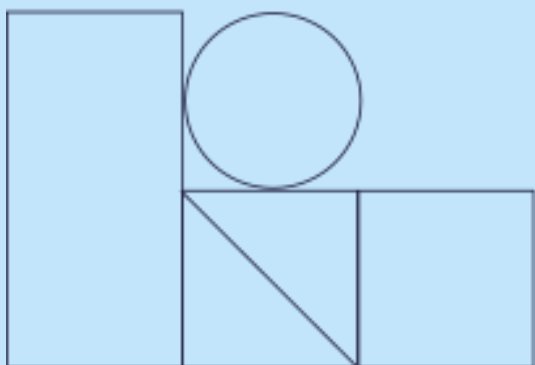


Fundamentos de Internet

El DNS y su funcionamiento

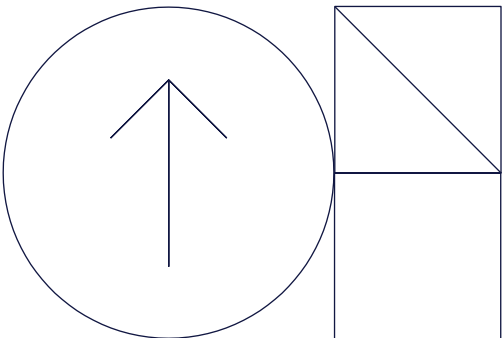


Índice

Introducción	3
¿Qué es el DNS?	4
El servidor DNS	5
Peticiones al DNS	6
Historia del servidor DNS	6
Las partes de un dominio	6
Qué significa “el servidor DNS no responde”	7

En este módulo vamos a conocer los principales conceptos y términos que debemos conocer.

Además, analizaremos cómo funcionan las redes y el funcionamiento de la Web.



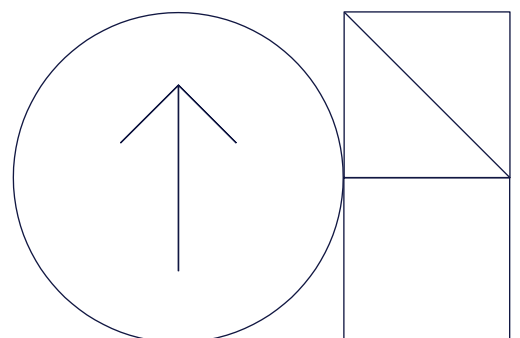
Introducción

El DNS es un sistema que contiene una lista de nombres de dominios que les permite a los usuarios encontrar una página en particular. Es fundamental para el funcionamiento de Internet, optimizar el desempeño de un sitio web y mejorar su seguridad.

El sistema DNS es crucial para la comunicación de sitios web en Internet. Cualquier estrategia que implique expansión en el entorno digital debe considerar este concepto, su configuración y sus implicaciones.

Es necesario comprender, por ejemplo, la relación entre DNS, la seguridad y el desempeño de un sitio web para poder mejorar los resultados.

Todos los navegantes usan el DNS a diario y funciona tan rápido que puede pasar desapercibido. Entonces, ¿cómo el DNS estructura exactamente la red?

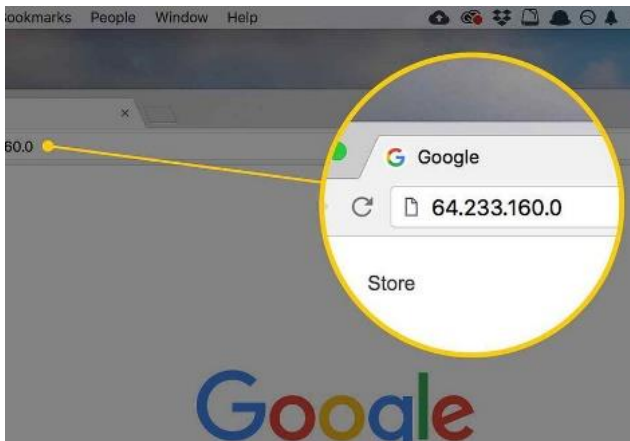


¿Qué es el DNS?

DNS es la sigla en inglés de **Domain Name System**, que en español significa Sistema de Nombres de Dominio. Como su nombre lo indica, es un registro que contiene nombres de sitios web y direcciones IP asociadas.

Esta correlación favorece la transferencia de datos entre computadoras y permite el acceso a Internet. Cuando entramos en *https://www.google.com* no solemos percatarnos de una realidad: tras el nombre del dominio se esconde otro nombre en clave, una IP que, gracias a las DNS, no tenemos que andar memorizando.

Eso sí, las DNS no son únicamente unas direcciones que sirven para conectar el servidor con los

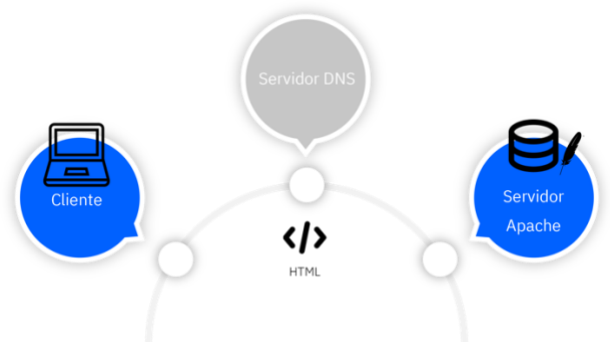


resultados que vemos en nuestro navegador. Son una de las herramientas clave que hacen funcionar internet.

Las DNS son un sistema jerárquico que se ocupa de administrar los nombres de dominio. Una especie de base de datos y traductor para que, en vez de leer la IP 172.11.122.45 —un número asociado a la máquina donde está alojado el dominio—, leamos miweb.com, algo legible y fácil de recordar.

Cuando entramos en cualquier navegador (Firefox, Chrome, Edge, etc.), este mantiene una conversación con el servidor DNS. Le pregunta cuál es la IP del dominio, coteja que esa información cuadra con la información correspondiente a ese nombre de dominio y le da al navegador una IP.

Con esa información, nuestro navegador nos muestra la página web correspondiente. Y ya está, es un trámite sencillo, rápido y seguro en el que intervienen tres elementos:



Cliente DNS: el que realiza peticiones de resolución de nombres.

Servidor DNS: los que contestan, resolviendo la petición mediante un sistema de árbol. Cuando configuramos nuestra conexión a internet por primera vez —la mayoría de las ocasiones las DNS vienen asignadas de forma automática—, estamos marcando las direcciones de los servidores DNS.

Zonas de autoridad: o, lo que es lo mismo, los servidores, responsables de resolver el dominio que estamos solicitando.

El servidor DNS

Los servidores son software, distintas herramientas que acuden a la base de datos del DNS para responder a las peticiones. La gran mayoría de nombres de dominios se alojan en un host concreto, así que es común confundir o llamar de la misma manera al servidor que aloja estas herramientas.

Así que para aclarar un poco las cosas vamos a profundizar en los tipos de servidor DNS:

Primario o maestro: aquel que guarda la información de los distintos nombres de dominio en su propia base de datos.

Secundario o esclavo: si un servidor DNS acude a otro, este se convierte automáticamente en secundario, ya que está tomando la información de segunda mano

Peticiones al DNS

Para conocer en mayor profundidad cómo navegamos, esta es la ruta que sigue la información de un simple dominio web:

1. Buscamos www.google.com en una página web en blanco. Así comienza una nueva petición.
2. El servidor DNS busca dentro de un filehost el archivo de texto plano que mapea los nombres. Lo hace acudiendo a nuestra ISP (proveedor de servicios de internet), aunque a veces sólo necesita acudir a la caché del navegador. La petición será dirigida, de forma automática, al servidor DNS que corresponda.
3. Si la info no está en la caché, la información se coteja con otro servidor y desde aquí se envía la IP correspondiente, lo que se conoce como forward lookup, es decir, “resolución recursiva”. Pero también existe otra forma de resolver el entuerto, mediante resolución iterativa, la vía inversa: el servidor DNS no puede resolver la petición, así que envía la petición al siguiente servidor de esta jerarquía. Ahora es el nuevo servidor el que debe enviar una nueva petición y repetir el proceso hasta que el nombre de dominio haya quedado resuelto. En resumen, si algo no encaja en la IP solicitada, el servidor DNS responsable acude al servidor DNS raíz, que está en un nivel más alto dentro de la jerarquía. Nosotros, como usuarios, ni tenemos que hacer nada ni percibimos cambios en esta transmisión de información.
4. Ahora el servidor acude a otro servidor más, porque el dominio .com forma parte de los dominios de nivel superior (TDL o Top-level domains). Este resolutor acudirá al Servidor de Nombres Autorizado que cuenta con toda la información del dominio y autoriza su consulta, lo que en la práctica se traduce como un acceso al servidor web.
5. Ya estamos dentro. La petición al DNS ha sido resuelta correctamente.

Historia del servidor DNS

Tendríamos que viajar al invierno de 1968. Hace un momento has leído “archivo de texto”. El primer archivo de texto plano de la historia se llamaba HOSTS.TXT y servía para asignar a cada nombre de host una IP de cada ordenador de Arpanet, la primera red de ordenadores interconectados online, el primer internet.

En Stanford, la informática Elizabeth Feinler fue la responsable de crear este directorio, mientras que en la Universidad del Sur de California era Jon Postel quien gestionaba el manteniendo de esta red. Así es, cada dirección fue asignada de forma manual, una a una. ¿Imaginas algo así en el mundo actual, con casi 6.000 millones de páginas web indexadas sólo en el internet público?

Con las especificaciones DNS establecidas, no fue hasta 1984, tras la conversión de Arpanet en una red gigantesca que interconectaba las principales universidades del país, cuando cuatro estudiantes de UC Berkeley recurrieron a BIND, un servidor de nombres Unix. BIND fue la base para la gran mayoría de software DNS utilizado en la actualidad.

Las partes de un dominio

Anteriormente avanzábamos que las DNS eran un elemento crucial en el esquema de Internet, un engranaje clave en su operatividad. Esto es porque, en todo dominio, están las DNS. Estas son las partes habituales en cualquier dominio:

- Protocolo de transferencia. Ejemplo: **http:**
- Subdominio. Ejemplo: **www**
- Dominio de primer nivel (TDL). Ejemplo: **Google**
- Dominio de segundo nivel (SDL): la terminación de dominios de nivel superior genéricos. Ejemplo: **.com**
- Uno o más subdominios o extensiones (ejemplo: miweb.com.cat; la parte “**.com.cat**” sería la extensión)

Además de estas secciones podría haber más, como rutas de páginas web, carpetas a directorios concretos o etiquetados de páginas, como por ejemplo <https://www.google.es/#cosas>

Qué significa “el servidor DNS no responde”

Pero la comunicación no siempre será fructífera. Cuando aparece la notificación de error “El servidor DNS no responde” significa que hay **un problema de conexión**, ya sea porque no se puede acceder a la información del servidor, a la web (porque esté temporalmente suspendida o caída) o quizá porque no tenemos acceso a internet. Sin respuesta no podremos acceder a la web. Por suerte, este es un problema con sencilla solución.

La primera solución es la más obvia: **reiniciar el router**. Aunque podemos hacerlo pulsando el botón de encendido y apagado, recomendamos desconectar el cable que lo enchufa a la corriente, esperar cinco segundos y volver a enchufar. Esto no borrará nuestros datos —como el nombre o ID del **wifi**. No reestablecerá al modo de fábrica el dispositivo, simplemente forzará una reconexión.

Y si el problema no es del router, puede ser del PC. Podemos finalizar todas las tareas y reiniciar el PC para comprobar si ahora funciona la conexión. También podemos cambiar de navegador, abrir red privada desde una pestaña de incógnito, desactivar temporalmente el firewall o limpiar la caché DNS tecleando “flushdns” desde el buscador de Windows.

- En Windows vamos a **Inicio**.
- Conexiones de Red o Abrir el Centro de redes y recursos compartidos.

- Ethernet o wifi, dependiendo de nuestra conexión y bajamos hasta Cambiar configuración del adaptador.
- Con click derecho sobre la conexión, pulsamos en Propiedades.
- Ahora tendremos que hacer clic sobre **Protocolo de Internet Versión 4 (TCP/IPv4)**
- Otra vez clic sobre Propiedades y luego en **Usar la siguiente dirección de servidor DNS**.
- En el espacio designado al servidor DNS preferido escribimos 8.8.8.8 y 8.8.4.4 como servidor DNS alternativo..
- Pulsamos aceptar y esperamos hasta que los cambios hayan sido aplicados. Se recomienda reiniciar el PC.

Por su parte, en MacOS:

- Desde el escritorio abrimos **Preferencias del sistema**.
- Buscamos el icono de Conexión de Red (una esfera azul).
- Clicamos con el botón derecho y pulsamos sobre la opción Abrir el panel de preferencias Red.
- Dentro de Ethernet vamos al recuadro que pone **Avanzado**.
- Ahora vamos hasta la tercera pestaña, la que indica DNS. Vamos a la opción + y hacemos clic.
- Borramos los campos con las DNS que haya y escribimos las nuevas, **8.8.8.8 y 8.8.4.4**. No debemos olvidar escribir los puntos correctamente.
- Pulsamos **Aplicar y Aceptar**, las dos opciones, y esperamos a que se actualicen, momento en el que ya podremos navegar con las nuevas