**Investigue sobre las diferentes clases de virus informáticos, sus comportamientos. Como detectarlos y protección contra virus.**

**VIRUS INFORMÁTICO**

Son aquellos programas que son creados con el fin de dañar computadoras se los conoce bajo el nombre de virus. Estos pequeños programas actúan sin el consentimiento ni conocimiento de los usuarios y lo que hacen es modificar el funcionamiento de las máquinas, borrar información o arruinarla, consumir memoria, entre otras acciones entre ellos tenemos.

**WORM O GUSANO INFORMÁTICO**

Es un malware que reside en la memoria de la computadora y se caracteriza por duplicarse en ella, sin la asistencia de un usuario. Consumen banda ancha o memoria del sistema en gran medida.

El worm informático es un pequeño programa dañino para el sistema y la base de datos en la transmisión de red. Tiene la capacidad de reproducirse para que sea más resistente ante la limpieza del sistema o antivirus.

Es por eso que este tipo de malware es considerado como un código verídico maligno. Inicialmente estos gusanos no llegaban a afectar gravemente el sistema operativo, ya que su primera función es tratar de multiplicarse para luego ocasionar algún daño en los datos de red.

Estos gusanos informáticos utilizan los correos electrónicos, programas tipo P2P, IRC o SMTP para propagarse. Una vez instalados en el sistema se auto envían a todos los contactos de la víctima, haciéndose pasar por mensajes importantes con archivos anexados para descargar.

Para su total eliminación requiere de programas antivirus que realicen una eficaz limpieza del sistema de forma parcial o total entre ellos tenemos el AVG Y AVAST que se encuentran de forma gratuita.



**CABALLO DE TROYA**

Este virus se esconde en un programa legítimo que, al ejecutarlo, comienza a dañar la computadora. Afecta a la seguridad de la PC, dejándola indefensa y también capta datos que envía a otros sitios, como por ejemplo contraseñas.

Generalmente los Caballos de Troya son utilizados para robar información, en casos extremos, obtener el control remoto de la computadora, de forma que el atacante consiga acceso de lectura y escritura a los archivos y datos privados almacenados, visualizaciones de las pantallas abiertas, activación y desactivación de procesos, control de los dispositivos y la conexión a determinados sitios de Internet desde la computadora afectada como los pornográficos.

Las computadoras infectadas se convierten en estaciones de trabajo remotas con todas o la mayoría de sus prestaciones favorables para el atacante. En algunas ocasiones limitan su uso a robar las claves de acceso a servicios como el Chat (IRC), FTP, Web (HTTP), correo o registrar los caracteres tecleados con el fin de encontrar posibles palabras claves, las cuales podrán ser posteriormente utilizadas en acciones fraudulentas.

Entre otras de las acciones está, utilizar las computadoras afectadas para lanzar ataques de negación de servicios a sus víctimas, las cuales son habitualmente servidores de Internet o de correo. Las trazas que dejan estos ataques llevan a las computadoras desde donde fueron lanzados, por lo que sus utilizadores pueden ser inculpados de delitos no cometidos. También, existen algunos códigos diseñados para desactivar antivirus y cortafuegos (firewalls), de manera que las computadoras afectadas resultan más sensibles a nuevos ataques.

Su procedimiento tiene como origen la inserción de un código no autorizado que realiza acciones no deseadas y desconocidas.

Existen medidas de protección que sin tener amplios conocimientos técnicos pueden ser aplicadas para protegernos de estos tipos de virus y de los programas malignos en general, tales como:

No ejecutar programas de origen desconocido, independientemente de las vías por las cuales los recibamos, aun cuando aparenten ser de fuentes conocidas. En caso de extrema necesidad, previa comprobación del envío por parte del emisor puede someterse a cuarentena auxiliándonos de antivirus y programas identificadores actualizados.

No enviar anexos, ni transferir archivos si no son solicitados y en este último caso, revisar antes de enviarlos.

Descargar aplicaciones desde sitios seguros

Mantener los sistemas actualizados, de ser posible con la última versión oficial de las aplicaciones que se utilizan, sobre todo las que se usan para acceder a los servicios de Internet, correo electrónico, mensajería instantánea y conversaciones en tiempo real, entre otros.

Comprobar la existencia de parches que solucionen vulnerabilidades en el Sistema Operativo.

Auxiliarse de herramientas que permiten comprobar las vulnerabilidades, e instalación de los parches correspondientes.

Utilizar aplicaciones y comandos del Sistema Operativo que permitan conocer el uso de los puertos.

Tener instalada y activa una aplicación cortafuegos (firewall), así como antivirus y programas identificadores de virus actualizados.



<http://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)>

**BOMBAS LÓGICAS O DE TIEMPO**

Se activan tras un hecho puntual, como por ejemplo con la combinación de ciertas teclas o bien en una fecha específica. Si este hecho no se da, el virus permanecerá oculto.

Una bomba lógica es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones pre programadas, en ese momento se ejecuta una acción maliciosa. Por ejemplo, un programador puede ocultar una pieza de código que comience a borrar archivos cuando sea despedido de la compañía (en un disparador de base de datos (trigger) que se dispare al cambiar la condición de trabajador activo del programador).

El software que es inherentemente malicioso, como virus o gusanos informáticos.

<http://es.wikipedia.org/wiki/Bomba_l%C3%B3gica>

**HOAX**

Carecen de la posibilidad de reproducirse por sí mismos y no son verdaderos virus. Son mensajes cuyo contenido no es cierto y que incentivan a los usuarios a que los reenvíen a sus contactos. El objetivo de estos falsos virus es que se sobrecargue el flujo de información mediante el e-mail y las redes. Aquellos e-mails que hablan sobre la existencia de nuevos virus o la desaparición de alguna persona suelen pertenecer a este tipo de mensajes.

**DE ENLACE**

Estos virus cambian las direcciones con las que se accede a los archivos de la computadora por aquella en la que residen. Lo que ocasionan es la imposibilidad de ubicar los archivos almacenados.

**DE SOBRE ESCRITURA**

Esta clase de virus genera la pérdida del contenido de los archivos a los que ataca. Esto lo logra sobrescribiendo su interior.

**RESIDENTE**

Este virus permanece en la memoria y desde allí esperan a que el usuario ejecute algún archivo o programa para poder infectarlo.

**DE FORMA GENERAL PARA LA DETECCIÓN O ELIMINACIÓN DE VIRUS INFORMÁTICO HAY QUE SEGUIR UNA SECUENCIA DE PROCEDIMIENTOS.**

* No instale en su computador un software Antivirus confiable (ver lista de opciones en la siguiente sección).
* Actualice con frecuencia su software Antivirus (mínimo dos veces al mes).
* Analice con un software Antivirus actualizado, cualquier correo electrónico antes de abrirlo, así conozca usted al remitente.
* Analice siempre con un software Antivirus los archivos en disquete o CD-ROM antes de abrirlos o copiarlos a su computador.
* No descargue, ni mucho menos ejecute, archivos adjuntos (attachement) a un mensaje de correo electrónico sin antes verificar con la persona que supuestamente envió el mensaje, si efectivamente lo hizo.
* No ejecute nunca un programa de procedencia desconocida, aun cuando el software Antivirus indique que no está infectado. Dicho programa puede contener un troyano [3] o un sniffer [4] que reenvíe a otra persona su clave de acceso u otra información.
* Instale los parches [5] de actualización de software que publican las compañías fabricantes para solucionar vulnerabilidades de sus programas. De esta manera se puede hacer frente a los efectos que puede provocar la ejecución de archivos con códigos maliciosos.
* Tenga cuidado con los mensajes alusivos a situaciones eróticas (versión erótica del cuento de Blancanieves y los Siete Enanitos, fotos de mujeres desnudas, fotos de artistas o deportistas famosos, etc.).
* Nunca abra archivos adjuntos a un mensaje de correo electrónico cuya extensión [6] sea “.exe”, “.vbs”, “.pif”, “.bat” o “.bak”.

**Relacione y describa los diferentes programas que permiten reunir las características técnicas de un computador.**

**SISOFT SANDRA**

Al igual que sus predecesores, la nueva versión de Sisoft Sandra nos permite obtener el rendimiento de varios dispositivos de nuestro ordenador como puede ser el procesador, la memoria o los discos duros, y compararlo con el obtenido por otros equipos.

Es capaz de mostrar información de: CPU, BIOS, administración avanzada de la energía, buses PCI y AGP, vídeo, memoria (Windows y DOS), unidades, puertos, teclado, ratón, tarjeta de sonido, impresora, dispositivos MCI, procesos, módulos OLE, volcados a CMOS.

**PC WIZARD 2010**

Completísima utilidad gratuita para analizar a fondo tu PC. PC Wizard es un excelente programa para conocer a fondo las características del PC



**EVEREST**

Es una completísima herramienta que, en unos pocos segundos, realiza un extenso y detallado análisis de tu PC, mostrando prácticamente todos los aspectos del sistema referentes a hardware, software, configuración de red y más.

El programa ofrece toda la información obtenida en su análisis en estructura de árbol. En ésta se clasifican los distintos elementos evaluados por Everest, que no sólo muestra información sobre los elementos del PC sino que además, si es posible, facilita enlaces a la web del fabricante para mayor información y/o descarga de controladores.



**CPU-Z**

Muestra detallada información acerca del nombre del procesador (velocidad tecnología –en micras-, familia, multiplicador, FSB, velocidad del BUS, etc.), información de caché de primer y segundo nivel, fabricante, modelo, chipset, BIOS, velocidad y memoria del bus AGP, tipo y cantidad de memoria RAM instalada así como el fabricante y la frecuencia a la que trabaja, y mucha más información.

