SEGURIDAD INFORMATICA

Seguridad informática Seguridad en Internet: malware, virus y crackers. El correo masivo y la protección frente a tipos de malware. Medidas de seguridad en software y hardware.

Cortafuegos. Programas espía. Cookies. Apropiación indebida de claves. Valoración de la importancia de la adopción de medidas de seguridad activa y pasiva. Redes sociales y seguridad ¿Qué entendemos por seguridad informática? ¿Qué implica esta seguridad? Seguridad Informática entendemos por seguridad informática el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, confidencialidad y disponibilidad.

Un sistema es íntegro si impide la modificación de la información a cualquier usuario no autorizado.

Un sistema es confidencial si impide el acceso a datos a usuarios no autorizados.

Un sistema es disponible si permite el acceso a usuarios autorizados cuando estos lo necesitan.

¿Contra qué nos debemos proteger? ¿Contra qué nos debemos proteger? Contra nosotros mismos: Que muchas veces borramos archivos sin darnos cuenta, eliminamos programas necesarios para la seguridad, aceptamos correos electrónicos perjudiciales para el sistema...Contra los accidentes y averías: Que pueden hacer que se estropee el ordenador y perdamos datos necesarios Contra los usuarios intrusos: Que bien desde el mismo ordenador o desde otro en la red pueden intentar acceder a nuestros datos Contra software malicioso (malware):Programas que aprovechan un acceso a nuestro ordenador para instalarse y obtener información, dañar el sistema o incluso llegar a inutilizarlo por completo23-Síntomas de ataque de un virus

Síntomas de ataque-El ordenador trabaja con una ralentización exagerada de los procesos o de la conexión a la red-Disminuye el espacio disponible en disco (salen avisos de que no hay espacio suficiente en éste)-Aparecen programas desconocidos, se abren páginas de inicio nuevas en el navegador o se añaden elementos que no se pueden eliminar-Aparecen iconos desconocidos en el escritorio (a veces no se pueden eliminar)-El teclado o el ratón hacen cosas extrañas34-LAS AMENAZAS SILENCIOSAS. Busca información sobre las siguientes amenazas que pueden afectarnos)Espía (Spyware)

b)Dialers

c)Spam

d)Adware (Advertisement Software)

e) Virus informático

f)Gusano informático

g)Troyano

h)Pharming

i)Spoofing (suplantación de identidad)

j)Phishing

k)Keylogger

l)Hijackers (secuestradores)

Las amenazas silenciosas...(II)Espía (Spyware)Se instala en el ordenador sin conocimiento del usuario y su finalidad es recopilar información para enviarla a servidores de Internet que son gestionados por compañías de publicidad. La información recopilada suele ser utilizada para enviarnos spam. Ralentizan mucho la conexión a la red. Dialers Eran programas que utilizaban el módem telefónico para realizar llamadas de alto coste (803, 806, 807...) Spam Se llama "correo basura"a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. Adware (AdvertisementSoftware) Hay programas (freewarey shareware) que muestran publicidad tras ser instalados como medio para financiarse. El problema puede surgirse estos programas actúan como spyware.

Las amenazas silenciosas...Virus informático Es un programa que se instala en el ordenador, sin conocimiento de su usuario y cuya finalidad es propagarse a otros equipos y ejecutar las acciones para la que fueron diseñados (pequeñas bromas, ralentización o apagado del sistema, destrucción total de información...) Gusano informático Es un tipo de virus cuya finalidad es multiplicarse e infectar todos los nodos de una red. Aunque no suelen implicar la destrucción de archivos, sí ralentizan el funcionamiento de las máquinas y de la red. Suelen propagarse por correo electrónico. Troyano Es un pequeño programa escondido en otros programas, fondos de pantalla, imágenes, etc.

cuya finalidad no es destruir información, sino disponer de una puerta de entrada para que otro usuario o aplicación recopile información de nuestra máquina o incluso tome control de la misma remotamente. 4 Las amenazas silenciosas...(III) Pharming Consiste en la redirección un nombre de dominio a un servidor distinto del auténtico. Esto se logra mediante la modificación de la entrada en un servidor DNS o mediante la modificación del fichero hosts local. Spoofing (suplantación de identidad) Por ejemplo la suplantación de páginas web por parte de un servidor local que está instalado en el equipo sin que el usuario lo sepa. También existe el mail spoofing, suplantando al remitente. Phishing Práctica delictiva que consiste en obtener información confidencial de forma fraudulenta. Aunque hay varias técnicas (URLs falsas, correos electrónicos con enlaces a páginas perniciosas) el XSS (Cross-SiteScripting) es bastante común. Keylogger Software que se encarga de almacenar pulsaciones de teclado. Hijackers(secuestradores)Programas que modifican el comportamiento o la configuración de otros programas (por ejemplo, en navegadores, modificando el motor de búsqueda)

¿Qué son Hackers? Expertos informáticos que, en principio, sólo se plantean retos intelectuales. No tienen por qué pretender causar daños; de hecho, hay empresas de hacking ético (white hacking) que ayudan a otras empresas a protegerse de ataques de hackers maliciosos o piratas informáticos (black hackers).

¿Qué son Crackers? Personas que se dedican a cambiar el funcionamiento de un programa comercial o bien a realizar aplicaciones que obtengan números de serie válidos para usarlos sin licencia.7-¿Qué son Cookies Son archivos de texto plano que se almacenan en el ordenador a través del navegador cuando visitamos ciertas páginas. Guardan información variada, para que en visitas posteriores, no tengamos necesidad de repetirla.

¿Qué son Hoaxes? Son cadenas de correo electrónico con bulos (noticias falsas) cuyo objetivo es captar direcciones de correo electrónico que posteriormente se pueden usar para spam, distribución de malware, phishing...

¿Qué son los antivirus? ¿Cómo funcionan? El antivirus Un programa antivirus es un programa cuya finalidad es detectar, impedir la ejecución y eliminar software malicioso. Cuando un antivirus analiza un archivo, compara éste con su base de datos de archivos maliciosos, también llamados firmas. También existen sistemas heurísticos que son capaces de detectar virus, aunque no existan firmas para ellos. Suelen funcionar comparando código "sospechoso"810-Describe los distintos niveles de protección de un antivirus: Nivel residente Nivel de análisis Los antivirus tienen distintos niveles de protección Nivel residente: analiza continuamente los programas que se están ejecutando en la memoria, los correos entrantes y salientes, las páginas web, etc. Consume recursos de nuestro ordenador y puede ralentizar Nivel de análisis: todos los archivos del disco duro, del sector de arranque, de discos externos... estos análisis se pueden (y deben) realizar periódicamente ¿Qué función tienen un programa cortafuegos o firewall? Cortafuegos (firewall)Un programa cortafuegos permite o prohíbe la comunicación entre las aplicaciones de nuestro equipo y la red, así como evitar ataques intrusos desde otros equipos al nuestro. Para permitir o prohibir el tráfico de información se han de establecer una serie de reglas en el firewall. Si hay algún intento de infracción de alguna de ellas, el programa nos avisará. 10

12-Qué función tiene un software anti spam? Software anti spam Son programas basados en filtros capaces de detectar el correo basura, tanto de entrada como de salida. Actualmente la mayoría de los antivirus tienen integrado un filtro anti spam. ¿Qué función tiene un software anti espía? Software anti espía Son programas similares a los antivirus, pero las bases de datos para comparar, en lugar de firmas de virus, tienen programas espías. Este tipo de programa es compatible con el antivirus y es aconsejable tener ambos instalados y ejecutándose de forma residente.1214-Medidas de prevención en nuestro ordenador Medidas de prevención-Realizar periódicamente copias de seguridad (back-ups) del sistema que permitan restaurarlo si es necesario-Tener instalados y actualizados antivirus y anti espías Tener actualizado el Sistema Operativo-Revisar sistemáticamente los dispositivos de almacenamiento externo que se conecten al equipo-Extremar el cuidado con los archivos descargados de internet o mediante programas P2P-Tener bien configurado el software cortafuegos-Prestar atención a las descargas gratuitas13

15-Qué amenazas atentan contra la persona y su identidad? Amenazas a la persona o su identidad Todos somos vulnerables y nuestra vulnerabilidad aumenta cuanto más nos exponemos. Entre los peligros que pueden amenazarnos están: El acceso involuntario a información ilegal o perjudicial-La suplantación de identidad, robos y estafas. Pérdida de intimidad o perjuicio a nuestra imagen-Ciber bullying o ciber acoso consistente en amenazas, chantajes, etc. utilizando, principalmente, plataformas sociales. ¿Qué peligros conlleva el uso de webcam?¡Cuidado con la webcam!

1.-Permite que te vean, pero tú no ves a quién te ve

2.-Pueden grabarte sin que lo sepas

3.-Muestra información relevante sobre ti y el lugar en el que te encuentras

4.-Puede ser activada sin que tú te des cuenta

Existen software para proteger a las personas: ¿puedes nombrar y explicar algunos de ellos? Software para proteger a la persona Existen programas que facilitan el control parental del uso de internet. Pueden limitar las búsquedas, permitir o bloquear sitios web, controlar los programas de mensajería instantánea, establecer filtros según la edad del menor, etc.