# DNS

## Servicio DNS

El DNS es una base de datos distribuida y jerárquica que gestiona y mantiene información asociada a nombres de dominio en redes como Internet. Su uso más común es la asignación de nombre de dominio a direcciones IP de los nodos de Internet y la localización de los servidores de correo electrónico de cada dominio. DNS permite traducir los nombres de dominio (campus.upc.edu) a sus respectivas direcciones IP (82.223.162.102).

Cuando queramos acceder a una maquina (Web, FTP, Telnet, etc.) en vez de recordar su IP, basta con recordar el nombre del servidor. DNS permite recordar fácilmente los nombres de todos los servidores conectados a Internet. El nombre es más fiable. La dirección numérica podría cambiar por muchas razones, pero no el nombre que identifica el servidor.

## Historia DNS

En un inicio, SRI (ahora SRI International) alojaba un archivo llamado HOSTS que contenía todos los nombres de dominio conocidos (la mayoría de los sistemas operativos actuales todavía pueden ser configurados para revisar su archivo hosts). El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo HOSTS no resultara práctico. EN 1983 apareció el primer sistema DNS, el cual ha ido evolucionando hasta el DNS moderno.

## Características básicas DNS

Es una base de datos jerárquica que contiene asociaciones de nombres de dominios a IP. Está formada por un conjunto de servidores distribuidos por todo Internet, en lugar de mantenerla centralizada en un único servidor. Sigue el paradigma cliente/servidor con nivel de transporte TCP/UDP y puerto 53. Usa un resolver que permite realizar las consultas a la BBDD. Utiliza un protocolo para intercambiar información de nombres.

## DNS en Windows

**C:\Windows\System32\drivers\etc** Este archivo contiene las asignaciones de las direcciones IP a los nombres de host. Cada entrada debe permanecer en una línea individual. La dirección IP debe ponerse en la primera columna, seguida del nombre de host correspondiente. La dirección IP y el nombre de host deben separarse con al menos un espacio.

**EJ: 127.0.0.1 localhost**

## DNS en Linux

Las aplicaciones que acceden al sistema DNS consultan inicialmente el fichero **/etc/hosts** donde está la correspondencia nombre-IP. Si no puede resolver el nombre, entonces intenta contactar con un servidor DNS. EN el fichero **/etc/resolv.conf** se guarda la IP de los servidores DNS primario y secundario y el dominio local.

| Example# cat /etc/hosts | Example# cat /etc/resolv.conf |
|---|---|
| 127.0.0.0 localhost | domain uu.vi.com |
| 201.24.31.87 pc1.uu.vi.com pc1 | nameserver 201.24.31.3 |
| 201.24.31.105 pc2.uu.vi.com pc2 | nameserver 201.24.31.4 |
| 201.24.31.105 pc3.uu.vi.com pc3 | |

## Jerarquía de dominios DNS

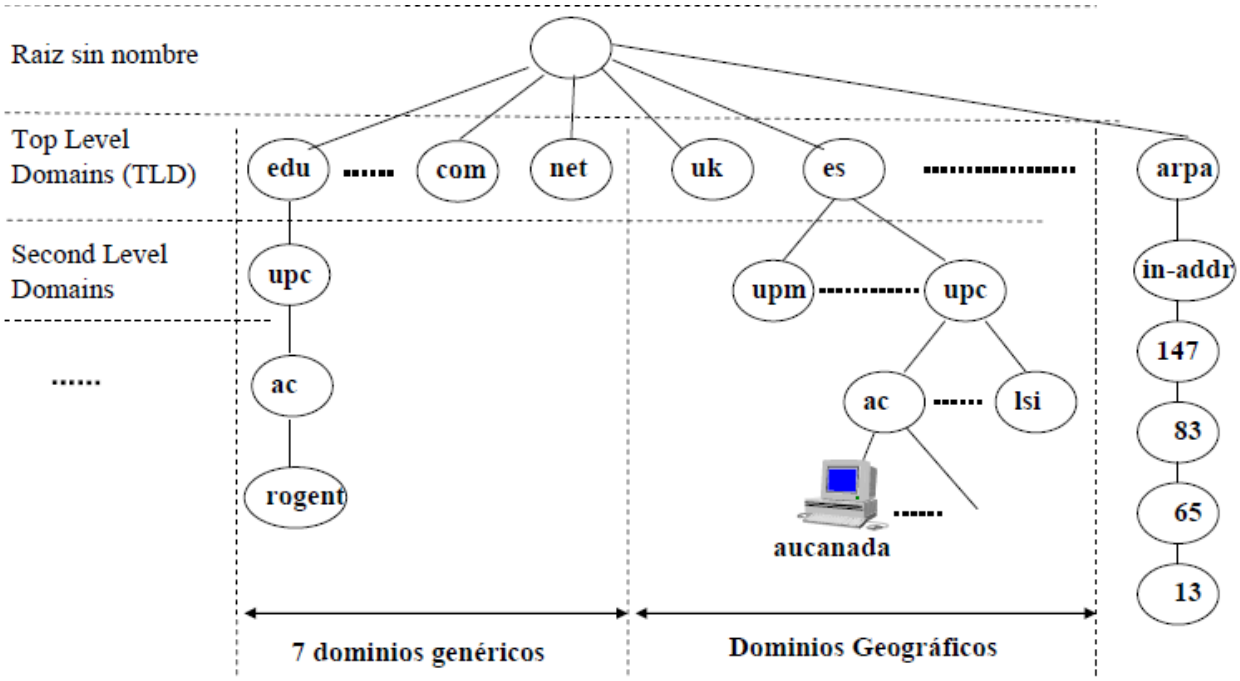
La jerarquía de DNS está organizada en dominios o zonas. Un dominio es un mecanismo de identificación utilizado en Internet. Es una rama en un árbol invertido llamado **espacio de nombre de dominio.** Un nombre de dominio consiste en dos o más etiquetas, separadas por puntos (formato texto)

- **host…subdominio1.dominio.TLD =>** Dominio de nivel superior (Parte final de un dominio de Internet)
- **rogent.ac.upc.edu => FQDN (Fully Qualified Domain Name)** Cuando el nombre incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo.

Cada etiqueta a la izquierda especifica una subdivisión o subdominio. El dominio y subdominio indican un conjunto de nombre que identifican a la organización:

- **ac.upc** designa el departamento de Arquitectura de Computadores de la UPC.

La parte más a la izquierda del dominio suele expresar el nombre de la máquina. Las empresas deben registrar su nombre para que pase a ser su marca en Internet (problemas con marcas ya registradas)




- **Dominio raíz sin nombre**

Los servidores raíz se encuentran al inicio de la jerarquía. Son los que responden cuando se busca resolver un dominio de 1º y 2º nivel. Actualmente está formado por 13 servidores root-servers que tienen las direcciones de los TLD (Top Level Domains):

a.root-server.net
b.root-server.net
.
.
m.root-server.net

.
Están distribuidos por todo el mundo.

- **Top Level Domain (TLD)**

La IANA clasifica los TLDs en 3 clases de dominios:

1) 7 dominios genéricos

| | |
|---|---|
| .com -> comercial | .int -> org. International |
| .mil -> militar | .org -> org. no gubernamental |
| .edu -> educación | .gov -> Institución gubernamental |
| .net -> centros de soporte de red | |

Propuesta (de CORE) para ampliar el numero de dominios genéricos: **.firm**, .**shop**, **.info**, **.web**, **.nom**, **.arts**, **.rec**

2) Dominios geográficos por países: **.es**, **.fr**, **.uk**, **.it**, etc.

3) 1 dominio de infraestructura: **.arpa**. Permite la resolución inversa de direcciones. Cada servidor gestiona una rama que comienza con la etiqueta **in-addr** de la que cuelgan las direcciones en sentido numérico inverso: **IP 147.83.65.13** estaría como **13.65.83.147.in-addr.arpa**

- **Second Level Domain (SLD)**

Cada uno de los TLD tiene un administrador (registrar en el argot DNS) que delega parte de su dominio en subdominios secundarios.

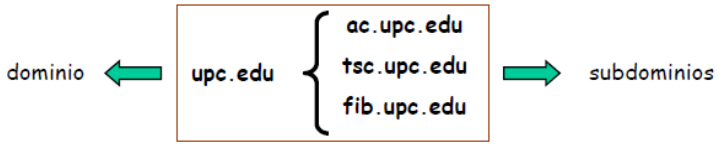
**Ejemplo**: campus.upc.edu

**campus:** Nombre de la maquina dentro del dominio de upc
**upc:** De com cuelga el dominio de nivel secundario upc, cuya administración está delegada al centro upc
**edu:** com es el TLD de comercial

## Dominio y zonas DNS

El dominio es un subárbol del espacio de nombres de dominio, es decir, un nodo con todos los nodos por debajo de él. El dominio contiene máquinas y otros dominios llamados subdominios.

La zona es un archivo que contiene ciertos registros de la BBDD del espacio de nombres de dominio, que pueden identificar a un dominio o más y permiten atender las peticiones de los clientes




## Zonas de autoridad DNS

Un servidor DNS almacena información acerca de algunas partes del espacio de nombres del dominio. Cada una de esas partes se llama **zona**. Se dice el servidor DNS tiene **autoridad sobre la zona**. 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. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos no han sido delegados a otras zonas de autoridad.

## Delegación de autoridad

La división de un dominio en subdominios no implica siempre la cesión de la autoridad sobre ellos. En principio un dominio puede mantener la autoridad sobre ellos. Pero también puede, si así lo decide delegar la autoridad de alguno/s de sus subdominios. Se define un **servidor de nombres de dominio DNS autoritario** para una zona como aquel que contiene los registros para dicha zona. Para ello se utilizan los registros de recursos SOA y NS.

## Servidores DNS

Los servidores de nombres se pueden clasificar en:

- Servidor primario (Primary name)
- Servidor secundario (Secondary name)
- Servidor caché (solamente)
- **Transferencia de la zona**

Es un proceso mediante el cual se obtiene información actualizada de la zona por medio de la red. Cada administrador de sistemas de una zona (dominio o subdominio) es responsable de:

- Mantener un servidor primario (disk file), que tiene la inforamcion de una zona y la autoridad sobre ella.
- Mantener uno o varios servidores de DNS secundarios (backups) independientes del primario pero que obtienen la información a partir de él.

Son servidores conocidos como **authority** del dominio. la información nueva {@IP, nombre} se añade al primario. Los secundarios la obtendrán ya que hacen **querys** del primario cada 2/3 horas. En estos servidores han de estar los nombres de los hosts que cuelgan de su dominio y el nombre y dirección de los servidores primarios y secundarios de las autoridades de los subdominios que haya delegado. Si la información no está en el DNS de la zona, los servidores DNS deben conocer la @IP de los root-servers para acceder y obtenerla.

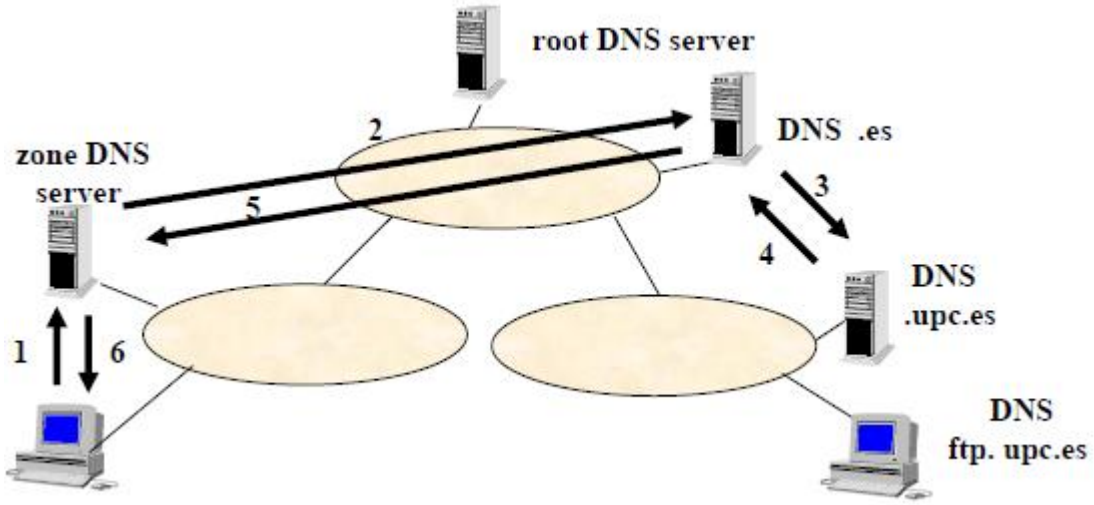
Los servidores DNS (no los resolver de la aplicación) disponen de caches para resolver nombres que han mapeado recientemente.

**Caching:** Los servidores DNS guardan en su cache las direcciones IP solicitadas un cierto tiempo indicado por TTAL (TTL típico 2 días). De esta manera, si el mismo host u otro vuelve a solicitar la resolución del mismo nombre, devolverá la dirección inmediatamente sin tener que hacer de nuevo la resolución.

## Consulta recursiva

Se realiza una petición de resolución de nombres al servidor DNS local, Si el servidor no dispone de dicha información reenvía la petición al servidor de nombres con autoridad que la contiene. De forma recursiva se buscará la información y será devuelta al cliente.

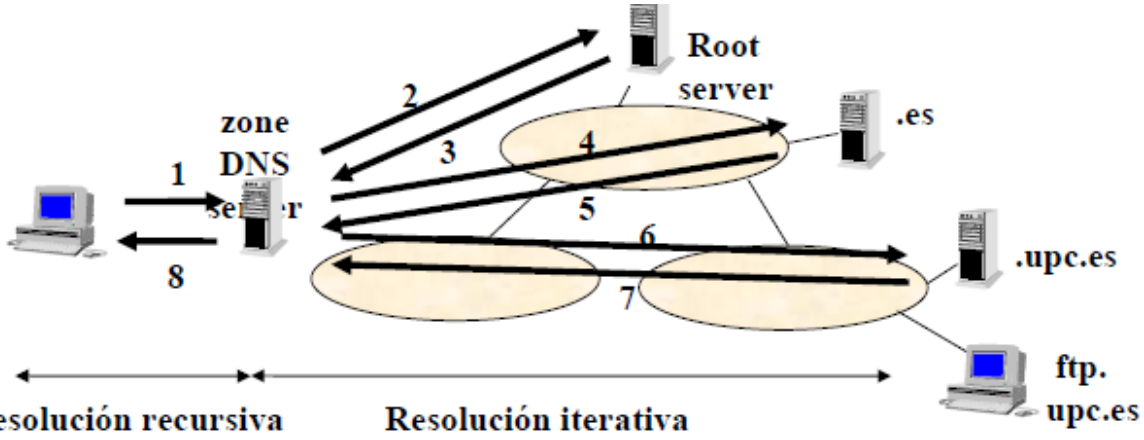
(1) Host pregunta por **ftp.upc.es** al servidor DNS de su zona (dominio)
(2) El servidor DNS de la zona pregunta al DNS server con dominio **.es**
(3) El servidor DNS **.es** pregunta al servidor DNS con dominio **.upc.es**
(4) El servidor DNS **.upc.es** le devuelve la @IP del servidor **ftp.upc.es** al dominio **.es**
(5) (6) Se devuelve la @IP del servidor **frp.upc.es** al cliente



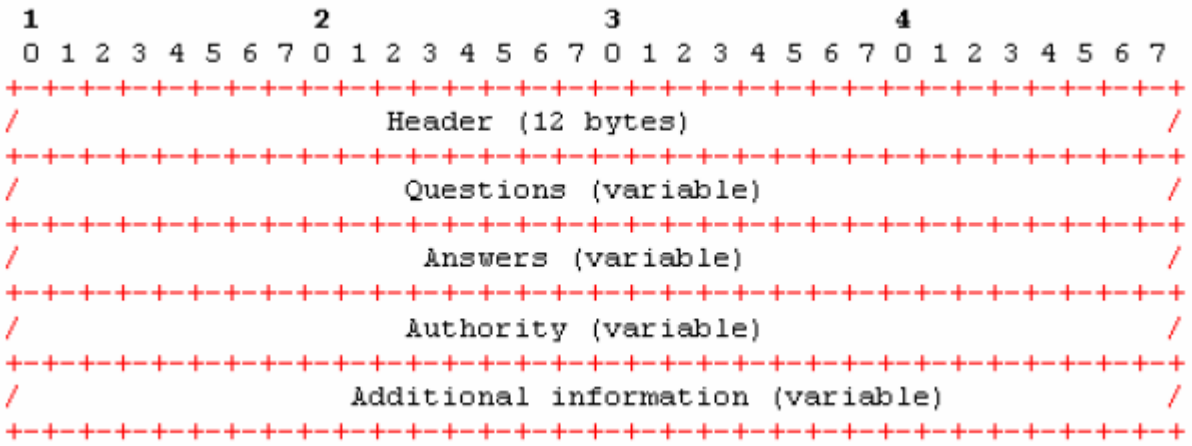
## Consulta iterativa (AKAMAI)

El servidor DNS local responde al cliente en función del contenido de su caché. Si no dispone de la información solicitada, entonces realiza una resolución iterativa: consulta iterativamente los servidores de os dominios hasta resolver la dirección buscada, comenzando siempre por un servidor raíz.

(1) Host pregunta por **ftp.upc.es** a su servidor DNS
(2) El server Zone DNS pregunta a su root server DNS
(3) El root server DNS le devuelve la @IP del servidor DNS con dominio **.es**
(4) Zone DNS pregunta al DNS **.es**
(5) DNS **.es** devuelve la @IP de DNS **.upc.es**
(6) Zone DNS pregunta a DNS **.upc.es.**
(7) DNS **.upc.es** devuelve @IP de server **ftp.upc.es**
(8) Zone DNS devuelve la @IP del server al host

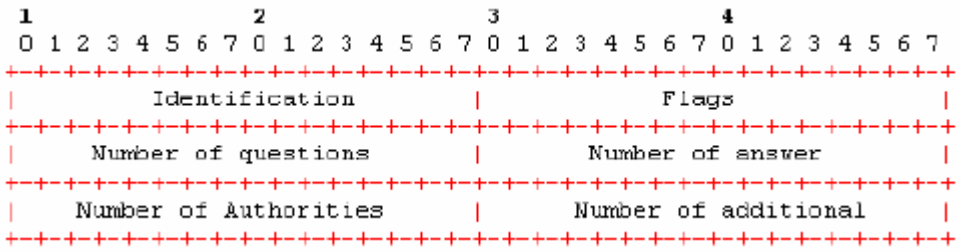



## Formato mensaje DNS




- Los campos Question, Answer, Authority y Additional son opcionales.
- **Header:** Especifica el tipo de mensaje
- **Question:** Especifica lo que se quiere resolver
- **Answer:** Especifica la respuesta
- **Authority:** Especifica el nombre de la autoridad del dominio
- **Additional:** Información adicional (típicamente, las @IP de las autoridades del dominio).

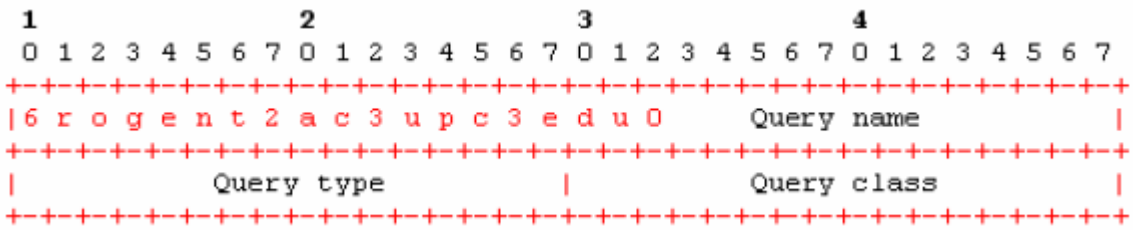
## Formato campo HEADER




- **Identification:** permite relacionar los mensajes de query (pregunta) y reply (respuesta). Es activado por el cliente y retornado por el servidor
- **16-bit flags**: Están divididos en múltiples campos. Los flags más importantes son
    - ***Flag QR (Query-Response):*** Si QR=0 mensaje de query (pregunta). Si QR=1 mensaje de reply (respuesta)
    - ***Flag AA (Authoritative Answer):*** Si AA=1 indica que ha respondido la autoridad del dominio. SI AA=0 indica que la respuesta estaba en la cache del servidor donde se ha hecho la pregunta. La respuesta no autoritativa si el DNS tiene que consultar otro DNS para obtener la respuesta. La respuesta puede ser autoritativa si el DNS tiene autoridad sobre el dominio consultado.
    - ***Flag RD (Recursion-Desired):*** Si la resolución serña recursiva o iterativa
- **Number of questions:** Nº de entradas en la sección **Questions**
- **Number of answer RRs:** Nº de entradas de la sección **Answers**
- **Number of Authority RRs:** N1 de entradas de la sección **Authority**
- **Number of additional RRs:** Nº de entradas de la sección **Additional**

## Formato campo QUESTION

Contiene las consultas al servidor de nombres. Normalmente tiene una sola cuestión.



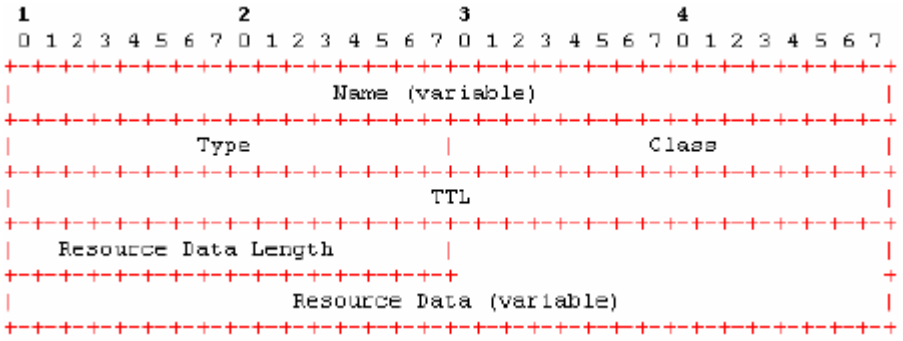

- **Query name:** Especifica el nombre que se quiere resolver. Es un campo que contiene un contador + string
- **Query type:** Especifica el tipo de pregunta. Hay hasta 20 valores diferentes
    - **Query type = 1:** Tipo A (Address) o resolución de IP a partir del nombre
    - **Query type = 2:** Tipo NS (Name Server) o resolución de un name server.
    - **Query type = 12:** Tipo PTR (Point Record) o resolución inversa (conozco la IP y quiero el nombre). Se da un nombre del tipo **7.40.45.180.in-addr.arpa**
    - **Query type = 13:** Tipo MX (Mail Exchange) para encaminar correo electrónico
- **Query class:** Especifica el tipo de dirección que se quiere resolver. En el caso de referirse a una dirección de Internet vale 1.

## Tipos de registros DNS

| Nombre del recurso | Tipo de registro | Función |
|---|---|---|
| Inicio de autoridad | SOA | Identifica al servidor autoritario de una zona y sus parámetros de configuración. |
| Servidor de nombres | NS | Identifica servidores de nombres autorizados para una zona. |
| Dirección | A | Asocia un nombre de dominio FQDN con una dirección IP. |
| Puntero | PTR | Asocia una dirección IP a un nombre de dominio FQDN. Para las búsquedas inversas. |
| Registro de correo | MX | Indica máquinas encargadas de la entrega de correo en el dominio. |
| Nombre canónico | CNAME | Permite asignar uno o más nombres a una máquina. Alias. |
| Text | TXT | Almacena cualquier información. |
| Servicio | SRV | Ubicación de los servidores para un servicio. |

## Formato de campos ANSWER, AUTHORITY

Los campos *Answer, Authority* y *Additional* están formados por secuencias de uno o más *Resource Records.* La siguiente figura muestra el formato de un RR.




- Los tres primeros campos (*Name, Type* y *Class*) tienen el mismo significado que el campo *Question.*
- **TTL (Time-to-live):** Es el número de segundos que un RR puede permanecer en la cache del cliente (normalmente 2 días)
- **Resource data lenght:** La cantidad de bytes del *Resource Data*
- **Resource data:** Depende del campo "*type*". Si Type=1 (Tipo A) es una IP y por tanto tiene 4 bytes. SI Type=2 (Tipo NS) es el nombre de la autoridad (resolución de un name server)

## Gestión de la asignación de dominios

La asignación de dominios es gestionada por la ICANN, entidad privada sin ánimo de lucro, que se encarga de dar tanto dominios genéricos como @IP. Los dominios genéricos son registrados por compañías a las que ICANN da el derecho a que actúen como tales bajo ciertas restricciones (Accredited Registrars). En España, el Ministerio de Fomento (servicio es-nic, **http://www.nic.es**) gestionado por INECO (empresa pública), se encarga del registro y asignación del dominio **.es**. En España, se puede pedir dominios a Nominalia (**http://www.nominalia.com**) o **http://interdomain.es**. La información de los administradores de los TLD se puede encontrar en **http://www.internic.net**. Internic tiene un lsitado de empresas que efectúan esta asignación. Internic es la autoridad que añade la información al DNS.