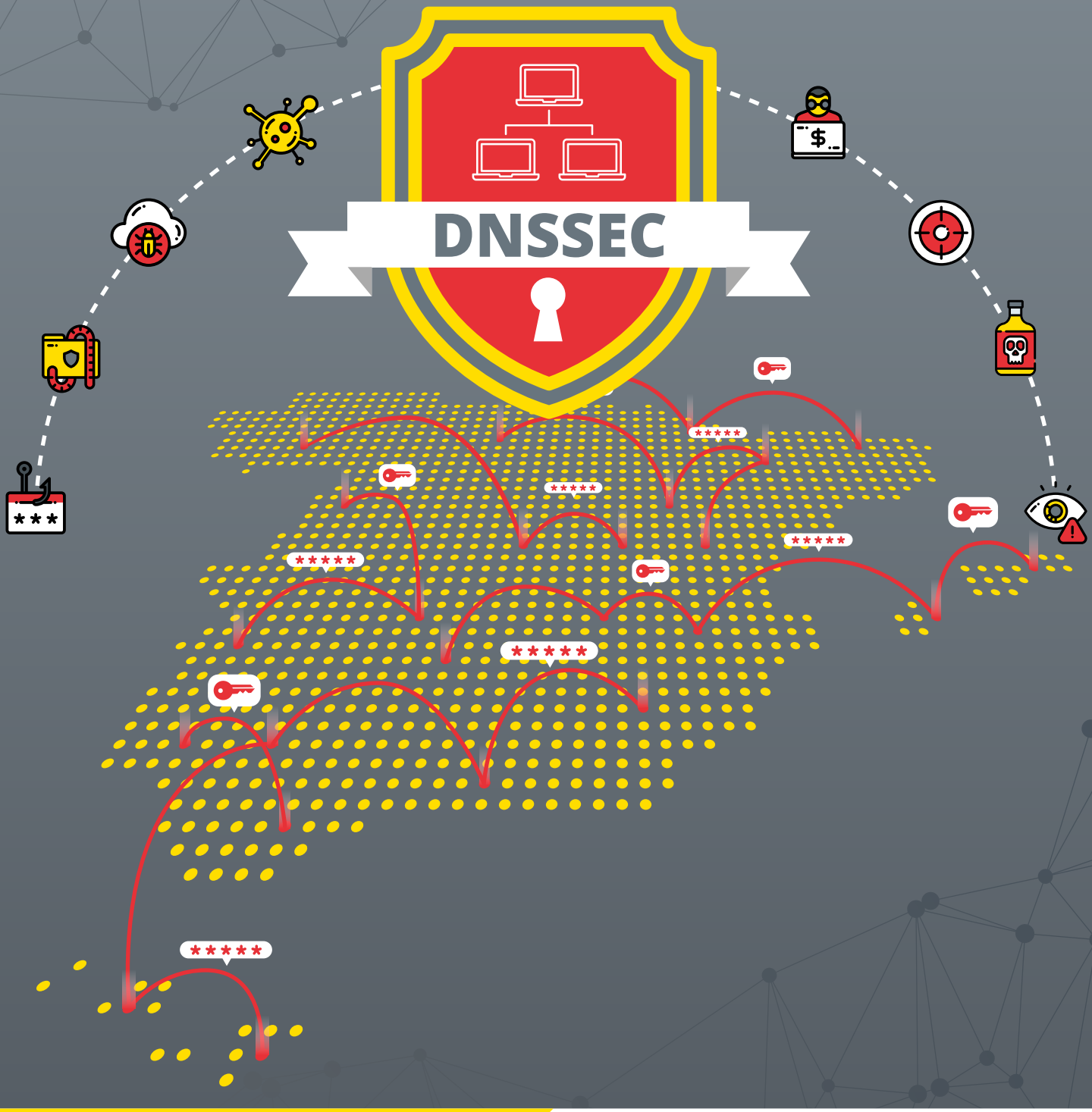
# ESTUDIO DEL ESTADO DE DNSSEC EN ESPAÑA




www.incibe.es

INSTITUTO NACIONAL
DE CIBERSEGURIDAD

SPANISH NATIONAL
CYBERSECURITY INSTITUTE

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

GOBIERNO DE ESPAÑA

MINISTERIO DE ECONOMÍA Y EMPRESA

*Noviembre 2018*

*CERTSI_ESTADO_DNSSEC_ESPAÑA_2018_v1.2*

# ÍNDICE

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# 1. SOBRE ESTA GUÍA

El objeto de la presente guía es ofrecer una visión detallada sobre el estado de implantación del protocolo DNSSEC en España, centrado en los dominios ".es" como dominio de alto nivel (TLD, *Top Level Domain*) de España, estableciendo adicionalmente una comparativa con las estadísticas de adopción de DNSSEC en otros países de Europa, Estados Unidos y en Internet de manera global.

La guía profundiza en los desafíos que debe abordar una organización que se plantee instaurar DNSSEC en sus dominios, indicando las alternativas técnicas disponibles y las opciones a nivel de proveedores de servicios y *hosting*, y analizando los costes que se derivarán en función del escenario elegido.

Dirigida a los responsables de organizaciones encargados de impulsar y/o evaluar la viabilidad de la implantación de DNSSEC, ya sea por iniciativa propia o a petición de los equipos técnicos de su organización, el objetivo de la guía es proporcionar una perspectiva independiente sobre la situación actual del protocolo DNSSEC en España, y concienciar sobre los beneficios que, desde el punto de vista de seguridad, se obtienen con la adopción de DNSSEC.

Para ello, en la presente guía se abordarán cinco áreas conceptuales principales, independientemente de su distribución a lo largo del presente documento:

- Introducción: descripción técnica detallada que permita entender las razones, beneficios, dificultades y desafíos asociados a la implantación de DNSSEC.
- Estado actual y nivel de implantación de DNSSEC en España, Europa, EEUU e Internet.
- Aspectos técnicos: requisitos para la implantación de DNSSEC, opciones disponibles y evaluación de otros servicios basados en DNSSEC.
- Aspectos organizativos: impacto sobre los recursos de la organización y los costes de abordar DNSSEC.
- Conclusiones del estudio.

De cara a la lectura de la presente guía y su formato, conviene saber que:

- Los términos anglosajones se presentan en *letra cursiva*, acompañados de sus equivalentes en castellano; éstos últimos se usarán a menos que no exista una equivalencia adecuada en lenguaje técnico.
- Los términos y expresiones en **letra negrita** corresponden a conceptos clave de DNSSEC que se desea resaltar en los apartados en que aparecen.
- Las referencias con formato "[Ref.- *nn*]" son enlaces a referencias bibliográficas relevantes en las que se puede consultar y ampliar la información proporcionada.
- Las referencias a pie de página corresponden a comentarios, referencias puntuales o aclaraciones sobre la información a la que acompañan.

# 2. INTRODUCCIÓN A DNS Y DNSSEC

El presente apartado ofrece una visión de contexto sobre el servicio DNS, incidiendo sobre las debilidades del protocolo DNS que hicieron necesaria la creación y aparición de DNSSEC. La misma se complementa con un análisis acerca de las dificultades y desafíos que tiene para una organización la adopción de DNSSEC.

## 2.1. Orígenes del servicio DNS

DNS son las iniciales de "*Domain Name System*" (sistema de nombres de dominio), cuyo objeto es proporcionar un mecanismo descentralizado para la identificación de ordenadores, servicios y otros recursos que forman parte de una red, ya sea privada o pública, es decir, integrada en Internet.

La función del servicio DNS es obtener, a partir del nombre de un recurso, fácil de recordar y escribir para una persona, la dirección IP correspondiente a dicho recurso, de forma que se pueda acceder a él, independientemente de dónde se encuentre dentro de la red (por ejemplo, en Internet).

La necesidad de un mecanismo de traducción entre nombres y direcciones IP estuvo estrechamente ligada a los orígenes de Internet. La Internet que se conoce hoy en día tuvo su origen a finales de los años sesenta, con el proyecto "ARPANET" [Ref.- 1] del Departamento de Defensa (DoD, *Department of Defense*) de los Estados Unidos, y que estableció una red de conmutación de paquetes entre un nodo origen y un nodo destino sobre una red distribuida. Aunque el proyecto ARPANET pretendía ser un medio de comunicación tolerante a fallos entre instituciones académicas y estatales, integrado en sus inicios únicamente por 4 nodos, pronto comenzaron a incorporarse nuevos ordenadores, que empleaban el protocolo NCP (*Network Control Protocol*), precursor del protocolo TCP, para intercambiar paquetes. En marzo de 1977, el mapa de ARPANET era el que se ilustra en la "Figura 1", extraída del documento [Ref.- 1].

Dado que ARPANET fue concebida para la comunicación entre equipos miembros de una misma red, a medida que nuevas redes de conmutación de paquetes independientes a ARPANET nacieron por todo el mundo, surgió la necesidad de crear una red de redes dinámica y robusta que permitiese la intercomunicación entre todas ellas, a través de un protocolo de transporte independiente de las diferentes tecnologías subyacentes a los equipos finales. Así surgió el protocolo TCP (*Transmission Control Protocol*), encargado de fragmentar los mensajes en el origen y transmitirlos de forma fiable al destino, en el que se recompone el mensaje original. La transmisión de estos fragmentos (que se denominan "paquetes") se lleva a cabo a través del protocolo IP (*Internet Protocol*), quien se encarga de buscar la mejor ruta entre las conocidas para entregar los paquetes o datagramas al equipo final. Para llevar a cabo su cometido, el protocolo IP define dos elementos fundamentales: el enrutamiento (mecanismo por el cual los paquetes se hacen llegar desde el equipo origen al equipo destino a lo largo de las distintas redes que existen entre ellos) y el direccionamiento (asignación de direcciones de redes, subredes y equipos dentro de la red global). Así, cada recurso de Internet recibe una dirección IP [Ref.- 2], que en su versión 4 (IPv4[1]) corresponde a un número binario de 32 bits que

[1] La versión 6 del protocolo IP (IPv6) hace uso de direcciones alfanuméricas más complejas y de mayor longitud.

identifica de manera lógica y jerárquica la conexión de un dispositivo. Típicamente, las direcciones IP se expresan en notación decimal, la cual se obtiene de dividir sus 32 bits en cuatro grupos de 8 bits (cuatro octetos o *bytes*) separados por puntos y calcular el valor decimal correspondiente a cada uno de esos octetos. Por ejemplo:

11010101 00000100 01101100 01000101 = 213.4.108.69

En 1990 ARPANET fue desmantelada, dando vía libre a la descentralización y privatización de lo que se conoce hoy en día como Internet.

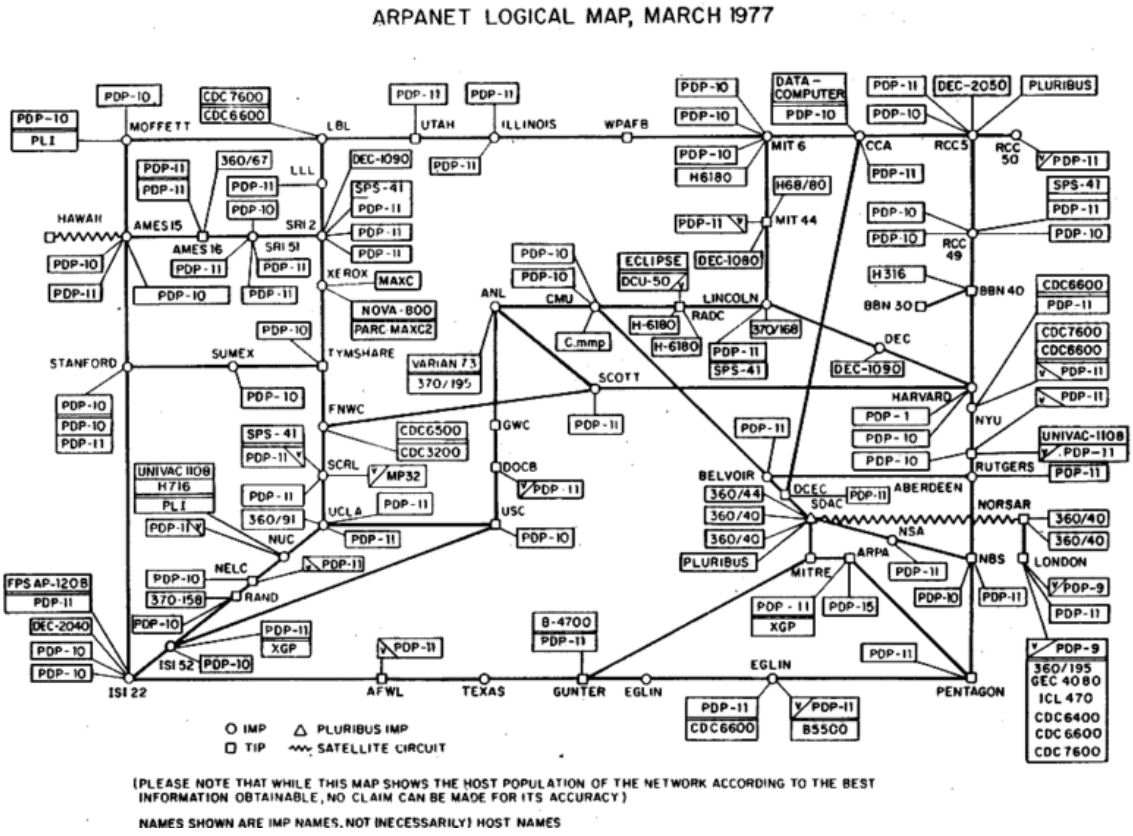



*Figura 1 - Mapa lógico de ARPANET en 1977*

Por tanto, para establecer una comunicación entre dos nodos, independientemente de su ubicación, es necesario conocer las direcciones IP del nodo origen y del nodo destino. Sin embargo, ni tan siquiera la notación decimal es fácil de recordar para los seres humanos, por lo que se decidió asociar a cada recurso un nombre único, en formato alfabético y también jerárquico, que simplificase su manipulación. Así, cada recurso en Internet llevará asociados una dirección y un nombre que lo identifiquen de forma unívoca, y se precisa un mecanismo que traduzca de uno a otro, de manera que el nombre del recurso -manejable por los humanos- pueda convertirse en la dirección IP que requieren las tecnologías de enrutamiento. Adicionalmente, el uso de nombres alfabéticos facilita que pueda accederse a un mismo recurso independientemente de los cambios que se produzcan en la red subyacente y en las redes que permiten llegar a él.

Los nombres alfabéticos se introdujeron en ARPANET al poco de su creación, a través del fichero "HOSTS.TXT", que originalmente era un fichero de texto albergado en cada sitio integrante de la red que proporcionaba el mapeo o traducción entre los nombres de

los equipos y las direcciones de red. Sin embargo, pronto fue evidente que el mantenimiento de múltiples copias de este fichero, además de poco eficiente, era muy sensible a errores, por lo que se propuso su centralización [Ref.- 3], dando lugar a una serie de debates que concluyeron con la decisión de que fuese el *Network Information Center* (NIC) del *Stanford Research Institute*, responsable del mantenimiento de la lista oficial de traducciones, quien albergase oficialmente el fichero *hosts* maestro, y que se encargase de su propagación al resto de nodos.

Este sistema de resolución centralizado estuvo vigente durante una década, pero la expansión de ARPANET llevó a que el fichero *hosts* creciese desproporcionadamente, haciendo que su transferencia y distribución fuese muy proclive a errores. Tras largas discusiones reflejadas en diversos RFCs (810, 811, 819 y 830), se llegó a la conclusión de que la solución pasaba por establecer un servicio de nombres distribuido, que culminó con la publicación del RFC 883 [Ref.- 4], en el que se establecieron las bases para la implementación del protocolo DNS, desde el formato de las direcciones, pasando por la organización jerárquica de los nombres de dominio, hasta su uso por parte de servicios de red como, por ejemplo, el correo electrónico.

## 2.2. Descripción del servicio DNS

A continuación, se proporciona una visión introductoria sobre el protocolo DNS. Para obtener una visión técnica detallada sobre el mismo, se recomienda la lectura de la "Guía de seguridad en servicios DNS" publicada por INCIBE y disponible en *https://www.certsi.es/sites/default/files/contenidos/guias/doc/guia_de_seguridad_en_servicios_dns.pdf* [Ref.- 5].

El propósito del servicio DNS es la traducción de los nombres de dominio de los recursos de Internet, o de cualquier red TCP/IP, como servidores de correo, servidores web, servicios de transferencia y/o compartición de ficheros, etc., a sus correspondientes direcciones IP y viceversa, de modo que dichos recursos estén accesibles para el usuario final sin que este necesite conocer la dirección IP del recurso e independientemente de si el recurso cambia de dirección. Por tanto, el servicio DNS es la guía o el listín telefónico de Internet, facilitando el poder localizar y contactar con los diferentes recursos existentes.

El sistema de nombres de dominio define una estructura jerárquica, distribuida y descentralizada, que parte de un nodo raíz (o *root*) representado por un "." del que cuelgan otros nodos, los cuales representan un subdominio del nivel inferior respecto al nodo raíz, aunque estos corresponden a los dominios de nivel superior (o TLDs) como, por ejemplo, .com, .net, .org o .es (considerándose este último como ccTLD, *Country Code* TLD). Esta distribución en árbol se extiende hacia abajo, de forma que cada nodo hijo representa un subdominio del nodo padre. La jerarquía finaliza en los nodos hoja, que representan el recurso final, y que no tienen hijos, tal como muestra la figura "Figura 2", extraída de la "Guía de seguridad en servicios DNS" [Ref.- 5].

Los dominios situados justo debajo del dominio raíz se denominan *Top Level Domains* o TLDs de primer nivel. Los dominios situados debajo de un TLD de primer nivel se conocen como TLDs de segundo nivel (zonas o dominios), y bajo ellos se encuentran otros subdominios o zonas de niveles inferiores. El nombre que se obtiene al recorrer la jerarquía desde el nodo hoja (que representa al recurso final) hasta el nodo raíz

(representado por ".") se denomina *Fully Qualified Domain Name* (FQDN), o nombre de dominio completamente cualificado, y permite referenciar de manera absoluta a un recurso determinado mediante su nombre.

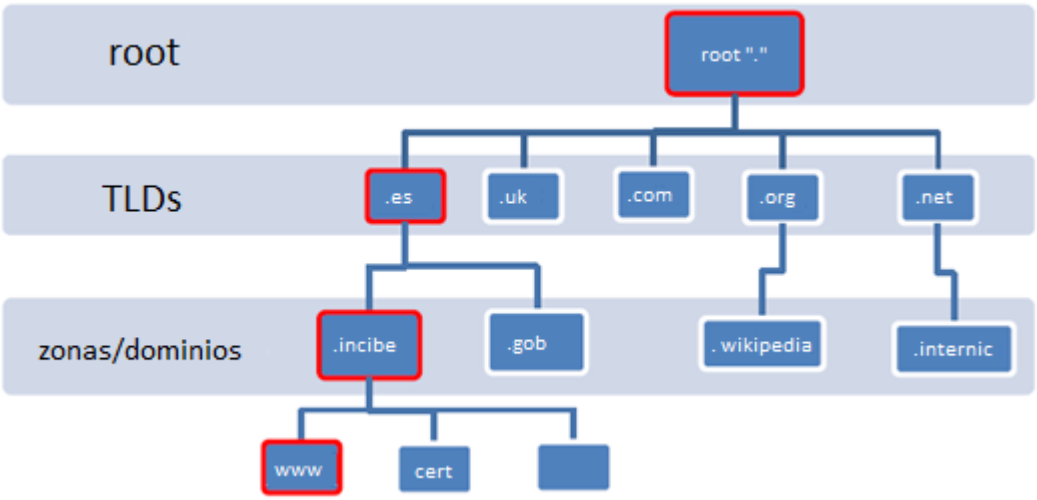



*Figura 2 - Diagrama del espacio de nombres de dominio*

En el ejemplo ilustrado por el diagrama anterior, el FQDN del recurso representado por el nodo etiquetado como "www" sería "www.incibe.es.", siendo ".es" el TLD de primer nivel y ".incibe.es" el TLD de segundo nivel (o de la zona o dominio). El "." al final del nombre representa el nodo raíz, que, aunque típicamente no es referenciado o mostrado, se requiere como parte del mecanismo de resolución de DNS.

Una **zona** es toda la jerarquía asociada a un dominio de nivel superior o intermedio dentro del espacio de nombres de dominio, es decir, la división de la jerarquía de dicho espacio a partir de dicho dominio hacia abajo. Cada nodo del árbol de dominios (salvo los nodos hoja) representa una zona, la cual es gestionada por un servidor DNS denominado **servidor autoritativo de** (o con autoridad sobre) **la zona**. Los servidores autoritativos de la zona son los responsables de la resolución de los nombres de todos los recursos que pertenecen a esa zona. En el diagrama de la imagen previa, son zonas diferenciadas ".", ".es", ".uk", ".com", ".org", ".net" y ".incibe" (junto a otros), y cada una de ellas estará gestionada por un servidor DNS, de ahí que el sistema de resolución de nombres sea distribuido.

La distribución del servicio de resolución de nombres permite a su vez a una organización, o a sus servidores DNS autoritativos, delegar la responsabilidad de gestión de partes de la zona sobre la que se tiene autoridad a otra organización, o a otros servidores DNS, que tendrán la autoridad sobre los subdominios de esa parte delegada.

El proceso de resolución o traducción de un nombre (en formato FQDN) a la dirección IP correspondiente tiene lugar cuando un cliente DNS (al que se conoce como ***resolver***) solicita la dirección IP para un recurso del que conoce su FQDN (por ejemplo, www.incibe.es). El *resolver* interrogará al servidor DNS que tenga definido en su configuración para que le devuelva la dirección IP del recurso. Debe tenerse en cuenta a lo largo de la presente guía que puede actuar como *resolver* tanto un cliente DNS final, como un servidor DNS intermedio que a su vez hace las funciones de cliente DNS. Si el

servidor DNS consultado no conoce la respuesta, puede proceder a obtenerla empleando dos métodos (dependiendo de cómo esté configurado):

- Recursivamente: el servidor DNS definido en el cliente actúa también como *resolver* (o cliente) interrogando a uno de los servidores DNS del dominio raíz (".") para que le dé la dirección IP del recurso (en el ejemplo, *www.incibe.es*); el servidor DNS del dominio "." le devolverá el *referral* (o servidor autoritativo) del dominio de primer nivel (TLD, en este caso, ".es"). El *resolver* consultará entonces al servidor autoritativo obtenido para la zona ".es" sobre la dirección IP del recurso, y este le devolverá el *referral* (o servidor autoritativo) del dominio de segundo nivel (en este caso, ".incibe.es"). De nuevo, el resolver interrogará al servidor DNS de la zona ".incibe.es", que, al ser autoritativo de la misma, conoce el recurso "www.incibe.es", por lo que devuelve su dirección IP al servidor DNS que está actuando como *resolver*, quien la traslada al cliente (o *resolver*) original.
- Iterativamente (o no recursivamente): en lugar de actuar como intermediario realizando las consultas recursivas, el servidor DNS definido en el cliente (recordad, cliente final u otro servidor DNS que está actuando como cliente) devuelve un puntero al servidor autoritativo del siguiente nivel al que debe trasladar la consulta, para que sea el cliente y/o servidor DNS (*resolver*) quien itere siguiendo el proceso recursivo descrito anteriormente hasta llegar a la respuesta solicitada. Las consultas y respuestas empleadas en el proceso recursivo descrito previamente sobre los servidores raíz, TLD y de zona son concretamente iterativas, obteniéndose el *referral* para el siguiente nivel en la jerarquía DNS.

El tipo de resolución descrito sobre estas líneas se conoce como **resolución directa** (traducción de un nombre a su dirección IP). Sin embargo, el servicio DNS también es responsable de lo que se denomina **resolución inversa**, que consiste en la traducción de una dirección IP en el nombre asociado. Para posibilitar la resolución inversa, se define un espacio de dominio especial, "**.in-addr.arpa.**", en el cual cada subdominio tiene una estructura de 4 etiquetas para IPv4, correspondientes a los 4 octetos de una dirección IP. También se define el dominio especial "**.ipv6.arpa.**", potencialmente con múltiples etiquetas, para IPv6:

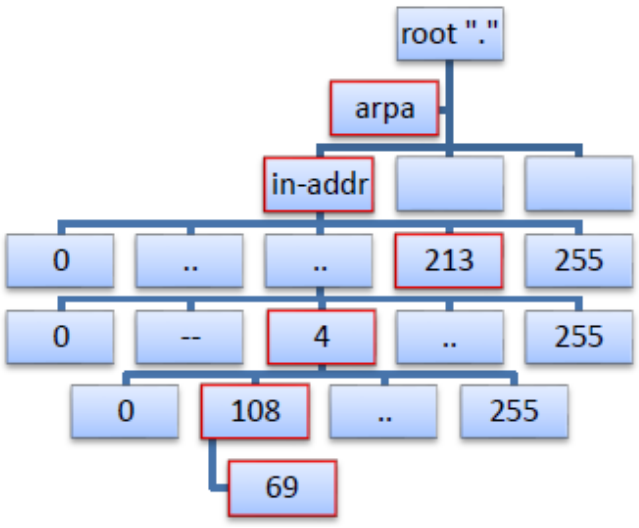



*Figura 3 - Diagrama del espacio de nombres de dominio "in-addr.arpa." (resolución inversa)*

En el ejemplo del diagrama correspondiente a la "Figura 3", extraído de la "Guía de seguridad en servicios DNS" [Ref.- 5], la dirección IP 213.4.108.69 tendría una representación en el espacio de nombres de dominio de resolución inversa correspondiente a "69.108.4.213.in-addr.arpa.", con los valores numéricos correspondientes a los cuatro octetos de su dirección IP invertidos.

La resolución inversa suele utilizarse como elemento de seguridad para verificar un recurso DNS en ambos sentidos e identificar ataques de suplantación de identidad (*spoofing*), por ejemplo, cuando no hay correspondencia o relación entre la resolución directa e inversa de dicho recurso.

En la actualidad, existen más de 1.500 dominios de alto nivel (TLDs, *Top Level Domains*) en el mundo, que están registrados en IANA (*Internet Assigned Numbers Authority*) [Ref.- 8]. Los TLDs de primer nivel se dividen en dos grupos:

- gTLD (*generic Top Level Domain*): los dominios genéricos (gTLD) no están asociados a países, sino que se gestionan por organismos internacionales como ICANN (*Internet Corporation for Assigned Names and Numbers*). Entre ellos, se encuentran los dominios principales, como ".com", ".info", ".org" o ".net", y también los denominados dominios patrocinados (sTLD, *sponsored* TLD), como el dominio ".cat" (Cataluña). Estos dominios están compuestos por tres o más caracteres.
- ccTLD (*country code Top Level Domain*): los dominios de país (ccTLD) corresponden a los TLDs de primer nivel que se reservan para un país o territorio independiente, y son gestionados por organismos propios designados por cada país. Estos dominios cuentan solo con 2 caracteres, asociados a su código de país o territorio (cc, *country code*). El correspondiente a España es el dominio ".es".

A fecha de elaboración del presente informe, de los más de 1.500 TLDs existentes, aproximadamente 1.200 TLDs corresponden a gTLDS[2], y unos 300 corresponden a ccTLDs. Debe tenerse en cuenta, que ICANN ha liberalizado significativamente el mercado de nuevos gTLDs, incorporándose a estos nuevos términos y nombres (*strings*)[3].

### 2.2.1. Tipos de servidores DNS

Dentro de la arquitectura del servicio DNS, o de un sistema o arquitectura DNS de una organización, se identifican los siguientes roles para los servidores DNS [Ref.- 20]:

- Servidor **maestro o autoritativo**: es el responsable de una zona (o zonas, o conjunto de dominios y/o subdominios), y almacena localmente los registros DNS asociados a los recursos de dicha zona, ofreciendo el servicio DNS a los clientes y/o servidores DNS (*resolvers*) que soliciten recursos de la zona sobre la que tiene autoridad. Los servidores que son solo autoritativos no responden a consultas recursivas ni disponen de capacidades de caché, ya que únicamente responden a consultas sobre la zona bajo su responsabilidad. Dentro de los servidores maestros o autoritativos, se distinguen:

[2] https://ntldstats.com/tld

[3] https://newgtlds.icann.org/en/program-status/delegated-strings

- Servidor (maestro) **primario**: almacena y dispone localmente de los ficheros con la copia maestra de los registros asociados a los recursos de la zona sobre la que tiene autoridad. Actualmente, también se emplea el término servidor DNS **maestro** para referenciar al servidor maestro primario.
- Servidores (maestros) **secundarios**: guardan una copia de la zona sobre la que tienen autoridad, obtenida desde el servidor maestro primario mediante una operación que se conoce en DNS como transferencia de zona (ZT, *Zone Transfer*) y que se ejecuta periódicamente. Los servidores DNS secundarios actúan como servidores de respaldo (en caso de indisponibilidad del servidor primario de la zona), por redundancia, y permiten a su vez distribuir o balancear la carga del servicio DNS, por rendimiento (habitualmente empleando una técnica de balanceo de carga conocida como DNS *round-robin*). Actualmente, también se emplea el término servidor DNS **esclavo** para referenciar a los servidores maestros secundarios.

Dentro de los servidores autoritativos se diferencian habitualmente los 13 **servidores DNS raíz** gestionados por ICANN (*Internet Corporation for Assigned Names and Numbers*), encargados de la gestión de la zona raíz o ".", los **servidores DNS de primer nivel (o TLDs)** gestionados por IANA (*Internet Assigned Numbers Authority*), encargados de la gestión de las zonas asociadas a los TLDs, y los **servidores con autoridad sobre una zona** concreta [Ref.- 21], gestionados por las organizaciones propietarias de cada una de esas zonas.

Adicionalmente, los servidores autoritativos se pueden clasificar en dos grandes categorías: privados, que ofrecen su servicio para la resolución de nombres de dominios y redes internas a la organización, y públicos, que ofrecen su servicio para la resolución de nombres de dominios públicamente disponibles en Internet.

- Servidor **caché**: se encarga de gestionar las consultas recursivas de los clientes y/o servidores DNS (*resolvers*) a los que ofrece su servicio y de almacenar la información obtenida en las respuestas sobre los registros DNS consultados por los clientes. Esto permite tanto agilizar las consultas DNS de cara a los clientes, debido a su proximidad a los mismos y a que se evita la realización de múltiples consultas DNS, como descargar a los servidores DNS autoritativos a los que irían destinados las consultas, al disponer de la respuesta previamente cacheada. El tiempo de validez de estos registros cacheados está definida por el parámetro TTL (*Time To Live*) asociado a las respuestas del protocolo DNS. Este tipo de servidores son también denominados servidores DNS ***resolver*** **recursivos** (***recursive resolvers*** o **DNS *recursors*** [Ref.- 21]).
- Dentro de los servidores de caché existen dos grandes categorías: privados, que son gestionados por las organizaciones para ofrecer el servicio de resolución de nombres a sus clientes internos, y públicos (o abiertos), también conocidos como *public* (u *open*) *DNS resolvers*, gestionados por empresas de telecomunicaciones o servicios de Internet (ISPs) y grandes proveedores de servicios e infraestructuras, como Google (8.8.8.8), Quad9 (9.9.9.9), Cloudflare (1.1.1.1[4]) u

[4] https://blog.cloudflare.com/announcing-1111/

OpenDNS (Cisco), para ofrecer el servicio de resolución de nombres a cualquier cliente públicamente en Internet.

- Servidor ***forwarder***: con el objetivo de limitar o centralizar todo el tráfico DNS generado desde el interior de una organización hacia el exterior (por ejemplo, hacia el resto de Internet), es decir, correspondiente a zonas externas a la organización, existe la posibilidad de que todos los clientes y/o servidores DNS (*resolvers*) de la organización hagan uso de un (o un conjunto) de servidor(es) DNS encargados de la gestión del servicio DNS hacia el exterior, denominados *forwarders*. Por su naturaleza, los *forwarders* simplemente trasladan las consultas que reciben de los clientes y/o servidores DNS (*resolvers*) a los que ofrecen su servicio a otros servidores con capacidades recursivas, como los servidores caché (tanto privados, como públicos). Aunque es habitual que los *resolvers* de tipo *forwarder* dispongan a su vez de una caché, no se encargan de hacer el trabajo asociado a resolver las consultas recursivas, por lo que requieren de menos recursos. Desde el punto de vista de seguridad, este tipo de servidores también permiten diferenciar o segmentar el tráfico DNS privado (interno a la organización) y público (asociado a Internet), haciendo uso de (o redireccionando el tráfico) a diferentes servidores DNS.

En realidad, desde el punto de vista de la funcionalidad, un mismo servidor DNS puede desempeñar múltiples de estos roles o funciones simultáneamente, aunque se desaconseja hacer uso de diferentes funcionalidades en el mismo servidor DNS, tanto desde el punto de vista de seguridad, como de rendimiento.

## 2.3. Riesgos de seguridad en la utilización del servicio DNS

Desde el punto de vista de seguridad, el protocolo DNS adolece en primer lugar de la utilización de UDP como protocolo de transporte. Este hecho le hace muy vulnerable a ataques basados en la suplantación de la dirección IP origen (*IP spoofing*), tanto de peticiones, como de respuestas. En el caso de hacer uso del servicio DNS para la ejecución de ataques de denegación de servicio (DoS, *Denial of Service*) se hace uso de peticiones DNS en las que la dirección IP origen ha sido suplantada por la del servidor víctima, para que las respuestas vayan dirigidas a este. En la ejecución de ataques de MitM (*Man-in-the-Middle*) se hace uso de respuestas DNS en las que la dirección IP origen del servidor DNS legítimo ha sido suplantada, para hacerse pasar por él. La mayoría de ataques sobre el protocolo DNS hacen uso de técnicas de suplantación de la(s) dirección(es) IP.

Adicionalmente, como problema fundamental, el protocolo DNS no hace uso de mecanismos de seguridad básicos, como autentificación, cifrado y/o integridad.

A continuación, se establece una clasificación no exhaustiva de los vectores de ataque que tienen algún tipo de relación con DNSSEC, y que permitirán valorar las ventajas e inconvenientes de su implantación como mecanismo de protección. Nótese que solo se incluyen en esta clasificación los vectores de ataque relacionados directamente con el protocolo DNSSEC, y no con el protocolo DNS, para el que también existen otras vías ofensivas de ataque. Para profundizar en los detalles relativos a la seguridad del protocolo DNS, se recomienda la lectura del capítulo 3 de la "Guía de seguridad en servicios DNS" [Ref.- 5]).

### 2.3.1. Ataques al protocolo DNS:

Se engloban en esta categoría aquellos ataques que aprovechan las debilidades en el diseño o implementación del protocolo DNS, que se resuelven con DNSSEC:

- Envenenamiento de caché DNS (***DNS cache poisoning***): este ataque permite introducir información DNS falsa en la caché de un servidor DNS. En julio de 2008, un investigador de seguridad llamado Dan Kaminsky publicó un estudio en el que se describía la manera de suplantar cualquier servicio en Internet (servidor web, servidor de correo, etc.) mediante la inyección remota de registros DNS falsos en las cachés de los servidores DNS que actuaban como *resolvers* recursivos [Ref.- 16]. Para ello, se aprovechaban las deficiencias del protocolo DNS respecto a los identificadores de las consultas DNS (*Query ID*) y a los puertos UDP empleados, potencialmente adivinables.
- Suplantación del servidor DNS (***DNS spoofing*** o ***DNS hijacking***): este ataque, en ocasiones mencionado en relación al ataque anterior, permite generar respuestas DNS desde un servidor malicioso para las consultas DNS que iban dirigidas al servidor DNS legítimo, pudiéndose manipular su contenido. Para ello, el atacante empleará técnicas de MitM[5] (como por ejemplo envenenamiento de la caché ARP, *ARP poisoning*, o manipulación de los protocolos de enrutamiento dinámicos), para redirigir el tráfico DNS y hacer que el *resolver* (ya sea un cliente final u otro servidor DNS actuando como cliente) crea que la respuesta a su consulta procede del servidor DNS legítimo, cuando en realidad ha sido manipulada y proporcionada por el servidor DNS malicioso.
- Tunelización de tráfico dentro del protocolo DNS (**DNS *tunneling***): este ataque encapsula o tuneliza los datos de otros protocolos, como por ejemplo HTTP o SSH, en las peticiones y respuestas del protocolo DNS. El objetivo de esta técnica es establecer un canal de comunicación encubierto, para exfiltrar información o para disponer de control remoto de los recursos involucrados, sin que su presencia sea detectada por los sistemas de detección de intrusos o cortafuegos.

### 2.3.2. Ataques sobre el servidor DNS:

Se engloban en esta categoría aquellos ataques que aprovechan debilidades en la configuración e implementación del propio servidor DNS y en los protocolos en que se apoya el servicio DNS (IP y UDP), y que no son resueltas por DNSSEC:

- Es posible manipular el servicio DNS aprovechando errores en la configuración del servidor DNS, vulnerabilidades en el software del servidor DNS (como por ejemplo, un desbordamiento de memoria en BIND[6]) o vulnerabilidades de otros servicios y aplicaciones que ejecutan en el mismo servidor. Este tipo de vulnerabilidades podrían permitir a un potencial atacante tomar control completo del servidor DNS y manipular su comportamiento y, por tanto, el comportamiento del servicio DNS que ofrece.

[5] Los ataques de DNS *spoofing* o *hijacking* también se pueden llevar a cabo mediante *malware* en el cliente víctima cuya resolución de nombres está siendo manipulada, o a través de la modificación no autorizada del servidor DNS.

[6] https://nvd.nist.gov/vuln/detail/CVE-2002-0684

- Ataques de denegación de servicio mediante amplificación DNS (***DoS DNS amplification attack***): en este ataque el servicio DNS no es el objetivo, sino el medio para atacar a otro servicio ubicado en un servidor víctima remoto, saturándolo con respuestas procedentes de uno o varios servidores DNS legítimos. El ataque consiste en suplantar la dirección IP origen del servidor víctima (de nuevo, empleando *IP spoofing*) desde un *resolver* (cliente DNS), para enviar numerosas consultas o peticiones a servidores DNS intermedios públicos u ***open resolvers***[7]. Los *open resolvers* enviarán sus respuestas al servidor víctima, al creer que las consultas procedían de este, cuyo tamaño en *bytes* será significativamente mayor con respecto al de la consulta, de ahí el concepto de amplificación del ataque, que en el caso del servicio DNS hace uso normalmente de un factor de amplificación de entre 5-10x. Generando un número suficiente de peticiones y empleando simultáneamente múltiples *open resolvers*, se puede saturar el ancho de banda del servidor víctima. En este caso, el uso de DNSSEC puede contribuir al éxito de este tipo de ataques al proporcionar respuestas de mayor tamaño que el protocolo DNS (debido a los registros criptográficos adicionales que DNSSEC incorpora).

### 2.3.3. Incidentes de seguridad relacionados con el servicio DNS

A la par que la tipología de los servicios que se prestan a través de Internet aumenta día a día, lo hacen también las amenazas que los afectan. Los atacantes emplean cada vez recursos más sofisticados para alcanzar sus objetivos fraudulentos, y se ven favorecidos por la heterogeneidad de las plataformas, la complejidad del software y las tecnologías subyacentes a todo servicio, así como el acceso cada vez más extendido a recursos "en la nube" por diversos tipos de usuarios (en la mayor parte de las ocasiones, de perfil no técnico).

Si bien resulta muy difícil proteger una organización frente a todo tipo de amenazas relacionadas con la ciberseguridad, con el uso de DNSSEC se garantiza que las transacciones DNS están protegidas frente a los siguientes ataques:

- Ataques de tipo MitM (*Man-in-the-Middle*), como *DNS spoofing*, centrados en la suplantación de la identidad y la integridad de los recursos asociados al servicio DNS, y encaminados a redirigir a los usuarios a recursos controlados por el atacante.
- Ataques de envenenamiento de caché DNS, consistentes en añadir y/o alterar los registros en los servidores DNS caché, de forma que una consulta DNS para un dominio concreto devuelva una dirección IP que pertenece a otro dominio, el cual está bajo el control del atacante.

Dado que el cliente no tiene modo de saber que la resolución DNS ha sido manipulada, el atacante puede redirigir a este a sitios y/o servicios fraudulentos o maliciosos que suplantan al legítimo, por ejemplo, en ataques de *pharming* y *phishing*, para el robo de credenciales o la distribución de *malware*.

[7] Un "*open resolver*" es un servidor DNS recursivo público y accesible para cualquier cliente (*resolver*) en Internet.

Aunque a priori pudiera parecer que es solo el usuario final quien sufre el perjuicio de estos ataques, una organización utilizada como objetivo del ataque también puede sufrir grandes pérdidas (e incluso verse abocada a la desaparición). A continuación, se listan algunos ejemplos reales de ataques acontecidos a lo largo de la última década y que podrían haberse evitado de haberse utilizado DNSSEC:

- En junio de 2008, la empresa BreakingPoint dedicada a la investigación en ciberseguridad, fue víctima de un ataque de envenenamiento de caché, causado por el tráfico entre el servidor DNS de la empresa y un servidor del proveedor AT&T que a su vez había sido comprometido por este tipo de ataque. Lo relevante de este incidente es que el propietario de BreakingPoint es HD Moore, el creador de la conocida herramienta Metasploit (uno de los entornos o *frameworks* de referencia para la explotación de vulnerabilidades), lo cual pone de manifiesto que incluso organizaciones estrechamente vinculadas y concienciadas con el mundo de la ciberseguridad pueden convertirse en víctimas de los ataques sobre el servicio DNS [Ref.- 12].
- En 2009, un importante banco de Brasil sufrió un ataque de envenenamiento de caché, que afectó al 1% de sus clientes, por el cual los accesos a sus servidores web eran redirigidos a sitios fraudulentos para el robo de credenciales [Ref.- 12].
- En 2013, los dominios de Malasia asociados a Google (google.com.my y google.my) fueron secuestrados, redirigiendo a los usuarios a una página web que atribuía el ataque a un grupo pakistaní. El proveedor del servicio de nombres del país MYNIC, único administrador para las direcciones web malayas, confirmó posteriormente el ataque [Ref.- 11].

Más recientemente, en abril de 2018, las debilidades de los protocolos de enrutamiento dinámico (en concreto BGP), junto a las debilidades del servicio DNS, fueron aprovechadas para secuestrar y suplantar el servicio DNS de Amazon (conocido como Route 53) y, por tanto, potencialmente todos los servicios disponibles bajo AWS (Amazon Web Services) para los clientes afectados. Mediante un elaborado ataque que únicamente duró dos horas y que se ilustra en la "Figura 4" [Ref.- 25], los atacantes, empleando servidores en Rusia, consiguieron obtener unos 150.000 dólares [Ref.- 26] en criptomonedas de MyEtherWallet, una pequeña cantidad comparada con los 17 millones de dólares existentes en la cartera digital de los atacantes a la que fueron transferidas las criptodivisas robadas.

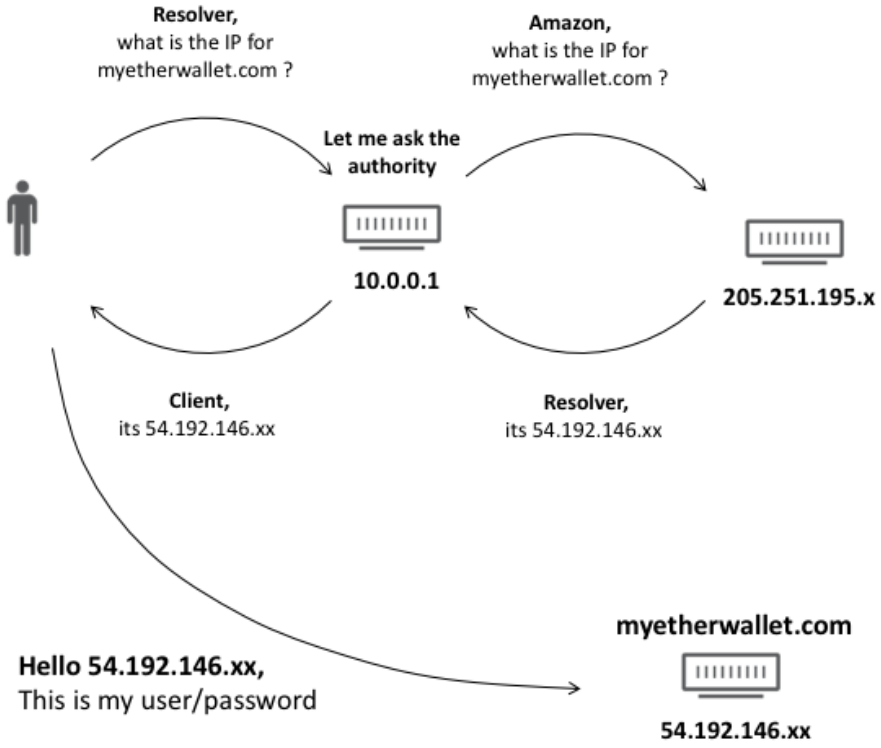



*Figura 4 - Ataque contra los servidores DNS de Amazon mediante BGP*

El impacto de este tipo de ataque podría haber sido mucho mayor, ya que el atacante podría haber usado un certificado de confianza válido, afectando a todos los usuarios del servidor víctima y no solo a los que se conectaron al servidor malicioso aceptando un error del certificado digital de HTTPS (TLS). Una vez se dispone de control sobre el servicio DNS de la víctima, el atacante puede emplear el servicio DNS para obtener certificados digitales válidos (incluso certificados comodín, válidos para todo el dominio[8]), por ejemplo, mediante el protocolo DNS-01 de validación para la emisión de certificados digitales mediante DNS de Let's Encrypt [Ref.- 27].

DNSSEC hubiera permitido evitar este ataque, ya que los registros DNS correspondientes al servidor web víctima no podrían haber sido firmados por el atacante, al no disponer este de la clave privada para dicho dominio.

Según el informe de 2017 publicado por Efficient iP [Ref.- 10], las tres cuartas partes (76%) de las organizaciones participantes en el estudio (APAC, Europa y Norte América) han sufrido ataques de DNS durante el último año, sufriendo robo de datos un 28% de ellas. Del total de estos ataques, el 35% son por *malware* cuyo objetivo es el DNS, el 32% son denegaciones de servicio distribuidas (DDoS), el 23% son envenenamientos de caché, un 22% está asociado a la exfiltración de datos a través de túneles DNS, y un 19% a nuevas vulnerabilidades de los servidores DNS o *0-day exploits*. El coste anual de

[8] https://community.letsencrypt.org/t/acme-v2-production-environment-wildcards/55578

los ataques DNS para las organizaciones de más de tres mil empleados se estima en más de 2 millones de dólares. Curiosamente, las organizaciones de España participantes en el estudio se encontraban entre las más concienciadas, en el tercer lugar, con un 38% de ellas conocedoras de los 5 ataques de DNS más comunes.

## 2.4. ¿Qué es DNSSEC?

Como la mayoría de protocolos empleados en Internet, DNS no fue diseñado desde el punto de vista de seguridad, y presenta numerosas carencias descritas anteriormente. DNSSEC son las siglas del protocolo[9] "*Domain Name System Security Extensions*", extensiones de seguridad del sistema de nombres de dominio (o DNS), una especificación del *Internet Engineering Task Force* (IETF) descrita en el RFC 2535 [Ref.- 9] en 1999 (originalmente en el RFC 2065, 2 años antes) que complementa el sistema DNS para definir un mecanismo por el cual un *resolver* configurado convenientemente puede verificar la autenticidad y la integridad de la respuesta a una consulta al servicio de nombres de una zona firmada. Posteriormente, la especificación de DNSSEC fue actualizada en el año 2005 mediante los RFCs 4033, 4034 y 4035 [Ref.- 28].

DNSSEC firma digitalmente los datos del servicio DNS y proporciona cadenas de confianza a lo largo de todo el espacio de nombres de dominio a fin de que el servicio DNS pueda validar sus transacciones.

Para ello, DNSSEC implementa una infraestructura o esquema de criptografía de clave pública o PKI (*Public Key Infraestructure*), ya que el proceso de firma debe llevarse a cabo en cada uno de los niveles de la jerarquía del servicio DNS. Los servidores raíz (".") publicarán la clave de los servidores de primer nivel o TLDs, por ejemplo, ".es", y estos a su vez publicarán la clave de los servidores autoritativos de zona, por ejemplo, ".incibe.es".

Es importante puntualizar que DNSSEC no cifra los datos intercambiados a través del servicio DNS.

Mediante firmas criptográficas DNSSEC certifica:

- **Integridad**: los datos no han sido alterados desde su emisión en el origen hasta su recepción en el destino.
- **Autenticidad**: los datos recibidos por el destino proceden de un origen de confianza, es decir, un servidor DNS autoritativo para la zona solicitada.
- **Respuestas negativas:** certifica la integridad y autenticidad de los datos incluso para datos no existentes, es decir, que las respuestas negativas de un dominio no existente correspondan efectivamente a registros que no existen en la zona solicitada (ver apartado "2.4.5. Gestión de recursos inexistentes en DNSSEC").

[9] En realidad, DNSSEC podría no considerarse un protocolo, sino únicamente un conjunto de extensiones de seguridad que amplían las capacidades del protocolo DNS. Por homogeneidad y simplicidad, la presente guía emplea también el término protocolo DNSSEC.

### 2.4.1. Nuevos registros asociados a DNSSEC

DNSSEC proporciona una secuencia de validación para los registros que se intercambian en una transacción DNS. Se basa en la incorporación de firmas digitales (mediante criptografía de clave pública) a los registros DNS que existen en una zona. Las firmas que acompañan a la respuesta DNS se pueden generar durante el proceso de firmado de la zona o en tiempo real, en función de las características de la zona.

Cuando a un servidor autoritativo de una zona que implementa DNSSEC llega una consulta por parte de un *resolver* que también soporta DNSSEC¸ el servidor autoritativo de la zona proporcionará tanto el registro DNS, como la firma asociada a él. Puesto que en la respuesta también incluye su clave pública, el *resolver* podrá comprobar si la firma es válida.

Para poder coexistir con el servicio DNS sin afectar a la forma en que este opera, DNSSEC simplemente añade nuevos datos o registros **RR** (***Resource Records***) a los ya existentes en el servicio DNS (como, por ejemplo, los tradicionales A, PTR, CNAME, NS, MX o TXT), y se asegura de no añadir ningún campo extra a los paquetes del protocolo DNS, para no influir en la compatibilidad hacia atrás y permitir la coexistencia.

Las actualizaciones introducidas a través de varios RFCs asociados a la evolución de DNSSEC contemplan la utilización de nuevos bits, como CD (*Checking Disabled*) y AD (*Authentic Data*) (RFC 4035 [Ref.- 28]), complementando el uso de *Extended DNS* (EDNS), que permite la utilización del bit DO ("DNSSEC OK") para que los *resolvers* con soporte de DNSSEC puedan poner en conocimiento de los servidores de nombres a quienes realizan sus consultas DNS que disponen de estas capacidades (RFC 3225 [Ref.- 33]).

En DNSSEC, todos los registros RR del mismo tipo asociados a un mismo recurso (por ejemplo, *www.incibe.es*) de una zona se agrupan en un único conjunto de registros denominado **RRset** (*Resource Record set*), como ilustra la "Figura 5".

Los RRset constituyen la unidad mínima de información que será firmada por DNSSEC, en lugar de los registros (RR) individuales y verificada en las transacciones de DNSSEC.

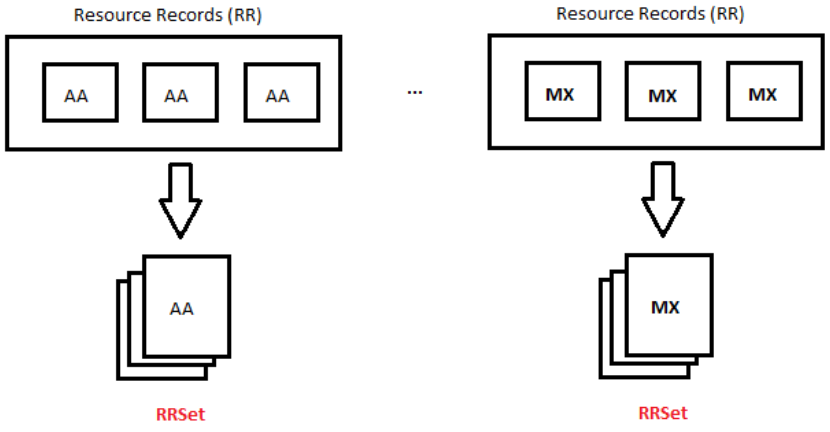



*Figura 5 - Proceso de agrupación de RRs en RRsets en DNSSEC*

Los nuevos registros que añade el protocolo DNSSEC son[10]:

- **RRSIG** (*Resource Record SIGnature*): registro que contiene la firma criptográfica empleada para autentificar los registros de DNSSEC (RRsets). La clave privada ZSK se emplea para generar una firma para cada uno de los RRset de una zona.
- **DNSKEY** (DNS *Key*): registro que contiene la clave pública de la ZSK (*Zone-Signing Key*), cuya clave privada asociada es empleada para la firma de los RRsets de la zona. Esta clave pública se emplea para verificar las firmas, registros RRSIG, de DNSSEC.
- **DS** (*Delegation Signer*): registro que contiene el nombre de una zona delegada, junto a una referencia al hash criptográfico del registro DNSKEY (que contiene la clave pública KSK) de la zona delegada. Su misión es vincular o enlazar la cadena de confianza de una zona padre a una zona hija. El registro DS se publica en la zona padre junto a los registros NS de delegación del servicio DNS hacia la zona hija.
- **NSEC** (*Next SECure*): registro que permite probar la negación de existencia (*denial of existence*) de un registro DNS (consultar apartado "2.4.1. Nuevos registros asociados a DNSSEC").
- **NSEC3** (*Next SECure* versión 3): se introdujo para solucionar el problema de enumeración de zona asociado al mecanismo del registro NSEC (consultar apartado "2.4.1. Nuevos registros asociados a DNSSEC").
- **NSEC3PARAM** (*Next SECure versión 3 PARAMeters*): Los servidores DNS autoritativos emplean este registro para determinar qué registros NSEC3 serán incluidos en las respuestas asociadas a recursos no existentes.

### 2.4.2. Claves criptográficas empleadas por DNSSEC

Cada zona DNS que implementa DNSSEC es la propietaria y responsable de generar una *clave de firma de la zona* (clave asimétrica, o par de claves pública y privada[11]), conocida como **ZSK** (*Zone-Signing Key*).

La clave privada ZSK (que debe ser almacenada de forma segura) se emplea para firmar digitalmente cada RRset de la zona (y no cada registro DNS individual). La firma obtenida como resultado se almacena públicamente en un registro RRSIG en el servidor de nombres para cada RRset:


[10] Existen otros registros específicos de DNSSEC, como CDS y CDNSKEY, que quedan fuera del alcance de la presente guía.

[11] Desde un punto de vista criptográfico, se podría hablar de la parte pública y de la parte privada de la clave ZSK, pero por simplicidad, dichas partes serán referenciadas como clave pública ZSK y clave privada ZSK. Este mismo criterio se aplicará para el resto de claves asimétricas, como por ejemplo la clave KSK.

*Figura 6 - Generación de la firma RRSIG para un RRset mediante la clave privada ZSK*

La clave pública ZSK se emplea para la verificación de las firmas digitales contenidas en los registros RRSIG. Para que los *resolvers* puedan verificar la firma de los RRsets correspondientes a la zona, el responsable de la zona debe distribuir la clave pública mediante un registro DNSKEY a través del servidor de nombres.

Cuando un *resolver* DNSSEC consulta la resolución de nombres de un recurso particular (RR en DNS), el servidor de nombres devolverá en su respuesta el RRset al que pertenece el recurso solicitado, e incorporará el registro RRSIG correspondiente. El *resolver* obtendrá adicionalmente del servidor DNS autoritativo el registro DNSKEY que contiene la clave pública ZSK, y la utilizará para validar la firma RRSIG y, en consecuencia, el registro RRSet y la validez de la respuesta DNS obtenida [Ref.- 19]:

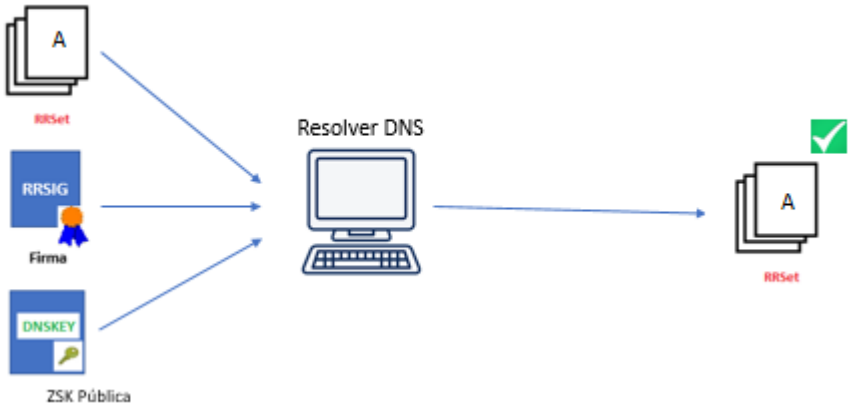



*Figura 7 - Proceso de validación de la firma de un RRset con la clave pública ZSK*

Si se tiene confianza en la validez de la clave pública ZSK asociada al registro DNSKEY, se puede confiar en la validez de todos los registros (RRsets) asociados a la zona.

Para que el receptor tenga la certeza de que la clave pública ZSK que se emplea es de confianza, hay que establecer un mecanismo de validación que asegure que el registro DNSKEY es auténtico y pertenece al servidor DNS autoritativo de la zona.

Este mecanismo pasa por definir una nueva clave de firma, denominada **KSK** (*Key-Signing Key*), de nuevo correspondiente a una clave asimétrica, o a un par de claves pública y privada. La clave KSK permite validar los registros DNSKEY exactamente igual que la clave ZSK permitía validar los registros RRset.

La clave privada KSK se emplea para firmar digitalmente el registro DNSKEY (que contiene la clave pública ZSK) y darle así validez. Para ello, de forma similar a como se firmaban los RRsets con la clave ZSK, la firma obtenida a través de la clave privada KSK para el registro DNSKEY se almacena públicamente en un nuevo registro RRSIG en el servidor de nombres.

Por su parte, la clave pública KSK se incorpora a un nuevo registro DNSKEY, y a su vez se engloba en un nuevo RRSet junto a la clave pública ZSK (al ser ambos registros DNS

del mismo tipo, en concreto, DNSKEY). Este RRSet de tipo DNSKEY es el que realmente se firma con la clave privada KSK para generar el RRSIG de tipo DNSKEY.

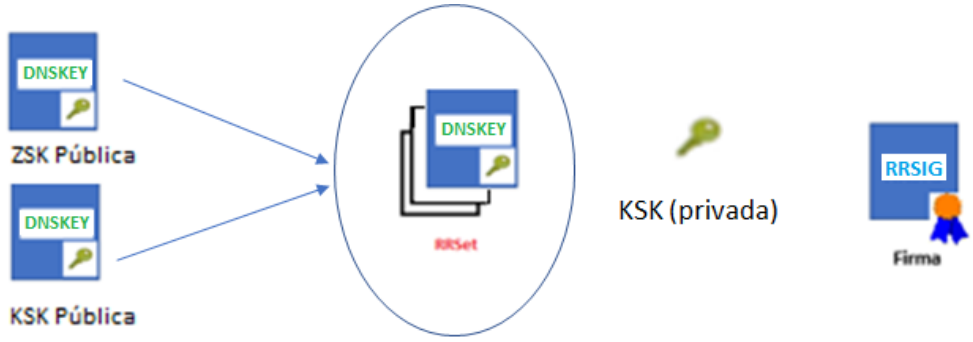



*Figura 8 - Generación de la firma del RRset de tipo DNSKEY mediante la clave privada KSK*

De nuevo, cuando un *resolver* DNSSEC consulta la clave pública ZSK de una zona, el servidor de nombres devolverá en su respuesta el RRset de tipo DNSKEY para la zona, e incorporará el registro RRSIG (la firma) correspondiente. El *resolver* obtiene adicionalmente del registro RRset de tipo DNSKEY la clave pública KSK, que utilizará para validar la firma RRSIG y, en consecuencia, el registro RRSet de tipo DNSKEY y la validez de la clave pública ZSK obtenida.

La clave KSK, por tanto, es una clave autofirmada, ya que su firma ha sido generada empleando la parte privada de la propia clave, lo que no añade autenticidad sobre la misma. Posteriormente, se analizarán los mecanismos adicionales necesarios en DNSSEC para obtener confianza en dicha clave.

La clave KSK es mucho más sensible que la clave ZSK, por lo que ha de ser más segura y estar mejor protegida. La separación del proceso de generación de firmas en dos claves permite alcanzar un equilibrio entre el nivel de seguridad deseado, el rendimiento del servicio DNS y las tareas de gestión y renovación de claves.

En resumen, DNSSEC emplea dos tipos de claves asimétricas (dos pares de claves):

- ***Zone-Signing Key* (ZSK)**, empleada para firmar los registros de una zona. Dado que esta clave se utiliza para firmar muchos registros (RRsets), debe tener un tamaño que no sobrecargue en exceso las necesidades de cálculo del proceso de firma. El consenso actual recomienda emplear claves de 1.024 bits, siendo este un tamaño adecuado de compromiso entre seguridad y rendimiento. Para evitar que, por su menor tamaño, esta clave pueda ser comprometida, se recomienda renovarla con una periodicidad baja (en torno a un mes).
- ***Key-Signing Key* (KSK)**, empleada para firmar las claves ZSK de zona. El número de registros que se firman con la clave KSK es bastante más reducido que el de los que se firman con la clave ZSK, por lo que, desde el punto de vista del rendimiento, se puede asumir que su longitud sea mayor. Por otra parte, como se describirá posteriormente, dado que el *hash* de esta clave KSK es el elemento que se emplea para verificar la cadena de confianza entre la zona padre y la zona hija, su renovación es una operación sensible que no debería realizarse con excesiva frecuencia, por la complejidad que tiene asociada. Por todo ello, se recomienda dotarla de un nivel de seguridad mayor, que permita que su

renovación pueda producirse entre un mínimo de un año y un máximo de dos años. El consenso actual (que no obligación, por lo que queda a criterio del administrador de la zona) recomienda emplear claves de 2.048 bits. El mecanismo de renovación debe planificarse concienzudamente, tal como se detalla en el apartado "4. Aspectos clave en el diseño e implantación".

### 2.4.3. Proceso de resolución de nombres en DNSSEC

Una vez detallados los nuevos registros incorporados en el protocolo DNSSEC, y las claves criptográficas necesarias, es posible disponer de una visión global del proceso de resolución de nombres de DNSSEC. Durante este proceso de resolución de nombres, el *resolver* DNSSEC (ver "Figura 9" para los pasos (1) y (2) y "Figura 10" para los pasos (3) y (4))[12]:

1. Solicita el registro (RRset) asociado al recurso de la zona que quiere resolver, junto al que se incluirá el registro RRSIG (firma) correspondiente.
2. Solicita el registro (RRset) de tipo DNSKEY que contiene las claves públicas ZSK y KSK, junto al que se incluirá el RRSIG de tipo DNSKEY (firma) correspondiente.
3. Verificará la firma del RRSIG que acompaña al RRset de tipo DNSKEY (paso 2) mediante la clave pública KSK también obtenida en ese mismo RRSet de tipo DNSSEY (paso 2).
4. Verificará la firma del RRSIG que acompaña al RRset del recurso consultado (paso 1) mediante la clave pública ZSK obtenida del registro DNSKEY (paso 2) y viendo si el resultado coincide con el RRSIG obtenido para ese RRset (paso 1).
5. Opcionalmente, almacenará en caché el RRset de tipo DNSKEY y su correspondiente registro RRSIG, para evitar sobrecargar a los servidores DNS y generar tráfico de red innecesario en futuras consultas.

[12] NOTA: la numeración de los pasos siguientes no representa una secuencia temporal, sino que pretende facilitar la interpretación de la figura.

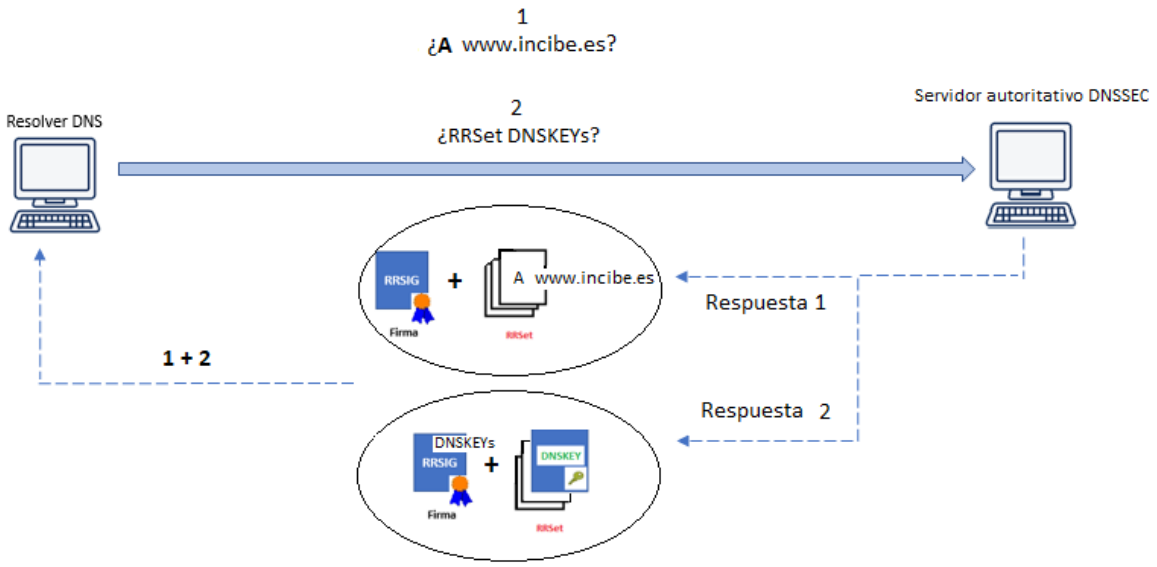



*Figura 9 - Resolución de nombres en DNSSEC: consulta al servidor y respuesta*

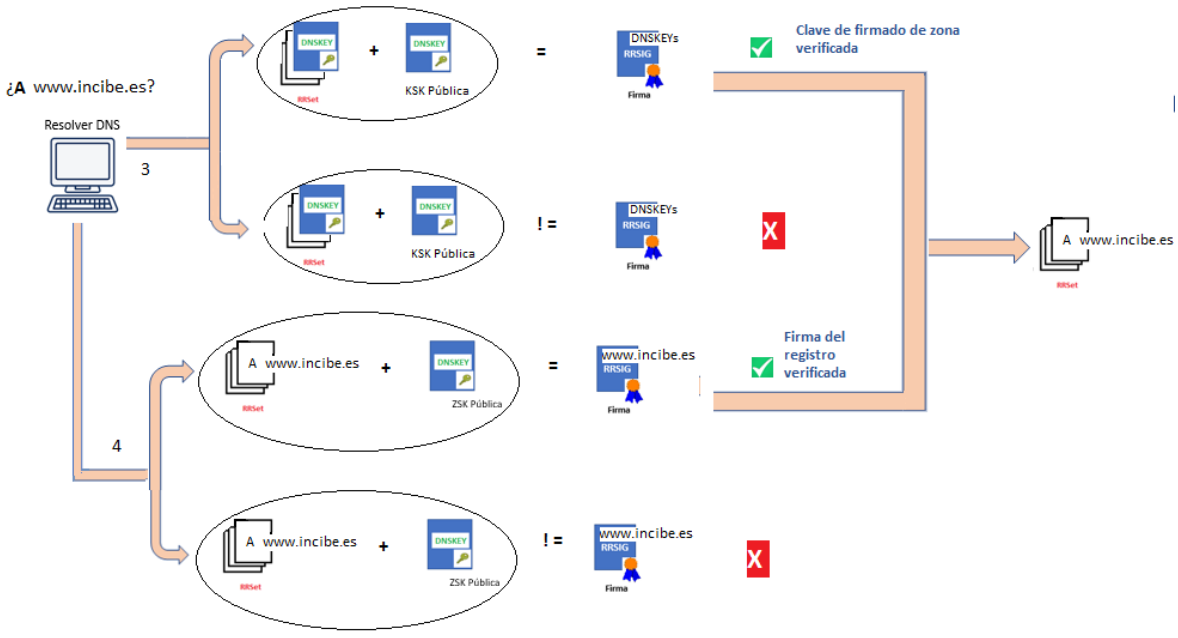



*Figura 10 - Resolución de nombres en DNSSEC: comprobación de la respuesta en el resolver*

Con los pasos descritos hasta este punto, el *resolver* DNSSEC puede verificar que el registro proporcionado para el recurso "www" por parte del servidor autoritativo de la zona "incibe.es" está firmado con la clave de zona (ZSK), y que la clave de zona está a su vez correctamente firmada con la clave de firma de zona (KSK). Pero, dado que la ZSK es autofirmada, falta ratificar que, efectivamente, las claves de firma empleadas pertenecen al servidor autoritativo legítimo. Para ello, hay que comprobar que se cumple la cadena de confianza (apartado "2.4.4. La cadena de confianza de DNSSEC"). Obviamente, para que la validación DNSSEC sea completa no sirve únicamente con que todas las zonas de

la cadena asociada a la consulta estén firmadas: es preciso también que el *resolver* formule la consulta indicando que desea realizar validación DNSSEC mediante la utilización de los bits DO ("DNSSEC OK") y AD ("AUTHENTIC DATA") descritos anteriormente.

### 2.4.4. La cadena de confianza de DNSSEC

Mediante las claves ZSK y KSK de DNSSEC se establece un nivel de confianza adecuado para una zona concreta. Sin embargo, el servicio DNS es jerárquico e incluye numerosas zonas que no operan de manera independiente, por lo que se hace necesario establecer relaciones de confianza entre una zona (hija) y su zona padre.

El elemento fundamental para el correcto funcionamiento de DNSSEC es el establecimiento de una **cadena de confianza** (*chain of trust*). Para que el receptor tenga la certeza de que la clave pública ZSK que se emplea para la verificación de las firmas es de confianza, ha de estar seguro de que la clave ZSK es auténtica y/o no ha sido comprometida. Si no se dispusiera de una cadena de confianza en DNSSEC, para evitar ataques de tipo MitM, el *resolver* recursivo tendría que almacenar y actualizar (manualmente o a través de otro canal) infinidad de claves públicas (una por cada servidor con el que estableciese comunicación), escenario que no es operativo por el elevado volumen de servidores DNS existentes.

Un ataque MitM en este escenario consistiría en que un atacante:

- Consigue interceptar las comunicaciones entre un *resolver* y un servidor DNS autoritativo.
- Genera una clave ZSK falsa para la zona a atacar.
- Consigue que el resolver acepte la clave pública ZSK mediante la manipulación también de la clave KSK

Por ello, es necesario establecer un mecanismo en DNSSEC que valide la clave pública KSK y, en consecuencia, la clave ZSK de una zona.

Si cualquiera de las relaciones intermedias de la cadena de confianza se rompe, no permitiendo llevar a cabo la validación de la autenticidad de las respuestas DNSSEC obtenidas, no sería posible confiar en DNSSEC, ya que un ataque MitM podría alterar los registros DNS obtenidos en las respuestas y redirigir a la víctima a cualquier dirección IP maliciosa.

La solución a dicho problema es la designación de un "***trust anchor***" (anclaje de confianza) en los servidores DNS raíz, es decir, una entidad con autoridad para la que se asume la confianza, en lugar de derivarse.

En el caso de DNSSEC, la confianza de toda la jerarquía de dominios comienza en la zona raíz. Así, para que la secuencia de validación se complete para un dominio concreto, cada organización o zona que se encuentra en el camino de resolución debe firmar la clave de la organización o zona inmediatamente inferior. Por ejemplo, para validar completamente el dominio "www.incibe.es", el servidor autoritativo de ".es" ha de validar y firmar la clave de ".incibe", y el servidor autoritativo raíz (".") debe validar y firmar la clave de ".es".

Se conoce como ***trust anchor*** al registro DNSKEY (normalmente asociado a la clave pública KSK de la zona raíz) que se configura en un *resolver* DNSSEC para validar

criptográficamente los resultados de una consulta hacia atrás (a lo largo de la jerarquía DNS), hasta llegar a una clave pública conocida (el *trust anchor*).

La pregunta que surge entonces es: ¿cómo se gestiona la cadena de confianza entre una zona padre y una zona hija? La solución se ofrece en DNSSEC a través de los registros **DS (*Delegation Signer*)**. Los registros DS permiten llevar la transferencia de confianza desde una zona padre a una zona hija ("Figura 11"):

- El responsable de una zona hija calcula el *hash* de su clave pública KSK.
- Ese *hash* se transfiere a la zona padre, que lo publica como registro DS asociado a esa zona hija.
- Cuando un *resolver* que soporta DNSSEC solicita al servidor padre el recurso NS de la zona hija, el padre le remitirá:
    - El RRSet del registro DS de la zona hija (lo que indica al *resolver* que la zona hija soporta DNSSEC).
    - El RRSIG del registro DS de la zona hija (firma con la ZSK del padre, como para el resto de los registros de la zona padre).
    - El RRSet de las DNSKEYs del padre.
    - El RRSIG de las DNSKEYs del padre (firmado con la KSK del padre).
    - El RRSet del registro NS de la zona hija solicitado.
    - El RRSIG asociado al RRSet del registro NS.

Cuando un servidor de nombres autoritativo de una zona padre remite a un *resolver* a una zona hija (proporcionando los registros DNS para los servidores de nombres autoritativos de la zona hija delegada, de tipo NS, *Name Servers*), adicionalmente le proporciona el registro DS correspondiente a la zona hija. La existencia del registro DS le permite a un *resolver* conocer que la zona hija ha implementado DNSSEC. Cuando el *resolver* reciba de la zona hija la clave pública KSK (mediante el registro DNSKEY asociado), calculará su *hash* y lo comparará con el del registro DS que le pasó el servidor DNS de la zona padre. Si ambos coinciden, el *resolver* habrá validado la clave KSK de la zona hija y podrá confiar en todos los registros firmados que procedan de la zona hija. Este proceso permite establecer una cadena de confianza en DNSSEC:

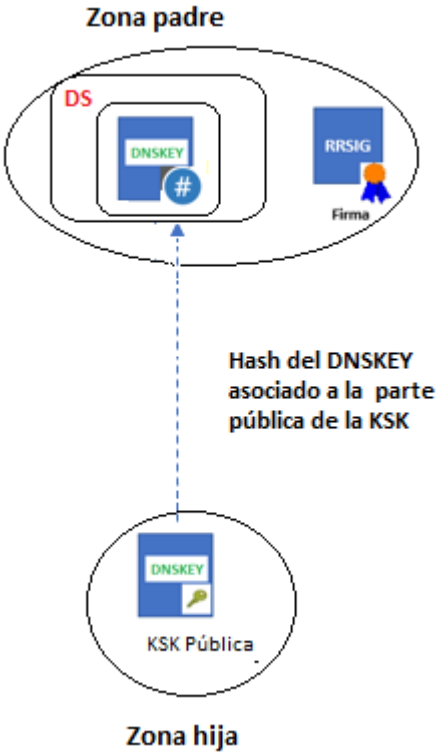



*Figura 11 - Registros DS de la zona hija en la zona padre*

Por su parte, cuando un *resolver* desea conocer el registro NS de una zona hija (en el ejemplo de la "Figura 12" se solicita a ".es" el NS asociado a "incibe.es"), ocurre lo siguiente (ver "Figura 12"):

1. El *resolver* pregunta por el registro NS de la zona hija ("incibe.es").
2. El servidor autoritativo de ".es" devuelve:
    a. El registro DS de "incibe.es" y su RRSIG.
    b. El registro NS de "incibe.es" y su RRSIG.
    c. El RRSet de las DNSKEYs de ".es" y su RRSIG.
3. El *resolver* valida el RRSet de las DNSKEYs de ".es" a través del RRSIG. Si la validación es exitosa, se confía en la zona padre ".es" y, por tanto, en el NS devuelto por ella.
4. El *resolver* se quedará con el registro DS de la zona hija. Cuando la consulte para obtener el recurso concreto, obtendrá de ella el DNSKEY de la KSK (en el ejemplo, asociado a "incibe.es"). Calculará el *hash* y lo comparará con el registro DS que le pasó la zona padre (".es").
5. Si el *hash* coincide con el DS, se confiará en los registros procedentes de la zona hija.

A causa de este mecanismo encadenado entre zonas padre y zonas hijas, y a las relaciones establecidas entre ambos, el proceso de renovación de la clave KSK de una zona hija requiere que su registro DS asociado sea actualizado en la zona padre. Esta es una de las operaciones más sensibles y delicadas a la hora de garantizar el correcto funcionamiento de DNSSEC. Tras el cambio de la clave KSK y la incorporación del nuevo registro DS a la zona padre, es preciso esperar hasta que el TTL del registro DS

correspondiente a la clave KSK anterior expire antes de borrarlo. Un fallo en esta operación provocaría que la zona hija no disponga de resolución. Como consecuencia se extrae que, dado que el sistema de nombres de dominio es un sistema distribuido y descentralizado, para que la validación de los registros DNS sea completa y pueda garantizarse que el cliente final se está conectando al recurso correspondiente a un nombre de dominio concreto, es preciso que DNSSEC esté operativo en cada paso de la resolución, y que se pueda validar la autenticidad e integridad de cada zona empezando por la zona raíz (".").

En resumen, la renovación de la clave KSK de una zona es un proceso más sensible, ya que tiene asociadas dependencias de la zona padre a través del registro DS. Sin embargo, la renovación de la clave ZSK es un proceso más sencillo, ya que se puede realizar de manera autónoma por parte del responsable de la zona, empleando su clave KSK existente.

Una vez se dispone de un mecanismo para establecer una cadena de confianza entre una zona y su zona padre, es necesario evaluar cómo se confía en el valor de los registros DS. Los registros DS son firmados como cualquier otro registro RRset, por lo que disponen de un registro RRSIG asociado en la zona padre. Para confiar en la autenticidad del registro DS y de su firma asociada, es necesario validar el mismo, así como la clave ZSK de la zona padre a través de su clave KSK. La clave KSK de la zona padre puede ser validada a través del registro DS de la zona superior, recorriendo toda la jerarquía DNS hasta llegar a la zona de más alto nivel o zona raíz.

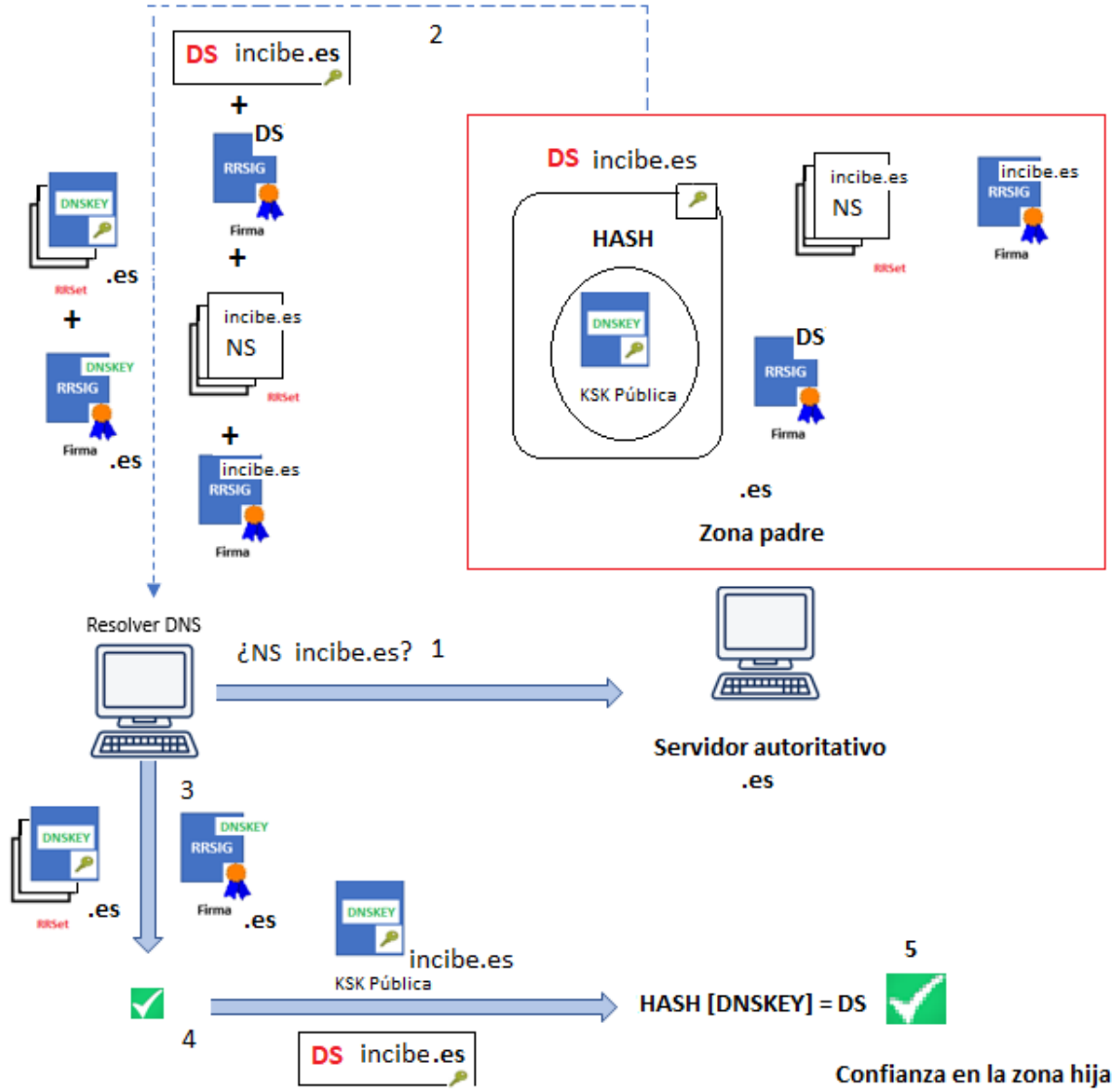



*Figura 12 - Proceso de validación de los registros DS y de las claves KSK de una zona hija*

La cadena de confianza establecida por DNSSEC finaliza con la validación de la autenticidad e integridad de los servidores raíz, que requiere de la intervención humana, ya que esta zona no dispone de ninguna zona padre que pueda validar su autenticidad. Este proceso de validación se conoce como la ceremonia de firmado de la zona raíz, o *Root Zone Signing Ceremony* [Ref.- 29], donde un conjunto concreto de personas seleccionadas estratégicamente a lo largo de todo el mundo, se reúnen para firmar un RRset de tipo DNSKEY que incluye las claves ZSK y KSK de la zona raíz (es decir, de los servidores de nombres raíz) de manera pública y bajo un estricto control de auditoría. Como resultado se genera el registro RRSIG del RRset de tipo DNSKEY de la zona raíz, que permite a cualquier servidor DNS verificar las claves ZSK y KSK de la zona raíz. La última ceremonia a fecha de elaboración de la presente guía fue la número 34 y se celebró el 15 de agosto de 2018 [Ref.- 29].

En resumen, en lugar de confiar en la clave KSK de la zona raíz a través del registro DS de la zona padre (inexistente), se asume que dicha clave es válida por los procedimientos de seguridad y gestión de la clave privada KSK de la zona raíz, y se establece el *trust anchor* principal en el servicio DNSSEC.

La "Figura 13" resume el mecanismo de resolución completo. En cada consulta a una zona padre (identificada por <número de secuencia>), el *resolver* obtendrá como respuesta (identificada por "R <número de secuencia>"), además del registro correspondiente al recurso solicitado, el registro DS de la zona hija, junto a la firma del registro DS y las DNSKEYs de la zona padre, que permitirán comprobar la autenticidad del siguiente eslabón según se describe en la "Figura 12".

Para la comprobación correspondiente a la zona raíz, el *resolver* tomará el RRSIG devuelto por el servidor autoritativo de dicha zona, asociado a la KSK pública de ".", y lo comparará con el RRSIG que tiene precompilado para la zona ".". Si la validación es positiva, se inicia la cadena de confianza y se dará por bueno el registro DS del TLD de nivel 1.

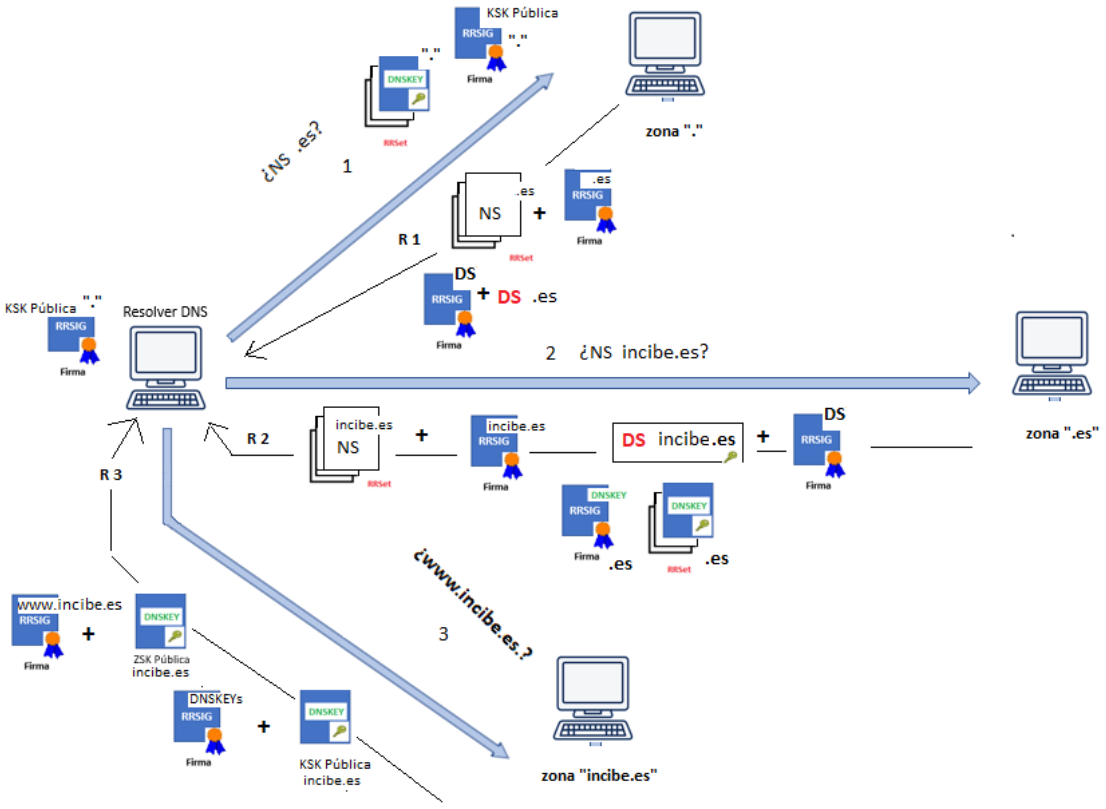



*Figura 13 - Secuencia de validación DNSSEC completa*

El despliegue inicial de DNSSEC en la zona raíz se realizó por acuerdos entre ICANN[13] y Verisign[14], completándose en julio de 2010 [Ref.- 7], de modo que actualmente está disponible para cualquier organización que se plantee la implantación de DNSSEC. En

[13] https://www.icann.org

[14] https://www.verisign.com

Internet existen 13 servidores de nombres raíz[15], es decir, encargados de gestionar el servicio DNS en el nivel más alto de la jerarquía ("."). En 2009, la transición de la zona raíz a DNSSEC se llevó a cabo en todos estos servidores, uno tras uno, desde finales de dicho año y progresivamente, con el objetivo de detectar efectos secundarios que podían haber sido pasados por alto, especialmente a nivel del tráfico DNS (por ejemplo, por el incremento en el tamaño de las respuestas del protocolo DNS).

Para posibilitar que el despliegue de DNSSEC sea exhaustivo para todos los nombres de dominio, adicionalmente al despliegue de DNSSEC en la zona raíz, los responsables de los TLDs de primer nivel (y de niveles inferiores) deben también desplegar DNSSEC en sus zonas, propagando así la cadena de confianza hasta los niveles inferiores de la jerarquía de dominios de DNS.

### 2.4.5. Gestión de recursos inexistentes en DNSSEC

Uno de los aspectos clave de DNSSEC es el modo en que resuelve el problema que se plantea en un escenario de **negación de existencia explícita** (*explicit denial of existence*) de recursos, es decir, cuando no existen registros DNS para un recurso concreto. El mecanismo por el cual se garantiza que una respuesta de negación de existencia es auténtica se conoce como "*authenticated denial of existence*", definido en el RFC 7129 [Ref.- 22], y es uno de los valores añadidos de DNSSEC sobre DNS.

Los servidores DNS tradicionales no definen un registro específico que represente que el recurso o subdominio por el que han sido interrogados no existe en su zona de autoridad, sino que, ante esa situación, devuelven una respuesta con un código de error que se denomina "NXDOMAIN" (*Non-eXistent Domain*) y cuyo campo "ANSWER" está vacío. Pero, desde el punto de vista de DNSSEC, en dicho escenario no podría realizarse la autentificación de la respuesta, ya que esta es vacía (debido a que la cabecera del paquete DNS no se firma en DNSSEC). Para solventarlo, DNSSEC añade dos nuevos registros:

- NSEC (*Next SECure*): ante la solicitud de registros DNS asociados a un recurso o subdominio en una zona concreta, el registro NSEC representa el siguiente registro que existe en la zona en orden canónico a partir del recurso consultado. NSEC resuelve el problema de recurso inexistente porque, si se consulta por un recurso que no existe, en lugar de un error, DNSSEC devolverá una respuesta cuyo registro NSEC apuntará al primer recurso que sí exista en la zona a partir del que fue solicitado. Por ejemplo, si un servidor tiene registros para "dns", "mail", "portal" y "www", y se le solicita el registro "test", el servidor DNSSEC devolverá un registro NSEC que contendrá "www" (al no existir ningún registro entre "test" y "www"). Este registro NSEC está firmado igual que cualquier otro registro RRset, por lo que el *resolver* puede validar su registro RRSIG correspondiente.
- NSEC3 (*Next SECure* versión 3): este registro se añadió para evitar un problema inherente a DNSSEC ocasionado por los registros NSEC, asociado a la revelación de los recursos y subdominios definidos en una zona.

[15] En realidad, el servicio DNS para la zona raíz de más alto nivel (".") es proporcionado por cientos de servidores DNS (que hacen uso de enrutamiento Anycast y de redundancia) asociados a los 13 servidores raíz, o a las 13 direcciones IP, definidos desde los orígenes del servicio DNS: https://www.cloudflare.com/learning/dns/glossary/dns-root-server/.

NSEC soluciona el problema de negación de existencia de un registro, pero la forma en que opera introduce otro problema: la exposición o revelación del contenido de la zona (*Zone Content Exposure*), que puede suponer un problema en aquellos dominios y zonas que tienen definidos registros que no se desea que sean conocidos desde el exterior si no se dispone de una referencia directa a los mismos (por ejemplo, un portal de empleados). Aunque los recursos DNS no se deberían considerar secretos, ya que el servicio no proporciona ninguna confidencialidad, en la práctica en ocasiones se dispone de recursos privados en una zona que no se desean dar a conocer ampliamente. Este problema surge por cómo se gestiona, a través del registro NSEC descrito previamente, una petición sobre un dominio inexistente [Ref.- 23]. Esta debilidad de DNSSEC permitiría la enumeración de registros en la zona consultada, de manera similar, aunque algo más compleja (al requerirse múltiples consultas DNSSEC) a la enumeración disponible cuando se permiten las trasferencias de zona DNS desde cualquier origen.

Este problema se debe al mecanismo de firma que usa DNSSEC para zonas estáticas. Una zona estática es el conjunto completo de registros (RRsets) que existen para un dominio. Cuando se usa DNSSEC para firmar una zona estática, los registros RRSIG de firma se crean mediante las claves KSK y ZSK. Siguiendo las buenas prácticas de seguridad de la industria, para no exponer las claves privadas de DNSSEC innecesariamente, habitualmente el proceso de firma de los registros se realiza en un servidor central de gestión de DNSSEC, y se transfieren posteriormente los registros de firma al servidor DNS autoritativo de la zona para su publicación. Otras implementaciones pueden hacer uso de técnicas para firmar los registros de DNSSEC en tiempo real[16].

Si un atacante quisiera conocer todos los recursos o subdominios de un dominio, podría solicitar la resolución de un recurso cualquiera (por ejemplo, para la zona "incibe.es", podría solicitar "test.incibe.es"). Al no existir el recurso, el servidor DNSSEC devolvería un registro NSEC apuntando al primer nombre de recurso que sí existe.

Iterando sobre los recursos devueltos en el registro NSEC, se puede reconstruir por completo los contenidos de la zona. Otra opción para el atacante sería solicitar los recursos NSEC de recursos conocidos que sí existen, para obtener la referencia al siguiente recurso en la zona. Para el ejemplo anterior, la zona firmada tendría los siguientes contenidos en el servidor DNS autoritativo:

```
incibe.es.          SOA    ( ... )
                    DNSKEY ( ... )
                    NS   dns.incibe.es.
                    NSEC dns.incibe.es. SOA DNSKEY NS RRSIG NSEC
                    RRSIG(NS)     ( ... )
                    RRSIG(SOA)    ( ... )
                    RRSIG(NSEC)   ( ... )
                    RRSIG(DNSKEY) ( ... )
dns.incibe.es.      A 192.0.2.1
                    TXT "Servidor DNS"
                    NSEC mail.incibe.es. A TXT RRSIG NSEC
                    RRSIG(A)    ( ... )
                    RRSIG(TXT)  ( ... )
                    RRSIG(NSEC) ( ... )
```

[16] https://www.cloudflare.com/dns/dnssec/ecdsa-and-dnssec/

```
mail.incibe.es.      A 192.0.2.2
                     TXT "Servidor de correo"
                     NSEC portal.incibe.es. A TXT RRSIG NSEC
                     RRSIG(A)     ( ... )
                     RRSIG(TXT)   ( ... )
                     RRSIG(NSEC)  ( ... )
portal.incibe.es. A  192.0.2.3
                     TXT "Portal"
                     NSEC www.incibe.es. A TXT RRSIG NSEC
                     RRSIG(A)     ( ... )
                     RRSIG(TXT)   ( ... )
                     RRSIG(NSEC)  ( ... )
www.incibe.es.       A 192.0.2.4
                     TXT "Servidor web"
                     NSEC incibe.es. A TXT RRSIG NSEC
                     RRSIG(A)     ( ... )
                     RRSIG(TXT)   ( ... )
                     RRSIG(NSEC)  ( ... )
```

*Figura 14 - Registros asociados a DNSSEC en el fichero asociado a la zona*

Los registros NSEC crean una cadena o lista enlazada circular entre todos los registros de la zona estática, que incluye todos los recursos o subdominios existentes en la misma. Cuando un servidor DNSSEC remite una consulta solicitando "test.incibe.es", recibiría un registro NSEC referenciando el siguiente recurso por orden canónico, es decir, "www" (desvelando así su existencia):

```
portal.incibe.es.      NSEC www.incibe.es. A TXT RRSIG NSEC
```

En la zona estática, aunque "test.incibe.es" debería seguir a "portal.incibe.es", el registro NSEC obtenido para el siguiente recurso corresponde a "www.incibe.es" y, por tanto, "test" no existe (debería estar entre ambos recursos). Iterando sobre los datos de los registros NSEC, se puede recorrer la zona por completo (ataque conocido como *zone enumeration* o *zone walking*) y saber cuáles son todos sus registros. Para evitar este inconveniente, surgió el registro NSEC3 que, en lugar de almacenar el nombre del siguiente recurso o subdominio existente para cada registro, almacena un *hash* criptográfico del mismo. Sin embargo, NSEC3 no es completamente inmune a los ataques de enumeración de zona, ya que, un atacante puede llevar a cabo múltiples consultas DNSSEC y conseguir un número suficiente de *hashes* a partir de los registros NSEC3 de recursos no existentes. Posteriormente, el atacante podría hacer uso de técnicas *offline*, no desvelando además sus actividades al no requerir interactuar posteriormente con los servidores DNS autoritativos, mediante ataques de diccionario (o fuerza bruta en el caso de nombres cortos) para adivinar los nombres de todos los recursos asociados a los diferentes *hashes* obtenidos previamente.

En el año 2014 se publicó una propuesta sobre la introducción de un nuevo registro, NSEC5, que pretende solventar por completo el problema de la enumeración de zonas de DNSSEC. Los detalles de NSEC5 quedan fuera del alcance de la presente guía, aunque se dispone de más información en el documento [Ref.- 24].

## 2.5. ¿Qué beneficios aporta DNSSEC?

Desde el punto de vista de los servidores de nombres intermedios, la implantación de DNSSEC proporciona **autenticidad** sobre los datos del servicio DNS, evitando los ataques de envenenamiento de caché DNS que pueden ser empleados por un atacante para redirigir a un usuario víctima hacia sitios maliciosos que suplantan a un servidor legítimo u ocasionar que los servicios de la organización estén inaccesibles.

Junto a una gestión correcta de las claves criptográficas DNSSEC también dificulta la realización de ataques MitM a nivel del servicio DNS, ya que, al establecerse una cadena de confianza a lo largo de toda la jerarquía de DNS, la **autenticidad e integridad** de los datos obtenidos puede ser completamente verificada.

Un atacante tendría que disponer de acceso a las claves privadas del servidor de nombre raíz y, partiendo de él, intentar modificar la validez del resto de la cadena (o alternativamente, a las claves privadas de un servidor de nombres intermedio, afectando a las zonas autoritativas a delegadas por este).

Estas capacidades de protección no eximen de que un servidor DNS pueda ser comprometido por otros medios, y que este acceso no autorizado permita la modificación y manipulación de los datos asociados al protocolo DNSSEC.

Desde el punto de vista tanto de los clientes DNS, como del propietario o responsable de un dominio, DNSSEC asegura la **integridad** de los datos del servicio DNS, es decir, que no han sido manipulados. No obstante, es importante destacar que DNSSEC no protege frente a ataques de secuestro de un dominio, en los que un atacante (habiendo obtenido previamente las credenciales de acceso para la gestión de dicho dominio víctima) cambia los registros asociados a los servidores DNS legítimos haciendo que apunten a sus propios servidores DNS falsos, desde los cuales podrá forzar a que el tráfico destinado a los servicios legítimos sea redirigido a sus servicios maliciosos.

Adicionalmente, DNSSEC también permite distribuir de manera confiable registros que encapsulen claves empleadas para proteger otros servicios, como el correo electrónico y las aplicaciones web, de forma que se establezca una comunicación de confianza entre organizaciones (ver apartado "4.3. DANE: Más allá del DNS").

El escenario ideal para establecer comunicaciones seguras en Internet pasa por la combinación de DNSSEC con otras tecnologías y protocolos de seguridad, como TLS (*Transport Layer Security*), empleado en múltiples servicios como, por ejemplo, el tráfico web mediante HTTPS, con el objetivo de proteger las comunicaciones entre usuarios y servicios a múltiples y complementarios niveles.

## 2.6. Dificultades y desafíos en la implantación de DNSSEC

La implantación de DNSSEC, si bien muy recomendable desde el punto de vista de seguridad para proteger las transacciones DNS de toda organización, implica una serie de dificultades y desafíos que deben evaluarse concienzudamente.

En este apartado se proporciona un resumen de los aspectos a considerar durante el proceso de diseño e implantación de DNSSEC por parte de una organización, que se describirán con mayor detalle en el apartado "4. Aspectos clave en el diseño e implantación" de la presente guía.

- Determinar si la gestión del dominio en el servicio DNS se delegará en un proveedor de servicios externo o se administrará localmente, dado que en DNSSEC un elemento fundamental es la gestión de las claves (ver apartado "4.1. Consideraciones organizativas").
- Sopesar las ventaja e inconvenientes a nivel técnico del uso de DNSSEC: el funcionamiento del protocolo DNSSEC presenta diferencias notables respecto a DNS en cuestiones básicas del día a día, las cuales hay que tener muy presentes para definir una operativa que garantice el correcto funcionamiento del servicio (ver apartado "4.2.2. Aspectos que afectan a la operativa del servicio DNSSEC").
- Evaluar las implicaciones organizativas derivadas del uso de DNSSEC: será preciso elaborar una lista detallada de requisitos a nivel organizativo, que incluyan el personal capacitado que será necesario dedicar a la correcta definición y ejecución de las políticas de gestión del entorno de DNSSEC (ver apartado "4.1. Consideraciones organizativas").
- Valorar correctamente las implicaciones económicas que tendrá para la organización la puesta en marcha de todos los recursos necesarios para la implantación de DNSSEC (ver apartado "4.4. Costes de implantación y motivación").

# 3. ESTADO ACTUAL Y NIVEL DE IMPLANTACIÓN

El presente apartado pretende ofrecer una imagen completa sobre el estado de implantación de DNSSEC, a nivel internacional (con datos para Europa, América y Asia) y particularizado para los dominios ".es". Se presentará su evolución en el tiempo, junto a estadísticas detalladas obtenidas de diversas fuentes, con referencias explícitas a cada una de ellas que permitan al lector profundizar en aquellos aspectos que considere más interesantes y obtener los últimos datos disponibles.

Por tanto, no solo se ofrecerá la visión del momento actual, sino que se proporcionará la información suficiente para conseguir los datos necesarios de cara a futuro.

## 3.1. Experiencia y visión internacional

La gestión de los TLDs de primer nivel se lleva a cabo a través de la figura conocida como "Registro" (*Registry* en terminología anglosajona). Para los ccTLDs, según el país, esta gestión se puede llevar a cabo a través de una entidad pública o privada. Así, por ejemplo, para el ccTLD de España, el Registry es "Red.es"; para los gTLDs ".com" y ".net", el Registro es Verisign. Por otra parte, el alta de un dominio de segundo nivel se realiza a través de un agente registrador (conocido como *Registrar* en terminología anglosajona), que recibe la petición del cliente final y la traslada al Registro correspondiente al TLD de primer nivel. Para más detalles sobre la relación entre ICANN, los *Registrars* y los *Registries*, se recomienda consultar la [Ref.- 59].

Los datos que se ofrecerán a lo largo del presente apartado están tomados de diversas fuentes, en función de los organismos competentes para las diversas zonas del servicio DNS.

Como se detalló en el apartado de introducción, DNSSEC se fundamenta en una cadena de confianza, que requiere que cada dominio confíe en el dominio de nivel superior. En la introducción de la presente guía se comentó que el despliegue de DNSSEC en la zona raíz (".") se completó en julio de 2010, con la generación de las claves raíz (KSK y ZSK) mediante el algoritmo de firma RSA-SHA256.

La siguiente tabla, obtenida a partir de los datos del estudio publicado por EURid [Ref.- 18] en octubre de 2010, ofrece una visión sobre el despliegue de DNSSEC en los 283 TLDs activos en dicha fecha:

| Año 2010 | Septiembre | Octubre |
|---|---|---|
| **Número total de TLDs** | 283 | 283 |
| **Número de TLDs con RRs de tipo DNSKEY (en su zona)** | 32 (11%) | 37 (13%) |
| **Número de TLDs con registros DS (en la zona . )** | 18 (6%) | 29 (10%) |

*Tabla 1 - Estadísticas del despliegue de DNSSEC en los TLDs (2010)*

A continuación, se ofrecerá una visión sobre el firmado de las zonas correspondientes a los TLDs de primer nivel.

### 3.1.1. Despliegue de DNSSEC a nivel de ccTLDs

Dado que la base para la implantación de DNSSEC a nivel de organización independiente que dispone de su dominio bajo el ccTLD asignado a su país tiene como requisito indispensable el firmado de la zona asociada al dominio del país al que pertenece, en este apartado se analizará el estado actual de las distintas regiones del mundo.

Para la obtención de estos datos, se han empleado los mapas de estado del despliegue de DNSSEC generados por Internet Society, fundada en 1992 por miembros del IETF (*Internet Engineering Task Force*) [Ref.- 17]. Internet Society publica semanalmente una serie de mapas del estado de DNSSEC para los ccTLDs en las distintas regiones del mundo. Además, Internet Society gestiona una lista de distribución de libre suscripción [Ref.- 70] en la que se publican estos datos, lo que permite obtener una visión actualizada de la evolución de los ccTLDs[17].

Para la elaboración de estos mapas, se establece una clasificación del estado de cada dominio (ccTLD) analizado:

- *Experimental* (experimental): se concede esta clasificación cuando Internet Society identifica algún tipo de actividad relacionada con DNSSEC procedente del organismo responsable del dominio ccTLD, como mensajes en listas de distribución, participación en formación relativa a DNSSEC, o presentaciones en conferencias, es decir, este estado no implica que se haya iniciado ningún tipo de acción efectiva para implantar DNSSEC en la zona asociada al dominio.
- *Announced* (anunciado): el organismo competente para el dominio ccTLD ha manifestado públicamente el despliegue de DNSSEC y el firmado de su zona.
- *Partial* (parcial): este estado significa que la zona del dominio se ha firmado públicamente mediante DNSSEC, pero su registro DS aún no está publicado en la zona raíz, es decir, el ccTLD no está aún ligado a una cadena de confianza, aunque sus servidores autoritativos ya publiquen registros firmados.
- *DS in Root* (registro DS en zona raíz): se alcanza este estado cuando la zona raíz publica el registro DS asociado al dominio ccTLD, integrándolo en la cadena de confianza global, con lo que los dominios de segundo nivel que cuelgan de él ya pueden realizar validación mediante DNSSEC.
- *Operational* (operativo): se obtiene este estado cuando el organismo competente del dominio ccTLD acepta delegaciones firmadas de dominios de segundo nivel bajo él. Esto permite que cualquier entidad que registre un dominio bajo dicho ccTLD pueda proceder a firmar dicho dominio y añadir su registro DS en la zona del dominio ccTLD padre (el que se encuentra en estado operativo).

#### 3.1.1.1. Visión global

Desde un punto de vista global o internacional, en base a los mapas publicados por Internet Society, cabe destacar que algunos ccTLDs habían completado su despliegue de DNSSEC en el año 2009, incluso antes de que se firmase el dominio o zona raíz (".") en el año 2010. Curiosamente, entre ellos, estaban países no necesariamente punteros tecnológicamente hablando, como Brasil y Namibia.

[17] Estos mapas están sujetos a la licencia "*Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License*" (https://creativecommons.org/licenses/by-nc-sa/3.0/deed.en_US) [Ref.- 17].

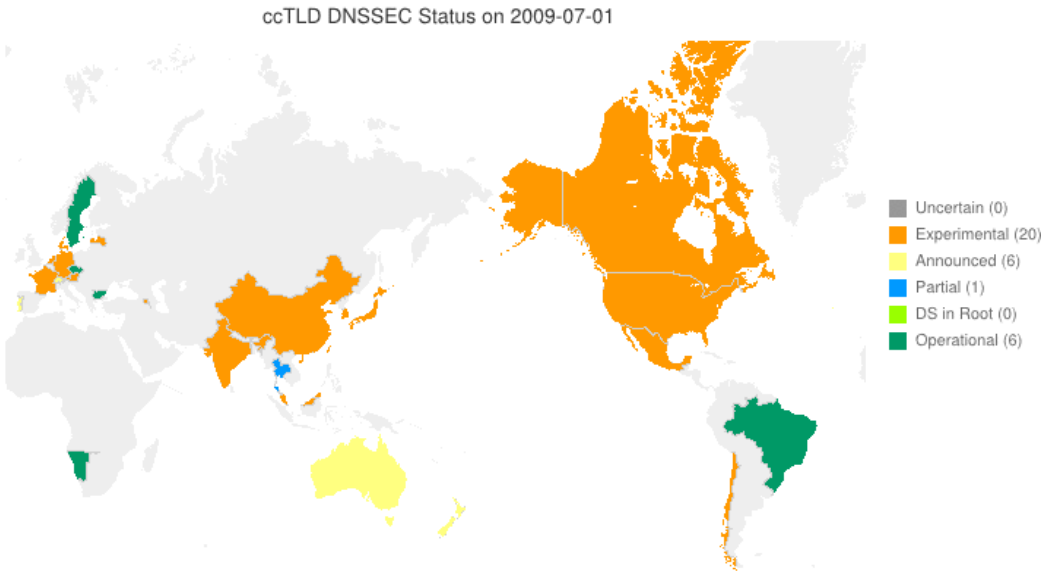



*Figura 15 - Mapa de estado de DNSSEC de los ccTLDs a nivel mundial (julio 2009)*

En julio de 2010, mes en el que se llevó a cabo el despliegue inicial de DNSSEC en la zona raíz, más países, incluyendo Estados Unidos y un número reducido de países de Europa, Oriente Medio y Asia también se encontraban en estado operativo.

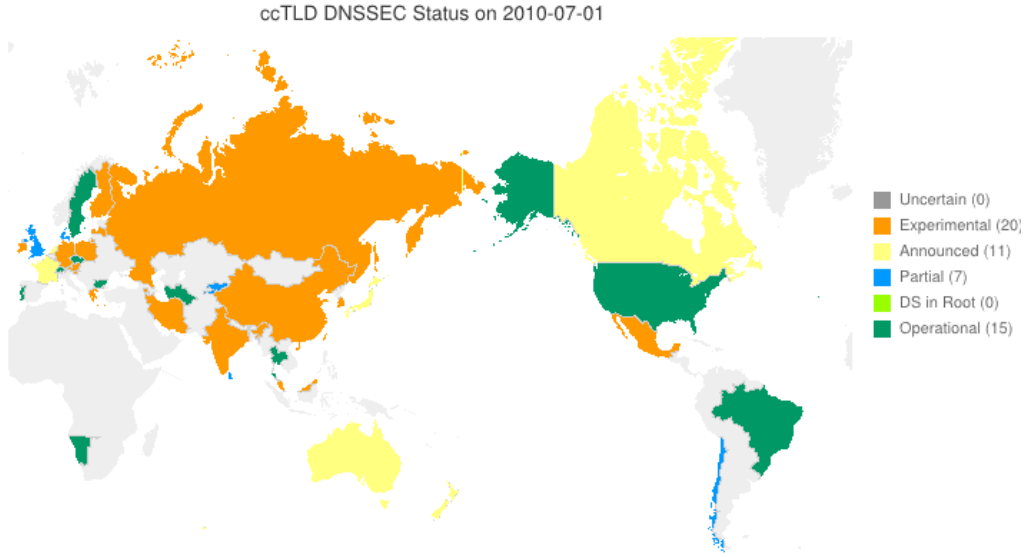



*Figura 16 - Mapa de estado de DNSSEC de los ccTLDs a nivel mundial (julio 2010)*

El mapa completo a fecha de elaboración de la presente guía muestra que los países considerados más desarrollados han realizado exitosamente el despliegue de DNSSEC en sus respectivos ccTLDs, encontrándose en estado operativo. Por tanto, nada impediría a día de hoy que el grueso de las operaciones de resolución de nombres del servicio DNS en Internet se realizase a través de DNSSEC.

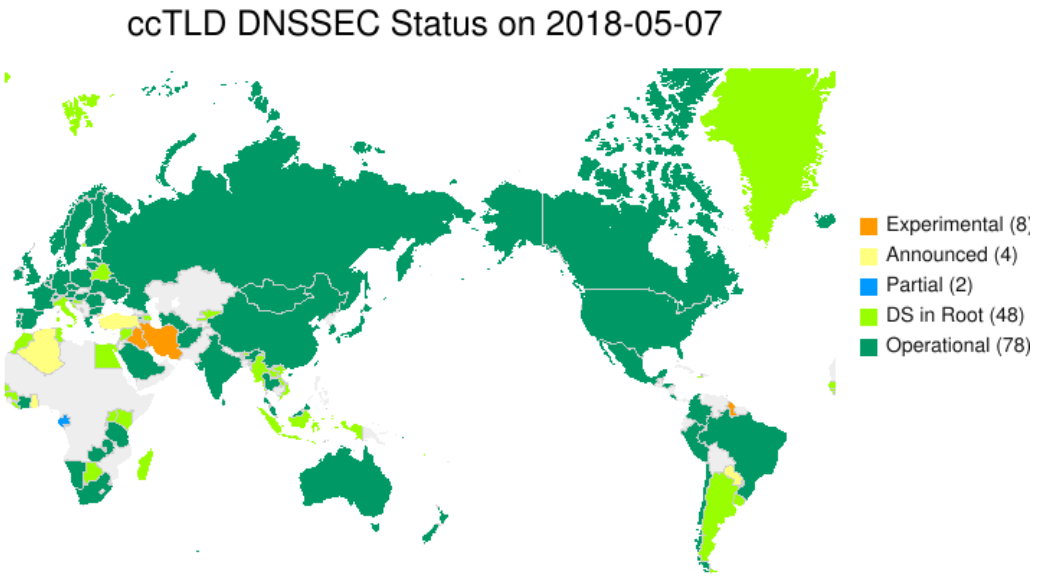



*Figura 17 - Mapa de estado de DNSSEC de los ccTLDs a nivel mundial (mayo 2018)*

Por su parte, los dominios que garantizan la resolución inversa, in-addr.arpa e ip6.arpa, se encuentran también firmados desde 2010.

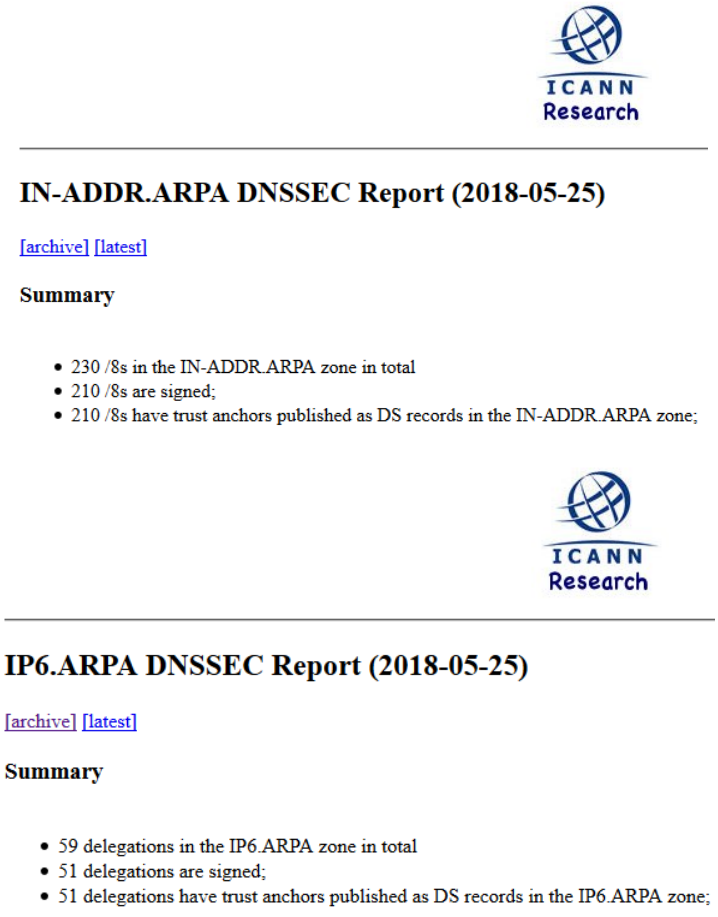



*Figura 18 - Despliegue de DNSSEC para resolución inversa*

### 3.1.1.2. Europa

Dentro del presente apartado, se incluye como elemento especial el despliegue de la zona ".eu", que se trata como un dominio ccTLD, aunque no corresponde a un único país, sino a toda Europa. EURid, el agente registrador del TLD de primer nivel ".eu" por acuerdo de la Comisión Europea de 2003 [Ref.- 18], inició el despliegue de DNSSEC para la zona ".eu" en dos fases, con objeto de poder evaluar tanto el impacto del incremento de los datos asociados a los procesos de generación y firmado de las zonas en DNSSEC, como para poner a prueba los procesos necesarios para la gestión de las claves DNSKEY:

- Se añadieron los registros DNSKEY de la clave de zona ZSK y los registros RRSIG correspondientes a las firmas de la zona ".eu", pero los registros DS correspondientes a la clave KSK fueron omitidos. Durante esta fase, EURid puso a prueba los procedimientos disponibles para los agentes registradores de Europa, ya que los registros DS que un agente registrador proporciona para un dominio eran cotejados con la información disponible en los servidores de nombres de dicho dominio, mediante las correspondientes claves de los registros DNSKEY, antes de ser publicados en la zona ".eu".
- En septiembre de 2010, el registro DS asociado a los registros DNSKEY de la clave KSK de la zona ".eu" fue publicado en la zona raíz ("."), completando así la cadena de confianza para el TLD ".eu".

En el estudio de EURid previamente mencionado [Ref.- 18], se publicaron las siguientes estadísticas relativas al despliegue de DNSSEC en los TLDs miembros del CENTR (*Council of European National Top-Level Domain Registries*), entidad europea, en septiembre de 2010.

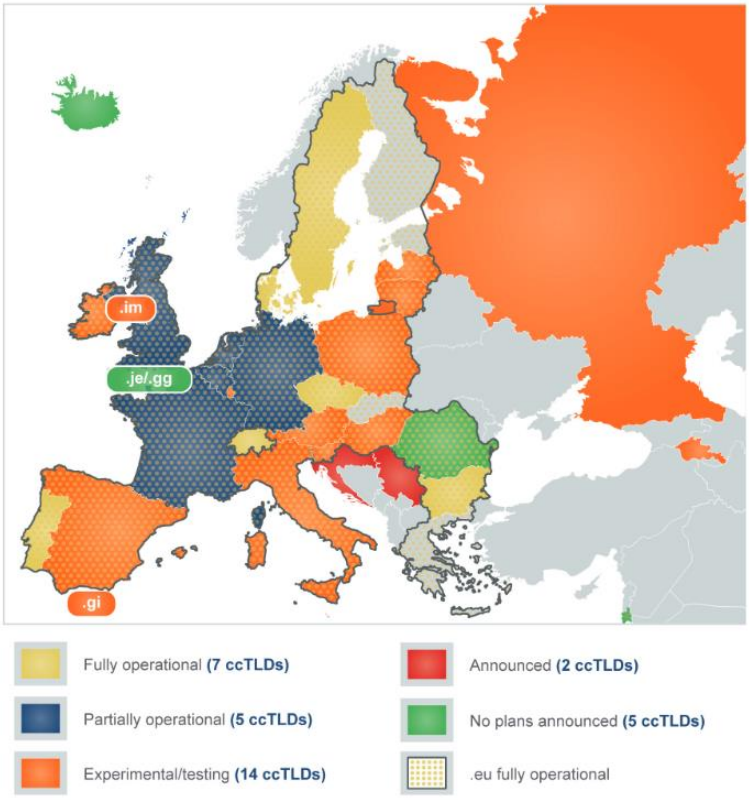


*Figura 19 - Implantación de DNSSEC en TLDs miembros del CENTR (septiembre 2010)*

Como puede apreciarse en la imagen, en aquel momento el dominio ".es" estaba en fase experimental desde el punto de vista de DNSSEC.

A continuación, se muestran los mapas con la evolución de DNSSEC de los ccTLDs europeos desde 2013 hasta la fecha de elaboración de la presente guía. En aquel momento inicial, agosto de 2013, el dominio ".es" continuaba en fase experimental.

En la actualidad, como se aprecia en el último mapa de la serie, todos los ccTLDs europeos salvo 8 están firmados, pero estos 8 ccTLDs están ya en la última fase de despliegue y han publicado su registro DS en la zona raíz.

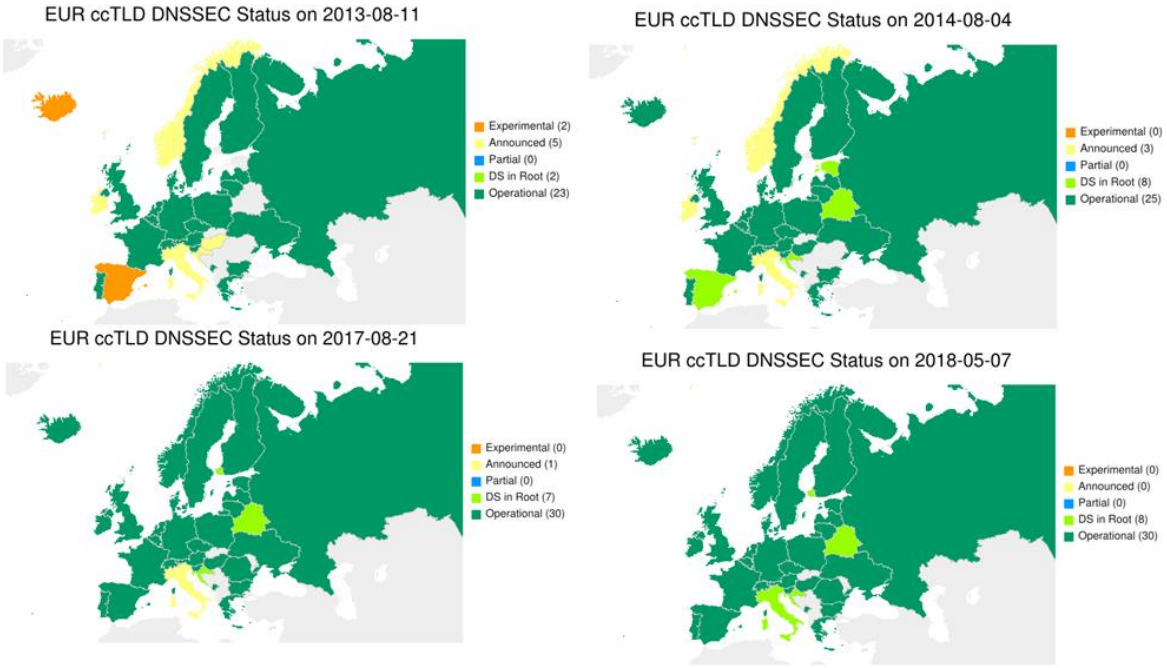



*Figura 20 - Mapas de estado de los ccTLDs de Europa y su evolución (2013-2018)*

### 3.1.1.3. América y Asia-Pacífico

A fecha de elaboración de la presente guía, el mapa de estado de DNSSEC de los ccTLDs del continente americano muestra que no todos los países han completado su despliegue. Entre ellos, se encuentran Venezuela, Ecuador, Bolivia y Cuba. Argentina ha publicado ya su registro DS en la zona raíz, pero aún no está completamente operativo. En Norte América, tanto Estados Unidos, como Canadá se encuentran en estado operativo.

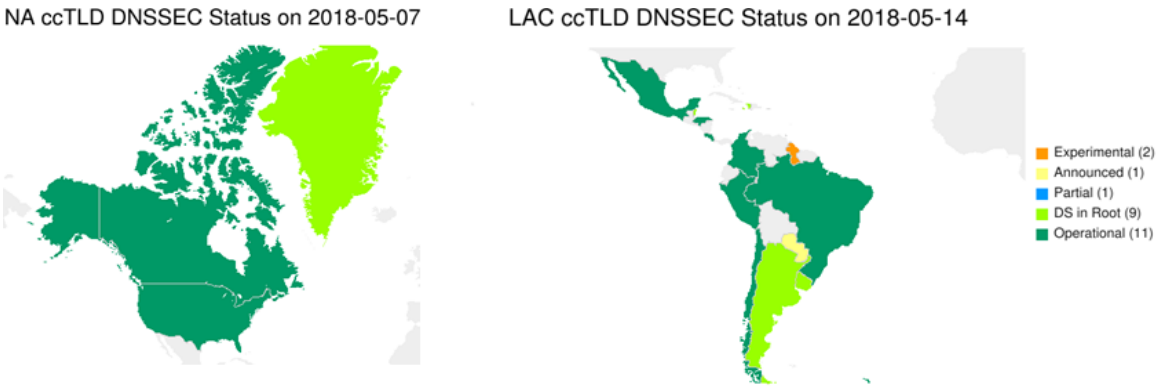



*Figura 21 - Mapas de estado de los ccTLDs de América (mayo 2018)*

Por su parte, la mayoría de los dominios de la zona Asia-Pacífico sí están en estado operativo, aunque todavía hay un número significativo de países que no lo están, sí han publicado ya su registro DS en la zona raíz. En la zona de Oriente Medio es dónde se identifican más países todavía en un estado menos maduro respecto a DNSSEC:

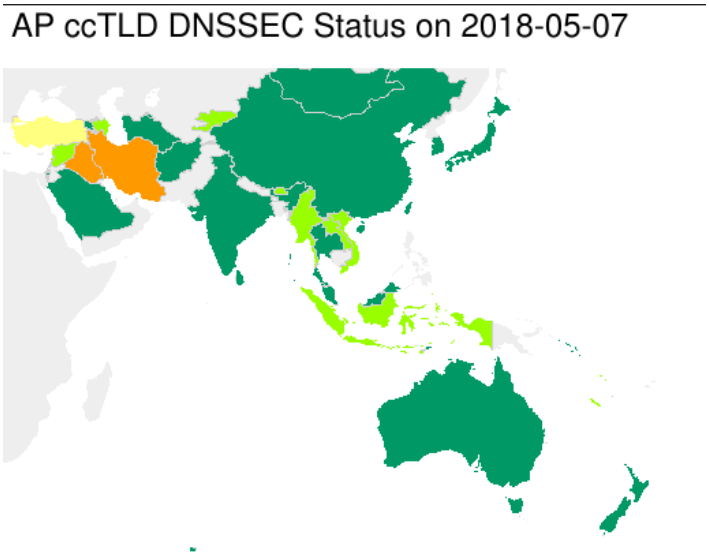



*Figura 22 - Mapa de estado de los ccTLDs de Asia-Pacífico (mayo 2018)*

### 3.1.2. Despliegue de DNSSEC a nivel de gTLDs

La obtención de estadísticas en función de la geografía para los gTLDs resulta muy compleja, dado que los dominios genéricos, como ".com", están disponibles para entidades de cualquier tipo (siempre que cumplan con los requisitos que establezca el órgano gestor del gTLD) independientemente de su localización geográfica.

El proyecto *ICANN Research* [Ref.- 48] ofrece informes diarios con las estadísticas de todos los TLDs de primer nivel, incluyendo tanto ccTLDs como gTLDs, y su estado respecto a DNSSEC. En el informe correspondiente al 11 de mayo de 2018, se observa que, de los 1.543 TLDs de primer nivel, 1.407 están firmados, y 1.399 tienen su registro

DS publicado en la zona raíz, por lo que pueden emplearse como eslabón de la cadena de confianza por parte de sus subdominios delegados.

Por lo que, solo 136 dominios de primer nivel de la zona raíz (menos del 10%) están aún sin firmar. El motivo de estas cifras tan elevadas de zonas firmadas para los dominios de primer nivel es que, por un lado, la mayoría de dichos dominios corresponden a ccTLDs (y la mayor parte de países ya ha completado el despliegue de su zona; ver apartado "3.1.1. Despliegue de DNSSEC a nivel de ccTLDs") y, por otro lado, que el ICANN obliga desde hace tiempo a todos los gTLDs de primer nivel a estar firmados en DNSSEC como requisito para darlos de alta en la zona raíz.

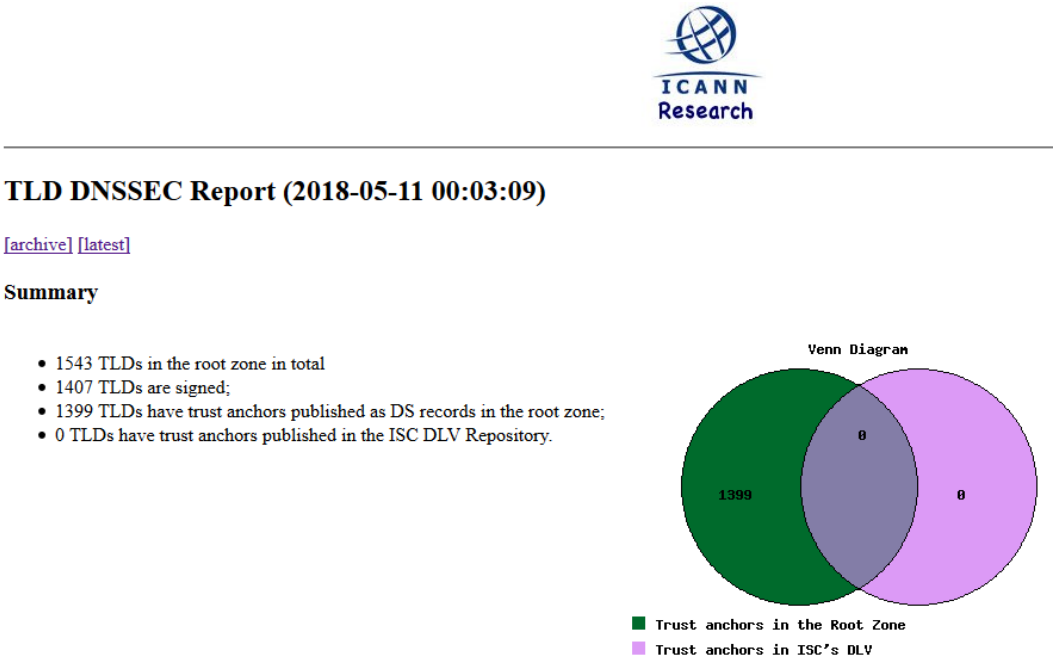



*Figura 23 - Informe de estado de DNSSEC en los TLD de primer nivel (mayo 2018)*

El gráfico que representa las siglas "DLV" (*DNSSEC Look-aside Validation*) hace referencia a una extensión del protocolo DNSSEC, que se diseñó como mecanismo de transición para facilitar la adopción temprana de DNSSEC. DLV permitía la firma y validación mediante DNSSEC de un dominio cuyo padre no estaba en la cadena de confianza o delegación establecida en la jerarquía de DNS. Este protocolo fue desmantelado por el ISC (*Internet Systems Consortium*) en septiembre de 2017.

Respecto a la evolución en el número de dominios firmados en los TLDs de primer nivel, también se dispone del siguiente gráfico publicado por ICANN en octubre de 2017:

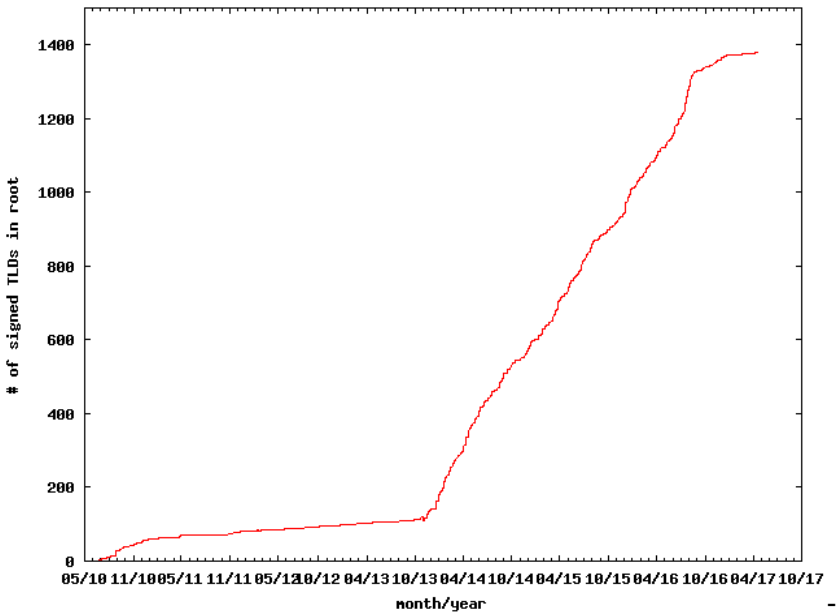



*Figura 24 - Gráfica de la evolución de TLDs firmados en la zona raíz*

Se observa que el despegue en la firma de los TLDs de primer nivel se inició a finales de 2013, y presentó un elevado incremento hasta finales de 2016. Tomando como valor para mayo de 2018 los 1.407 dominios firmados de la "Figura 23", se sigue observando un ligero aumento en el número total de dominios firmados en la zona raíz, aunque lógicamente (debido a la complejidad de disponer del 100% de dominios TLD firmados), a medida que el número de TLDs de primer nivel firmados se acerca al número total de TLDs de la zona raíz, el gráfico de crecimiento se aplana.

Complementariamente, la siguiente gráfica de nTLDStats[18], proporciona los detalles de los gTLDs, reflejándose que del total de más de 1.200 gTLDs existentes, y de sus más de 23 millones de dominios de segundo nivel delegados, únicamente están firmados algo más de un 0,5% (125.291 zonas).

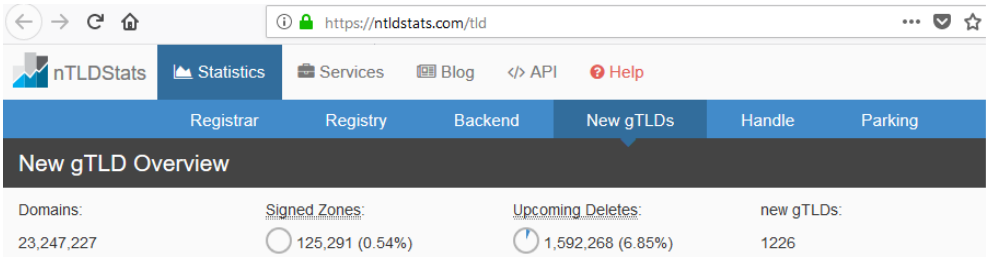



*Figura 25 - Estadísticas globales y de adopción de DNSSEC en los gTLDs a nivel mundial*

### 3.1.3. Despliegue de DNSSEC en TLDs de segundo nivel y niveles inferiores

Para la obtención de estadísticas relativas a los TLDs de segundo nivel (y niveles inferiores) hay que diferenciar dos casos:

[18] https://ntldstats.com/tld

- TLDs de segundo nivel asociados a un ccTLD: pueden analizarse bajo criterios geográficos. Dada la elevada cantidad de países existentes, se ofrecerán únicamente los datos que se consideren de más interés, teniendo en cuenta que, además, no todos los países publican cifras relativas a DNSSEC.
- TLDs de segundo nivel asociados a un gTLD: debido al carácter distribuido y descentralizado del servicio DNS, la obtención de cifras basadas en localización geográfica para los principales dominios de Internet. (.com, .org, .net) es tremendamente complicada, sin que se hayan podido encontrar referencias de las que sea posible obtener estadísticas de relevancia geográfica.

Por este motivo, la clasificación realizada en este apartado no es homogénea.

### 3.1.3.1. DNSSEC en Estados Unidos

A continuación, se mostrarán datos obtenidos del NIST (*National Institute of Standards and Technology*), que tiene en marcha un programa para estimar la implantación de IPv6 y DNSSEC en el gobierno de los Estados Unidos (dominios ".gov") y en las universidades americanas (dominios ".edu"). El NIST no utiliza sondeos en tiempo real para la elaboración de estas estadísticas, sino muestras obtenidas para un subconjunto de TLDs de segundo nivel [Ref.- 30]. Dada la especificidad del estudio, no se proporcionarán todos los datos aportados por él, pero sí los siguientes gráficos resumen que ilustran la situación actual de la implantación de DNSSEC en los TLDs de segundo nivel de las instituciones gubernamentales y las universidades americanas.

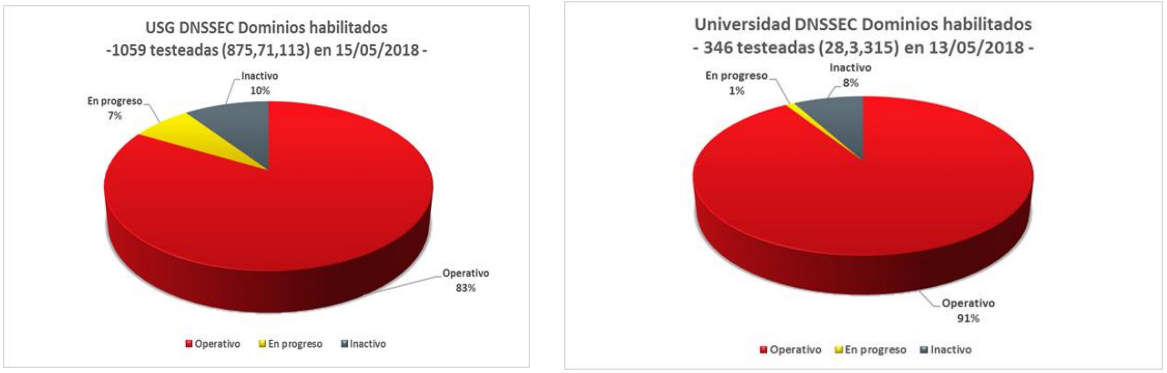



*Figura 26 - Estimaciones del NIST de despliegue de DNSSEC en gobierno y universidades americanas*

A fecha de elaboración de la presente guía, es llamativa la amplia difusión de DNSSEC en los TLDs de segundo nivel del gobierno de los Estados Unidos, que supera el 80%. Sin embargo, las universidades americanas distan mucho de estos niveles de implantación, con únicamente un 8% de dominios dónde DNSSEC está operativo.

Dentro de este programa de seguimiento, se pueden obtener más detalles sobre el estado de los TLDs de segundo nivel del dominio ".gov"[19] y de las universidades ".edu"[20].

### 3.1.3.2. DNSSEC en los dominios ".com", ".net" y ".edu"

[19] *https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov*

[20] *https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-edu*

En este apartado se persigue ofrecer una visión lo más concisa posible de la implantación de DNSSEC en los dominios gTLD más extendidos. Casi cualquier organización, independientemente del país en el que opere, suele registrar su dominio, además de bajo el ccTLD de uno o varios países, bajo el dominio ".com". Por ello, los datos que aquí se reflejan resultan de especial relevancia a nivel internacional.

La empresa DomainTools ofrece estadísticas generales sobre el número de dominios de nivel 2 existentes, ordenados por orden decreciente (ver "Figura 27") [Ref.- 52]. A modo de referencia, se puede ver como existen casi 135 millones de dominios ".com", más de 14 millones de dominios ".net", más de 10 millones de dominios ".org", y 3,7 millones de dominios ".eu".

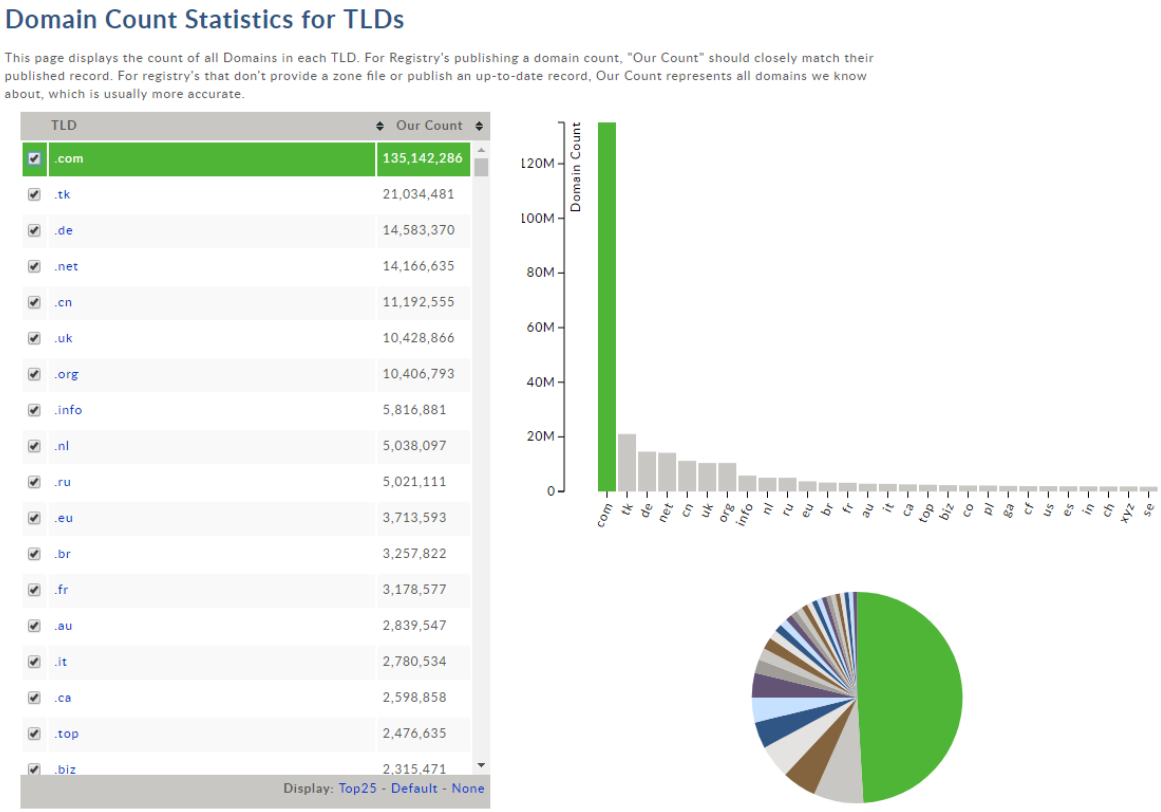



*Figura 27 - Estadísticas de TLDs de nivel 2*

Por otra parte, Verisign, en el marco de la estrecha relación que mantiene con el ICANN en las cuestiones referentes a DNSSEC, publica interesantes estadísticas sobre DNSSEC, además de guías de referencia y herramientas centradas en este protocolo. Uno de los recursos que ofrecen para dar la visión de los dominios ".com", ".net" y ".edu" es el ScoreBoard [Ref.- 53], en el que se recogen diariamente las cifras relativas a dominios que emplean DNSSEC. A fecha de elaboración de la presente guía, estas cifras son las siguientes:

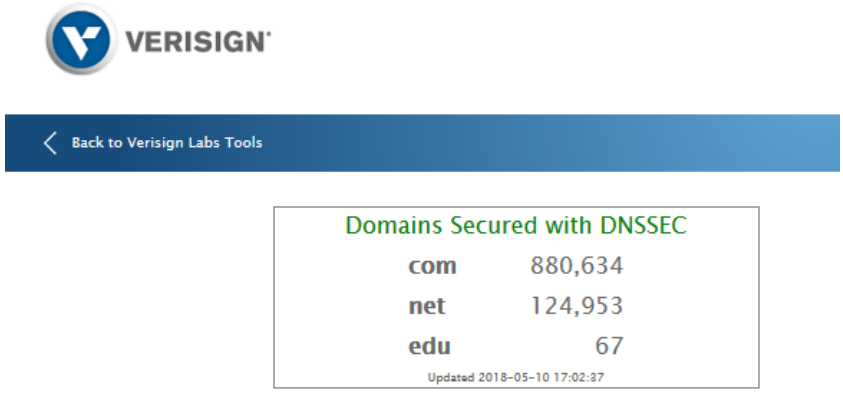



*Figura 28 - Indicadores de implantación de DNSSEC en ".com", ".net" y ".edu" (obtenidas de la herramienta "ScoreBoard" de Verisign)*

Por tanto, si tomamos el número de la "Figura 27 - Estadísticas de TLDs de nivel 2" que refleja unos 135 millones de dominios ".com", y tomamos el número de la "Figura 28" que refleja unos 880 mil dominios con DNSSEC, solo el 0,65% del total de dominios ".com" habría desplegado DNSSEC.

ScoreBoard ofrece adicionalmente capacidades para obtener la evolución a lo largo del tiempo de la adopción de DNSSSEC. La siguiente gráfica muestra un crecimiento exponencial en el número de dominios delegados dentro de los gTLDs más utilizados (".com" y ".net") que tienen ya registros DS en la zona padre, es decir, en los gTLDs correspondientes. En el eje de abscisas se presenta el año asociado a la obtención de la muestra (desde el año 2010 hasta la actualidad, año 2018), y en el eje de ordenadas el número de dominios con registros DS en términos absolutos.

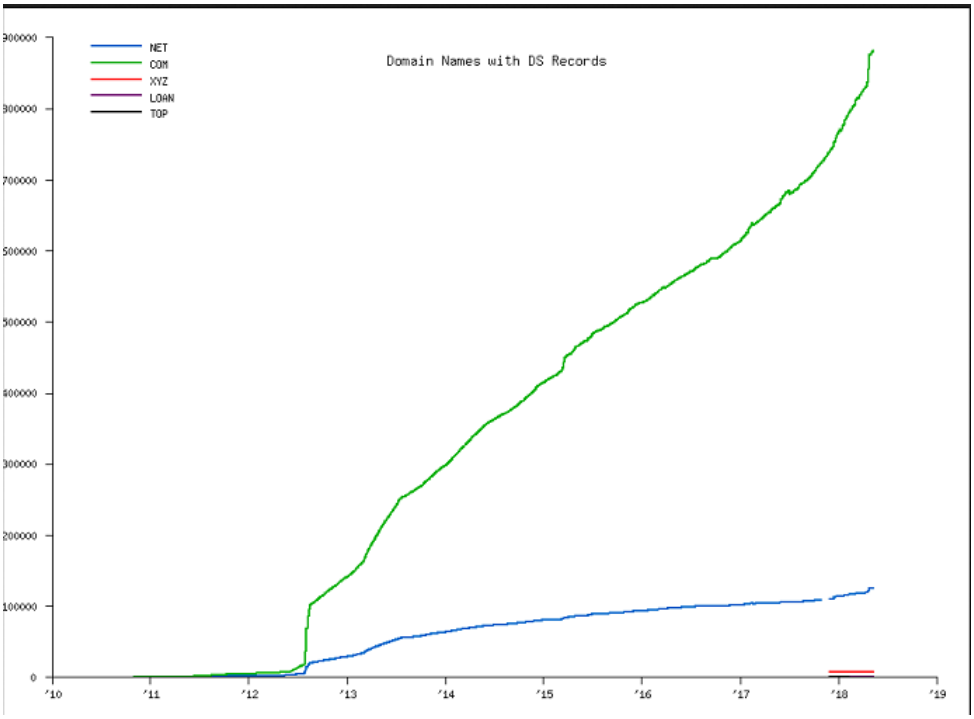



*Figura 29 - Evolución del número total de dominios ".com" y ".net" con registros DS publicados*

Esta gráfica con datos absolutos permite confirmar la evolución de los 880 mil dominios ".com" con DNSSEC existentes actualmente, y de los casi 125 mil dominios ".net". En el primer caso, ".com", el incremento más significativo comenzó a mediados de 2012. A partir de 2013, se observa un crecimiento lineal, que se mantiene en la actualidad (aunque el porcentaje global de dominios ".com" con DNSSEC sigue siendo muy reducido, menor al 1%). En el segundo caso, ".net", el incremento ha sido más paulatino, comenzando el mismo año 2012 y evolucionando de manera constante (pero mucho más reducido que para los dominios ".com") a lo largo de los años.

También es posible obtener una gráfica con la evolución, en términos relativos (o porcentuales), de los dominios que tienen su registro DS en la zona padre del dominio gTLD correspondiente, en comparación con el número total de dominios existentes en las zonas indicadas. Debe tenerse en cuenta que el código de colores entre la gráfica previa y la siguiente se ha invertido entre los dominios ".com" y ".net".

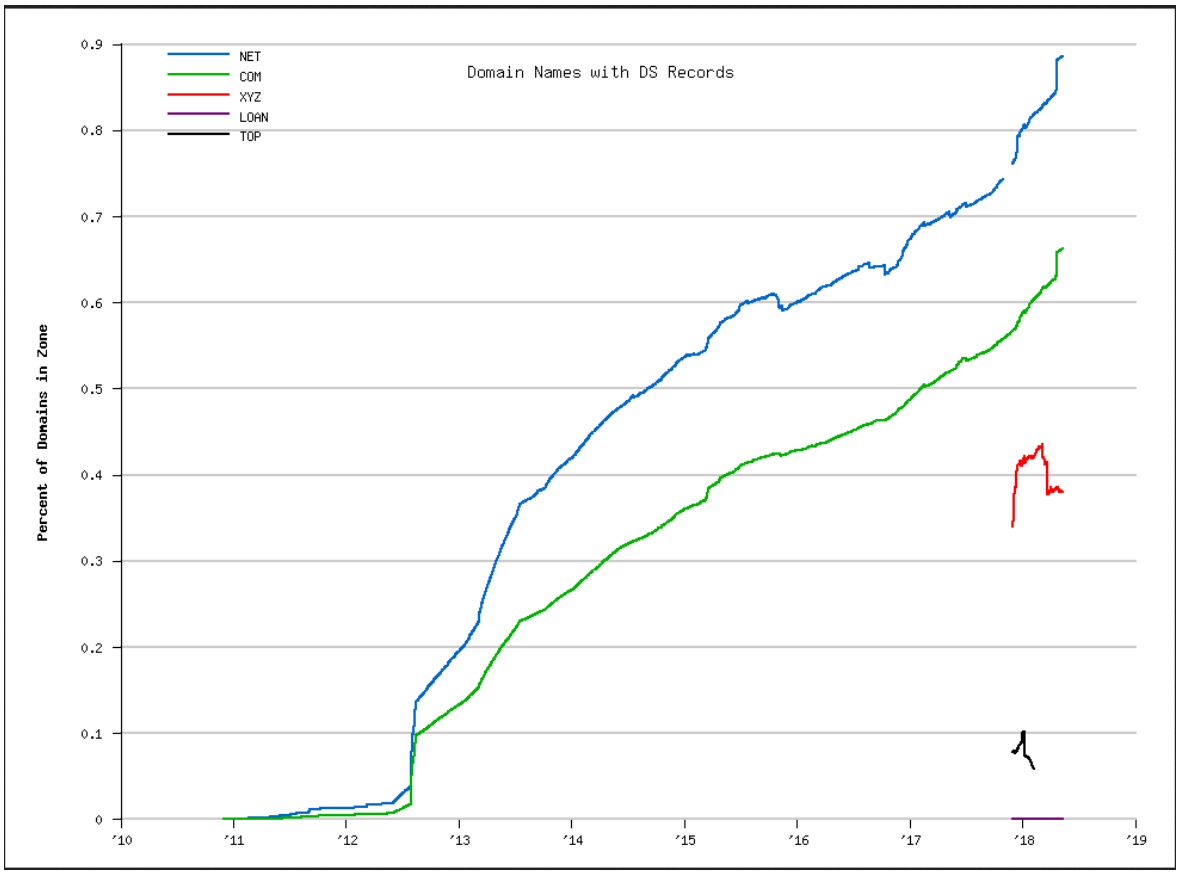



*Figura 30 - Evolución del porcentaje de dominios ".com" y ".net" con registros DS publicados*

En base a esta gráfica, se observa que el porcentaje de los dominios ".com" y ".net" con DNSSEC se ha incrementado más significativamente en el último año, frente a la progresión de años previos. Adicionalmente, se constata que el porcentaje de dominios con soporte para DNSSEC es superior, respecto al número total de dominios, en el dominio ".net" (casi del 0,9%) que en el dominio ".com" (0,65%), pese a que en valor absoluto es al contrario, debido al tamaño de la zona ".com" frente a la zona ".net".

No se observan discrepancias entre las estadísticas del NIST y las de Verisign en relación al porcentaje de dominios con soporte de DNSSEC en el dominio ".com", con un

porcentaje del 0,65%, constatándose que el nivel de despliegue, aun incrementándose cada año significativamente, sigue siendo bajo globalmente.

Al igual que para los TLDs de segundo nivel de los dominios ".gov" y ".edu" descritos en el apartado "3.1.3.1. DNSSEC en Estados Unidos", el NIST también analiza de forma general el dominio ".com":


*Figura 31 - Estimaciones del NIST de despliegue de DNSSEC en la industria (dominio ".com")*

Si bien estos datos han de tomarse con cierta cautela por proceder de muestras que no necesariamente proporcionan una visión completa, ya que el total de dominios probados es ligeramente superior a mil[21], sí puede concluirse de nuevo que el nivel de madurez de DNSSEC en la industria asociada al dominio ".com" (principalmente) es aún muy bajo (en este caso, aproximadamente, de un 3%). Todos los detalles relativos a los datos del NIST sobre el dominio ".com" y la industria se pueden obtener desde el enlace *https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-com.*

Asimismo, y también en base a muestras y no de manera completamente exhaustiva, existe interés en analizar de forma general el dominio ".com". La compañía Verisign ofrece una herramienta online denominada SecSpider [Ref.- 49] que permite obtener estadísticas en tiempo real sobre distintos parámetros del despliegue global del servicio DNSSEC, y su seguimiento. SecSpider recoge una enorme cantidad de datos de los registros RRsets que se reciben en diversas localizaciones y en diferentes momentos del día. En base a estos datos, se calculan tres parámetros (o métricas) cuyo valor oscila de 0 a 1:

- *Availability* (disponibilidad): mide si el sistema puede proporcionar todos los datos consultados para todas las sondas empleadas (puede ocurrir que algunas sondas puedan recoger un dato concreto y otras no). Como parte de los datos que se ofrecen a través de este parámetro se encuentran las claves públicas KSK y ZSK de la zona DNS.
- *Verifiability* (verificabilidad): determina si el sistema final puede verificar criptográficamente los datos que recibe, con objeto de saber cómo de segura es la cadena de delegación confianza (un valor de 1 implica que la todas las zonas son

[21] El análisis de la industria del NIST incluye principalmente dominios ".com", aunque también se añade algún dominio ".net" y ".org", extraídos de la lista "Fortune 1000" así como de la lista de Alexa de los 100 sitios web más relevantes en US: https://fedv6-deployment.antd.nist.gov/govmon.html.

accesibles desde una raíz y un valor de 0 que la zona está aislada). Este parámetro ofrece un grafo que relaciona la zona consultada con su zona padre y en el que se representan las cadenas de confianza entre ellas.

- *Validity* (validez): para cada registro DS que una zona padre tiene para las zonas hijas en las que delega, indica si existe la correspondiente clave DNSKEY en la zona hija, lo que permite determinar si la delegación se ha desplegado de forma correcta.

Los detalles sobre estos parámetros, incluidas las fórmulas que se emplean para calcularlos, pueden obtenerse de la aplicación SecSpider [Ref.- 50]. A continuación, se destacan los detalles más relevantes e ilustrativos sobre el uso de DNSSEC proporcionados por las diferentes pestañas de la aplicación SecSpider:

- "*Hierarchy*": ofrece una gráfica en la que se representan los 10 despliegues de DNSSEC de mayor tamaño, en base al volumen o número total de dominios con soporte para DNSSEC, ordenados por TLD.

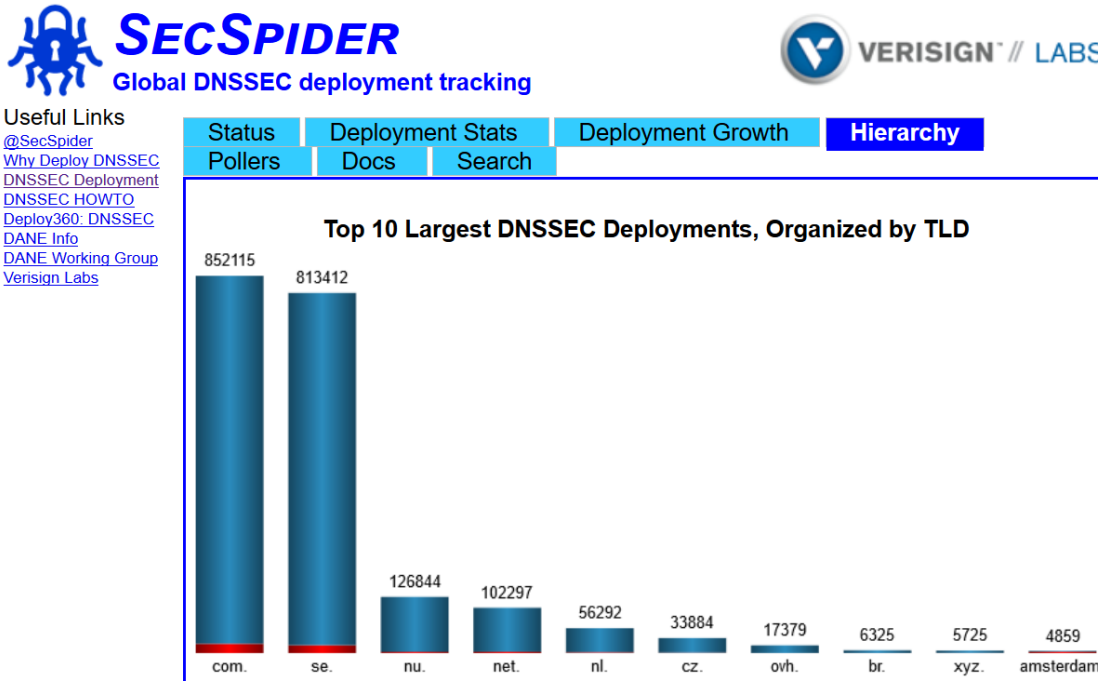



*Figura 32 - Despliegues de DNSSEC de mayor tamaño ordenados por TLD (SecSpider)*

- "*Deployment Stats*": estadísticas actualizadas que incluyen el número total de zonas que tienen DNSSEC habilitado, indicándose el tipo de algoritmos de firma empleados y la distribución de los tiempos de validez de las claves. Adicionalmente se recopilan estadísticas del uso de DANE (ver apartado "4.3. DANE: Más allá del DNS") y de la existencia de registros TLSA.

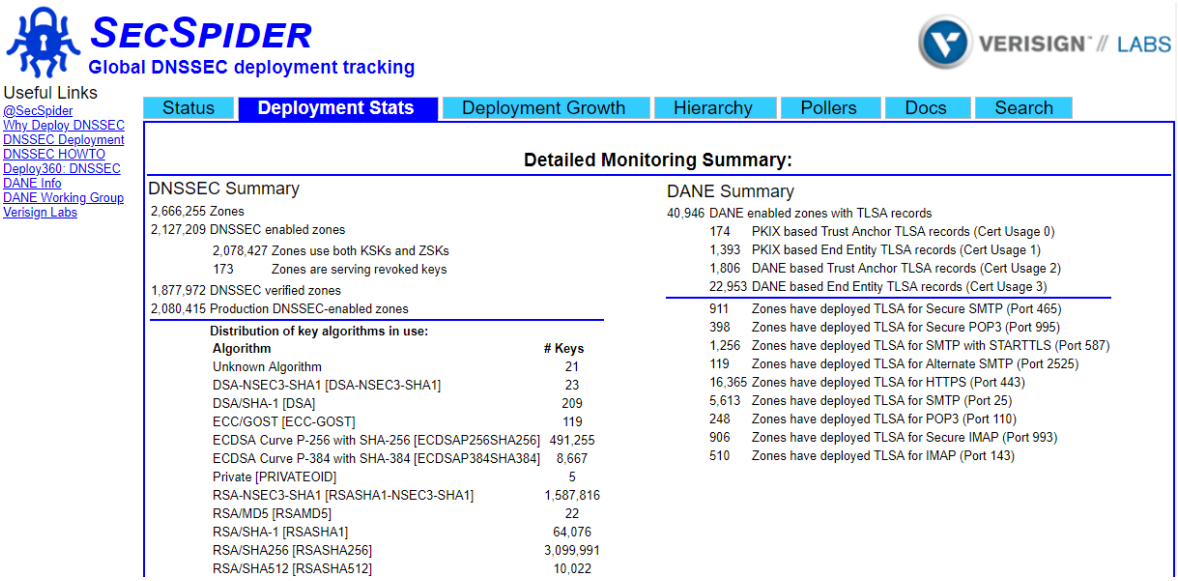



*Figura 33 - Estadísticas de despliegue de DNSSEC y DANE (SecSpider)*

- "*Deployment Growth*": ofrece una gráfica de distribución sobre la evolución y crecimiento en el uso de DNSSEC a lo largo del tiempo, donde destaca el interés en DNSSEC en el año 2013 (línea roja; corroborando las estadísticas analizadas previamente).

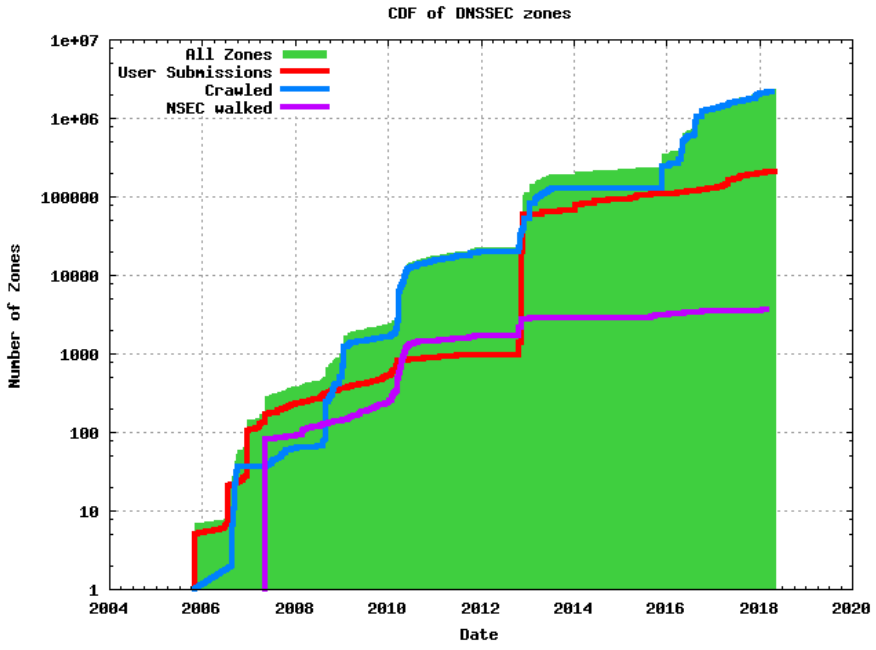



*Figura 34 - Crecimiento del despliegue de DNSSEC (SecSpider)*

- "*Status*": permite introducir la referencia a una zona concreta (por ejemplo, "com") y calcular para ella los tres parámetros descritos anteriormente (disponibilidad, verificabilidad y validez). La zona ".com", a fecha de elaboración de la presente guía, se proporcionan los siguientes datos de disponibilidad, incluyendo detalles geográficos en un mapa de los servidores DNS listados (identificados como

autoritativos para el dominio o zona consultada), junto a numerosas otras estadísticas detalladas de los registros de DNSSEC.

DNSKEYs

| Key Type | Key Length | Key |
|---|---|---|
| KSK | 2048 | AQPDzldNmMvZFX4NcNJ0uEnKDg7tmv/F3MyQR0lp BmVcNcsIszxNFxsBfKNW9JYCYqpik8366LE7VbIc NRzfp2h9OO8HRl+H+E08zauK8k7evWEmu/6od+2b oggPoiEfGNyvNPaSI7FOIroDsnw/taggzHRX1Z7S OiOiPWPNIwSUyWOZ79VmcQ1GLkC6NlYvG3HwYmyn Qv6oFwGv/KELSw7ZSdrbTQ0HXvZbqMUI7BaMskmv gm1G7oKZ1YiF7O9ioVNc0+7ASbqmZN7Z98EGU/Qh 2K/BgUe8Hs0XVcdPKrtyYnoQHd2ynKPcMMITEih2 /2HDHjRPJ2aywIpKNnv4oPo/ |
| ZSK | 1024 | AQOz+iBqxZtCKBBqKsO/i9JVchZ2Z1pFCWnj+pFH Ji3uPWiYWsAMvtMpInRPfV1Ot9m+8nHPxSkvOL2+ bttj4jEK6uUfTarET4wAMSh2k9rX2h+9kVQDjcuR wfFXV5bAmFd3j57hic7FEYVSxXtNUVU7BPaFRHuF r3OrQHQXaR4IeQ== |

DNSKEY PMTU status for **"com."** at Mon May 14 01:43:09 2018 GMT

| Name Server What is This? | DNSKEY Fit In PMTU? What is This? | RRSIG Expiration What is This? | Smallest Buffer What is This? | Optimal Buffer What is This? | Largest Buffer What is This? | Percent Pollers What is this? |
|---|---|---|---|---|---|---|
| h.gtld-servers.net. 192.54.112.30 | Yes | 8 | 743 | 831 | 4096 | 100.0% |
| k.gtld-servers.net. 192.52.178.30 | Yes | 8 | 743 | 831 | 4096 | 100.0% |
| d.gtld-servers.net. 192.31.80.30 | Yes | 8 | 743 | 831 | 4096 | 100.0% |
| b.gtld-servers.net. 192.33.14.30 | Yes | 8 | 743 | 831 | 4096 | 100.0% |
| g.gtld-servers.net. 192.42.93.30 | Yes | 8 | 743 | 831 | 4096 | 100.0% |
| c.gtld-servers.net. 192.26.92.30 | Yes | 8 | 743 | 831 | 4096 | 100.0% |
| i.gtld-servers.net. | Yes | 8 | 743 | 831 | 4096 | 100.0% |

*Figura 35 - Disponibilidad de la zona ".com" a nivel de DNSSEC (SecSpider)*

Otra página con información muy interesante de DNSSEC, que permite incluso monitorizar en tiempo real a nivel de zona TLD el estado del servicio DNSSEC, es "http://rick.eng.br" [Ref.- 32]. A través del enlace *http://rick.eng.br/dnssecstat/*, se presenta (ordenada por fecha de firmado del registro DS) la lista de los dominios gTLDs y ccTLDs que han desplegado su registro DS en la zona raíz. Esta clasificación permite conocer la incorporación de nuevos TLDs según se va produciendo. Hasta hace un tiempo, el propietario de este sitio web mantenía una relación con ICANN a través de la cual se ofrecían estadísticas para dominios de nivel 2 e inferiores, pero la relación ha cesado y actualmente solo presenta estadísticas para TLDs de primer nivel. Esta información permite corroborar, por ejemplo, la inclusión del registro DS para el dominio ".es" en la zona raíz en julio de 2014.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ngo. | | Public Interest Registry | 18-JUL-2014 | 0.24 | 8/3365 | 5:2 7:1 8:4 13:1 |
| lgbt. | | Afilias plc | 18-JUL-2014 | 1.60 | 35/2183 | 7:32 8:1 13:2 |
| lacaixa. | | CAIXA D'ESTALVIS I PENSIONS DE BARCELONA | 18-JUL-2014 | 100.00 | 1/1 | 10:1 |
| krd. | | KRG Department of Information Technology | 18-JUL-2014 | 0.22 | 1/457 | 8:1 |
| auction. | | United TLD HoldCo, Ltd. | 18-JUL-2014 | 1.45 | 51/3519 | 7:45 8:1 13:5 |
| hr. | | CARNet - Croatian Academic and Research Network | 16-JUL-2014 | - | 335/- | |
| es | | Red.es | 16-JUL-2014 | | 16047/- | |
| gent. | | Combell nv | 12-JUL-2014 | 1.28 | 44/3444 | 7:26 8:18 |
| scb. | | The Siam Commercial Bank Public Company Limited ("SCB") | 11-JUL-2014 | 24.00 | 6/25 | 8:6 |
| nrw. | | Minds + Machines GmbH | 11-JUL-2014 | 13.40 | 2588/19312 | |
| bio. | | STARTING DOT LIMITED | 11-JUL-2014 | 3.45 | 585/16958 | |
| melbourne. | | The Crown in right of the State of Victoria, represented by its Department of State Development, Business and Innovation | 10-JUL-2014 | 0.17 | 18/10366 | 8:12 13:6 |

*Figura 36 - Fechas de despliegue del registro DS de los TLDs en la zona raíz de DNSSEC*

La selección de un dominio concreto en dicha tabla enlaza con la página oficial de IANA *https://www.iana.org/domains/root/db/<NOMBRE_DE_DOMINIO>.html*, que muestra los detalles oficiales del registro asociado al dominio.

En el enlace *http://rick.eng.br/mon*, se ofrece una lista de nombres de dominio (TLD), ordenada por nivel de cumplimiento inverso, que permite ver en una escala de colores el porcentaje de registros RRSIG que el dominio tiene dentro de su periodo de validez (o con firma inválida u otros problemas). La selección de un dominio concreto abre otra ventana en la que se ofrecen todos los detalles sobre él.

### 3.1.3.3. DNSSEC en Europa

En el presente apartado se ofrecen diversas estadísticas que ilustran la heterogeneidad en el despliegue de DNSSEC a nivel europeo, marcada especialmente por la no existencia de políticas relativas al mismo, ni a nivel general, ni a nivel de la eurozona.

Para el dominio ".eu", en base a las estadísticas publicadas por EURid de 2017 [Ref.- 31], se observa que en la zona ".eu" hay un incremento del 27,32% en los dominios firmados con DNSSEC, pese a que el incremento en el número total de dominios ".eu" solo representa el 1,38%. Esto quiere decir que un número significativo de los dominios ya existentes en la zona ".eu" están migrando a DNSSEC:

| Dominios .eu | 2016 | 2017 | Incremento anual |
|---|---|---|---|
| Número total | 3.762.970 | 3.815.055 | 52.085 → 1,38 % |
| Dominios con DNSSEC | 348.401 | 443.600 | 95.199 → 27,32 % |

*Tabla 2 - Evolución y estadísticas de los dominios ".eu" con DNSSEC*

En el mismo informe de estadísticas se ofrece una gráfica que representa la evolución de dominios firmados con DNSSEC en la zona ".eu", aunque se observa una errata en la función que representa el crecimiento en valor absoluto, por lo que a continuación se presenta una gráfica calculada a partir de los valores absolutos que figuran en ella:

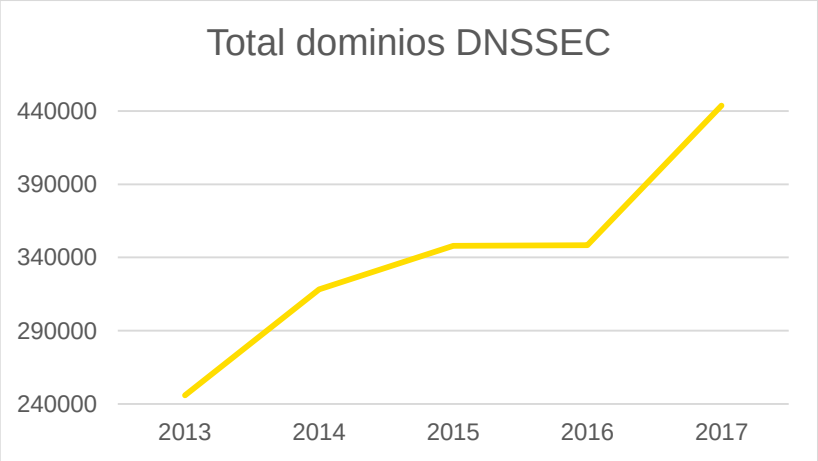



*Figura 37 - Incremento en los dominios firmados con DNSSEC en la zona ".eu" (2013-2017)*

Según ilustra la "Figura 32", el país europeo con mayor despliegue de DNSSEC en los TLDs de nivel 2 dentro de su ccTLD es Suecia, con más de ochocientos mil dominios ".se", es decir, en torno al 44% [Ref.- 35]:


*Figura 38 - Evolución reciente de los dominios totales bajo el dominio ".se" (Suecia)*

Otro país europeo con gran concienciación en el uso de DNSSEC es Holanda, con aproximadamente un 52% de TLDs de nivel 2 bajo el ccTLD ".nl" [Ref.- 36]:

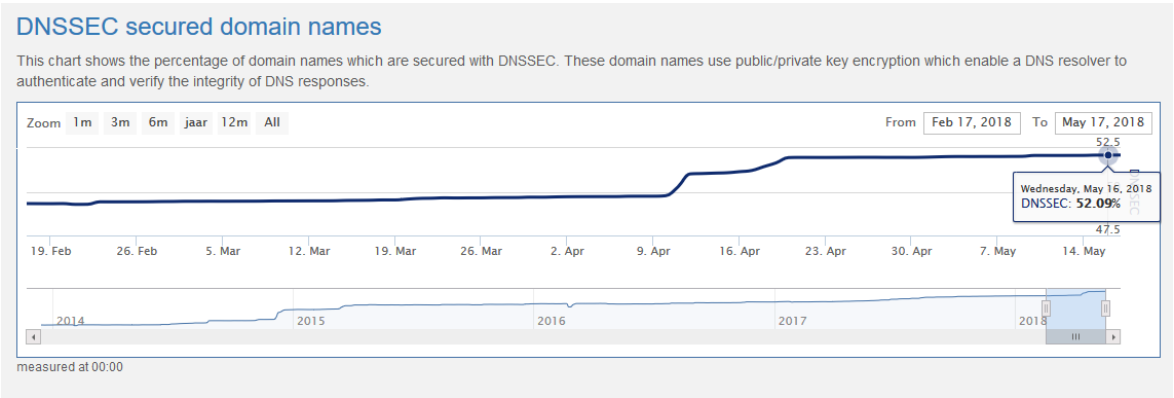



*Figura 39 - Porcentaje de TLDs de nivel 2 de Holanda (cominio ".nl") con DNSSEC*

Según un estudio realizado por el organismo responsable del ccTLD ".nl" (SIDN), ya en 2016 existían en Holanda 5,6 millones de dominios, y, de ellos, 2,5 millones habían desplegado DNSSEC [Ref.- 37]. El porcentaje de dominios bajo el dominio ".nl" con soporte para DNSSEC se ha incrementado incluso en la actualidad.

Además de haber completado sus despliegues a nivel de ccTLD desde un principio, en estos países han existido iniciativas para incentivar el despliegue de DNSSEC en los TLDs de nivel 2, entre ellas, incentivos económicos para los dominios registrados con DNSSEC, tanto a nivel de agente registrador como de propietario del dominio.

En el extremo contrario, se encuentra Portugal (".pt"), que, pese a haber desplegado su ccTLD en la zona raíz en 2010, presenta un porcentaje de dominios con DNSSEC muy

bajo: de un total de 3.240.000 dominios activos en mayo de 2018, solo 15.400 tienen activo DNSSEC (un 4,77%). Los datos, obtenidos del agente registrador del dominio ".pt" [Ref.- 67], muestran que el número de dominios con DNSSEC presenta un crecimiento negativo en los últimos meses:


| Mês | .pt | .com.pt | Outros | Total |
|---|---|---|---|---|
| Janeiro | 10.693 | 259 | 9 | 10.961 |
| Fevereiro | 8.920 | 231 | 6 | 9.157 |
| Março | 10.125 | 260 | 18 | 10.403 |
| Abril | 9.010 | 200 | 5 | 9.215 |
| Maio | 9.482 | 226 | 21 | 9.729 |
| Junho | 5.691 | 164 | 13 | 5.868 |

***Figura 40 - Dominios registrados en Portugal (zona ".pt")***

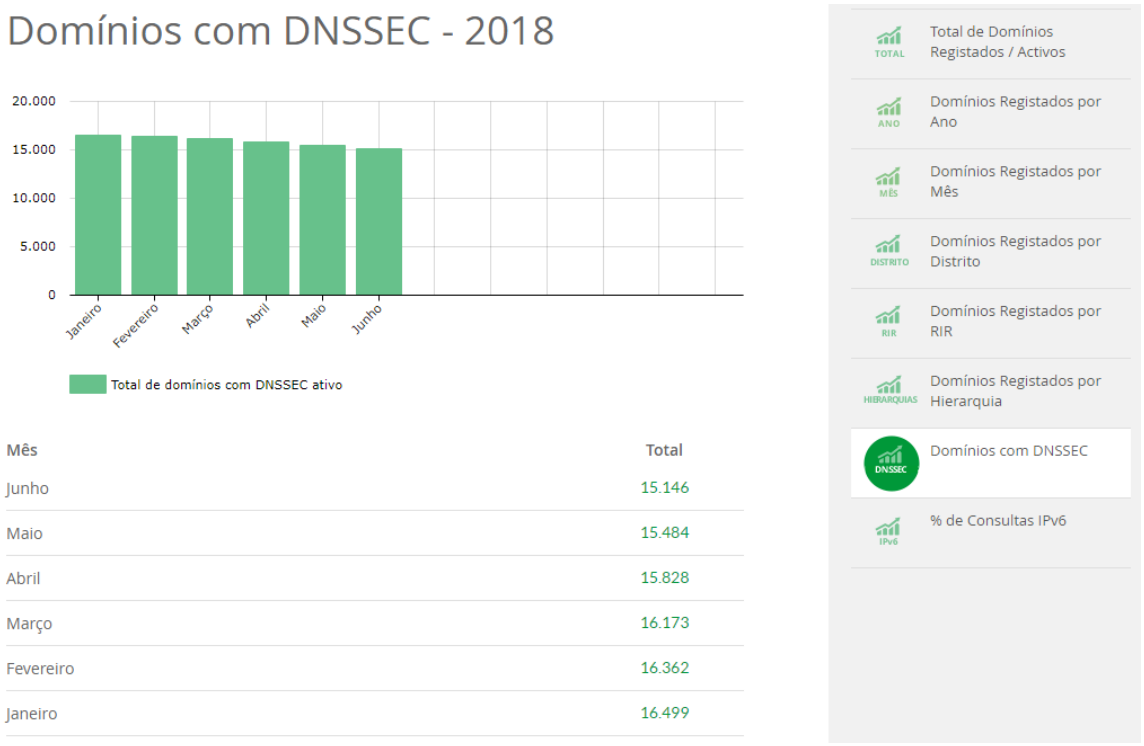



*Figura 41 - Dominios registrados en Portugal (dominio ".pt") con DNSSEC*

### 3.1.4. Validación de las transacciones DNSSEC en los *resolvers*

Hasta ahora, el análisis del estudio sobre la implantación de DNSSEC del presente apartado se ha centrado en el despliegue efectuado en los TLDs de distintos niveles. Sin embargo, una métrica clave de cara a conocer el uso real del protocolo DNSSEC es el porcentaje de validación de las transacciones de resolución de nombres, entendiendo como tal el número de consultas al servicio DNS que se realizan y completan íntegramente con DNSSEC. Sin embargo, la obtención de estas estadísticas es compleja, dado que no es posible establecer mecanismos exhaustivos que midan y clasifiquen en tiempo real los datos necesarios para conocer el porcentaje de validación a nivel mundial (o por geografías).

APNIC Labs ofrece una herramienta que proporciona estadísticas sobre el sobre el porcentaje de validación de las transacciones DNSSEC a nivel mundial, permitiendo modificar la ventana de tiempo (en días) utilizada para los cálculos 92 [Ref.- 51]. Adicionalmente a la gráfica del mapa del mundo proporcionada, en la que, al situar el cursor sobre un país concreto, se presenta el porcentaje de validación de DNSSEC para dicho país, se proporcionan una serie de tablas por región (continente), subregión (división geográfica de los continentes) y país, con el porcentaje de validaciones y el número de muestras recogidas. Todas las tablas están ordenadas de mayor a menor porcentaje de validación.

En el mapa, en color verde se muestran los países con un porcentaje de validación superior al 70%, y en color rojo los inferiores al 10%. Como se aprecia, España, que ronda cifras en torno al 8%, se encuentra aún lejos de otros países de su entorno,

destacando dentro de Europa Portugal, Suecia y Noruega, estos dos últimos con porcentajes cercanos al 80%.

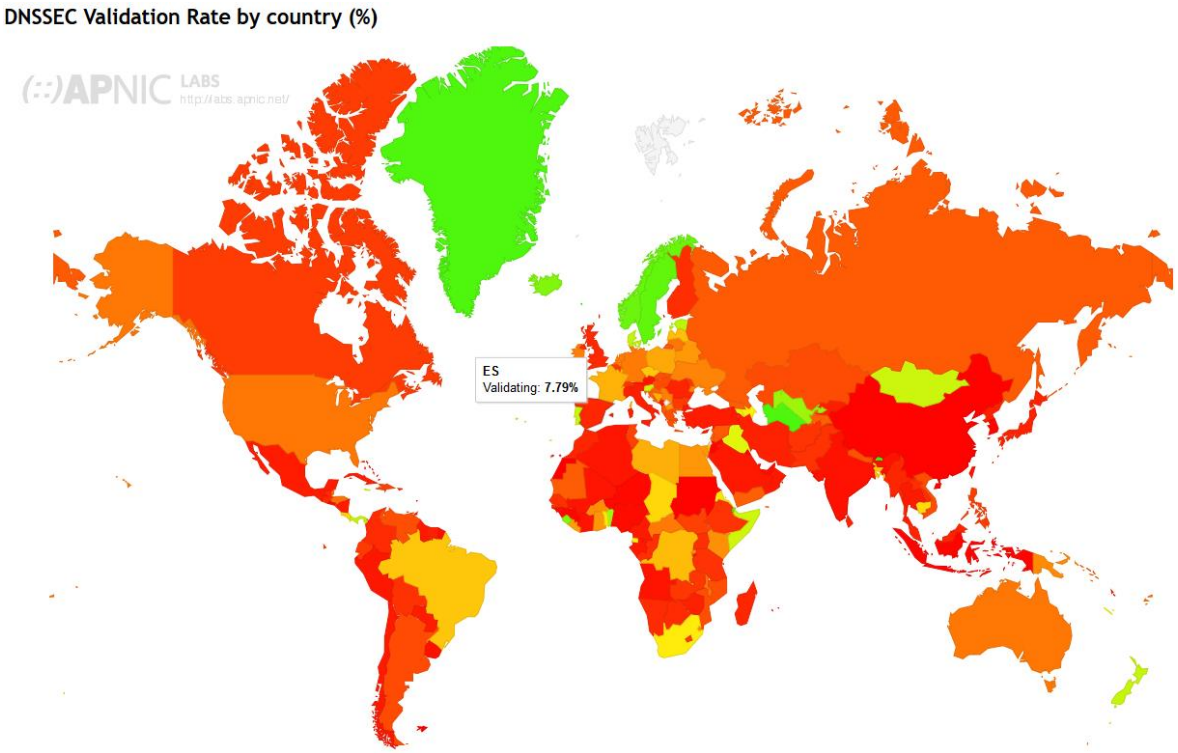



*Figura 42 - Mapa del porcentaje de validación de DNSSEC a nivel mundial*

Los cálculos para medir la validación de DNSSEC realizados a través de esta herramienta (que lleva 4 años recopilando datos) se basan en scripts embebidos en anuncios *online* que se incluyen en una campaña de publicidad que se distribuye a un número significativo de clientes finales a nivel mundial. A través de estos *scripts*, se fuerza la resolución DNS hacia los sistemas que analizan los datos (utilizados exclusivamente para este propósito), quienes, mediante el análisis de las consultas DNS que reciben, pueden determinar si el cliente final está haciendo uso de DNSSEC, es decir, enviando sus consultas a través de *resolvers* que llevan a cabo la validación de DNSSEC. Para ello, como la mayoría de clientes finales tienen configurados dos o más servidores DNS recursivos para asegurar la disponibilidad del servicio DNS, hay que tener en cuenta las siguientes consideraciones de cara a definir un procedimiento de actuación ante una consulta DNS:

- En un cliente final, si no se obtiene respuesta del *resolver* en el tiempo especificado o si se recibe como respuesta un código SERVFAIL o REFUSED, el cliente puede volver a formular la pregunta DNS a otro de sus servidores recursivos.
- Si para la obtención de medidas de validación de DNSSEC se emplea el concepto de que las respuestas firmadas que se validan se devuelven al cliente y las firmadas para las que falla la verificación se retienen, hay que ser más cuidadoso en la medición. Podría ocurrir que el cliente, consultando a otro de los servidores

recursivos que tuviese configurado, recibiese la respuesta por DNS (y no DNSSEC) y la medida podría ser incorrecta.

Por tanto, para evitar este problema, el sistema de medida realiza dos consultas DNS: una devolverá una respuesta firmada de forma válida por el servicio DNSSEC y la otra se firmará, pero con una firma incorrecta. Con este par de consultas, los clientes finales se podrán agrupar en tres categorías:

- Si ninguno de los servidores recursivos DNS utilizados por el cliente final realiza validación por DNSSEC, el cliente será capaz de resolver ambas consultas (y además no solicitará los registros de DNSSEC), porque no habrá validado la información de firma de ninguna de ellas.
- Si alguno de los servidores recursivos DNS utilizados por el cliente final realiza validación DNSSEC pero otros no, entonces el cliente, aunque solicite los registros de DNSSEC relativos a la firma, será capaz igualmente de resolver ambas consultas.
- Si todos los servidores recursivos DNS configurados en el cliente final realizan validación por DNSSEC, el cliente solicitará los registros de DNSSEC pero solo podrá resolver la consulta que se recibió con la firma correcta.

Para el cómputo de los porcentajes mostrados en el mapa de la herramienta de APNIC Labs, se considera que disponen de soporte para DNSSEC solo los clientes asociados a la categoría 3, es decir, aquellos que no pudieron resolver la consulta correctamente firmada (lo que implicaría que todos los servidores recursivos DNS configurados están empleando DNSSEC).

La herramienta de APNIC Labs permite modificar la ventana temporal entre dos días y 120 días para el cálculo de los datos, y presenta una tabla por regiones, subregiones y países ordenados por orden decreciente en el porcentaje de validación de transacciones DNSSEC, tal como ilustra la siguiente imagen:

**Plot Type:** DNSSEC Validating

**Date:** Auto **Window (Days)** 2

**Color Range (max value)** Auto

Redraw

| Code | Region | DNSSEC Validates | Uses Google PDNS | Samples | Weight | Weighted Samples |
|---|---|---|---|---|---|---|
| XA | World | 11.87% | 10.37% | 587,297,002 | 1 | 587,297,002 |
| XF | Oceania | 30.06% | 6.46% | 4,278,814 | 1.09 | 4,681,097 |
| XC | Americas | 21.29% | 11.92% | 170,313,993 | 0.67 | 114,918,753 |
| XE | Europe | 21.10% | 9.84% | 72,873,461 | 1.32 | 96,398,929 |
| XB | Africa | 13.16% | 23.29% | 33,210,450 | 1.53 | 50,854,928 |
| XD | Asia | 5.23% | 7.98% | 306,611,567 | 1.05 | 320,443,339 |
| XG | Unclassified | 0.00% | 100.00% | 2,035,042 | 0 | 0 |

| Code | SubRegion | DNSSEC Validates | Uses Google PDNS | Samples | Weight | Weighted Samples |
|---|---|---|---|---|---|---|
| QR | Micronesia, Oceania | 57.56% | 47.62% | 165,817 | 0.18 | 30,462 |
| XK | Southern Africa, Africa | 42.96% | 18.81% | 652,011 | 8.23 | 5,369,286 |
| XR | Central Asia, Asia | 32.78% | 19.31% | 1,412,853 | 3.78 | 5,341,008 |
| QP | Australia and New Zealand, Oceania | 30.53% | 4.30% | 3,874,214 | 1.11 | 4,303,037 |
| XP | South America, Americas | 24.42% | 16.65% | 24,796,514 | 1.8 | 44,725,368 |
| QQ | Melanesia, Oceania | 23.89% | 31.77% | 169,051 | 1.76 | 298,195 |
| QO | Western Europe, Europe | 23.76% | 7.45% | 13,839,889 | 2.09 | 28,907,463 |
| QM | Northern Europe, Europe | 23.63% | 5.16% | 18,665,752 | 0.87 | 16,313,642 |
| XQ | Northern America, Americas | 22.17% | 7.00% | 132,523,915 | 0.41 | 54,705,188 |
| XW | Eastern Europe, Europe | 20.68% | 12.81% | 18,209,676 | 1.81 | 33,041,035 |
| XH | Eastern Africa, Africa | 18.11% | 22.90% | 3,349,099 | 2.69 | 9,007,256 |

*Figura 43 - Porcentaje de validación de transacciones DNSSEC por regiones*

Los datos obtenidos por esta herramienta muestran que, por regiones, Oceanía valida en torno al 30% de transacciones, mientras que Europa y Norte América en torno al 22%, quedando Asia al final de la tabla, con países como China y Korea, que apenas utilizan DNSSEC.

| CC | Country | DNSSEC Validates | Uses Google PDNS | Samples | Weight | Weighted Samples |
|---|---|---|---|---|---|---|
| MF | Saint Martin (French part), Caribbean, Americas | 93.52% | 21.96% | 3,624 | 0 | 0 |
| FO | Faeroe Islands, Northern Europe, Europe | 91.67% | 6.55% | 9,824 | 0.87 | 8,518 |
| PM | Saint Pierre and Miquelon, Northern America, Americas | 90.46% | 96.31% | 2,003 | 0 | 0 |
| GL | Greenland, Northern America, Americas | 89.68% | 29.09% | 11,327 | 0.59 | 6,662 |
| KI | Kiribati, Micronesia, Oceania | 89.63% | 13.53% | 3,068 | 0.87 | 2,669 |
| IS | Iceland, Northern Europe, Europe | 87.06% | 7.69% | 31,038 | 1.9 | 59,030 |
| SE | Sweden, Northern Europe, Europe | 81.54% | 5.51% | 1,254,202 | 1.3 | 1,624,207 |
| NO | Norway, Northern Europe, Europe | 79.90% | 9.12% | 495,269 | 1.85 | 916,843 |
| DJ | Djibouti, Eastern Africa, Africa | 79.36% | 83.40% | 22,401 | 0.89 | 19,862 |
| BT | Bhutan, Southern Asia, Asia | 77.87% | 28.74% | 95,617 | 0.55 | 52,688 |
| SL | Sierra Leone, Western Africa, Africa | 74.77% | 88.57% | 30,562 | 1.06 | 32,378 |
| FM | Micronesia (Federated States of), Micronesia, Oceania | 74.29% | 53.79% | 8,674 | 0.67 | 5,791 |
| AI | Anguilla, Caribbean, Americas | 73.75% | 74.49% | 8,213 | 0 | 0 |
| DM | Dominica, Caribbean, Americas | 72.82% | 55.59% | 10,919 | 0.79 | 8,583 |
| BB | Barbados, Caribbean, Americas | 71.84% | 37.75% | 161,283 | 0.25 | 40,189 |
| BJ | Benin, Western Africa, Africa | 68.04% | 56.09% | 144,081 | 0.78 | 112,405 |
| KY | Cayman Islands, Caribbean, Americas | 64.40% | 29.45% | 16,790 | 0.48 | 8,073 |
| NR | Nauru, Micronesia, Oceania | 64.23% | 68.16% | 534 | 0 | 0 |
| EE | Estonia, Northern Europe, Europe | 63.60% | 7.84% | 161,578 | 1.29 | 208,734 |
| PT | Portugal, Southern Europe, Europe | 61.31% | 12.40% | 939,441 | 1.29 | 1,210,386 |
| NZ | New Zealand, Australia and New Zealand, Oceania | 60.58% | 5.65% | 717,197 | 1.03 | 742,057 |
| JM | Jamaica, Caribbean, Americas | 60.18% | 33.75% | 1,130,140 | 0.19 | 219,852 |

*Figura 44 - Porcentaje de validación de transacciones DNSSEC por países*

Como se puede observar, los países del norte de Europa (Islandia, Suecia y Noruega) validan un elevado porcentaje de las transacciones del servicio de resolución de nombres mediante DNSSEC. Por su parte, en el continente americano son las islas del Caribe quienes destacan en esta tasa.

En la página «http://rick.eng.br" [Ref.- 32], analizada previamente en el apartado "3.1.3.2. DNSSEC en los dominios ".com", ".net" y ".edu"», concretamente en el enlace *http://rick.eng.br/dnssecstat/*, se ofrece una estadística que incluye el porcentaje de dominios de primer y de segundo nivel que se encuentran firmados, y también un porcentaje global de validación de transacciones DNSSEC, basado en los cálculos de la herramienta de APNIC Labs:

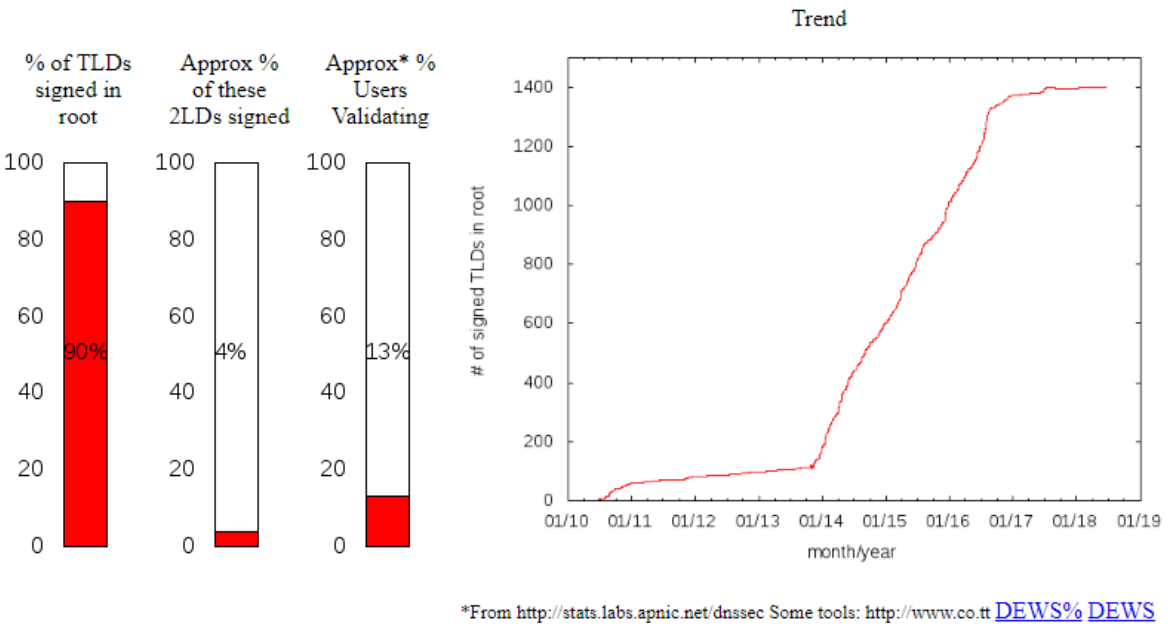


*Figura 45 - Porcentaje de dominios de primer y segundo nivel firmados con DNSSEC*

Como muestra esta estadística, en la que se indica que el 90% de los TLDS de primer nivel están firmados en la zona raíz, y que únicamente un 4% de los TLDs de segundo nivel están firmados dentro de los TLDs de primer nivel, se refleja también que aproximadamente el 13% de las transacciones DNSSEC a nivel mundial se están validando.

El SIDN holandés [Ref.- 36] ofrece estadísticas para los dominios de Holanda (bajo el ccTLD ".nl") sobre porcentajes de consultas recibidas por *resolvers* DNS con capacidades DNSSEC (32,7%) frente a las recibidas por *resolvers* DNS tradicionales (67,3%). El estudio considera que un *resolver* DNS valida DNSSEC cuando envía más de cien consultas al día solicitando registros DS o DNSKEY con el bit "DO" activo (ver apartado "2.4.1. Nuevos registros asociados a DNSSEC"). Se toman los datos de los servidores autoritativos para evitar cálculos erróneos en escenarios donde el cliente final soporta DNSSEC pero el *resolver* DNS intermedio no.

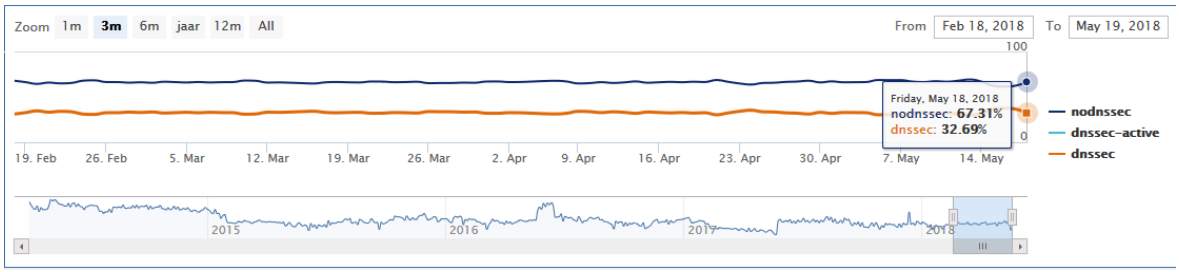



*Figura 46 - Porcentaje de consultas validadas por DNSSEC en Holanda (SIDN)*

Complementando los datos previos, SIDN dispone de estadísticas sobre el número total de *resolvers* DNS únicos que validan DNSSEC y para los que reciben peticiones en Holanda, actualmente en torno a 19.000:

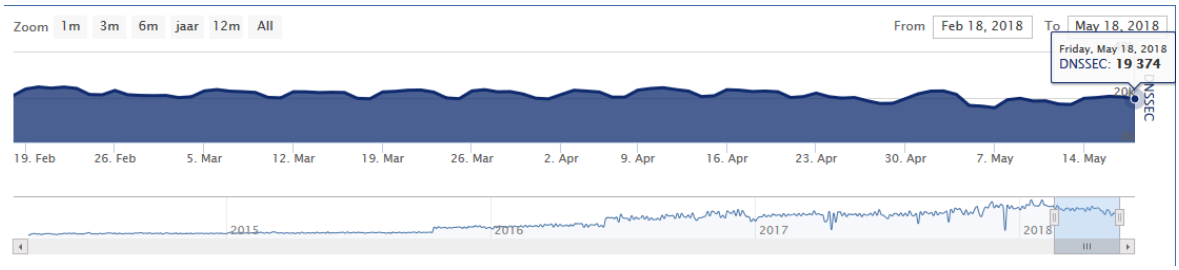



*Figura 47 – Resolvers DNS procesando consultas DNSSEC en Holanda*

Adicionalmente, SIDN ha realizado estudios complementarios tomando medidas para los *resolvers* DNS objetivo a través de la red RIPE Atlas [Ref.- 37]. Utilizando un total de 500 sondas de RIPE Atlas localizadas en Holanda, se evaluó si las consultas DNS las lleva a cabo un *resolver* que realiza validación DNSSEC (utilizando los *resolvers* de las propias sondas). El resultado del estudio confirmó que tan solo un 6% de consultas DNS eran validadas, frente al 32,7% de su análisis principal, o al 12% de APNIC Labs.

Como se aprecia en las figuras anteriores, en Holanda se valida en torno a un 32% de las transacciones DNSSEC. El número obtenido por la herramienta de APNIC Labs es inferior (25%), lo cual puede deberse a la especificidad del estudio de SIDN, centrado en

Holanda, frente al de APNIC, que distribuye su campaña de recogida de medidas por todo el mundo:

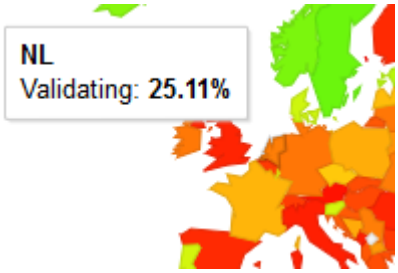



*Figura 48 - Porcentaje de consultas validadas por DNSSEC en Holanda (APNIC Labs)*

Complementariamente, la web de SIDN ofrece un mapa geográfico con las localizaciones de los *resolvers* que, en función de las métricas recogidas por ellos, validan DNSSEC:

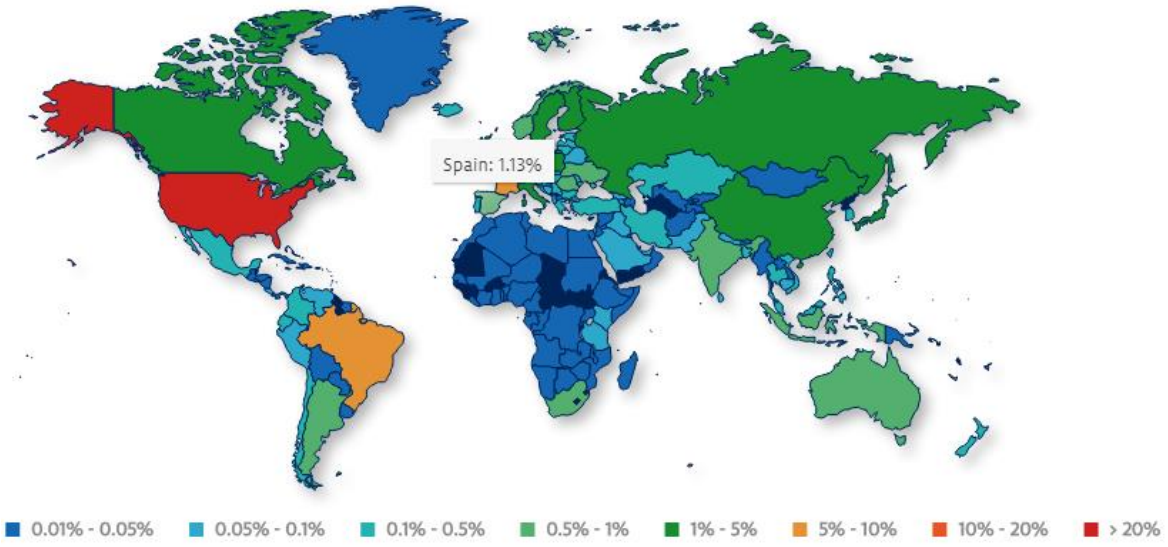



*Figura 49 - Distribución geográfica de resolvers que validan DNSSEC en Holanda (SIDN)*

De ellos, el 21% están localizados en Estados Unidos, seguido de Holanda con el 12,7% y Francia con el 8% del total. Como se puede ver, solo el 1,13% de los *resolvers* DNSSEC que hace consultas en Holanda se ubican en España.

También es posible obtener datos de validación de los diez sistemas autónomos más grandes (en términos de consultas recibidas en dominios holandeses) y su participación en las consultas con *flags* de validación. El tamaño del *resolver* se define por el número total de consultas recibidas desde *resolvers* internos al sistema autónomo:

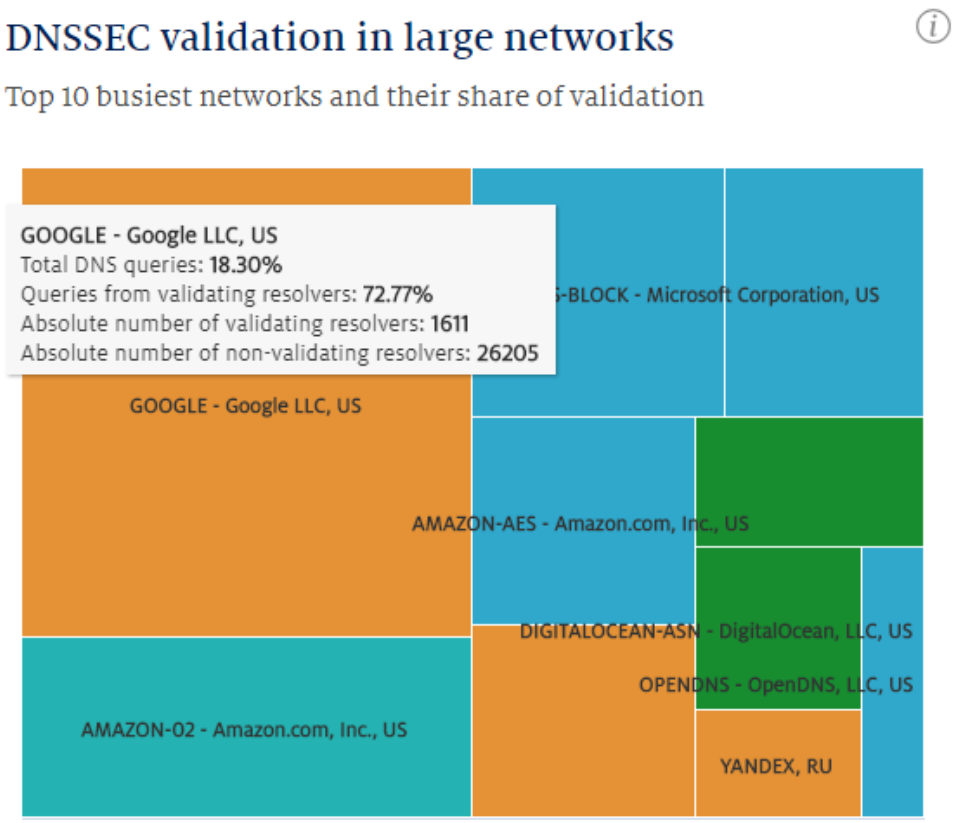



*Figura 50 - Consultas DNSSEC enviadas por open resolvers en Holanda*

## 3.2. DNSSEC en España

En este apartado se ofrecen los datos de implantación de DNSSEC en España, que permitirán establecer el escenario sobre el que cualquier organización a cargo de una zona dependiente del ccTLD ".es" deberá integrar su implementación de DNSSEC.

### 3.2.1. Contexto de DNSSEC en la zona ".es"

El organismo responsable del ccTLD ".es" es **Red.es**, o red.es (Entidad Pública Empresarial dependiente del Ministerio de Economía y Empresa), quien desde febrero del año 2000 gestiona, añade, modifica y borra los datos asociados con el nombre de dominio y, consecuentemente, el registro de nombres de dominio identificados y delegados en las zonas bajo la zona ".es". Red.es gestiona y actualiza la infraestructura técnica que asegura el rendimiento, la disponibilidad y la adaptación ante eventualidades de la zona ".es".

Respecto a DNSSSEC, Red.es es responsable de la generación de claves criptográficas, custodia la clave privada, y firma de forma segura los registros DNSSEC en la zona ".es".

Asimismo, Red.es es responsable de la generación, la exportación segura y el mantenimiento de los registros DS para su publicación en la zona raíz, con el objetivo de

completar la cadena de confianza (*trust of chain*) de DNSSEC, y complementariamente, publica una "Declaración de Políticas y Procedimientos" (DPS)[22].

En España, el alta de un nombre de dominio (independientemente de su relación con DNSSEC) se rige por la normativa ORDEN ITC/1542/2005, de 19 de mayo. Según esta normativa, cualquier persona física o jurídica o entidad sin personalidad que tenga intereses o mantenga vínculos con España puede solicitar la asignación de un nombre de dominio en la zona ".es".

La asignación de un nombre de dominio de segundo nivel (aquel que cuelga directamente del dominio ".es") se realiza sin comprobación previa y por orden de recepción de la solicitud, salvo en el caso de términos prohibidos o reservados.

La asignación de un nombre de dominio de tercer nivel del grupo ".com.es", ".nom.es" y ".org.es" también se realizará según el criterio descrito previamente para los TLDs de segundo nivel. Los TLDs de tercer nivel ".gob.es" y ".edu.es" han de pasar por la verificación del cumplimiento de una serie de requisitos, disponibles en el "Manual de Usuario Final" publicado en "dominios.es" [Ref.- 14].

### 3.2.2. TLDs de segundo nivel

Las estadísticas publicadas en este apartado han sido proporcionadas por "**dominios.es**" [Ref.- 13], integrado en "Red.es". Parte de estos datos son a su vez suministrados por los agentes registradores, que son quienes informan a "dominios.es" de la configuración de DNSSEC para los dominios a su cargo. "dominios.es" ofrece también servicios de registro a usuarios y organizaciones particulares, es decir, actúa a su vez como agente registrador.

A fecha de elaboración de la presente guía, "dominios.es" trabaja con 103 agentes registradores, de los cuales 36 ofrecen servicios de DNSSEC.

Es responsabilidad de los agentes registradores facilitar a "dominios.es" los registros DS de las zonas que, siendo gestionadas por ellos, habilitan DNSSEC, y también es su responsabilidad verificar la validez de dichos registros, ya que "dominios.es" no realiza ninguna validación sobre ellos salvo comprobaciones básicas (como el formato asociado al tipo de algoritmo de firma utilizado para generar el registro DS). Es también responsabilidad del agente registrador asegurarse de que el propietario de las claves privadas (asociadas a las claves KSK y ZSK de cada zona) es el titular del dominio. Para los titulares de los dominios registrados directamente a través de "dominios.es" que desean incluir sus registros DS en la zona ".es", existe la herramienta de gestión de dominios SGND (Sistema de Gestión, y Registro, de Nombres de Dominio, bajo ".es")[23].

Los registros DS de un TLD de segundo nivel se pueden incluir en los servidores de la zona ".es" en cualquier momento a partir de que se produzca el alta o registro del dominio. La publicación de un nuevo dominio se realiza en la siguiente distribución del fichero de zona desde el momento del alta. A fecha de elaboración de la presente guía, el fichero de zona se distribuye cada 4 horas.

[22] *http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/valoresanadidos/dnssec*

[23] https://www.nic.es/sgnd/login.action

Según los datos proporcionados por "dominios.es" a fecha 20 de abril de 2018, la evolución de la implantación de DNSSEC en España crece de forma significativa: en enero de 2018, el número de dominios delegados en la zona ".es" y que tenían configurado DNSSEC era de unos 10.700. En abril de 2018 (solo 4 meses después), este número alcanza los 14.500 dominios, es decir, un crecimiento cercano al 35%. La siguiente tabla muestra la evolución en la implantación de DNSSEC en España (dominio ".es") desde el año 2014:

| Fecha | Total dominios .es | Total dominios .es con DNSSEC |
|---|---|---|
| 16/04/2018 | 1.907.906 | 14.496 |
| 31/12/2017 | 1.890.026 | 10.659 |
| 31/12/2016 | 1.838.066 | 5.729 |
| 31/12/2015 | 1.795.413 | 2.837 |
| 31/12/2014 | 1.755.224 | 21 |

*Tabla 3 - Evolución y estadísticas de los dominios ".es" con DNSSEC*

Como se puede apreciar en las siguientes gráficas, la evolución del número de dominios ".es" sigue una progresión lineal, mientras que la de los dominios ".es" que implementan DNSSEC experimenta un ascenso muy significativo, especialmente en los últimos meses.

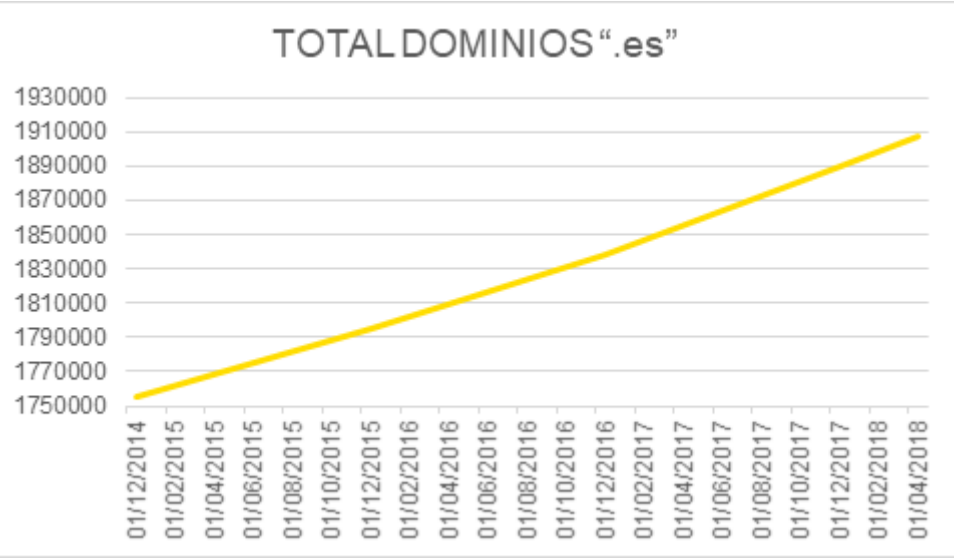



*Figura 51 - Evolución de los dominios ".es"*

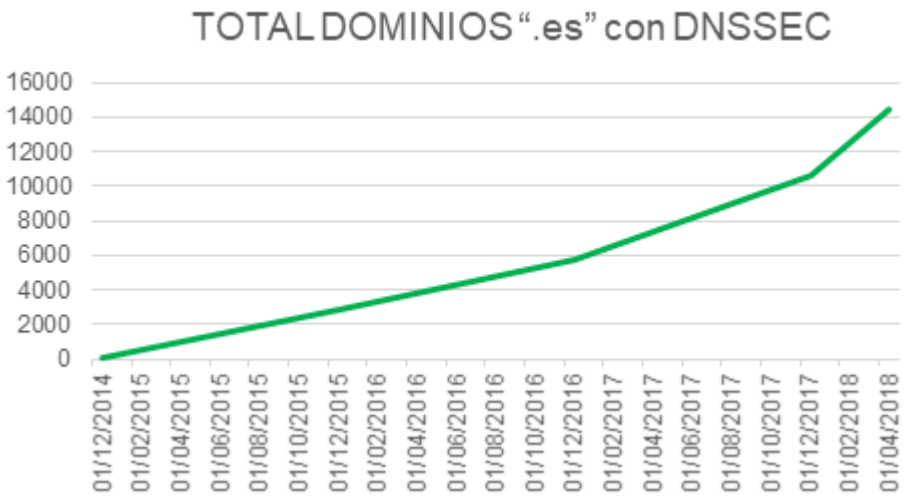



*Figura 52 - Evolución de los dominios ".es" con DNSSEC*

Sin embargo, las anteriores estadísticas no reflejan las causas subyacentes a esta progresión en la implantación de DNSSEC. Para ampliar el foco del análisis, es necesario centrarse en los números asociados a los agentes registradores de dominios en la zona ".es" que, a su vez, aparte del servicio de registro del dominio, ofrecen servicios de gestión y configuración del servicio DNS, y potencialmente DNSSEC, a sus clientes.

La siguiente tabla proporciona una visión sobre los dominios gestionados por cada uno de los 36 agentes registradores que ofrecen el servicio DNSSEC a sus clientes (del total de 103 agentes registradores que operan en la zona ".es"). A fecha de elaboración de la presente guía, se observa que solo el 0,84% del total de dominios ".es" han implementado DNSSEC:

| | Dominios con DNSSEC | Total dominios | % dominios DNSSEC del proveedor | % dominios del proveedor sobre el total de dominios .es | % dominios del proveedor sobre el total dominios DNSSEC |
|---|---|---|---|---|---|
| 1 | 15 | **355.522** | 0,004219% | **20,82%** | 0,1039% |
| 2 | 14 | 19771 | 0,070811% | 1,16% | 0,0970% |
| 3 | 1 | 15944 | 0,006272% | 0,93% | 0,0069% |
| 4 | 9 | **119.802** | 0,007512% | 7,02% | 0,0623% |
| 5 | 2 | **190.817** | 0,001048% | 11,17% | 0,0139% |
| 6 | 96 | 52768 | 0,181928% | 3,09% | 0,6650% |
| 7 | 9 | 15589 | 0,057733% | 0,91% | 0,0623% |
| 8 | 1 | 2211 | 0,045228% | 0,13% | 0,0069% |
| 9 | 12 | 87885 | 0,013654% | 5,15% | 0,0831% |
| 10 | **2263** | **2587** | **87,475841%** | **0,15%** | **15,6761%** |
| 11 | 5 | 466 | 1,072961% | 0,03% | 0,0346% |
| 12 | 66 | 12470 | 0,529270% | 0,73% | 0,4572% |
| 13 | 2 | 33226 | 0,006019% | 1,95% | 0,0139% |

| | | | | | |
|---|---|---|---|---|---|
| **14** | 3 | 15753 | 0,019044% | 0,92% | 0,0208% |
| | 2 | 5872 | 0,034060% | 0,34% | 0,0139% |
| **16** | 1 | 3132 | 0,031928% | 0,18% | 0,0069% |
| **17** | 48 | 27913 | 0,171963% | 1,63% | 0,3325% |
| **18** | 2 | 3664 | 0,054585% | 0,21% | 0,0139% |
| **19** | 85 | **112.594** | 0,075492% | 6,59% | 0,5888% |
| | 1 | 14850 | 0,006734% | 0,87% | 0,0069% |
| **21** | 12 | 627 | 1,913876% | 0,04% | 0,0831% |
| **22** | 2 | 2638 | 0,075815% | 0,15% | 0,0139% |
| **23** | 65 | 56804 | 0,114429% | 3,33% | 0,4503% |
| **24** | 6339 | 99208 | 6,389606% | 5,81% | 43,9111% |
| | 3 | 46614 | 0,006436% | 2,73% | 0,0208% |
| **26** | 2 | 84827 | 0,002358% | 4,97% | 0,0139% |
| **27** | 1 | 10076 | 0,009925% | 0,59% | 0,0069% |
| **28** | 11 | 7679 | 0,143248% | 0,45% | 0,0762% |
| **29** | 4509 | 42396 | 10,635437% | 2,48% | 31,2344% |
| | 1 | 3535 | 0,028289% | 0,21% | 0,0069% |
| **31** | 1 | 842 | 0,118765% | 0,05% | 0,0069% |
| **32** | 46 | **97.221** | 0,047315% | 5,69% | 0,3186% |
| **33** | 3 | 53883 | 0,005568% | 3,16% | 0,0208% |
| **34** | 799 | 77017 | 1,037433% | 4,51% | 5,5348% |
| | 3 | 27935 | 0,010739% | 1,64% | 0,0208% |
| **36** | 2 | 3430 | 0,058309% | 0,20% | 0,0139% |
| | **14436** | **1707568** | **0,845413%** | **99,99%** | **100,0000%** |

*Tabla 4 - Estadísticas de dominios ".es" con DNSSEC por agente registrador*

La siguiente gráfica proporciona las estadísticas de los agentes registradores del dominio ".es", ordenados de menor a mayor según el número total (o porcentaje) de dominios ".es" que gestionan, resaltando en color rojo el número total (o porcentaje) de dominios ".es" con DNSSEC que también gestionan:

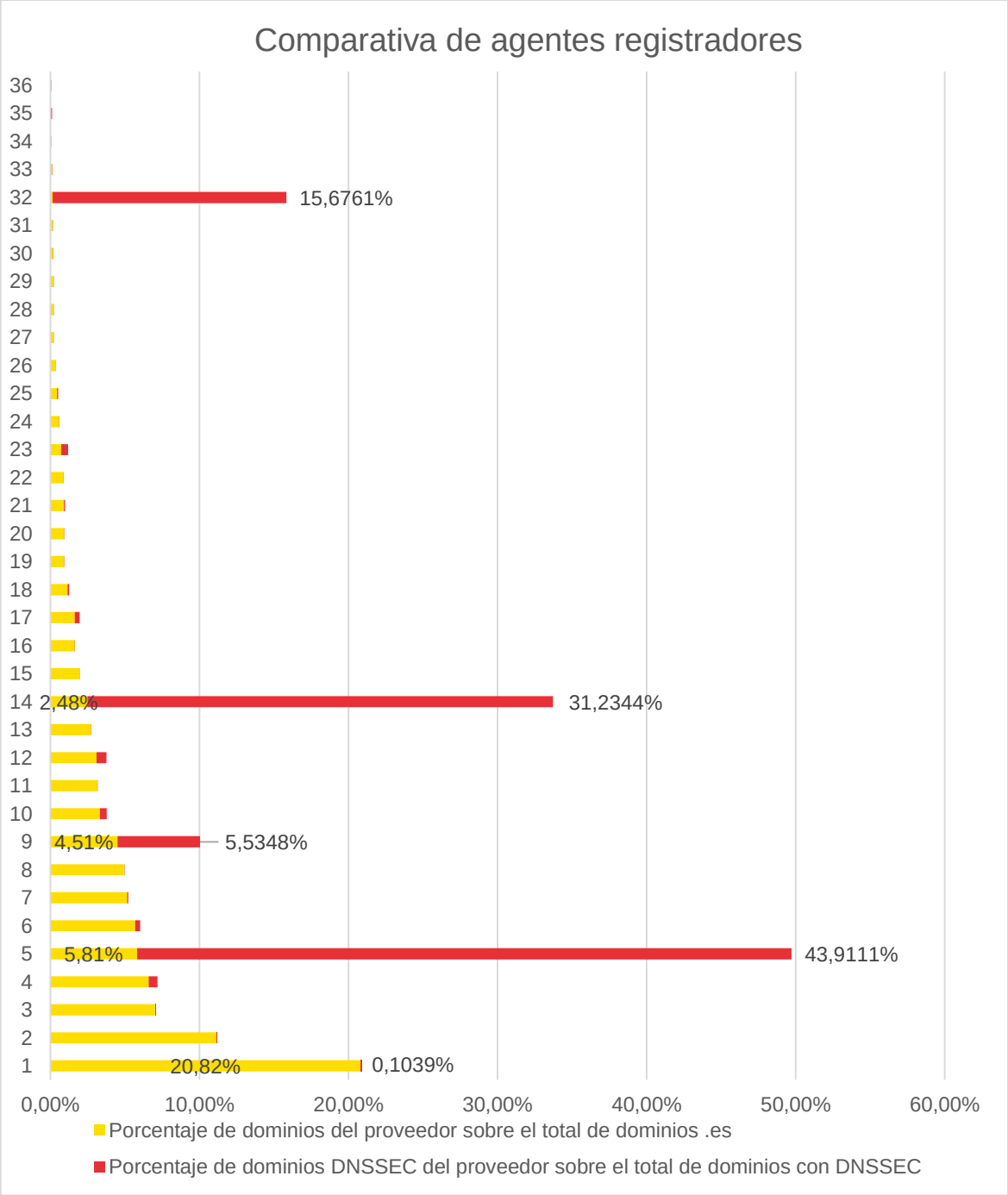



*Figura 53 - Comparativa de dominios ".es" con y sin DNSSEC por agente registrador*

A la vista de los datos anteriores, se obtienen las siguientes conclusiones:

- De los 36 agentes registradores que ofrecen DNSSEC a sus clientes en la zona ".es", solo 3 de ellos realmente aportan cifras significativas en cuanto al porcentaje

de implantación total de DNSSEC, con un 44%, 31% y 15,6% respectivamente (expresados en la última columna de la "Tabla 4"; estos agentes han sido destacados en color rojo en la tabla). Existe un cuarto agente registrador que aporta un 5,5% adicional de dominios DNSSEC.

- El agente registrador de la fila 10 en la "Tabla 4", pese a tener solamente una cuota del 0,15% sobre el total de dominios ".es" registrados, representa el 15,67% del total de dominios DNSSEC. Llama aún más la atención que sus cifras relativas constatan que el 87,47% de todos los dominios que este agente gestiona, implementan DNSSEC. Consultado el responsable técnico de "dominios.es", ratifica que este agente registrador activa el servicio DNSSEC *por defecto* para sus nuevas altas de dominios, lo cual constituye una ventaja crucial para sus clientes, pues obtienen los beneficios del protocolo DNSSEC sin necesidad de planificar su implantación.
- También destaca positivamente el agente registrador de la fila 24 en la "Tabla 4", ya que debido a que tiene casi un 6% del total de dominios ".es", su apuesta por DNSSEC hace que aporte casi un 44% del total de dominios ".es" con DNSSEC (aunque estos suponen únicamente algo más de un 6% de todos sus dominios).
- El agente registrador con más dominios ".es" a su cargo (fila 1), responsable del 20,82% del total de dominios ".es", con 355.522 dominios registrados, solo tiene implantado DNSSEC para 15 de ellos (un 0,10% del total de dominios con DNSSEC).
- Esta misma situación se repite con el resto de agentes registradores con un mayor número del conjunto total de dominios. El resto de agentes con un número cercano o superior a los diez mil dominios ".es" (filas 4, 5, 19 y 32) tampoco superan, ninguno de ellos, el 0,6% del total de dominios con DNSSEC.
- Finalmente, del total de 36 agentes registradores con dominios DNSSEC, el 96,3% de los dominios de DNSSEC son gestionados por los 4 registradores mencionados inicialmente, que, sin embargo, solo ostentan el 13% del total de dominios ".es".

Según las estadísticas obtenidas de APNIC Labs [Ref.- 51], el número de transacciones DNSSEC validadas desde *resolvers* ubicados en España está en torno al 8% (las imágenes que se presentan a continuación corresponden a datos de enero de 2018 y mayo de 2018 respectivamente), y demuestran un leve incremento en este breve período:

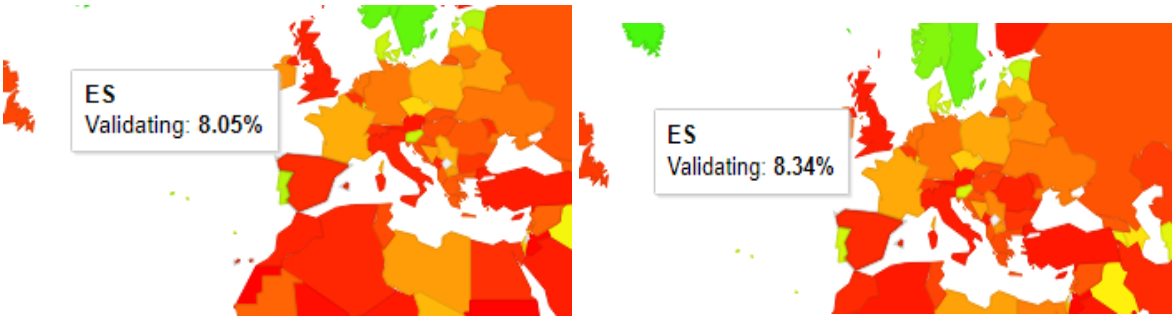



***Figura 54 - Porcentaje de validación de transacciones DNSSEC en España entre enero y mayo de 2018***

Sin embargo, esta cifra está bastante por debajo de la media europea, que ronda el 21% como ilustra la "*Figura 43*", y muy por debajo de Portugal, en torno al 61%. Cabe destacar como posible justificación que, mientras que Portugal fue uno de los primeros países del

mundo en firmar su ccTLD y desplegar su registro DS en la zona raíz (en el año 2010), fue a finales de 2014 cuando la zona ".es" estuvo totalmente operativa:

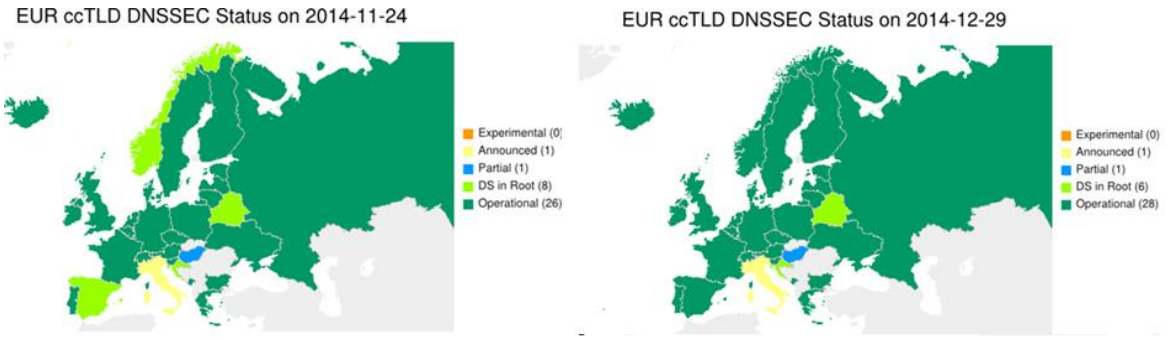



*Figura 55 - Despliegue de la zona ".es" de DNSSEC en la zona raíz (noviembre y diciembre de 2014)*

# 4. ASPECTOS CLAVE EN EL DISEÑO E IMPLANTACIÓN

La decisión de implantar DNSSEC pasa por valorar cuidadosamente diversos aspectos, tanto a nivel organizativo como técnico. El presente apartado tiene por objeto dar una visión general sobre los procedimientos, recursos y políticas que los responsables de seguridad de una organización deben considerar de cara a la toma de decisiones en las distintas fases del despliegue, desde el planteamiento inicial, pasando por la evaluación y el diseño, hasta la puesta en marcha del servicio y su posterior mantenimiento.

## 4.1. Consideraciones organizativas

El correcto despliegue del servicio DNSSEC requiere un planteamiento inicial detallado que permita definir el ámbito y alcance del servicio, entendiendo como tales su aplicación tanto en la parte cliente como servidor del servicio DNS, así como en su aplicación al entorno corporativo y/o a la presencia pública de la organización en Internet.

Adicionalmente, es necesario definir y planificar muchos otros aspectos que tienen una influencia directa en el servicio de DNSSEC, o en otros servicios que se ven afectados por DNSSEC como, por ejemplo, quién estará encargado de la gestión de DNSSEC.

Son tres los aspectos principales a determinar: ámbito, alcance y modelo:

- Ámbito: decidir si la implantación se llevará a cabo en la parte cliente DNS (*resolver*), que se encarga de la validación, en la parte servidora (responsable de la firma de la zona), o en ambas (de forma que el beneficio de la implantación de DNSSEC sea completo). Sin embargo, no necesariamente han de abordarse simultáneamente, pues no existe ningún impedimento para poder validar zonas DNSSEC sin que se hayan firmado los propios dominios, o, al contrario, para poder ofrecer la propia zona firmada de modo que los *resolvers* externos puedan validarla sin que internamente se realice validación de zonas externas.
- Alcance: determinar si el despliegue abarcará los servicios de resolución únicamente internos, los externos, o ambos. Es importante reseñar que, a nivel técnico, serán de aplicación todos los aspectos tratados a lo largo de la presente guía, a excepción de la publicación de los registros DS en los servidores autoritativos externos a la organización.
- Modelo: decidir si la gestión de la zona se hará como parte de los sistemas de información corporativos (ya sea de forma directa o a través de otra organización que los opera) o si se externalizará hacia un proveedor de servicios de *hosting* DNS. En este último caso, el elemento fundamental será la selección del proveedor cuyos servicios se adapten mejor a los requisitos identificados. El proceso de transferencia de una zona o dominio entre agentes registradores, o proveedores de servicios, es un trámite administrativo contemplado en el servicio DNS que, en principio, no debería tener implicaciones específicas si aún no se ha desplegado DNSSEC.

Adicionalmente, se debe valorar qué otros servicios y soluciones podrán beneficiarse del uso de DNSSEC una vez la infraestructura de confianza asociada y proporcionada por DNSSEC haya sido desplegada como, por ejemplo, el servicio de correo electrónico o e-mail, navegación web, etc. (ver apartado "4.3. DANE: Más allá del DNS").

### 4.1.1. Soporte de DNSSEC en proveedores de servicios

Previamente a la selección del proveedor, es preciso establecer qué criterios técnicos relativos a la operación de DNSSEC son obligatorios y cuáles opcionales, a fin de determinar qué operador/-es los ofrecen.

Se evaluarán las políticas que cada proveedor candidato tiene en marcha, en especial, los algoritmos de firma que soporta, así como sus procesos de gestión. En España, es habitualmente el agente registrador del dominio quien se encarga de subir los registros DS de la zona (junto a los registros NS) a los servidores de nombres de la zona ".es", por lo que, si la gestión del dominio no la realiza la misma entidad que tiene su registro, habrá que determinar si es viable la colaboración entre ambos o si resulta más conveniente transferir el registro del dominio al operador que lo gestiona o viceversa.

ICANN proporciona una lista oficial de agentes registradores [Ref.- 40] que ofrecen servicios de DNSSEC (incluyendo los TLDs con los que operan). Este listado no es completo ya que, a fecha de elaboración de la presente guía, únicamente muestra 5 agentes registradores con soporte para DNSSEC en el dominio ".es", por lo que no debe tomarse como el único, sino que se presenta como referencia. De hecho, en la sección de "Actualidad y noticias" de **dominios.es** [Ref.- 68], de octubre de 2015, se anuncia que, a fecha octubre de 2015, eran 13 los proveedores que ofrecían servicios de DNSSEC el ".es".

De cara tanto a la implantación de DNSSEC como a su posterior operación, una vez seleccionado el proveedor, será preciso obtener de él los detalles sobre cómo genera, custodia y despliega en la zona padre los registros DS asociados a las nuevas zonas que se desee firmar.

### 4.1.2. Soporte de DNSSEC en servidores propios

En el caso de que la gestión de la zona se lleve a cabo actualmente como parte de los sistemas de información (o servidores DNS) propios, será necesario identificar los dominios en los que se implantará DNSSEC. La introducción de soporte para DNSSEC por parte de la organización puede constituir en sí mismo un condicionante para redefinir si se cambia el modelo existente y se pasa a gestionar el servicio DNS con un proveedor de servicios externo, frente a seguir manteniéndolo en la infraestructura corporativa.

Incluso en el caso de que el dominio sea gestionado por la propia organización, habrá que contactar con el agente registrador que registró el dominio y acordar con él los procedimientos para la transferencia de los registros DS para la zona, y los plazos en los que este los trasladará a los responsables de la zona ".es" para identificar cuándo la zona estará operativa desde el punto de vista de DNSSEC.

Es decir, habitualmente, se mantiene una dependencia entre la organización y el agente registrador original, aunque la gestión del servicio DNS no esté externalizada.

## 4.2. Consideraciones técnicas

DNSSEC no es un servicio "*out-of-the-box*", en el sentido de que no basta con actualizar el software de DNS para activar el protocolo DNSSEC. Su correcto despliegue técnico y posterior operativa requieren la puesta en marcha de procedimientos de configuración y

de un plan de mantenimiento. Los aspectos técnicos cobran especial relevancia, pues una configuración incorrecta puede llevar a que el servicio DNS, y en consecuencia (debido a su dependencia), el resto de los servicios de la organización, queden inaccesibles, con el consiguiente impacto económico y de imagen. En la [Ref.- 61], IANIX proporciona una lista de incidentes relativos a DNSSEC que provocaron pérdida de servicio.

De manera oficial, el IETF publicó originalmente un conjunto de buenas prácticas de operación del servicio DNSSEC a través del RFC 4641 en el año 2006, que fueron posteriormente actualizadas mediante el RFC 6781 a finales del año 2012 [Ref.- 56].

Nuevamente, el escenario es diferente en función del modelo de gestión del servicio DNSSEC para el dominio de la organización (ver apartado "4.1. Consideraciones organizativas"). A continuación se describirán las cuestiones técnicas asociadas al despliegue de DNSSEC en general, pero las soluciones a algunas de ellas podrán venir impuestas por el proveedor del servicio DNS en los escenarios en que la gestión de la zona se haya externalizado, por lo que, desde el punto de vista del propietario del dominio, el margen de acción se puede ver reducido a conocer en detalle y utilizar los procedimientos proporcionados por su proveedor. En los casos en que el servicio DNS del dominio es gestionado por la propia organización, o para aquellos parámetros que sean configurables a través del proveedor de servicios, los aspectos técnicos deben ser analizados concienzudamente y puestos en práctica para evitar incidencias en el servicio DNSSEC.

### 4.2.1. Aspectos que afectan a la implantación del servicio DNSSEC

Entre los aspectos técnicos a tratar se encuentran, en primer lugar, las **soluciones software** y los **requisitos hardware** asociados al despliegue de DNSSEC, tanto para los servidores DNS autoritativos como para los *resolvers* DNS.

DNNSEC, desde el punto de vista del usuario final, realiza la misma función que el servicio DNS, coexistiendo con él tanto dentro como fuera de la organización. Idealmente, se deberá disponer de un **entorno de desarrollo** que permita realizar todas las pruebas necesarias (firmado de zonas, despliegue del servicio, evaluación del rendimiento, análisis de errores, etc.) antes de proceder a la puesta en **producción** del servicio DNSSEC.

Los siguientes apartados proporcionan recomendaciones que se aplican principalmente en escenarios en los que el servicio de resolución de nombres es gestionado por la propia organización. En el caso de que el servicio DNS se externalice en un proveedor de servicios, solo serán de aplicación aquellas recomendaciones sobre las que la organización disponga de capacidad de actuación en función de la versatilidad y flexibilidad ofrecida por el proveedor respecto a los recursos empleados y a la configuración del servicio DNSSEC.

#### 4.2.1.1. Implantación de DNSSEC en los servidores DNS autoritativos

El punto de partida para la implantación es seleccionar un **software de los servidores DNS autoritativos** que soporte DNSSEC, como BIND [Ref.- 41] o el servidor DNS de *Microsoft Windows Server* 2012. Otros productos de código abierto que implementan

DNSSEC para el rol de servidor son YADIFA [Ref.- 39], NSD [Ref.- 46] y Knot DNS [Ref.- 43].

La selección del software que se empleará como servidor DNS debe tener en cuenta la integración de los servidores DNS con la arquitectura y entorno tecnológico actual de la organización. Entre las capacidades que se deben exigir al software del servidor DNS están las de auditoría, de forma que sea posible revisar en detalle las transacciones DNS procesadas y proceder a la corrección de las mismas en caso necesario. Esta recomendación aplica tanto a los servidores DNS autoritativos como a los *resolvers* (ver apartado "4.2.1.2. Implantación de DNSSEC en los *resolvers*").

Asimismo, se debe seleccionar el **hardware para los servidores** en los que se implementará el servicio de nombres con soporte para DNSSEC, teniendo en cuenta que las operaciones de firma conllevan una mayor carga computacional (especialmente si se realizan en tiempo real), y que consumirán más ancho de banda, ya que las transferencias de datos en el protocolo DNSSEC son de mayor tamaño que en el protocolo DNS.

Además de los requisitos hardware asociados a los servidores DNS, se deberá estudiar el **dimensionamiento de la red,** de los equipos de red (*routers*, *firewalls*, etc.) y de otros componentes de red y/o de seguridad perimetrales (cortafuegos o *firewalls*, sistemas de detección de intrusos o IDS, balanceadores, etc.) en función del ancho de banda estimado para el servicio DNSSEC.

El siguiente elemento es la selección del **algoritmo criptográfico de firma** y el **esquema de claves** (par de claves, pública y privada), tanto de la clave asociada a la firma de la zona (ZSK) como de la clave asociada a la firma de las claves de zona (KSK). Ambas claves tienen distinto propósito y se emplean de forma diferente, por lo que el análisis de requisitos de su definición y utilización debe acometerse para cada una de ellas de forma independiente. En ambos casos, se debería analizar:

- El algoritmo de firma y la longitud de las claves, de forma que sean suficientemente robustos desde el punto de vista de seguridad, pero que no sobrecargue en exceso ni al servidor DNS autoritativo ni a los *resolvers* DNS recursivos que formularán las consultas, requiriendo recursos o capacidad de computación excesiva.
- La longitud de los *hashes* criptográficos a emplear: SHA-1, SHA-256, SHA-384, SHA-512, etc.
- El período de validez de las claves (condicionado desde el punto de vista de seguridad por los dos factores previos), y su proceso de renovación.
- El procedimiento de renovación de las claves, especialmente de la clave KSK, por su impacto en entornos y servidores DNS externos.
- La correcta generación y el almacenamiento seguro de las claves, más concretamente de la clave privada, de forma que no estén accesibles a través de recursos disponibles *online* o de equipos y redes sin un nivel de seguridad elevado (idealmente).
- El uso de las mismas o distintas claves para el firmado de distintas zonas o subzonas, recomendándose desde el punto de vista de seguridad independizar las claves de cada zona.
- Se deben tener en cuenta consideraciones adicionales si la clave KSK va a ser utilizada como *trust anchor* [Ref.- 56].

De cara a la gestión de las claves, existe un proyecto denominado "**OpenDNSSEC**"[24], cuyo objetivo es simplificar las tareas de firmado de zona y mantenimiento de las claves DNSKEY.

Respecto a la configuración del servicio DNSSEC, hay que considerar el **uso de registros NSEC o NSEC3** para la gestión de recursos DNS inexistentes en función del riesgo que pueda suponer (o no) la enumeración de zona. Asimismo, se deben definir los parámetros de estos registros, incluyendo el algoritmo de *hashing*, el número de iteraciones y la semilla.

En caso de que exista **delegación de la zona en subzonas**, habrá que planificar la creación y distribución de los correspondientes registros DS de las zonas hija a la zona padre, y valorar para cada una de ellas todos los aspectos técnicos señalados para la zona principal.

Se recomienda habilitar (al menos inicialmente) el **registro de *logs* de los servidores DNS** al máximo nivel de detalle, incluyendo las capacidades de auditoría, a fin de poder verificar la validez de la zona firmada y detectar posibles fallos o incidencias antes de la publicación completa y generalizada de la zona en los servidores DNS autoritativos externos.

#### 4.2.1.2. Implantación de DNSSEC en los *resolvers*

Además de los aspectos de implantación de DNSSEC en el lado del servidor, es decir en los servidores DNS autoritativos, para que el servicio DNSSEC resulte efectivo no hay que obviar las tareas de diseño y configuración necesarias en el lado cliente (o servidores DNS *resolver*).

Dentro de la categoría de *resolvers* DNS, existen dos tipos, y en todos ellos se recomienda la implantación de DNSSEC para que los potenciales errores en el proceso de resolución de nombres se procesen correctamente y no den lugar a ambigüedad:

- ***Stub resolvers***: corresponden al cliente DNS (software, aplicación o librería) de los sistemas clientes finales, que necesitan acceder a numerosos servicios internos o disponibles en Internet, empleando el servicio de resolución de nombres.
- **Servidores caché recursivos o *resolvers* DNS**: aquellos servidores DNS que, a petición de un cliente final, se encargan de centralizar las consultas, trasladándolas a los respectivos servidores DNS autoritativos. Tienen establecida en su configuración una cadena de confianza (*trust anchor*) de toda la jerarquía de DNSSEC que habitualmente comienza en la zona raíz.

Dado que no es recomendable desde el punto de vista de seguridad (a nivel perimetral), escalabilidad y rendimiento que los clientes finales realicen las consultas directamente sobre el servidor de nombres autoritativo, especialmente para la resolución de nombres en Internet, se ha de configurar correctamente el/los *resolvers* recursivos que dan servicio a los clientes internos para que formulen las consultas y procesen correctamente las respuestas de DNSSEC. Es importante destacar que la validación de DNSSEC solo

[24] https://www.opendnssec.org/

tendrá éxito si está habilitada en todos los *resolvers* recursivos involucrados en el proceso de resolución. En caso contrario, los *stub resolvers* podrían estar protegidos o no en función de a qué *resolver* se encaminase su consulta y las validaciones que fueran realizadas por este.

Por su parte, para que un servidor autoritativo de una zona proporcione respuestas firmadas, se requiere que el *resolver* indique en su consulta que soporta este mecanismo.

Un elemento fundamental en los servidores DNS resolver es asegurarse de que se establece de manera fiable el ***trust anchor*** de más alto nivel **de la zona raíz**, para que sea posible disponer de la cadena de confianza completa a través de la jerarquía de DNS.

El **software de los servidores caché** debe disponer de soporte para DNSSEC a la hora de resolver consultas recursivas, y el **hardware** debe dimensionarse de forma que soporte el mayor ancho de banda y carga computacional asociados al protocolo DNSSEC. Complementariamente, se puede configurar que el *resolver* DNS recursivo externo de la organización apunte a un ***open resolver*** que valide las transacciones mediante DNSSEC. No obstante, para que este escenario sea seguro y resistente frente a ataques MitM, se debería definir un canal de comunicación seguro entre el servidor DNS recursivo de la organización y el *open resolver*, por ejemplo, mediante DNS sobre TLS. Entre los *open resolvers* más conocidos que soportan DNSSEC se encuentran el de Cloudflare (1.1.1.1) [Ref.- 45] y el de Google (8.8.8.8) [Ref.- 44].

### 4.2.2. Aspectos que afectan a la operativa del servicio DNSSEC

Una vez el servicio DNSSEC ha sido puesto en marcha de forma exitosa, desde el punto de vista del usuario final, este realiza la misma función que el servicio DNS, coexistiendo con él; aunque el servicio DNS es un servicio de naturaleza dinámica y en el que pueden realizarse cambios sencillos y muy frecuentes que dan lugar a actualizaciones de manera distribuida, el diseño e implementación de DNSSEC conlleva elementos técnicos adicionales que pueden afectar a esa flexibilidad del servicio DNS y a la operativa diaria si no se planifican correctamente.

**Diseñar un mecanismo eficaz para detectar errores y analizar el comportamiento del protocolo y servicio DNSSEC**, tanto para servidores DNS autoritativos como *resolvers* (motivo por el cual se describe en la introducción de este apartado), es un hándicap importante en la planificación técnica, dado que las herramientas que existen actualmente para el mantenimiento y monitorización de DNSSEC son más escasas que las existentes para DNS y pueden no tener el mismo nivel de madurez ni de funcionalidad, especialmente las comerciales. Esto puede conllevar que la identificación de problemas resulte más difícil y se requiera mayor intervención manual en lugar de automatizada por parte del personal administrador y responsable del servicio DNSSEC.

#### 4.2.2.1. Operación de DNSSEC en los servidores DNS autoritativos

La principal prioridad en la operativa de DNSSEC es asegurar que la cadena de confianza empleada para la verificación de las firmas de los registros del servicio DNS no se rompe, pues en caso contrario la zona podría convertirse en una isla (o entorno aislado) y no poder resolverse correctamente, tanto desde el exterior como desde el

interior, por lo que la **definición de la política gestión de claves** ha de ser muy exhaustiva.

En el caso de las **claves ZSK y KSK**, y al igual que para la implantación de DNSSEC (ver apartado "4.2.1.1. Implantación de DNSSEC en los servidores DNS autoritativos"), debido a que tienen distinto propósito y se emplean de forma diferente, el análisis de requisitos de su operación y mantenimiento debe acometerse para cada una de ellas de forma independiente. En ambos casos, se debería analizar:

- Periodo de renovación.
- Mecanismo de renovación, incluyendo el proceso para trasladar los registros DS firmados con la nueva KSK a la zona padre.
- Procedimientos de renovación de forma que se asegure que el tiempo de propagación de los cambios no afecta al servicio.
- Análisis del algoritmo de firma empleado para la zona para ver si procede su reemplazo.
- Necesidad de utilizar registros NSEC3 si surgen riesgos asociados a la enumeración de zona.

En relación con los elementos anteriores, deberá definirse una **política de *backup*** (copias de seguridad) **y restauración** del servidor DNS que tenga en cuenta el período de validez de las claves de DNSSEC, incluyendo los registros DS de subdominios o subzonas pertenecientes a la zona objetivo (si existen), a fin de no restaurar nunca registros DNSSEC (especialmente DNSKEY y DS) que estén próximos a expirar o que hayan sido firmados con claves antiguas ya expiradas.

Adicionalmente, se ha de planificar un **procedimiento manual de revocación/renovación de claves para situaciones excepcionales o de emergencia**, por ejemplo, ante un potencial ataque que comprometa cualquiera de las claves de DNSSEC, de forma que el personal técnico a cargo de la gestión del dominio pueda actuar ágil y eficazmente ante el incidente de seguridad.

**DNSSEC introduce el concepto de "tiempo absoluto" en el esquema de resolución de nombres**, al contrario que en el servicio DNS, donde el tiempo solo es relativo y basado en el TTL (*Time To Live*) de los registros, ya que las firmas (registros RRSIG) tienen un período de validez Por tanto, los *resolvers* y los servidores DNS autoritativos deben estar sincronizados en tiempo para evitar que los registros sean considerados inválidos por parte del *resolver* por un problema de referencia horaria.

Se debe planificar el esquema de replicación de una zona entre el servidor DNS primario y los secundarios para evitar que existan **inconsistencias durante el tiempo de propagación de la zona** que ocasionen que los *resolvers* puedan obtener respuestas diferentes en función del servidor que gestione su consulta.

Dado que DNSSEC no protege las **operaciones de transferencia de zona**, se debe evaluar otras opciones para sincronizar los datos del servicio DNS entre diferentes servidores autoritativos de una zona, mediante registros TSIG (*Transaction SIGnature*) definidos originalmente en el RFC 2845 y reemplazado posteriormente por el RFC 3645 [Ref.- 69].

El proceso de **transferencia de una zona entre agentes registradores**, así como la de gestión del dominio entre proveedores de servicios, que en DNS es un trámite

administrativo contemplado en el servicio, puede tener implicaciones relevantes una vez ya ha sido desplegado DNSSEC. No existe un procedimiento estándar establecido para la realización de este traspaso entre agentes registradores, por lo que se recomienda contactar con los agentes origen y destino de la transferencia para coordinar todos los detalles de esta operación (incluyendo el traspaso o migración de las claves DNSSEC de la zona).

#### 4.2.2.2. Operación de DNSSEC en los *resolvers*

Dado que las ***trust anchor* de la zona raíz** (".") vienen pre-compiladas en las aplicaciones, software y servicios que soportan DNSSEC, es importante actualizar el software de los *resolvers* DNS, así como prestar atención a la ceremonia de firma de la zona raíz, para poder adaptar y actualizar la configuración de DNSSEC frente a los cambios que se producen en el ecosistema DNSSEC a nivel global [Ref.- 29].

Adicionalmente, se ha de planificar un **procedimiento manual de revocación/renovación de la cadena de confianza de emergencia**, por ejemplo, ante un potencial ataque que comprometa las claves de DNSSEC empleadas como ***trust anchor*** en los servidores DNS *resolver*.

Es importante **analizar los *logs* de los *resolvers*** para detectar fallos o errores de validación. Los errores aislados probablemente no tendrán importancia, pero, si se observan muchos errores relativos a un TLD de nivel superior concreto, pueden indicar un fallo grave en dicho dominio o incluso reflejar la existencia de un incidente de seguridad, que puede tener impacto directo para los usuarios. En este caso, se recomienda deshabilitar temporalmente la validación DNSSEC para ese dominio en particular, en función del tipo de tipo de incidente identificado.

## 4.3. DANE: Más allá del DNS

El modelo criptográfico empleado actualmente por la mayor parte de los servicios en Internet basados en TLS (por ejemplo, correo electrónico o e-mail, HTTPS, VPNs, etc.) implica la existencia de autoridades certificadoras (CAs, *Certificate Authorities*) en cuya firma se confía para dar por válidas la identidad y firmas de las demás entidades, ya que pueden emitir certificados digitales para cualquier nombre de dominio. Este modelo presenta el inconveniente de que, si la clave privada de una CA se ve comprometida (algo que ha ocurrido en varias ocasiones a lo largo de la historia), podrá emitirse un nuevo certificado digital falso que reemplace el certificado legítimo de una entidad, permitiendo suplantar, e interceptar y manipular las comunicaciones de todos los servicios del dominio afectado (asociados a dicho certificado).

El modelo establecido por DNSSEC en lo relativo a la cadena de confianza en las claves criptográficas de cada zona mejora en varios aspectos el modelo típico de confianza en las CAs:

- Asocia la clave a un nombre de dominio en el servicio (en lugar de a una entidad identificada por una cadena de caracteres).
- Las claves están firmadas de manera distribuida por la zona padre del dominio (y solo por ella).

- La clave que asegura la cadena de confianza (*trust anchor*) está codificada en el software cliente y/o servidor de DNSSEC, pero solo para un único dominio (la zona raíz), y no para multitud de autoridades certificadoras de diferentes regiones, países, y organizaciones.

DANE (*DNS-Based Authentication of Named Entities*), definido inicialmente en el RFC 6698 [Ref.- 63] y actualizado posteriormente mediante el RFC 7671 [Ref.- 64], surge como una iniciativa para aprovechar la infraestructura de DNSSEC para almacenar y firmar los certificados digitales que se usan en TLS, de forma que dichos certificados (y/o sus claves públicas) se vinculen con el nombre del servidor dentro de su dominio en el servicio DNS (que a su vez está asociado a la entidad responsable de dicho dominio). Con ello, se reduce significativamente el ámbito e impacto frente a un hipotético incidente de seguridad en el que se comprometan las claves, ya que este solo afectaría a los servicios pertenecientes a esa jerarquía DNS y no a cualquier otra entidad (principio de "*mínimo privilegio*"). Es decir, DANE es un conjunto de mecanismos de autentificación para el establecimiento de comunicaciones criptográficamente seguras a través de la vinculación del certificado digital con el nombre del dominio a través de DNSSEC.

DANE incorpora los denominados registros TLSA (Transpor Layer Security Authentiacation), que son registros RR del servicio DNSSEC, que asocian el certificado digital o la clave pública de un servidor TLS con el nombre de dominio al que pertenece dicho registro. Cuando se utiliza DANE para establecer la conexión con un servicio basado en TLS, se obtiene el certificado digital del servicio en la negociación inicial del protocolo TLS y, en paralelo, se realiza una consulta DNSSEC para comprobar que el certificado que se recibió concuerda con el registro TLSA correspondiente. El formato de los registros TLSA es el siguiente:

```
puerto._protocolo_transporte.dominio
```

Por tanto, se puede utilizar para autentificar cualquier servicio basado en TLS, como por ejemplo HTTPS o correo electrónico (referenciado posteriormente):

```
_443._tcp.www.dominio.com
_25._tcp.mail.dominio.com
```

Con base en las estadísticas publicadas en SecSpider [Ref.- 58], se constata que el despliegue de DANE es aún muy reducido, suponiendo menos del 2% de las zonas con soporte para DNSSEC:

**Detailed Monitoring Summary:**

DNSSEC Summary

2,666,245 Zones
2,127,204 DNSSEC enabled zones
2,078,422 Zones use both KSKs and ZSKs
173 Zones are serving revoked keys
1,877,970 DNSSEC verified zones
2,080,410 Production DNSSEC-enabled zones

**Distribution of key algorithms in use:**

| Algorithm | # Keys |
|---|---|
| Unknown Algorithm | 21 |
| DSA-NSEC3-SHA1 [DSA-NSEC3-SHA1] | 23 |
| DSA/SHA-1 [DSA] | 209 |
| ECC/GOST [ECC-GOST] | 119 |
| ECDSA Curve P-256 with SHA-256 [ECDSAP256SHA256] | 491,247 |
| ECDSA Curve P-384 with SHA-384 [ECDSAP384SHA384] | 8,667 |
| Private [PRIVATEOID] | 5 |
| RSA-NSEC3-SHA1 [RSASHA1-NSEC3-SHA1] | 1,587,621 |
| RSA/MD5 [RSAMD5] | 22 |
| RSA/SHA-1 [RSASHA1] | 64,025 |
| RSA/SHA256 [RSASHA256] | 3,099,854 |
| RSA/SHA512 [RSASHA512] | 9,997 |

DANE Summary

40,944 DANE enabled zones with TLSA records
174 PKIX based Trust Anchor TLSA records (Cert Usage 0)
1,393 PKIX based End Entity TLSA records (Cert Usage 1)
1,806 DANE based Trust Anchor TLSA records (Cert Usage 2)
22,943 DANE based End Entity TLSA records (Cert Usage 3)

911 Zones have deployed TLSA for Secure SMTP (Port 465)
398 Zones have deployed TLSA for Secure POP3 (Port 995)
1,255 Zones have deployed TLSA for SMTP with STARTTLS (Port 587)
119 Zones have deployed TLSA for Alternate SMTP (Port 2525)
16,361 Zones have deployed TLSA for HTTPS (Port 443)
5,609 Zones have deployed TLSA for SMTP (Port 25)
248 Zones have deployed TLSA for POP3 (Port 110)
905 Zones have deployed TLSA for Secure IMAP (Port 993)
510 Zones have deployed TLSA for IMAP (Port 143)

*Figura 56 - Estadísticas de despliegue de DNSSEC y DANE (SecSpider)*

Desde el punto de vista del servidor, la incorporación de DANE a una infraestructura que ya implemente DNSSEC resulta sencilla, pues simplemente requiere añadir los correspondientes registros TLSA a la zona DNS.

Complementariamente, existen otras iniciativas para extender las capacidades de autentificación que aporta DNSSEC, por ejemplo:

- Añadir registros a zonas DNS con los certificados de las CAs de confianza.
- Almacenar certificados digitales, o referencias a certificados digitales, que proporcionen mecanismos alternativos para probar su autenticidad fuera del ámbito de la jerarquía de CAs (PKI, Public Key Infrastructure) que los emitió.
- Almacenar los identificadores de las claves SSH en el servicio DNS para proporcionar mecanismos de autenticación a los administradores de sistemas en los correspondientes servidores.
- Almacenar referencias a metadatos de identidad de la organización en el servicio DNS.

Con respecto a la integración de DANE en otros protocolos[25] y servicios, el RFC 7672 [Ref.- 66] detalla el uso de DNSSEC para el protocolo SMTP (Simple Mail Transfer Protocol) de envío de mensajes entre servidores de correo electrónico, mientras que el RFC 8162 [Ref.- 65] de mayo de 2017 describe como hacer uso de DNSSEC para asegurar la autenticidad, integridad y cifrado de correos electrónicos mediante S/MIME. En agosto de 2016 se creó el RFC 7929 [Ref.- 57] para aplicar los mecanismos DANE a OpenPGP, empleado también para autentificar y cifrar correos electrónicos y ficheros. A fecha de elaboración de la presente guía, este estándar sigue en fase experimental.

[25] https://tools.ietf.org/html/rfc7673

## 4.4. Costes de implantación y motivación

Tanto los costes de implantación de DNSSEC como los beneficios derivados de este servicio han de analizarse desde el punto de vista del rol o papel que se juega en el despliegue de este protocolo.

Los datos aportados en este apartado proceden de un estudio publicado en 2009 por ENISA (European Network and Information Security Agency) sobre los costes de despliegue de DNSSEC [Ref.- 6]. Entre paréntesis se refleja la nomenclatura empleada por ENISA para referirse a cada rol en dicho estudio.

- Usuario final: de cara a los equipos de usuario final, los costes pueden considerarse prácticamente nulos, ya que se reducen a disponer de una versión de un *stub resolver* que soporte DNSSEC y seguir el manual de usuario para realizar la configuración pertinente, existiendo diversas alternativas tanto comerciales como de código abierto. Son los principales beneficiarios de la implantación de DNSSEC, por lo que, teniendo en cuenta que su relación coste/beneficio es máxima, son los principales interesados en promover el despliegue.
- Propietario del dominio gestionado por un proveedor de servicios: dado que, a fecha de elaboración de la presente guía, se constata que existen en España agentes registradores que proporcionan soporte para DNSSEC sin coste adicional, e incluso algunos lo habilitan por defecto, también se puede considerar que para los responsables de un dominio el uso de DNSSEC no tiene una repercusión económica relevante. Igual que en el caso anterior, su relación coste/beneficio es máxima.
- Agente registrador (*registrar* o RAR): dado su papel crítico en el correcto funcionamiento de las cadenas de confianza de DNSSEC, se requiere que los agentes registradores dispongan de experiencia en los procesos, especialmente en la gestión de claves y en su transferencia a las entidades de nivel superior propias de cada país y/o zona. Su papel depende de si actúan como meros intermediarios entre el propietario del dominio y el responsable del TLD de nivel superior o sí, además, realizan labores de forma directa en el despliegue y mantenimiento de la zona.
- Registro (*registry* o RY): esta figura es la responsable de la gestión y operación de los TLDs de primer nivel, ya sean ccTLDs o gTLDs y, por ende, de garantizar la cadena de confianza de DNSSEC. Dado que la mayor parte de zonas TLD ya están firmadas, no se entrará en detalles sobre los costes asociados a este tipo de organizaciones. Respecto a la motivación de los Registros (*Registries*) de cara al despliegue de DNSSEC, se puede considerar que éticamente tienen la responsabilidad de aplicar las mejores prácticas con el fin de aumentar la seguridad de Internet relativa al servicio de resolución de nombres, que es, por otra parte, objeto de múltiples ataques de gran impacto a nivel mundial. Dado que buena parte de los registros son entidades públicas y organizaciones sin ánimo de lucro, los objetivos de coste/beneficio no suelen estar entre sus prioridades más directas.
- Operador de zona (ZO): ya sea como propietario o responsable de un dominio autogestionado o como proveedor del servicio de gestión de dominios para sus clientes, sobre esta figura recae todo el peso de poner en marcha las medidas

reflejadas en los apartados "4.1. Consideraciones organizativas" y "4.2. Consideraciones técnicas", a fin de adecuar su infraestructura, su personal y sus procedimientos al modelo requerido por el servicio DNSSEC.
- Operador de un *resolver* recursivo (RRO): debe asegurarse de que el servicio de nombres sea fiable de cara al usuario final, validando en su extremo la cadena de confianza de DNSSEC sin penalizar el rendimiento del servicio.

Como se deduce del listado anterior, DNSSEC beneficia de forma directa a usuarios finales y propietarios de dominios gestionados en proveedores de servicios, con el mínimo coste. Dado que el grueso a nivel económico del despliegue de DNSSEC recae sobre la parte servidora (frente a los clientes DNS), a continuación se dará una visión general de los costes y motivaciones en función del rol de cada una de las figuras citadas anteriormente.

El estudio de ENISA [Ref.- 6] se elaboró a partir de entrevistas a 20 empresas que habían tenido algún tipo de relación con el despliegue de DNSSEC, desempeñando distintos roles, y con distintos niveles de experiencia, designadas por consenso entre el grupo de ENISA experto en DNS, el CENTR y Deloitte. La lista de estas empresas, procedentes en su mayor parte de Suecia, República Checa y Holanda, está disponible en el apartado 4 y en el Apéndice A del estudio.

El estudio divide los costes en dos categorías:

- CAPEX (*Capital Expenditures*): gastos que una organización dedica a adquirir bienes o recursos, o a mejorar los existentes, y de los cuales se esperan beneficios.
- OPEX (*Operational Expense*): costes que se derivan de la operativa y mantenimiento del propio servicio, de los cuales no se espera beneficio directo.

Los costes dependen fundamentalmente de la situación de partida de cada agente, quedando el análisis exhaustivo fuera del ámbito de aplicación de este estudio.

### 4.4.1. Costes de implantación en el agente registrador

El agente registrador puro, entendido como agente que media para el alta del dominio entre el solicitante (*registrant*) y el responsable del TLD de primer nivel (*registry*), sin proporcionar ningún servicio adicional, ha de conocer detalladamente los procedimientos necesarios para dar de alta un dominio con soporte para DNSSEC. Sin embargo, estos procedimientos han de estar claramente definidos por el responsable del TLD, por lo que, de cara al agente registrador, no se incurre en ninguna complejidad extra más allá de adaptarse a ellos.

En función de la complejidad de los procesos necesarios para ofrecer el servicio de DNSSEC de cara al usuario final, el estudio de ENISA estima que la inversión puede rondar los 5.000 € en CAPEX y otros 5.000 en OPEX, es decir, un total de 10.000 €, y no depende del número de zonas registradas por el agente registrador, ni del tamaño de la organización.

La motivación para un agente registrador de cara a ofrecer DNSSEC es aprovechar la ventaja competitiva de cara a sus clientes respecto a agentes registradores que no lo ofrecen.

### 4.4.2. Costes de implantación en un operador de zona

Como responsable de la organización a cargo de la operación a nivel técnico de zonas DNS y/o nombres de dominio, el operador de zona es el agente encargado de la operación y el mantenimiento de la infraestructura de los servidores de nombre.

El estudio de ENISA ofrece resultados muy dispares, de modo que distingue entre lo que denomina "big savers" (grandes ahorradores) y los "big spenders" (grandes gastadores). De media, los *big savers* adoptaron DNSSEC con un CAPEX medio de 27.000 €; sin embargo, el CAPEX de los *big spenders* fue de 608.000 € de media, sin poderse establecer una relación entre el número de zonas o de consultas procesadas y los costes asociados.

Table 2 – **Total CAPEX cost for Registrars and Zone Operators**

| # ID | Role | Total CAPEX Cost |
|---|---|---|
| # 17 | RY; ZO | 1.329.940€ |
| # 18 | RY; ZO | 787.700€ |
| # 11 | ZO | 335.590€ |
| # 1 | ZO; RRO | 321.000€ |
| # 12 | RAR; ; ZO; RRO | 266.240€ |
| # 4 | ZO | 36.059€ |
| # 2 | RY; RAR; ZO | 28.600€ |
| # 20 | ZO | 26.023€ |
| # 6 | ZO | 22.617€ |
| # 19 | RAR; ZO; RRO | 17.000€ |
| # 10 | RAR; ZO | 6.575€ |
| # 5 | ZO | 5.100€ |
| # 13 | RAR; ZO | 4.855€ |
| # 4 | RAR | 4.620€ |

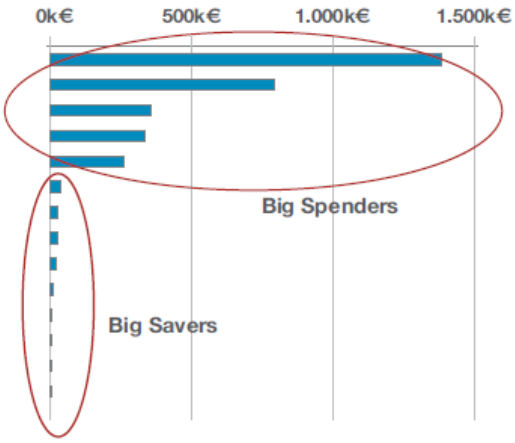



*Figura 57 - CAPEX para agentes registradores (RARs) y operadores de zona (ZOs)*

El estudio de ENISA permitió determinar que los *big spenders* adoptaban un posicionamiento estratégico hacia DNSSEC, contribuyendo al desarrollo de herramientas de código abierto y a las políticas de implementación del protocolo, como gestión de claves y definición de procesos para su operación. Por el contrario, los *big savers* simplemente hicieron uso de las herramientas ya existentes, reduciendo su estrategia a simplemente adaptarse a la tecnología. Pese a ello, la mayor parte de los *big savers* (con inversión inferior a 100.000 €) atribuyeron en torno al 90% a los gastos de desarrollo.

Ningún participante del estudio hacia uso de software comercial, sino de herramientas de código abierto con mayor o menor nivel de personalización según las características de la organización. Se estima que el 83% de las organizaciones emplea este tipo de herramientas.

A nivel de personal técnico, se observó que los *big spenders* pusieron más recursos a disposición del despliegue de DNSSEC.

La gestión de claves es uno de los principales elementos que compete a los *registries*, siendo objetivo primordial automatizar su gestión lo máximo posible. Los *registries* fueron los agentes que más revelaron su interés hacia las tecnologías HSM (*Hardware Security Module*) para poder almacenar de forma segura las claves privadas, pero la inversión en estos elementos resultó dispar, yendo desde los 100 € a los 25.000 €.

La mayor parte de los participantes reveló haber incurrido en costes de formación a su personal, pero no se dieron cifras concretas alegándose que la formación fue parte del presupuesto general dedicado a formación de la organización.

Respecto al OPEX, el único gasto cuantificable que se proporcionó por parte de los participantes del estudio fue el dedicado a mejorar el ancho de banda y a poner en marcha procedimientos que redujesen el impacto de DNSSEC en las operaciones de transferencia de zona. Algunos participantes indicaron que la necesidad de ancho de banda se había duplicado, frente a otros, que identificaron un incremento en torno a un 15%.

El estudio indica que el CAPEX por cada zona desplegada con DNSSEC para un *big saver* fue inferior a 7 €.

La motivación de cara a los operadores de zona para promover el uso de DNSSEC es ofrecer un servicio diferenciador respecto a la competencia de cara a sus clientes. Sin embargo, para ello se requiere que exista la demanda suficiente. Algunos agentes registradores cobran una pequeña cantidad a sus clientes por la gestión del dominio con DNSSEC (según el estudio, en torno a 2 €), por lo que también podría obtenerse un beneficio directo si aumentase la demanda. Al reducirse el CAPEX por zona según aumente el nivel de experiencia del operador, y teniendo en cuenta que su infraestructura ya está preparada (tras la inversión inicial), el aumento de la demanda, unido a la disminución en los costes de operación del dominio, podría suponer un incremento significativo de los beneficios totales.

### 4.4.3. Costes de implantación en un operador de un dominio propio

Dada la heterogeneidad de cada organización, resulta imposible proporcionar cifras relativas a los costes de despliegue cuando una organización se encarga de la gestión de su servicio DNSSEC. De cara a la evaluación de estos costes, los responsables de una organización que gestiona su zona han de tener en cuenta todos los aspectos técnicos y organizativos detallados en los apartados "4.1. Consideraciones organizativas" y "4.2. Consideraciones técnicas". Partiendo de la situación actual de sus sistemas dedicados al servicio de nombres estándar (DNS), de las capacidades técnicas del personal responsable del mismo, de los procesos operativos disponibles, de la infraestructura de comunicaciones y de su compromiso con la seguridad, se podrá iniciar el análisis detallado de los costes a prever.

Desde el punto de vista de una organización que gestiona su propio dominio, el grado de necesidad para desplegar DNSSEC depende enormemente de si la seguridad es en sí misma un beneficio que justifica el coste de la inversión. Por ejemplo, el sector financiero

o de la industria 4.0 son dos de los que podrían estar potencialmente más interesados en la adopción de DNSSEC.

Por otra parte, existen también beneficios proporcionados por DNSSEC en la autentificación de servicios corporativos de cara a los usuarios finales, garantizando que las comunicaciones internas se realizan también con el máximo nivel de seguridad.

### 4.4.4. Costes de implantación en un operador de un *resolver* recursivo

Como responsable de un *resolver* recursivo que proporciona servicio de resolución a los clientes finales (típicamente este rol lo ejercen los provedores de servicios de Internet, o ISPs, *Internet Service Providers*), el operador del *resolver* debe garantizar la disponibilidad del servicio de nombres de cara al cliente final, tanto para zonas con DNSSEC como sin él, y sin perjuicio del rendimiento del sistema.

Los *resolvers* DNS recursivos son el principal objetivo de los ataques de envenenamiento de caché. Sin embargo, dado que la mayoría de ISPs tienen desplegada una gran infraestructura para proporcionar servicio (superior a 200 servidores de nombres para los casos analizados en el estudio de ENISA), desplegar DNSSEC supone un esfuerzo (además de un coste) importante, que muchos de ellos no acaban de ver justificado desde el punto de vista de la inversión requerida.

Su motivación para implantar DNSSEC sería erigirse como elemento diferenciador frente a los *resolvers* de otros proveedores, especialmente teniendo en cuenta que ya existen *open resolvers* que implementan DNSSEC. La disponibilidad de soporte para DNSSEC por parte de *open resolvers* públicos ampliamente utilizados a nivel mundial, como el de Cloudflare o Google, puede colaborar a ampliar su adopción.

# 5. CONCLUSIONES DEL ESTUDIO

Los datos reflejados a lo largo de la presente guía muestran que la situación tecnológica y de la infraestructura de DNSSEC a fecha de su elaboración es favorable para el despliegue continuado del servicio DNSSEC. Además del soporte para DNSSEC existente en la zona raíz, donde el 91% de los TLDs de primer nivel están firmados, debe tenerse en cuenta que ICANN impone como requisito para los nuevos gTLDs que implementen DNSSEC. Respecto a los ccTLDs asociados a los diferentes países y regiones, la mayor parte están ya operativos a nivel mundial, proporcionando el servicio DNSSEC a los responsables de los dominios de segundo nivel e inferiores.

Sin embargo, los datos recabados a lo largo del presente estudio demuestran que la implantación de DNSSEC es aún muy baja en los TLDs de segundo nivel e inferiores. Con cifras en torno al 0,65% para el dominio ".com" y del 0,9% para el dominio ".net", se constata que, a pesar de que la zona raíz se firmó en el año 2010 y que los principales TLDs de primer nivel estuvieron disponibles desde el año 2013, la industria no ha incorporado DNSSEC entre sus medidas prioritarias de protección contra ataques. A nivel de país, destacan en Europa Suecia y Holanda, en los que las iniciativas de impulso sí han tenido efecto tanto a nivel de servidores como de clientes DNS.

Entre las razones que pueden subyacer a esta realidad se identifican:

- Falta de concienciación sobre la conveniencia del uso del servicio DNSSEC para evitar ciertas amenazas de seguridad que pueden afectar a la operativa de los servicios en Internet y en las propias organizaciones.
- Falta de conocimiento técnico sobre las tecnologías DNSSEC en organizaciones y entidades pequeñas, que lleva a estas a no demandarlo a los agentes registradores.
- Falta de conocimiento técnico sobre las tecnologías DNSSEC en el usuario final, que lleva a estos a no demandarlo a las organizaciones y proveedores de servicios.
- Temor a incurrir en errores técnicos que puedan tener un impacto directo en el servicio DNS y provoquen que la zona quede inaccesible.
- No obtener un retorno de inversión directo e inmediato.
- Desde el punto de vista de los agentes registradores y registros, expectativas de incurrir en gastos de operación y despliegue que no se compensen con la captación de nuevos clientes y los potenciales beneficios obtenidos.
- Consideración de que ser un pionero implica más riesgos que beneficios.
- La premisa de que, a diferencia de otros servicios, el éxito en la implantación de DNSSEC depende, no solo del propio despliegue, sino de que su adopción también se lleva a cabo por parte del resto de la comunidad.

Particularizando para España, se añade el hándicap de que el dominio ".es" no estuvo completamente operativo hasta finales del año 2014, cuatro años después de que se completase el despliegue de la zona raíz. Los datos proporcionados por "dominios.es" parecen indicar que las organizaciones no están todavía demandando el servicio DNSSEC a los agentes registradores.

Aunque la investigación de Dan Kaminsky en 2008 [Ref.- 16] reveló que el envenenamiento de caché podía provocar efectos nefastos si este tipo de vulnerabilidad conseguía explotarse sobre el servicio DNS, los casos documentados hasta ahora no han

tenido el suficiente impacto (principalmente porque muchas organizaciones prefieren no revelar los ataques de que han sido objeto) y porque, hasta el momento, no han supuesto amenazas globales a gran escala.

Sin embargo, dada la total dependencia de Internet (y de sus numerosos servicios y aplicaciones) en el servicio DNS, y a que la adopción de DNSSEC ha de planificarse cuidadosamente, si en algún momento se consiguiese explotar el envenenamiento de caché con suficiente repercusión, el tiempo de reacción de la mayor parte de organizaciones y servicios se dilataría irremisiblemente y significativamente.

Adicionalmente, una vez desplegada la infraestructura de DNSSEC, la misma puede ser aprovechada para incrementar la seguridad de otros servicios comunes, como navegación web (HTTPS) y correo electrónico a través de DANE.

Dado que, desde el punto de vista de las organizaciones que tienen sus dominios DNS gestionados por proveedores de servicios externos, la adopción de DNSSEC tiene un coste de implantación reducido y puede ser relativamente sencilla (existen en el mercado proveedores que lo ofrecen e incluso lo habilitan por defecto), parece tener sentido demandar la incorporación de DNSSEC a los servicios de los agentes registradores y operadores de zona. Respecto a las organizaciones que gestionan sus propios dominios DNS, y que poseen personal técnico capacitado para planificar el despliegue de DNSSEC y recursos materiales suficientes para acomodar los nuevos requerimientos, parece recomendable hacer un estudio y valorar los beneficios del protocolo DNSSEC.

En el estudio de ENISA descrito en el apartado "4.4. Costes de implantación y motivación" se constata que los costes asociados al despliegue de DNSSEC son muy dependientes del rol de los distintos agentes que forman parte del ecosistema del servicio DNSSEC y su nivel de implicación. Sin embargo, no se puede obviar el hecho de que este estudio se realizó en una fase muy incipiente del despliegue del protocolo. A medida que la tecnología avanza y los procedimientos se estandarizan, el coste de la adopción de DNSSEC se decrementa. Por ejemplo, con la puesta en marcha del proyecto OpenDNSSEC para automatizar el proceso de gestión y mantenimiento de las claves y el firmado de zonas, el coste del despliegue se reduciría al coste de configuración de dicha herramienta.

Dado que en la actualidad los avances en los procedimientos y en las herramientas resultantes del esfuerzo de las organizaciones pioneras en el despliegue de DNSSEC están a disposición de toda la comunidad, los costes de implantación han de resultar significativamente menores para aquellas organizaciones que estén interesadas en iniciar su despliegue de DNSSEC.

De cara a que los operadores de zona y los operadores de *resolvers* recursivos vean justificada su inversión en el servicio DNSSEC, resulta crucial que el mercado lo demande y se pueda obtener un beneficio, indirecto (a nivel de captación de clientes), o directo (por los posibles cargos asociados al servicio).

El análisis publicado por APNIC respecto a la reducida adopción de DNSSEC [Ref.- 55], expone como dos agentes registradores que se beneficiaron de una iniciativa a nivel de país (en Holanda y Suecia) consistente en recibir descuentos por parte del ccTLD para los dominios registrados con DNSSEC, solo soportan DNSSEC para los dominios ".nl" y ".se" respectivamente, es decir, para aquellos para los que se obtenía el descuento. Pese a que, una vez puestos en marcha los mecanismos asociados al servicio DNSSEC, como

la propagación de los registros DS, podrían haberlo ofrecido para cualquier otro dominio, los incentivos recibidos motivaban su aplicación únicamente a los dominios promocionados.

En resumen, debido a que para los usuarios finales y para los propietarios de dominios gestionados externamente, el coste de implantación es muy bajo y, sin embargo, el beneficio a nivel de confianza y seguridad ofrecido por DNSSEC es relevante, se debería demandar la utilización del servicio DNSSEC de manera más generalizada, para impulsar a los agentes implicados a ofrecerlo, tanto a agentes registradores, como a los operadores de zona y a los operadores de *resolvers* recursivos gestionados por proveedores de servicios.

Desde el punto de vista institucional, la adopción de DNSSEC podría verse impulsada si se llevasen a cabo tanto medidas de concienciación (a todos los niveles: usuario final, agentes registradores, proveedores de servicios y organizaciones, públicas y privadas) como medidas de incentivación, teniendo en mente que la seguridad ha de ser un compromiso de todos.

Con todo, si bien a nivel conceptual DNSSEC puede parecer complejo y requiere de conocimientos técnicos suficientes, a día de hoy el software, las herramientas, aplicaciones y soluciones que lo implementan tienen un nivel de madurez suficiente, y proporcionan capacidades para el despliegue y la gestión del dominio en producción que permiten automatizar gran parte de los procesos y simplificar significativamente su la implantación en el entorno.

# 6. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:


| Referencia | Título, autor, fecha y enlace web |
|---|---|
| [Ref.- 1] | "ARPANET". Wikipedia.<br>URL: https://es.wikipedia.org/wiki/ARPANET |
| [Ref.- 2] | "Dirección IP". Wikipedia.<br>URL: https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP |
| [Ref.- 3] | "RFC 606: Host Names On-line". IETF. December 1973.<br>URL: https://tools.ietf.org/html/rfc606 |
| [Ref.- 4] | "RFC 883: Domain Names: Implementation and Specification". IETF. November 1983.<br>URL: https://tools.ietf.org/html/rfc883 |
| [Ref.- 5] | "Guía de seguridad en servicios DNS". CERTSI - INCIBE (Instituto Nacional de Ciberseguridad de España). 9 de abril de 2014. URL: https://www.certsi.es/sites/default/files/contenidos/guias/doc/guia_de_seguridad_en_servicios_dns.pdf<br>URL: https://www.certsi.es/blog/guia-dns |
| [Ref.- 6] | "The Costs of DNSSEC Deployment". European Network and Information Security Agency. November 2009. URL: https://www.enisa.europa.eu/publications/archive/dnsseccosts/<br>URL: https://www.enisa.europa.eu/publications/archive/dnsseccosts/at_download/execSummary<br>URL: https://www.enisa.europa.eu/publications/archive/dnsseccosts/at_download/fullReport |
| [Ref.- 7] | "Root DNSSEC". ICANN.<br>URL: http://www.root-dnssec.org/ |
| [Ref.- 8] | "(DNS) Root Zone Management". IANA.<br>URL: https://www.iana.org/domains/root |
| [Ref.- 9] | "RFC 2535: Domain Name System Security Extensions". IETF. March 1999.<br>URL: https://tools.ietf.org/html/rfc2535<br>URL: https://tools.ietf.org/html/rfc2065 |
| [Ref.- 10] | "DNS Threat Survey 2017". Efficient IP. June 2017.<br>URL: http://www.efficientip.com/wp-content/uploads/PR_DNS_Threat_Survey_2017.pdf<br>URL: http://www.efficientip.com/resources/white-paper-dns-security-survey-2017/ |
| [Ref.- 11] | "MYNIC Official Announcement". MYNIC. October 2013.<br>URL: https://www.mynic.my/en/news.php?id=162 |
| [Ref.- 12] | "DNS Attack Writer a Victim of His Own Creation". PCWorld. July 2008.<br>URL: https://www.pcworld.com/article/149126/dns_attack_writer.html |
| [Ref.- 13] | "Dominios.es". Red.es (Ministerio de Economía y Empresa).<br>URL: http://www.dominios.es/dominios/ |
| [Ref.- 14] | "Manual de Usuario Final" (SGND 7.12, Versión 2.18). Red.es. Septiembre 2017.<br>URL: http://www.dominios.es/dominios/sites/dominios/files/Manual_TPV_Santander.pdf |
| [Ref.- 15] | "Estadísticas: Los dominios '.es' alcanzaron 1.907.730 registros en marzo". dominios.es. 25 abril 2018. URL: http://www.dominios.es/dominios/es/actualidad-y-noticias/comunicados/estad%C3%ADsticas-los-dominios-%E2%80%9Ces%E2%80%9D-alcanzaron-1907730-registros-en |
| [Ref.- 16] | "CVE-2008-1447: DNS Cache Poisoning Issue ("Kaminsky bug")". ISC Knowledge Base. July 2008. URL: https://kb.isc.org/article/AA-00924<br>URL: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html<br>URL: https://www.kb.cert.org/vuls/id/800113 |
| [Ref.- 17] | "DNSSEC Deployment Maps". Internet Society.<br>URL: https://www.internetsociety.org/deploy360/dnssec/maps/ |
| [Ref.- 18] | "Overview of DNSSEC deployment worldwide". EURid. October 2010.<br>URL: https://eurid.eu/media/filer_public/b0/bd/b0bdb289-a629-4d67-a256-6491b70539c0/insights_dnssec1.pdf |
| [Ref.- 19] | "How DNSSEC Works". Cloudflare.<br>URL: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/ |

| Referencia | Título, autor, fecha y enlace web |
|---|---|
| [Ref.- 20] | "DNS and BIND". 5th Edition. Paul Albitz, Cricket Liu. O'Reilly. February 2009. URL: http://shop.oreilly.com/product/9780596100575.do |
| [Ref.- 21] | "DNS Server Types". Cloudflare. URL: https://www.cloudflare.com/learning/dns/dns-server-types/ |
| [Ref.- 22] | "RFC 7129: Authenticated Denial of Existence in the DNS". IETF. February 2014. URL: https://tools.ietf.org/html/rfc7129 |
| [Ref.- 23] | "DNSSEC Complexities and Considerations". Cloudflare. URL: https://www.cloudflare.com/dns/dnssec/dnssec-complexities-and-considerations/ |
| [Ref.- 24] | "NSEC5: Provably Preventing DNSSEC Zone Enumeration". IACR. July 2014. URL: https://eprint.iacr.org/2014/582 URL: https://eprint.iacr.org/2014/582.pdf |
| [Ref.- 25] | "BGP Hijack of Amazon DNS to Steal Crypto Currency". Dyn. April 25, 2018. URL: https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/ |
| [Ref.- 26] | "BGP leaks and cryptocurrencies". Cloudflare. April 24, 2018. URL: https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/ URL: https://arstechnica.com/information-technology/2018/04/suspicious-event-hijacks-amazon-traffic-for-2-hours-steals-cryptocurrency/ |
| [Ref.- 27] | "A Technical Deep Dive: Securing the Automation of ACME DNS Challenge Validation". EFF. February 2018. URL: https://www.eff.org/deeplinks/2018/02/technical-deep-dive-securing-automation-acme-dns-challenge-validation URL: http://letsencrypt.readthedocs.io/en/latest/challenges.html |
| [Ref.- 28] | "RFC 4033: DNS Security Introduction and Requirements". IETF. March 2005. URL: https://tools.ietf.org/html/rfc4033 "RFC 4034: Resource Records for the DNS Security Extensions". URL: https://tools.ietf.org/html/rfc4034 "RFC 4035: Protocol Modifications for the DNS Security Extensions". URL: https://tools.ietf.org/html/rfc4035 |
| [Ref.- 29] | "The DNSSEC Root Signing Ceremony". Cloudflare. URL: https://www.cloudflare.com/dns/dnssec/root-signing-ceremony/ URL: https://www.iana.org/dnssec/ceremonies |
| [Ref.- 30] | "Estimating IPv6 & DNSSEC External Service Deployment Status". NIST (The United States National Institute of Standards and Technology). URL: http://fedv6-deployment.antd.nist.gov |
| [Ref.- 31] | "EURid in 2017". EURid. 2017. URL: https://eurid.eu/media/filer_public/b0/d7/b0d78531-a9ff-416f-934b-713b6bdeedf5/annual_report_2017.pdf |
| [Ref.- 32] | "rick.eng.br". Rick Lamb. URL: http://rick.eng.br URL: http://rick.eng.br/mon/ |
| [Ref.- 33] | "RFC 3225: Indicating Resolver Support of DNSSEC". IETF. December 2001. URL: https://tools.ietf.org/html/rfc3225 |
| [Ref.- 34] | "Declaración de Políticas y Procedimientos para DNSSEC en la zona ".ES"". Dominios.es. URL: http://www.dominios.es/dominios/sites/dominios/files/files/Declaraci%C3%B3n%20de%20Pol%C3%ADticas%20y%20Procedimientos%20para%20DNSSEC%20en%20la%20zona%20%20ES.pdf |
| [Ref.- 35] | "Growth .se". IIS. URL: https://www.iis.se/english/domains/domain-statistics/growth/?chart=active |
| [Ref.- 36] | "DNSSEC secured domain names". SIDN Labs. URL: https://stats.sidnlabs.nl/#/dnssec |
| [Ref.- 37] | "Measuring DNSSEC Configuration of Upstream Resolvers with RIPE Atlas". SIDN Labs. May 2016. URL: https://www.sidnlabs.nl/downloads/presentations/RIPE72_Measure_DNSSEC_with_Atlas.pdf |
| [Ref.- 38] | "Estatísticas". dominios.pt. URL: https://www.dns.pt/pt/estatisticas/?tipo=0&ordem=9&ano=2018&graph=0&subm=Filtrar |
| [Ref.- 39] | "YADIFA. A True Name Server Alternative". CloudFlare. URL: https://www.yadifa.eu |

| Referencia | Título, autor, fecha y enlace web |
|---|---|
| [Ref.- 40] | "Registrars that support end user DNSSEC management, including entry of DS records". ICANN. April 2017. URL: https://www.icann.org/resources/pages/deployment-2012-02-25-en |
| [Ref.- 41] | "BIND". ISC. URL: https://www.isc.org/downloads/bind/ |
| [Ref.- 42] | "Unbound". NLNETLABS. URL: https://www.nlnetlabs.nl/projects/unbound/about/ |
| [Ref.- 43] | "Knot DNS". CZ.NIC. URL: www.knot-dns.cz |
| [Ref.- 44] | "Google Public DNS". Google. URL: https://developers.google.com/speed/public-dns/docs/using |
| [Ref.- 45] | "Announcing 1.1.1.1": CloudFlare. URL: https://blog.cloudflare.com/announcing-1111/ |
| [Ref.- 46] | "NSD". NLnet Labs. URL: https://www.nlnetlabs.nl/projects/nsd/about/ |
| [Ref.- 47] | "DNSSEC Information". IANA. URL: https://www.iana.org/dnssec |
| [Ref.- 48] | "TLD DNSSEC Report ". ICANN Research. URL: http://stats.research.icann.org/dns/tld_report/ |
| [Ref.- 49] | "SecSpider". Verisign. URL: http://secspider.verisignlabs.com/ |
| [Ref.- 50] | "SecSpider Usage". Verisign. URL: http://secspider.verisignlabs.com/docs.html#usage |
| [Ref.- 51] | "DNSSEC Validation Rate by country". APNIC Labs. URL: https://stats.labs.apnic.net/dnssec |
| [Ref.- 52] | "Domain Count Statistics for TLDs". Domain Tools. URL: http://research.domaintools.com/statistics/tld-counts/ |
| [Ref.- 53] | "DNSSEC ScoreBoard". Verisign Labs. URL: https://scoreboard.verisignlabs.com/ |
| [Ref.- 54] | "DNSSEC Timeline". Internet Society. URL: https://wiki.tools.isoc.org/DNSSEC_History_Project/Timeline |
| [Ref.- 55] | "Why DNSSEC deployment remains so low". APNIC Blog. December 2017. URL: https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/ |
| [Ref.- 56] | "RFC 4641: DNSSEC Operational Practices.". IETF. URL: https://tools.ietf.org/html/rfc6781 |
| [Ref.- 57] | "RFC 7929: DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP". IETF. August 2016. URL: https://tools.ietf.org/html/rfc7929 |
| [Ref.- 58] | "SecSpider Stats". Verisign. URL: http://secspider.verisignlabs.com/stats.html |
| [Ref.- 59] | "What is ICANN, and How is it Related to Registries and Registrars?". DomainTools. URL: https://www.domaintools.com/support/what-is-icann-and-how-is-it-related-to-registries-and-registrars |
| [Ref.- 60] | "OpenDNSSEC". URL: http://www.opendnssec.org |
| [Ref.- 61] | "Major DNSSEC Outages and Validation Failures". Ianix. URL: https://ianix.com/pub/dnssec-outages.html |
| [Ref.- 62] | "DNSSEC Deployment Study". InterConnect Comunications. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0015/19131/domain-name-security.pdf |
| [Ref.- 63] | "RFC 6698: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA". IETF. August 2012. URL: https://tools.ietf.org/html/rfc6698 |
| [Ref.- 64] | "RFC 7671: The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance". IETF. October 2015. URL: https://tools.ietf.org/html/rfc7671 |

| Referencia | Título, autor, fecha y enlace web |
|---|---|
| [Ref.- 65] | "RFC 8162: Using Secure DNS to Associate Certificates with Domain Names for S/MIME". IETF. May 2017. URL: https://tools.ietf.org/html/rfc8162 |
| [Ref.- 66] | "RFC 7672: SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)". IETF. October 2015. URL: https://tools.ietf.org/html/rfc7672 |
| [Ref.- 67] | "Domínios com DNSSEC - 2018". Domínios.pt". 2018. URL: https://www.dns.pt/pt/estatisticas/?tipo=0&ordem=9&ano=2018&graph=0&subm=Filtrar |
| [Ref.- 68] | "Trece Agentes Registradores ya han implantado el protocolo de seguridad DNSSEC para dominios ".es"". Actualidad y noticias de dominios.es. Octubre 2015. URL: http://www.dominios.es/dominios/es/actualidad-y-noticias/comunicados/trece-agentes-registradores-ya-han-implantado-el-protocolo-de |
| [Ref.- 69] | "RFC 2845: Secret Key Transaction Authentication for DNS (TSIG)". IETF. May 2000. URL: https://tools.ietf.org/html/rfc2845 "RFC 3645 - Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)". IETF. October 2003. URL: https://tools.ietf.org/html/rfc3645 |
| [Ref.- 70] | "dnssec-maps: An announce-only list for distribution of DNSSEC deployment maps ". Internet Society. URL: https://elists.isoc.org/mailman/listinfo/dnssec-maps "The dnssec-maps Archives ". URL: https://elists.isoc.org/pipermail/dnssec-maps/ |

# 7. GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

Dado la amplitud de siglas y términos empleados habrá que añadir un glosario que los abarque todos, y pueda servir de ayuda al lector.




INSTITUTO NACIONAL DE CIBERSEGURIDAD