Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria, Matagalpa

UNAN MANAGUA – FAREM MATAGALPA

Monografía para optar al título de Licenciado en Ciencias de la Computación

Tema

Evaluación de la Red Inalámbrica en el Hospital Escuela Cesar Amador Molina, basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013 Matagalpa, I semestre 2015.

Autores:

Br. Edgard Daniel López Uriarte

Br. Héctor Antonio Zamora Aguilar

Tutor:

Lic. Julio Selva Ochoa

Asesora:

Lic. Cleidys Flores Escoto

Matagalpa, Agosto, 2015

Universidad Nacional Autónoma de Nicaragua, Managua

Facultad Regional Multidisciplinaria, Matagalpa

UNAN MANAGUA – FAREM MATAGALPA

Monografía para optar al título de Licenciado en Ciencias de la Computación

Tema

Evaluación de la Red Inalámbrica en el Hospital Escuela Cesar Amador Molina, basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013 Matagalpa, I semestre 2015.

Autores:

Br. Edgar Daniel López Uriarte

Br. Héctor Antonio Zamora Aguilar

Tutor:

Lic. Julio Selva Ochoa

Asesora:

Lic. Cleidys Flores Escoto

Matagalpa, Agosto, 2015

DEDICATORIA

Primeramente a Dios por darme vida, salud y fuerza para llegar a culminar una de mis metas.

A mis padres que me educaron desde muy pequeño, siempre dándome el mejor ejemplo para que lograra ser alguien en la vida, ellos han sido el pilar fundamental para seguir adelante, siempre apoyándome y haciendo el mayor esfuerzo con mucho amor y cariño para que lograra llegar hasta donde estoy.

A mis hermanos que de una u otra manera siempre me han apoyado y han pasado con migo los momentos más difíciles.

A mis verdaderos amig@s que me han dado los mejores consejos y me han acompañado en los buenos y malos momentos han sido de inspiración para superarme y nunca caer.

Y a todos los que me han dado la mano para cuando más lo he necesitado.

Edgard Daniel López Uriarte

DEDICATORIA

A Dios por permitirme llegar a este momento tan especial en mi vida, él que me ha dado los triunfos y fortaleza en los momentos difíciles para continuar cuando a punto de caer he estado, de igual forma dedico esta tesis a mi madre Lesbia Aguilar Zeledón que ha sabido formarme con buenos sentimientos, hábitos y valores.

A mi pequeña hija Angie Zamora García que es un regalo de Dios y es mi fuente de inspiración.

A mi Tía Martha Zamora quien me extendió una mano cuando más la necesite y es mí motivación a superarme.

A mi familia en general porque me han brindado su apoyo incondicional y por compartir conmigo buenos y malos momentos.

Héctor Antonio Zamora Aguilar

AGRADECIMIENTOS

Agradecemos a Dios por darnos la vida, gracias a su misericordia y su bondad, de poder concluir una etapa más de nuestras vidas.

A nuestros maestros y sus sabios conocimiento para poder ser profesionales de excelencia.

A nuestro tutor Lic. Julio Selva, por confiar en nuestra persona y apoyarnos incondicionalmente para realizar el estudio.

A nuestra asesora Lic. Cleidys Flores Escoto por su paciencia, sus consejos y calidez.

A todos los que formaron parte para la realización de este estudio y a cada uno de ellos gracias.

Edgard Daniel López Uriarte

Héctor Antonio Zamora Aguilar

AVAL DEL TUTOR

RESUMEN

La presente investigación tiene como objetivo la evaluación de la red inalámbrica en el Hospital Escuela Cesar Amador Molina, basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013 Matagalpa, I semestre 2015.

El trabajo se estructuro basado en los objetivos específicos que fueron establecidos de los cuales proceden las variables de estudio impresas en el marco teórico que avala la autenticidad y cientificidad de la investigación. De igual manera se elaboró un diseño metodológico que guió la metodología de investigación aplicada, ésta vislumbra el enfoque de investigación, población y las técnicas e instrumentos para la recopilación de la información.

Se aplicaron instrumentos que consistieron en una guía de entrevista aplicada al encargado de informática, entrevista a profundidad al experto en redes y en última instancia una tabla de matriz de resultados; se revisaron los controles de seguridad y normas de los estándares IEEE 802.11 por medio de una guía ítems.

El presente estudio describe las bases teóricas para entender el funcionamiento y conocer la solución al problema, aportando documentación de referencia para futuras toma de decisiones para mejorar el medio no guiado.

Los resultados de esta investigación demuestran que la red no cumple del todo con los objetivos de los controles de seguridad. Sin embargo la principal dificultad encontrada de la red está en que el router se inhibe constantemente implicando reiniciar el equipo periódicamente. De esto se derivan los problemas de conexión en el día a día. A todo se suman las oscilaciones de corriente alterna que ponen en riesgo la vida útil de los equipos de la red. Para toda esta problemática se sugiere implementar un sistema SAI y se establezcan controles de seguridad para la red inalámbrica.

Índice

Índice de figuras

Índice de tablas

Índice de anexos

I INTRODUCCIÓN

El uso de tecnologías de redes inalámbricas es una necesidad inminente en las instituciones, ya que brinda beneficios de conexión, movilidad en áreas libres y lugares poco espaciosos disminuyendo costos de instalación y mantenimiento. Desde hace algunos años las instituciones educativas en salud han destinado recursos económicos para la obtención y retroalimentación de la información en los futuros profesionales. Para encontrar debilidades de conexión a la red existen evaluaciones fundamentales tanto físicas como lógicas.

El objeto de estudio de esta investigación se centró en la evaluación de la red inalámbrica del Hospital Escuela Cesar Amador Molina de Matagalpa con el estándar IEEE 802.11 y los controles de seguridad ISO 27002-2013), I semestre 2015. Para ello, se realizó una descripción del estado actual de la red inalámbrica y se identificaron problemáticas existentes para sugerir mejoras a las dificultades identificadas.

El presente documento tiene soporte científico por un marco teórico con respecto a sus variables de estudio. La metodología utilizada se basó en la información presente en el diseño metodológico, en el cual está impreso el tipo y enfoque de la investigación, población, técnica de recopilación de datos y variable de estudio.

II ANTECEDENTES

A través del estudio de fuentes bibliográficas se encontraron investigaciones que satisfacen variables del estudio en cuestión, a continuación se describen cada uno de ellos:

En la Escuela de Ingeniería de Antioquía, Medellín (Colombia), Montoya & Ovalle, (2012), realizaron una investigación acerca de la evaluación del desempeño en redes inalámbricas de sensores mejoradas con agentes móviles, proponiendo como mecanismo la reprogramación autónoma, concluyendo que la solución más eficiente, que fue probada y evaluada en una red inalámbrica formada por 40 nodos que detectan fugas de amoniaco en tiempo real, determinó que el punto clave consiste en disminuir el consumo de energía producto de las confirmaciones y retransmisiones innecesarias de datos y procedimientos, desde los nodos sensores hasta la estación base. Este hecho representa, además de la disminución en el consumo energético, un ahorro significativo en el tiempo de convergencia de la red.

En Colombia, Mendigaña & Reina (2008), realizaron una investigación sobre el diseño, implementación y configuración de una Red Inalámbrica en la Corporación Universitaria minuto de Dios (Girardot) para que las personas relacionadas con la misma tengan acceso a Internet desde cualquier lugar de la sede finalmente se logró implementar la red inalámbrica con su respectiva seguridad y se obtuvo una buena cantidad de usuarios en muy poco tiempo.

En la Facultad Regional Multidisciplinaria de Matagalpa, Nicaragua, Rivas (2010), realizó un estudio para el diseño de la red inalámbrica con servidor de software libre Linux Suse evaluando la red cableada, el cual determinó que la red cableada se encuentra saturada y el diseño de red inalámbrica permitiría descongestionar el uso de los laboratorios de computación. También Mendoza (2012), realizó una evaluación de la red de computadoras de la FAREM Matagalpa donde se encontro una red en constante crecimiento tanto en la cantidad de equipos como de los servicios a brindar, se identifico fortaleza y debilidades de la seguridad lógica de la red.

III JUSTIFICACIÓN

El Hospital Escuela Cesar Amador Molina cuenta con una gran población de estudiantes que realizan prácticas de Medicina, Enfermería y Carreras afines a la Salud, la mayoría de ellos cuentan como apoyo tecnológico dispositivos portátiles para acceder a la red inalámbrica de internet ubicada en la parte sur del hospital.

Es notable la importancia de una red inalámbrica que brinde servicios web, de acuerdo a las necesidades de los usuarios en este caso los doctores, enfermeras, estudiantes y personal administrativo. Esta es una red que poco a poco ha tenido un incremento de equipos y usuarios conectados a la red con una mayor demanda de requerimientos en cobertura y servicios.

La aplicación de esta evaluación marcará una pauta ya que la unidad de salud no cuenta con ningún estudio de esta índole, ayudando a tener documentación idónea de la red inalámbrica actual para futuras toma de decisiones para mejorar dificultades y tener referencia para requerimientos de entidades cooperantes.

Es por ello que se necesita identificar las debilidades y requerimientos para mejorar el diseño, cobertura, seguridad y servicios de la red inalámbrica, así como también las condiciones físicas, por tal razón este trabajo investigativo tiene como finalidad evaluar la condición actual de la red inalámbrica en el Hospital Escuela Cesar Amador Molina, I semestre 2015.

Con los resultados de la evaluación de esta red se darán sugerencias para mejorar su diseño, cobertura y seguridad utilizando la infraestructura y recursos de la red como primera opción para mejorar los servicios que actualmente brinda la red, todo esto con el fin de beneficiar a los usuarios y encargados de la administración de la red de forma tal que esta tenga un desempeño óptimo en la operatividad.

IV PLANTEAMIENTO DEL PROBLEMA

Actualmente existe un alto nivel de dependencia a la red de internet por las diferentes actividades que se pueden realizar por ejemplo la búsqueda de información, compartir datos, entre otros. Sin embargo una de las actividades con mayor índice son las investigativas y se requiere tener acceso inmediato a una red de internet, más aún si éstas se encuentran sujetas a procesos de aprendizajes facilitados por centros de prácticas y educación superior donde está en juego la vida del ser humano, el grado de conocimientos que requiere cada uno de los involucrados es muy esencial para desempeñarse con profesionalismo en el ámbito laboral que requiere la población.

El Hospital Escuela Cesar Amador Molina posee una red inalámbrica de conexión a internet, esta red fue creciendo de acorde a la necesidad de la institución sin tomar en cuenta un estudio con base científico por lo tanto la red está expuesta a amenazas físicas y lógicas.

Al identificar dificultades y fortalezas se puede sugerir mejoras a la infraestructura tanto física como lógica de la red lo que facilitaría y beneficiaría al personal del hospital, además esto agilizaría las actividades didácticas de estudiantes que actualmente rotan en las instalaciones del centro asistencial.

Por ello, se necesitan buscar alternativas que mejoren las necesidades a través de la red, por lo antes mencionado se desea conocer si:

¿La red inalámbrica del Hospital Escuela Cesar Amador Molina, Matagalpa cumple con el estándar 802.11 y controles de seguridad ISO 27002-2013?

V OBJETIVOS

General

Evaluar la red inalámbrica en el Hospital Escuela Cesar Amador Molina Matagalpa basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013, I semestre 2015.

Específicos

1. Describir el estado actual de la red inalámbrica en Hospital Escuela Cesar Amador Molina Matagalpa, I semestre 2015.

2. Verificar el cumplimiento de criterios de norma IEEE 802.11 y controles de seguridad ISO 27002-2013 de la red inalámbrica del Hospital Escuela Cesar Amador Molina Matagalpa, I semestre 2015.

3. Identificar las principales dificultades y fortalezas en el funcionamiento de la red inalámbrica del Hospital Escuela Cesar Amador Molina Matagalpa, I semestre 2015.

4. Sugerir mejoras a las dificultades identificadas en la red inalámbrica Hospital Escuela Cesar Amador Molina Matagalpa, I semestre 2015.

VI MARCO TEÓRICO

Descripción de ámbito

El Hospital Regional Cesar Amador Molina está ubicado en la parte norte de la ciudad de Matagalpa, fundado en año 1984 siendo hospital de referencia de los 14 municipios existentes. El 22 de febrero del año 2013 fue certificado como Hospital Escuela donde los estudiantes de cuarto y quinto año de medicina podrán culminar sus estudios de medicina general además hacen pasantías estudiantes de Tecnología Médica, Farmacia, Radiología, Fisioterapia, Auxiliares de Enfermería, Enfermería Profesional, Psicología. En la actualidad cuenta con una biblioteca médica y una biblioteca de enfermería. Brinda atención a la población matagalpina en medicina general y con especialidades de Ortopedia, Oftalmología, Urología, Medicina Interna, Gineco-Obstetricia, Dermatología, Otorrinolaringología, Pediatría, Fisiatría, Hemato-oncología.

6.1 Redes

6.1.1 Definición

Según Dordoigne & Atelin (2006), una red “es un medio que permite a personas o grupos compartir información y servicios”.

A medida que se ha desarrollado la tecnología se ha tenido que implementar nuevas formas de trabajo que permitan el intercambio de información masiva siendo unas de estas técnicas las redes.

Actualmente, se puede observar en la mayoría de organizaciones e instituciones la estructuración de cableados que permiten la conexión de equipos informáticos. Un ejemplo de ello las impresoras y fotocopiadoras con conexión a la red.

6.1.2 Servicios

CCNA (2014), los servicios de red son programas de computación que respaldan la red humana. Distribuidos en toda la red, estos servicios facilitan las herramientas de comunicación en línea como emails, foros de discusión, boletines, salas de chat y

mensajería instantánea. Por ejemplo: en el caso un servicio de mensajería instantánea proporcionado por dispositivos en la nube, debe ser accesible tanto para el emisor como para el receptor.

Las personas generalmente buscan enviar y recibir distintos tipos de mensajes a través de aplicaciones informáticas; estas aplicaciones necesitan servicios para funcionar en la red. Algunos de estos servicios incluyen Word Wide Web, email, mensajería instantánea y telefonía IP. Los dispositivos interconectados a través de medios para proporcionar servicios deben estar gobernados por reglas o protocolos.

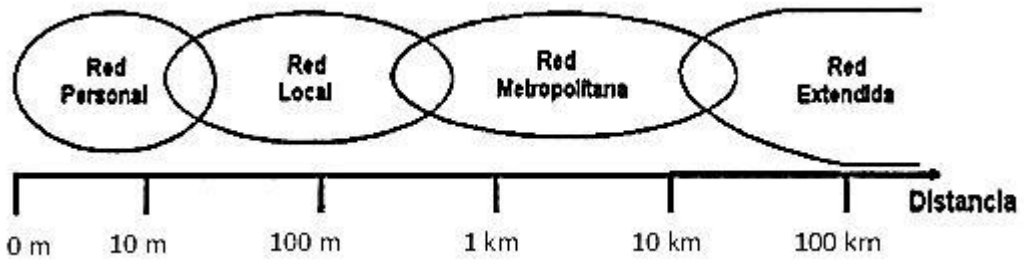
La academia de CISCO describe los servicios de red como programas de computación que respaldan la red humana siendo estos una herramienta que facilita la comunicación, el servicio web es el comúnmente más utilizado.

Hoy en día la web se ha popularizado y es uno de los servicios que más se utiliza, por tal razón toda red debe prestar este servicio a los usuarios.

6.1.3 Tipos de Redes

A continuación se describen los tipos de redes

Figura No. 1 Tipos de redes



Fuente: Dordoigne & Atelin (2006)

.

6.1.3.1 Red de Área Personal (Personal Área Network)

Dordoigne & Atelin (2006), el alcance de red más restringido en ingles se llama Personal Área Network (PAN). Centrada en el usuario, designa una interconexión de equipos informáticos en un espacio de una decena de metros en torno al usuario, el Personal Operating Space (POS).

Ésta puede extenderse a diez metros de proximidad entre los demás usuarios, es la red comúnmente más utilizada dado por el espacio que puede abarcar.

La mayoría de personas tienen su propia red PAN, con el simple hecho de contratar un servicio de conexión a internet. Cada proveedor de servicios de internet, facilita un enrutador donde se puedan conectar una serie de equipos siempre y cuando estén al alcance establecido.

6.1.3.2 Redes de Área Local o LAN (Local Área Network)

Andrew (2003), comenta que las redes de área local (generalmente conocidas como LAN son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud.

El desarrollo de la red LAN ha contribuido generalmente para compartir información y dispositivos dentro de una misma institución o empresa, con el fin de que toda información extraída de la red sea de carácter privado y utilizada de la mejor manera. Por ello cada empresa que utiliza equipos informáticos para administración de la información cuenta con una red local, con la que comparten dispositivos tales como impresoras, servidores que forman parte de la red, implementando políticas que aseguran la información propia de la empresa o institución.

Por ejemplo las empresas como la Productos Lácteos S.A necesitan la comunicación constante con las diferentes áreas que se encuentran distribuidos por su infraestructura y para ello hacen uso de correos corporativos que están configurados bajo una conexión LAN.

6.1.3.3 Redes de área Metropolitana o MAN (Metropolitan Área Network)

Andrew (2003), una red de área metropolitana (MAN) abarca una ciudad.

Tal como se explicó anteriormente la amplitud de esta red es de mayor distancia conformada por una cantidad de usuarios equivalentes a una ciudad.

Las empresas que brindan servicios de cable, telefonía móvil y convencional, son las más comunes, capaz de operar una red de esta magnitud y brindar los servicios a miles de clientes que forman parte de la red al suscribir su servicio. Otro ejemplo claro de la redes MAN es la cadena de cajeros automáticos pertenecientes a la diferentes empresas bancarias.

6.1.3.4 Red de área amplia o WAN (Wide Área Network)

Andrew (2003), dice que una red de área amplia (WAN), es la que abarca una gran área geográfica, con frecuencia un país o un continente con un conjunto de máquinas diseñado para programas (es decir, aplicaciones) de usuario.

De acuerdo al crecimiento de la población y a la necesidad de estar comunicados las redes han venido evolucionando y desarrollándose tanto en servicios como en tamaño, es así como surgen las redes de área amplia abarcando hasta la totalidad de países y continentes a nivel mundial.

La red de área amplia (WAN) comúnmente más conocida por las personas es la internet (Interconexión de redes), a través de la internet se puede estar conectados con el resto del mundo. A través de la internet se pueden hacer uso de diversos servicios en línea a nivel mundial tales como el trámite de visa, transacciones bancarias, envío de remesas, videos conferencias, entre otros... a continuación la Figura No. 2 se muestra claramente la distribución y comunicación mundial.

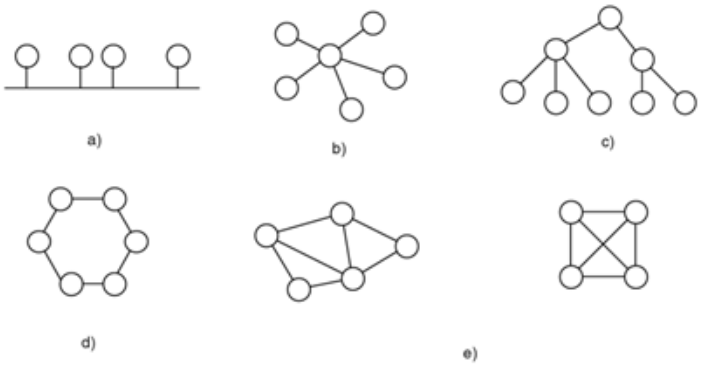
Figura No. 2 Representación de una red Amplia WAN

Fuente: Dordoigne & Atelin, (2006)

6.1.4 Topologías

De acuerdo a Serra (2002) la topología (de red) es la disposición lógica de los elementos (enlaces, nodos) de una red. Así pueden definirse diversos modelos de topologías básicas tal como se puede observar en la Figura No.3.

Figura No. 3 Topología de Red



Fuente: Serra, (2002)

Uno de los elementos esenciales para el diseño de una red son las topologías que no son más que una forma de distribución ordenada, secuencial y disponibilidad de los

servicios a través de la red. Éste diseño depende de los recursos económicos y fin al que responde.

Cada una de las empresas e instituciones poseen un diseño diferente de acorde a las necesidades.

6.1.4.1 Bus o canales

En la topología de Bus o Canal “todos los nodos están unidos por un único enlace común, además los módulos de comunicaciones están conectados (colgados) de un único medio de comunicación (bus) que recorre todas las estaciones”, Serra (2002).

Para Riera & Alabau (1992) en ésta topología no es necesario efectuar encaminamientos ya que los mensajes recorrerán sucesivamente todas las estaciones siguiendo el orden de conexión, aquí la topología es de difusión y todas las estaciones reciben simultáneamente la información.

Cada información que es enviada a través de la red debe recorrer cada uno de los host agregados a la red recibiendo y descartando la información recibida hasta encontrar su host destino.

Hoy en día son pocas las redes con topología de bus pero podemos tomar como un ejemplo muy claro la señal de televisión por cable, la señal es retransmitida a todos los usuarios en un solo sentido.

6.1.4.2 Estrella

Riera & Alabau (1992), todas las estaciones están unidas, mediante medios bidireccionales, a un módulo nodo central que efectúa funciones de conmutación. Es también de aplicación frecuente en redes muy centralizadas o en sistemas de control.

Conjunto de equipos conectados a través de medios con direcciones a un nodo principal.

Las empresas en aras de la modernización tienen estaciones telefónicas IP internas siendo frecuente la topología estrella donde todos los usuarios dependen de un nodo central o casa matriz para mejorar la comunicación entre sus departamentos.

6.1.4.3 Árbol

Riera & Alabau (1992)**,** es una extensión de la arquitectura en estrella por interconexión de varias. Permite establecer una jerarquía clasificando a las estaciones en grupos y niveles según el nodo a que están conectadas y su distancia jerárquica al nodo central.

Las características similares a la red en estrella, reduce la longitud de los medios de comunicación incrementando el número de nodos. Se adapta a redes con grandes distancias geográficas y predominancia de tráfico, características más propias de una red pública de datos que de una red privada local.

Los distintos nodos están distribuidos en forma de ramificaciones sucesivas a partir de un único nodo raíz Serra (2002).

Dispositivos interconectados clasificados por grupos o niveles dependiendo del nodo y su distancia jerárquica. Puede ampliarse según la cantidad necesaria de usuarios agregando subnodos o nodos hijos.

Redes en expansión sin control de su ampliación física tienden a desarrollarse con topología de árbol implementada en grandes edificios por la magnitud de su crecimiento.

6.1.4.4 Anillo

Los nodos están unidos en cadena, uno tras otro, cerrándose ésta sobre si misma (de un único nodo raíz), Serra (2002).

Los módulos de comunicaciones de las estaciones están interconectados formando un anillo, de forma que todas las informaciones pasan por todos los módulos que únicamente envían a la estación los paquetes a ella destinados. Riera & Alabau (1992).

El flujo de información pasa por todos los equipos y se envían de manera única los paquetes destinados cerrando el anillo un nodo antes al nodo raíz.

Para prevenir la caída de la red se utiliza topología anillo para tener un medio de emergencia o ruta de protección ante cualquier eventualidad.

6.1.4.5 Malla

Los distintos nodos están más o menos densamente unidos entre sí por enlaces directos (sin seguir ninguna jerarquía particular). Cuando cualquier nodo está unido directamente a todos los demás mediante un enlace directo. Serra (2002).

El coste en los medios de comunicación depende de número de conexiones y suele ser elevado, ganando sin embargo en fiabilidad frente a fallos y en posibilidades de reconfiguración. El coste de instalación al aumentar el número de estaciones es también grande y sobre todo de dificultosa realización en una red ya instalada lo que representa un gran inconveniente en redes locales. No se adapta a grandes dispersiones geográficas pero permite tráficos elevados con retardos medios bajos. Riera & Alabau (1992).

Nodos unidos simultáneamente de forma directa sin jerarquía y pueden transmitir sin tener riesgo alguno de pérdida de conexión siendo una red muy robusta por su disponibilidad.

Esta topología se implementa en la telefónica móvil que provee cualquier de las operadoras existentes en el país. La comunicación se logra desde cualquier nodo disponible siempre y cuando estemos dentro de la cobertura de la red.

6.1.5 Red Inalámbrica

6.1.5.1 Origen

Mendigaña & Reina (2008), el origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizados por ingenieros de

IBM en suiza, consisten en utilizar enlaces infrarrojos para crear una red local en una fábrica.

Las redes locales inalámbricas tuvieron origen de experimentos con enlaces infrarrojos por ingenieros de la IBM.

En la actualidad este tipo de red es utilizada en la mayoría de instituciones y centros de estudios para brindar acceso a red inalámbrica a usuarios desde sus dispositivos.

6.1.5.2 Definición

Andreu J. Servicios en Red, (2010), las redes inalámbricas wireless (wireless network) son redes sin cable que se suelen comunicar por medios no guiados a través de ondas electromagnéticas. La transmisión y la recepción se efectúan a través de antenas.

Las redes inalámbricas se comunican a través de ondas electromagnéticas utilizando dispositivos con antenas que efectúan la transmisión y recepción normalmente una antena suele realizar ambos modos.

La instalación de una red inalámbrica privada dentro de un campus se debe emplear con dispositivos intermediarios como repetidores para alcanzar la distancia requerida.

6.1.5.3 Ventajas

Andreu J. Servicios en Red (2010), rápida instalación de la red: no necesita cablear, ni pedir permisos de obras, levantar las calles y calzadas de las ciudades.

Permiten movilidad: el medio de transmisión (de envío y recepción) no está sujeto a ningún cable, lo que permite una movilidad dentro del radio de recepción de señal.

Menos costes de mantenimiento: al no tener cableado, los costes de mantenimiento se reducen.

Productividad: las redes inalámbricas propician la colaboración, el teletrabajo.

Es la única solución para zonas a las que no llega el cableado, como es el caso de las zonas rurales diseminadas.

La ventaja principal radica en que la red no necesita cableado permitiendo accesibilidad, movilidad, menos costes de mantenimiento y es de modo productiva.

La mayoría de centroS de estudios superior brindan el servicio de red inalámbrica a los alumnos siendo propicio para no incurrir en mayores gastos de instalación y mantenimiento.

6.1.5.4 Desventajas

Andreu J. , Servicios en Red (2010) menciona que cambios atmosféricos: la lluvia, el viento (vientos fuertes, tornados, huracanes).

Interferencias externas: De otros emisores de microondas.

Falta de seguridad: Al emitirse libremente por el aire para poder ser interceptado por cualquiera, lo que requiere aumentar la seguridad y la encriptación.

Más errores: Por las interferencias.

Más costes iníciales: Los dispositivos, antenas. Son más caros.

La velocidad: es más limitada.

Los costos de adquisición de los dispositivos al instalar la red son altos. Los fenómenos naturales afectan directamente a las redes inalámbricas incurriendo en interferencias. La seguridad es un problema inminente debido a la libre emisión de la señal. Poseen velocidad limitada de acuerdo a la distancia.

Las redes inalámbrica que están bien instaladas presentan una desventaja que es común en la mayoría de redes estamos hablando de la seguridad ya que toda nuestra información está viajando por el medio (aire) y cualquier intruso con conocimientos suficientes puede tomarla y utilizarla para hacer daño.

6.1.5.5 Redes inalámbricas según su tecnología

6.1.5.5.1 Infrarrojos

Gil, Pomares, & Candelas (2010), Las comunicaciones mediante infrarrojos se llevan a cabo mediante transmisores/receptores que modulan luz infrarroja. Las distancias alcanzadas son pequeñas (varios metros como mucho). Son empleados en los mandos a distancias de muchos dispositivos que envían datos en banda base.

Tecnología de corto alcance inundado de interferencias el cual logra comunicación a través de ondas de luz que es modulada.

Medio de comunicación utilizado en sistemas de alarmas de seguridad para pequeñas empresas. Teniendo presencia comúnmente en control remoto de equipos domiciliares que incorporan esta tecnología.

6.1.5.5.2 Bluethooth

Carballar Falcón (2010), bluethooth es una tecnología que, al contrario de Wi-Fi, no tiene por objetivo soportar redes de ordenadores, sino, más bien, para comunicar un ordenador con cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, una PDA con su ordenador.

Sistema de comunicación entre un equipo y sus respectivos dispositivos periféricos.

Utilizado para la conexión entre un smartphone y su dispositivo periférico por ejemplo: auricular (manos libres).

6.1.5.5.3 Wi-Fi

Hoy en dia la mayoria de dispositivos electronicos tales como computadores portatiles, smartphone entre otros trabajan con tecnologia wifi, según Carballar (2010), una comunicación inalámbrica es aquella que se lleva a cabo sin el uso de cables de interconexión entre los participantes; por ejemplo, una comunicación con teléfono móvil

es inalámbrica, mientras que una comunicación por teléfono fijo tradicional de cable no lo es.

La red de comunicación Wi-Fi no utiliza cables para conexión entre dispositivos ocupando niveles de preferencia entre todo tipo de usuario.

En sitios públicos y privados se disponen comúnmente de redes Wi-Fi convirtiéndose en un sistema de comunicación personal.

6.1.5.5.4 Microondas por satélites

Gil, Pomares, & Candelas (2010), un satélite de comunicaciones esencialmente una estación que retransmite microondas. Se usa como enlace entre dos o más receptores/transmisores terrestres denominados estaciones bases. El satélite recibe la señal en una banda de frecuencia, lo amplifica y posteriormente lo retransmite en otra banda.

Estación que enlaza dos o más receptores/transmisores terrestres amplificando microondas.

La estación televisa mexicana transmite en un área local y a larga distancia utilizando antenas transmisoras con enlace satelital por medio de microondas.

6.1.5.5.5 Microondas terrestres

Herrera (2003), los sistemas de radio por onda de tierra (o de superficie) se emplean para transmitir ondas de relativamente baja frecuencia en el rango de 50 KHz a 2 MHz. Se emplean principalmente para transmisiones de radiodifusión, sobre todo para radiodifusoras comerciales, y de radionavegación.

Sistema de microondas terrestres que transmite en un radio multidireccional con frecuencia en rango de 50 KHz a 2 MHz que operan sobre mástiles de varios metros de altura.

Una estación de radio con cobertura nacional como es la “Radio Ya” que transmite ondas por superficie relativamente bajas de alta potencia.

6.1.5.5.6 Onda de radio

Herrera (2003), microondas (MO) son el nombre que reciben las ondas de radio cuya frecuencia es mayor a los 1000 KHz (1GHz) y cuya longitud de onda es de unos cuantos centímetros.

Microondas (MO) de mayor alcance con enlaces troncales de punto a punto entre dos ciudades utilizando antenas pequeñas altamente direccionales.

Empresa operadora de telefonía Movistar presente en todo Nicaragua realiza transporte de sus servicios a través de enlaces troncales de onda de radio tales como telefonía móvil, transporte de datos corporativos e internet.

6.1.5.5.7 Wimax

Sánchez Herrera, (2012), acrónimo de World Wide Interoperability for Microwave Access (Interoperabilidad Mundial para Acceso por Microondas), es una norma de transmisión por ondas de radio de última generación que permite la recepción de datos por microondas y retransmisión por ondas de radio.

Sistema de última generación de recepción de datos por microondas y retransmisión por ondas de radio donde se crean estaciones o nodos para retransmisión de los servicios a clientes.

La empresa IBW ha impulsado proyecto de servicios de conectividad basada en el estándar WIMAX que proporciona internet móvil sobre frecuencias licenciadas a través de pequeños nodos.

6.1.6 Diseño de Redes

6.1.6.1 Diseño de Red Física

Mendigaña & Reina (2008), Las redes inalámbricas están organizadas en 3 configuraciones lógicas:

- Enlace punto a punto.
- Enlace punto a multipunto.
- Enlace multipunto a multipunto.

La redes inalámbricas se organizan en configuraciones logicas: nodo a nodo, nodo a multiples nodos o multiples nodos a multiples nodos.

Las empresas a nivel mundial organizan sus equipos según el diseño más factible para que sus clientes accedan a la red.

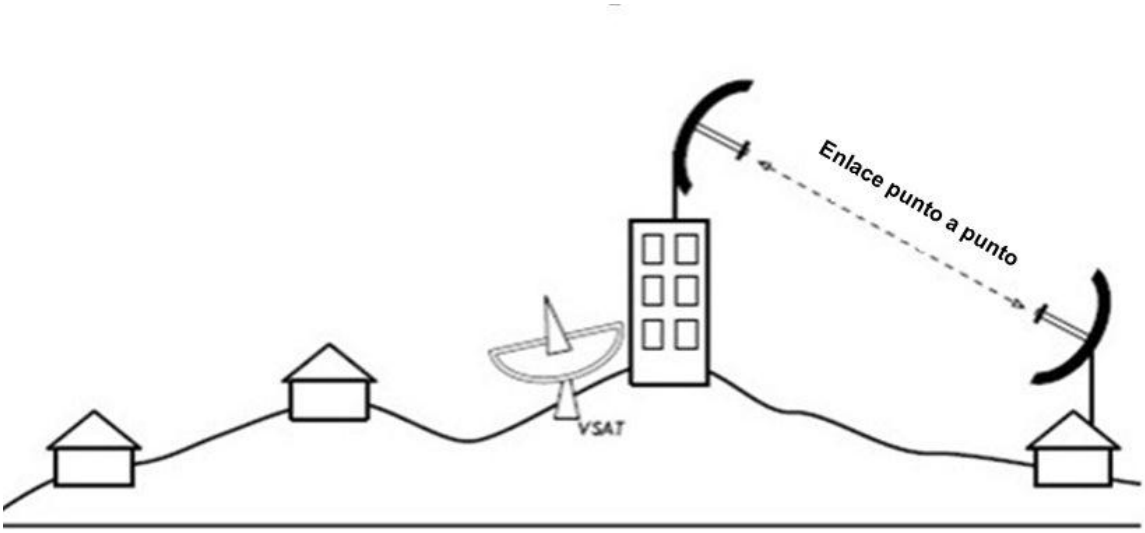
6.1.6.1.1 Enlaces punto a punto

Mendigaña & Reina (2008), Los enlaces punto a punto generalmente se usan para conectarse a internet donde dicho acceso no está disponible de otra forma. Uno de los lados del enlace punto a punto estará conectado a internet.

Es la forma de conectarse a internet a través de un nodo con acceso a internet mientras el otro nodo solo hace enlace de conexión.

La institución gubernamental MAGFOR utiliza conexión punto a punto con el proveedor de servicio de internet a través de un radio enlace inalámbrico.

Figura No. 4 Enlace Punto a Punto



Fuente: Mendigaña& Reina, (2008)

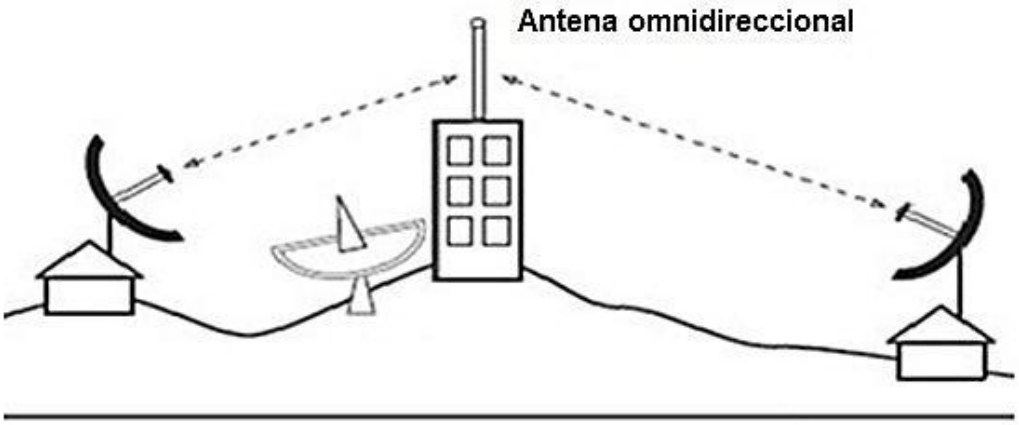
6.1.6.1.2 Enlaces punto a multipunto

Mendigaña & Reina (2008), la siguiente red comúnmente encontrada es la punto a multipunto donde varios nodos están hablando con un punto de acceso central, esta es una aplicación punto a multipunto.

Los enlaces punto a multipunto son comunes y su conexión esta basada en un nodo central comunicando con el resto de nodos perifericos.

La conexión de punto a multipunto es la utilizada por los parque wifi existentes en las cabeceras departamentales de todo el pais de Nicaragua que utiliza dispositivos Cisco denominado Meraki.

Figura No. 5 Enlace Punto a Multipunto



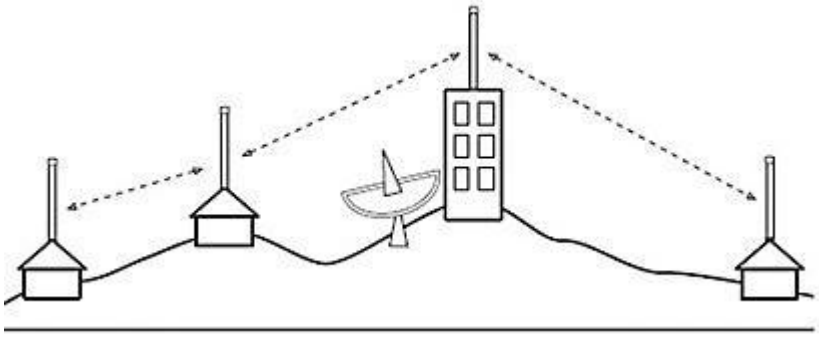
Fuente: Mendigaña & Reina, (2008)

Es la red más común encontrada donde múltiples nodos se conectan a internet a través de un nodo central que proporciona la conexión.

6.1.6.1.3 Enlaces multipunto a multipunto

Mendigaña & Reina (2008), en una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.

Figura No. 6 Enlace Multipunto a Multipunto



Fuente: Mendigaña & Reina, (2008)

Enlace multipunto a multipunto es la comunicación directamente entre todos los nodos sin jerarquía superior.

6.1.6.2 Diseño de Red Lógica

6.1.6.2.1 Modelo de Referencia OSI

Andrew (2003), este modelo está basado en una propuesta desarrollada por la ISO (Organización Internacional de los Estándares) como un primer paso hacia la estandarización internacional de los protocolos utilizados en varias capas Day y Zimmermann (1983).

El modelo OSI tiene 7 capas. Podemos resumir brevemente los principios que se aplicaron para llegar a dichas capas:

Una capa se debe crear donde se necesite una abstracción diferente.

Cada capa debe realizar una función bien definida.

La función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.

Los límites de las capas se deben elegir a fin de minimizar el flujo de información a través de la interfaces.

La cantidad de capas debe ser suficientemente grande para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

La Interconexión de sistemas abiertos nace de una propuesta desarrollada por la Organización Internacional de los Estándares para lograr la estandarización internacional.

Capa física

Andrew (2003), en esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación.

La Capa física se encarga de enviar un bit y que con seguridad se reciba este mismo en el extremo opuesto.

Capa física crea una señal de dígitos binario que pueda ser interpretada al otro lado de la red a través de medios físicos de una red tal como fibra óptica, cable de cobre o aire.

Capa de enlace de datos

Andrew (2003), la tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión.

La capa de enlace de datos fragmenta los datos de entrada en tramas en forma secuencial y el receptor envía un acuse de recibo de cada trama recibida.

La capa de datos provee una comunicación eficiente libre de errores en máquinas adyacentes perteneciente a la misma red o subred.

Capa de red

Andrew (2003), Esta capa controla las operaciones de la subred. Un aspecto clave del diseño es determinar cómo se enrutan los paquetes desde su origen hasta su destino. Las rutas pueden estar basadas en tablas estáticas codificadas en la red.

La capa de red enruta los paquetes desde su origen hasta su destino basadas en tablas estáticas codificadas en la red.

La capa de red proporciona un esquema para que una computadora A pueda encontrar una computadora B en la red.

Capa de transporte

Andrew (2003), La función básica de esta capa es aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasar estás a la capa de red y asegurarse de que todas piezas lleguen correctamente al otro extremo.

Capa de transporte recibe datos de las capas superiores y las divide en unidades pequeñas y las pasa a la capa de red asegurándose que lleguen al otro extremo de forma correcta.

La capa de transporte es un puente entre dos puntos, hace una conexión de extremo a extremo y mantiene el flujo de la red.

Capa de sesión

Andrew (2003), esta capa permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen varios servicios, como el control del diálogo (dar seguimiento a quien le toca transmitir).

Capa de sesión permite establecer conexiones entre usuarios teniendo control del diálogo administrando token para que los dos extremos realicen una operación crítica simultáneamente.

Una conversación con la aplicación whatsapp se logra mediante la capa de sesión ya que establece una comunicación entre 2 dispositivos por medio de una sesión activa.

Capa de presentación

Andrew (2003), a diferencia de las capas inferiores, a las que les corresponde principalmente mover bits, a la capa de presentación le corresponde la sintaxis y la semántica de la información transmitida.

La capa de presentación se encarga de operar la parte de las estructuras abstractas correspondiendo el orden y los significados de la información transmitida.

Capa de presentación se encarga de entrar a mi computadora a través de un escritorio remoto desde otro terminal ubicado en otro lugar manejando estructuras de datos abstractas.

Capa de aplicación

Andrew (2003), esta capa contiene varios protocolos que los usuarios requieren con frecuencia. Un protocolo de aplicación de amplio uso es HTTP (protocolo de transferencia de hipertexto), que es la base de World Wide Web.

La capa de aplicación opera con varios protocolos que los usuarios usan a diario haciendo peticiones desde el navegador a los servidores de la página requerida.

Al interactuar con un cajero automático de un banco estamos haciendo uso de la capa de aplicación.

6.1.6.2.2 Modelo TCP / IP

Dordoigne & Atelin (2006), a principios de los años 70, Bob Kahn, del Defense ARPA (DARPA), ex ARPA, trabaja con VintonCerf, investigador de Stanford Institute, sobre nuevos protocolos que permitieran conectar redes. Así nace el TCP/IP. En 1979, Arpanet emigra hacia TCP/IP.

La integración de los protocolos de internet en el UNIX Berkeley Software Distribution (BSD) y la difusión casi gratuita en las universidades contribuyó a mejorar el éxito de esta generación.

En los años 70 BodKahn, del Defense ARPA, laboro con VintonCerf, investigador de Stanford Institute investigaron sobre nuevos protocolos para lograr conectar redes de ahí Arpanet emigra a TCP/IP. En 1978 Arpanet utiliza líneas telefónicas y toma el nombre de internet.

La generación de los protocolos:

La familia TCP/IP, que implicaba varias decenas de protocolos, define un modelo de 4 capas de red.

Se trata de los conocidos protocolos de comunicación y aplicación para conectar sistemas heterogéneos, independientes de la capa física.

El Transmisión Control Protocol (TCP) es un protocolo de enrutamiento que garantiza un servicio fiable, orientado a la conexión de un grupo importante de octetos.

En contraste con el TCP, el Datagram Protocol (UDP) es el protocolo de enrutamiento no orientado a la conexión. Es muy rápido pero poco fiable.

El Internet Protocolo (IP) proporciona un sistema de entrega de paquetes, sin conexión y no fiable. Administra las direcciones lógicas, que dividen el identificador del nodo en un número de red lógico y un número de periférico sobre 4 octetos (en IP versión 4).

El protocolo IPv6 o IP Next Generación (NG) ya está disponible en varios sistemas operativos como Linux o Windows. Se puede activar en el momento que se desee. Bajo Windows XP basta con escribir el comando IPv6 install y después reiniciar el ordenador.

Una de las claves del éxito de los protocolos de internet reside en el hecho de que el modelo propuesto es independiente de las capas físicas y de conexión de datos (capas 1 y 2 del modelo OSI).

Los protocolos TCP/IP son decenas y se definió en modelo de 4 capas de red simplificando el modelo OSI que contiene 7 capas.

El Transmission Control Protocol (TCP) que proporciona enrutamiento orientado a la conexión, Datagram Protocol (UDP) da enrutamiento no orientado a la conexión, El Internet Protocol (IP) tiene un sistema de entrega de paquetes sin conexión y no confiable y El protocolo IPv6 o IP Next Generación (NG) disponible en sistemas operativos Linux o Windows.

6.1.7 Tipos de medios

6.1.7.1 Medios Alámbricos

Herrera (2003), los medios alámbricos de transmisión se utilizan en la redes de cómputo para instrumentar lo que se conoce como cableado de la red.

Es el intercambio de información entre los nodos de la red a través de un medio físico que es generalmente un cable de cobre.

Los Ciber de la ciudad de Matagalpa tienen estructuradas sus redes con cable de cobre para minimizar los costos de instalación.

6.1.7.2 Electromagnéticos

Herrera (2003), otro medio de transmisión de información es el “espacio libre”. Se trata de un medio electromagnético, toda vez que la señal se propaga a través de él es de naturaleza electromagnética, es decir, ondas a base de campos eléctricos y magnéticos que se conocen como ondas de radio.

Comunicación con regiones difíciles, en donde el tendido de cables y de mantenimiento no es práctico.

Es el medio electromagnético que ocupa el espacio libre para que la señal se propague a través de la naturaleza electromagnética siendo una forma efectiva de comunicación.

La Policial Nacional utiliza radiocomunicación basado en ondas hertzianas para la comunicación con sus patrullas en todo el casco urbano de la ciudad de Matagalpa.

6.1.7.3 Fibra óptica

Herrera (2003), la fibra óptica es una nueva tecnología de cable que se utiliza para la instalación de redes locales. Consiste en un núcleo central muy delgado de vidrio con alto índice de refracción de la luz.

Fibra óptica es una nueva tecnología para montar redes WAN, consistiendo en un cable con núcleo de vidrio que hace refracción a la luz estando cubierto por varias capas que tiene funciones de amortiguamiento, aislamiento y protección.

La ciudad de Matagalpa posee anillos de fibra óptica de diferentes empresas de telecomunicaciones logrando satisfacer las necesidades de miles de usuarios.

6.1.8 Dispositivos de una red inalámbrica

Figura No. 7 Dispositivos de Una Red Inalámbrica

Fuente: Andreu J. (2011)

6.1.8.1 Router

El Router o enrutador es un periférico de comunicaciones empleado para enlazar diferentes redes entre sí.

Al igual que el switch, el router se conecta al equipo a través del puerto RJ-45 (Ethernet) y en determinados modelos, por puerto serie para entrar en modo consola. Gallego (2010).

A través de este dispositivo se pueden enrutar muchas redes, a la vez aplicar diferentes configuraciones de protocolos, seguridad y direccionamientos.

Al implementar una red de acceso a internet es parte fundamental la instalacion de un enrutador, este es el punto de conexion entre la internet y la red privada del usuario. De igual manera puede ser utilizado dentro de una red privada para el direccionamiento de subredes.

6.1.8.2 Modem

Un modem es un equipo que se encarga de transmitir y recibir datos por un cable o medio radioeléctrico. Si disponemos de una conexión ADSL o de una empresa de cable, el equipo que nos instalan en nuestras casas dependiendo si es un modem ADSL o modem cable. Carballar, (2010)

Tenemos diferentes tipos de modem todo en dependencia del tipo de medio o tecnología que nos brinda el operador al que se esta suscrito, los modem instalados se encargan de dar acceso ya sea a un servicio de datos o internet atraves la red del proveedor de servicio.

En nuestro país podemos observar que tenemos muchos proveedores de servicios donde los modem más conocidos son de conexion ADSL, Cable y 3G.

6.1.8.3 Switch (Conmutador)

Este dispositivo es el responsable de analizar la información que recibe de cada uno de los terminales de la red y encaminarla a su destino correspondiente. Digamos que es como una central de comunicación de datos, Carballar (2010).

Todos los datos paquetes enviados desde cada uno de los dispositivos primeramente pasan por el switch es ahi donde donde se determina hacia donde será su destino, si pertenece a la misma red o salir hacia internet.

Para implementar una red inalámbrica o cableada se debe de tomar en cuenta el tipo de switch a instalar ya que si se desea tener conexión de manera inalámbrica debemos de tener muy en cuenta esta característica.

6.1.8.4 Punto de Acceso o Access Point (AP)

El punto de acceso no sólo es el medio de intercomunicación de todos los terminales que forman la red sino que también es el puente de interconexión de la red fija e internet, Carballar (2010).

Un AP puede tener una distancia determinada para brindar acceso a los usuarios, podemos tener acceso a el, soló y únicamente a través de dispositivos inalámbricos.

La instalación de un AP solamente se utiliza en lugares donde necesitamos tener acceso inalámbrico, si bien vemos estos tienen la misma función de un switch, la cantidad de AP instalados en una red será variable de acuerdo a la amplitud del local o lugar.

6.1.8.5 Repetidor inalámbrico

Un repetidor inalámbrico es un equipo que recibe la señal de radio de un punto de acceso y la retransmite, extendiendo de esta forma el área de cobertura de dicho punto de acceso, Carballar (2010).

Dispositivo que se utiliza de puente para retransmitir tráfico de red de un punto a otro utilizado para transmitir a mayor distancia la señal de forma inalámbrica.

Para la instalacion de una red inalámbrica con una distancia de gran magnitud, sera indispensable la utilización de dispositivos repetidores los cuales permiten abarcar una mayor longitud de señal inalámbrica.

6.1.8.6 Dispositivos finales

6.1.8.6.1 Dispositivos con acceso inalámbrico (Computadores, Impresoras, Celulares, Tablet)

Tener acceso a una red inalámbrica nos proporciona muchas ventajas, simplemente hay que pensar en la alternativa actual: utilizar formularios en papel, copiar del papel al ordenador, manejar información impresa no actualizada, tener que moverse para conseguir acceder a la información de la empresa. Carballar Falcon, (2010).

Todo dispositivo móvil o pórtatil con acceso inalámbrico se convierte en un dispositivo final de la red, desde estos dispositivos tenemos accesos a toda la informacion necesaria alojada en la red de datos o internet.

El objetivo de implementar una red inalámbrica en cualquier institución o negocio es poder acceder a ella mediante dispositivos inalámbricos o lo que llamamos dispositivos finales, desde diferentes lugares y así mismo tener acceso a información actualizada mediante la conexion a la red.

6.1.8.6.2 Placas Inalámbricas

Andreu J (2011), las placas wireless o tarjetas wireless también se rigen por los estándares 802.11, soportando velocidades entre 11,54 o 600 Mbps.

Placas que pueden recibir ancho de banda con velocidades de hasta 600 Mbps dependiendo de la necesidad de los usuarios.

Tarjetas inalámbricas (wireless) Cisco LAN Client 802.11a que alcanza velocidades de 54 Mbps puede ser ensamblada en ordenadores que no cuenten con tecnología inalámbrica.

6.1.9 Dificultades en el funcionamiento de la red inalámbrica

La tecnología WI-FI es flexible y fácil de utilizar, pero no hay que olvidar que usa las ondas de radio, que, como todas las ondas, tienen un alcance limitado así lo explica Soyer (2005).

Desde que surge la tecnología WI-FI se han implementado una serie de protocolos y mejoras, todo con el fin de disminuir las diferentes dificultades al utilizar esta tecnología que hoy en día se ha convertido en una de las más utilizadas e implementadas en la mayoría de dispositivos electrónicos.

Una red local inalámbrica es muy vulnerable a interrupciones por motivos físicos, como lógicos, un ejemplo es la red inalámbrica de UNAN FAREM Matagalpa, donde los dispositivos están expuestos a manipulaciones físicas.

6.1.9.1 Distancia

El hardware WI-FI básico tiene un alcance teórico de 30 metros en interior y de 100 metros en exterior. En la práctica hay que contar más bien con un alcance de 10 a 15 metros interior, Soyer (2005).

En el exterior, cuente la distancia entre su punto de acceso y la pared externa (inferior a 15 metros) y la distancia entre dicha pared y el lugar del jardín en que desee instalarse (como máximo, 10 metros).

La distancia de alcance de una red inalámbrica siempre va a depender de la cantidad de obstáculos que se encuentren, tal como es explicado por Soyer, si vemos el alcance entre una pared y el dispositivo es menor que el alcance en exterior.

Este factor se debe tomar en cuenta cuando se está instalando una red inalámbrica diseñando la manera que cada dispositivo alcance su máximo alcance, ubicándolo en lugares estratégicos, un dispositivo muy conocido son los modem que brindan las empresas proveedoras de internet estos tienen un alcance máximo de 30 metros en interiores y 100 metros en exteriores.

6.1.9.2 Obstáculos

Si quita los potenciales obstáculos y fuentes de interferencia, la mayoría de aparatos inalámbricos pueden alcanzar distancias de casi el doble de lo que puede esperar adentro. Wiley & Canada (2011).

Cada obstáculo que interviene en una red inalámbrica provocá pérdidas de señal entre el punto de acceso y los dispositivos que se conecten a el. Por tal razon se debe de instalar la cantidad de puntos de accesos necesarios para cubrir por completo cada área que conforme esta red.

Dificilmente se lograra eliminar por completo los obstáculos en una red inalámbrica, solo podemos jugar con la ubicación de los equipos garantizando una conexión casi estable,

para referencia podemos tomar una red publica como son los parques centrales de cada municipio de Nicaragua.

6.1.9.3 Seguridad

Las reglas cambian significativamente en las redes inalámbricas. A pesar de que el alcance aparente de su punto de acceso puede ser de unos pocos cientos de metros, un usuario con una antena de gran ganancia puede ser capaz de hacer uso aunque este a varias manzanas de distancia, Commons (2007).

Las ondas de radios pueden ser interceptadas por cualquier individuo con intencion de realizar daños a la red utilizando herramientas diseñadas para realizar ataques y poner en peligro la información personal o privada de cada usuario o de la institución a la que pertenece la red.

Esta es la razon por la que cada empresa debe adoptar medidas de seguridad que protejan y garanticen la confiabilidad de la red, donde cada usuario sin temor alguno pueda tener acceso a la informacion a tráves de la red.

6.1.9.3.1 Seguridad Física

Cuando instala una red, usted está construyendo una infraestructura de la cual la gente dependerá y por lo tanto, la red debe ser confiable. Para la mayoría de los casos, las interrupciones en los servicios ocurren a menudo debido a alteraciones hechas por las personas, accidentalmente o no, Commons (2007).

La seguridad física es una de las prioridades a tener en cuenta ya que el acceso y la visibilidad al público pone en riesgo toda una red, el poner alertas, rotulos y etiquetas es una de las formas para que todas las personas esten alertas antes cualquier incidente que puedan provocar.

En la gran mayoría de empresas y redes privadas podemos observar la gran deficiencia de la infraestructura de la red y la vulnerabilidad de las redes expuestas a cualquier alteración, donde las principales causas son provocadas por personas.

6.1.9.3.1.1 Políticas de Seguridad Físicas

Según Castro, Diaz, Alzorriz, & Sancristobal (2012), las políticas de seguridad son una serie de procedimientos relacionados con las seguridad física, tanto en el aspecto de control de acceso físico a equipos como el de tener planes de contingencia y emergencia.

Las políticas de seguridad son el protocolo a seguir por parte de los recursos humanos involucrados en la manipulación de equipos informáticos de la red.

En Nicaragua no todas las empresas e instituciones tienen políticas de seguridad debido a los costos que repercuten su mantenimiento y adquisición.

6.1.9.3.1.2 Accesos a personal

El espacio en el que se encuentre el hardware debe contar con diferentes restricciones de acceso a personas, en función del impacto que tendría sobre la zona el robo o el deterioro de los equipos y sobre todo, de la información, Aguilera Lopez (2010).

El hardware o partes físicas de una red es de las partes más importante para el buen funcionamiento por tal razón deben estar en lugares seguros donde solamente haya ingreso por personal autorizado.

Si bien la mayoría de empresas toman en cuenta estas medidas de seguridad no todas la aplican correctamente, ya sea por falta de información o capacitaciones técnicas a sus trabajadores, en Nicaragua nos encontramos en un país donde los recursos económicos son bastantes limitados solo las grandes empresas logran cumplir por completo el aseguramiento de sus equipos implementando tecnologías, normas y protocolos de accesos al personal que desee realizar algún cambio en hardware o software.

6.1.9.3.1.3 Racks

Los Racks suponen una medida de seguridad más, puesto que sirven para organizar de forma adecuada los dispositivos, lo que disminuye el riesgo de cortocircuitos a causa de un cableado mal instalado, y favorecen la colocación en zonas seguras y bien protegidas, Aguilera Lopez (2010).

Los Racks favorecen en gran medida la organización de equipos, de igual manera protegen el hardware de descargas y riesgos eléctricos.

En nuestro país se pueden observar casi en todas las redes la utilización de Racks, pero no se garantiza la protección correcta a los equipos debido a la mala instalación eléctrica o un cableado mal estructurado.

6.1.9.3.1.4 Armarios ignífugos

Los armarios ignífugos están equipados con sistemas que los protegen del fuego además, están fabricados con materiales aislantes. Esta definición no varía para los armarios ignífugos con aplicación en el mundo de la informática, y algunos armarios rack ya cuentan con estos sistemas, Aguilera Lopez (2010).

Este sistema protege los equipos contra incendios aislando totalmente la parte exterior con la interior donde están ubicados estos equipos

La aplicación de estos sistemas en nuestras redes nos brinda un punto más a favor de la seguridad para proteger los equipos principales tales como router y switch ya que son los principales elementos de una red.

6.1.9.3.1.5 Instalación Eléctrica

Si prácticamente todo el hardware funciona mediante corriente eléctrica, es natural considerarlo como un punto importante a tener en cuenta al hablar de seguridad, Aguilera Lopez (2010).

Podemos ver la red eléctrica desde dos puntos de vista: la externa, que pertenece a la compañía proveedora de electricidad, y la interna, que es propiedad de la empresa.

La instalación eléctrica en un factor sumamente importante para el funcionamiento de equipos, ya sea la conexión interna como la externa debe acoplarse para estar atentos ante cualquier eventualidad a la vez tener un medio de comunicación con la empresa proveedora de este servicio.

Tal vez muchos ven esta parte como un factor fundamental y que todo dependerá de la empresa proveedora de este servicio, pero a lo interno se deben tomar muchas medidas basadas en normas eléctricas, ya que un sobre voltaje, descargas eléctricas hasta el ambiente donde se encuentre un equipo influye en la vulnerabilidad de este y hasta puede ser dañado por esta causa.

6.1.9.3.1.6 SAI

Los sistemas de alimentación ininterrumpida, también llamados SAI constituyen un elemento básico en la protección de nuestro hardware y por extensión, de los datos almacenados en él.

A pesar de lo que su nombre nos pueda sugerir, estos dispositivos no sirven para seguir trabajando durante un corte de electricidad prolongado, sino que nos permiten guardar con seguridad los datos si falla el suministro eléctrico, Aguilera Lopez (2010).

Este elemento protege de forma temporal la información existente al momento de un corte eléctrico, dando el tiempo necesario para guardar información y apagar normalmente todos los equipos.

Para la compra de este equipo se debe de tener en cuenta el tiempo que durará la energía después de un corte energético, en el mercado existen diferentes equipos de protección con diferentes costos económicos, por tal razón es un sistema muy fácil de adquirir obteniendo un gran beneficio en la seguridad de la red.

6.1.9.3.1.7 Temperatura

El funcionamiento idóneo de los equipos informáticos es a baja temperatura, y la ideal se encuentra entre 15 y 25 ºC, aunque trabajan sin dificultad entre los 10 y los 32 ºC, Aguilera Lopez (2010).

La climatización o temperatura se debe trabajar de acuerdo a la exigencias o normas establecidas de manera que la climatización proporciones un ambiente idóneo a los equipos.

El mal funcionamiento en equipos puede ser provocado por la temperatura, este comportamiento se encontrará en lugares con alta temperatura provocando que los equipos no trabajen al cien por ciento, es por ello que se deben implementar sistemas que garanticen la climatización conveniente.

6.1.9.3.2 Seguridad Lógica

La seguridad lógica se encarga de asegurar la parte software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y datos, Cervigon & Alegre (2011).

Siempre que se escuche hablar de la seguridad lógica nos referimos a la configuracion de aplicaciones. Hoy en dia existen muchos softwares diseñados especificamente para la seguridad en las redes, pueden ser descargados desde la internet.

6.1.9.3.2.1 Firewall

Los autores Castro, Diaz, Alzorriz, & Sancristobal (2014), explican que el uso de cortafuegos puede permitir segmentar el tráfico de la red inalámbrica del de la red interna, o segmentar el tráfico de distintos segmentos de red inalámbrica.

Como ya se ha analizado en temas anteriores, muchas de las soluciones de cortafuegos disponibles hoy en día proporcionan otras funcionalidades más allá del control de acceso de nivel 3. Algunos de ellos incluyen funcionalidad de detección de

intrusiones, antivirus. Al enrutar el tráfico de la red inalámbrica a través de un cortafuego de este tipo se aporta nuevas capas de seguridad a la red.

El uso de Firewall o corta fuegos aseguran la red en nivel o capa tres a través de software que hoy en día proporcionan diferentes funcionalidades.

Un corta fuegos es una forma de seguridad donde se pueden implementar muchas técnicas y funcionalidades dependiendo del conocimiento técnico que se tenga se pueden ir agregando más y más métodos seguros en la red.

6.1.9.3.2.2 Nombre de la red (SSID)

El SSID (Service Set Identifier) es un código único incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. Dependiendo de si la red inalámbrica funciona en modo ad-hoc o en modo infraestructura, el SSID se denomina BSSID (Basic Service Set Identifier) o ESSID (Extended Service Set Identifier) respectivamente. El BSSID suele ser la dirección MAC del equipo y, por lo tanto, es única. El ESSID es el nombre de 32 caracteres de la red. Todos los puntos de acceso de una red deben tener el mismo ESSSID así lo define Andreu, Pellejero, & Lesta, Fundamentos y aplicaciones de seguridad en redes WLAN (2006).

El nombre de la red como comúnmente se conoce los detallan los autores antes mencionados como un código único de 32 caracteres alfanuméricos, cada dispositivo debe comunicarse a través del SSID de la red para ser identificado.

La configuración del SSID es de las partes básicas de una red, estas se configuran como ocultas o visible de acuerdo a la confidencialidad de la red, normalmente se identifican por el nombre de la institución o cliente.

6.1.9.3.2.3 Contraseña

Andreu, Pellejero, & Lesta, Fundamentos y aplicaciones de seguridad en redes WLAN, (2006), la autenticación para acceder a una red se realiza mediante la utilización de una contraseña. Generalmente, la contraseña se envía al servidor con cifrado unidireccional tras llevar a cabo un mezclado (hash) de la misma. En caso de emplearse un sistema de almacenamiento de contraseñas es necesario asegurarse de que el método de EAP elegido es compatible con formato de almacenamiento de la contraseña. Para una flexibilidad mayor, se debe elegir un método EAP (Extensible Authentication Protocol) que permita que el servidor AAA (Authentication, Authorization, Acounting) empleado tenga acceso a la contraseña en texto claro. Almacenar contraseñas en texto claro requiere utilizar los métodos de EAP que cifran el canal entre el usuario y el punto de acceso (como las TTL o PEAP).

Una contraseña en la red es la forma de poder acceder a una red segura de esta forma es como el usuario se auténtica y la red le permite el ingreso a la misma, se pueden utilizar protocolo de autenticación para brindar una mayor seguridad entre el punto de acceso y el usuario.

En la actualidad se busca la forma crear contraseñas seguras utilizando números, símbolos, letras mayúsculas y minúsculas y así sucesivamente, aunque no todos los administradores de una red implementan este tipo de seguridad.

6.1.9.3.2.4 ACL

Según Aguilera Lopez (2010), las listas de control de acceso son un elemento más en la seguridad de las redes ya que son utilizadas para permitir el acceso de los usuarios a determinadas aplicaciones, bases de datos u otras áreas de la información, agrupándolos según el criterio de privilegios de acceso.

Controlan el tráfico en router y switch, encargándose de filtrar el tráfico que pasa por estos dispositivos, pudiendo permitir o denegar el acceso, así como restringirlo durante determinadas horas y días a la semana.

Listas de acceso es como se conoce, la función de estas lista es la de limitar el acceso solamente a las redes permitidas esta restricción es realizada mediantes configuraciones en enrutadores y conmutadores para denegar o permitir accesos.

La configuración de las listas de acceso se realiza mediantes requerimientos para permitir el acceso o denegar el acceso interno o externo esto dependerá de las políticas de seguridad de la empresa.

6.1.10 Mejoras a las dificultades de una red

El autor Valdivia (2014), define algunas medidas básicas para mejorar la seguridad y conseguir una WLAN con una seguridad aceptable.

Asegurarse de disponer una política adecuada de seguridad en la utilización de red inalámbrica.

Realizar un inventario completo de todos los dispositivos inalámbricos de la red, evaluando el equipamiento, firmware y actualizaciones. Establecer si los puntos de acceso son apagados durante los periodos de tiempo en los que no son utilizados. Evaluar la configuración, autenticación y cifrado de las redes inalámbricas, como verificar el cambio de los SSID que viene por defecto en los puntos de acceso. Verificar que todos los clientes inalámbricos poseen un antivirus instalado.

Las mejoras a la seguridad son primordiales cuando se trata de una red inalámbrica y muy importante aplicar estas medidas expuestas por el autor.

En el Sistema Local de Atención Integral de Matagalpa, se instaló una red donde están implementadas la mayoría de medidas básicas tanto físicas como lógicas.

6.1.10.1 LAN Virtuales (VLAN)

Las VLAN son grupos de ordenadores relacionados lógicamente entre sí por un número de grupo (número de VLAN) y configurados por el administrador del conmutador,

gracias al software de configuración, residente en el sistema operativo del conmutador, Castro, Diaz, Alzorriz, & Sancristobal (2014).

Las redes virtuales son agrupadas por grupos separados dentro de una misma red, esta configuracion es realizada dentro del switch o enrutador para birndar una mejor organizacion y seguriddad de diferentes áreas dentro de una empresa.

Aplicar redes virtuales (LAN) en una red donde tenemos muchas áreas o departamento nos facilita la gestion y nos brinda una mayor seguirdad y confidencialidad a la información que es manejada en cada area, donde se pueden aplicar diferentes configuraciones para garantizar las exigencia de una red segura.

6.1.10.2 IPV6

Voinea (2011), la nueva versión del protocolo IP recibe el nombre de ipv6, aunque es también conocido comúnmente como IPv6 (Protocolo de Internet de Nueva Generación), el número de este protocolo es el 6 frente a la versión 4 utilizada hasta entonces.

Con este protocolo al ser compatible con IPV4 no existe problema en utilizar los dos protocolo en una red, lo que pretende es expandir la cantidad de IP disponibles donde cada equipo puede tener una IP pública asignada.

En nuestro país aún sigue en un estado de experimentación ya que casi un cien por ciento de empresas no han dado el siguiente paso y continúan trabajando con el protocolo IPV4.

6.1.10.3 Ubicación de dispositivos

Carballar (2010), en cualquier caso, a la hora de colocar más de un punto de acceso, el primer impulso es distribuirlos por donde mejor parezca a primera vista, o en todo caso, utilizar el sistema de prueba y error. A veces funciona.

Esto significa que, antes de comenzar a poner punto de acceso por paredes y techos, no hará falta responder a algunas preguntas.

Podemos decir que, en general, el proceso constaría de los siguientes pasos:

1. Realizar un analisis previo que nos permita determinar las necesidades de cobertura y las posibilidades localizaciones de los puntos de acceso.
2. Instalar y configurar los puntos de acceso.
3. Instalar las interconexiones entre los distintos puntos de acceso.
4. Configurar el acceso a internet.
5. Configurar los terminales.

El ubicar los equipos en el lugar adecuado, garantiza el buen funcionamiento de la red ya sea inalámbrica o cableada, por tal razón se está de acuerdo con el autor. Cada vez que se instale una red inalámbrica debemos de tomar en cuenta todos y cada uno de los pasos anteriormente mencionados.

La buena ubicación de los dispositivos inalámbricos dará satisfacción a los clientes o usuarios un ejemplo que está a la vista de todos es el proyecto de parques wifi, vemos que cada AP está ubicado en lugares estratégicos donde cualquier persona puede llegar con su laptop o dispositivo inalámbrico y hacer uso de la red,

6.1.10.4 Evitar interferencias

Carballar (2010), la distancia, las interferencias y las distorsiones hacen que las señales de radio del punto de acceso se vayan perdiendo. El repetidor regenera las señales digitales y las amplifica, consiguiendo renovar el alcance del punto de acceso a la nueva posición del repetidor.

En zonas con mucha interferencia nos podemos apoyar de repetidores de tal manera que los datos siempre viajen hasta su destino sin poner en riesgo la información.

Tenemos diferentes formas para evitar las interferencias en campos abiertos podemos ubicar los AP en puntos estratégicos y alejar de equipos que irradien señal que pueda interferir con el funcionamiento de la red.

6.1.10.5 Ocultación del SSID

Castro, Diaz, Alzorriz, & Sancristobal (2014), se ha comentado anteriormente que el administrador puede configurar los puntos de acceso de su red para que omitan el SSID de la red en sus paquetes baliza con el objeto de ocultar su red a posibles atacantes pueden llegar a obtener el SSID.

El SSID es el nombre con el que aparece la red inalámbrica, al ocultar este nombre solo clientes autorizados podrán encontrarla y conectarse a ella.

Cuando encendemos una computadora con tarjeta inalámbrica observamos una gran cantidad de redes con diferentes nombre a través de ella un atacante puede sustraer datos convenientes para conectarse a esta red, es por esta la razón que se recomienda oculta el SSID de la red.

6.1.10.6 Uso de Repetidores

Carballar (2010), la principal utilización de repetidores es extender el área de cobertura de un punto de acceso, aunque hay quien los utiliza para extender el alcance de un bridge punto a punto.

Cuando se desea tener una conexión a la red con una distancia muy alejada de un AP, es necesario considerar la instalación de repetidores para extender el alcance de la misma.

Para hacer uso de un repetidor debemos tomar en cuenta que distancia queremos que abarque la señal, por ejemplo si tenemos una red inalámbrica que abarca 50 m cuadrados y tenemos usuarios a 100 m sin duda se tiene que instalar un repetidor inalámbrico para hacer llegar la señal inalámbrica.

6.2 Estándares de red inalámbrica y controles de seguridad

6.2.1 IEEE 802.11

Estándar que fue ratificado en Julio de 1997. Funciona en la banda de 2,4 GHz con velocidades de transmisión máximas de 2Mbps. Incluye velocidades de transmisión de 1Mbps y 2 Mbps, dependiendo de la distancia entre el punto de acceso y la estación inalámbrica y de las condiciones de utilización del canal, Andreu, Pellejero, & Lesta (2006).

Este estándar utiliza diferentes modulaciones tanto en la capa de enlace como en la capa física para adaptarse a diferentes condiciones y distancias ocupando velocidades máximas de 2 Mbps, también utilizaba un protocolo para evitar colisiones entre los paquetes de datos, este estándar fue el primero de esta familia.

Hoy en día el uso de este estándar en redes WLAN es poco común, fue utilizado en las primeras redes inalámbricas que se instalaron donde se experimentaron muchas debilidades tal como la interoperabilidad en diferentes condiciones ambientales.

6.2.1.1 IEEE 802.11b

Estándar que fue ratificado en septiembre 1999 y ha sido y de momento sigue siendo el estándar más utilizado en las redes WLAN europeas. IEEE802.11b extiende el uso del DSSS del IEEE 802.11 Hasta obtener velocidades máximas de transmisión de datos de 11 Mbps, Andreu, Pellejero, & Lesta (2006).

Según el autor, este es uno de los estándares más utilizados, es por ello que se está de acuerdo, puede ser observado en diferentes equipos inalámbricos, este estándar tiene muchas mejoras en comparación con versiones anteriores puede alcanzar una velocidad hasta de 11 Mbps y utiliza una única modulación DSSS.

Los equipos inalámbricos tales como router, ap, pc, y repetidores, de diferentes marcas tienen compatibilidad con este estándar dependiendo de la marca este estándar debe

ser agregado para sobrevivir en el mercado podemos mencionar algunas marcas como, Cisco, Hp, Canon, Dell, Toshiba, entre otras.

6.2.1.2 IEEE 802.11a

Estándar ratificado en septiembre 1999, pero los primeros equipos en el mercado no aparecieron hasta el año 2,001. Una de sus características es que llega a alcanzar velocidades de hasta 54 Mbps gracias a la utilización de OFDM (ortogonal frequency-division multiplexing) con 52 subportadoras.

Este estándar opera en la banda de 5GHz. Hasta el año 2003 no ha sido posible su uso en Europa para redes WLAN. En Estados Unidos, sin embargo, estaba regulado su uso por lo que el IEEE802.11a es el estándar más utilizado en EEUU. Andreu, Pellejero, & Lesta (2006).

Este estándar se caracteriza por alcanzar velocidades máximas de hasta 54 Mbps utilizando esquemas de codificación más sofisticados y trabajando sobre banda de 5GHz, aunque este estándar no ha sido muy utilizado por tener un menor rango de cobertura.

Podemos utilizar este estándar en empresas donde se trabaje sobre una red inalámbrica y que se utilice mucho ancho de banda para las operaciones de la misma por ejemplo para gestión de dispositivos remotos.

6.2.1.3 IEEE 802.11g

Este estándar ratificado en el año 2003 garantiza la compatibilidad con los dispositivos IEEE 802.11b y ofrece unas velocidades de hasta 54 Mbps, al igual que el estándar IEEE802.11a. Andreu, Pellejero & Lesta (2006)

Según el autor este estándar es una versión de unificación del estándar 802.11b y 802.11a por lo tanto es compatible con cada uno de ellos logrando las mismas características tanto en velocidad y modulación pero trabaja en la banda de 2.4 GHz y propone un protocolo de seguridad mucho mejor WPA.

Este estándar se convierte en uno de los mejores para implementar en una red inalámbrica con el simple hecho de lograr las mismas funcionalidades de los demás, se puede implementar en redes privadas donde se maneje mucha información propia de una empresa.

6.2.1.4 Tabla 1 Estándares Físicos y de Optimización

Estándares IEEE 802.11	Capa del modelo OSI en el que son de aplicación	Descripción
A	Física	Capa física con velocidades de hasta 54 Mbps operando en la banda de 5 GHz
B	Física	Capa física con velocidades de hasta 11 Mbps operando en la banda de 2,4 GHz
C	MAC	Operaciones de bridging
D	Física	Dominios internacionales
E	MAC	Modificación de la capa MAC para proveer calidad de servicio
F	Ambas	Interoperabilidad entre puntos de acceso
G	Física	Capa física con velocidades de hasta 54 Mbps operando en la banda de 2,4 GHz
H	Ambas	Coordinación con los estándares HiperLAN2 europeos
I	MAC	Estándar para dotar a las redes de seguridad
J	Ambas	Estándar específico para regular las bandas de frecuencias japonesas de 4,9 y 5 GHz
K	Ambas	Mejora del estándar original para permitir la gestión de recursos radio
M	Ambas	Mantenimientos de estándares previos
N	Ambas	Capa física con velocidades de hasta 100 Mbps
P	MAC	Modificación de la capa MAC para permitir el hand-off a velocidades vehiculares
R	MAC	Modificación de la capa MAC para permitir roaming rápido
S	Ambas	Estándar para redes Mesh

Fuente: Andreu, Pellejero, & Lesta (2006)

6.2.2 ISO/IEC 27002

El nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. El portal de ISO 27000, (2005).

Guia aplicable a la seguridad de la red recomendados con riguroso controles a seguir.

Todas las empresas internacionales se apegan a los estandares ISO para cumplir con medidas y normas de seguridad, contribuyendo de esta manera con su proceso de expansion.

6.2.2.1 CONTROLES DE SEGURIDAD ISO/IEC 27002

6.2.2.1.1 Control de Accesos

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. El portal ISO 27002 en Español, (2013) sugiere que la cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso efícaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

De acuerdo al estandar la concientizacioin de los usuarios es una parte importante para mantener la seguridad y confidencialidad de los accesos tales como contraseña y seguiridad de los equipos, concientizando acerca de sus responsabilidades es asi como define este estandar.

En empresas e instituciones de Nicaragua es probable se haga conciencia acerca de la confidencialidad y accesos pero la poblacion no toma conciencia al cien por ciento esta regla, la mayoria de ellos comparten los accesos con compañeros de trabajos y amigos, de esta manera las redes y sistemas se vueven mas inseguros poniendo en riesgo las operaciones.

6.2.2.1.2 Cifrado

El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. En el portal ISO 27002 en Español, (2013) la aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

Este estandar en su control de cifrado sugiere el desarrollo de políticas sobre el uso de controles criptográficos y gestión de claves con el objetivo de asegurar una adecuada proteccion de su confidencialidad e integridad de el cual se esta totalemente de acuerdo y se debe poner en práctica lo antes mencionado.

La implementacion de políticas y el establecimiento de una gestión de claves en las redes de la instituciones Nicaraguense se debe de conciderar de mucha importancia, actualmente no todas las instituciones implementan una política de seguridad por tal razón las redes y transmisión de datos se vuelven vulnerable a cualquier amenza humana.

6.2.2.1.3 Seguridad física y Ambiental

El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados.

El control de los fáctores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la organización estén físicamente fuera del mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud) todo esto es definido por El portal ISO 27002 en Español, (2013)

Se esta de acuerdo con esta norma de control de la ISO 27002 ya que la seguridad tanto física como ambiental se componen de diversos mecanismos y técnicas para minimizar los riesgos y daños, en la información estableciendo perímetros de seguridad contra accesos físicos y el correcto control de factores ambientales internos y externos brindan mayor seguridad en las operaciones de la organización.

En Nicaragua muchas redes implementan técnicas o métodos diseñados para la protección físicas de los equipos unas más seguras que otras y en la mayoría los equipos externos siempre quedan vulnerable a contactos físicos de esta manera queda a simple vista el riesgo e inseguridad con la que actualmente al no implementar una política confiable.

6.2.2.1.4 Seguridad en las Telecomunicaciones

El objetivo del control de seguridad en las telecomunicicaciones especificado por el portal ISO 27002 en Español (2013), es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección. La información confidencial que pasa a través de redes públicas suele

requerir de controles adicionales de protección. Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante.

Este control establece y deja como objetivo asegurar toda la información que es transportadas por la red protegiendo la infraestructura y gestión segura de soporte requiriendo el monitoreo y protección de la información, aplicando políticas formal de intercambio.

Las redes actuales se deben de proteger física y lógicamente para brindar a los usuarios y a las instituciones como tal el uso seguro de redes sin riesgos de pérdidas por un mal diseño o implementación de seguridad.

VII PREGUNTAS DIRECTRICES

1. ¿Cuál es el estado actual de la red inalámbrica en el Hospital Escuela Cesar Amador Molina de Matagalpa, I semestre 2015?

2. ¿Cumple los criterios de norma IEEE 802.11 y controles de seguridad ISO 27002-2013 la red inalámbrica del Hospital Escuela Cesar Amador Molina Matagalpa, I semestre 2015?

3. ¿Cuáles son las principales dificultades y fortalezas en el funcionamiento de la red inalámbrica del Hospital Escuela Cesar Amador Molina de Matagalpa,I semestre 2015?

4. ¿Qué mejoras pueden sugerirse en pro de las mejoras a las dificultades identificadas en la red inalámbrica en el Hospital Escuela Cesar Amador Molina de Matagalpa, I semestre 2015?

VIII DISEÑO METODOLÓGICO

Enfoque de investigación

En la investigación realizada se aplicó parte el razonamiento deductivo que se comienza con la teoría, se utilizó el análisis de la información para extraer los datos, siendo una investigación objetiva porque no se afecta el proceso que se estudia, por tal razón el enfoque de la investigación es cuantitativo con técnicas cualitativas, usando técnicas de recolección de datos (entrevistas, entrevista a profundidad y observación no participativa).

Tipo de investigación según su alcance, diseño y corte

Según su alcance, esta investigación es descriptiva porque se relató cómo ocurre el proceso y en qué condiciones se da.

Según su diseño, es no experimental porque no se manipularon variables y se describió de forma real y natural lo que está sucediendo en el fenómeno estudiado.

Por su corte es transversal porque el estudio ocurrió en un período determinado, en este caso el I semestre año 2015.

Universo de estudio

El área de estudio fue el Hospital Escuela Cesar Amador Molina de Matagalpa. El universo de estudio fue el encargado de informática y un experto en redes.

Recolección y análisis de datos

Las técnicas de recolección de datos fueron a través de:

- ✓ Entrevista dirigida al encargado de informática. (Ver anexo N°.2)
- ✓ Entrevista a profundidad dirigida a un experto en redes. (Ver anexo N°.3)
- ✓ Observación no participativa (Ver anexo N°.4)

Para dar cientificidad a la investigación, se hizo uso de los métodos teórico y empírico, Este método se aplicó mediante herramientas de recolección de información y a través de la experiencia adquirida por medio de la teoría en esta temática.

El análisis de la información se realizó a través de los métodos deductivo e inductivo, haciendo uso de síntesis, matriz de resultados (Ver Anexo N°6), análisis, comparación y triangulación de la información (Ver Anexo N°5 y N°6).

La información recolectada se procesó a través de herramientas informáticas como paquetería ofimática (Microsoft Word y Excel 2010).

Los materiales que se utilizaron para el desarrollo, análisis y elaboración del informe final fueron: Computadoras, fotocopiadora, papel bond, cámara digital, lápices y cuadernos.

Las Variables de estudio fueron (ver anexo N°. 1):

1. Evaluación de la red inalámbrica.
    1.1 Dificultades y Fortalezas de la red inalámbrica
2. Estándares de red inalambrica y controles de seguridad

IX ANÁLISIS Y DISCUSIÓN DE RESULTADOS

El objetivo principal de este estudio es realizar la evaluación de la red inalámbrica del Hospital Escuela Cesar Amador Molina de conformidad a la norma IEEE 802.11 y controles de seguridad ISO 27002-2013, durante el primer semestre 2015. Para lograr este cometido se plantearon los siguientes objetivos específicos, los cuales se enfocan en identificar las principales dificultades y fortalezas de la red inalámbrica, además se proponen mejoras a las dificultades identificadas fundamentadas científicamente con las normas y controles.

Se utilizó entrevista como técnica de recolección de datos al encargado de informática y entrevista a profundidad al experto en redes. Durante el estudio a la red del Hospital Escuela Cesar Amador Molina se realizó observación no participativa de los controles y estándares normados.

Para el procesamiento de la información se construyó una matriz para las entrevistas realizadas (Ver Anexo N°5), dicha información se complementó con observación no participativa aplicada a la red inalámbrica del Hospital Escuela César Amador Molina.

Se pregunta al encargado de la red del Hospital Escuela César Amador Molina sobre los servicios que tiene la institución a través de la red (Ver Anexo N°5), este argumenta que es la navegación web sin acceso restringido a la internet.

El servicio web es de suma importancia ya que a través de este se puede navegar por la internet, acceder a cuentas de correo páginas web, foros, entre otras.

Según CCNA (2014), los servicios facilitan la comunicación en línea, las personas generalmente buscan enviar y recibir distintos tipos de mensajes a través de aplicaciones informáticas; estas aplicaciones necesitan servicios para funcionar en la red

Se le preguntó al encargado del área de informática del Hospital Escuela César Amador Molina acerca de los beneficios que proporciona la red inalámbrica (Ver Anexo N°5) el cual expresó que le ayuda a descongestionar la red LAN cableada, esto significa

que los puntos de red existentes son limitados por lo que es necesario hacer uso de ambos tipo de red; por otro lado se hace la pregunta al experto en redes acerca de los beneficios de una red inalámbrica (Ver Anexo N°6), manifiesta que un beneficio fundamental es la movilidad en el acceso a la red, simplicidad de arquitectura y bajo costo de mantenimiento.

La red inalámbrica facilita el acceso de conexión a los usuarios por tal razón es una necesidad en una institución donde visitan o permanece una cantidad considerable de persona, es aquí donde radica la importancia de esta red ya que descongestiona salas donde no hay espacios suficientes para que todos accedan a la red.

Según Andreu (2010), las redes inalámbricas permiten movilidad dentro del radio de recepción de señal.

En la entrevista realizada al encargado se consulta sobre el tipo de tecnología de comunicación que se utiliza en la red inalámbrica (Ver Anexo N°5) a lo que responde que la tecnología que utiliza es Wifi, es la tecnología más común en la mayor parte de las instituciones; por otro lado se le consulta al experto en redes sobre qué tecnología recomienda utilizar en una red inalámbrica (Ver Anexo N°6), este responde que para pequeñas oficinas Wireless Personal Área Network el uso de tecnología Bluetooth para evitar molestas conexiones y para redes WLAN el uso de la tecnología WIFI.

Es importante la selección adecuada de una tecnología de comunicación para la red porque si se falla desde este punto se vería afectado el desempeño de la red por otra parte actualmente la mayoría de computadora se conectan a través de Wifi es muy poco probable que funcione una red con tecnología Bluetooth.

Carballar (2010) afirma que bluethooth es una tecnología que, al contrario de Wi-Fi, no tiene por objetivo soportar redes de ordenadores.

según Carballar (2010), una comunicación inalámbrica es aquella que se lleva a cabo sin el uso de cables de interconexión entre los participantes; La red de comunicación Wi-Fi no utiliza cables para conexión entre dispositivos ocupando niveles de preferencia entre todo tipo de usuario.

En la entrevista realizada al encargado de informática se pregunta cuales los problemas que como administrador de la red enfrenta cada día (Ver Anexo N°5), expresó que el principal problema que enfrenta cada día es con problemas de energía eléctrica por las oscilaciones de corriente alterna, esta situación pone en riesgo los equipos de la red de esta manera el enrutador y los puntos de acceso se inhiben constantemente, es tedioso estar revisando y en casos extremos reiniciando los equipos de la red; no obstante se consulta al experto sobre las características que deben tener los dispositivos en una red inalámbrica para brindar un servicio de calidad (Ver Anexo N°6), dando como respuesta que para brindar un servicio de calidad en redes afirma que los equipos deben ser muy confiable para mantener su nivel de salida estable, independiente del tiempo de conexión de los usuarios. (No debe de ser afectado por la temperatura de operación, a largo plazo).

Una red estable con un buen diseño e implementación debe permanecer en funcionamiento continuo sin afectación alguna por factores externos, es un grave problema que los equipos fallen constantemente, este mal funcionamiento causan que la red se vuelva inoperable donde se tiene que utilizar de esfuerzo físico para poner la red en funcionamiento.

Gallego (2010) expresa que el router o enrutador es un periférico de comunicaciones empleado para enlazar diferentes redes entre sí.

Se le consulta en la entrevista al experto en redes la ventaja de constar con un sistema SAI para interrupciones de la energía eléctrica en la red inalámbrica (Ver anexo N°6), menciona que con un sistema SAI habrá protección permanente sobre fallo e interrupciones del fluido eléctrico, más confiabilidad en el servicio, finalmente la inversión en baterías, (tiempo de respaldo) determinará el tiempo que se tendrá protegida la red. De la misma manera recomienda como medida de seguridad fisica la alimentación eléctrica debe de estar dentro de norma básica, en la medida de lo posible alimentado con un SAI, o mayormente conocido como UPS.

Es necesaria la adopción de estos sistemas en una red así de esta manera se evita el deterioro de los equipos y el riesgo de sufrir daños al momento de una variación de voltaje de energía eléctrica.

Aguilera Lopez (2010), menciona que SAI a pesar de lo que su nombre nos pueda sugerir, estos dispositivos no sirven para seguir trabajando durante un corte de electricidad prolongado, sino que nos permiten guardar con seguridad los datos si falla el suministro eléctrico.

Según el experto en redes en la pregunta realizada sobre la importancia de una red inalámbrica (Ver Anexo N°6), responde los siguiente las redes inalámbricas proporcionan el mayor nivel de conexiones posible, esto indica que la cantidad de usuarios conectados es mayor; sin embargo cuando se pregunta al encargado de informática que si considera importante la red inalámbrica (Ver Anexo N°5) comenta que si, por que los usuarios pueden acceder a la redes Wifi las 24 horas del día.

Es una ventaja utilizar una red inalámbrica ya que se puede definir o utilizar a su máxima capacidad las conexiones inalámbricas, siempre y cuando se cuente con un ancho de banda suficiente para navegación la red no tendría problema de saturación.

Para Andreu (2010), las redes inalámbricas wireless (wireless network) son redes sin cable que se suelen comunicar por medios no guiados a través de ondas electromagnéticas. También Andreu J. Servicios en Red (2010), define la ventaja como: Rápida instalación de la red: no necesita cablear, ni pedir permisos de obras, levantar las calles y calzadas de las ciudades.

Permiten movilidad: el medio de transmisión (de envío y recepción) no está sujeto a ningún cable, lo que permite una movilidad dentro del radio de recepción de señal.

Menos costes de mantenimiento: al no tener cableado, los costes de mantenimiento se reducen.

Productividad: las redes inalámbricas propician la colaboración, el teletrabajo.

También se indaga al encargado de informática sobre las consideraciones que se tomaron en cuenta para ubicar los AP como se puede observar (Ver Anexo N°5) el menciona que para ubicar los puntos de acceso se tomó en cuenta el área con menos obstáculos para una mejor señal y cobertura, esto significa que para evitar puntos ciegos se selecciona el área libre obstáculos; no obstante se pregunta al experto en redes sobre la ubicación idónea de un AP, para que garantice una conexión estable (ver anexo N°6) expresa que los puntos de acceso deben estar alejado de paredes, muebles, impresoras, teléfonos y cualquier otro lugar que afecte su funcionamiento.

Para la ubicación de los puntos de acceso se debe tomar en cuenta todos factores que impliquen un mal funcionamiento es por ello que el área debe ser bien estudiada, para que estos garanticen la conexión total en un área determinada y planificada por un diseño de la red y así no se afecte el funcionamiento de la misma.

Wiley & Canada (2011), hace mencion al principal problema de interferencias, si quita los potenciales obstáculos y fuentes de interferencia, la mayoría de aparatos inalámbricos pueden alcanzar distancias de casi el doble de lo que puede esperar adentro.

Según el encargado de informática en la entrevista realizada indagando sobre el radio de cobertura en metros de cada AP (ver anexo N°5), nos comenta que tiene cobertura de 20 metros, mientras que al experto se le consulta cuales consideraciones se toman en cuenta para la mejor cobertura de un AP (Ver Anexo N°6), y manifiesta los siguiente, la escogencia de operación del AP en GHz. la frecuencia en definitiva influye en determinar el alcance, a mayor frecuencia menor cobertura.

En la red inalámbrica influye mucho el rango de cobertura de cada AP, por tal razón este debe tener un radio que se adapte a las necesidades de la institución, una cobertura de 20 metros es bastante limitado si necesita movilizarse dentro de la institución.

Soyer (2005), describe que el hardware WI-FI básico tiene un alcance teórico de 30 metros en interior y de 100 metros en exterior. En la práctica hay que contar más bien con un alcance de 10 a 15 metros interior, en el exterior, cuente la distancia entre su

punto de acceso y la pared externa (inferior a 15 metros) y la distancia entre dicha pared y el lugar del jardín en que desee instalarse (como máximo, 10 metros).

Carballar (2010), menciona que el punto de acceso no sólo es el medio de intercomunicación de todos los terminales que forman la red sino que también es el puente de interconexión de la red fija e internet.

En entrevista realizada al experto en redes se pregunta sobre los aspectos que considera necesario para la selección adecuada de una topología de red (Ver Anexo N°6), expresa que la velocidad de acceso a Internet, la tecnología o más bien el estándar a emplear y necesidad de cada institución se toma en cuenta para seleccionar la topología de red, de igual forma se pregunta al encargado de la red qué topología implementaron en la infraestructura de la red (Ver Anexo N°5), indica que la red del Hospital Cesar Amador Molina se extendió y formo topología estrella conforme a la necesidad se agregaron más puntos de acceso.

Para la implementación de una topología adecuada el experto hace referencia a la necesidad de cada institución, estándar entre otros; lamentablemente en la red del Hospital Escuela Cesar Amador Molina no se tomó en cuenta ningún aspecto para la selección de la topología ya que no existe ningún diseño de red, simplemente se formó a medida que la red fue creciendo.

Riera & Alabau, (1992), menciona que en la topología estrella todas las estaciones están unidas, mediante medios bidireccionales, a un módulo nodo central que efectúa funciones de conmutación.

Al realizar la siguiente pregunta al experto en redes sobre las ventajas y desventajas de utilizar un repetidor (Ver Anexo N°6), ostenta que los repetidores permiten crear redes de mayor tamaño, aunque el abuso de estos reduce abruptamente la velocidad de todos los usuarios del enrutador y expresa que el uso de repetidores debe ser muy bien justificados, en la mayoría de los casos evitados, son soluciones puntuales y no globales.

No es recomendable el uso de repetidores sin ninguna necesidad ya que estos reducen la velocidad afectando directamente la red, tal y como menciona el experto estos cambios en la red deben ser muy bien justificados antes de optar por esta solución de conexión.

Carballar (2010), menciona que un repetidor inalámbrico es un equipo que recibe la señal de radio de un punto de acceso y la retransmite, extendiendo de esta forma el área de cobertura de dicho punto de acceso.

Para conocer las recomendaciones del experto sobre las interferencias se preguntó qué medidas recomienda para evitar interferencias y mejorar una red inalámbrica (Ver Anexo N°6), el experto en redes expresa que hay que evitar instalar equipos que causen mal funcionamiento al enrutador, no ubicarlos cerca de equipos que generen fuertes transientes de energía, los armónicos (contaminación eléctrica) generado por estos son de frecuencia infinita y generan fuertes interferencias, ejemplos:

Aires acondicionados, deshidratadores, Motores de A.C. y/o D.C.

Como ya se ha mencionado anteriormente para tener un buen funcionamiento en la red se debe evitar cualquier tipo de interferencia ya sea por contaminación eléctrica o por obstáculos de esta manera se garantiza una conexión estable a la red.

La tecnología WI-FI es flexible y fácil de utilizar, pero no hay que olvidar que usa las ondas de radio, que, como todas las ondas, tienen un alcance limitado así lo explica Soyer (2005).

El estandar ISO/IEC 27002 es una guia aplicable a la seguridad de la red recomendados con riguroso controles a seguir. Los estándares son un sistema de reglas prescrito, condiciones o requerimientos que atañen a las definiciones de los términos.

Durante el estudio se realizó observación no participativa a la red inalámbrica del Hospital Escuela César Amador Molina (Ver anexo N°.4) para revisar si cumple con controles de seguridad, donde los puntos que se evaluaron fueron los siguientes:

Tabla 2 Verificación de cumplimiento de controles de seguridad ISO 27002-2013

La Red Inalámbrica cumple:	**ITEMS**	
Control de Accesos		
Políticas de control de acceso a la red	Sí ___	No_X__
Proceso formal para acceder a la red	Sí __X_	No___
Asignación de acceso con privilegios especiales restringidos y controlados	Sí ___	No_X__
Revisión con regularidad los derechos de acceso de los usuarios	Sí ___	No_X__
Se exige a los usuarios uso de buenas prácticas para seguridad confidencial	Sí ___	No_X__
Controles criptográficos		
Política de control que regule uso de criptografía	Sí _X__	No___
Política de uso, protección y ciclo de vida de las claves criptográficas	Sí ___	No_X__
Seguridad física y Ambiental		
Definición de perímetros de seguridad para la protección de las áreas e instalaciones	Sí ___	No_X__
Áreas seguras protegidas mediante controles de entrada	Sí ___	No_X__
Protección física contra desastres naturales, ataques maliciosos o accidentes.	Sí ___	No_X__
Equipos protegidos de amenazas, peligros ambientales y de oportunidades de accesos no autorizados.	Sí ___	No_X__
Equipos protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.	Sí ___	No_X__
Cables eléctricos y de telecomunicaciones que Transportan datos protegidos contra la intercepción, interferencia o posibles daños.	Sí _X__	No___

Mantenimiento de los equipos adecuado para garantizar disponibilidad e integridad continúa.	Sí ___	No_X__
Verificación de todos los equipos que contengan medios de almacenamiento, antes eliminación o reutilización	Sí _X__	No___
Seguridad en las Telecomunicaciones		
Administración y control de las redes para proteger información en sistemas y aplicaciones.	Sí ___	No_X__
Segregación de las redes en función de los grupos de servicios, usuarios y sistemas de información.	Sí ___	No_X__

Fuente: Elaboración propia a partir de verificación del cumplimiento de controles de seguridad a la red inalámbrica.

Se procedió a revisar dicho documento evaluando si existían cada uno de estos ítems de lo antes descrito, donde se pudo observar que los controles de seguridad no se cumplen. Reflejando de esta manera que poseen controles de seguridad deficiente.

Las normas ISO/IEC 27001, ISO/IEC 27002 están enfocadas a todo tipo de organizaciones (por ej. empresas comerciales, agencias, gubernamentales, organizaciones sin ánimo de lucro), tamaños (pequeña, mediana o gran empresa), tipo o naturaleza. El portal ISO 27002 en Español (2013)

Por medio de observación se verificó si la red cumple con protección física contra desastres naturales ataques maliciosos o accidentes (Ver Anexo N°4), se procedió a observar físicamente y no cuenta con ningún tipo de protección que evite accidentes o ataques físicos.

De esta manera se observa que la red es muy vulnerable ante cualquier situación ya sea externa como desastres naturales como cualquier intento de daño físico.

El portal ISO 27002 en Español (2013), tiene como objetivo minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

Se realiza observación a cerca del cumplimiento de equipos protegidos de amenazas, peligros ambientales y de oportunidad de accesos no autorizados, de la misma manera no cumple con esta norma poniendo en riesgo la red.

Al no implementar normas de seguridad la red esta desprotegida totalmente de toda amenaza y cualquier persona tiene la oportunidad de tener contacto con los equipos.

El portal ISO 27002 en Español (2013), el establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados

Se realiza observacion en compañía del encargado de la red, sobre el cumplimiento de control ISO, equipos protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo (Ver Anexo N°7), no se observa protección alguna por fallas de suministro eléctrico, los equipos estan conectados a corriente AC permanentemente.

La red inalámbrica es vulnerable a variación de voltaje e interrupciones disminuyendo la vida útil de los dispositivos de la red e interrumpiendo la operatividad de la red, sino se cuenta con un sistema de regulación de voltaje y acumulación de energía en DC en cualquier momento los equipos se dañaran.

El portal ISO 27002 en Español (2013), el control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

Consultando al encargado de informática para observar la protección de intercepción se verificá que el transporte de datos este protegido contra la intercepción interferencia o posibles daños, se observa la protección física de cableados protegidos en canaletas y ductos evitando la intercepcion física de datos trasnportados a través de cables troncales.

La protección de física del transporte de datos es una medida importante para garantizar la confiabilidad de la información, esta manera la red fisica se encuentra segura ante posibles daños e intersepción.

Según Castro, Diaz, Alzorriz, & Sancristobal (2012) las políticas de seguridad son una serie de procedimientos relacionados con las seguridad física, tanto en el aspecto de control de acceso físico a equipos como el de tener planes de contingencia y emergencia. Las políticas de seguridad son el protocolo a seguir por parte de los recursos humanos involucrados en la manipulación de equipos informáticos de la red.

Con el apoyo del encargado de la red se comprueba que la red cumpla con un mantenimiento de los equipos adecuados para garantizar disponibilidad e integridad continua (Ver Anexo N°7), no existe un plan de mantenimiento adecuado de los equipos que conforman la red.

El no implementar un plan de mantenimiento pone en riesgo los equipos, sino se toman medidas todos estos dispositivos se le ira reduciendo la vida útil y afectando gradualmente el desempeño de la red.

Se verifican todos los equipos que contengan medios de almacenamiento, ante eliminacion o reutilización (Ver Anexo N°7), se solicita apoyo del administrador de la red e indica que todo equipo que es deshechado tiene que ir sin ninguna informacion que perjudique a la institución, ya que cualquier dato almacenado es confidencial.

El almacenamiento de información alojada en los dispositivos en este caso router y swiches, debe ser formateado cuando se realiza un cambio si se va a reutilizar de igual forma se debe borrar todo lo contenido en el y asi garantizar no se filtre información privada de la institucion.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la organización estén físicamente fuera del

mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud) todo esto es definido por, El portal ISO 27002 en Español, (2013)

Se evaluó por medio de observación el siguiente parámetro de control de la ISO, existe administración y control de las redes para proteger información en sistemas y aplicaciones (Ver Anexo N°7), no existe control de las redes por medio de ningún servidor para proteger la información de la red inalámbrica.

Se debe proteger la información transportada por la red, dado que por esta pasan datos de personal interno y externo de la institución dejando vulnerable ante amenazas.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección, El portal ISO 27002 en Español (2013).

A través de observacion se evaluó la existencia de segregación de redes en función de los grupos de servicios, usuarios y sistemas de información (Ver Anexo N°7), encontrando que la red no esta segregada en grupos de servicios, todos los usuarios se conectan con los mismos privilegios.

Es necesario la segregación de la red en sub redes o VLAN para proteger la informacion de acuerdo a la actividad que realizán o áreas que existen en la institución y así tener el control de los permisos habilitados de acuerdo a las necesidades.

El portal ISO 27002 en Español (2013), los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante.

Se evalua el estandar IEEE 802.11 b y n a través de una observación utilizando una guía de items donde se aplican los parámetros de este estándar.

Tabla 3 Verificación de cumplimiento de estandar IEEE 802.11

Parámetros evaluados:	**ITEMS**	
Estándar IEEE 802.11b	Sí _X__	No___
Estándar IEEE 802.11g	Sí _X__	No___
Estándar IEEE 802.11n	Sí _X__	No___
Frecuencia en GHz 2.4	Sí _X__	No___
Velocidad menor o igual 11 Mbps	Sí _X__	No___
Velocidad menor o igual 50 Mbps	Sí _X__	No___
Velocidad igual o mayor a 100 Mbps	Sí _X__	No___

Fuente: Elaboración propia a partir de verificación del cumplimiento de estandar IEEE802.11 a la red inalámbrica.

Los equipos utilizados cumplen con los estándares mencionado, de los cuales se hace uso de acuerdo a la necesidad.

Estándar IEEE 802.11b que fue ratificado en septiembre 1999 ha sido y de momento sigue siendo el estándar más utilizado en las redes WLAN europeas. IEEE802.11B extiende el uso del DSSS del IEEE 802.11 Hasta obtener velocidades máximas de transmisión de datos de 11 Mbps, Andreu, Pellejero, & Lesta (2006).

Estandar IEEE 802.11 n, Capa física con velocidades de hasta 100 Mbps, Andreu, Pellejero, & Lesta (2006)

Tabla 4 Dificultades y fortalezas encontradas en la red

No.	Dificultad	Fortaleza
1		Proceso formal para acceder a la red
2		Política de control que regule la criptografía
3		Cumple con el parámetro de cables eléctricos y de telecomunicaciones que transportan datos protegidos contra intercepción, interferencia o posibles daños
4		Se cumple con la verificación de todos los equipos que contengan medias de almacenamientos antes de eliminación o reutilización
5		Estándar IEEE 802.11b Frecuencia en GHz 2.4 Velocidad menor o igual 11 Mbps
6		Estándar IEEE 802.11g Frecuencia en GHz 2.4 Velocidad menor o igual 50 Mbps
7		Estándar IEEE 802.11n Frecuencia en GHz 2.4 Velocidad igual o mayor a 100 Mbps
8	Oscilaciones de voltaje AC	
9	Cobertura de la red	
10	No existe diseño de red documentado	
11	No existen políticas de control de acceso a la red.	
12	No tiene asignación de acceso con privilegios especiales restringidos y controlados	
13	No se realiza revisión con regularidad los derechos de acceso de los usuarios.	
14	No se exige a los usuarios uso de buenas prácticas para seguridad confidencial.	
15	No existe política de uso, protección y ciclo de vida de las	

No.	Dificultad	Fortaleza
	claves criptográficas.	
16	No tiene definición de perímetros de seguridad para la protección de las áreas e instalaciones.	
17	No cuenta con áreas seguras protegidas mediante controles de entrada.	
18	No tiene protección física contra desastres naturales, ataques maliciosos o accidentes.	
19	No cumple con el control de equipos protegidos de amenazas, peligros ambientales y de oportunidad de accesos no autorizados	
20	No cumple con la norma de control equipos protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo	
21	No cumple mantenimiento de los equipos adecuado para garantizar disponibilidad e integridad continúa	
22	No cumple con Administración y control de las redes para proteger información en sistemas y aplicaciones	
23	No cumple con la segregación de las redes en función de los grupos de servicios, usuarios y sistemas de información.	

Fuente: Elaboración propia a partir de resultados de entrevista realizada al encargado, verificación del cumplimiento de controles de seguridad y estandar IEEE 802.11 a la red inalámbrica .

X CONCLUSIONES

A partir del estudio que se realizó de la Evaluación de la Red Inalámbrica en el Hospital Escuela Cesar Amador Molina, basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013 Matagalpa, I semestre 2015. Se llegó a las siguientes conclusiones:

- La red cuenta con servicio de navegación web, tecnología wifi de comunicación, dispositivos básicos para la red inalámbrica y ancho de banda de 3 Mbps.

- De acuerdo al estándar IEEE 802.11 y controles de seguridad del ISO 27002-2013 la red inalámbrica no cumple con la mayoría de criterios y parámetros verificados.

- Las principales dificultades que limitan el funcionamiento óptimo de la red están en la falta de políticas de seguridad y la falta de mantenimientos constantes en la red. Al revisar y evaluar los controles de seguridad de la red, se cumple con el proceso formal para acceder a la red y política de control que regule uso de criptografía.

- Se sugiere la implementación de políticas de seguridad de acceso físico en factores externos que contribuyan al mejoramiento continúo de la red y lógico para segregación de redes en función de grupos de servicios y usuarios así como reactivar y destinar un servidor para la gestión de la red inalámbrica.

XI RECOMENDACIONES

Se sugiere mejoras a las dificultades encontradas, durante el proceso de investigación, por tal motivo a través de este documento se hacen las siguientes recomendaciones:

- Para mejorar la disponibilidad del Router y Puntos de Acceso (AP), se sugiere implementar un Sistema de Alimentación Ininterrumpida (SAI) a la red inalámbrica (Ver Anexo N°3).

- Que a la red inalámbrica del Hospital Escuela César Amador Molina se le implemente controles de seguridad, principalmente los controles de acceso asignando privilegios especiales y restricciones.

- Se recomienda la implementación de un servidor para la gestión de la red inalámbrica, de esta manera aplicar todas las medidas de seguridad a la red.

- Se sugiere aplicar lo planteado en el Anexo N°8.

XII BIBLIOGRAFÍA

Aguilera Lopez (2010), Seguridad Informatica. Madrid, España: Editex.

Andreu, F., Pellejero, I., & Lesta, A. (2006). Fundamentos y aplicaciones de seguridad en redes wlan. Barcelona, España: Marcombo S.A.

Andreu, J. (2010). Servicios en Red. Pozuelo de Alarcón, Madrid: Editex. http://books.google.com.ni/books?id=vhit3ZmGQPsC&pg=PA213&dq=Red+Inal%C3%A1mbrica&hl=es&sa=X&ei=7K9FVMHEOc61sQTco4LYCQ&ved=0CCUQ6AEwAA#v=onepage&q=Red%20Inal%C3%A1mbrica&f=false

Andreu, J. (2011) Instalacion de equipos de red. Configuracion (redes locales). Madrid: Editex, S.A.

Andrew, T. (2003). Redes de computadoras. Mexico: Pearson Education.

Carballar, J. (2010). WI-FI: Lo que se necesita conocer. Madrid, España: RC Libros.

Castro, M., Diaz, G., Alzorriz, I., & Sancristobal, E. (2014). procesos y herramientas para la seguridad de redes. Madrid: www.uned.es/publicaciones.

CCNA, C. (10 de Noviembre de 2014). Aspectos basicos de networking. http://www.uhu.es/diego.lopez/CCNA/CCNA_Exploration_4.0_Aspectos_basicos_de_Networking_Espanol.pdf

Cervigon, A., & Alegre, M. (2011). Seguridad informática. Madrid, España: paraninfo, SA.

Commons, C. (2007). Redes Inalambricas en los Paises en Desarrollo. Limehouse Book Sprint Team.

Díaz, G., Mur, F., Sancristóbal, E., Castro, M.-A., & Peire, J. (2012). Seguridad en las comunicaciones y en la informacion. Madrid: www.uned.es/publicaciones.

Dordoigne, J., & Atelin, P. (2006). Redes informatícas conceptos fundamentales. Barcelona, España: Ediciones ENI.

El portal de ISO 27000. (2005). http://www.iso27000.es/iso27000.html

El portal ISO 27002 en Español. (2013). http://www.iso27000.es/iso27002.html

Gallego, J. (2010). PCPI - Montaje de componentes informaticos. Madrid, España: Editex, S. A.

Gil, P., Pomares, J., & Candelas, F. (2010). Redes y transmisión de datos. San Vicente, España: Universidad de Alicante.

Herrera, E. (2003). Tecnologías y redes de transmisión de datos. Balderas 95, Mexico DF.: Limusa.

Mendigaña, C., & Reina, A. (2008). Diseño, implementacion y configuracion de una red inalambrica en la corporacion universitaria minuto de dios. colombia: corporacion universitaria minuto de dios.

Mendoza, L. (2012). Evaluación de la Red de Computadores de Unan Managua Farem Matagalpa, periodo 2012. Matagalpa : Facultad Regional Multidisciplinaria Matagalpa.

Montoya , A., & Ovalle , D. (Julio de 2012). Evaluación de Red Inalámbrica . http://revista.eia.edu.co/articulos17/EIA%2017%20%28pp.%20151-166%29%20art.11.pdf

Riera, J., & Alabau, A. (1992). Teleinformatica y redes de computadoras. Barcelona, España: foinsa - Passatge Gaiola.

Rivas, R. (2010). Diseñar una red inalambrica con servidor de software libre linux suse. Matagalpa, Niacaragua.

Rodrigues, R., Canales, A., Peña, T., Castro, G., & Reyes, G. (2009). www.lamjol.info/index.php/encuentro/article/download/49/47

Sánchez Herrera, J. (2012). Nuevas tendencias en comunicación. Madrid, España: Editorial Esic.

Serra, X. (2002). Análisis de redes y sistemas de comunicaciones. Barcelona: Centre de Publicacions del Campus Nord.

Soyer, L. (2005). WI-FI instalar una red inalambrica en casa. Barcelona: Ediciones ENI.

Valdivia, C. (2014). Sistemas informaticos y redes. Madrid, España: Ediciones paraninfo S.A.

Voinea, J. (2011). Redes de comunicaciones. Administracion y gestion. Almeria.

Wiley, J., & Canada, S. (2011). TI para pequeñas empresas. Ontario, Canada.

XII Anexos

ANEXO 1

Operacionalización De Variables

Operacionalización de Variables						
Variable	**Concepto**	**Subvariable**	**Indicador**	**Interrogantes**	**Técnica**	**Informantes**
Evaluación de la red inalámbrica	Evaluación de una red inalámbrica es el proceso de identificar debilidades y fortalezas contrastadas con estándares definidos.	Infraestructura Lógica	Servicios de Red	¿Cuáles son los servicios que tiene la institución a través de la red?	Entrevista	Encargado de Informática
				¿Qué beneficios le proporcionan los servicios de la red?	Entrevista	Encargado de Informática
				¿Qué áreas de la institución comparten información a través de los servicios de la red?	Entrevista	Encargado de Informática
			Topología	¿Existe un documento sobre el diseño de la red lógico o físico? En caso decir que sí, ¿nos puede facilitar o mostrar usted el ejemplar?	Entrevista	Encargado de Informática
				¿Qué topología implementaron en la infraestructura de la red?	Entrevista	Encargado de Informática
				¿Qué aspectos considera necesario para la selección adecuada de una topología de red?	Entrevista a Profundidad	Experto en Redes
				¿Considera usted que es necesario implementar VLAN y cuáles son las ventajas en una red inalámbrica?	Entrevista a Profundidad	Experto en Redes

Operacionalización de Variables						
Variable	**Concepto**	**Subvariable**	**Indicador**	**Interrogantes**	**Técnica**	**Informantes**
		Infraestructura Física	Tecnologías de Redes Inalámbricas	¿Qué tipo de tecnología de comunicación utiliza en la red?	Entrevista	Encargado de Informática
				¿Qué tecnología recomienda utilizar en una red inalámbrica?	Entrevista a Profundidad	Experto en Redes
				Tecnologías de la Redes Inalámbricas	Tabla de Análisis	
			Tipos de Medios	¿Considera importante la existencia de una red inalámbrica?	Entrevista	Encargado de Informática
				¿Cuáles son los beneficios de una red inalámbrica?	Entrevista a Profundidad	Experto en Redes
				¿Cuenta la infraestructura de la red con algún servicio troncal de fibra óptica?	Entrevista	Encargado de Informática
			Dispositivos de una red inalámbrica	¿Cuáles son los componentes físicos que se utilizan en la construcción de una Red WIFI?	Entrevista a Profundidad	Experto en Redes
				¿Cuáles son las características que debe tener un equipo que emite señal inalámbrica para brindar un servicio de calidad?	Entrevista a Profundidad	Experto en Redes
				¿Cuáles son las ventajas y desventajas de utilizar un repetidor?	Entrevista a Profundidad	Experto en Redes
				¿Considera necesaria la instalación de repetidores para mejorar la cobertura de una red inalámbrica?	Entrevista a Profundidad	Experto en Redes

Operacionalización de Variables						
Variable	**Concepto**	**Subvariable**	**Indicador**	**Interrogantes**	**Técnica**	**Informantes**
				¿Cuál es el área de ubicación actual del enrutador?	Entrevista	Encargado de Informática
				¿Cuál es la ubicación idónea de un AP, para que garantice una conexión estable?	Entrevista a Profundidad	Experto en Redes
			Distancia	¿Cuáles fueron las consideraciones que se tomaron en cuenta para ubicar los AP?	Entrevista	Encargado de Informática
				¿Cuál es el radio de cobertura en metros de cada AP?	Entrevista	Encargado de Informática
				¿Cuál es la distancia máxima apropiada para conectar un dispositivo a una red inalámbrica?	Entrevista a Profundidad	Experto en Redes
			Obstáculos	¿Cuáles son los problemas que usted como administrador de la red enfrenta cada día?	Entrevista	Encargado de Informática
				¿Cuáles son los obstáculos que generan puntos ciegos en una red inalámbrica?	Entrevista a Profundidad	Experto en Redes
				¿Qué medidas se recomiendan para evitar interferencias y mejorar una red inalámbrica?	Entrevista a Profundidad	Experto en Redes
			Diseño de Red Física	¿Cuál es el enlace actual de red inalámbrica?	Entrevista	Encargado de Informática
				¿Cuál es el ancho de banda que utiliza la red?	Entrevista	Encargado de Informática

Operacionalización de Variables						
Variable	**Concepto**	**Subvariable**	**Indicador**	**Interrogantes**	**Técnica**	**Informantes**
Controles de seguridad estándar ISO 27002-2013	Norma ISO 27002-2013 corresponde a una guía de buenas prácticas en seguridad de la información con controles definidos.	Controles de seguridad	Control de Accesos	Políticas de control de acceso a la red	Observación	SI____ NO ___
				Proceso formal para acceder a la red	Observación	SI____ NO ___
				Asignación de acceso con privilegios especiales restringidos y controlados	Observación	SI____ NO ___
				Revisión con regularidad los derechos de acceso de los usuarios	Observación	SI____ NO ___
				Se exige a los usuarios uso de buenas prácticas para seguridad confidencial	Observación	SI____ NO ___
			Controles criptográficos	Política de control que regule uso de criptografía	Observación	SI____ NO ___
				Política de uso, protección y ciclo de vida de las claves criptográficas	Observación	SI____ NO ___
			Seguridad física y Ambiental	Definición de perímetros de seguridad para la protección de las áreas e instalaciones	Observación	SI____ NO ___
				Áreas seguras protegidas mediante controles de entrada	Observación	SI____ NO ___
				Protección física contra desastres naturales, ataques maliciosos o accidentes.	Observación	SI____ NO ___

Operacionalización de Variables						
Variable	**Concepto**	**Subvariable**	**Indicador**	**Interrogantes**	**Técnica**	**Informantes**
				Equipos protegidos de amenazas, peligros ambientales y de oportunidades de accesos no autorizados.	Observación	SI____ NO ___
				Equipos protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.	Observación	SI____ NO ___
				Cables eléctricos y de telecomunicaciones que transportan datos protegidos contra la intercepción, interferencia o posibles daños.	Observación	SI____ NO ___
				Mantenimiento de los equipos adecuado para garantizar disponibilidad e integridad continúa.	Observación	SI____ NO ___
				Verificación de todos los equipos que contengan medios de almacenamiento, antes eliminación o reutilización	Observación	SI____ NO ___
			Seguridad en las telecomunicaciones	Administración y control de las redes para proteger información en sistemas y aplicaciones.	Observación	SI____ NO ___
				Segregación de las redes en función de los grupos de servicios, usuarios y sistemas de información	Observación	SI____ NO ___

ANEXO 2

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

(UNAN – Managua)

Facultad Regional Multidisciplinaria, Matagalpa

(FAREM – Matagalpa)

ENTREVISTA

Preguntas de entrevista al encargado de informática para conocer el estado actual y las dificultades de la red inalámbrica del Hospital Escuela César Amador Molina. La información que nos proporcione será de relevancia para determinar la situación actual de la red inalámbrica.

1. ¿Cuáles son los servicios que tiene la institución a través de la red?

2. ¿Qué beneficios le proporcionan los servicios de la red?

3. ¿Qué áreas de la institución comparten información a través de los servicios de la red?

4. ¿Posee un inventario actualizado de los equipos de la red?

5. ¿Existe un documento sobre el diseño de la red lógico o físico? En caso decir que sí, ¿nos puede facilitar o mostrar usted el ejemplar?

6. ¿Qué topología implementaron en la infraestructura de la red?

7. ¿Considera importante la existencia de una red inalámbrica?

8. ¿Qué tipo de tecnología de comunicación utiliza en la red?

9. ¿Cuál es el enlace actual de red inalámbrica?

10. ¿Cuál es el ancho de banda que utiliza la red?

11. ¿Cuenta la infraestructura de la red con algún servicio troncal de fibra óptica?

12. ¿Cuáles fueron las consideraciones que se tomaron en cuenta para ubicar los AP?

13. ¿Cuál es el radio de cobertura en metros de cada AP?

14. ¿Cuáles son los problemas que usted como administrador de la red enfrenta cada día?

15. ¿Cuentan con políticas de seguridad físicas para administrar la red inalámbrica y control interno?

16. ¿Cuál es la norma eléctrica que utiliza para la instalación de dispositivos que forman parte de la red?

17. ¿Cuál es el área de ubicación actual del enrutador?

18. ¿Cómo administra usted el acceso a la red?

19. ¿Mencione los tipos de dispositivos a través de los cuales los usuarios tienen acceso a la red?

20. ¿Utiliza encriptación para las contraseñas de acceso a la red?

ANEXO 3

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

(UNAN – Managua)

Facultad Regional Multidisciplinaria, Matagalpa

(FAREM – Matagalpa)

ENTREVISTA

Preguntas de entrevista a profundidad al experto en redes para recomendar mejoras a la red inalámbrica. La información que nos proporcione nos dará una guía para mejorar la situación actual de la red.

¿Qué aspectos considera necesario para la selección adecuada de una topología de red?

¿Cuáles son los beneficios de una red inalámbrica?

¿Qué tecnología recomienda utilizar en una red inalámbrica?

¿Cuáles son los componentes físicos que se utilizan en la construcción de una Red WIFI?

¿Cuáles son las características que deben tener los dispositivos en una red inalámbrica para brindar un servicio de calidad?

¿Cuál es la importancia de la red inalámbrica?

¿Cuáles son las ventajas y desventajas de utilizar un repetidor?

¿Cuál es la distancia máxima apropiada para conectar un dispositivo a una red inalámbrica?

¿Cuáles son los obstáculos que generan puntos ciegos en una red inalámbrica?

¿Qué consideraciones se toman en cuenta para la mejor cobertura de un AP?

¿Qué medidas se recomiendan para evitar interferencias y mejorar una red inalámbrica?

¿Cuál es la medida de seguridad física que usted recomienda para brindar mayor seguridad a los puntos de acceso?

¿Cuál es la ventaja de constar con un sistema SAI para interrupciones de la energía eléctrica en la red inalámbrica?

¿Cuál es la ubicación idónea de un AP, para que garantice una conexión estable?

¿Qué medidas de seguridad lógicas sugiere para una red inalámbrica?

¿De qué forma recomienda se configure el usuario y contraseña de una red inalámbrica?

¿Considera usted que es necesario implementar VLAN y cuáles son las ventajas en una red inalámbrica?

ANEXO 4

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

(UNAN – Managua)

Facultad Regional Multidisciplinaria, Matagalpa

(FAREM – Matagalpa)

La Red Inalámbrica cumple:	**ITEMS**	
Control de Accesos		
Políticas de control de acceso a la red	Sí ___	No____
Proceso formal para acceder a la red	Sí ___	No____
Asignación de acceso con privilegios especiales restringidos y controlados	Sí ___	No____
Revisión con regularidad los derechos de acceso de los usuarios	Sí ___	No____
Se exige a los usuarios uso de buenas prácticas para seguridad confidencial	Sí ___	No____
Controles criptográficos		
Política de control que regule uso de criptografía	Sí ___	No____
Política de uso, protección y ciclo de vida de las claves criptográficas	Sí ___	No____
Seguridad física y Ambiental		
Definición de perímetros de seguridad para la protección de las áreas e instalaciones	Sí ___	No____
Áreas seguras protegidas mediante controles de entrada	Sí ___	No____

Protección física contra desastres naturales, ataques maliciosos o accidentes.	Sí ___	No____
Equipos protegidos de amenazas, peligros ambientales y de oportunidades de accesos no autorizados.	Sí ___	No____
Equipos protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.	Sí ___	No____
Cables eléctricos y de telecomunicaciones que Transportan datos protegidos contra la intercepción, interferencia o posibles daños.	Sí ___	No____
Mantenimiento de los equipos adecuado para garantizar disponibilidad e integridad continúa.	Sí ___	No____
Verificación de todos los equipos que contengan medios de almacenamiento, antes eliminación o reutilización	Sí ___	No____

Seguridad en las Telecomunicaciones

Administración y control de las redes para proteger información en sistemas y aplicaciones.	Sí ___	No____
Segregación de las redes en función de los grupos de servicios, usuarios y sistemas de información.	Sí ___	No____

OBSERVACIONES:

_____
_____
_____
_____
_____

ANEXO Nº 5

Matriz de resultados de entrevista aplicada encargado del área de Informática de Hospital Escuela Cesar Amador Molina

Pregunta	Respuesta
1 ¿Cuáles son los servicios que tiene la institución a través de la red?	Navegación web
2 ¿Qué beneficios le proporcionan los servicios de la red?	Permite descongestionar la red LAN cableada
3 ¿Qué tipo de tecnología de comunicación utiliza en la red?	WIFI
4 ¿Cuáles son los problemas que usted como administrador de la red enfrenta cada día?	El enrutador y los AP se inhibe constantemente, Problemas de corriente eléctrica, variación de voltaje AC
5 ¿Considera importante la red inalámbrica?	Si, por que los usuarios pueden acceder a la red las 24 horas del día
6 ¿Cuáles fueron las consideraciones que se tomaron en cuenta para ubicar los AP?	El área con menos obstáculos para una mejor señal y cobertura.
7 ¿Cuál es el radio de cobertura en metros de cada AP?	20 m
8 ¿Qué topología implementaron en la infraestructura de la red?	Tipo estrella

ANEXO Nº 6

Matriz de resultados de entrevista aplicada a experto en redes

Pregunta	Respuesta
1 ¿Cuáles son los beneficios de una red inalámbrica?	Movilidad en el acceso, simplicidad de la arquitectura y bajo costo de mantenimiento
2 ¿Qué tecnología recomienda utilizar en una red inalámbrica?	Para redes pequeñas, en el hogar o pequeñas oficinas, wireless Personal Área Network, puede emplear el protocolo Bluetooth, para evitar molestas conexiones y para facilitar la implementación de la misma. Y para redes WLAN se puede implementar a través de tecnología WIFI.
3 ¿Cuáles son las características que deben tener los dispositivos en una red inalámbrica para brindar un servicio de calidad?	Debe de ser muy confiable para mantener su nivel de salida estable, independiente del tiempo de conexión de los usuarios. (No debe de ser afectado por la temperatura de operación, a largo plazo)
4 ¿Cuál es la ventaja de constar con un sistema SAI para interrupciones de la energía eléctrica en la red inalámbrica?	Obviamente habrá protección permanente sobre fallo e interrupciones del fluido eléctrico, habrá más confiabilidad en el servicio, finalmente la inversión en baterías, (tiempo de respaldo) determinará el tiempo que se tendrá protección en la red. De la misma manera recomienda como medida de seguridad física la alimentación eléctrica debe de estar dentro

Pregunta	Respuesta
	de norma básica, en la medida de lo posible alimentado con un SAI, o mayormente conocido como UPS.
5 ¿Cuál es la importancia de una red inalámbrica?	Mayor nivel de conexiones posible. (Evita incluir puntos de accesos), (repetidores)
6 ¿Cuál es la ubicación idónea de un AP, para que garantice una conexión estable?	Alejado de paredes, muebles, impresoras, teléfonos y cualquier otro lugar que afecte su funcionamiento
7 ¿Qué consideraciones se toman en cuenta para la mejor cobertura de un AP?	Escogencia de operación del AP en GHz. La frecuencia en definitiva influye en determinar el alcance, a mayor frecuencia menor cobertura.
8 ¿Qué aspectos considera necesario para la selección adecuada de una topología de red?	Velocidad de acceso a Internet, tecnología o más bien el estándar a emplear y necesidad de cada institución.
9 ¿Cuáles son las ventajas y desventajas de utilizar un repetidor?	Permite crear redes de mayor tamaño, aunque el abuso de estos reduce abruptamente la velocidad de todos los usuarios de enrutador, debe de ser muy bien justificados y en la mayoría de los casos evitados, son soluciones puntuales y no globales.

Pregunta	Respuesta
10 ¿Qué medidas se recomiendan para evitar interferencias y mejorar una red inalámbrica?	Evitar instalar equipos que puedan ocasionar mal funcionamiento del router, no ubicarlos cerca de equipos que generen fuertes transiente de energía, los armónicos generado por estos son de frecuencia infinita y generan fuertes interferencias, ejemplos: Aires acondicionadores, deshidratadores, Motores de A.C. y/o D.C.

ANEXO N° 7

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

(UNAN – Managua)

Facultad Regional Multidisciplinaria, Matagalpa

(FAREM – Matagalpa)

Según la norma IEEE 802.11 b /n la red inalámbrica utiliza:	**ITEMS**	
Estándar IEEE 802.11b	Sí ___	No___
Estándar IEEE 802.11g	Sí ___	No___
Estándar IEEE 802.11n	Sí ___	No___
Frecuencia en GHz 2.4	Sí ___	No___
Velocidad menor o igual 11 Mbps	Sí ___	No___
Velocidad menor o igual 50 Mbps	Sí ___	No___
Velocidad igual o mayor a 100 Mbps	Sí ___	No___

OBSERVACIONES:

_____
_____
_____
_____
_____
_____

ANEXO N°8

SUGERENCIAS PARA ASEGURAR EL FUNCIONAMIENTO OPTIMO EN LA RED INALAMBRICA DEL HOSPITAL ESCUELA CESAR AMADOR MOLINA, MATAGALPA.

Evaluación realizada en el primer semestre del año 2015.

Después de la realización de esta evaluación basada en el estándar ISO 270002: 2013 y estándar IEEE 802.11, se encontraron las siguientes dificultades sugiriendo implementar y poner en practica cada uno de los puntos y parámetros evaluados a los que se hace referencia, con el fin de tener una red inalámbrica con un desempeño optimo y confiable.

No.	Dificultad	Sugerencia	Acciones	Herramienta
1	Oscilaciones de voltaje AC	1. Instalar sistema de Alimentación Ininterrumpida	Adquisición de equipos SAI	-
2	Cobertura de la red	1. Utilizar equipos de mayor cobertura	Configurar potencia apropiada para AP	Manual de Usuario
3	No existe diseño de red documentado	1. Diseño adecuado de una topología	Realizar estudio para el diseño de red	Packet Tracert
4	No existe Políticas de control de acceso a la red.	1. Restringir la cantidad de tiempo de uso a la red a los dispositivos externos a la institución. 2. Bloqueo de páginas como redes sociales para evitar la saturación en la red. 3. Tener un registro	Realizar un manual con políticas internas, adecuado a las necesidades de los usuarios para que estos tengan acceso a la red tomando en cuenta las sugerencias.	Herramientas básicas como Word office

No.	Dificultad	Sugerencia	Acciones	Herramienta
		de usuarios conectados de acuerdo a la MAC de cada dispositivo		
5	No tiene asignación de acceso con privilegios especiales restringidos y controlados	1. Asignar privilegios especiales a usuarios internos y externos. 2. Crear grupos de usuarios con privilegios que se adapten a la necesidad de cada usuario.	Investigar el cargo y tareas que realiza cada usuario.	
6	No se realiza revisión con regularidad los derechos de acceso de los usuarios.	1. Actualizar la base de datos del personal y verificar el cumplimiento de sus derechos en la red.	Crear una base de datos del personal que accesa a la red para tener un registro actualizado de cada uno de ellos.	My SQL
	No se exige a los usuarios uso de buenas prácticas para seguridad	1. Capacitar a los usuarios para el uso de buenas prácticas para la	Crear reglamento interno sobre prácticas de confidencialidad.	

No.	Dificultad	Sugerencia	Acciones	Herramienta
	confidencial.	conservación y confidencialidad de usuarios y contraseñas. 2. Sanción a usuarios que revelen información confidencial de la red.		
9	No existe política de uso, protección y ciclo de vida de las claves criptográficas.	1. Cambiar claves criptográficas de la red cada 15 días como mínimo y un máximo de 30 días.	Crear rol y poner en práctica como una tarea más en la administración de la red.	
10	No tiene definición de perímetros de seguridad para la protección de las áreas e instalaciones.	1. Definir áreas vulnerables a daños físicos de equipos o dispositivos. 2. Utilizar rótulos como medidas de seguridad a la red, para la información de usuarios y evitar el acceso a		

No.	Dificultad	Sugerencia	Acciones	Herramienta
		estas instalaciones.		
11	No cuenta con áreas seguras protegidas mediante controles de entrada.	1. Autorizar acceso a las áreas protegidas solo al personal de administración de la red. 2. Indicar al personal de seguridad el control diario de acceso		
12	No tiene protección física contra desastres naturales, ataques maliciosos o accidentes.	1. Proteger equipos ante amenazas naturales como descargas eléctricas.	Implementar una estructura de aterrizaje hacia tierra para descargas eléctricas.	
13	No cumple con la norma de control de equipos protegidos de amenazas, peligros ambientales y de oportunidad de accesos no autorizados			

No.	Dificultad	Sugerencia	Acciones	Herramienta
14	No cumple con la norma de control equipos protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros basicos de apoyo	1. Instalar sistema de alimentación ininterrumpida para protección contra cortes de energía comercial y suministros básicos de apoyo.	Adquisición de equipo SAI.	Mano de obra.
15	No cumple mantenimiento de los equipos adecuado para garantizar disponibilidad e integridad continúa	1. Realizar mantenimientos preventivos de los dispositivos que componen la red cada 30 días.		
16	No cumple con Administración y control de las redes para proteger información en sistemas y aplicaciones	1. Instalar un servidor para la administración y control de la red.	**Instalar** SERVIDOR HP PROLIANT ML150 G6 Procesador (1) Intel ® Xeon ® E5504 (2.00GHz/4-	Sistema Operativo Debían 8 ‘Jesie’ y la implementación de un portal cautivo para vigilar el trafico http, utilizando pf Sense

No.	Dificultad	Sugerencia	Acciones	Herramienta
			core/4MB/80W, DDR3-800) del procesador La memoria caché Integrado 1 x 4 MB de caché L3 memoria 4 GiB (2 x 2GiB) PC3-10600E Unbuffered memoria ECC avanzada NOTA: Total de 12 ranuras DIMM Controlador de red HP Embedded NC107i PCI Express Gigabit Server Adapter Controlador de almacenamiento	

No.	Dificultad	Sugerencia	Acciones	Herramienta
			HP Smart Array P410 controlador w / Cero de memoria caché de la controladora RAID (RAID 0,1, 0 +1) SAS: 8.0TB (4 x 2 TB de 3,5 ") máximo SATA: 8.0TB (4 x 2 TB de 3,5 ") máximo Unidad de discos ópticos HP media altura SATA DVD-ROM Unidad óptica Fuente de alimentación 460W sin	

No.	Dificultad	Sugerencia	Acciones	Herramienta
			conexión en caliente, sin fuente de alimentación redundante Fans Dos (2) - sin conexión en caliente, no redundante los ventiladores del sistema Teclado / ratón Factor de forma Torre de 5U	