



ANTIVIRUS

RESIDENTES : Son los más comunes, los más necesarios y los más complejos. Son los Antivirus que están constantemente vigilando el sistema para evitar que no hay ningún tipo e intrusión

ANALIZADORES DE BAJA DEMANDA: utilizan el mismo motor de búsqueda que el residente, se encargan de analizar partes del sistema solamente cuando el usuario lo ordena. SOn llamados en ocasiones especiales. Puede usarse, por ejemplo para analizar un disquete o para revisar la información antigua no utilizada.

VIRUS

Adware:

El adware está conectado muy de cerca con el spyware, y muchos programas spyware se instalan con la intención de ejecutar programas adware. El adware lanza publicidad, muy a menudo en la forma pop-ups. Estos están personalizados para el usuario, basados principalmente en su comportamiento en Internet.

Dialer:

Es un programa que suele ser utilizado para redirigir, de forma maliciosa, las conexiones mientras se navega por Internet. Su objetivo es colgar la conexión telefónica que se está utilizando en ese momento (la que permite el acceso a Internet, mediante el marcado de un determinado número de teléfono) y establecer otra, marcando un número de teléfono de tarificación especial. Esto supondrá un notable aumento del importe en la factura telefónica.

Gusano: Un gusano de red infecta otros ordenadores y se propaga automáticamente en una red, independientemente de la acción humana. El hecho de que no depende de acción humana para propagarse, lo hace más rápido que un virus.

Hoax: Mensaje de Correo electrónico que informan de la aparición de nuevos virus que producen efectos catastróficos en nuestros PCS, como podéis imaginar son falsos y el único objetivo es captar direcciones de correo electrónico

Joke: programa que muestra en pantalla falsos mensajes que advierten de la inminente realización de acciones destructivas en el ordenador, simulan dichas acciones o realizan modificaciones en la configuración de la pantalla, el mouse, etc

Spyware (Software de espionaje):

Son programas que rastrean los hábitos de comportamiento del usuario y su información personal para luego enviar esta información a terceros sin la autorización o conocimiento del mismo.

Troyano: Programa malicioso camuflado dentro de otro programa aparentemente útil e inofensivo. Los troyanos pueden ir incluidos dentro de programas conocidos, de forma que es necesario controlar la fuente de donde se obtiene el software.



GLOSARIO:

Definiciones de alguno de los términos más utilizados o referenciados en Internet:

- **Antivirus / Programas antivirus:**
Son todos aquellos programas que permiten analizar la memoria, las unidades de disco y otros elementos de un ordenador, en busca de virus.
- **Bug:**
Este término se emplea para indicar un fallo o error en un programa informático.
- **Caché:**
Es una pequeña sección de la memoria de un ordenador.
- **Cookies:** Es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una *cookie* para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo una cookie no identifica a una persona, sino a una combinación de computador y navegador.
- **Carding:**
Uso fraudulento de tarjetas de crédito y débito y sus números y claves a través de Internet.
- **Certificado:**
Documento digital emitido por una entidad independiente que garantiza la identidad de los sistemas y personas en Internet. La seguridad del certificado está protegida por técnicas criptográficas.
- **Cookie:**
Es un fichero de texto que, en ocasiones, se envía a un usuario cuando éste visita una página Web. Su objetivo es registrar la visita del usuario y guardar cierta información al respecto.
- **Cracker:**
Es una persona interesada en saltarse la seguridad de un sistema informático.
- **DirectX:** Interfaz de programación bajo Windows, que permite acceder directamente al hardware (por ejemplo, tarjetas gráficas y de sonido). Es empleado para programar juegos en este sistema.



- **Dominio o Nombre de Dominio:** Es un nombre registrado que identifica al sitio de la red de una organización accesible por los usuarios de Internet. Por ejemplo, agpd.es, es el nombre de dominio de la Agencia Española de Protección de Datos.
- **Firewall / Cortafuegos:**
Su traducción literal es muro de fuego, también conocido a nivel técnico como cortafuegos. Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.
- **freeware:** Aplicaciones de uso gratuito que pueden encontrarse en Internet.
- **Hacker:**
Persona que accede a un ordenador de forma no autorizada e ilegal.
- **HIPERTEXTO:** Todo documento que está vinculado (hipervínculo) con otros documentos a través de enlaces (links). Al ingresar a ese enlace se puede acceder al documento enlazado.
- **HTTP (HyperText Transfer Protocol):**
Protocolo de transferencia de hipertexto. Es un sistema de comunicación que permite la visualización de páginas Web, desde un navegador. http En los años 90 apareció un protocolo de Internet llamado HTTP y nació la Worl Wide Web, una inmensa red de servidores HTTP que envían archivos por Internet y a la que se conoce por los diminutivos de "W3", "WWW" o "la Web". Mucha gente confunde la Web con Internet, siendo la primera tan sólo uno de los muchos servicios disponibles en Internet.
- **IP:** Cada ordenador presente en Internet tiene asignado un número o dirección IP único y se usa como identificativo del mismo a la hora de establecer una conexión con un determinado servidor
- **ISP (Internet Service Provider):**
Una empresa que brinda acceso y servicios de Internet en alguna forma, normalmente por dinero.
- **JavaScript:**
Es un lenguaje de programación que aporta características dinámicas (datos variables en función del tiempo y el modo de acceso, interactividad con el usuario, personalización, etc.) a las páginas Web, escritas en lenguaje HTML.
- **Keylogger (Capturador de teclado):**
Programa que recoge y guarda una lista de todas las teclas pulsadas por un usuario. Dicho programa puede hacer pública la lista, permitiendo que terceras personas conozcan estos datos -lo que ha escrito el usuario afectado (información introducida por teclado: contraseñas, texto escrito en documentos, mensajes de correo, combinaciones de teclas, etc.).



- **.Javascript:**
es un lenguaje de Scripts comparativamente simple, desarrollado por Netscape para utilizar en páginas Web. Permite aumentar la interactividad y la personalización de un sitio. El JavaScript tiene características comunes al Java, pero no es tan complejo y tiene menos espectro de acción.
- **JPEG** Grupo de expertos fotográfico común Joint Photographic Experts Group
- **Link:** Una traducción muy literal de Link podría ser "acoplamiento", en el sentido práctico de internet este término está referido a un **enlace, hipervínculo**. El **link** crea una conexión con otro documento web por medio de la dirección URL.
- **Malware:**
El malware informático es el término para el código malicioso diseñado para molestar o destruir un sistema informático.
- **Muleros:**
Personas interpuestas que cooperan (a veces de manera inconsciente e) en la comisión de delitos, por ejemplo transfiriendo fondos desde unas cuentas a otras.
- **Navegador:**
Un navegador Web o navegador de Internet es el programa que permite visualizar los contenidos de las páginas Web. También se conoce con el nombre de browser. Ejemplos: Internet Explorer, Netscape Navigator, Firefox, etc.
- **Página Web** (Page Web)
Una parte constitutiva de un sitio Web vinculada a otros documentos mediante vínculos hipertexto
- **Pharming:**
El pharming es una nueva modalidad de fraude online que consiste en suplantar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página Web falsa.
- **Phishing:**
Se define así el conjunto de técnicas usadas para el conocimiento fraudulento de los datos de identificación y de autenticación de los clientes de la banca electrónica.
- **Pop-ups:**
El pop-ups son ventanas emergentes que salen durante la navegación, normalmente contienen publicidad.



- **Portal de Internet** es un sitio web cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios, entre los que suelen encontrarse buscadores, foros, documentos, aplicaciones, compra electrónica, etc. Principalmente están dirigidos a resolver necesidades específicas de un grupo de personas o de acceso a la información y servicios de a una institución pública o privada.
- **Proxy:**
Sistema informático cuya misión es hacer de intermediario entre un sistema y otro a través de Internet. Entre las misiones de un proxy están acelerar el acceso a Internet, filtrar los contenidos a los que se ha accedido y proteger los sistemas evitando su comunicación directa.
- **Puertas traseras:**
Una puerta trasera es un programa que abre su ordenador para dar acceso sin que el usuario lo permita.
- **Router:**
Un dispositivo (o programa de software) que maneja la conexión entre dos o más redes. Se encargan de buscar la dirección de destino de los paquetes que pasan por ellos y deciden hacia qué ruta enviarlos.
- **Scam:**
Sistema para captar 'muleros'. Básicamente con anuncios de trabajo en prensa e Internet.
- **Shareware:**
Son versiones de evaluación de un producto software, de uso gratuito, que sirven básicamente para probar el producto antes de adquirirlo definitivamente.
- **Sitio web** (en inglés: **website**) es un conjunto de páginas web, típicamente comunes a un dominio de Internet o subdominio
- **Skimming:**
Obtener los números de las tarjetas por medio de la copia de bandas magnéticas.
- **SMIME (Secure Multi Propose Mail Extensión):**
Protocolo seguro de intercambio de correo electrónico.



- **SNMP (Simple Network Management Protocol):**

Es un conjunto de estándares de comunicación entre dispositivos conectados a la red sobre TCP/IP. Ejemplos de estos dispositivos pueden ser: routers, hubs y switches. Se dice que un dispositivo es "compatible con SNMP" si este puede ser monitoreado y/o controlado usando mensajes SNMP. Los mensajes SNMP son conocidos como "PDU's" - Protocol Data Units, o traps.

Los dispositivos compatibles con SNMP contienen un software "agente" para recibir, enviar y actuar sobre los mensajes SNMP. Existen programas de software para la administración de dispositivos vía SNMP que están disponibles para cada una de las plataformas más comunes y por lo regular se incluyen con el dispositivo a administrar. Algunos programas de software SNMP están diseñados para administrar y monitorear una amplia variedad de dispositivos.
- **Spam:**

Es correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos.
- **SSL (Secure Socket Layer):**

Se trata de un protocolo de seguridad estándar que transmite la información cifrada entre el navegador y el servidor Web a través de Internet. SSL proporciona privacidad para datos y mensajes, así como autenticación de los datos. De acuerdo con la convención establecida, la dirección de las páginas Web que requieren una conexión SSL comienza con https: en lugar de http:
- **URL (Uniform Resource Locator):**

Dirección a través de la cual se accede a las páginas Web en Internet (o a otros ordenadores).
- **Virus:**

Los virus son programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables
- **WWW:** Telaraña mundial Permite incorporar multimedia e hipertextos en internet, dando origen a la Web como la conocemos.