Unidad 3: Seguridad Informática

Seguridad física:

Se entiende como el conjunto de medidas y protocolos para controlar el acceso físico a un elemento. Aplicado a la seguridad informática lo constituyen las medidas para evitar que personas no autorizadas puedan alcanzar una terminal o dispositivo concreto.

Seguridad lógica:

Son los diferentes protocolos, algoritmos y programas que pueden manipulan directamente la información controlando el acceso a la misma desde terceras partes. Las contraseñas, cifrados y códigos son parte de la seguridad lógica.

Seguridad humana: Es la que reside en el propio usuario que maneja la información. Es la responsabilidad que éste toma sobre la información y las medidas y protocolos de conducta que lleva a cabo para gestionarla adecuadamente. La elección de contraseñas seguras, no divulgación de claves y el uso de herramientas de seguridad son seguridad humana.

Protección de datos mediante cifrado

LA CRIPTOGRAFÍA:

El cifrado de mensajes es sin duda uno de los sistemas más antiguos para proteger las comunicaciones. Diferentes sistemas de codificación, han ido evolucionando a lo largo de la historia, pero ha sido con la aplicación de máquinas y ordenadores a la criptografía cuando los algoritmos han conseguido verdadera complejidad.

Cifrado simétrico: Utiliza la misma clave para cifrar y descifrar. La clave es compartida por el emisor y por el receptor del mensaje, usándola el primero para codificar el mensaje y el segundo para descodificarlo.

Cifrado asimétrico: Utiliza dos claves distintas, una para cifrar y otra para descifrar. La clave para cifrar es compartida y pública, la clave para descifrar es secreta y privada. El emisor utiliza la clave pública del receptor para cifrar el mensaje y, al recibirlo, el receptor utiliza su propia clave privada para descifrarlo. Este tipo de criptografía es también llamada de clave pública.

FUNCIONES HASH:

Son funciones, llamadas de reducción criptográfica, que tienen carácter irreversible. Estas funciones operan sobre los datos obteniendo de ellos una clave que los representa de manera casi unívoca. La propiedad fundamental de estos algoritmos es que si dos claves hash son diferentes, significa que los datos que generaron dichas claves son diferentes.

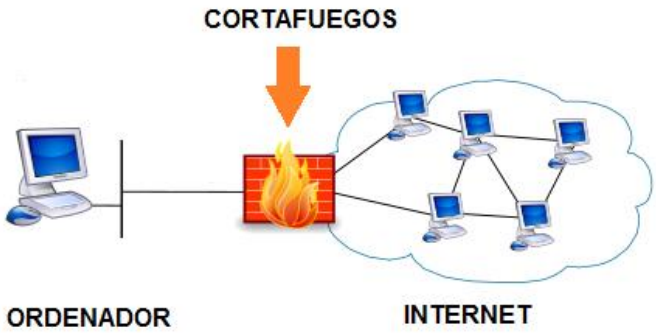
ESTEGANOGRAFÍA:

Es un conjunto de métodos y técnicas para ocultar mensajes u objetos dentro de otros, de modo que no se perciba la existencia de los primeros. Un mensaje oculto formado por la primera letra de cada frase de un texto es una forma de esteganografía. Existen programas capaces de introducir datos en imágenes o archivos de música aprovechando las limitaciones de los sentidos humanos, bien en forma de frecuencias inaudibles en un archivo de audio o pequeñas «imperfecciones» en una imagen.

Protección de las comunicaciones

LOS CORTAFUEGOS:

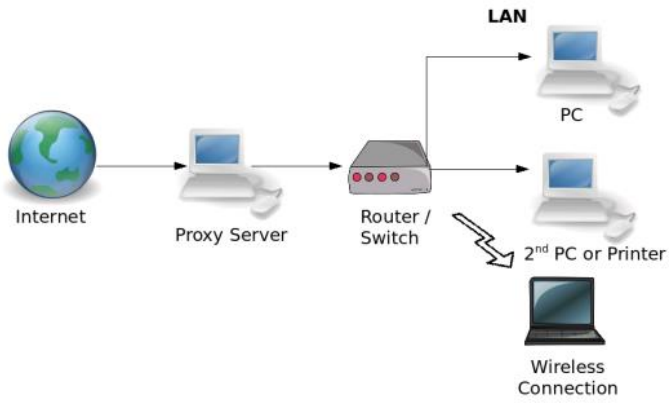
Un cortafuegos o firewall es un elemento encargado de controlar y filtrar las conexiones a red de una máquina o conjunto de máquinas. Se trata de un mecanismo básico de prevención contra amenazas de intrusión externa. Supone la barrera de protección entre un equipo o red privada y el mundo exterior. Controla el acceso de entrada y salida al exterior, filtra las comunicaciones, registra los eventos y genera alarmas.



LOS SERVIDORES PROXY

Es un ordenador que hace de intermediario entre un cliente y un destino. Cuando un cliente desea una información, conecta con el servidor proxy en lugar de hacerlo con el servidor de destino.
El servidor proxy contacta con el servidor de destino como si fuese el propio cliente y, una vez obtenida la información se la envía al ordenador que inició la petición.

En una red local un servidor proxy puede dar este servicio a todos los ordenadores, de forma que las comunicaciones no se realizan con el exterior sino únicamente con el servidor proxy. Por otro lado, este servidor es el único que accede e intercambia datos con la red externa.



Seguridad de la red Wi-Fi

Cuando la información viaja por ondas de radio, éstas son accesibles para cualquier receptor que se encuentre dentro del área que abarcan, esté autorizado o no.
Con la proliferación de este tipo de redes es bastante frecuente encontrar que un mismo terminal recibe señales de diversas redes colindantes. Es importante entonces proteger las comunicaciones Wi-Fi de posibles intrusos.
Existe un doble motivo para ello. En primer lugar, para asegurar la confidencialidad de las comunicaciones de una red. En segundo, para evitar que un intruso pueda utilizar la red para llevar a cabo acciones ilegales que acabarán siendo imputadas al dueño de la misma.
Para proteger redes Wi-Fi se usan diversos protocolos de seguridad los más habituales son: WEP, WPA y WPA2, siempre que se pueda se ha de utilizar éste último puesto que es el más seguro.

Navegación segura: protocolo https
Este protocolo de comunicación web cifrado es una versión segura del protocolo http de web, y es común en las comunicaciones con entidades bancarias, tiendas en línea y servicios privados. Cuando se accede a una página que requiere este protocolo el navegador del cliente y el servidor se ponen de acuerdo en realizar una comunicación cifrada. Es frecuente que algunos navegadores indiquen el acceso a este servicio utilizando un icono en forma de candado.

Navegación segura: certificado digital

Un certificado digital (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual 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. Uno de los elementos que se pueden utilizar como certificado digital es el DNI electrónico.

MALWARE

Se denomina malware al programa cuya finalidad es infiltrarse o dañar un ordenador sin el conocimiento del dueño. Son programas «disfrazados» con el objetivo de engañar al usuario. Los virus informáticos son el tipo más común de malware, por lo que es habitual ese nombre para denominar a todos los tipos de programas hostiles. Cuando surgieron los virus estos eran una demostración de la habilidad de sus programadores, posteriormente el malware producía efectos muy visibles en los equipos (apagar el ordenador, cambiar caracteres, borrar archivos...).

Hoy en día el malware se produce para:
● Robar información como datos personales, contraseñas, números de cuenta.
● Crear red de ordenadores zombies o botnet para utilizarlos para el envío masivo de spam, phishing o realización de ataques de denegación de servicio.
● Vender falsas soluciones de seguridad para solucionar el problema. Por ejemplo nos dicen que tenemos un virus y que hay que pagar una cantidad para conseguir el programa para eliminarlo.
● No dejar arrancar el equipo o cifrar el contenido de determinados archivos y solicitar el pago de una cantidad para solucionarlo.

Virus

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus actúan cuando se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado con lo cual el proceso de replicado se completa.

Gusanos

Son muy parecidos a los virus pero la gran diferencia es que se propagan solos, sin la necesidad de ser ejecutados por un ser humano. Esto hace que los gusanos sean muy peligrosos ya que tienen la capacidad de replicarse en el sistema. El daño que puede causar un gusano es que consume mucha memoria del sistema, logrando que los servidores y ordenadores no respondan.

Troyanos
Son programas que disfrazan y esconden una función no deseada en un programa aparentemente inofensivo.
● Puertas traseras o backdoors. Modifican el sistema para permitir una puerta oculta de acceso al mismo.
● Keyloggers. Almacenan, de forma que no pueda advertirlo el usuario, todas las pulsaciones de teclado que éste efectúa.
● Software espía o spyware. Una vez instalado envía al exterior información proveniente del ordenador del usuario de forma automática.
● Adware. Son programas de publicidad que muestran anuncios, generalmente mediante ventanas emergentes o páginas del navegador.

Sistemas de protección contra virus y troyanos

Antivirus

Son programas diseñados para detectar y eliminar el software dañino. Tienen dos mecanismos básicos de detección de amenazas:

1º Comparación: buscando entre los programas el patrón de código que coincida con los almacenados en una biblioteca de patrones de virus conocidos.
2º Detección: de programas hostiles basados en el comportamiento. El antivirus conoce una serie de comportamientos sospechosos y estudia a los programas que, por su código, estén preparados para llevarlos a cabo.

Antispyware

Aunque hoy en día los antivirus tratan de ampliar su protección hacia cualquier tipo de malware, en ocasiones es necesario utilizar programas específicos para detectar el spyware, que complementan la actividad del antivirus.

Propagación del malware

Las forma en que llegan a los equipos son:

Explotando una vulnerabilidad o fallo de seguridad, bien del sistema operativo o de algún programa que tengamos instalado. Para evitar este problema conviene tener siempre actualizado el sistema operativo y los programas porque periódicamente las empresas fabricantes sacan actualizaciones de seguridad para solventar los fallos detectados.

Mediante Ingeniería social. Es decir convenciendo al usuario de que realice determinada acción como instalar algún programa o drivers creyendo que se instala un elemento necesario, o accediendo a una web con contenido malicioso.
Por un archivo malicioso que puede llegar como adjunto de un mensaje de correo, a través de una red P2P o de un archivo que se descargue de Internet o una carpeta compartida. Para prevenir es mejor analizar con un antivirus todo archivo descargado de Internet y de procedencia dudosa. Al utilizar dispositivos extraíbles como memorias USB. Simplemente por conectar una memoria USB se puede infectar un equipo. Para evitarlo se pueden utilizar antimalware específico para memorias USB o deshabilitar el autoarranque de estos dispositivos.

PROTECCIÓN PARA UNA NAVEGACIÓN SEGURA

La mejor manera de protegerse es ser consciente de la existencia de peligros y hacer un uso de la red y del software que minimice el riesgo. La prudencia es la principal herramienta y se ha de extremar la cautela para evitar tener problemas de seguridad. El usuario es a veces el eslabón más débil en la seguridad informática.

Protección de contraseñas y datos personales

Como regla de oro, debemos evitar dar nuestros datos personales en Internet, salvo en aquellas páginas en las que tengamos plena confianza. Por supuesto, esto incluye cualquier información personal, familiar, financiera o de costumbres. Absolutamente ningún banco nos va a pedir nunca nuestro número de cuenta, DNI o tarjeta por Internet ni por correo electrónico, por lo que NUNCA debemos facilitar estos datos si supuestamente nuestro banco nos los pide. Además, si las claves de acceso son ellos los que nos las generan y facilitan... ¿qué sentido tiene que luego nos las pidan vía

E-Mail?
Una medida muy interesante si vamos a realizar compras por Internet es la de abrir una cuenta con su correspondiente tarjeta exclusivamente para este fin. No debemos guardar nuestras claves y contraseñas en el ordenador, y tampoco habilitar la opción de que algunos programas y
páginas Web recuerden estas contraseñas. Si hacemos esto la utilidad de la contraseña se pierde completamente. Otro punto de gran importancia es el tipo de claves que solemos utilizar. Una clave, para ser medianamente segura tiene que constar al menos de 8 dígitos alfanuméricos, a ser posible mezclados números y letras, y si el programa nos lo permite, mezclar mayúsculas y minúsculas, y por supuesto sin tener ninguna relación con nosotros. La mayoría de los programas

para romper claves se basan en una serie da algoritmos preestablecidos sobre las combinaciones más habituales a estudiar y mediante el método de la fuerza bruta. Es decir, que a partir de un dato conocido (y a algunos se les pueden introducir más de uno), empieza a generar una serie de combinaciones y a ejecutar combinaciones que guarda en una base de datos. Estas combinaciones están basadas en los criterios más usuales utilizados en las claves.
Hay que tener también cuidado con las habituales preguntas para recordar la contraseña. Cualquier persona que nos conozca mínimamente puede acceder a estos datos en cuestión de minutos.

Protección de privacidad

Los ordenadores almacenan la información, aunque nosotros no queramos. Guardan las páginas web que hemos visitado, los archivos que hemos descargado, las búsquedas que hemos hecho en Google, datos que hemos rellenado en un formulario.

Algunos de los sitios donde se guarda esta información son:

Historial del navegador.

Aquí se guardan las páginas web que hemos visitados. Si queremos evitar que alguien sepa que páginas hemos visitado podemos borrar el historial
o utilizar la navegación privada.

Cookies.

Es una especie de contenedor de datos que los sitios webs y el navegador que estamos empleando utilizan con el propósito de almacenar información de nuestra interacción con las webs que visitamos, con el fin de utilizarlos para diversos cometidos, el principal de ellos, recordar preferencias y configuraciones. Por ejemplo se pueden mantener listas de compras o productos elegidos en sitios webs de comercio electrónico,
personalizar para adaptar a nuestras necesidades sitios webs personales o de noticias, entre muchos otros beneficios muy importantes para la navegación. El problema es que con las cookies se tiene la capacidad de realizar seguimientos de los movimientos que realiza el usuario dentro de un sitio, lo cual puede ser recopilado y usado con fines ajenos a su propósito original.

Archivos descargados, imágenes y webs se guardan en una carpeta de archivos temporales de Internet.

Protección frente a descargas y programas maliciosos

No todos los archivos que se reciben por correo o se descargan gratuitos de la red están limpios de amenazas. Es importante comprobar y pensar antes de ejecutar. Debemos utilizar un programa antivirus y mantenerlo actualizado. Igualmente debemos desconfiar de las clásicas barras de ayuda y navegación (las conocidas toolbar). Cierto que algunas son de una gran utilidad y confianza (como es el caso de MSN toolbar o de Google toolbar, por poner algún ejemplo), pero también hay muchas que ya no lo son tanto, y cuya única finalidad real es la de enviar a terceros información sobre nuestro sistema y hábitos de navegación. Es muy habitual que se
instalen al instalar otros programas. Los programas de intercambio (los conocidos programas P2P) también puede ser otra vía de propagación de malware, sobre todo de troyanos.