Seguridad Informática - 2º SMR
Tema 5: Seguridad activa en el sistema y redes.

5.1 Introducción

La seguridad activa como ya vimos en el primer tema se refiere al conjunto de medidas que previenen o intentan evitar los daños en el sistema informático.

Además, cada vez que nos conectamos a Internet se produce un intercambio de información entre nuestro equipo y la red.

Si alguien se hace con esta información podríamos vernos afectados por grandes volúmenes de tráfico no deseado y ser víctima de un ataque de denegación de servicio.

Ningún dispositivo, por sencillo que sea, está libre de sufrir un ataque, por lo que es muy importante minimizar las posibilidades de que esto ocurra. Existen diversas herramientas que nos permitirán proteger los equipos de la red, como los cortafuegos y los proxys.

En este tema aprenderemos a mejorar la seguridad del acceso al ordenador, impedir la carga de un sistema operativo desde un dispositivo extraíble, a configurar las contraseñas en las cuentas, a mejorar la seguridad ante los ataques definiendo contraseñas y mecanismos de autenticación, además de las técnicas y herramientas para proteger los equipos en las redes.

5.2 Seguridad de acceso al ordenador

Debemos asegurar el arranque mediante contraseñas y como recordaremos el acceso a la BIOS es muy importante así que es de gran importancia proteger su entrada mediante una contraseña.

El uso de **contraseña para entrar en la BIOS** evitará que personas no autorizadas modifiquen la configuración del ordenador, así como cambios en el orden de arranque, evitando así que se permita arrancar el sistema desde medios extraíbles, y por tanto, evitando el acceso a los datos almacenados en él.

También se puede poner **contraseña al gestor de arranque GRUB**, tanto para evitar que accedan a su configuración como para evitar que entren en los sistemas operativos gestionados por este gestor.

Otra medida de seguridad sería el **cifrado de particiones** que se puede realizar con cualquier software de encriptación de disco.

5.3 Identificación y autenticación de los usuarios

Se denomina identificación al momento en que el usuario se da a conocer en el sistema; y autenticación a la verificación que realiza el sistema sobre esta identificación.

Existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden utilizarse solas o combinadas:

- Algo que solamente el usuario **conoce**: una clave, un PIN …
- Algo que la persona **posee**: una tarjeta magnética...
- Algo que el individuo **es** y que lo identifica unívocamente: huellas dactilares, la voz...
- Algo que el usuario es **capaz de hacer**: patrones de escritura...

Hay sistemas de seguridad que combinan distintos métodos por ejemplo cuando vamos a sacar dinero del cajero automático se combina el uso de una tarjeta magnética (algo que poseo) con la petición de un PIN (algo que sé).

5.3.1 Contraseñas seguras

Siguiendo los siguientes criterios se puede conseguir una contraseña segura:

- **Que no sea corta**. Cada carácter que se agrega a la contraseña aumenta exponencialmente el grado de protección que ésta ofrece. Las contraseñas deben contener al menos 8 caracteres; lo ideal es que contenga 14 o más. Muchos sistemas admiten el uso de la barra espaciadora para las contraseñas, de modo que pueden crearse frases compuestas de varias palabras (una frase codificada). Por lo general, una frase codificada resulta más fácil de recordar que una cadena simple, además de ser más larga y más difícil de adivinar.
- **Combina letras, números y símbolos**. Cuanto más diversos sean los tipos de caracteres de la contraseña, más difícil será adivinarla.
- **No incluyas secuencias ni caracteres repetidos**.
- **Evita utilizar únicamente sustituciones de letras por números o símbolos similares**. El 1 por la i o la @ por a. Son fácilmente descifrables. Sí son útiles combinados con otras medidas como mayor longitud o errores ortográficos voluntarios o variaciones entre mayúsculas y minúsculas.
- **No utilices palabras del diccionario de ningún idioma**.
- **No utilices el nombre de inicio de sesión**.
- **No deben usarse sólo letras mayúsculas o sólo minúsculas**.
- **No debemos utilizar información personal: nombre de familiares, fecha de nacimiento, número de teléfono...**
- **No debemos invertir palabras reconocibles, como atatap, añesartnoc …**
- **No se debe escribir la contraseña en ningún sitio.**
- **No debemos enviar la contraseña a ningún correo electrónico que nos la solicite ni comunicársela a nadie por teléfono**.

- **Se deben limitar el número de intentos fallidos**.
- **Siempre se deben cambiar las contraseñas por defecto de routers y otros periféricos**.
- **No se debe utilizar la misma contraseña para distintas máquinas o sistemas**.
- **Las contraseñas deben caducar**, se deben cambiar por lo menos una vez al año.
- **No debemos permitir que las aplicaciones recuerden las contraseñas**.

5.3.2 Sistemas biométricos

Las tecnologías de identificación de personas, basadas en mediciones de características biológicas y sociales están teniendo un auge importante, incluso a niveles particulares.

Biometría es la "parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos".

Cuando este estudio cuantitativo se automatiza utilizando métodos matemáticos y ayudado por ordenadores, se llama Biometría informática. La identidad que se construye utilizando estos procedimientos se llama identidad biométrica de la persona.

Sistema biométrico es un sistema automatizado que realiza tareas de biometría. Es decir, un sistema que basa sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida y/o verificada de forma automatizada.

Tipos de Biometría:

- **Biometría fisiológica**: se basa en medidas o datos de partes del cuerpo humano. Las más importantes son la medidas de las huellas dactilares, el iris, la retina, la voz, la mano y el rostro.
- **Biometría conductual**: se basa en las medidas o datos de acciones de una persona, e indirectamente en sus características físicas. Las más importantes son el uso de un teclado y la firma de la persona.

Estos sistemas funcionan en dos partes:

- Una primera parte de registro, donde se recogen los datos mediante los sensores adecuados y se establece la relación entre esos datos obtenidos con la identidad de la persona suministrada y se guardan estos datos con esta relación.
- Una segunda parte que consiste en la identificación propiamente dicha del usuario para permitirle o no el acceso al sistema correspondiente. En esta parte se recoge de nuevo mediante los sensores los datos biométricos establecidos (huella, voz...) y se comparan con los guardados anteriormente en la parte de registro. Si coinciden, entonces se valida la identidad del usuario.

Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

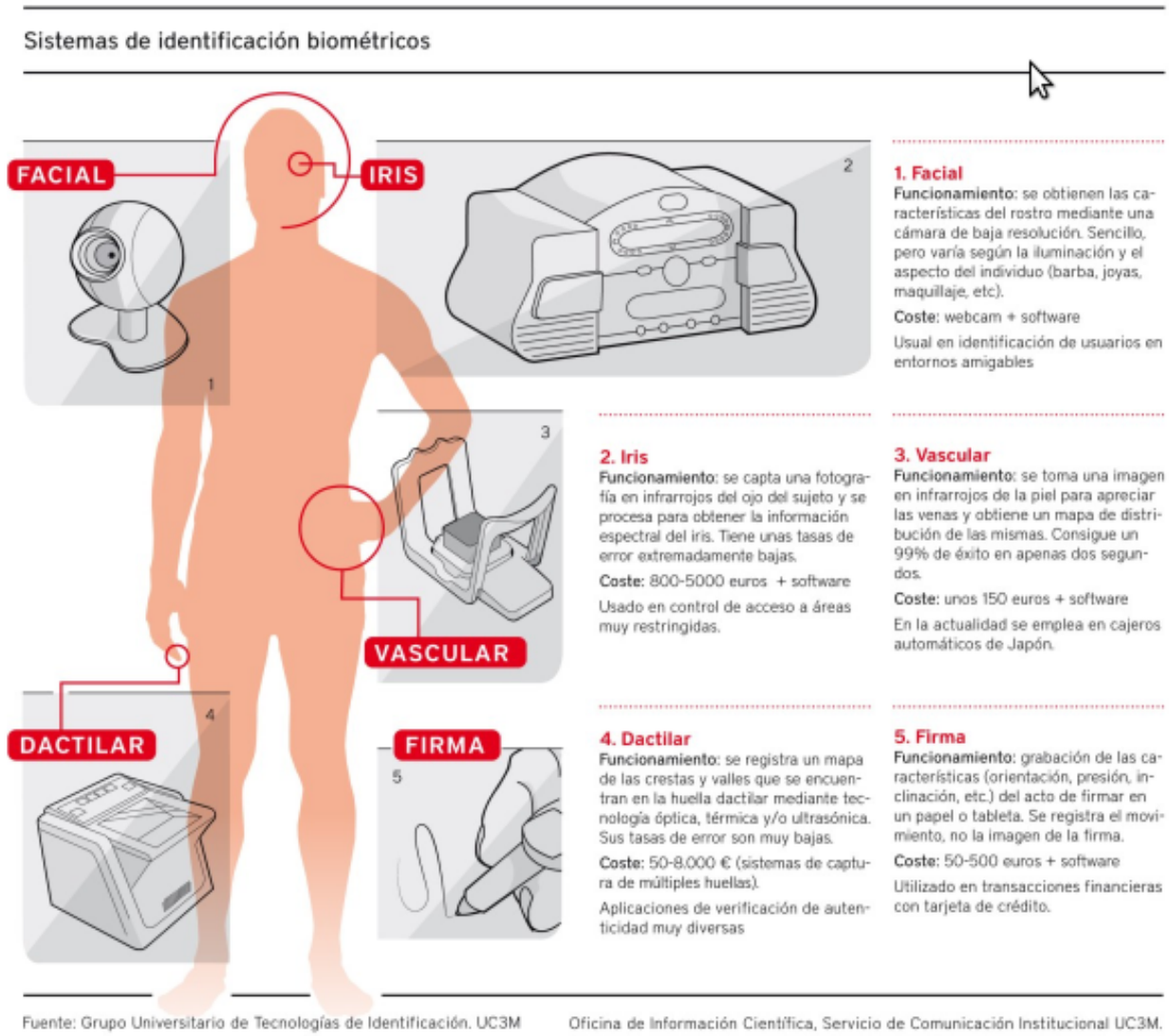
- Rostro,
- Termograma del rostro,
- Huellas dactilares,
- Geometría de la mano,

- Venas de las manos,
- Iris,
- Patrones de la retina,
- Voz,
- Firma.

Algunos de estos indicadores biométricos pueden combinarse dando paso a la Biometría Multi-Modal. Por ejemplo, son clásicas las siguientes combinaciones:

- Iris + Huella dactilar + Rostro.
- Iris + Huella dactilar + Venas.
- Huella dactilar + Firmas.

La siguiente imagen muestra los diferentes métodos más usuales:



TÉCNICA	VENTAJAS	DESVENTAJAS
Reconocimiento de cara	Fácil, rápido y barato	La iluminación puede alterar la autenticación
Lectura de huella digital	Barato y muy seguro	Posibilidad de burla por medio de réplicas, cortes o lastimaduras pueden alterar la autenticación
Lectura de iris/retina	Muy seguro	Intrusivo (molesto para el usuario)
Lectura de la palma de la mano	Poca necesidad de memoria de almacenamiento de los patrones	Lento y no muy seguro
Reconocimiento de la firma	Barato	Puede ser alterado por el estado emocional de la persona
Reconocimiento de la voz	Barato, útil para accesos remotos	Lento, puede ser alterado por el estado emocional de la persona, fácilmente reproducible

5.4 Vulnerabilidades del sistema

Los sistemas operativos son programados y sometidos a numerosas pruebas antes de ser lanzados al mercado, pero no se descubren sus verdaderas vulnerabilidades hasta que son atacados por hackers, crackers... Entonces, esos agujeros son corregidos lo más rápido posible y pasados a los sistemas mediante las actualizaciones. De ahí la importancia de tener el sistema actualizado en todo momento.

5.4.1 Tipos de atacantes

- **Hackers**: Gente apasionada por la seguridad informática. Sienten una gran curiosidad y se dedican a intentar encontrar vulnerabilidades en los sistemas operativos y de seguridad existentes, pero sin ningún ánimo de producir daño o de obtener beneficio económico. También son llamados hackers de sombrero blanco o white hat, en referencia a las antiguas películas del oeste donde el bueno llevaba sombrero blanco y el malo sombrero negro.
- **Crackers o hackers de sombrero negro**: Los medios utilizaban la palabra hacker para refererirse a cualquier ataque independientemente de su finalidad. Los propios hackers inventaron otra palabra para aquellos hackers cuya finalidad era maliciosa. La palabra cracker viene de CRiminal hACKER.
- **Preakers**: Expertos en telefonía. Phone crackers. Sabotean las líneas telefónicas intentando obtener un beneficio económico.
- **Ciberterroristas**: Expertos en intrusismo en la red que se ponen al servicio de de organizaciones o países para el espionaje o el sabotaje informático.
- **Programadores de virus**: Expertos en programación que realizan pequeños programas que se propagan por la red ocasionando daños.
- **Carders**: Atacan sistemas de tarjetas bancarias, especialmente cajeros automáticos.
- **Sniffers**: Son personas que se dedican a escuchar el tráfico de red, para intentar descifrar mensajes que circulan por ella.

- **Lammers**: También conocidos como wannabes o script-kiddies o click-kiddies, son chicos jóvenes que se creen hackers o lo hacen creer a los demás cuando en realidad no tienen grandes conocimientos informáticos. Suelen bajarse herramientas o programas de Internet para realizar ataques y los ponen en marcha sin saber como funcionan.
- **Newbies**: Hackers novatos.

5.4.2 Tipos de ataques

5.4.2.1 Según los objetivos de la seguridad que vulneran

- **Interrupción**: Vulnera de disponibilidad del recurso. Pueden ser: denegación de servicio, apagado manual de un recurso...
- **Intercepción**: Ataca la confidencialidad. La información cae en manos no autorizadas. Por ejemplo: captura de información en la red o copia de archivos no autorizada.
- **Modificación**: Vulnera el objetivo de integridad. Los datos han sido manipulados por alguna persona no autorizada. Por ejemplo: modificación de un programa para que haga algo diferente, DNS spoofing...
- **Fabricación**: Ataca el objetivo de la autenticidad. Se trata de modificaciones para conseguir un producto similar al atacado de forma que sea difícil distinguir del original. Por ejemplo: phising.

5.4.2.2 En función de la forma de actuar

Spoofing:

O suplantación de la personalidad. Este ataque consiste en falsear algún dato de un PC atacado. Este tipo de ataque se usa en redes ethernet conmutadas, es decir, redes que hacen uso de un switch como elemento de interconexión entre diferentes PC's.

- **Arp spoofing**: Consiste en engañar a la tabla arp que los equipos guardan en memoria. Esta tabla relaciona IP con direcciones MAC. Con esta técnica podemos hacer creer al equipo atacado que la IP del atacante es la de otro equipo también atacado en la red.
- **DNS spoofing**: consiste en falsear la respuesta del servidor DNS, por ejemplo para proporcionar la IP de un equipo con una página similar a la de un banco para pedir las contraseñas.

Sniffing o análisis de tráfico:

En redes comunicadas mediante hub es un juego de niños ya que el hub difunde todos los mensajes por todos los puertos. Mediante un switch es más complicado porque los mensajes sólo se envían por el puerto adecuado. Para conseguir este ataque se suele utilizar el MAC flooding que consiste en saturar la memoria del switch para que pierda su tabla de direcciones de forma que termina trabajando como un hub y se puede ver todo el tráfico de red sin problema.

Conexión no autorizada a equipos servidores:

Consiste en descubrir agujeros en la seguridad del sistema y establecer una conexión no autorizada. Puede ser por haber descubierto las contraseñas de usuarios, o utilizando herramientas malware que aprovechan las puertas traseras o agujeros para permitirnos conectarnos.

Denegación de servicio:

También conocido por sus siglas DoS (Denial of Service). Se realiza contra servidores para evitar que sigan dando el servicio que ofrecen. La mayoría de estos ataques son realizados desde muchos ordenadores que han sido convertidos en zombies. Este ataque se llama DoS distribuido.

- **Zombie**: Ordenador en el que un cracker ha instalado software malicioso para hacerse con el control del mismo.

Inundación de peticiones SYN o SYN Flood:

Consiste en hacer una petición de conexión a un servidor y no contestar. Este ataque produce una saturación en las conexiones abiertas del servidor y puede llegar a producir el colapso del servidor. Con el comando netstat se pueden revisar las conexiones abiertas y comprobar si estamos siendo atacados con este método.

Dialers:

Se hicieron famosos a principio de los noventa cuando la mayoría de la gente se conectaba a Internet mediante módem. Consistía en hacer llamar al módem sin conocimiento del usuario a un teléfono con tarificación especial.

Ingeniería social:

Consiste en obtener información secreta de un usuario u organismo para utilizarla posteriormente de forma fraudulenta. Suelen ser correos electrónicos llamativos o páginas que suplantan a las verdaderas donde nos piden información secreta como códigos...

- **Phising**: Es un ejemplo de ingeniería social.

Spyware

Un spyware es un pequeño programa que se instala en nuestro equipo con el objetivo de espiar nuestros movimientos por la red y robar nuestros datos, de modo que a través de él puede obtenerse información como nuestro correo electrónico y contraseña, la dirección IP de nuestro equipo, nuestro teléfono, páginas buscadas y visitadas, así como cuánto tiempo se pasa en ellas, u otros datos igualmente importantes como las descargas realizadas, las compras que hacemos por Internet e incluso el número de tu tarjeta. A medida que recopilan esta información la envían a empresas de publicidad de Internet para comercializar con nuestros datos.

Este tipo de software se instala sin que tengamos conocimiento de ello y trabaja en segundo plano, de modo que no nos damos cuenta de su presencia, aunque existen una serie de indicios que pueden alertarnos de que están ahí:

- Cambian las páginas de inicio o búsqueda del navegador.

- Se abren pop-ups por todos lados, incluso aunque no estemos conectados ni tengamos abierto nuestro navegador, llenando la pantalla.
- Aparecen barras de búsquedas de sitios como Hotbar, etc., que no podemos eliminar.
- Falsos mensajes de alerta en la barra de Windows (al lado del reloj) de supuestas infecciones que no podemos eliminar.
- Cuando navegamos por Internet hay veces que no se llega a mostrar la pagina Web que queremos abrir, ya que el tráfico de red va cada vez más lento.

> **Ejercicios propuestos**
>
> **5.4.1.** Busca información sobre diferentes herramientas que permitan bloquear spyware u otro código malicioso en nuestro equipo.

5.4.3 Software malicioso

Actualmente, gracias al uso generalizado de las TIC, los sistemas de información se han convertido en objetivo de todo tipo de ataques. Por esta razón es fundamental identificar qué recursos y elementos necesitan protección así como conocer los mecanismos o herramientas que podemos utilizar.

Con el nombre software malicioso o malware agrupamos los virus, gusanos, troyanos y en general todos los tipos de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario y producir efectos no deseados.

5.4.3.1 Clasificación.

La siguiente clasificación la realizaremos en función de estos criterios:

- Por su capacidad de propagación.
- Por las acciones que realizan en el equipo infectado.

5.4.3.1.1 Por su capacidad de propagación

- **Virus**: Su nombre es una analogía de los virus reales ya que infectan otros archivos. Los ficheros infectados generalmente son ejecutables: .exe, .src, .com, .bat; pero también pueden infectar otros tipos como macros de Office. Los virus se ejecutan cuando se ejecuta el fichero infectado, aunque algunos están programados para activarse cuando se cumpla una condición concreta, como por ejemplo una fecha. Cuando están en ejecución suelen infectar otros ficheros del mismo tipo que el anfitrión original del virus. Los virus fueron el primer tipo de código malicioso que surgió.
- **Gusanos**: Su característica principal es realizar el máximo número de copias posibles de sí mismo. Se suelen propagar por los siguientes métodos: Correo electrónico, Redes de compartición de ficheros P2P, Explotando alguna vulnerabilidad, Mensajería instantánea, Canales de chat. Suelen utilizar ingeniería social para incitar al receptor a que abra un determinado fichero que contiene la copia del gusano. Correos llamativos que inciten la apertura del fichero adjunto, nombres de películas de actualidad... Además, como los gusanos no infectan ficheros, para garantizar su ejecución suelen modificar algunos parámetros del

sistema, por ejemplo la lista de de programas de inicio, el registro para forzar su ejecución en algún momento...

- **Troyanos**: Carecen de rutina propia de propagación, pueden llegar al sistema de diferentes formas: Descargado por otro programa malicioso. Descargado sin conocimiento del usuario al visitar una página web. Dentro de otro programa que simula ser inofensivo.

5.4.3.1.2 Según las acciones que realizan

- Adware
- Bloqueador
- Bomba lógica
- Broma (Joke)
- Bulo (Hoax)
- Capturador de pulsaciones (Keylogger)
- Clicker
- Criptovirus (Ransomware)
- Descargador (Downloader)
- Espía (Spyware)
- Exploit.
- Herramienta de fraude.
- Instalador (Dropper)
- Ladrón de contraseñas (PWStealer)
- Marcador (Dialer)
- Puerta trasera (Backdoor)
- Rootkit
- Secuestrador del navegador (browser hijacker)

> **Ejercicios propuestos**
>
> **5.4.2.** Busca la explicación de cada uno de los malware vistos arriba. Una pregunta del examen será definir algunos de ellos.
>
> **5.4.3.** Busca información sobre 5 ejemplos reales y muy peligrosos de malware. Primero pon la definición del tipo de malware y después haz una ficha con el nombre, nombre de archivo y método de propagación e infección y mecanismo de reparación.

5.5. Seguridad en redes cableadas

Tradicionalmente las redes cableadas se han considerado más seguras que las redes inalámbricas, sobre todo si se trata de una red local aislada y confinada en un edificio.

Desgraciadamente esto no es tan sencillo: el uso de Internet ha hecho que los emplazamientos de los equipos de una misma red puedan situarse a miles de km de distancia, pero siga siendo necesario mantener la conectividad entre ellos.

Podemos protegernos de intrusiones externas mediante el uso de redes privadas virtuales (VPN).

5.5.1 Red privada virtual (VPN)

¿Qué es?

Una VPN o Red privada virtual es, básicamente, una red virtual que se crea dentro de otra red, habitualmente Internet. Las VPN permiten, mediante el uso de Internet, establecer una conexión remota de modo directo, independientemente de donde se encuentren físicamente. Además, como utilizan protocolos de seguridad, el acceso a los recursos tiene carácter privado.

Para un cliente VPN se trata de una conexión que se establece entre su equipo y el servidor de su organización, pero la manera en que se realiza es transparente a él, simplemente los datos le son enviados igual que si llegaran a través de la LAN a la que se conecta.

¿Cómo funciona?

Las VPN se basan en establecer un túnel entre los dos extremos de la conexión y usar sistemas de encriptación y autenticación para asegurar la confidencialidad e integridad de los datos que se transmiten.

Una vez establecida la conexión, los paquetes de datos se envían encriptados a través del túnel establecido.

Instalación y configuración

Cuando implementemos una VPN, será necesario realizar la instalación y configuración de dos partes bien diferenciadas, el servidor y el cliente.

5.6. Seguridad en redes inalámbricas

Ventajas que nos proporcionan las redes inalámbricas:

- Movilidad: nos permite conectarnos desde cualquier punto.
- Escalabilidad: podemos añadir equipos fácilmente y con un coste reducido.
- Flexibilidad: permite colocar un equipo en cualquier punto.

Inconvenientes de las redes inalámbricas:

- Menor rendimiento: el ancho de banda es mucho menor.
- Seguridad: cualquiera que esté en el alcance de la red puede aprovechar una vulnerabilidad para colarse en la red o descifrar mensajes.
- Interferencias: la red es mucho más sensible a interferencias.

5.6.1. Tecnologías Wi-Fi

El estándar IEEE 802.11 define los protocolos para la comunicación inalámbrica:

Protocolo	Frecuencia	Alcance aproximado	Velocidad	Otros
802.11a	5GHz	50 metros	54 Mbit/s	Menos interferencias. Sensible a obstáculos
802.11b	2,4GHz	100 metros	11 Mbit/s	Menos sensible a obstáculos. Más sensible a interferencias.
802.11g	2,4GHz	100 metros	54 Mbit/s	Mismas interferencias que el anterior.
802.11n	2,4GHz 5GHz	100 metros	600 Mbit/s	Compatibles con todos los anteriores

Los dispositivos electrónicos Wi-Fi que interactúan entre sí pueden seguir diferentes estándares, y tendrán que ser compatibles entre ellos para poder comunicarse.

5.6.2. Conceptos de redes Wi-Fi

Lo más habitual en redes Wi-Fi es la topología infraestructura en la que existe un punto de acceso que es el encargado de gestionar el proceso de comunicación entre todas las estaciones Wi-Fi.

Para que un cliente pueda comunicarse con la red tiene que estar aociado al punto de acceso y para poderse asociar tiene que pasar un proceso de autenticación. Una vez pasado este proceso, la estación quedará asociada al punto de acceso y podrá comunicarse con este y a través de él con otros equipos.

5.6.3. Seguridad Wi-Fi

Habitualmente queremos controlar quien se conecta a nuestra red. Podemos aplicar varias medidas de seguridad:

- **Nivel físico**: podemos intentar controlar la señal producida por los puntos de acceso y las interferencias recibidas. A través de la utilización de diferentes antenas podemos intentar conseguir que la señal salga lo menos posible de los límites deseados.
- **Nivel de enlace**: a través de contraseña o de control de acceso a través de una característica del cliente, como la MAC o nombre de usuario y contraseña.

> **Ejercicios propuestos**
>
> **5.6.1.** Consulta en alguna tienda on-line cual sería el coste de un router inalámbrico y 3 adaptadores WiFi, dos para portátil y uno para el ordenador del aula. Averigua si todos los elementos seleccionados son compatibles. Si no lo son, escribe por qué.
>
> **5.6.2.** ¿Qué diferencia en coste hay entre montar una red con 3 equipos 802.11g y 802.11n?

5.7. Seguridad WEP

Wired Equivalente Privacy: Sistema de cifrado estándar que se utilizó inicialmente para el cifrado del protocolo 802.11. Intenta dar a las redes inalámbricas la seguridad que se tiene en las redes cableadas.

Cuando se utiliza WEP, el punto de acceso y las estaciones de trabajo tienen que compartir una clave.

WEP utiliza un algoritmo llmada RC4 para a partir de la clave WEP y de un vector de inicialización de 24 bits, generar una secuencia aleatoria, llamada semilla, la cual utilizará para cifrar la comunicación con el punto de acceso.

Existen dos métodos a través de los cuales un usuario puede autenticarse con un punto de acceso WEP:

- **Abierta (open)**: La estación puede autenticarse sin necesidad de utilizar la clave WEP, simplemente con solicitar la asociación, el punto de acceso dará por asociada a la estación. Después de este proceso de autenticación la estación solo podrá comunicarse con el punto de acceso si conoce la clave WEP utilizada para encriptar la comunicación.
- **Clave compartida (shared key)**: Cuando una estación envía una solicitud de asocia- ción al punto de acceso, este envía un texto sin cifrar a la estación, llamado «desafío». El punto de acceso solo asociará a las estaciones que devuelvan correctamente cifrado con la clave WEP dicho texto.

5.8. Seguridad WPA

Debido a los problemas de seguridad descubiertos en el estándar WEP, el comité de estandarización 802.11i comienza a investigar una nueva solución.

Los estándares WPA y WPA2 se centrar en asegurar el proceso de autenticación y el cifrado de las comunicaciones. Se proponen dos soluciones en ambos estándares:

- WPA Empresarial: Requiere la utilización de un servidor RADIUS.
- WPA Personal: Requiere compartir una clave entre todas las estaciones de la red y no requiere la utilización de un servidor RADIUS.

5.8.1. Seguridad WPA personal.

WPA personal utiliza PSK (Pre-Shared-Key) o clave precompartida para el proceso de autenticación. Durante este proceso se negocia entre las estaciones y el punto de acceso la sucesión de claves que se van a utilizar para cifrar la comunicación posterior. Cada estación negocia su propia clave, por lo que las claves utilizadas por cada estación son diferentes, y además cambian cada cierto tiempo.

Existen dos tipos de encriptación en WPA:

- **TKIP** (protocolo de integridad de clave temporal): Es un protocolo que partiendo de una clave (que no es la precompartida) compartida entre el punto de acceso y todas las estaciones, genera nuevas claves diferentes para cada cliente renovables cada cierto tiempo.

- **AES** (cifrado avanzado estándar) es un algoritmo más robusto y complejo que TKIP. Es preferible utilizar AES que TKIP, por ser este más avanzado y seguro. Como inconveniente requiere hardware más potente. No todos los dispositivos W-Fi son compatibles con todos los estándares, hay que comprobar que las estaciones que se van a conectar son compatibles con dichos estándares.

5.8.2. Seguridad WPA empresarial

El principal inconveniente de los sistemas de seguridad anteriores es el hecho de que las estaciones de trabajo tienen que conocer la contraseña de acceso. Cuanta más gente conozca la contraseña más riesgo hay de que caiga en malas manos. Se podrían perder equipos con la contraseña guardada, se podría averiguar mediante ingeniería social...

Además existe también el inconveniente de la dificultad del cambio de contraseña. Si hay muchos equipos que utilizan el punto de acceso, no se puede cambiar la contraseña con mucha frecuencia.

Para solventar estos problemas se crea la seguridad WPA empresarial.

Según especifica el estándar 802.1x se definen tres elementos en la estructura necesaria para poder utilizar la arquitectura WPA empresarial:

- **Peticionario**: la estación de trabajo que está intentando acceder a la red.
- **Autenticador**: elemento encargado de permitir el acceso o no a un peticionario. En nuestro caso es el punto de acceso.
- **Servidor de autenticación**: encargado de comprobar la identidad del peticionario y permitir o negar el acceso, informando al autenticador.

5.9. Bibliografía:

- Costas Santos, Jesús Seguridad informática Editorial RA-MA
- Seoane Ruano, César et al. Seguridad informática Editorial McGraw- Hill
- http://recursostic.educacion.es/observatorio/web/es/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad
- http://recursostic.educacion.es/observatorio/web/es/software/servidores/1065-listas-de-control-de-acceso-acl