

Terminología básica

Conceptos esenciales para un acercamiento a la relación entre seguridad e Internet.

Prólogo

Por favor, consulte la [introducción](#) a nuestra sección Glosarios, para una mejor comprensión de los criterios, terminología y convenciones utilizadas.

🔍 Presionando el atajo de teclado **Control + F** podrá hacer búsquedas simples en esta página.

Glosario

ActiveX

Es una tecnología desarrollada especialmente para funcionar en entornos Windows 9x y NT y para la creación de páginas de Internet activas.

Esta tecnología es implementada mediante elementos denominados controles ActiveX, que son programas dedicados, a través de los cuales, el navegador asigna un espacio rectangular donde el programa tendrá la absoluta responsabilidad de interactuar con el usuario. La tecnología ActiveX soporta instalación completa y automatizada. Cuando el navegador encuentra un hipervínculo HTML a un elemento de control, primero verifica si ese elemento ya se encuentra en el ordenador del usuario, es decir, si ha sido usado anteriormente.

Si encuentra el elemento de control, el navegador comienza la transferencia necesaria de datos para comenzar la ejecución de este componente.

Si el elemento de control no está disponible en el ordenador del usuario, el navegador accede a la dirección de Internet especificada en el cuerpo de la página, procediendo a descargar, instalar y registrar el control ActiveX dentro del sistema para posteriormente ejecutar el componente.

Agrupamiento

Bundling

Distribución conjunta de varios programas, generalmente relacionados, de forma tal que cuando se instala el grupo de programas, se pueden instalar también múltiples componentes.

En muchos casos, el agrupamiento resulta muy práctico y útil para el usuario.

Sin embargo, a veces algunos componentes de programas no deseados, como los contenidos de *adware* molesto o dañino, pueden venir agrupados con las aplicaciones que se instalan voluntariamente en el sistema.

En esos casos, dichos programas podrían funcionar en un ordenador, sin el conocimiento ni la aceptación del usuario.

***Alternate Data Stream**

Ver [Flujo alternativo de datos](#).

Análisis de fuga

LeakTest

Complejos procesos a través de los cuales se verifica la capacidad de un cortafuegos para evitar la fuga de datos hacia el exterior del ordenador.

Ancho de banda

Bandwith

Es la máxima velocidad a la cual los datos pueden ser enviados o recibidos a través de una conexión.

Cuanto mayor sea la cantidad de datos a enviar/recibir, mayor deberá ser el ancho de banda disponible para poder efectuar la transferencia, como por ejemplo, en la transmisión y reproducción de video y/o música en tiempo real.

Aplicaciones Java

Applet

Son programas de reducidas dimensiones, escritos en el lenguaje Java, que pueden ser incluidos en páginas desarrolladas en HTML, de la misma forma que se incluye una imagen. Al usar un Applet Java en un navegador que admite este tipo de tecnología, el código del Applet es transferido al sistema del usuario y ejecutado en el navegador mediante la Máquina Virtual Java (JVM).

***Applet**

Ver [Aplicaciones Java](#).

Archivo hosts

Archivo almacenado en el ordenador del usuario, que se utiliza para buscar la dirección del Protocolo de Internet (*IP; Internet Protocol*) de un dispositivo conectado a la red del ordenador.

Es sabido que algunos programas espía cambian el archivo *hosts* para desviar automáticamente a los usuarios, desde el sitio al que ellos quieren acceder hacia otros sitios que el desarrollador del programa espía desea que visiten.

***Bandwidth**

Ver [Ancho de banda](#).

***Banner**

Ver [Imagen publicitaria](#).

Barra de sistema

System tray

Parte de la barra de tareas de Windows que contiene la hora y los iconos de cada programa que se está ejecutando. Habitualmente, en la barra de sistema están los iconos de los programas residentes que son aquellos que pueden ser llamados instantáneamente.

Barra de tareas

Task bar

Barra habitualmente situada en el sector inferior del escritorio de Windows, donde a cada aplicación en ejecución le corresponde un botón representativo.

BHOs

Browser Helper Object

Objeto asistente del navegador

Ver [Complemento del navegador](#).

***Boot, Booting**

Ver [Carga del sistema](#) .

***Boot sector**

Ver [Sector de inicio](#).

Botnet

Tipo de programa de control remoto, en especial un conjunto de programas robot (*bots*), que se ejecutan de manera autónoma.

Habitualmente la expresión *botnet* define a una grupo de ordenadores maliciosamente controlados de forma remota (ordenadores *zombies*), que ejecutan programas dañinos (gusanos o troyanos, entre otros) bajo un comando en común, y controlan la infraestructura de las redes públicas o privadas.

Los *botnets* se utilizan para enviar correo no deseado de manera remota, para instalar más programas espía sin consentimiento, o con otros fines ilícitos.

Broadcast

Ver [Difusión](#).

***Campus Area Network**

Ver [Red de área extendida](#).

***CAN**

Campus Area Network

Ver [Red de área extendida](#).

Carga del sistema

Boot, Booting

La carga del sistema comienza después de encender el ordenador y de la inicialización del procesador, a partir del cual se ejecuta la verificación automática de encendido (POST, Power On Self Test) y es buscado el [sector de inicio](#) en el disco de inicio.

Si dicho sector es encontrado, el contenido del mismo será copiado en la dirección 00000:7C00, y se le cederá el control.

Si el disco de inicio es el disco duro, se copiará el contenido del registro principal de inicio (MBR, Master Boot Record) en la memoria. Y desde allí, buscará en la tabla de particiones cuál es la que contiene el sector de inicio activo, para leerlo.

El código insertado en el sector de inicio buscará los archivos básicos del sistema operativo, los leerá y ejecutará uno de ellos. Y de esta forma, el sistema operativo tomará el control del ordenador.

Cifrado

Ver [Encriptación](#).

Claves del registro

Anotaciones individuales en el registro.

El valor de las claves se modifica cada vez que se instala un nuevo programa o se modifican los valores de la configuración.

A menudo, los programas espía modifican los valores de las claves del registro para tomar el control de algunas partes del sistema.

Esos cambios pueden obstaculizar la función habitual del ordenador.

Ciente

Es un ordenador que accede y toma información de otro ordenador ubicado en forma remota, al que se denomina Servidor.

COM

Los archivos con extensión .COM contienen código de procesamiento ejecutable, capaces de trabajar a través de un solo segmento.

Complemento

Plug-In

Módulo de programa adicional que funciona con un programa principal para mejorar las prestaciones de este último.

Complemento del navegador

Componente de un programa que interactúa con un navegador de Internet, para brindar determinadas funcionalidades o realizar ciertas operaciones, que de otra forma no se incluirían en el navegador.

Un ejemplo típico son los complementos para mostrar formatos de gráficos específicos, reproducir archivos de audio y vídeo o agregar barras de herramientas que incluyan servicios de búsqueda, o de defensa contra la adulteración de direcciones IP.

Sin embargo, los complementos también son capaces de realizar operaciones potencialmente indeseables como, por ejemplo, dirigir los resultados de búsqueda hacia un sitio, espiar el comportamiento de navegación del usuario y su historial de conexiones, o instalar *adware* molesto o dañino u otros programas no deseados.

Los tipos de complementos del navegador incluyen:

- [Controles ActiveX](#)
Tipo de complemento del navegador que se descarga y ejecuta en Internet Explorer de Microsoft.
- [Objeto asistente del navegador](#)
Tipo de complemento del navegador que se ejecuta cada vez que se inicia Internet Explorer.
- **Extensiones Firefox de Mozilla**
Complemento del navegador específico de Firefox de Mozilla.

Conexión compartida de Internet

ICS, *Internet Connection Sharing*

Tecnología implementada en los sistemas Windows 98SE y superiores, que permite, en una red local, que un equipo se conecte directamente a Internet y el resto de los ordenadores de dicha red, compartan esta conexión a Internet como una sola cuenta de acceso, pudiendo utilizar de forma independiente distintos tipos de servicios y aplicaciones Web, como mensajeros, navegadores y correo electrónico, entre muchos otros.

Amplíe la información leyendo [Proxy](#) y [Router](#).

Control de conexiones PPTP

ver [PPTP](#)

Cookie

Es un archivo con una pequeña porción de información que es transferida desde un servidor hacia el navegador del visitante, siendo guardado en el disco duro del ordenador cliente durante un tiempo variable, que puede oscilar entre una sesión abierta y un plazo extendido.

En ciertas circunstancias, dicha información, puede ser enviada al servidor de origen.

Habitualmente, es usada para individualizar las preferencias de navegación del usuario.

Cookie de seguimiento

Es una *cookie* que se utiliza para investigar los hábitos de navegación de los usuarios.

Este tipo de *cookies* son un método propio de la tecnología de seguimiento.

Habitualmente, son empleadas por anunciantes que desean analizar y manejar los datos de publicidad, pero pueden utilizarse para crear un perfil y realizar un seguimiento detallado de la actividad del usuario.

Sin embargo, las *cookies* de seguimiento son simples archivos de texto, de tamaño mucho más limitado que los programas ejecutables instalados en los ordenadores de los usuarios. Mientras que las aplicaciones pueden registrar cualquier dato o actividad del ordenador (ver [Monitor del sistema](#)), las *cookies* son simplemente un registro de las actividades en un solo sitio de Internet, o en sus sitios relacionados.

Cortafuegos

Firewall

Programa o dispositivo físico usado para actuar como barrera protectora entre un ordenador y la red a la cual éste se conecta.

Cortafuegos integrado de Windows

ICF, Internet Connection Firewall

Herramienta incluida en Windows XP y superiores para actuar como barrera protectora entre un ordenador y la red a la cual éste se conecta.

Cuenta con funciones básicas de seguridad y su uso pudiera generar una falsa sensación de seguridad debido a lo primitivo de su implementación.

Cracker

Es la denominación que se le da al individuo que logra obtener acceso no autorizado a un ordenador.

Criterios objetivos

Son ciertos factores de comportamiento que las empresas de aplicaciones para la seguridad informática consideran para decidir si un determinado proceso o programa puede ser definido como espía.

Cuarentena

(Informática)

Proceso de aislamiento de archivos que impide su ejecución y/o posibles daños al ordenador y/o sistema.

Datagrama

Es la unidad de los mensajes o datos que son transmitidos a través de una red TCP/IP.

Cada datagrama (también denominado Paquete) es una entidad independiente que contiene la dirección de origen y destino de los datos así como el método de transporte en la red.

Datagrama IP

Es la unidad de los mensajes o datos que son transmitidos a través de una red TCP/IP utilizando el protocolo IP.

Cada datagrama (también denominado Paquete) es una entidad independiente que contiene la dirección de origen y destino de los datos así como el método de transporte en la red.

Datagrama UDP

Es la unidad de los mensajes o datos que son transmitidos a través de una red TCP/IP utilizando el protocolo UDP.

Cada datagrama (también denominado Paquete) es una entidad independiente que contiene la dirección de origen y destino de los datos así como el método de transporte en la red.

DDoS

Distributed Denial of Service Attack

Ataque distribuido de denegación de servicio

Método usado para sobrecargar, reiniciar el ordenador o apagar un sistema remoto, al atacarlo con tráfico desde otros equipos.

Los ataques DDoS a menudo se inician utilizando los sistemas comprometidos de usuarios de Internet, por lo general, utilizando *botnets*.

Un agresor puede explotar una vulnerabilidad en un sistema de ordenadores y convertir ese sistema en el 'amo' (*master*) del ataque DDoS, utilizando programas para el control remoto de otros ordenadores.

Posteriormente, el intruso utilizará el sistema *master* para identificar y controlar *zombies* capaces de realizar el ataque.

***Denial of Service**

Ver [DoS](#).

Descargador

Programa diseñado para recuperar e instalar archivos adicionales.

Los descargadores pueden ser herramientas útiles para automatizar actualizaciones de programas esenciales, tales como las de sistemas operativos, navegadores, aplicaciones antivirus, herramientas contra programas espía, juegos y otros tipos de aplicaciones útiles o de entretenimiento.

Las actualizaciones automatizadas sirven también para corregir oportunamente las vulnerabilidades de seguridad.

Los descargadores no autorizados son utilizados por terceros para descargar programas potencialmente no deseados sin notificación o consentimiento del usuario.

Descargador automático

trickler

Programa de descarga automática, diseñado para instalar o reinstalar programas realizando descargas lentas en segundo plano, de forma tal que la descarga sea menos notoria y no dificulte otras funciones.

Los descargadores se utilizan habitualmente para permitir que un programa espía se instale o reinstale de manera silenciosa, después de la eliminación de sus componentes por parte del usuario.

Descarga conducida

Drive-by-download

Descarga automática de programas al ordenador del usuario cuando visita un sitio de Internet o visualiza un correo electrónico en formato html, sin el consentimiento del usuario y a menudo sin ningún tipo de notificación.

Las descargas conducidas se realizan, por lo general, explotando ciertos agujeros de seguridad, o debido a una disminución de las configuraciones de seguridad en el ordenador del usuario.

Descifrador de contraseñas

Programa de análisis de seguridad diseñado para permitir que una persona recupere o descifre contraseñas perdidas, olvidadas o desconocidas.

El descifrador de contraseñas puede adivinar una contraseña al ejecutar un ataque de fuerza bruta, por ejemplo, probando cada combinación de caracteres para encontrar la contraseña correcta, o al ejecutar un ataque de diccionario, por ejemplo, probando palabras comunes de diccionarios grandes, que los usuarios podrían utilizar como contraseña.

Si bien puede ser una herramienta legal utilizada por administradores de seguridad y funcionarios de agencias de aplicación de la ley, los descifradores de contraseñas presentan una amenaza significativa para la seguridad y la privacidad cuando se utilizan de manera ilícita.

DHCP

Dynamic Host Configuration Protocol

Protocolo de configuración dinámica de servidores

Es un protocolo utilizado para la asignación dinámica de direcciones IP que puede soportar también métodos simples de asignación estática de direcciones, permitiendo que dichas direcciones puedan ser establecidas tanto manual como automáticamente.

DHCP puede ser fuente de problemas al intentar coordinar direcciones en las bases de datos entre los servicios DHCP y DNS, así como por la naturaleza de la inestabilidad de las direcciones IP, que pueden complicar los procedimientos de control en las redes involucradas.

Difusión

Broadcast

Es un tipo especial de dirección IP usada para enviar un mensaje a todos los nodos de una red.

Hay dos formas de envío:

- Difusión limitada

Limited broadcast

Si la dirección IP tiene sus bits binarios en 1, el paquete es transmitido a todos los nodos de la red local pertenecientes al origen del paquete.

- Difusión limitada de mensajes

Limited broadcasting message

Si la dirección IP y el identificador de red tiene sus bits binarios en 1, el paquete es transmitido a todos los nodos de la red local con la dirección especificada.

*Difusión limitada

Ver [Difusión](#).

*Difusión limitada de mensajes

Ver [Difusión](#).

Dirección IP

Es la dirección de Internet asignada oficialmente y con formato numérico compuesto por 4 bytes, usualmente representada por cuatro números decimales separados por un punto, conteniendo dos sectores de información, según recomendaciones del NIC (*Network Information Center*, Centro de información de redes):

- El número de red
- El número de nodo.

Existen direcciones reservadas para ser utilizadas libremente por el administrador en redes locales para ordenadores y otros tipos de nodos, mientras que las direcciones públicas son asignadas por la [Autoridad de asignación de números de Internet](#) (IANA, *Internet Assigned Numbers Authority*) o sus delegaciones autorizadas, para redes individuales y servidores en Internet.

La dirección IP es utilizada en el estrato a nivel de red.

Ejemplo:

Dirección IP: 194.224.216.18

Dirección DNS

Es la dirección de Internet asignada con formato texto, en la cual los nombres de los diferentes dominios se encuentran separados por un punto.

Esta dirección mantiene una correspondencia entre la dirección IP en una red y una base DNS.

Ejemplo:

Dirección IP: 194.224.216.18

Nombre de dominio (también denominada dirección DNS): www.protegerse.com

DNS

Domain Name Service

Servicio de nombres de dominio

Es el sistema de nombres asignados oficialmente por la [Autoridad de asignación de números de Internet](#) (IANA, *Internet Assigned Numbers Authority*) para redes individuales y servidores en Internet, con un método más sencillo de recordar que la dirección IP compuesta por un grupo de cuatro conjuntos de números separados por un punto.

Ejemplo:

Dirección IP: 194.224.216.18

Nombre de dominio (también denominada dirección DNS): www.protegerse.com

El sistema DNS requiere una configuración estática de su base de datos para poder definir correctamente la correspondencia unívoca entre el nombre de dominio de Internet y su dirección IP, y de ese modo, traducir automáticamente uno en otro.

El protocolo DNS es un protocolo de servicio auxiliar en el nivel de aplicaciones con un funcionamiento asimétrico definiendo el servicio DNS para servidores y para clientes.

- **DNS para servidores**

Mantienen una parte de la base de datos distribuida que contiene la correspondencia entre nombres y direcciones IP.

Esta base de datos es distribuida de acuerdo a la administración de dominios en Internet y mediante una estructura jerárquica.

- **DNS para clientes**

Los clientes conocen la dirección IP del servidor al cual quieren acceder y transfieren una solicitud mediante el nombre DNS de acuerdo al protocolo IP, y esperan por la dirección IP que corresponde a ese nombre.

Si esa información solicitada se encuentra alojada en la base de datos del servidor, éste inmediatamente transfiere la respuesta al navegador.

Si la información solicitada no se encuentra en ese servidor, la solicitud es transferida a otro servidor de dominio que repite el procedimiento y así sucesivamente hasta encontrar o no, la necesaria correspondencia, según la estructura jerárquica de dominios de Internet.

La base de datos DNS tiene una estructura denominada Area de dominios por nombre, y en cada dominio (cada nodo del árbol jerárquico) se encuentra un nombre, pudiendo contener sub-dominios.

El nombre de dominio identifica su posición en la base de datos en relación con el dominio padre, y cada punto en el nombre, actuando como separador, permite conformar la estructura jerárquica y su correspondencia con los nodos de dominio.

***Domain Name Service**

Ver [DNS](#).

DoS

Denial of Service

Denegación de servicio

También se lo conoce como: Ataque DoS y Ataque por denegación de servicio.

Este tipo de ataque es producido en un ordenador por parte de otro ordenador en una red local o en Internet y se lleva a cabo aprovechando errores en el conjunto de programas o sistema operativo que soporta una red y/o sus protocolos, produciendo perturbaciones en las condiciones normales de operación, culminando habitualmente con la caída del sistema.

Una forma habitual de producir las perturbaciones, es el envío de gran cantidad de peticiones de respuesta a conexiones efectuadas desde múltiples servidores remotos utilizando técnicas de enmascaramiento de direcciones IP.

Droneware

Programas utilizados para tomar el control remoto de un ordenador y, por lo general, utilizado para enviar correo electrónico no deseado de manera remota, ejecutar ataques DDOS o albergar imágenes ofensivas en Internet. Ver también [Botnet](#).

***Dynamic Host Configuration Protocol**

Ver [DHCP](#).

Elevación de privilegios

Proceso que permite a una persona o dispositivo obtener privilegios no autorizados, habitualmente, el acceso a un ordenador o red con derechos de Administrador.

Empaquetador

Programa que puede comprimir y/o encriptar un archivo ejecutable, de forma tal que se evite que la imagen en memoria del archivo coincida con el archivo real guardado en un disco.

Algunas veces los empaquetadores son utilizados para la protección de copias, pero también se usan a menudo para que los programas espía sean más difíciles de detectar y/o analizar.

Emparchado del kernel

Kernel hooking o kernel patching

Se refiere a la utilización de mecanismos no documentados, para modificar o reemplazar código del [núcleo del sistema operativo](#).

✘ Esta técnica, viola fundamentalmente la integridad del núcleo de Windows, y Microsoft ha desalentado permanentemente su aplicación.

La modificación del núcleo del sistema operativo podría provocar un funcionamiento impredecible, inestabilidad del sistema, y problemas de rendimiento, con el consecuente riesgo de pérdida de datos y disminución de la productividad del usuario.

El **emparchado del kernel** se ha convertido en un mecanismo utilizado por los desarrolladores de código malicioso, para atacar los sistemas Windows.

Los motivos para emparchar el *kernel* son muy variados.

Los desarrolladores de aplicaciones contra código malicioso, por ejemplo, podrían interceptar llamadas del sistema para prevenir que los programas que ellos han determinado como maliciosos, creen procesos en el sistema.

Los objetivos de este tipo de aplicaciones son loables, pero estas prácticas también podrían causar problemas de rendimiento y confiabilidad.

El mayor riesgo del **emparchado del kernel** proviene de los virus y los creadores de programas espía que usan esta técnica con intenciones maliciosas, y para esconder su presencia.

Los autores de códigos maliciosos se ven motivados a emparchar el núcleo del sistema porque es un mecanismo poderoso para atacar el ordenador del usuario, y sus datos.

Con el emparchado se pueden implementar [rootkits](#), que también esconden la presencia de otros programas dañinos en el sistema.

Este tipo de aplicaciones pueden ser extremadamente potentes, por ejemplo, permitir capturar contraseñas de cuentas bancarias y monitorizar todas las actividades del usuario.

Encriptación

También denominado **Cifrado**

Proceso mediante el cual se protegen archivos (o textos, contraseñas, etc.) de su lectura o comprensión directa a través de convertir su valor original en un lenguaje cifrado, como podría ser reemplazando determinadas letras por números, expresiones matemáticas, o cualquier combinación que impida su lectura sin poseer las claves o secuencias que permitieron el proceso de transformación.

***Enrutador**

Ver [Router](#).

EULA

End User License Agreement

Acuerdo de licencia de usuario final.

Pacto entre un fabricante y un usuario de programas de ordenadores que especifica los términos de uso supuestamente acordados por parte del usuario.

El fabricante de programas especifica los parámetros y limitaciones de uso, lo que incluye un contrato vinculante.

Algunas empresas utilizan el EULA como el único medio de divulgación del comportamiento del programa (incluyendo agrupamiento, uso de los datos del usuario, entre otros).

Explotación / explotación de seguridad

Programa que aprovecha un agujero o vulnerabilidad en el sistema de un usuario para obtener acceso no autorizado al sistema.

Extensión de un archivo

En los sistemas Windows, la extensión de un archivo, es un identificador que está inserto en la denominación de un fichero, localizado a la derecha del mismo, y a continuación del punto (que actúa como un separador).

Si bien es frecuente que la extensión de un archivo esté compuesta por tres caracteres, no es obligatorio que esto sea así.

En otros sistemas operativos, la denominación de un fichero puede carecer de extensión y ser válido también.

Ejemplos:

- nombre (propiamente dicho).**extensión**
- setup.**exe**
- documento.**doc**
- planilla.**xls**

La extensión de un archivo se asocia con una aplicación determinada, de tal forma que si se pulsa dos veces sobre un fichero con una extensión .DOC (por ejemplo) se abrirá el programa predeterminado (Word, para este ejemplo) que a su vez abrirá el documento .DOC seleccionado en primer término.

Algunas amenazas informáticas, a través de distintas técnicas, enmascaran la verdadera extensión de un archivo.

***File Transfer Protocol**

Ver [FTP](#).

***Firewall**

Ver [Cortafuegos](#)

Flujo alternativo de datos

Alternate Data Stream

Extensión del sistema de archivos de Windows NT de Microsoft (*NTFS, NT Filing System*) que brinda compatibilidad con archivos creados utilizando el sistema jerárquico de archivos de Apple (*HFS, Hierarchical Filing System*).

Las aplicaciones deben agregar código especial si desean acceder y manipular datos almacenados en un flujo alternativo.

Algunos programas espía utilizan estos flujos para evadir la detección.

FTP

File Transfer Protocol

Protocolo de transferencia de archivos

Es un servicio de Internet para transferir archivos entre un ordenador y otro.

***Gateway**

Ver [Puerta de enlace](#).

***Gateway to Gateway Protocol**

Ver [GGP](#).

GGP

Gateway to Gateway Protocol

Protocolo de Puerta de enlace a Puerta de enlace

Es un protocolo para conectar dos Puertas de enlace e interactuar entre ellas, especialmente en la ejecución de tareas de control.

***Graphics User Interface**

Ver [GUI](#).

GRE

Generic Routing Encapsulation

Encapsulado genérico de enrutamiento

Un método para enviar datos criptografiados desde un ordenador a otro a través de una red local.

Guiones

En un lenguaje de programación no compilado que puede estar basado en distintos lenguajes y que se utiliza para automatizar tareas repetitivas.

GUI

Graphics User Interface

Interfaz gráfica de usuario

Programas gráficos que permiten que el usuario interactúe con los ordenadores a través de representaciones de objetos fácilmente identificables, como iconos, botones, analogías con un escritorio, etc.

Los ordenadores Apple Macintosh fueron los primeros en introducir una interfaz consistente de representación gráfica, seguido muchos años después por los sistemas Windows.

Herramientas de gestión de estado

Tecnologías utilizadas para almacenar y poner a disposición, información acerca del "estado" de un sistema, es decir, datos acerca de las condiciones y operaciones. Las *cookies* son la forma más común de la herramienta de gestión de estado, debido a que pueden utilizarse para almacenar datos provistos a un sitio de Internet y mantener una sesión de la aplicación en Internet.

Las herramientas de gestión de estado pueden utilizarse como tecnología de seguimiento.

Herramientas piratas

Programas de análisis de seguridad que pueden utilizarse para investigar, analizar o comprometer la seguridad de los sistemas.

Algunas herramientas piratas son programas con propósitos múltiples, mientras que otras tienen algunos usos legales.

HTML

HyperText Markup Language

Lenguaje de marcas de hipertexto

Lenguaje de programación que permite, mediante el uso de etiquetas y códigos apropiados, escribir páginas prioritariamente para Internet y que pueden ser interpretadas correctamente por un navegador.

Las páginas desarrolladas en lenguaje HTML pueden contener hipervínculos, imágenes y texto con formato, así como una variedad de efectos para mejorar la estética y la navegabilidad del usuario que accede a las mismas.

*HyperText Markup Language

Ver [HTML](#).

ICMP

Internet Control Message Protocol

Protocolo de control de mensajes de Internet

Permite la generación de mensajes de error, de paquetes de texto y de mensajes informativos concerniente al protocolo IP y entre ordenadores conectados a una red.

| Valor del campo | Descripción |
|-----------------|---|
| 0 | Respuesta del eco |
| 3 | Destino inaccesible |
| 4 | Disminución del tráfico desde el origen |
| 5 | Redireccionar (cambio de ruta) |
| 8 | Solicitud de eco |
| 10 | Solicitud de enrutador |
| 11 | Tiempo excedido para un datagrama |
| 12 | Problema de parámetros en datagrama |
| 13 | Solicitud de marca de tiempo |
| 14 | Respuesta de marca de tiempo |
| 16 | Respuesta de información |
| 17 | Solicitud de máscara de dirección |
| 18 | Respuesta de máscara de dirección |

Un mensaje ICMP **Solicitud de eco** es uno de los métodos más simples para verificar las condiciones operativas de un código de red.

Una vez que se recibe una señal de eco, cualquier nodo de la red genera una **Respuesta de eco** y la devuelve a la fuente.

Si la fuente recibe una respuesta a dicha solicitud, esto indica que los componentes más importantes del sistema de tráfico están en buenas condiciones.

Un mensaje ICMP **Destino inaccesible** es generado por una puerta de enlace, cuando no puede entregar un datagrama IP.

El datagrama, es la unidad de datos, o paquete, transmitida en una red TCP/IP. Cada datagrama contiene direcciones de fuente y de destino y datos.

Un mensaje ICMP **Disminución del tráfico desde el origen** se transmite desde el nodo a la fuente de datagrama en el suceso en que la cola entrante está superpoblada. En este caso, se quita el datagrama de la cola.

Un mensaje ICMP Redireccionar es un mensaje que se transmite cuando una puerta de enlace detecta que una ruta no satisfactoria es utilizada, entonces la puerta de enlace envía un pedido de cambio de ruta en la tabla de enrutamiento.

Un mensaje ICMP **Anuncio de IP** transmite un aviso de su dirección IP.

El mensaje ICMP **Tiempo excedido para datagrama** es enviado cuando un datagrama es transferido de una puerta de enlace a otra más veces de lo que se le está permitido (normalmente esto indica una ruta cíclica).

Un mensaje ICMP **Problema de parámetro en datagrama** es enviado por una puerta de enlace si ocurre un problema durante la transmisión de un datagrama específico que no está dentro de la diversidad de los mensajes antes mencionados. El datagrama debe abandonarse debido a este error.

Los mensajes ICMP **Solicitud de marca de tiempo** y **Respuesta de marca de tiempo** son utilizados para sincronizar los relojes en un nodo de la red.

Los mensajes ICMP **Solicitud de información** y **Respuesta de información** han quedado obsoletos. Se utilizaban antes por los nodos de la red para determinar las direcciones internas en la red, pero hoy se consideran antiguas y no deberían usarse.

Los mensajes ICMP **Solicitud de máscara de dirección** y **Respuesta de máscara de dirección** son utilizados para encontrar la máscara de una red secundaria. Por ejemplo, cuáles bits definen la dirección en la red.

Un nodo local envía una solicitud de máscara de dirección a una puerta de enlace, y recibe una respuesta de máscara de dirección como réplica.

***ICF**

Internet Connection Firewall

Ver [Cortafuegos integrado de Windows](#).

***ICS**

Internet Connection Sharing

Ver [Conexión compartida de Internet](#).

IGMP

Internet Group Management Protocol

Protocolo de administración de grupos de Internet

Permite a la red transmitir mensajes a un conjunto de ordenadores, siendo usado por nodos y enrutadores (*routers*) para el envío de mensajes, informando sobre datos físicos de la red local y como los nodos están combinados en grupos y a el grupo al cual pertenece cada nodo.

Imagen publicitaria

Banner

La publicidad en Internet suele tener forma rectangular, con una imagen en formato .GIF o .JPG y un hipervínculo que lleva al usuario hacia el servidor del anunciante.

Inspección dinámica de paquetes

Stateful Inspection

La tecnología de cortafuegos para la inspección dinámica de paquetes mantiene una tabla de sesiones activas TCP y UDP, siendo más segura que el filtrado de paquetes tradicional porque permite un trayecto de búsqueda más pequeño por donde el tráfico puede pasar, obteniendo de ese modo, un mejor control de los mismos.

Internet

Red mundial que abarca miles de redes con varios miles de millones de sitios con información de diverso tipo. Aunque muchas veces se confunde Internet con la Web, Internet comprende distintos tipos de servicios y elementos, en una lista muy amplia y variada, como por ejemplo

- Correo electrónico.
- Transferencia de archivos mediante FTP.
- Internet Relay Chat (IRC).
- Navegación mediante protocolo HTTP.
- Sitios y páginas desarrolladas en lenguaje HTML (Páginas Web).
- Telnet.

***Internet Control Message Protocol**

Ver [ICMP](#).

***Internet Group Management Protocol**

Ver [IGMP](#).

***Internet Protocol**

Ver [IP](#).

IP

Internet Protocol

Protocolo de Internet

Es un estrato de red en el protocolo TCP/IP encargado de dividir los datos en paquetes para poder ser transmitidos en la red.

Java

Lenguaje de programación para el diseño y desarrollo de aplicaciones, especialmente para su uso en Internet, pudiendo operar en diferentes plataformas de trabajo.

***Java applet**

Ver [Aplicaciones Java](#).

JavaScript

En un lenguaje de programación no compilado basado en código Java, que se integra dentro de páginas HTML con el objetivo de mejorar la navegabilidad e interacción con el usuario.

***Kernel**

Ver [Núcleo del sistema operativo](#).

***Kernel hooking**

Ver [Emparchado del kernel](#).

***Kernel Patch Protection**

KPP

Ver [Protección contra el emparchado del kernel](#).

***Kernel patching**

Ver [Emparchado del kernel](#).

***KPP**

Kernel Patch Protection

Ver [Protección contra el emparchado del kernel](#).

***LAN**

Local Area Network

Ver [Red de área local](#).

***LeakTest**

Ver [Análisis de fuga](#).

***Local Area Network**

Ver [Red de área local](#).

***Limited broadcast**

Ver [Difusión](#).

***Limited broadcasting message**

Ver [Difusión](#).

***Local Area Network**

Ver [Red de área local](#).

Loopback

Bucle, también denominado Lazo cerrado

Dirección IP (127.0.0.1) reservada para retroalimentación de la información que se obtiene al verificar un programa, en un nodo, sin la necesidad de tener que enviar paquetes a la red local.

***Macro**

Ver [Guiones](#).

***MAN**

Metropolitan Area Network

Ver [Red de área extendida](#).

Marcador

Marcador es un término informal para referirse al programa de marcado.

MBR

Master Boot Record

Es un programa ubicado en el sector de inicio maestro del disco. Se encuentra en el primer sector del disco duro físico. Contiene el código de inicio y la tabla de particiones.

MD5

El algoritmo MD5, es en esencia, una forma de verificar la integridad de los datos, siendo mucho más confiable que el uso de la suma de verificación (*Cheksum*) o cualquier otro método usado comunmente hasta el presente.

Menú contextual

Es un menú que aparece al pulsar, con el botón secundario del ratón, sobre un objeto .

Las opciones desplegadas dependen de la posición del cursor del ratón y los elementos involucrados, cambiando según el objeto seleccionado y las posibilidades que éste admite.

***Metropolitan Area Network**

Ver [Red de área extendida](#).

Modelado de riesgos

Proceso utilizado por proveedores de soluciones contra programas espía para determinar la clasificación de los mismos, tanto en términos de nivel como de tipo de riesgo.

Modo Invisible

Ver [Modo oculto](#) .

Modo Oculto

Stealth mode

Condición en la cual un ordenador puede acceder a Internet sin ser visible para otros ordenadores.

Monitor del sistema

Programa de seguimiento utilizado para controlar la actividad del ordenador.

Los monitores del sistema ofrecen diversas funcionalidades, pero pueden registrar algunos o todos los siguientes elementos: pulsaciones de teclas, capturas de pantallas, correos electrónicos, salas de conversaciones, mensajes instantáneos, sitios de Internet visitados, programas ejecutados, tiempo utilizado en sitios de Internet o usando programas o nombres de usuarios determinados, contraseñas u otros tipos de datos en tránsito.

La información se almacena generalmente para una posterior recuperación, o se transmite a un proceso o persona remota utilizando el monitor.

Los registradores de pulsaciones y los capturadores de pantallas son tipos de monitores del sistema.

***Multicast**

Ver [Multidifusión](#).

Multidifusión

Multicast

Emisión simultánea de varios canales de trabajo.

Es un grupo especial de direcciones IP que comienzan con la secuencia 255.

Si la dirección de multidifusión es especificada en la asignación de direcciones de un paquete, todos los nodos que tienen esa dirección recibirán ese paquete.

Los nodos identifican por ellos mismos a los grupos que pertenecen y el mismo nodo puede ser incluido en varios grupos.

Los mensajes son denominados mensajes de grupo.

La dirección de un grupo no está fraccionada dentro de la red local y el campo con el número de nodo es procesado por el enrutador de una forma especial.

NetBIOS

Network Basic Input/Output System

Es un protocolo fundamental desarrollado por IBM para compartir archivos e impresoras en una red local.

NetBIOS es soportado por IBM (IBM PC LAN), Novell NetWare, Microsoft Windows para Grupos de Trabajo y sistemas de redes desarrollados por otras compañías.

***Network Basic Input/Output System**

Ver [NetBIOS](#)

Nodo

Punto de confluencia de una red, como puede ser un ordenador dentro de una red local o una terminal conectada a un servidor.

Núcleo del sistema operativo

Kernel

Es el módulo central de un sistema operativo.

Es el primero en cargarse, y permanece en la memoria principal. Por esta razón, es importante que el núcleo sea lo más pequeño posible, sin dejar de ofrecer los servicios esenciales que necesitan otras partes del sistema operativo o demás aplicaciones para funcionar correctamente.

El *kernel* es responsable del manejo de la memoria, la administración de procesos y tareas, y la gestión de los discos.

🔧 Como todos los programas dependen de él, una pequeña modificación de su código podría provocar que las aplicaciones se congelen, o que funcionen de un modo no esperado.

La "pantalla azul de la muerte" (*Blue Screen of Death*, BSoD), característica en los sistemas Windows, es el resultado de un error en el *kernel*, o de la acción incorrecta de un controlador ejecutándose en él, sucediendo esto de forma tan severa que el sistema no puede recuperarse.

Una de las formas con las que Microsoft intenta prevenir la aparición de esta pantalla, es intentando mantener la integridad del *kernel*, restringiendo los programas que pueden ejecutarse e interactuar con él.

🚨 **Importante:** Consulte [Emparchado del kernel](#).

Objeto asistente del navegador

BHO, Browser Helper Object

Tipo de complemento del navegador que se ejecuta cada vez que se inicia Internet Explorer.

Las barras de herramientas son una forma común de BHO.

***Patchguard**

Ver [Protección contra el emparchado del kernel](#).

PIE

United Virtualities Persistent Identification Element

Elemento de identificación persistente de virtualidades unidas.

PIE de virtualidades unidas es una tecnología de seguimiento que utiliza Macromedia Flash, diseñada como alternativa al uso de una *cookie* y que es un ejemplo de tecnología pasiva de seguimiento.

Política de privacidad

Aviso legal acerca de cómo la empresa gestiona la información personal del usuario.

La política de privacidad debe contener información acerca de la recolección de información y los usos secundarios de los datos, incluyendo cómo se comparte la información con terceros y quiénes son estos terceros.

***Plug-In**

Ver [Complemento](#).

PPTP

Point-to-Point Tunneling Protocol

Protocolo para una conexión encapsulada punto a punto

PPTP es una tecnología que permite establecer comunicaciones sobre Internet no interceptables, debido a su alto grado de seguridad.

Procedimiento remoto de llamada

RPC, Remote Procedure Call

RPC es una tecnología que soporta aplicaciones distribuidas (aquellas que poseen componentes localizados en diferentes ordenadores) y es utilizada, entre otras, cuando una aplicación necesita usar una función que se está ejecutando en otro ordenador de la red local.

Programa con publicidad

Programa que muestra contenido publicitario.

Programa de análisis de seguridad

Programa utilizado por un ordenador para analizar o sortear las protecciones de seguridad.

Programa de seguimiento

Programa que controla el comportamiento del usuario o reúne información acerca del usuario, algunas veces incluyendo información identificable de forma personal o confidencial, a través de un programa ejecutable.

Programa de control remoto

Programa utilizado para permitir el acceso o control remoto de sistemas de ordenadores.

Programa de descarga automática

Cualquier programa utilizado para descargar e instalar programas, sin interacción con el usuario.

Programa de marcado

Programa que utiliza el módem de un ordenador para realizar llamadas o acceder a servicios.

Es posible que los usuarios quieran eliminar marcadores que se inicien sin su participación activa, dado que puede resultar en cargos telefónicos inesperados y/o generar el acceso a contenidos no buscados o indeseados.

Programa modificador del sistema

Programa utilizado para modificar el sistema del usuario y cambiar su experiencia de uso, por ejemplo, modificando la página principal, la página de búsqueda, el reproductor de medios predeterminado o las funciones del sistema del nivel inferior.

Protección contra el emparchado del kernel

Kernel Patch Protection

KPP

La **Protección contra el emparchado del kernel** monitoriza si el código del kernel o los recursos clave que este utiliza, han sido modificados.

Si el sistema operativo detecta un parche no autorizado en ciertas estructuras de datos, o código, iniciará el apagado del sistema.

✍ *Kernel Patch Protection* no evita que el sistema sea atacado por virus, [Rootkits](#), u otros códigos maliciosos en su totalidad.

Sirve para prevenir un único método para comprometer el sistema: el emparchado de las estructuras del kernel, o su código, para manipular las funcionalidades del núcleo.

Proteger la integridad del kernel es fundamental para resguardar el sistema de ataques maliciosos, y de problemas de seguridad inadvertidos, como consecuencia del emparchado.

Actualmente, *Kernel Patch Protection* no forma parte de las nuevas medidas de seguridad de Windows Vista de 32 bits, pero sí ha sido incorporado en las versiones de 64 bits de Microsoft Windows, incluyendo Windows Server 2003 SP1, Windows XP, Windows XP Professional x64 Edition y Windows Vista x64, con la denominación de **Patchguard**.

Protocolo

Es un conjunto de reglas aceptadas para un particular tipo de intercambio de comunicaciones.

Los ordenadores que intenten transferir datos entre sí deberán utilizar el mismo tipo de protocolo para que la comunicación sea posible y la transferencia sea realizada correctamente.

***Protocolo de datagrama de usuario**

User Datagram Protocol

Ver [UDP](#).

Protocolos de servicio

Un método usado por un Servidor para actualizar información en un ordenador Cliente.

***Protocolo SMB para el servidor de bloque de mensaje**

Ver [SMB](#).

Proxy

Es un programa que administra las conexiones entrantes y salientes, redireccionando todas las comunicaciones entrantes hacia puertos diferentes evitando el acceso no autorizado a redes privadas.

También se lo utiliza para centralizar y distribuir la conexión entre Internet y una red local permitiendo que cada ordenador pueda conectarse a Internet a través de una conexión compartida y evitando que deba hacerlo a través de una conexión saliente individual.

Amplíe la información leyendo [Conexión compartida de Internet](#) y [Router](#).

Puerta de enlace

Gateway

Es un ordenador que permite la conexión de dos tipos diferentes de redes y transmite paquetes de una red a otra.

Funcionamiento similar a un Enrutador (*Router*).

Puerto

El puerto de un ordenador es un dispositivo que se define por programación y que no necesariamente debe tener una asignación física en el equipo. A cada aplicación se le asigna un número de puerto según el tipo de dato que será transmitido.

RAT

Remote Access Tools

Herramienta de acceso remoto/administración

Aplicación ejecutable diseñada para permitir el acceso remoto o controlar un sistema.

La herramienta RAT es un tipo de programa de control remoto.

Si bien esta herramienta tiene muchos usos legales, los agresores pueden utilizarla con fines maliciosos para iniciar o finalizar aplicaciones, instalar o desinstalar nuevos programas o realizar otras acciones no deseadas o no autorizadas.

Red

Una red se compone de dos o más ordenadores unidos a través de un medio físico y vinculados mediante programas y procedimientos adecuados, que les permite compartir datos y/o recursos entre sí.

*Red de área en edificios

CAN, Campus Area Network

Ver [Red de área extendida](#).

Red de área extendida

WAN, Wide Area Network

En su sentido más amplio, es una red extendida situada en un espacio más amplio que la Red de área local pudiendo incluir, o no, otras redes más pequeñas.

En determinadas circunstancias, se la define más específicamente según el alcance geográfico:

- **Red de área en edificios**
CAN, Campus Area Network
Una red extendida que ofrece interconectividad a varios edificios dentro de un mismo predio privado, habitualmente espacios universitarios.
- **Red de área metropolitana**
MAN, Metropolitan Area Network
Una red extendida que ofrece interconectividad a ordenadores y/o redes locales ubicadas todas dentro de la misma ciudad o área geográfica.
- **Red de área extendida**
WAN, Wide Area Network
Una red extendida que ofrece interconectividad a ordenadores y/o redes locales ubicada en áreas geográficas distintas y dispersas.

Red de área local

LAN, Local Area Network

Es aquella red que está situada en un mismo espacio físico o edificio.

También se la menciona como red local.

*Red de área metropolitana

MAN, Metropolitan Area Network

Ver [Red de área extendida](#).

Referencia

Referrer

También llamado Remitente, es parte de una petición HTTP que contiene la URL de la última página visitada antes del envío de dicha petición.

*Referrer

Ver [Referencia](#).

Registro

Bases de datos integradas en ciertos sistemas operativos, que almacenan información, incluyendo preferencias del usuario, datos de configuración y licencias, y acerca del equipamiento físico y de los programas instalados en el ordenador del usuario.

Regla

Es un conjunto de valores combinados que, al cumplirse determinadas condiciones, lanza la ejecución de acciones establecidas previamente.

Una regla debe tener definidos:

- **Criterios**

La ocurrencia de uno o más sucesos o eventos.

Según el programa para el cual se definen las reglas, las condiciones a cumplir deberán verificarse parcial o totalmente para que exista correspondencia.

Ejemplos:

- **Correspondencia parcial**

Cuando el protocolo especificado sea... **o** cuando la dirección especificada sea...

- **Correspondencia total**

Cuando el protocolo especificado sea... **y** cuando la dirección especificada sea...

🔗 Por ejemplo: un cortafuegos como Outpost Firewall sólo admite correspondencia total para dar por cumplidos los criterios establecidos.

- **Acciones**

Al cumplirse todos los criterios establecidos frente a un suceso detectado, se ejecuta una o más acciones establecidas previamente.

Las acciones se ejecutan secuencialmente y mientras que en algunos casos se admite más de una acción posible, en otros, las acciones son excluyentes entre sí, al definirse estos valores en la creación de la regla.

Ejemplos:

- **Acciones múltiples**

Permitir **y** ejecutar aplicación.

- **Acciones excluyentes**

Permitir **o** bloquear.

⚠ **Importante:** Generalmente, sucede que si se han definido varias reglas con los mismos criterios, sólo se ejecutará la primera que los detecte según el orden en que están listadas.

Regla predefinida

Es una [regla](#) con valores predeterminados por los desarrolladores del programa que las utiliza y que han establecido ciertos criterios frecuentes y sus acciones correspondientes, de forma tal que el usuario no tenga necesidad de definir una serie (más o menos compleja) de criterios y acciones, simplificando la tarea de configuración.

Por ejemplo: Al ejecutar Internet Explorer, Outpost Firewall le ofrece la posibilidad de utilizar la regla predefinida denominada **Browser** o **Navegador** que incluye la definición de conexiones HTTP, HTTPS, SOCKS, PROXY, Ghoper, *Web Folders* (Carpetas de Internet), FTP, FTP DATA.

*Remitente

Ver [Referencia](#).

*Remote Procedure Call

Ver [Procedimiento remoto de llamada](#).

Residente

Una aplicación residente es aquella que puede ser invocada en cualquier momento utilizando la propiedad **TSR** (*Terminate and Stay Resident*, Terminar y permanecer latente), a diferencia de las aplicaciones "no residentes" en las que una vez concluida su ejecución, estas son descargadas de la memoria operativa y no pueden ser ejecutadas nuevamente sin su carga previa.

Router

Enrutador

Es un dispositivo que permite la conexión de dos tipos diferentes de redes y transmite paquetes de una red a otra. Funcionamiento similar a una Puerta de Enlace (*Gateway*) y en determinadas circunstancias puede ser usado para conectar, y compartir, la conexión de varios ordenadores de una red local a una misma cuenta de acceso de Internet. Amplíe la información leyendo [Conexión compartida de Internet](#) y [Proxy](#).

***Script**

Ver [Guiones](#).

Sector de inicio

Boot sector

El sector de inicio, contiene información sobre el disco lógico, y el programa para cargar el sistema operativo en la memoria y ejecutarlo. Está ubicado en el primer sector del disco lógico.

***Secure Sockets Layer**

Ver [SSL](#).

Servidor

Es un ordenador que permite el acceso y entrega información a otro ordenador ubicado en forma remota, al que se denomina Cliente.

***Servidor Proxy**

Ver [Proxy](#).

SMB

Service Message Block

Bloque del servicio de mensaje

SMB es un método para compartir archivos de red que son usados mediante el protocolo NetBIOS.

SMB trabaja principalmente a través de series de peticiones de un ordenador cliente y de un servidor que responde. En prácticamente todas las versiones de Windows existen aplicaciones cliente y servidor SMB.

Socket

Es un dispositivo que permite la conexión entre dos equipos a través de la dirección IP del servidor y un número de puerto.

Por ejemplo: el servidor escucha las peticiones en un puerto y cuando las peticiones del cliente arriban, el servidor otorga un dispositivo -Socket- para concretar la operación.

SSL

Secure Sockets Layer

Capa segura en dispositivos de transporte de datos

Es un protocolo diseñado para soportar acceso seguro a servidores de Internet y permitir el intercambio de datos utilizando criptografía, entre dichos servidores y ordenadores cliente.

***Stateful Inspection**

Ver [Inspección dinámica de paquetes](#).

SYS

Los archivos con extensión .SYS generalmente contienen un controlador del sistema. Los mismos son cargados en la memoria durante el inicio del sistema operativo.

***System tray**

Ver [Barra de sistema](#).

***Stealth mode**

Ver [Modo oculto](#).

***Task bar**

Ver [Barra de tareas](#).

TCP

Transmission Control Protocol

Protocolo de control de transmisión

El mayor protocolo de transporte de datos en red y en Internet, asegurando una distribución confiable ya que retransmite los datos si fuera necesario.

Tecnologías de seguimiento pasivo

Tecnologías utilizadas para controlar el comportamiento del usuario o reunir información acerca del mismo, algunas veces incluyendo información personal o confidencial.

Tecnología subyacente

Una de las tecnologías listadas en la tabla anterior, que ha sido utilizada para perjudicar a los usuarios. Sin embargo, con aviso, consentimiento y control adecuado, estas mismas tecnologías podrían brindar un beneficio a los consumidores.

Telnet

Terminal emulation protocol of TCP/IP

Protocolo para la emulación de terminal mediante TCP/IP

Protocolo que permite operar un ordenador remoto como una terminal distante a través de Internet, vinculando distintas herramientas como navegadores, bases de datos, carpetas y una amplia gama de recursos.

*Terminal emulation protocol of TCP/IP

Ver [Telnet](#).

*Transmission Control Protocol

Ver [TCP](#).

UDP

User Datagram Protocol

Protocolo de datagrama de usuario

Es un protocolo que provee herramientas simples de bajo nivel para la transmisión y recepción de paquetes de red directamente a las aplicaciones.

El protocolo UDP no controla la transferencia de datos y no define la correlación entre los mensajes individuales recibidos y los enviados.

Dado que UDP no garantiza una transferencia confiable, las aplicaciones que usan este protocolo numeran cada paquete y, si es necesario, inician la retransmisión de los mismos. Todas las aplicaciones que requieren difundir (*broadcast*) o agrupar funciones en conexiones IP debería operar sólo con el protocolo UDP.

*Uniform Resource Locator

Ver [URL](#).

*Universal Resource Locator

Ver [URL](#).

URL

Uniform Resource Locator

Localizador uniforme de recursos

Anteriormente: *Universal Resource Locator*

Localizador universal de recursos

Es la dirección de un recurso de Internet, como un sitio, una página o un archivo entre otras posibilidades.

Una URL está compuesta por un conjunto de elementos que definen protocolo y ubicación entre otros, ordenados de una forma determinado y según una estructura jerárquica establecida:

[Protocolo]://[Servidor][:Puerto]

- **Protocolo**

Nombre del protocolo utilizado para establecer la comunicación: http, ftp, etc.

Si no se indica, el navegador asume que es http.

Después del nombre del protocolo se inserta "://".

Ejemplo: [http://](#)

- **Servidor**

Se indica la dirección IP o DNS (o nombre de dominio).

Ejemplo

- Dirección IP: **67.15.68.49**
- Dirección DNS: **www.outpost-es.com**

- **Puerto**

Es un parámetro opcional, si no se indica, el navegador asume que es el puerto 80 para una conexión HTTP y 23 para una conexión FTP.

Se debe escribir ":" antes del número de puerto.

Ejemplo: **:80**

- o **Ruta**

Es la ubicación de la página que se ha de acceder.

Si no se indica, el navegador asume que es la página principal, siendo habitualmente index.html.

Antes de la ruta, se debe anteponer el signo "/".

Ejemplo: **/outpost/features/otros/benefitspro.html**

Diversos ejemplos:

- <http://www.outpost-es.com:80/pressroom/index.html>
- <http://www.outpost-es.com/pressroom/index.html>
- <http://67.15.68.49:80/pressroom/index.html>
- <http://67.15.68.49/pressroom/index.html>
- <http://www.outpost-es.com>

***User Datagram Protocol**

Ver [UDP](#).

Usuario

Propietario del sistema o administrador designado.

En un sistema hogareño, comúnmente es cada persona que opera el ordenador.

VBScript

Visual Basic Script

Es un programa desarrollado como un subconjunto del lenguaje Visual Basic, sólo apto para plataformas Windows, y que se integra dentro de páginas HTML con el objetivo de mejorar la navegabilidad e interacción con el usuario.

***Visual Basic Script**

Ver [VBScript](#).

Verificador de puertos

Programa de análisis de seguridad, utilizado para descubrir los servicios de redes de ordenadores que brinda un sistema remoto.

La verificación de puertos indica dónde explorar en busca de una debilidad.

***WAN**

Wide Area Network

Ver [Red de área extendida](#).

***Web**

Ver [World Wide Web](#).

***Wide Area Network**

Ver [Red de área extendida](#).

WiFi

Wireless Fidelity

Conexión inalámbrica de alta fidelidad

[Red de área local](#) conectada por ondas de radio de alta frecuencia que permite comunicaciones flexibles entre ordenadores y/o dispositivos compatibles.

La falta de conexión por medios físicos (como cables) presenta altos riesgos de seguridad y potenciales infiltraciones que pudieran permitir fuga de información, invasión a la privacidad, etc.

Los equipos que utilizan este tipo de conexiones requieren sistemas muy robustos de protección.

Wireless

Conexión inalámbrica

Conexión entre distintos ordenadores o variados dispositivos compatibles utilizando ondas de radio en vez de medios físicos.

World Wide Web

También se la conoce por su acrónimo "www" o directamente como Web.

Red mundial de documentos HTML interconectados entre sí y distribuidos entre servidores en el mundo entero.

Es un subconjunto perteneciente a Internet, que tiene como principal característica la de permitir hipervínculos entre las páginas, accediendo a través del protocolo HTTP, así como la posibilidad de visualizar imágenes y transmitir sonidos, permitiendo, con el desarrollo de nuevas tecnologías, la presencia de contenido interactivo y/o dinámico.

Para acceder a visualizar las páginas Web es necesario contar con un navegador compatible.

***www**

Ver [World Wide Web](#)