Redes de área local e inalámbricas (interconexiones Wi-fi, Bluetooth).

Ing. Pedro Gómez

Introducción

Este capítulo presenta una introducción a redes de comunicaciones y sus tipos de interconexión, así como los servicios que se prestan al interior de una organización o del hogar, de igual manera se pueden identificar los procesos importantes de su funcionalidad como la interconectividad, el acceso a la red, el acceso a recursos compartidos y en general de comunicación con otros usuarios, o sistemas de información como consultas de información, verificación de estados de cuentas, hasta pago de servicios y productos en línea, tareas que se han vuelto normales para el usuario en la actualidad, dejando de lado la seguridad de la información y los riesgos en los que se incurre si estas no son configuradas de manera adecuada o si se hace un mal uso del servicio. La seguridad de la información sobre la red es una actividad compleja en la medida en que cada vez se presentan más vulnerabilidades que son utilizadas por Hackers, o crackers utilizando técnicas de reconocimiento de debilidades, así como exploración de nombres de dominio, direcciones IP, entre otras de ahí la importancia de conocer los diferentes riesgos que se presentan y poder tomar medidas preventivas antes de que estos ocurran.

Las redes de telecomunicaciones la conforman una serie de dispositivos, y equipos los cuales están interconectados de forma física y lógica a través de los dispositivos de red y de protocolos de comunicaciones que permitan compartir datos, información, aplicaciones, voz e imágenes. Las redes son la base de la infraestructura que permite la conectividad para la prestación de servicios que se ofrecen a través de la web, en la actualidad, la mayor parte de la población mundial utiliza a diario de una serie de aplicaciones y servicios que hacen las labores diarias más fáciles evitando desplazamientos y pérdidas de tiempo, dando cubrimiento a necesidades de laborales, personales y de entretenimiento. La demanda de mayores servicios a través de la red como son los servicios de correo, videoconferencias, televisión en línea, videos y demás servicios, han hecho que la tecnología se modifique y actualizarse para prestar servicios cada vez más eficientes utilizando mayor ancho de banda y tiempos de transmisión más cortos, a un costo más bajos para dichos servicios. La disminución de los costos en algunos componentes como son los equipos de cómputo en Colombia los cuales están libres de impuestos, hacen que el acceso a la red tenga un gran volumen de usuarios que no podrían hacer su trabajo si

llegase a desconectar o perder la conectividad de manera constante, esto hace que las redes de comunicación tengan un gran relevancia en la calidad de la prestación del servicio.

Las redes basan su comunicación en el uso de hosts o dispositivos finales, los cuales hacen la tarea de transmitir o recibir los mensajes de datos a través la red. Los equipos pueden dividirse en dos categorías una de estas es cliente o servidor, sin embargo, un cliente puede prestar los dos servicios o funcionales de acuerdo con la necesidad del usuario. Un equipo cliente puede ser configurado como servidor y partir de este se pueden ofrecer servicios u otros equipos o dispositivos conectados a la red, por su parte un servidor presta servicios de acceso a varios clientes o usuarios y puede servir para almacenar varios tipos de aplicaciones que requieran los usuarios de la organización

Para constituir una red de computadores se necesita de por lo menos dos computadores capaces de intercambiar información a través de diferentes medios de transmisión. En realidad, las redes que se construyen en torno a esta conexión pueden tener diferentes tamaños y características, así como los computadores pueden utilizar diferente *software* y poseer un *hardware* totalmente distinto el uno del otro. Por tanto, es importante que se establezcan algunas reglas, protocolos y se utilizan diversos dispositivos que garanticen el correcto funcionamiento de la red para que esta pueda proveer y mantener los servicios a los usuarios.

Tipos de redes

Existen diferentes tipos de redes que permiten interconectar los dispositivos y compartir los archivos, y recursos de la red de acuerdo con las necesidades y tamaño de las empresas y hogares. De conformidad con estas características podemos clasificarlas en:

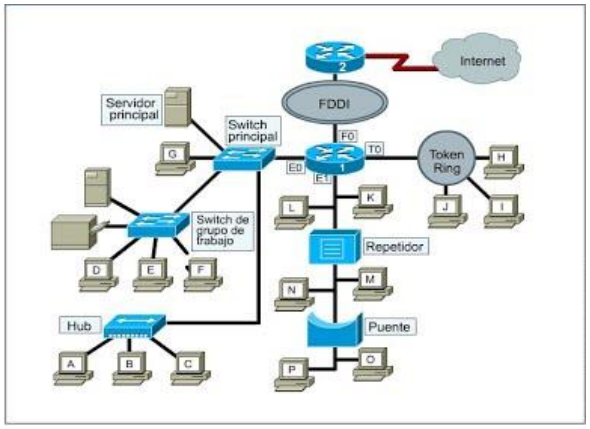
Redes de área personal (PAN).

(Internetpasoapaso, s.f.)

Son las redes más pequeñas y hacen referencia las redes que se conforman generalmente en los hogares compuestas de dispositivos como equipos de cómputo e

impresoras, su alcance es limitada y su cobertura está limitada a un alcance de 10 metros.

Redes de área Local (LAN).

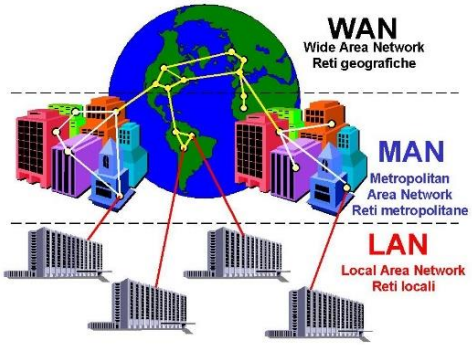


(Internetpasoapaso, s.f.)

Red de área local conformada por un grupo de equipos y tienen una cobertura geográfica pequeña, pueden implementadas desde hogares oficinas edificios entre otros, estas interconectan varios dispositivos y son administradas por una persona u organización, actualmente estas redes poseen un ancho de banda de alta velocidad para la trasmisión de datos, voz y videos.

Redes de Área Metropolitana (MAN). Son redes que prestan servicios de interconectividad en áreas más extensas que las LAN y permiten prestar generalmente servicios a una entidad en particular que Esta ubicada en una misma ciudad o región geográfica

Redes de Área Amplia (WAN).



(Internetpasoapaso, s.f.)

Componentes de las redes

Las redes de área local están conformadas por varios elementos que hacen que su unión a través de la infraestructura física de red permita brindar los servicios de interconectividad y acceso a recursos compartidos de la red. Los principales componentes que podemos encontrar son:

Estaciones de trabajo

Las estaciones de trabajo son los dispositivos o equipos de cómputo que se interconectan entre sí a través de las conexiones de red, para el envío y recepción de información, así como para compartir y acceder a recursos para la gestión de la información. Estos equipos una vez instalados y configurado con un sistema operativo generalmente Windows o Linux, pueden compartir sus recursos como aplicaciones y servicios, de igual manera pueden acceder a los servidores para realizar

consultas y transacciones de información de acuerdo con los niveles de acceso previamente establecidos. Para conocer los componentes de las redes es necesario definir qué tamaño tiene la red, ya que los elementos que la conformen van a depender de la complejidad de esta. Existen redes simples conformadas por dos computadores y redes donde miles de computadores se encuentran interconectados.

Servidores

Son equipos con gran capacidad de procesamiento y almacenamiento que pueden atender diferentes peticiones de los usuarios de manera simultánea, de igual manera están configurados con sistemas operativos desarrollados para atender requerimientos multitarea y poder prestar servicios de acceso aplicaciones y recursos compartidos desde cualquier punto de la red. Los servidores prestan diferentes tipos de servicios como servidores de aplicaciones, servidores de archivos, servidores web para alojamiento de páginas, servidores de datos y servidores de correo electrónico entre otros.

Tarjeta de Red.

Dispositivo que permite la comunicación entre estación de trabajo con otros dispositivos de la red. Todos los equipos o estaciones de trabajo traen instalada una tarjeta de red o NIC (Network Interface Card), la cual tiene un número de identificación único denominado dirección MAC (de Media Access Control) es un identificador de 48 bits y es único por cada dispositivo lo cual hace que se pueden hacer rastreo de registros de acceso por dicha dirección sin lugar a equivocación, a través de esta es que cada estación de trabajo realiza el enlace físico a la red.

Hubs

Es un dispositivo conformado por varios puertos y su función es de un repetidor de los datos que ingresan por un puerto y se difunden a través de los demás puertos de tal manera que la información dependiendo de su destino puede ser tomada o enviada a través de la red hasta que pueda llegar a otro hub o una estación destino.

Routers

El router tiene una funcionalidad en las redes, el cual permite la comunicación entre dos redes de área haciendo que los paquetes de una red puedan ser trasmitidos o reenviados otro router para que los datos puedan ser entregados a su destino. Los rotes poseen unas sus tablas con las listas de redes que se pueden comunicar y que están a su alcance para el envío y recepción de paquetes de datos.

Redes inalámbricas

Las redes inalámbricas son de uso cada días más frecuente en diferentes espacios tanto público como privadas, y podemos afirmar que estas son una extensión de las redes de área local LAN, permitiendo que esta red pueda ampliar su rango de cobertura y brindar funciones de movilidad y de portabilidad, para un tipo de usuarios son cada vez más móviles, y tienen un gran numero variado de dispositivos por medio de los cuales pueden acceder a los recursos de LAN des de sus puestos de trabajo y además desean acceder a los recurso de la rede desde cualquier punto de la organización.(Mishell & Giomayra, 2018)

Las redes comunicación inalámbrica han adquirido gran relevancia debido a la portabilidad y facilidad de conexión en la organización y diferentes escenarios donde se utilizan, están facilitan la conexión de dispositivos como teléfonos móviles, tabletas, equipos portátiles los cuales pueden compartir recursos entre ellos, o con otros usuarios conectados a la red de área local LAN.

Características de una red wifi

Una de las principales características de las redes wifi es uso del estándar IEEE.802.11a de ethernet, el cual todos los fabricantes de equipos con comunicación inalámbrica lo pueden desarrollar e integrar en sus equipos sin ninguna dificultad de compatibilidad en los modos de establecer un conexión y realizar una comunicación, entre las ventajas de usar este tipo de tecnología es la facilidad de instalación, la no dependencia de cableado y concentradores para su comunicación con otros dispositivos de la red, así como los bajos costos para su implementación. El estándar 802.11a permite alcanzar hasta una velocidad de transmisión de datos de 54 megabytes por segundo en el espectro de frecuencia de los 5ghz, utilizando 8 canales y es compatible con otros estándares como el 802.11b que pueden transmitir hasta 11mps en una frecuencia de 2,5gz utilizando 3 canales no sobrepuestos, siendo este estándar el más utilizado.

Las redes inalámbricas pueden actuar de manera descentralizada de una infraestructura de red de área local como una red independiente que permite prestar un tipo específico de servicio o dar una cobertura de servicios a una población especifica. Sin embargo, dada la necesidad de la organización estas pueden integrarse a como un brazo de la red de área local permitiendo el acceso a los mismos recursos que presta la rede de área local, solo que, de manera

móvil, donde cada nodo o usuarios interactúa con los demás permitiendo el envío y recepción de información dentro del rango y parámetros configurados para tal fin dando al usuario una autonomía y flexibilidad de movimiento particular (Muñoz, Porta, & Contreras, 2014)

Las redes inalámbricas permiten la interconexión entre uno o varios dispositivos por medio de ondas electromagnéticas utilizando el espacio, a cambio de las conexiones físicas de cableado, de acuerdo con su tamaño al igual que las redes de área local LAN tienen su clasificación de acuerdo con el número de equipos ó dispositivos que las integran, así como su alcance y cobertura de la señal

WPAN. (Wireless Personal Área Network). Red inalámbrica de área Personal, las cuales tienen una cobertura limitada utilizadas para instalaciones caseras o conexiones vía bluetooth

WLAN (*Wireless Local Área Network*) Redes de área local inalámbricas, al igual que las rede s de área local LAN, las Wireless LAN, ofrecen la facilidad de interconexión sin medios fiscos y pueden están conformados por diferentes dispositivos como equipos de cómputo, impresoras, dispositivos móviles, tabletas. Una de sus características es su facilidad de configuración, así como la movilidad que ofrecen sus usuarios para conectarse desde cualquier lugar de la organización, pueden ser implementadas a nivel de casa, oficina o una organización completa. Las redes inalámbricas WLAN, trabajan bajo estándar IEEE802.11x, el cual ha sido incorporado para facilitar al conectividad y reducción de costos de las empresas que desean utilizar este tipo de interconexión y compartir el ancho de banda con los diferentes dispositivos conectados a la red a través de los puntos de acceso a dicha red.

Las velocidades alcanzadas para la trasmisión de datos entre dispositivos que utilizan la red inalámbrica bajo el estándar 802.11a y 802.11b alcanzan hasta los 54Mbps. Para dichas transmisiones estos estándares utilizan los canales 1, 6 11, para evitar la interferencia estos canales son utilizados sobre la frecuencia 2.4ghz, la elección del canal es importante dado que las comunicaciones se compartirán con los demás usuarios conectados a la rede y por lo tanto a mayor número de conexiones menor velocidad y mayor interferencia, aunque la mayoría de routers, inalámbricos traen una configuración de canal por defecto, esta se puede modificar dependiendo de la marca del router este, trae una herramienta para analizar el espectro electromagnéticos y seleccionar el canal más óptimo para

establecer la comunicación. Otra forma de establecer el canal adecuado es utilizar una herramienta de monitoreo gratis llamada wifi analyzer, que permite monitorear el espectro e indicar cual s el canal más adecuado para el dispositivo y su entorno, lo cual le garantiza una conexión estable y eficiente.

La tasa de transmisión empleada dependerá del estándar del dispositivo, así para 801.11b el límite superior estará en los 11 Mbps, y para 802.11a y 802.11b en 54 Mbps. En la mayoría de los dispositivos, es seleccionable una tasa inferior al límite del estándar.

WMAN (*Wireless Metropolitan Área Network*). Son redes de área metropolitana inalámbricas, estas funcionan bajo el estándar IEEE 802.16x ó WiMax, los medios de trasmisión utilizados según sus frecuencias pueden ser ondas de radio, microondas terrestres o vía satélite y los rayos infrarrojos. Estas redes tienen una cobertura amplia para cubrir con su señal una ciudad o un territorio, la conectividad entre el emisor y el receptor debe tener visibilidad de conexión dado que la conexión se hace punto a punto, de acuerdo con el rango de frecuencia a transmitir, la comunicación se puede hacer por ondas de radio, microondas y rayos infrarrojos.

Comunicación por ondas. Estas son representadas campos eléctricos los cuales se propagan en forma de andas de manera transversal, estas viajan a la velocidad de luz, sufren una ralentización al atravesar diferentes materias dependiendo de su conformación y permeabilidad del objeto, durante la trasmisión estas ondas pasan por diferentes estados como son: Reflexión electica la cual consiste en desplegar los rayos de luz en diferentes direcciones una vez estos se han estrellado con algún objeto, un ejemplo seria al chocar con un espejo el reflejo sale en diferentes direcciones,

Refracción eléctrica. Esta hace referencia al cambio de dirección obtenida por u rayo de luz al atravesar un objeto.

difracción y absorción.

Comunicación por infrarrojos

Los protocolos estándares para la comunicación en las redes inalámbricas metropolitanas son los 802.11 802.11a, 802.11b, 802.11c, 8’2.11d, hasta el 802.11s. Cada uno de estos ofrece unas características de comunicación que difieren de la capacidad de ancho de banda, el acceso a la red y la velocidad para trasmisión de video y voz en línea de forma simultánea.

Tabla: estándares de trasmisión inalámbricos

Protocolo	Descripción
802.11	Primer estándar que permite un ancho de banda de 1 a 2 Mbps. Trabaja a 2,4 GHz
802.11a	Llamado también WiFi5. Tasa de 54 Mbps. Trabaja en torno a 5 GHz, frecuencia menos saturada que 2,4.
802.11b	Conocido como WiFi. El más utilizado actualmente. Las mismas interferencias que para 802.11 ya que trabaja a 2,4 GHz. Tasa de 11 Mbps.
802.11c	Es una versión modificada del estándar 802.1d, que permite combinar el 802.1d con dispositivos compatibles 802.11 en el nivel de enlace de datos.
802.11d	Este estándar es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Define los requisitos de ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo. Está destinado a mejorar la calidad del servicio en el nivel de la capa de enlace de datos.
802.11f	Su objetivo es lograr la interoperabilidad de puntos de acceso (AP) dentro de una red WLAN mutiproveedor. El estándar define el registro de puntos de acceso dentro de una red y el intercambio de información entre ellos cuando un usuario se traslada desde un punto de acceso a otro.
802.11g	Ofrece un ancho de banda de 54 Mbps en el rango de frecuencia de 2,4 GHz. Es compatible con el estándar 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h	El objetivo es que 802.11 cumpla los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tengan control de la potencia de transmisión y selección de frecuencia dinámica.
802.11i	Aprobada en Julio 2004, se implementa en WPA2. Destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el protocolo de encriptación AES.
802.11n	Se basa en la tecnología MIMO. Trabajará en la frecuencia de 2.4 y 5 GHz. Soportará tasas superiores a los 100Mbps.
802.11s	Redes Mesh o malladas.

(Networkworld, s.f.)

Conexiones redes Bluetooh

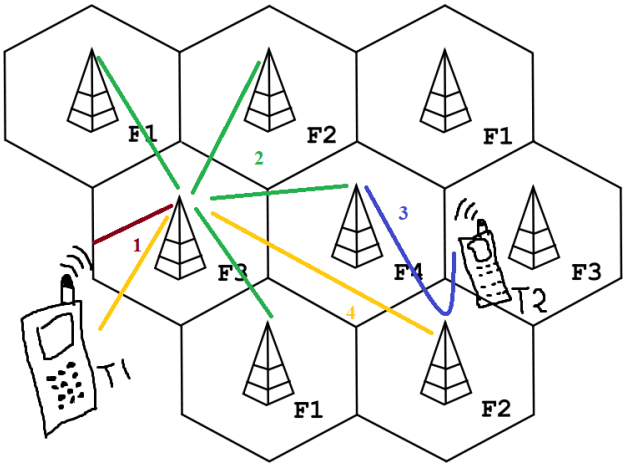
El bluetooh es un estándar de la tecnología inalámbrica utilizada para interconectar dispositivos que permite la funcionalidad dicho estándar, es comúnmente utilizado en las redes de área personal PAN, para el envío y recepción de información en entornos de ofician o casa en los cuales las instancias de conexión no son muy distantes la frecuencia para utilizada para estas comunicaciones es de 2,4 GHz. La tecnología bluetooh ha tenido varias versiones desde su creación desde la versión 1.0 hasta la versión 5.0, en las cuales su variación son los tiempos de trasmisión, la capacidad de trasmisión de datos medida en mps, la cual va incrementando en cada nueva versión y la funcionalidad y aplicabilidad de esta tecnología, la cual en su última versión se está focalizando al funcionamiento de los dispositivos para el internet de las cosas como una tecnología con un futuro por desarrollar y que cada día toma más fuerza.

Comunicaciones en Redes de telefonía móvil

Dado el auge de las comunicaciones en móviles en Colombia y uso de dispositivos móviles daremos una mirada general al concepto y funcionalidad de estas, se dará un repaso a cada uno de los componentes de la red de telefonía móvil celular y sus componentes **Telefonía móvil celular TMC.**

De acuerdo con el documento de la Universidad Nacional del Rosario acerca de la tecnología móvil, en el año 2003 donde se refiere lo siguiente:

La definición de la Telefonía Móvil Celular (TMC), es una red que se conforma por diferentes áreas, las cuáles a su vez se dividen en celdas (células) hexagonales que se encajan para poder formar un patrón de panal, como se muestra en la figura a continuación, Esta división permite la re-utilización de frecuencias a través del área o ciudad, permitiendo que muchas personas puedan acceder a una llamada telefónica simultáneamente., y las señal pueda ser retomada o trasportada de una celda a otra si el usuario está en movimiento.



(Rodriguez, s.f.)

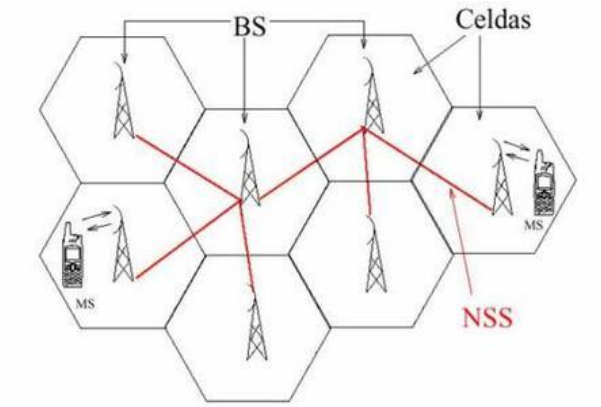


Figura 2. Clúster de una Red Móvil
(Rodriguez, s.f.)

En cada área geográfica de una red de telefonía móvil celular se distribuyen un determinado número de canales de radio celular; esto significa que cada transceptor con un área envolvente tiene un subconjunto fijo de canales de radio disponibles, basados en el flujo de tráfico anticipado.

Como se mencionó anteriormente, las áreas se componen de celdas; la forma de hexágono de cada celda se debe a que la transmisión que proporciona es más efectiva que la de un patrón circular, dado a que elimina espacios presentes entre los círculos adyacentes (técnicamente elimina la interferencia cocanal.

Una célula o celda se define por tres características: tamaño físico, tamaño de población a la cual le va a proporcionar cobertura y patrones de tráfico, siendo estas dos últimas las más importantes. De acuerdo con el tipo de celda varían de tamaño, pueden abarcar desde pocos metros hasta 64 kilómetros cuadrados o más. El radio mínimo está determinado por limitaciones técnicas en los procesos de handoff (manos libres) y de instalación de equipos. Para dar mayor servicio se utilizan celdas de menor tamaño. El número de celdas por área lo define el operador y lo establece de acuerdo con los patrones de tráfico establecidos con anterioridad.

Existen diferentes tipos de celdas, debido a que la densidad de población en un país es muy variada. Éstas se dividen principalmente en:

Macroceldas: Son celdas grandes, para áreas con población dispersa. Estas celdas por su alcance se utilizan por ejemplo en poblaciones como Zipaquirá, Cajicá, Chía en el área suburbana.

Microceldas: Estas celdas son usadas para áreas densamente pobladas. Estas celdas son utilizadas en ciudades principales como Bogotá, de acuerdo con el operador de la red se establece por ejemplo una o más para cubrir un barrio de la ciudad.

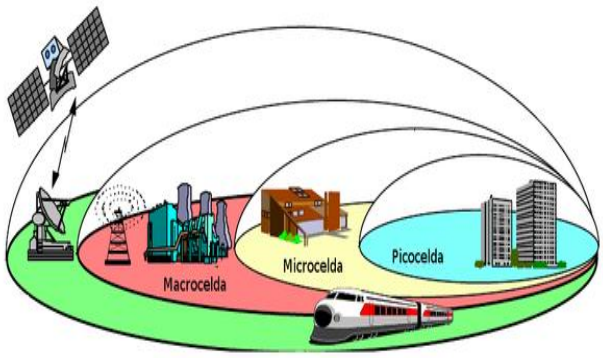
Picoceldas: Son las celdas de menor tamaño utilizadas para interiores. Estas celdas son utilizadas para dar cobertura a todo un edificio por ejemplo el edificio de Colpatria.

Celdas Selectivas: Son celdas con una forma particular de cobertura, como por ejemplo para dar cobertura a una universidad; siempre

y cuanto la unidad móvil se encuentre dentro del circulo (360 grados).

Una definición de Telefonía Móvil Celular (TMC), podemos decir que es una red compuesta por diferentes áreas, las cuáles a su vez se dividen en celdas (células) hexagonales que se encajan para poder formar un patrón de panal. Esta división permite la reutilización de frecuencias a través del área o ciudad, permitiendo que muchas personas puedan acceder a una llamada telefónica simultáneamente. En cada área geográfica de una red de telefonía móvil celular se distribuyen un determinado número de canales de radio celular; esto significa que cada transceptor en su espacio de cobertura posee una agrupación de canales habilitados de radio, de acuerdo con el flujo de tráfico. e. (Gómez, Polo, & Rivera, 2011).

Celdas Paraguas: Son celdas que tienen el nivel de potencia aumentado, para reducir el número de handoff. Estas celdas son colocadas por ejemplo en las carreteras donde el móvil puede variar significativamente de una estación base a otra.



(Revista.unam.mx, s.f.)

Riesgos en redes de área local

Las mayores preocupaciones que se tienen una vez se tiene un dispositivo o equipo conectado a la red, son los riesgos de ataques por parte de hackers quienes están atentos a identificar falencias de seguridad que surgen desde la falta de configuración apropiada del sistema operativo hasta la exposición a externa que se tiene por falta de protecciones de acceso a externos como firewalls que denieguen el acceso a personas no autorizadas que pueda acceder a la información y afectar la integridad y disponibilidad de esta. Algunos de los riesgos más frecuentes los que se exponen los equipos o dispositivos de red son:

Virus. Son los más frecuentes que se hacen a través de programas desarrollados generalmente para afectar un servicio u ocasionar daño a un servicio, se reciben a través de la web, o a través de correo electrónicos.

Hackers: Acceso a la red o recursos compartidos, de personas no autorizadas con el objeto de obtener información el acceso no autorizado de un tercero a todo o parte del nuestro sistema de información.

Denegación de servicios: consisten en el bloqueo parcial o tal de los recursos de un servidor para lo cual el atacante utiliza técnicas de envío de múltiples peticiones de un determinado servicio de esta manera demandando muchos recursos del servidor atacado a atender dicha solitud dejando lento o bloqueado el servicio para los demás.

Tipos de Ataques y Vulnerabilidades en redes

Existe diferentes tipos de ataques los cuales cada di son más frecuentes y son realizado por diferentes motivos desde un mecanismo de protesta contra una entidad o gobierno hasta la búsqueda de atacar con el objeto de obtener acceso a información relevante para cualquier propósito

DHCP Spoofing El protocolo DHCP (Dynamic Host Configuration Protocol) es un componente integral para la funcionalidad del protocolo de internet (IP) de las redes actuales. Su función es configurar automáticamente equipos clientes con direcciones IP y algunos otros parámetros relevantes para la red como la máscara de red, la puerta de enlace (Gateway), o los servidores DNS (Domain Name System) (Mukthar, 2012). Los ataques básicamente se realizan suplantando un servidor de servicios DHCP, capturando las solicitudes realizadas por los clientes y una vez obtenida la información del usuario puede tomar su dirección IP ya través d esta lanzar ataques a la red

.

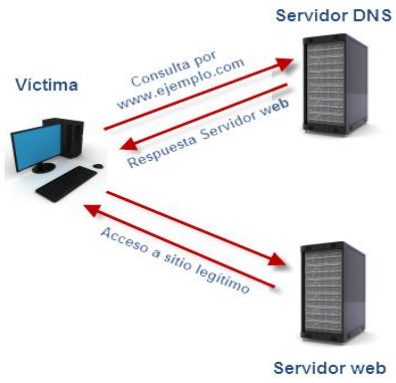
Escaneos de puertos. Una de las practicas comunes para denegar servicios de red es el escaneo de puertos básicamente orientado a revisar que puertos en los servidores web, servidores de bases de datos, servidores de correo, e identificar cuales se encuentran abiertos y a partir de esta información el atacante obtiene el número del puerto y estado del mismo, si el puerto se encuentra abierto ofrece una puerta de entrada la cual utiliza para el acceso o inicio de un ataque por demanda de un servicio (Villalón, 2002). Verificar el estado de un puerto es una actividad fácil de realizar utilizando una herramienta como, TCPing que servirá para realizar escaneos de puertos en sistemas Windows, desde la línea de comando de una manera muy sencilla, herramientas como nmap, ssh, o putty, para sistemas Linux.

Spoofing. Conocido como suplantación de identidad, es un ataque que se realiza con el objeto de interceptar la información del usuario y modificar o alterarla su contenido, para

hacerlo el atacante utiliza un el nombre de un dominio conocido ejemplo el nombre del sitio de una entidad bancaria y lo asocia a una dirección IP Falsa y con algún tipo de invitación hace que los usuarios accedan al sitio y registren sus datos de ingreso y contraseñas, dejando al atacante la información, con la que puede acceder y realizar diferentes tipos de acciones. En este proceso interviene el atacante, la víctima o atacado y el sitio suplantado (Villalón, 2002).

Existen diferentes tipos de ataques spoofing entre ellos se tienen:

Dns Spoofing.



(Catoira, 2012)

El ataque tipo DNS spoofing afecta la integridad de la información y ocurre cuando se suministra una dirección IP distinta a la cual se tiene asignada, una vez el equipo establecido como objetivo a atacar pregunta por una dirección, se le indica una respuesta de dirección falsa antes que reciba, la respuesta correcta. Si es bastante rápida, este procesara la información antes de que lo haga el sitio real. Se trata de vulnerar la relación existente de un nombre de dominio, la cual está asociada a una dirección IP, en el momento de realizar una consulta de resolución de nombre de dominio, es decir, se le entrega a quien hace la consulta una dirección IP diferente a la que realmente está asociado el dominio real, o viceversa. Para lograrlo se falsifica las entradas o tablas de relación dominios-ip, del servidor DNS. Esto permite que las entradas afectadas alteren o infecten el cache de los demás servidores DNS, y esto hace parecer que se está accediendo al sitio real, del cual se requiere un servicio, lo que se conoce como DNS Poisoning (Calles y González, 2011).

ARP Spoofinng. Técnica mediante el atacante utiliza el envío de tramas de datos falsificadas de direcciones arp (address resolution protocol), en una red de área local. Como resultado el atacante asocia la dirección MAC, con la dirección IP real asignada de un equipo o servidor en la red. Una vez se logró establecer la relación, el equipo servidor empezará a enviar la información al equipo suplantado, y este recibirá toda la información que se traspase en dichas conexiones. Estos ataques denominados también redirección ARP, reenvían el tráfico de uno o varios equipos de la red de área local, al equipo del cracker. Este proceso se realiza dentro de la

red de área local de las víctimas, revisando como funciona dentro de la red, se recuerda que la comunicación entre equipos o dispositivos de red se hace mediante el envío de datos (Detoisien, 2005).

Denegación de servicios (en inglés: **Denial of Service o DoS**) El atacante tiene como propósito limitar total o parcialmente la disponibilidad de un determinado recurso o servicio, el cual puede ser bloqueado, como ejemplo un número de puerto, un nombre de servicio, o un bloqueo de acceso a un aplicativo en particular.

Dentro de los tipos de denegación de servicio podemos mencionar algunos de los más importantes:

Consumo de recursos: Los recursos que se tiene para poder ofrecer los servicios como ancho de banda, acceso a bases de datos o aplicaciones son atacados mediante la técnica de inundación generalmente orientada hacia los servidores de la organización sobre los cuales está funcionando la mayoría de los servicios.

Modificación de datos configuración. Ocurre cuando un atacante logra ingresar a un servidor y alterar o modificar la configuración de los mismos afectado la prestación de los servicios, o bloqueando el servicio a los usuarios.

Daño físico de los componentes de la red. Cuando los elementos de la red no están debidamente asegurados o protegidos, estos pueden ser alcanzados y afectados físicamente por el atacante el cual puede ocasionar daños fiscos como cortocircuitos inducidos, desconexión de la red de datos, desconexión de la red eléctrica, daño ocasionado por golpes.

Intercepción de datos confidenciales, aunque no dañe directamente los sistemas informáticos, un tercero que consiguiera obtener de forma indebida datos o documentos confidenciales puede causar perjuicio importante. Dentro de estos podemos mencionar el acceso a claves de usuario las cuales pueden caer en manos terceros ajenos a la organización y ser utilizadas de manera fraudulenta para modificar o alternar la información

Ataques por spam o correos no deseados (ataque SMTP)

Los correos no deseados son los que más reciben los usuarios a través de sus cuentas de correo y por lo general tiene como finalidad hacer publicad los cuales son enviados de manera masiva desde servidores de correo se envían indiscriminadamente a varias listas de correo, usuarios individuales o grupos de noticias. Existen dos tipos de correos spam los mensajes de correo comercial no solicitados y mensajes de correo masivo no solicitados. En términos generales los correos no deseados

tienen como finalidad hacer publicidad de servicios o productos no requeridos afectando al receptor, llevando a la casilla de recibidos de un servidor o buzón en particular, induciendo al usuario a acceder a sitios de promociones de productos que no requiere en los que tienen contendidos fraudulentos, con virus, o sitios dedicados a extraer datos como ubicación, usuario. contraseñas con fines de realizar ataques o robo de información.

Cuando se reciben correos no deseados de cuentas desconocidas o redes sociales esos deben ser marcados como spam para que no se sigan propagando y en la medida en que se pueda identificar las direcciones IP de los sitios de origen para agregarlas a sitios no deseados, o solicitar al administrador de seguridad que esta sea incluida en las listas no deseadas de tal manera que en un futuro cualquier mensaje proveniente de dichas direcciones sea bloqueado.

Algunos ejemplos de spam que podemos mencionar cuando se reciben coreos con información sobre el recibo de pagos de dinero por ingresar a un sitio o incrementar su salario de amena sencilla, que hacen atractiva la oferta para el usuario y lo inducen a ingresar a un sitio, de igual manera correos recibidos de oficinas bancarias facturas por cuotas de pago, así como correos de pago de infracciones detectadas por foto multas, pago de impuestos a la Dian enviados desde correos que suplantan las direcciones de correo oficiales de las instituciones suplantadas, haciendo que el usuario actué de forma desprevenida y entregue sus datos y de igual manera propague los mensajes recibidos dentro de sus listas de contactos frecuentes. La afectación del servicio de conectividad es el principal objetivo que buscan este tipo de ataques, dado que maximizan el consumo de ancho de banda, requieren de un mayor solicitudes de conexiones, de igual manera hacen un mayor consumo de espacio de almacenamiento y demandan de mayor capacidad de recursos como la memoria para el procesamiento de las peticiones y servicios. Es recomendable mantener la bandeja de entrada del buzón de correo desocupada, y tener una copia de seguridad de los correos de los mensajes relevante que requieren posteriores consultas

Ataques web. Una de las debilidades que más explotan los atacantes es la relacionada con las apelaciones web, en las que se busca identificar las vulnerabilidades que existentes las interacciones entre sus componentes, las cuales pueden ser interceptadas a través de la inyección de código o sentencias de cortas de software que permiten tomar la información que se envió a través de servicios como los de validación de cuentas requerimientos de servicios en línea. Los ataques web utilizan la inyección de código malicioso creado especialmente para disuadir las aplicaciones y

poder acceder a la información crítica para la organización. Por otra parte, también pueden afectar la disponibilidad de un servicio, dado que la mayoría de las transacciones se hacen a través de aplicaciones que funcionan sobre la web, convirtiéndose de esta manera en una oportunidad para que los atacantes despliegen sus programas de inyección de código maliciosos y obtengan la información confidencial de manera fraudulenta de forma ilegal, o puedan llegar a tomar control de la sesión del usuario y través de esta realizar operaciones no autorizadas.

Gran parte de los ataques realizados por este medio tienen una probabilidad alta de ocurrencia debido a la no actualización de los sistemas operativos de acuerdo con las recomendaciones de los fabricantes los cuales están sacando de forma permanente parches o actualizaciones de sus sistemas con el objetivo de evitar vulnerabilidades detectadas por los usuarios, o falta de implementación de políticas de seguridad sobre sus servidores, en general los ataques vía web son muy variados y estos utilizan los bugs de las páginas web para que el servidor en entregue información a usuarios no registrados.

Riesgos en redes wifi

Existen diferentes dificultades o puntos de falencia al hacer uso de las redes inalámbricas las cuales pueden ser explotadas por diferentes tipos de ataques presentando grandes riesgos para la funcionalidad y la información que se maneja por parte de los usuarios. Una de las principales es la configuración inicial de seguridad dada que los dispositivos generalmente están configurados para que se activen de forma automática brindando el servicio de conexión a dispositivos que se encuentren alrededor dentro de su rango de conexión, estas configuraciones generalmente no están realizadas con buenas prácticas de seguridad y permiten que personas no autorizadas accedan a la red sin la debida autorización.

Los conceptos de seguridad aplicados a las redes de área local pueden ser aplicados de cierto modo las redes wifi con el objeto de garantizar la seguridad del entorno establecido por la red, las consecuencias que se presentan de manera frecuente por el ataque a la red wifi son:

Contraseñas: La mayoría de los dispositivos que hacen uso de las redes wifi, poseen varias vulnerabilidades de acceso debido a sus configuraciones y la más frecuente es la falta de contraseñas fuertes de acceso, dejan do abierta la posibilidad de que sea vulnerado.

Consumo de ancho de banda: Al no tener una protección adecuado de registro a nuestra red esta puede tener un número de conexiones

no autorizadas, lo que hace que de forma automática el ancho de banda sea compartido con otros usuarios afectado de forma directa el servicio,

Accesos no autorizados: El acceso de equipos no autorizados se da como consecuencia de una inadecuada configuración de los dispositivos de acceso a la red wifi, o de la falta de monitoreo de la misma en el cuales se pueden observar las tendencias de consumo de anchos de banda o peticiones de servicio de recursos de la red, lo cuales son los principales riesgos en que se incurre a tener este tipo de acceso generando riesgos de perdida d de información, robo de contraseñas para acceso a cuenta de correo y cuentas bancarias por parte de hackers.

Responsabilidad legal: El riesgo de acceso a la red wifi es alto dado los niveles básicos de seguridad establecidos y los cuales son vulnerados a ves de forma sencilla y sistémica. Sin embargo, cabe recordar que la vulneración de la seguridad con propósitos de afectar la funcionalidad del equipo, modificar o alterar la información de manera irregular, así como borrar o sustraer información sin la debida autorización están penalizados por la legislación colombiana, lo que hace que quien incurra en cualquiera de estas prácticas puede ser denunciado por estos hechos.

Otros de los riesgos que se tienen con la implementación redes wifi, es la emisión de ondas radioeléctricas de hasta 100mw, los cuales pueden afectar a los seres humanos, discusión que siempre se ha dado y está en estudio por diferentes organismos de regulación tecnológica de comunicaciones, dichas radiaciones no ionizantes pueden emitir niveles suficientes para calentar tejidos biológicos según se desprende de varios estudios y reconoce la propia Unión Europea (UE).

La identificación los riesgos es fundamental para el buen funcionamiento de la red, uno de los procesos que se realizan para identificar posibles falencias son los monitoreos de red ya sea de área local o red inalámbrica, los cuales ayudan a identificar los riegos a que están expuestos los dispositivos y su información una vez conectados a la red, los cuales pueden ir desde perdida de información hasta la exposición a un ataque por un tercero. Algunos de estos riegos son:

- ✓ Ralentización de servicios
- ✓ Fuga de información a entes externos
- ✓ Ataque cibernético
- ✓ Espionaje
- ✓ Sabotaje
- ✓ Virus en los equipos

Una vez identificados los posibles riegos se debe realizar un análisis y evaluación de estos

y su posible impacto en la organización. Los riesgos de asociados con los dispositivos y componentes de red sensibles de la organización si se utilizan los medios adecuados y los controles más efectivos, tienen una probabilidad de ocurrencia baja basados en las estadísticas, sin embargo, el impacto para la institución en caso de que se materialice uno de estos riesgos en de nivel crítico o muy crítico por la misma naturaleza de la información pueden afectar la disponibilidad y funcionalidad de los servicios de red de la organización.

		Severidad del Riesgo			
Probabilidad	Catastrófico	Peligroso	Mayor	Menor	Insignificante
5. Frecuente	5A	5B	5C	5D	5F
4. Ocasional	4A	4B	4C	4D	4F
3. Remoto	3A	3B	3C	3D	3F
2. Improbable	2A	3B	2C	2D	2F
Extremadamente improbable	1A	1B	1C	1D	1F

Tabla 1. Identificación de Riesgos

La presente tabla muestra la probabilidad del riesgo y su impacto en caso de ocurrencia de acuerdo con el monitoreo y la identificación constante de los riesgos hallados debe evaluarse, analizarse de acuerdo con esta, establecer un tratamiento adecuado para cada uno de estos en caso de ocurrencia, así como los responsables de llevar a cabo dicha actividad.

Mecanismos de prevención y seguridad

En la actualidad es de vital importancia el manejo de la seguridad de los dispositivos de conectividad que prestan los servicios de red de la organización, estos deben estar al tanto de los riesgos y las amenazas que surgen cada vez con mayor frecuencia, presentando los niveles de impacto mayor en caso de ocurrencia, por lo tanto surge la necesidad de establecer los mecanismos de prevención y seguridad que garanticen la funcionalidad de la infraestructura de conectividad y la disponibilidad de los servicios que se prestan sobre esta, para lograrlo se deben establecer procedimientos de control, con ayuda de elementos o herramientas de software de monitoreo, que generen alertas de prevención de riesgos y activen mecanismos de seguridad que garanticen la protección total de recursos que hacen parte del sistema de conectividad, hardware, software, recursos humanos, tecnológicos y datos sensibles que son de vital importancia para la institución, todos integrados por protocolos, normas y directivas transitorias y permanentes.

Uno de los mecanismos de seguridad y prevención de ataques de la rede se hace a través del monitoreo constantes, por lo tanto, esta una actividad indispensable en la organización, y deben existir un área responsable de dicha actividad. Los reportes de estos monitoreos nos informa los potenciales riesgos y posibles vulnerabilidades que se presentan de manera continua en la red, los cuales no son fáciles de identificar para un usuario que no está familiarizado con estos, y a partir de los resultados se deben actualizar y/o cambiar los proceso y las políticas de seguridad establecidas con el fin de proteger la información y evitar el acceso de usuarios no autorizados los recursos, así como de impedir el acceso a los dispositivos activos de la red, con fines diferentes a los establecidos.

Protocolos de seguridad

Las buenas prácticas de seguridad informática hacen que los administradores de la infraestructura tic, establezcan planes de seguridad y creen manuelas de buenas prácticas para el uso adecuado de los activos tecnológicos de la organización, procurando que la información pueda llegar a ser vulnerada por los intrusos. Para complementar esta labor además de las decisiones de una buena práctica, los equipos activos y sistemas de información deben tener instalados los protocolos estándares de seguridad conocidos los cuales traen incorporados mecanismos y procedimientos que hacen que las transacciones y/o peticiones entre usuarios sean más confiables. Algunos de estos protocolos son:

IPSEC. Es un estándar que brinda servicios de seguridad de comunicación a los protocolos basados en IP, TCP y UDP, por los servicio

que ofrece se ha vuelto en un estándar implementado por la mayoría de fabricantes de dispositivos de comuniones, y de igual manera se ha incorporado en las últimas versionas de los diferentes operativos, una de sus principales características es que es un estándar desarrollado bajo el esquema de código abierto y es compatible con otros estándares de seguridad, de igual manera garantiza la escalabilidad para futuros desarrollos. Algunas de las ventajas que brinda el estándar está el garantizar el acceso seguro a uno nodo o equipo que accede de forma remota, permite realizar transacciones de comercio electrónico entre empresa – empresa ya que garantiza integridad y la confidencialidad la seguridad de extremo a extremo.

Ipsec está conformado por un conjunto estándares de seguridad para integrar distintas formas de encriptación. Combina mecanismos y tecnologías de clave pública con programas o algoritmos de encriptación como son (DES, 3DES, IDEA), así como algoritmos para descifrar como son MD5 y SHD-1. El Ipsec está conformado por dos componentes, uno enfocado a la seguridad el cual a su vez está compuesto por el (AH) autenticado de cabecera y el (ESP) que es la carga de seguridad de encriptación la cual le brinda seguridad al tráfico IP. El segundo componente hace referencia al protocolo para la gestión de claves, el cual permite a los dispositivos que se van a comunicar establezcan la interconexión compartiendo los parámetros y características de la comunicación.

SSL (sokect Security Layer). Capa de conexione seguras es un protocolo que utiliza certificados para las transacciones que se realizan a través de Internet, está basado en la estructura de clave secreta clave pública y es utilizado para garantizar la integridad de la información que viaje en internet para ser entregada de un nodo origen al nodo destino. El protocolo ssl funciona como una capa más del modelo tcp/ip, ubicada entre la capa de aplicación y la capa de red., lo cual lo hace como un módulo más que funciona de forma independiente. Ssl es un protocolo sencillo de aplicar ye s utilizado por la mayoría de navegadores web, utiliza un algoritmos DES(Data encryption Standar) PARA ENCRIPTAR y para la verificación de la comunicación MD5(Message Digesth algorithm), para realizar el proceso de comunicación segura con el protocolo ssl, se inicia con una petición de comunicación entre los nodos, una vez las parte sestan de acuerdo con al comunicaciones establecen los parámetros de transmisión una vez establecido el proceso se hacen verificaciones periódicas de la comunicación hasta finalizar el proceso. De igual manera el protocolo ssl es el encargado de hacer las solicitudes de forma segura entre clientes y servidor de tal manera

que cada sesión que se establece este haciendo el proceso adecuado

Protocolo SSH (Secure Shell). EL interpretador de ordene seguras es usado para comunicarse entre el un cliente a servidores virtuales remotos a través de la red, El SSH utiliza mecanismos de encriptación que hacen que la información trasmitida a través de la red no sea fácil de descifrar, el mecanismos de cifrado de la SSH es de clave publica

El protocolo SSH o más conocido como “Secure Shell” (Interprete de órdenes seguro) nombre que también identifica al programa, es utilizado para acceder a máquinas virtuales remotas a través de una red. SSH usa técnicas de cifrado que hacen que la información viaje por el medio de manera legible, garantizando que ninguna tercera persona pueda descubrir el usuario, la contraseña de conexión ni lo que se escribe durante toda la sesión. Por otra parte SSH usa criptografía de llave pública para autenticar el equipo remoto y permitir al mismo autenticar al usuario si es necesario, sin embargo también permite el reenvío de puertos TCP de forma arbitraria y de conexiones X11 (Tecnología que permite ejecutar sesiones X11 remotas de manera rápida y con excelente calidad gráfica, fue desarrollada por la compañía francesa NoMachine, la cual ofrece aplicaciones cliente y servidor de manera gratuita (pero no libre) y también de manera comercial). Un servidor SSH por defecto, escucha el puerto TCP 22. Un programa cliente de SSH es utilizado generalmente para establecer conexiones a un dominio sshd que acepta conexiones remotas. Ambos se encuentran comúnmente en los sistemas operativos más modernos, incluyendo Mac OS X, Linux, Solaris y OpenVMS. Existen actualmente dos versiones de SSH (versión 1 y versión 2)

HTTPS

- **Escaneo de vulnerabilidades**

1.

Entre los procedimientos a nivel global se encuentran:

- Verificación de accesos: Mediante aplicaciones que informen anomalías, incluyendo fecha, hora, recurso y detalles técnicos.
- Chequeo del tráfico de red: también mediante aplicaciones que entreguen informes periódicos de los programas que se ejecutan, quién es el encargado de monitorear los datos generados, los intervalos de monitoreo, etc.
- Monitoreo de los volúmenes de correo: Permite entregar detalles como el ingreso de “spam” a la red, posibles invasiones o mal uso de los recursos de la red.
- Monitoreo de conexiones activas: Este procedimiento se efectúa con el fin de prevenir que algún usuario deje su

terminal abierta y sea posible que alguien use su cuenta. También se usan aplicaciones para monitorear la actividad de las conexiones de los usuarios. Si la cuenta tiene cierto tiempo inactiva, cierra la sesión y genera un informe (log) con el acontecimiento.

- Monitoreo de modificación de archivos: Permite determinar la modificación no autorizada de los recursos de software y/o de la integridad de estos. Este es quizás el procedimiento más importante dentro de lo que es seguridad global, pues permite saber si, por ejemplo, un archivo es eliminado o la presencia de algún tipo de virus en el sistema.
- Respaldos de seguridad: No sólo es importante respaldar la información que se encuentra en la red, sino además la configuración de todos los recursos de la red, incluyendo la labor que desempeña cada elemento de la red, a fin de crear una respuesta rápida en el momento de que se suscite un problema.
- Verificación de terminales: Esto se hace mediante la revisión de los programas instalados en los equipos terminales de la red, lo que permite monitorear qué aplicaciones sin licencia, archivos bajados potencialmente peligrosos (virus, programas satélites).
- Monitoreo de puertos: Permite saber qué puertos están habilitados en la red, en los enrutadores y en el servidor. Esto se puede hacer incluso con los mismos enrutadores, los cuales poseen aplicaciones integradas que permiten administrar los puertos en forma más eficiente.
- Información de los procedimientos: Esto es la clave para cualquier sistema que desee evitar el mayor número de problemas en una red. Informando apropiadamente, mediante seminarios internos de seguridad, vía e-mail y publicaciones periódicas, se llega a más gente de manera más eficiente.
- Determinación de los niveles de responsabilidad y acceso: Es importante además identificar a cada usuario en un grupo determinado (por ejemplo, equipo técnico, oficina gerencial, oficina zonal, alumnos, profesor, etc.) para determinar el nivel de acceso a los recursos de la red.
- Recuperación del sistema: En caso de un ataque o un colapso eventual del sistema (Se quemó el servidor, necesidad de actualizar todos o algunos recursos de la red) es necesario preparar un procedimiento que regule la forma de recuperarlo a través de los respaldos de seguridad

realizados. Para ello se debe estimar la forma y los costos (en materiales y en tiempo) para llevar a cabo la restauración.

- Listas de elementos a verificar (check-list): Es importante enlistar todos los procedimientos, con el fin de asegurar la realización de cada uno en su totalidad.

1. Seguridad en NetBIOS

El sistema operativo más usado actualmente es Windows. La mayoría de las redes corporativas ocupan este sistema operativo por una razón muy sencilla: es "amigable" y "fácil de usar". Pero es un sistema cerrado. No admite modificaciones, ni libertad de acción en sus subrutinas. Esto quizás por un lado es positivo, ya que también entrega un sistema muy difícil de romper, desde el punto de vista de un atacante. Como sea, los sistemas operativos de Microsoft usan el protocolo NetBIOS para comunicarse entre sí. Esto significa una gran desventaja desde el punto de vista comunicacional, debido a que otros sistemas operativos no requieren de NetBIOS para comunicarse entre sí, pero sí para comunicarse con terminales que usan sistemas operativos Microsoft (como todo en Microsoft, es exclusivo de su sistema operativo, pero con un buen parche… quien sabe). Este protocolo a su vez debe ir sobre otro de inferior nivel que puede ser uno de los siguientes: NetBEUI, IPX/SPX o TCP/IP. Desde la implementación de Windows Vista, el protocolo NetBEUI (Interfaz de usuario extendida de NetBIOS) ya no se usa, pero también debido a la falta de interés en este último sistema operativo, lo incluiremos en el estudio. A la implementación de NetBIOS sobre TCP/IP se la conoce como NBT. La ventaja en una red Microsoft es que esta implementación nos permite compartir archivos e impresoras en una red Microsoft. Por lo general, en redes en las que se encuentran presentes equipos Microsoft la mejor combinación es usar NBT, aunque a veces es mejor usar otras combinaciones, como es en el caso de una red LAN con conexión a Internet. En este caso, quizás la mejor combinación es NetBIOS sobre IPX/SPX, que además tiene la ventaja de compatibilidad con otros sistemas operativos. Dentro del tema, quizás uno de los mayores problemas a los que nos enfrentamos cuando se habla de redes Microsoft, son las carpetas compartidas. Grave error. La mayoría considera trivial incluir una contraseña para acceder a una carpeta compartida de "sólo lectura". Y lo que es peor, ignora absolutamente que esta carpeta puede ser vista por todos los usuarios de Internet. En efecto, si tiene montado el protocolo NetBIOS sobre TCP/IP, la carpeta será considerada como

compartida no sólo por todos los usuarios de la red local, sino por todos los usuarios de Internet. Esto se evita de manera relativamente sencilla: se configura el enrutador filtrando los puertos que usan NBT para uso exclusivo de la red local. Esto también obviamente aplica a redes WAN. Otras maneras de incrementar la seguridad de las redes son: uso de tarjetas de booteo (boot disks) en los terminales de la red, trabajar con enrutadores confiables (Cisco Systems para redes WAN, no menos de D-Link para redes LAN) y por supuesto, informar a los usuarios acerca de las normas y regulaciones de uso de la red.