

## Guía informativa DNS



**Versión 1.1**

## Índice

<b>1. Introducción .....</b>	<b>3</b>
<b>2. Requisitos de configuración .....</b>	<b>4</b>
<b>3. Para más información .....</b>	<b>9</b>

## 1. INTRODUCCIÓN

---

Antes de que realizar la delegación o cambios en la delegación de una zona de DNS de dominios bajo “.es” mediante la aplicación de gestión de nombres de dominio accesible en la dirección web <https://www.dominios.es/>, es aconsejable que los servidores de DNS especificados estén operativos y accesibles en Internet, dando respuestas autorizadas para el dominio en cuestión y correctamente configurados de acuerdo con las normas técnicas del DNS en general y de las recogidas en este documento en particular. En caso contrario, el nombre de dominio podría presentar problemas y no estar completamente accesible en Internet.

Toda zona de DNS, tanto de segundo como de tercer nivel delegada bajo “.es”, habrá de ser mantenida y gestionada de forma técnicamente competente. Esto implica que los servidores de DNS donde esté delegada deben permanecer (al igual que lo estaban en el momento de la delegación) operativos, accesibles en Internet, dando respuestas autorizadas para el dominio en cuestión y correctamente configurados de acuerdo con las normas técnicas del DNS en general y de las recogidas en este apartado en particular.

Cualquier cambio que afecte a la delegación de un dominio bajo “.es” (alta, baja o modificación de nombre o dirección IP de servidores de DNS para el dominio) debe ser previsto y planificado con antelación suficiente y solicitado a Red.es mediante el procedimiento establecido al efecto. En caso de incompetencia o negligencia técnica, un dominio de DNS registrado y delegado bajo “.es” podría ser dado de baja de forma temporal o definitiva.

## 2. REQUISITOS DE CONFIGURACIÓN

---

1. Para la delegación de un dominio de DNS de segundo nivel bajo “.es”, es necesario disponer al menos de dos servidores autorizados de DNS para el dominio en cuestión, o de un servidor autorizado de DNS y el servidor secundario de Dominios.es. Se recomienda que los servidores autorizados para el dominio sean más de dos (hasta un máximo de siete) y estén físicamente en redes y localizaciones distintas (por ejemplo, el primario en la organización titular del dominio y un secundario en el proveedor que le da acceso a Internet).
2. Los nombres de los servidores autorizados especificados en la solicitud deben ser los nombres canónicos de dichos equipos (nunca un alias) y deben coincidir con los que aparezcan apuntados por registros NS en el servidor primario de la zona en cuestión. En el caso del servidor primario, el nombre debe también coincidir con el que en el propio servidor de DNS aparezca como origen en el SOA de la zona.
3. Todos los servidores de DNS autorizados de toda zona de segundo o tercer nivel bajo “.es” deben estar accesibles desde cualquier punto de Internet en general, y desde el servidor primario de “.es” en particular (al menos por medio de TCP y UDP al puerto 53).
4. Todos los servidores de DNS autorizados de toda zona de segundo y tercer nivel bajo “.es” deben estar dando respuestas autorizadas (*authoritative answer*) y consistentes para la zona en cuestión.
5. Toda la información contenida dentro de un dominio bajo “.es” (a cualquier nivel) deberá ser correcta y contar con las autorizaciones que sean precisas. En concreto, no está permitido poner registros de cualquier tipo (NS, A, MX, CNAME, etc.), en cualquier zona de DNS de segundo o tercer nivel bajo “.es”, apuntando a equipos externos a la propia organización titular del dominio en cuestión sin contar con autorización expresa para ello (esta acción podría suponer la baja del dominio).
6. Está prohibido efectuar lame delegations en o bajo cualquier zona de DNS de segundo o tercer nivel bajo “.es”. Una *lame delegation* consiste en poner un registro NS para un dominio o subdominio apuntando a un equipo

que no está configurado como servidor autorizado para dicha zona. Esta acción se considerará más grave si la máquina a la que se está apuntando de forma errónea es de un tercero externo a la propia organización titular del dominio y podría suponer la baja de éste.

7. El servidor primario de cualquier zona de segundo o tercer nivel bajo “.es” deberá poner *glue records* (es decir, registros de tipo A para servidores autorizados de la zona) únicamente para aquellos servidores que se encuentren bajo el propio dominio asociado a la zona y nunca para aquellos que sean externos al mismo (dicha acción podría suponer la baja del dominio).
8. Está prohibido que una organización configure un servidor de DNS (aunque fuesen de “sólo caché”) como *forwarder* apuntando a un servidor externo del que no se tenga permiso explícito para hacerlo (dicha acción podría suponer la baja del dominio).
9. Los clientes de DNS de una organización deben apuntar únicamente a servidores de DNS internos (o externos de los que se cuente con permiso explícito).
10. El fichero de caché o de los servidores de la raíz (normalmente denominado “named.root”, “named.cache” o “named.ca”) de todo servidor de DNS deberá estar siempre actualizado con la última versión del mismo.
11. Con el fin de servir de ayuda a la hora de detectar y solucionar problemas e inconsistencias entre el servidor primario y en los secundarios, el formato del número serie del SOA recomendado para cualquier zona de DNS por debajo de “.es” (a cualquier nivel) es el siguiente: **AAAAMMDDXX**. Es decir, 10 dígitos, donde:
  - AAAA = año de la última modificación de datos en la zona
  - MM = mes de la última modificación de datos en la zona
  - DD = día del mes de la última modificación de datos en la zona
  - XX = número de modificación de datos en la zona en el día

Por ejemplo, el número serie 2025031203 en el SOA de una zona se correspondería con su tercera modificación el día 12 de marzo de 2025.

12. Con el fin de optimizar al máximo la relación "tráfico de DNS/rapidez de propagación de cambios en DNS", los valores normales recomendados de los parámetros del registro SOA para zonas de DNS de segundo y tercer nivel bajo ".es" son los siguientes:

- SOA TTL = 3600 (1 hora)
- Refresh = 7200 (2 horas)
- Reetry = 3600 (1 hora)
- Expire = 2592000 (30 días)
- Minimum = 3600 (1 hora)

En circunstancias especiales (por ejemplo, en caso de que se prevean cambios importantes o numerosos en la zona), los valores anteriores del TTL asociado al registro SOA y los tiempos de Refresco, Reintento y TTL mínimo pueden ser temporalmente modificados a la baja, con la suficiente antelación al momento previsto para las modificaciones para que los cambios se propaguen en Internet con mayor celeridad y se reduzca el tiempo de caché en los servidores DNS *resolvers*. Es importante destacar que el tiempo de caché negativa que usarán los *resolvers* para nombres de dominio no existentes será el mínimo del TTL asociado al registro SOA y el parámetro *Minimum* especificado en dicho registro. En estos casos, los valores mínimos recomendados son los siguientes:

- SOA TTL = 900 (15 minutos)
- Refresh = 3600 (1 hora)
- Retry = 1800 (30 minutos)
- Expire = 2592000 (30 días)
- Minimum = 900 (15 minutos)

Es importante que el mecanismo de Notificaciones y transferencias de zona en el servidor primario y los secundarios funcione correctamente. Mediante el uso de Notificaciones DNS, los servidores secundarios pueden realizar el proceso de transferencia de zona inmediatamente después de recibir una notificación, sin tener que esperar al vencimiento del tiempo de *Refresh*.

13. Transferencias de zona (AXFR/IXFR). Se recomienda el configurar el soporte para transferencias de zona incrementales (IXFR) para optimizar el ancho de banda consumido y tiempo de transferencia. La primera vez

que se transfiera la zona a un servidor secundario, se transfiera de forma completa (AXFR). Dependiendo del volumen de cambios que incorpore la actualización del fichero de zona podría ocurrir que la transferencia sea de tipo AXFR a pesar de tener IXFR habilitado.

14. En el caso de que el servidor de Dominios.es esté haciendo de servidor secundario opcional para la zona de segundo o tercer nivel bajo “.es” en cuestión, los valores mínimos de los parámetros del SOA mencionados en el apartado anterior no son recomendados sino obligatorios. En este caso, el poner valores de Refresh, Retry y Minimum inferiores a los mínimos obligatorios podría suponer que el dominio sea dado de baja.
15. El campo *mail address* del SOA de cualquier zona de DNS de segundo o tercer nivel bajo “.es” debe contener siempre una dirección de correo electrónico (típicamente conocida como dirección de *hostmaster*) válida y regularmente atendida por las personas de contacto técnico para el dominio en cuestión, con la que se pueda contactar en caso necesario. A la hora de especificar dicha dirección en el SOA de la zona, es necesario sustituir el carácter “@” por el carácter “.” (por ejemplo, “hostmaster.dominio.es” para representar la dirección de email “hostmaster@dominio.es”).
16. Se recomienda que para todo dominio de segundo y tercer nivel bajo “.es” la dirección de email “postmaster@nombrededominio.es” exista y sea regularmente atendida por el responsable de mensajería electrónica de la organización titular del dominio.
17. Con el fin de aportar seguridad al servicio DNS, y evitar (entre otros) ataques de suplantación, se recomienda el uso DNSSEC siempre que sea posible. DNSSEC no cifra las respuestas DNS, sino que añade firmas (*Resource Records* tipo RRSIG) a las respuestas y, en el caso de no existencia de respuesta (NXDOMAIN), devuelve *resource records* tipo NSEC o NSEC3 que permiten al validador comprobar que la respuesta es correcta. En resumen, las tres funcionalidades de seguridad que aporta DNSSEC son:
  - Autenticación del origen de los datos
  - Integridad de los datos
  - Prueba de no existencia de datos

Las dos primeras funciones se consiguen con las firmas (RRSIG) y la tercera con los registros tipo NSEC o NSEC3. DNSSEC utiliza algoritmos de cifrado de clave asimétrica, generando normalmente dos pares de claves: la KSK (*Key Signing Key*) y la ZSK (*Zone Signing Key*). Cada par de claves está compuesto por una clave privada, que se usa para generar las firmas, y una clave pública que será utilizada por los validadores (*DNS resolvers*) para determinar si las respuestas son correctas.

Para que la **validación DNSSEC** que realizan los *DNS resolvers* sea correcta, es necesario que la cadena de confianza sea completa a lo largo de todo el árbol DNS. Es necesario que todos los dominios padre (en este caso el dominio “.es” y el dominio “.” o “root”) estén firmados y que cada dominio padre contenga el registro DS (*Delegation Signer*) de los dominios hijo. El registro DS es un *hash* de la KSK pública. Los validadores DNS realizarán validaciones de las claves públicas de todos los dominios padre hasta llegar al *root* (*trust anchor*). En otras palabras, cada dominio padre posee en su fichero de zona un registro DS para cada dominio hijo que implemente DNSSEC que permite validar la cadena de confianza.

Antes de publicar el registro tipo DS en el dominio padre (en este caso el registro de dominios “.es”) conviene asegurarse de que las claves públicas están correctamente publicadas en el fichero de zona DNS y sean correctas. Asimismo, conviene verificar que las firmas (RRSIG) y registros NSEC o NSEC3 que contiene el fichero de zona sean válidas y vigentes. En el momento de publicar el registro DS en el dominio padre, los validadores DNS (*resolvers*) empezarán a validar las respuestas.

### 3. PARA MÁS INFORMACIÓN

---

1. "DNS and BIND (4th. Edition)", P. Albitz y C. Liu, Ed. O`Reilly & Associates, ISBN 0-596- 00158-4, Abril 2001.
2. Para obtener una lista completa y actualizada de los RFC relacionados con el DNS que puedan ir apareciendo, se sugiere visitar (en inglés):  
<https://www.rfc-editor.org/> y <https://www.statdns.com/rfc/>
3. Presentaciones ISC (Internet Systems Consortium) (en inglés):  
<https://www.isc.org/presentations/>
4. Guía para la implementación y buenas prácticas de DNSSEC:  
[https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe\\_guia\\_de\\_implantacion\\_y\\_buenas\\_practicas\\_de\\_dnssec.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe_guia_de_implantacion_y_buenas_practicas_de_dnssec.pdf)