

Tema 5. Redes y Seguridad

1.- Introducción.....	2
2.- Redes de Ordenadores.....	2
2.1.- Clasificación de Redes.....	2
2.1.1.- Clasificación según su tamaño o cobertura.....	2
2.1.2.- Según el medio de conexión:.....	3
2.2.- Topología de Red.....	3
2.2.1.- Red en Bus.....	4
2.2.2.- Red en Estrella.....	4
2.2.3.- Red en Anillo.....	5
2.2.4.- Red en árbol.....	5
2.2.5.- Red en Malla.....	5
2.3.- Dispositivos de Red.....	6
2.3.1.- Cableado.....	6
2.3.2.- Tarjeta de Red.....	6
2.3.3.- Dispositivos de Conexión de Red.....	7
2.3.3.1.- Modem.....	7
2.3.3.2.- Concentrador o Hub.....	7
2.3.3.3.- Conmutador o Switch.....	8
2.3.3.4.- Punto de Acceso Inalámbrico o WAP.....	8
2.3.3.5.- Enrutador o Router.....	9
2.3.3.6.- Router ADSL.....	9
2.4.- Protocolos y Servicios.....	9
2.4.1.- Dirección IP.....	10
2.4.2.- Máscara de Subred.....	10
2.4.3.- Servicio de Nombres de Dominio o DNS.....	11
2.4.4.- Parámetros de Red.....	11
2.4.5.- Configuración Básica de Red.....	11
2.4.6.- Funcionamiento Básico de una Red.....	11
2.4.7.- Red inalámbrica.....	12
2.4.8.- Bluetooth.....	12
3.- Seguridad Informática.....	12
3.1.- Mitos y Falacias de la Seguridad.....	13
3.2.- ¿Contra qué debemos protegernos?.....	13
3.3.- Riesgos y Amenazas.....	14
3.3.1.- Factores de Riesgo.....	14
3.4.- Técnicas de Seguridad.....	14
3.4.1.- Contraseñas.....	15
3.4.2.- Encriptación o Criptografía.....	15
3.4.2.1.- Sistema de Clave Privada.....	15
3.4.2.2.- Sistema de Clave Pública.....	16
3.4.3.- Software de Seguridad.....	16
3.5.- Identidad Digital.....	16
3.5.1.- Certificado Digital.....	16
3.5.2.- Firma Digital.....	17

1.- Introducción

Todos los ordenadores de la sala están conectados entre sí, pero ¿cómo se comunican?

Todos nos conectamos alguna vez a Internet, pero ¿cómo funciona?

Hemos oído hablar de virus, spam, troyanos, pero ¿qué riesgos tengo y cómo puedo prevenirme?

¿Qué diferencias hay entre un modem y un router?

2.- Redes de Ordenadores

Red de Ordenadores: Es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, ondas o cualquier otro método, que comparten información (archivos), recursos (discos, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc.

Una **Intranet** es una red de ordenadores privados que utiliza la misma tecnología que en Internet para compartir de forma segura información o programas del sistema operativo... pero evita que cualquier usuario de Internet pueda ingresar.

Internet: es un conjunto descentralizado de redes de ordenadores interconectadas, que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas que la componen funcionen como una red lógica única, de alcance mundial.

Extranet: es una red de ordenadores privada que utiliza Internet como medio de comunicación con otras redes de ordenadores, para compartir información, recursos y servicios de forma segura.

Actividad 1.

2.1.- Clasificación de Redes

2.1.1.- Clasificación según su tamaño o cobertura

WPAN: Red Inalámbrica de Área Personal es una red para la comunicación entre distintos dispositivos (ordenadores, puntos de acceso a internet, móviles, PDA, impresoras) cercanos al punto de acceso. Tamaño: unos pocos metros. Aplicación: uso personal. Tecnologías Wifi y/o Bluetooth.

LAN: red de área local, es la interconexión de varios ordenadores y periféricos. Tamaño: limitada a un edificio o a un entorno de 200 metros. Aplicación: interconexión de ordenadores en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. Una intranet es una LAN. Ejemplo: la red del instituto.

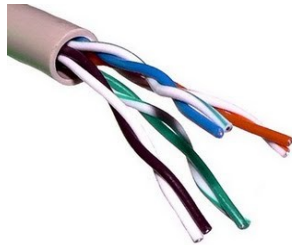
MAN: Red de área metropolitana es una red que conecta diversas LAN cercanas geográficamente entre sí a alta velocidad. Tamaño: área de alrededor de cincuenta kilómetros. Ejemplo: red de Universidad o una localidad.

WAN: Red de área amplia, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo de este tipo de redes sería Rediris.

Actividades 2 y 3

2.1.2.- Según el medio de conexión:

- Medios guiados o redes alámbricas: utilizan cables para conectarse.
 - Cable coaxial (similar al de la TV)
 - Par trenzado (similar al del teléfono)



- Fibra óptica



- Medios no guiados o redes inalámbricas: no utilizan cables para conectarse.
 - Ondas de radio (wifi y bluetooth)
 - Infrarrojos (similar al mando a distancia, requiere visión directa)

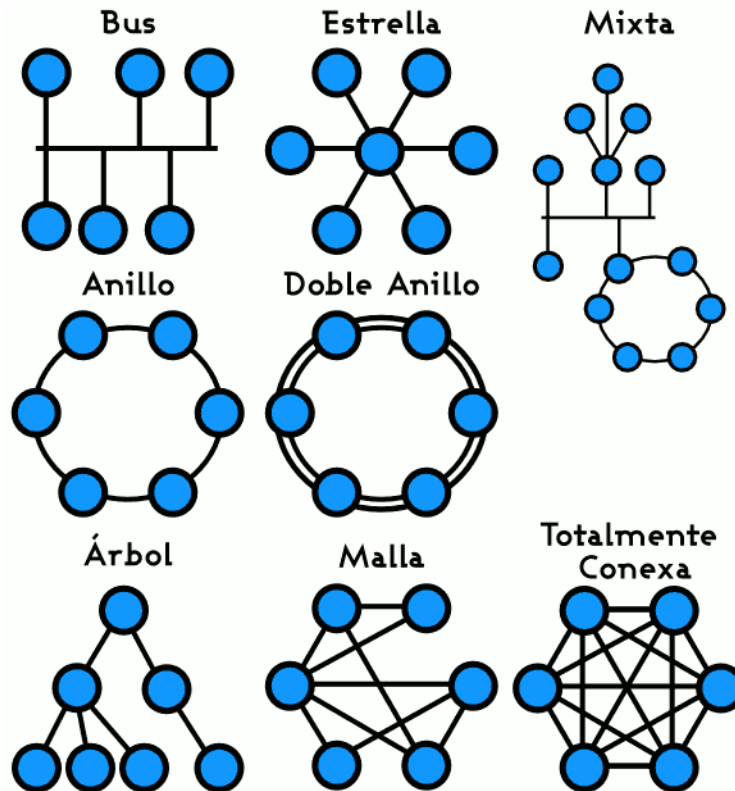
Actividad 4.

2.2.- Topología de Red

Define como están conectadas computadoras, impresoras y otros dispositivos de red.

Describe la disposición de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos.

La topología influye enormemente en el funcionamiento de la red.



Actividad 5.

2.2.1.- Red en Bus

Se caracteriza por tener un único canal de comunicaciones, denominado bus, el cual comparten y al que se conectan los diferentes dispositivos.

Ventajas:

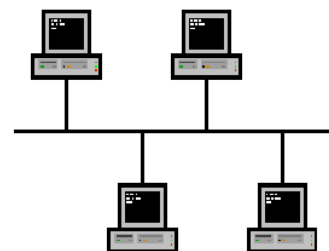
Fácil implementación y crecimiento

Simplicidad

Desventajas:

Un fallo en el bus degrada toda la red

Solo se puede transmitir un mensaje al mismo tiempo. Si hay mucho tráfico, los mensajes colisionan.



2.2.2.- Red en Estrella

Es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

Ventajas

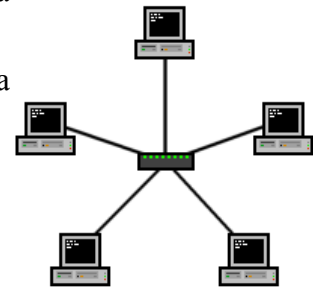
Si un PC se desconecta o se rompe el cable solo ese queda fuera de la red.

Permite que todos los nodos se comuniquen entre sí de manera conveniente.

Desventajas

Si el nodo central falla, toda la red se desconecta.

Es cara, necesita el nodo central y más cable que la red en bus o anillo.

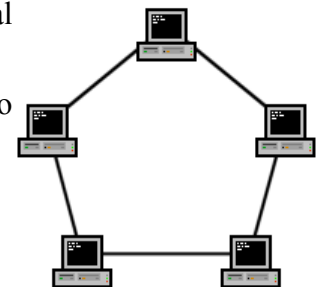


2.2.3.- Red en Anillo

Cada nodo está conectada a la siguiente y la última está conectada a la primera. Cada nodo tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.

La comunicación se hace por el paso de un token o testigo, que es como un cartero que pasa recogiendo y entregando paquetes de información.

Ventajas: Facilidad de implementación y crecimiento.



Desventajas: Si un nodo deja de funcionar, se pierde la comunicación en toda la red.

Una variante es la red en doble anillo.

2.2.4.- Red en árbol

Los nodos están colocados en forma de árbol, es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.

Tiene un nodo de enlace troncal desde el que se ramifican los demás nodos.

Ventajas

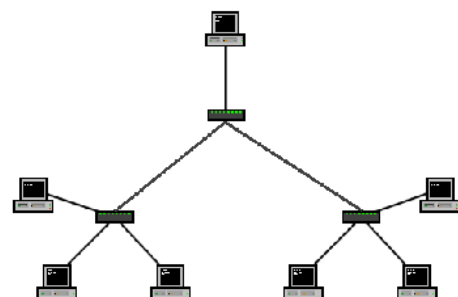
Si falla algún nodo el resto sigue

Podemos priorizar y aislar Pcs

Fácil crecimiento.

Desventajas

Cara, se requiere mucho cable y concentradores



2.2.5.- Red en Malla

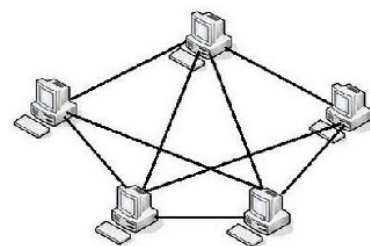
Cada nodo está conectado a varios nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos.

Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones

Ventajas:

Si falla un cable, hay más caminos

Si falla un nodo, el resto continúa.



Desventajas: es carísima.

Actividades 6, 7 y 8

2.3.- Dispositivos de Red

2.3.1.- Cableado

Consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local.

Suele tratarse de cable de par trenzado de cobre, pero también puede ser fibra óptica o cable coaxial.

El Par Trenzado

Esta formado por 4 pares (8 cables).

Utiliza normalmente el conector RJ45.

Actualmente se utilizan las categorías 5 y 6 que permiten velocidades de hasta 1000Mbps

El cable coaxial esta en desuso en las LAN, y la fibra óptica todavía no se ha implantado de forma masiva.

Realizaremos una práctica donde crimparemos un cable.

2.3.2.- Tarjeta de Red

Es un dispositivo que permite a cualquier ordenador conectarse, enviar y recibir información, en un red de ordenadores.

Cada tarjeta de red tiene un número de identificación único de 6 pares de dígitos en hexadecimal llamado **dirección MAC** o **dirección física**.

Ejemplo: 00:1D:7D:00:70:B4

Tipos de Tarjetas de Red

- Alámbricas o Ethernet
- Inalámbricas o Wi-fi

Tarjeta de red Ethernet:

Conector RJ45 (hembra) y par trenzado

Velocidades: 10, 100 y 1000 Mbps

Integradas en placa o de expansión (PCI)

Tarjeta de red Wi-fi:



Conexión inalámbrica o por ondas de radio.

Velocidades: 11, 54 y 108 Mbps

Radio de acción: 50 – 100 m máximo, depende de los obstáculos y las conexiones.

Integradas en placa, de expansión (PCI) y externas (conexión USB)



Actividades 9 y 10

2.3.3.- Dispositivos de Conexión de Red

Equipos electrónicos que utilizamos para conectar ordenadores, impresoras... para formar una red de ordenadores.

Cada tipo de dispositivo tiene distintas funciones y establece una topología de red distinta.

Clasificación de los Dispositivos de Conexión:

- Modem
- Concentrador o Hub
- Conmutador o Switch
- Punto de acceso inalámbrico o Wap.
- Enrutador o Router
- Router ADSL

2.3.3.1.- Modem

(MOdulador-DEModulador) Periférico de entrada/salida, que sirve para a conectar un ordenador a Internet o a otras redes, por medio de la línea telefónica. (en desuso)

Otros tipos de Modem

- Modem RDSI: modem especial que utiliza tecnología telefónica digital (en desuso)
- Modem Cable: modem especial que conecta a Internet aprovechando una red de televisión por cable (coaxial o fibra óptica)
- Modem ADSL: modem especial que conecta a Internet mediante la tecnología ADSL, que explota al máximo las capacidades del cable de pares del telefono.

2.3.3.2.- Concentrador o Hub

Un concentrador o Hub funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos.

Un Hub siempre implementa una red con topología en Bus.

Ventajas: es un dispositivo simple y barato.

Desventajas:

Incrementa el tráfico

Solo puede enviar información un nodo a la vez.

No aporta ninguna seguridad

Aplicaciones: LAN muy pequeñas, con poco tráfico

Actualmente esta en desuso



2.3.3.3.- Conmutador o Switch

Su función es interconectar dos o más nodos pasando datos de acuerdo con la dirección MAC de destino de los paquetes en la red.

Un Switch siempre implemente la red con topología en estrella.

Ventajas:

Solo envían la información a su destinatario.

Aportan más seguridad

Permiten varias conexiones simultáneamente

Aplicaciones: LAN



2.3.3.4.- Punto de Acceso Inalámbrico o WAP

Es un dispositivo que interconecta de forma inalámbrica otros dispositivos para formar una red inalámbrica.

Normalmente un WAP también se conecta a una red cableada (por medio de un hub o un switch), y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Solo permite la conexión inalámbrica a la red.

Establece topología de red en bus.

Desventaja: Se degrada rápidamente con muchos nodos.

Existen dispositivos, switches y routers, que lo llevan incorporado.



2.3.3.5.- Enrutador o Router

Un router es un dispositivo para la interconexión de redes informáticas que permite determinar la ruta que debe tomar el paquete de datos.

Toma las decisiones de enrutado a partir de la dirección IP de destino del paquete.

Implementan excelentes niveles de seguridad, pudiendo filtrar paquetes en función de diversos parámetros.

Habitualmente interconectan Switches, o se conectan con otros routers que forman parte de Internet.

No son adecuados para interconectar Pcs.



2.3.3.6.- Router ADSL

El router ADSL es un dispositivo que permite conectar uno o varios equipos o incluso una LAN a internet por medio de la tecnología ADSL.

Tiene alguna de las funcionalidades de seguridad y filtrado de un router.

En realidad esta formado por varios dispositivos en un solo aparato:

- Modem ADSL que nos da acceso a Internet
- Switch de 4 puertos
- Punto de Acceso Inalámbrico



Actividad 11

2.4.- Protocolos y Servicios

Un protocolo es un conjunto de reglas estandarizadas, usadas por computadoras para comunicarse unas con otras a través de una red.

El funcionamiento de Internet y las redes de computadores se basan en la familia de protocolos TCP/IP.

IP provee un servicio de envío de datos no fiable. Se hará lo mejor que se pueda.

La utilidad de IP es encontrar un camino para los paquetes de datos, el mejor posible, para ello utiliza las direcciones IP y los routers.

TCP garantiza que los datos se entregaran sin errores y ordenados.

Actividad 12

2.4.1.- Dirección IP

Una **dirección IP** es un número que identifica de manera lógica a una tarjeta de red dentro de una red que utilice el protocolo IP. (Es configurable, la establece la red)

No confundir con la dirección MAC que es una dirección física (No configurable, impuesta por el fabricante)

Formato de dirección IP: número de 32 bit que suele ser mostrado en cuatro grupos de números decimales de 8 bits (0-255)

Ejemplo: 10.32.0.168

Actividad 13

Un ordenador queda perfectamente identificado por su dirección Mac y su dirección IP.

Pero, ¿como identificamos una red?

Todos los dispositivos que pertenecen a la misma red, comparten los primeros bits de su dirección IP, estos identifican a la red. Y los bits que cambian, identifican a los distintos ordenadores

Ejemplos:

10.32.7.xxx red de ordenadores de alumnos del IES

192.168.0.xxx red de ordenadores de casa

2.4.2.- Máscara de Subred

La **Máscara de Subred** permite distinguir los bits que identifican a la red, de los que identifican a cada ordenador.

Un ordenador puede saber a partir de la dirección IP de otro, si este pertenece a la misma red que él o a otra distinta.

Formato de la Máscara de Subred: tiene 32 bits al igual que la IP, donde todos los bits que identifican a la red son 1 y todos los que identifican a los ordenadores son 0.

Habitualmente se escribe en decimal, al igual que la IP.

Ejemplos: 255.255.255.0, 255.255.0.0

Actividad 14

Servicio: es un conjunto de actividades que buscan responder a las necesidades de un cliente.

2.4.3.- Servicio de Nombres de Dominio o DNS

Para facilitar el uso de Internet, se asigna a los servidores que la constituyen nombres que son más fáciles de recordar que las direcciones IP.

Este Sistema de Nombres esta estructurado y jerarquizado y se denomina DNS.

El **Servidor DNS** proporciona al computador la dirección IP que corresponde al nombre que le ha dicho el usuario.

Ejemplos: `www.google.es` : 173.194.34.19 `www.manuelquinto.es` : 87.106.195.136 (hacer ping)

Actividad 15.

2.4.4.- Parámetros de Red

Para conectarnos a una Red de Ordenadores necesitamos los siguientes parámetros.

- Dirección IP: para identificar nuestro ordenador dentro de la red.
- Máscara de Subred: para que nuestro ordenador sepa a que red pertenece y quienes la forman.
- Puerta de Enlace Predeterminada: dirección del dispositivo al que mandamos todos los paquetes cuyo destinatario real no pertenece a la misma red que nuestro ordenador.
- Servidor DNS: dirección IP del ordenador que me da el Servicio de Nombres de Dominio.

Actividad 16 y 17

2.4.5.- Configuración Básica de Red

Para conectarnos a una red, debemos tener todos los parámetros que hemos visto.

La primera forma de conseguirlos es **configurarlos de forma manual**. Como hemos visto en clase.

Otra forma de obtenerlos es utilizando DHCP.

DHCP o Protocolo Configuración Dinámica de Servidor, es un protocolo que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente

Actividad 18

2.4.6.- Funcionamiento Básico de una Red

Ordenador conectado y configurado en la red:

IP: 10.33.7.171

Máscara de Subred: 255.255.255.0

Puerta de Enlace: 100.33.7.1

DNS: 10.33.7.1

Queremos conectarnos a `http://es.wikipedia.org`

En primer lugar debemos obtener la dirección IP asociada a ese nombre.

Comprobamos si el servidor DNS esta en nuestra misma red con nuestra IP y nuestra máscara.

Como si que está, le envío un mensaje con el nombre y me devuelve la IP asociada al mismo: 91.198.174.2

Ahora tengo que pedirle al servidor web de wikipedia, cuya IP conozco que me manda la página web.

Compruebo si la IP a la que quiero mandar el mensaje 91.198.174.2 pertenece a mi red 10.33.7.xxx.

Como no pertenece, le envío el mensaje a la puerta de enlace predeterminada 10.33.7.1

La puerta de enlace predeterminada es un router que esta conectado al menos a dos redes, a la nuestra y a otra. Por tanto, tendrá el doble de parámetros, los de nuestra red, y los de la otra.

Operará de la misma forma hasta llegar al servidor web, y en el mensaje de vuelta, se hará también lo mismo.

Actividad 19

2.4.7.- Red inalámbrica

Todo lo que hemos comentado sobre configuración de una red es aplicada si la red es inalámbrica.

La principal diferencia reside en si la red dispone de seguridad o no.

Si la red inalámbrica tiene la seguridad habilitada, debemos conocer la contraseña para poder acceder a ella.

Tipos de Contraseñas: WEP, WPA2

2.4.8.- Bluetooth

Bluetooth es una especificación para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia.

Viene integrado en distintos aparatos electrónicos: móviles, PDA, portátiles... se puede poner en Pcs mediante tarjetas de expansión internas o USB.

Objetivos:

Facilitar las comunicaciones entre equipos móviles y fijos...

Eliminar cables y conectores entre éstos.

Facilitar la sincronización de datos entre equipos personales.

Ventaja de simplificar el descubrimiento y configuración de los dispositivos, ya que éstos pueden indicar a otros los servicios que ofrecen, sin un control explícito de direcciones de red, permisos...

Radio de acción: unos 10 m

3.- Seguridad Informática

Seguridad: estado de cualquier tipo de información (informático o no) que esta libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

La seguridad informática consiste en asegurar que los recursos del sistema de información sean

utilizados de la manera que se decidió y que el acceso y la modificación de la información allí contenida, sólo sea posible a las personas acreditadas y dentro de los límites de su autorización.

La seguridad en la informática es utópica porque no existe un sistema 100% seguro.

Para que un sistema sea seguro debe tener estas cuatro características:

- **Integridad:** La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad:** La información sólo debe ser legible para los autorizados.
- **Disponibilidad:** Debe estar disponible cuando se necesita.
- **Irrefutabilidad (No repudio):** El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Actividad 20

3.1.- *Mitos y Falacias de la Seguridad*

Mi sistema no es importante para un cracker. ¿quien va a querer obtener información mía?

Generalmente los ataques se realizan de forma automática, sin saber a quien.

Estoy protegido pues no abro archivos que no conozco. Pero existen otras formas de contagio: arranque de pendrive, MSN, Internet...

Como tengo antivirus estoy protegido

En general los antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer.

Como dispongo de un firewall no me contagio

Un firewall de protege de conexiones no deseadas, pero y las deseadas... puertos emule, páginas de descargas, MSN...

Tengo un servidor web cuyo S.O. es Unix (Linux) actualizado

No tendrás problemas con de virus, ni de seguridad en el núcleo del sistema, pero y el PHP, Perl y demás Scripts...

3.2.- *¿Contra qué debemos protegernos?*

Contra nosotros mismos

Borramos archivos y programas, o instalamos programas y abrimos correos

Contra accidentes y averías

Subidas de tensión, incendios, inundaciones...

Contra usuarios intrusos

Desde Internet o desde nuestro propio ordenador

Contra Software malicioso o malware

3.3.- *Riesgos y Amenazas*

Malware o software malicioso: es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas.

3.3.1.- *Factores de Riesgo*

- Código sin confirmar: Un código que se puede ejecutar por la irresponsabilidad o ignorancia del usuario.
- Defectos o Bugs: La mayoría de los S.O. contienen errores que se pueden aprovechar por el malware, mientras no se ponga el parche correspondiente.
- Homogeneidad: Cuando todos los PCs de una red usan el mismo S.O.
- Sobre-privilegios del código: La mayoría de los S.O. permiten que el código sea ejecutado por un usuario con todos los derechos.
- Sobre-privilegios del usuario: Algunos S.O. permiten que los usuarios modifiquen sus estructuras internas.

Virus informático: es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

Su objetivo es infectar y propagarse, se camuflan en otros programas.

Los hay que borran archivos, nos desconectan de Internet, apagan el ordenador...

Worm o Gusano: es un malware que tiene la propiedad de duplicarse a sí mismo. No destruyen archivos, simplemente consumen recursos: memoria y ancho de banda...

Troyano: bajo una apariencia inofensiva se ejecuta de manera oculta en el sistema y permite el acceso remoto de un usuario no autorizado al sistema.

Spyware: son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para enviarla a través de Internet.

Dialers: programas que llaman a un n° telefónico de tarifa especial (806), para conectar través del módem, a páginas de juegos, adivinación o pornográficas...

Spam o correo basura: los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades.

Hoax o bulo: noticia falsa, intento de hacer creer a un grupo de personas que algo falso es real, principalmente engaños por medio de email.

Adware: Este software muestra publicidad que aparecen inesperadamente en el equipo.

Pharming permite a un atacante redirigir un nombre de dominio a otra máquina distinta. Con la obtención de obtener datos bancarios...

Phising: el estafador se hace pasar por tu banco y te pide que rellenes tus datos y contraseñas...

Actividad 21

3.4.- *Técnicas de Seguridad*

- Seguridad Activa: intenta evitar los daños

- Contraseñas adecuadas
- Encriptación
- Software de Seguridad: antivirus, antispyware...
- Seguridad Pasiva: intenta minimizar las consecuencias
 - Copias de Seguridad
 - Sistema Ininterrumpido de Alimentación, SAI

Actividad 22

3.4.1.- Contraseñas

Debe ser suficientemente larga, 8 caracteres mínimo

Evitar nombres o números fácilmente averiguables sobre nosotros, nombre de padres, mascotas, nº de DNI, matrícula de coche o moto...

Evitar palabras que se puedan encontrar en un diccionario en español o inglés.

Evitar contraseñas obvias como repetir el nombre de usuario, o las combinaciones de teclas evidentes como qwerty o asdfg y similares.

Debe incluir letras en mayúsculas y minúsculas alternadas: PasSwoRd

Debe incluir números y no solo al principio o al final. La O y el 0, la i y el 1.

Debe incluir caracteres especiales como por ejemplo: !@\$&€”%. sustituir a por @, e por €

Comprueba tu contraseña

Actividad 23

3.4.2.- Encriptación o Criptografía

"escritura oculta". son las técnicas utilizadas para cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Clasificación.

- Sistema de Clave Privada o Simétrico
- Sistema de Clave Pública o Asimétrico

3.4.2.1.- Sistema de Clave Privada

Se usa una misma clave para cifrar y descifrar mensajes.

Una vez ambas partes tienen la clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

Toda la seguridad está en clave utilizada. El algoritmo es conocido.

El principal problema está en el intercambio de claves.

3.4.2.2.- Sistema de Clave Pública

Usa un par de claves para el envío de mensajes. Las dos pertenecen a la persona que envía el mensaje.

Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

Si el remitente usa la clave pública para cifrar el mensaje, sólo la clave privada del destinatario podrá descifrar este mensaje, Se logra confidencialidad del envío del mensaje.

Si el emisor usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. Se consigue la identificación y autenticación del remitente. Esta idea es el fundamento de la firma electrónica.

Actividad 24.

3.4.3.- Software de Seguridad

Antivirus: programas que detectan, bloquean, desinfectan y previenen una infección de virus informático.

Actualmente son capaces de reconocer otros tipos de malware, como spyware, troyanos, etc.

Habitualmente quedan residentes en memoria, y escanean constantemente los archivos, las conexiones...

El consumo de recursos suele ralentizar el ordenador en mayor o menor medida.

Firewall o Cortafuegos: es una parte de un sistema o una red diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre Internet y nuestra red.

Existen Firewall software, hardware y combinados.

Actividad 25

AntiSpyware: es un software que se encarga de buscar, detectar y eliminar spywares o espías en el sistema.

Existen aplicaciones independientes o como módulos o herramientas incorporadas dentro de otra aplicación mayor, como un antivirus.

AntiSpam: programas que detectan el correo basura desde nuestro ordenador o desde el servidor.

3.5.- Identidad Digital.

Identidad 2.0 o identidad digital, es la verificación de la identidad en línea utilizando tecnologías tales como el standard OpenID.

Se pretende la identificación en transacciones cuyo proceso es similar al mundo real, como por ejemplo una licencia de conducir de un modo simple y abierto.

3.5.1.- Certificado Digital

Un certificado digital (también conocido como certificado de clave pública o certificado de

identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad (por ejemplo: nombre, dirección y otros aspectos de identificación) y una clave pública.

3.5.2.- Firma Digital

Se dice firma digital a un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico.

Una firma digital da al destinatario seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión.

Consiste en un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.