**Resumen Sistema de Nombres de Dominio DNS**

**Definición**

Es la forma en que los nombres de dominio de internet se encuentran y se traducen a direcciones de protocolo de internet (IP).

El Sistema de Nombres de Dominio (Domain Name System o DNS, por sus siglas en inglés) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes.

**¿Cómo surgió?**

Para llegar a la denominación DNS se tuvieron que implementar de forma escalada un tipo de reglas escritas llamadas RFC’s que contienen información sobre los procedimientos de internet(normas).

Ante la expansión de la red, se hizo imposible recordar todas las direcciones IP de los equipos.

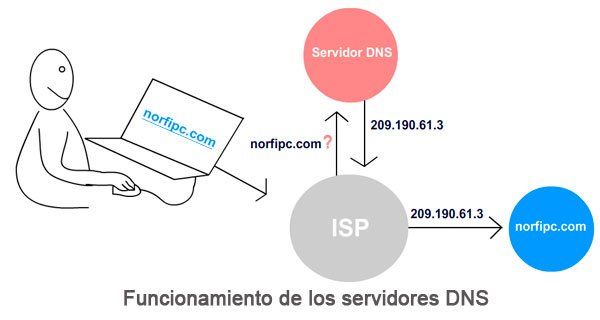
Concretamente en noviembre de 1983 el Grupo de Trabajo de Ingeniería de Internet publicaron los RFC’s 1034 y 1035 donde se estandariza el DNS.

**Uso principal**

Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS.

Por ejemplo, si la dirección IP del sitio Google es 216.58.210.163, la mayoría de la gente llega a este equipo especificando www.google.com y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable.



El proveedor de servicios de Internet, (ISP, por la [sigla](https://es.wikipedia.org/wiki/Sigla) en [inglés](https://es.wikipedia.org/wiki/Idioma_ingl%C3%A9s) de Internet service provider) es la [empresa](https://es.wikipedia.org/wiki/Empresa) que brinda [conexión a Internet](https://es.wikipedia.org/wiki/Conexi%C3%B3n_a_Internet) a sus clientes. Un ISP conecta a sus usuarios a [Internet](https://es.wikipedia.org/wiki/Internet) a través de diferentes tecnologías como [ADSL](https://es.wikipedia.org/wiki/L%C3%ADnea_de_abonado_digital), [cable módem](https://es.wikipedia.org/wiki/Cablem%C3%B3dem), [GSM](https://es.wikipedia.org/wiki/GSM), [dial-up](https://es.wikipedia.org/wiki/Dial-up), etc.

**Componentes**

Para la operación práctica del sistema DNS se utilizan 3 componentes:

Los clientes fase 1: un programa cliente DNS que se ejecuta en la computadora del usuario y genera peticiones DNS.

Los servidores DNS: contestan peticiones de los clientes, tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

Las zonas de autoridad: es una parte del espacio de nombre de dominios sobre la que es responsable un servidor DNS que puede tener autoridad sobre varias zonas.

**Entendiendo las partes de un nombre de dominio**

Un [nombre de dominio](https://es.wikipedia.org/wiki/Dominio_de_Internet) usualmente consiste en dos o más partes ( «etiquetas»), separadas por puntos cuando se las escribe en forma de texto. Por ejemplo, www.ejemplo.com o es.wikipedia.org

A la etiqueta ubicada más a la derecha se le llama dominio de nivel superior. Como com en www.ejemplo.com u org en es.wikipedia.org

Cada etiqueta a la izquierda especifica una subdivisión o subdominio. En teoría, esta subdivisión puede tener hasta 127 niveles, y cada etiqueta puede contener hasta 63 caracteres, pero restringidos a que la longitud total del nombre del dominio no exceda los 255 caracteres, aunque en la práctica los dominios son casi siempre mucho más cortos.

Finalmente, la parte más a la izquierda del dominio suele expresar el [nombre de la máquina](https://es.wikipedia.org/wiki/Nombre_de_equipo) (hostname). El resto del nombre de dominio simplemente especifica la manera de crear una ruta lógica a la información requerida. Por ejemplo, el dominio es.wikipedia.org tendría el nombre de la máquina "es", aunque en este caso no se refiere a una máquina física en particular.

El DNS consiste en un conjunto jerárquico de servidores DNS. Cada dominio o subdominio tiene una o más zonas de autoridad que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido. La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios.

**Jerarquía DNS**

El espacio de nombres de dominio tiene una [estructura arborescente](https://es.wikipedia.org/wiki/Topolog%C3%ADa_arb%C3%B3rea).

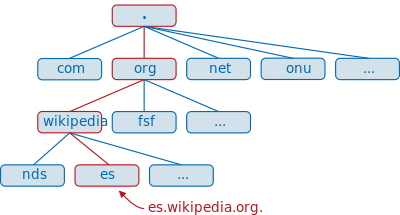
Las hojas y los nodos del árbol se utilizan como etiquetas de los medios. Un nombre de dominio completo de un objeto consiste en la concatenación de todas las etiquetas de un camino.

Un nombre de dominio termina con un punto (aunque este último punto generalmente se omite). Un nombre de dominio correctamente formado, es por ejemplo este: www.ejemplo.com. (Incluyendo el punto al final).

Un nombre de dominio debe incluir todos los puntos y tiene una longitud máxima de 255 caracteres.

Un nombre de dominio se escribe siempre de derecha a izquierda. El punto en el extremo derecho de un nombre de dominio separa la etiqueta raíz de la jerarquía. Este primer nivel es también conocido como dominio de nivel superior.

Los objetos de un dominio DNS (por ejemplo, el nombre del equipo) se registran en un archivo de zona, ubicado en uno o más servidores de nombres.



**Tipos de servidores DNS**

Primario o maestros: guardan los datos de un espacio de nombres en sus ficheros.

Secundarios o esclavos: obtienen los datos de los servidores primarios a través de una transferencia de zona.

Locales o caché: cuando se les realiza una consulta estos a su vez consultan a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la repetición de estas peticiones en el futuro continuo o libre.

**Tipos de resolución de nombres de dominio**

El proceso de resolución normal se lleva a cabo de la siguiente manera:

El servidor DNS local recibe una consulta recursiva desde el resolver del host cliente.

El DNS local realiza las consultas iterativas a los servidores correspondientes.

El servidor DNS local entrega la resolución al host que solicitó la información.

El resolver del host cliente entrega la respuesta a la aplicación correspondiente.

**Temas de seguridad**

La expansión de Internet en el sector comercial en los 90s cambió los requisitos de las medidas de seguridad para proteger la integridad de los datos y la [autenticación](https://es.wikipedia.org/wiki/Autenticaci%C3%B3n) de los usuarios.

Muchos temas de vulnerabilidades fueron descubiertos y explotados por usuarios maliciosos. Uno de esos temas es el [envenenamiento de caché DNS](https://es.wikipedia.org/wiki/Envenenamiento_de_cach%C3%A9_DNS), en la cual los datos son distribuidos a los resolvedores de caché bajo el pretexto de ser un servidor de autoridad de origen, contaminando así el almacenamiento de datos con información potencialmente falsa y largos tiempos de expiración.

Las respuestas DNS tradicionalmente no estaban firmadas [criptográficamente](https://es.wikipedia.org/wiki/Criptograf%C3%ADa), permitiendo muchas posibilidades de ataque; las [extensiones de seguridad del DNS](https://es.wikipedia.org/wiki/Domain_Name_System_Security_Extensions) (DNSSEC) modifican el DNS para agregar la posibilidad de tener respuestas firmadas criptográficamente

[DNSCurve](https://es.wikipedia.org/wiki/DNSCurve) ha sido propuesto como una alternativa a DNSSEC. Otras extensiones, como [TSIG](https://es.wikipedia.org/w/index.php?title=TSIG&action=edit&redlink=1), agregan soporte para autenticación criptográfica entre pares de confianza y se usan comúnmente para autorizar transferencias de zona u operaciones dinámicas de actualización.

Algunos nombres de dominio pueden ser usados para conseguir efectos de engaño. Por ejemplo, paypal.com y paypa1.com son nombres diferentes, pero puede que los usuarios no puedan distinguir la diferencia dependiendo del tipo de letra que estén usando.

Este problema es grave en sistemas que permiten nombres de dominio internacionalizados, ya que muchos caracteres en [ISO 10646](https://es.wikipedia.org/wiki/ISO_10646) pueden aparecer idénticos en las pantallas típicas de computador. Esta vulnerabilidad se explota ocasionalmente en [phishing](https://es.wikipedia.org/wiki/Phishing).

Técnicas como el [FDNS inverso con confirmación adelantada](https://es.wikipedia.org/wiki/Forward_confirmed_reverse_DNS) pueden también usarse para validar los resultados de DNS.

**Tipos de registro DNS**

Los tipos de registros más utilizados son:

A = Dirección (address). Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.

AAAA = Dirección (address). Este registro se usa en [IPv6](https://es.wikipedia.org/wiki/IPv6) para traducir nombres de hosts a [direcciones IPv6](https://es.wikipedia.org/wiki/Direcci%C3%B3n_IPv6).

CNAME = Nombre canónico (canonical Name). Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio.

NS = [Servidor de nombres](https://es.wikipedia.org/wiki/Servidor_de_nombres) (name server). Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio.

[MX](https://es.wikipedia.org/wiki/MX_(registro)) = Intercambio de correo (mail exchange). Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

PTR = Indicador (pointer). También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.

SOA = Autoridad de la zona (start of authority). Proporciona información sobre el servidor DNS primario de la zona.

SRV = Service record (SRV record).

ANY = Toda la información de todos los tipos que exista. (No es un tipo de registro, sino un tipo de consulta)

