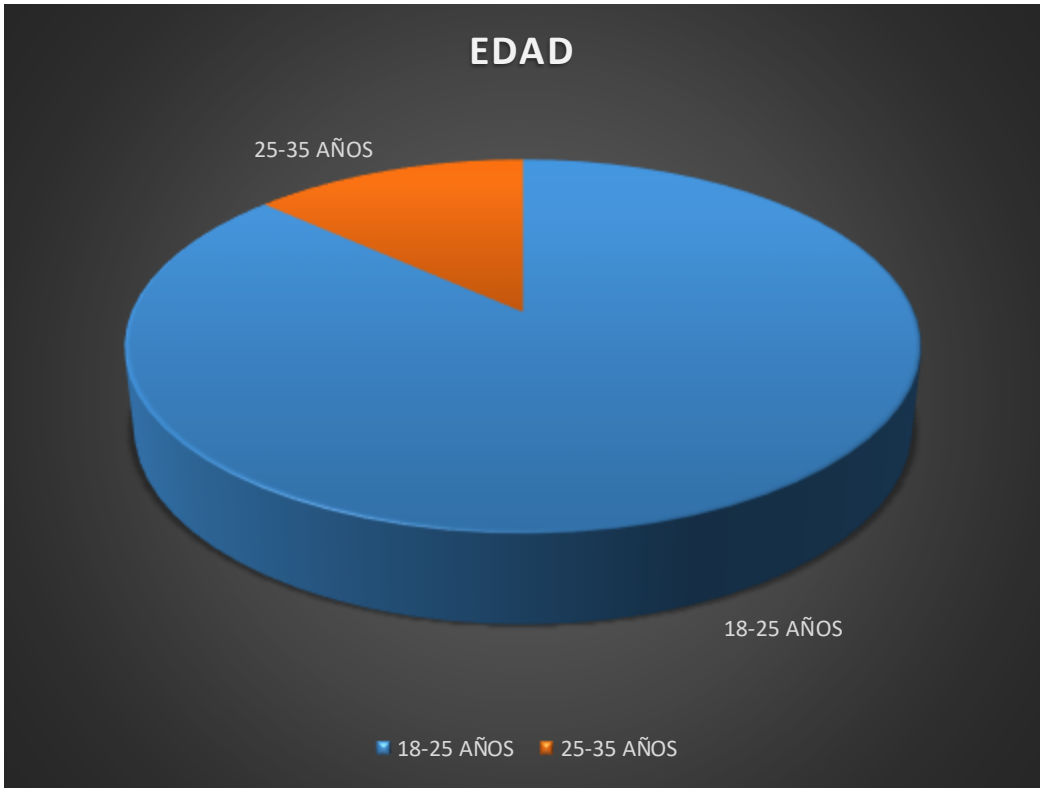
En el siguiente apartado se presenta los resultados a través de graficas que nos permitieron realizar un análisis e interpretación de la información para conocer la situación que prevalece respecto a la problemática del poco conocimiento información de la seguridad en redes informáticas de la universidad del sureste de la cuidad de Frontera Comalapa, Chiapas, que a su vez fue la base para la construcción de las recomendaciones y propuestas.

4.2 PROCESAMIENTO DE LA INFORMACIÓN

TABLA 1: DATOS PERSONALES

VARIABLE	DETALLE	FRECUENCIA	PORCENTAJE
EDAD	18-25 AÑOS	13	87%
	25-35 AÑOS	2	13%
	TOTAL	**15**	**100%**
SEXO	FEMENINO	14	93%
	MASCULINO	1	7%
	TOTAL	**15**	**100%**
ESCOLARIDAD	PREPARATORIA	9	60%
	UNIVERSIDAD	6	40%
	TOTAL	**15**	**100%**
OCUPACIÓN	ESTUDIANTES	9	60%
	PROFESIONISTAS	2	13%
	OTROS	4	27%
	TOTAL	**15**	**100%**

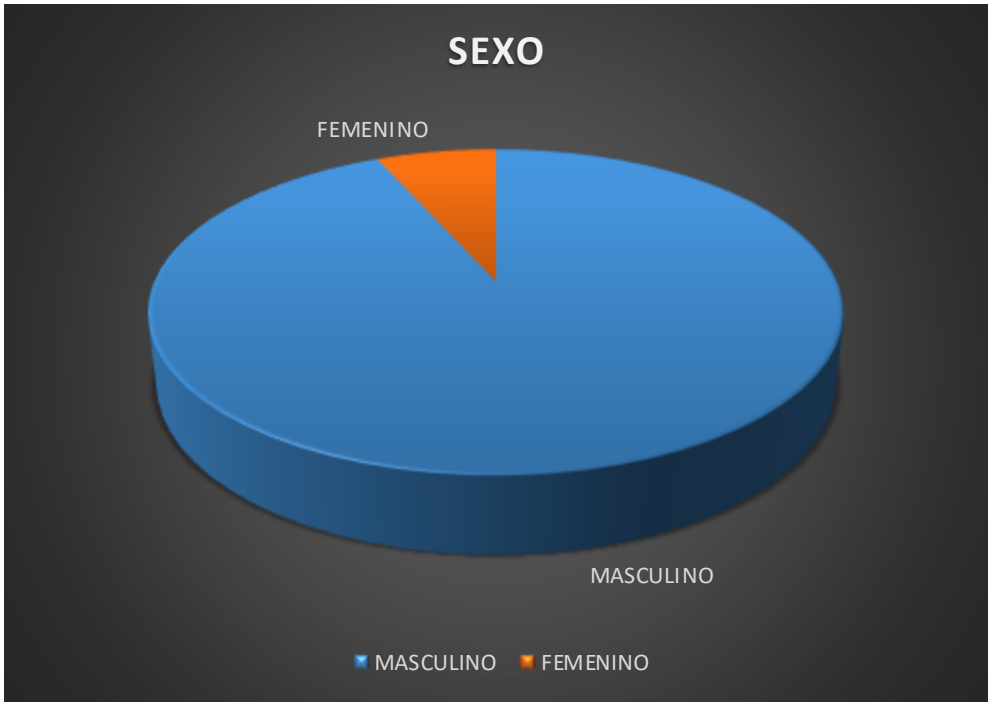
GRÁFICA 1



ANÁLISIS: La gráfica anterior presenta la variable de edad y observamos que el mayor número de porcentaje, es decir el 87% corresponde a personas de entre 18 a 25 años y el otro 13% a personas de 25 a 35 años de edad.

INTERPRETACIÓN: En la gráfica presentada podemos observar la diferencia tan notable entre los grupos de edad, ya que la mayoría corresponde a edades de adultos jóvenes y la menor parte a personas en edades avanzadas y de esta forma podemos interpretar claramente que las personas con menos edad tienen más tentativa de captar la información proporcionada.

GRÁFICA 2



ANÁLISIS: De acuerdo a la gráfica presentada se observa que el 93% de los encuestados pertenecen al sexo masculino y solo 7% al sexo femenino.

INTERPRETACIÓN: En la gráfica de arriba observamos que casi el total de las personas encuestadas son hombres y solo una persona es del sexo femenino. Esto no determina nada para nuestra investigación ya que todos debemos tener los mismos conocimientos acerca de las redes informáticas es un tema que tanto hombres y mujeres deben conocer.

GRÁFICA 3

ANÁLISIS: La grafica de arriba arroja los resultados de la variable escolaridad y se observa que la mayor parte de los encuestados con un 60% tiene la preparatoria terminada, y el 40% del porcentaje restante están cursando una carrera universitaria.

INTERPRETACIÓN: En la gráfica presentada observamos que la mayor parte de las personas encuestadas con un alto porcentaje tienen terminada la preparatoria y mientras que algunas de las personas encuestadas ya están en un nivel superior de estudios realizando una profesión.

GRÁFICA 4

ANÁLISIS: En la tabulación de la variable ocupación se observa que el mayor porcentaje con un 60% se trata de personas que aún están estudiando un nivel escolar o una carrera universitaria, un 13% ya son profesionistas dedicados y finalmente el 27% se dedican a otros diferentes oficios.

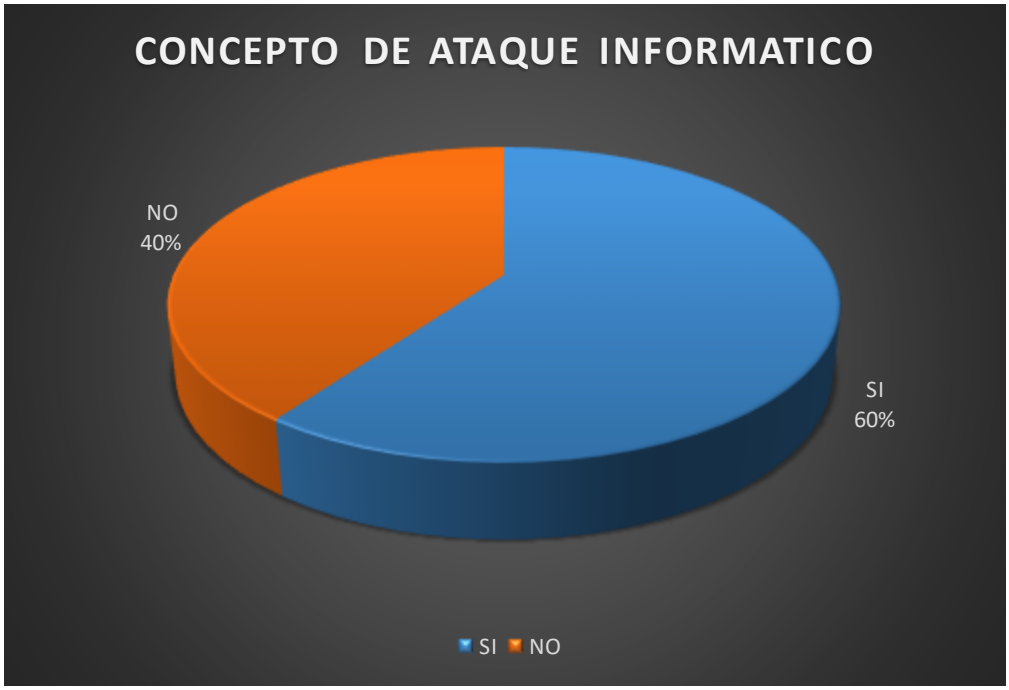
INTERPRETACIÓN: La grafica anterior nos presenta la distribución de la ocupación de los encuestados y podemos observar que la mayoría de personas de nuestra muestra aún son estudiantes y la menor parte ya se dedican a un trabajo profesional, lo que nos da la conclusión de pensar que al recibiendo conocimientos por las instituciones escolares, estas personas pueden tener un mayor amplio conocimiento acerca de las redes informáticas y por ende se puede decir qué cada vez hay menos desinformación sobre la tecnología y sus medios.

TABLA 2: DATOS DE CONOCIMIENTO

VARIABLE	DETALLE	FRECUENCIA	PORCENTAJE
CONCEPTO DE ATAQUE INFORMATICO	SI	12	60%
	NO	3	40%
	TOTAL	**15**	**100%**
CONOCIMIENTOS ACERCA DE LOS ANTIVIRUS	SI	15	100%
	NO	0	0%
	TOTAL	**15**	**100%**
INFORMACION ACERCA DE LOS BENEFICIOS DE LOS ANTIVIRUS	SI	14	93%
	NO	1	7%
	TOTAL	**15**	**100%**
CONOCIMIENTOS SOBRE NO COMPARTIR SU CONTRASEÑA DE INTERNET	SI	13	87%
	NO	2	13%
	TOTAL	**15**	**100%**
CONOCIMIENTOS ACERCA DE COMO ES UN ATAQUE INFORMATICO	SI	8	53%
	NO	7	47%
	TOTAL	**15**	**100%**
DISPOSITIVOS ELECTRONICOS MAS USADOS	TELEFONO MOVIL	13	87%
	LAPTOP	2	13%
	TOTAL	**15**	**100%**
PEROSONAS QUE TIENEN UNA RED WIFI EN SU CASA	SI	12	80%
	NO	3	20%
	TOTAL	**15**	**100%**

PERSONAS QUE SE HAN CONECTADO A UNA RED PUBLICA	SI	11	73%
	NO	4	27%
	TOTAL	**15**	**100%**
PERSONAS QUE CAMBIAN FRECUENTEMENTE SU CONTRASEÑA DE INTERNET	SI	3	20%
	NO	12	80%
	TOTAL	**15**	**100%**
CONOCIMIENTO DE ACERCA DE ALGUIEN QUE HALLA SIDO VICTIMA DE UN VIRUS INFORMATICO	SI	2	13%
	NO	13	87%
	TOTAL	**15**	**100%**
PERSONAS QUE HAN DESCARGADO ALGO DE INTERNET	SI	15	100%
	NO	0	0%
	TOTAL	**15**	**100%**
PERSONAS QUE HAN COMPARTIDO SU RED WIFI	SI	10	67%
	NO	5	33%
	TOTAL	**15**	**100%**
PERSONAS QUE GUARDAN INFORMACION PERSONAL EN SU DISPOSITIVO MOVIL	SI	12	80%
	NO	3	20%
	TOTAL	**15**	**100%**
CONOCIMIENTO ACERCA DE CAMBIAR LA CLAVE WIFI FRECUENTEMENTE	SIEMPRE	3	20%
	A VECES	4	27%
	NUNCA	8	53%
	TOTAL	**15**	**100%**
PERSONAS QUE FRECUENTEMENTE DESCARGAN ARCHIVOS DE INTERNER	SIEMPRE	5	33%
	A VECES	10	67%
	TOTAL	**15**	**100%**

GRÁFICA 5



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 60% si conoce el concepto si tiene un buen conocimiento acerca sobre las redes informáticas y de la tecnología y solo el 40% no conoce el concepto o tienen nulo o escaso conocimiento de este tema.

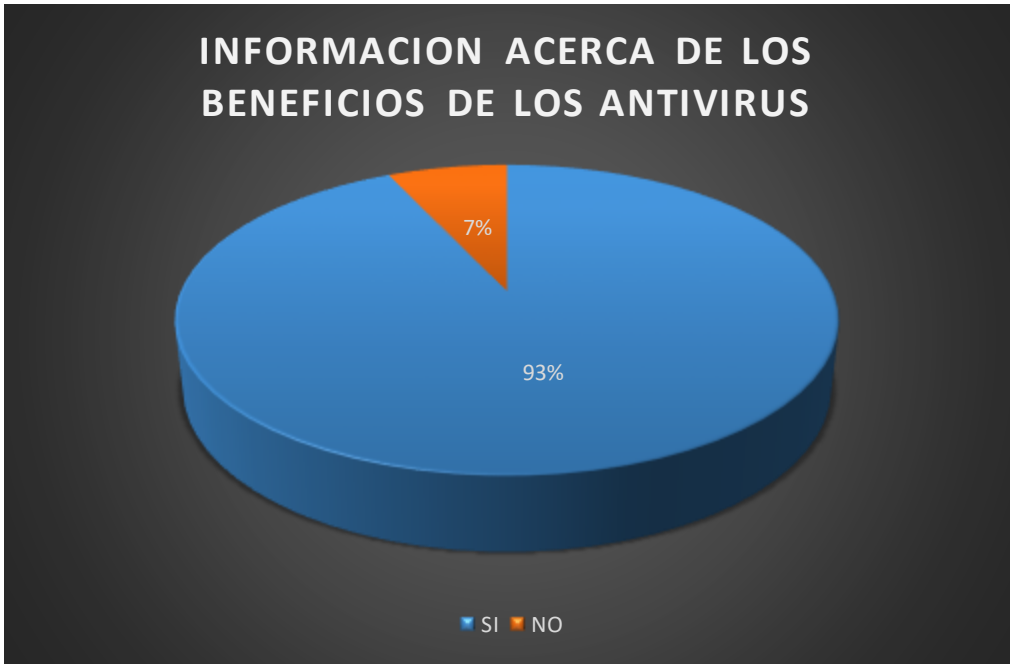
INTERPRETACIÓN: En esta grafica podemos dar cuenta que la mayoría de las personas encuestadas si tiene el conocimiento de que son las redes informáticas y los tipos de seguridad en ella, si han escuchado este término, pero en realidad no conocen todos lo que conlleva en ellas y como están funcionan internamente a la vez como no tienen un amplio conocimiento sobre cómo enfrentarse ante un ataque informático, virus.

GRÁFICA 6

ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 100% si conoce el concepto y funcionalidad de los antivirus como este ayuda en los dispositivos electrónicos contra virus y ciberataques y su gran importancia.

INTERPRETACIÓN: En esta grafica podemos dar cuenta que todas las personas que fueron encuestadas saben la funcionalidad y la gran importancia de tener un antivirus en sus dispositivos electrónicos, con el fin de protegerse ante virus y robo de su información personal o bancaria.

GRÁFICA 7



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 93% si tiene conocimiento de los beneficios de tener un antivirus instalado en sus dispositivos electrónicos, mientras que el 7% tiene poca información de los beneficios de tener un antivirus instalado.

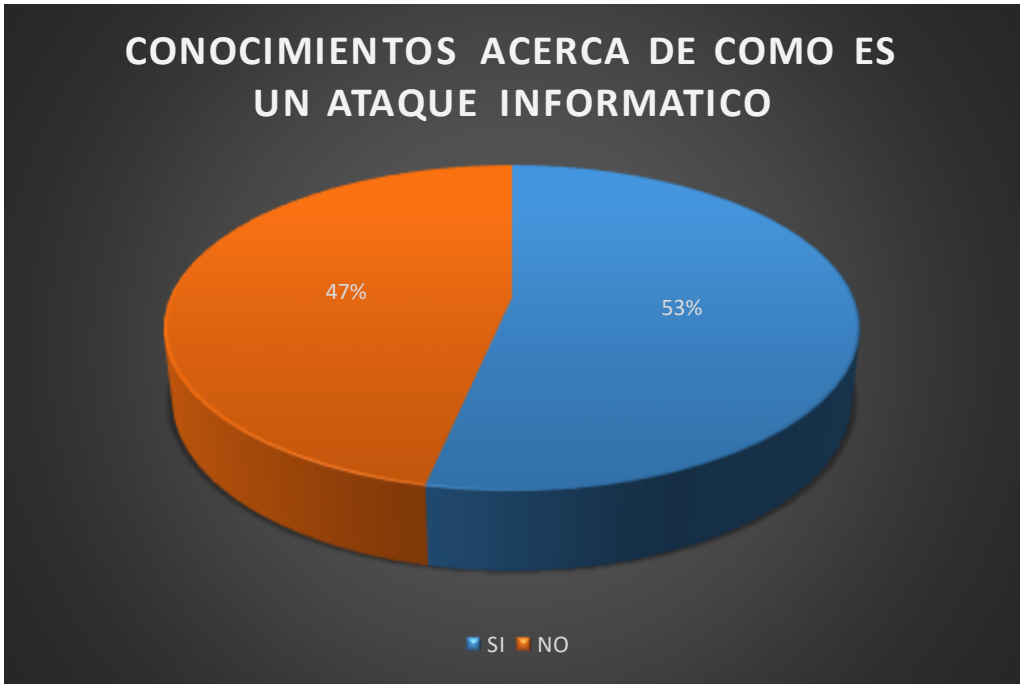
INTERPRETACIÓN: En esta grafica podemos dar cuenta que la mayoría de las personas que fueron encuestadas saben de los beneficios de tener un antivirus en sus dispositivos electrónicos instalados para tener una mayor seguridad al tener información personal guardados en sus dispositivos electrónicos.

GRÁFICA 8

ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 87% no comparten la contraseña de red wifi con el fin de salvar su información y alguno pueda llegar a sustraerla sin permiso previo, mientras que el 7% si comparte la contraseña de su red wifi ya que tiene nula información acerca de los ataques cibernéticos.

INTERPRETACIÓN: En esta grafica podemos dar cuenta que la mayoría de las personas no comparten su red wifi por temor a que algunos puedan hackear su red y sustraer su información personal a través de la red wifi y solo alguno si la comparten con otros ya que tiene poco conocimiento sobre los robos de información por medio de redes inalámbricas.

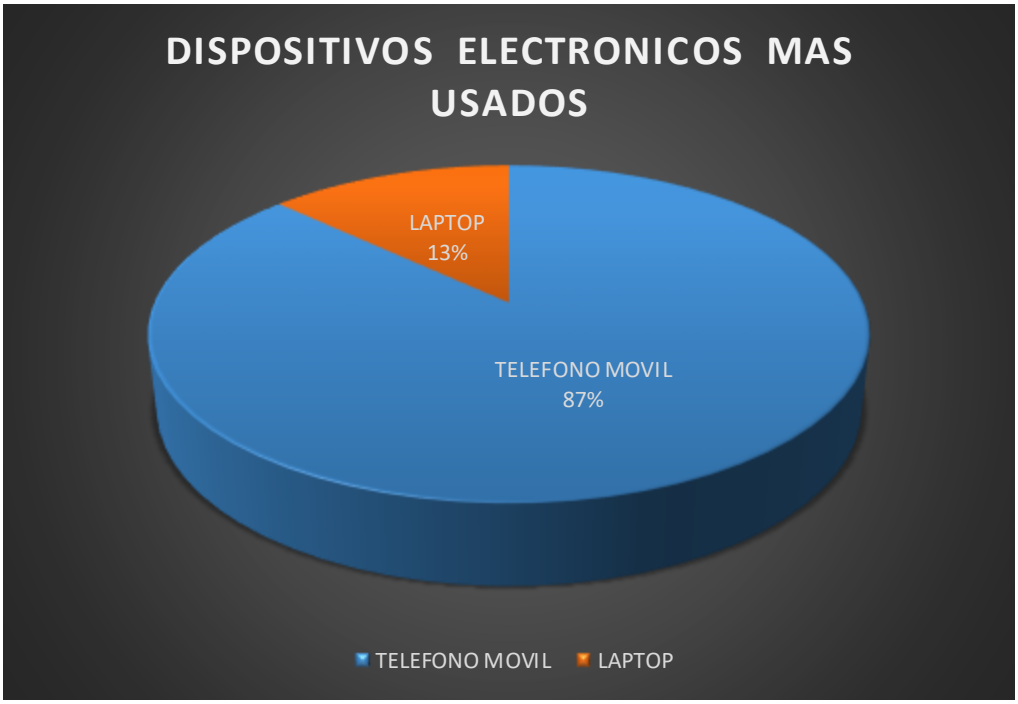
GRÁFICA 9



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 53% de las personas saben lo que es un ataque informático o ciberataque, mientras que el 47% desconoce acerca de los ataques cibernéticos o informáticos.

INTERPRETACIÓN: En esta grafica podemos dar cuenta casi la mitad de las personas no saben lo que es un ataque informático y no familiarizan este término, pero un poco más de la mitad de los encuestados sabe que son los ataques los ataques informáticos y cuáles son sus diferentes variantes.

GRÁFICA 10



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 87% usan más a menudo un teléfono móvil para realizar sus trabajos y guardar toda su información ahí, mientras que el 13% prefieren usar una laptop para hacer sus trabajos y guardar todo tipo de información ahí por su factibilidad y uso.

INTERPRETACIÓN: En esta grafica podemos dar cuenta que la mayoría de las personas encuestadas prefieren usar un teléfono celular para realizar todos sus trabajos, guardar información de todo tipo ahí y además de poder comunicarse con otras personas por su factibilidad de adquirir un teléfono móvil les sabe un poco más económico y cómodo de usar que una laptop que abarca más funcionalidades.

GRÁFICA 11

ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 80% cuentan con una instalación de red wifi privada para realizar todas sus búsquedas, descargas y trabajos, mientras que el 20% no cuentan con ninguna red wifi en su casa y se limitan a usar datos móviles o en su defecto ir a un cibercafé para realizar sus diferentes trabajos.

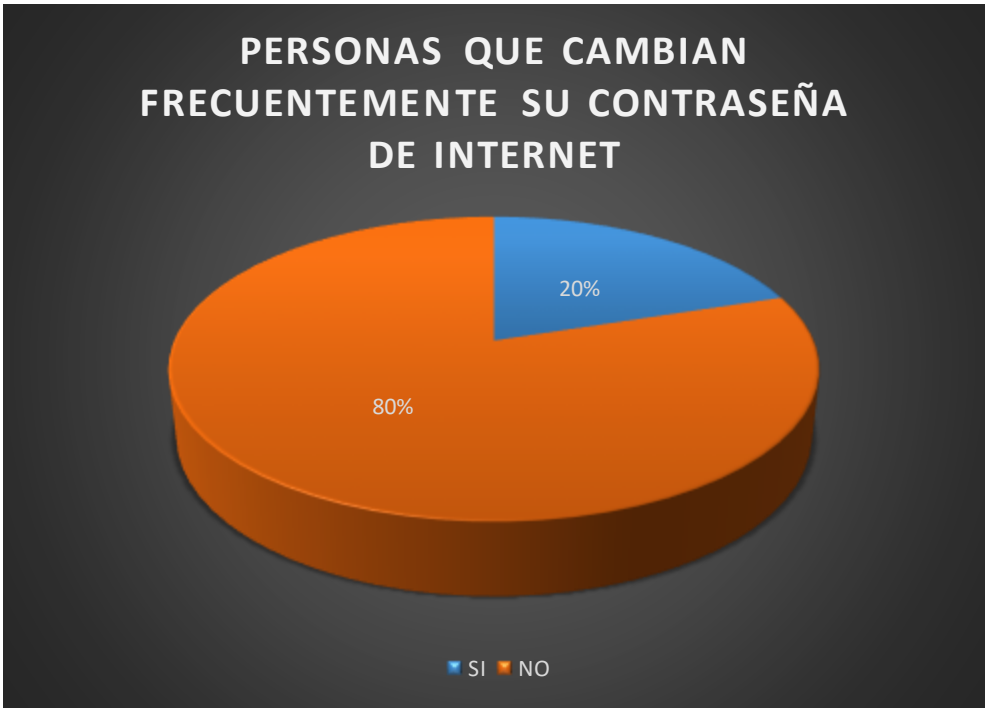
INTERPRETACIÓN: En esta grafica podemos dar cuenta que la mayoría de las personas encuestadas cuentan con una instalación de red de internet en su hogar ya que les brinda una mayor seguridad a la hora de navegar por internet, a comparación de los que no tienen y tiene que recurrir a redes públicas o cibercafés con el miedo de sufrir algún ciberataque.

GRÁFICA 12

ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 73% se han conectado a una red pública por diferentes motivos y necesidades, mientras que el 27% nunca han usado una red pública porque saben el peligro que lleva conectarse a este tipo de redes.

INTERPRETACIÓN: En esta grafica podemos dar cuenta que la mayoría de las personas encuestadas se han conectado a una red gratis o publica ya que por motivos de urgencia o por no contar con una red wifi en su hogar han usado estas, algunos sabiendo los peligros de usar estas redes pero por necesidades de buscar o enviar algo por internet las han usado este tipo d red gratis, solo muy pocos jamás las han usado por que tiene un amplio conocimiento sobre las redes informáticas y los peligros de ella.

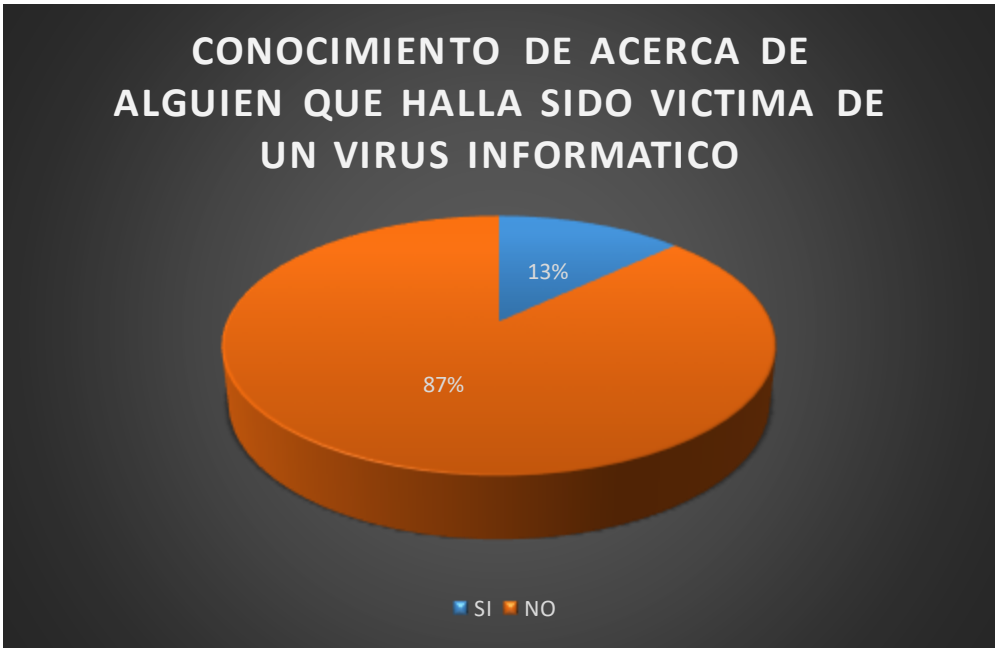
GRÁFICA 13



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 80% jamás ha cambiado la contraseña por defecto que viene en su red wifi o simplemente no cuentan con una red wifi en su hogar, mientras que el 20% cambia frecuentemente o a menudo su clave de wifi por motivos de tener una mayor seguridad de su red.

INTERPRETACIÓN: En esta grafica podemos dar cuenta que la mayoría de las personas encuestadas jamás ha modificado su clave de wifi desde el día que se las instalaron, esto se debe al poco conocimiento de modificar las claves wifi del modem y solo muy pocos saber acerca de esto.

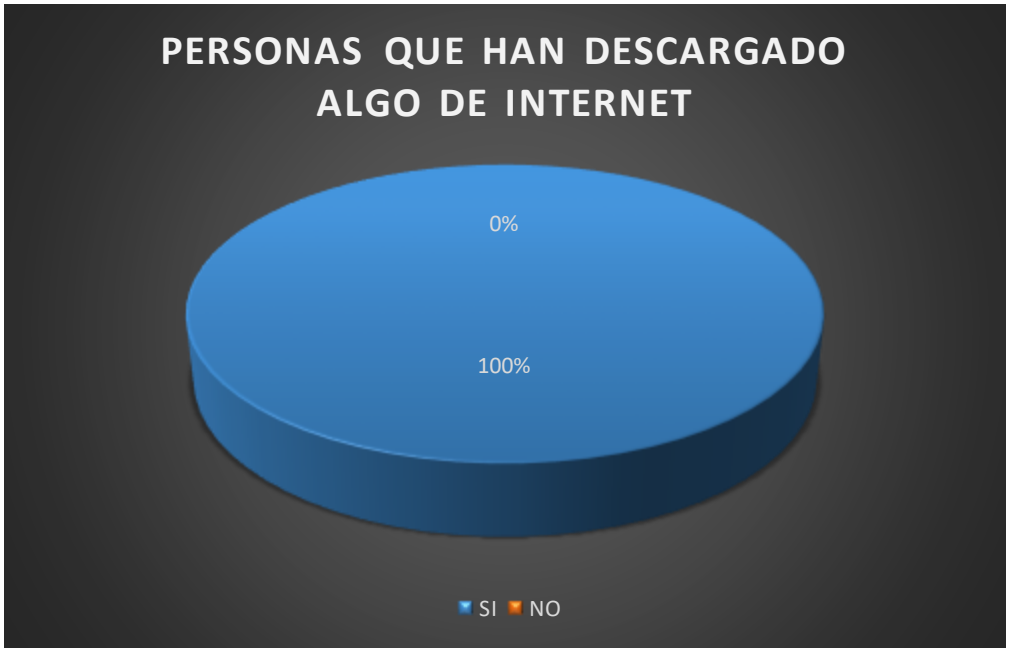
GRÁFICA 14



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 87% desconoce de alguien que hubiera sufrido un ciberataque y solo el 13% conocen a alguien que hubiera sido víctima de esto.

INTERPRETACIÓN: En esta grafica podemos dar cuenta que la mayoría de las personas encuestadas no saben realmente si algún conocido o familiar hubiera sido víctima de algún virus informático por ende se puede decir que suele haber muy a menudo ese tipo de ataques informáticos en esta localidad, solo algunos han sabido de alguien que sufrió esto tipo de ataque y le hayan robado su información personal.

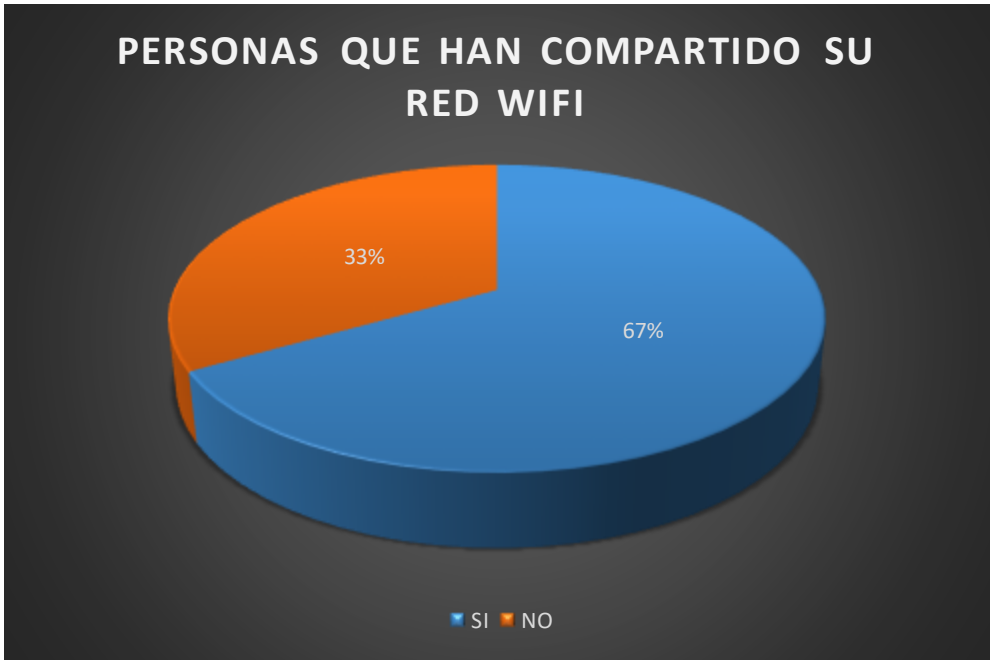
GRÁFICA 15



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 100% han descargado alguna vez algún archivo de internet sea cual sea.

INTERPRETACIÓN: En esta grafica nos podemos dar cuenta que todas las personas que fueron encuestadas han descargado archivos de internet de cualquier tipo sin importar de donde provenga, casi nadie o bueno nadie jamás ha negado hacer esto, se le podría llamar como una actividad cotidiana del día a día estando en una red informática.

GRÁFICA 16



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 67% han compartido su red wifi con algún conocido o familiar, mientras que el 33% de ellos jamás lo han hecho o por ende no cuentan con este servicio en su hogar.

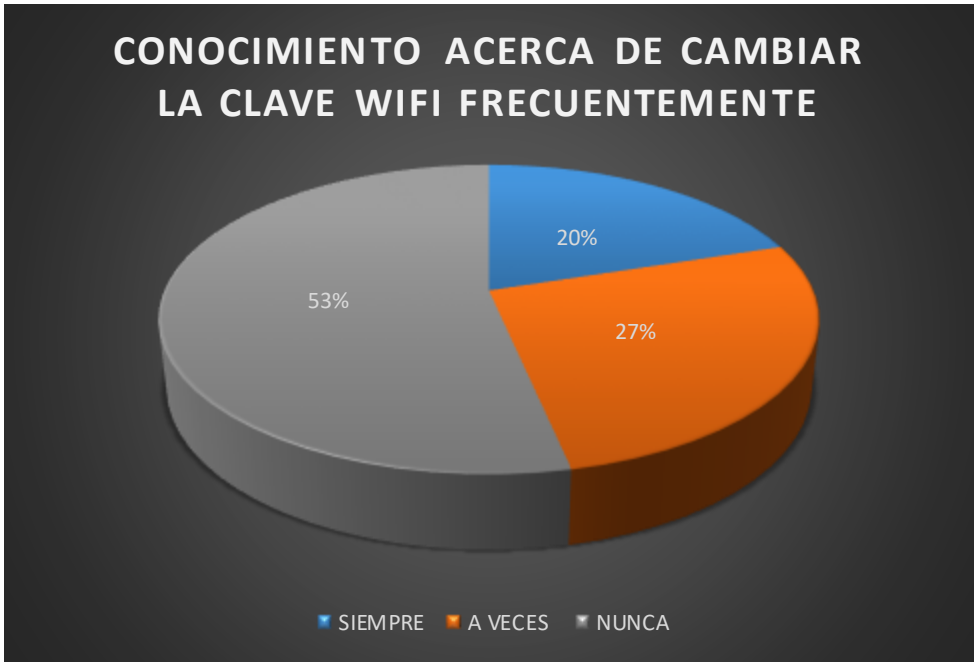
INTERPRETACIÓN: En esta grafica nos podemos dar cuenta qué casi todas las personas encuestadas han compartido su red wifi por diferentes motivos ya sea por visitas, por familiares o amigos a los que les brindan acceso a su red, pero todos coinciden que jamás la compartirían con algún desconocido, mientras que el resto no comparten su red ya sea por razones personales o simplemente por seguridad y por ultimo por no tener este servicio en su hogar.

GRÁFICA 17

ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 80% guardan información personal en sus teléfonos por su practicidad, mientras que el 20% de ellos no suelen guardar este tipo de información en sus teléfonos móviles.

INTERPRETACIÓN: En esta grafica nos podemos dar cuenta qué casi todas las personas encuestadas suelen guardar muy a menudo información personal en sus teléfonos ya que todos concluyen que es más practico hacerlo ahí que usar algún tipo de dispositivo diferente para guardar cosas personales y solo unos pocos no suelen guardar archivos personales en este dispositivo porque saben que no es del todo seguro tener ese tipo de información guardada ahí.

GRÁFICA 18



ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 53% suelen cambiar su contraseña de su red wifi muy a menudo por motivos de mayor seguridad, mientras que el 27% de ellos no suelen cambiar tan seguido su contraseña de su red wifi, pero lo han hecho y por último el 20% jamás han hecho cambios en su red wifi y la han dejado tal cual con la configuración predeterminada del modem.

INTERPRETACIÓN: En esta grafica nos podemos dar cuenta qué casi la mitad de los encuestados han cambiado de contraseña a su red wifi por motivos de seguridad, por si alguien pudo descifrar su contraseña anterior y por último para no sufrir algún ataque por virus informático, algunos si hacen el cambio de contraseña pero es rara vez que realizan esta acción y finalmente solo unos pocos jamás han hecho esta acción por motivos de que no tiene conocimientos para cambiar la clave wifi de su modem o simplemente no cuentan con este servicio en su hogar.

GRÁFICA 19

ANÁLISIS: La grafica anterior muestra que, de la población encuestada para el trabajo de investigación, el 67% de ellas descargan archivos de cualquier tipo de internet y en cualquier medio, mientras que el 33% es rara vez que realizan descargas de archivos de internet solo algunas veces.

INTERPRETACIÓN: En esta grafica nos podemos dar cuenta qué casi la todas las personas encuestadas han descargado archivos de internet muy frecuentemente, desde una simple imagen o documente de texto hasta archivos de gran tamaño ya que para todos descargar archivos de internet ya es algo muy normal hoy en día y siempre lo hacemos en nuestro día a día, y solo algunos no hacen esta acción frecuentemente solamente cuando tengan la necesidad de hacerlo descargan archivos de internet.