Guía de implementación de las DNSSEC para los ccTLD

Oficina del Director de Tecnologías de la ICANN

Yazid Akanho y Paul Muchene
OCTO-029
Noviembre de 2021

ÍNDICE

1 INTRODUCCIÓN 4

1.1 Destinatarios de este documento 4

2 LAS DNSSEC Y SU VALOR PARA EL DNS 5

3 REQUISITOS PREVIOS Y REQUERIMIENTOS PARA LA IMPLEMENTACIÓN DE LAS DNSSEC 5

3.1 Documentación del sistema existente 5
3.2 Auditoría de la infraestructura existente 6
3.3 Redactar una política y declaraciones de prácticas de DNSSEC 7
3.3.1 ¿Qué es una Política de DNSSEC y una Declaración de Prácticas de DNSSEC? 7
3.3.2 Cómo redactar una DP y una DPS 8
3.3.3 Selección de algoritmos criptográficos para una zona 10
3.3.4 Denegación de existencia: NSEC o NSEC3 11
3.4 Participación de los registradores 12

4 CRONOGRAMA 13

5 ESCENARIOS DE IMPLEMENTACIÓN DE LAS DNSSEC 14

5.1 Servidor primario para firmas en línea (primario oculto) 14
5.2 Firma en línea “bump-in-the-wire” 15

6 FIRMA DE UN TLD 16

7 TRASPASO DE CLAVES Y ALGORITMOS 17

7.1 Traspaso de la ZSK 18
7.2 Traspaso de la KSK 19

8 OTRAS CONSIDERACIONES PARA LAS ZONAS FIRMADAS 19

9 ANULAR LA FIRMA DEL TLD SI ES NECESARIO 21

10 HERRAMIENTAS ÚTILES PARA IMPLEMENTAR LAS DNSSEC 21

10.1 Depurador para DNSSEC de Verisign 21
10.2 DNSVIZ 22

11 CONCLUSIÓN 23

A EJEMPLO DE POLÍTICAS DE DNSSEC Y DECLARACIONES DE PRÁCTICAS DE DNSSEC 24

B EJEMPLO DE ZONA SIN FIRMAR Y FIRMADA 24

B.1 Zona sin firmar 24
B.2 Zona firmada 25

C LISTA DE VERIFICACIÓN PARA LA IMPLEMENTACIÓN DE LAS DNSSEC 26

C.1 Inicio y preparación 26
C.2 Implementación y monitoreo 27

D MÁS INFORMACIÓN 28

Este documento forma parte de la serie de documentos de la Oficina del Director de Tecnologías (OCTO) de la ICANN. Consulte la página de publicaciones de la OCTO para ver la lista de los documentos que integran la serie. Si tiene preguntas o sugerencias sobre cualquiera de estos documentos, envíelas a octo@icann.org.

Este documento respalda el objetivo estratégico de la ICANN de mejorar la responsabilidad común de preservar la seguridad y estabilidad del Sistema de Nombres de Dominio (DNS) mediante el fortalecimiento de la coordinación de este sistema en asociación con partes interesadas relevantes. Forma parte del objetivo estratégico de la ICANN de fortalecer la seguridad del DNS y del Sistema de Servidores Raíz (RSS) del DNS.

1 Introducción

En los últimos años, la seguridad se ha convertido en un tema cada vez más importante en Internet. En lo que respecta al Sistema de Nombres de Dominio (DNS), se han propuesto y desarrollado varios protocolos de seguridad a lo largo de los años, y las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) son uno de los protocolos más significativos. Las DNSSEC ayudan a asegurar las respuestas del DNS agregando la autenticación del origen de los datos y la protección de la integridad de los datos.

La zona raíz del DNS gestionada por la ICANN fue firmada por primera vez con las DNSSEC en julio de 2010. En el momento de la publicación de esta guía, todos los dominios genéricos de alto nivel (gTLD) estarán firmados con las DNSSEC, en parte debido a las obligaciones contractuales con la ICANN. Por otro lado, solo se han firmado alrededor del 60 % de los dominios de alto nivel de código de país (ccTLD). Una de las razones que podría explicar esta tendencia a nivel de ccTLD es la falta de visibilidad de los administradores de ccTLD en el proceso de asegurar sus zonas con las DNSSEC.

Por lo tanto, la Oficina del Director de Tecnologías (OCTO) de la ICANN ha publicado esta guía para ayudar a los operadores de registros de ccTLD a seguir el proceso que pueda ayudarles a firmar sus zonas con las DNSSEC. No abarca el segundo aspecto de las DNSSEC, que es la validación que se produce principalmente en los resolutores recursivos del DNS, normalmente ubicados en proveedores de servicios de Internet (ISP), en grandes operadores de nubes públicas o en redes corporativas.

1.1 Destinatarios de este documento

Esta guía está destinada principalmente a proporcionar a los administradores de registros de ccTLD, al personal, a las partes interesadas, en particular a los registradores, a los solicitantes de registro, y a cualquier otra persona, una descripción general de las DNSSEC y de cómo pueden ser implementadas por un registro en la firma de zonas. Este documento no entra en detalles de configuración técnica, sino que sirve como guía para una comprensión básica del protocolo de las DNSSEC, los requisitos previos y las consideraciones de implementación en la firma de zonas de un ccTLD.

Incluso si ya está operando un TLD firmado con DNSSEC, este documento podría ayudarlo a identificar puntos a mejorar, como las mejores prácticas actuales en términos de algoritmos o la documentación adecuada del servicio del DNS en general. Si usted es un operador de ccTLD, o administra zonas bajo un ccTLD firmado, esta guía puede ayudarlo en sus primeros pasos. A pesar de que todos los operadores de gTLD ya han firmado sus zonas, también podrían obtener información sobre las mejores prácticas operativas de las DNSSEC que se describen en este documento y utilizarlas como base para generar conciencia sobre las DNSSEC entre sus registradores y registratarios.

Existe una gran cantidad de documentos sobre los aspectos teóricos, técnicos y operativos de las DNSSEC, y esta guía cita a varios de estos documentos como referencia. Por lo tanto, se invita a los lectores a consultar estos documentos citados si desean profundizar en su conocimiento o comprensión de algún aspecto relacionado con las DNSSEC.

2 Las DNSSEC y su valor para el DNS

El Sistema de Nombres de Dominio (DNS) es un sistema de nombres jerárquico, distribuido y descentralizado para Internet. Al igual que una guía telefónica que vincula nombres a números de teléfono, el DNS ayuda a convertir la información de los nombres de dominio en direcciones IP y viceversa. El DNS se considera un servicio fundamental en Internet, pero no se diseñó originalmente con fuertes mecanismos de seguridad para proporcionar integridad y autenticidad a sus datos. Con el transcurso de los años, se ha descubierto una serie de vulnerabilidades que amenazan la confiabilidad y credibilidad del DNS, y las DNSSEC ayudan a abordar algunas de ellas.

Las DNSSEC se definen y especifican principalmente en tres documentos de estándares de Internet: RFC 4033, *Introducción y requisitos de seguridad del DNS*; RFC 4034, *Registros de recursos para las Extensiones de Seguridad del DNS*; y RFC 4035, *Modificaciones de protocolo para las Extensiones de Seguridad del DNS*. Las DNSSEC utilizan la criptografía de clave pública (la generación de pares de claves públicas y privadas) para agregar al DNS capacidades de autenticación del origen de los datos, la integridad de los datos, la verificación y la denegación de existencia autenticada. En concreto, agrega firmas digitales y un nuevo conjunto de tipos de registros de recursos y bits de encabezados de mensajes (etiquetas) al DNS, que pueden utilizarse para verificar las respuestas del DNS de una zona firmada. Cabe destacar que las DNSSEC no cifran ningún dato de los mensajes del DNS y, por tanto, no proporcionan confidencialidad.

Una vez que un dominio está firmado con las DNSSEC, las firmas digitales son generadas por el administrador de la zona utilizando una clave privada y se publican como un registro de Firma Digital de Registro de Recursos (RRSIG) en el archivo de zona como parte de los datos de zona del dominio. Cuando un resolutor recursivo de seguridad, también conocido como resolutor de validación, envía una consulta del DNS a un servidor autoritativo del dominio firmado, la respuesta del DNS contiene el registro de recursos en texto claro o en un formato no cifrado y su firma digital asociada. El resolutor utiliza entonces la firma digital que ha recibido para validar esta respuesta del DNS. Para ello, el resolutor de validación también solicita otra información relacionada con las DNSSEC, como la clave pública que se almacena en el registro DNSKEY y que el administrador del dominio publica en los datos de zona.

3 Requisitos previos y requerimientos para la implementación de las DNSSEC

3.1 Documentación del sistema existente

Debido a la función fundamental que desempeña el DNS en Internet y a la necesidad de evitar la interrupción del servicio en cualquier circunstancia, es importante mantener una documentación actualizada que describa la infraestructura, las operaciones y los procesos del DNS. Por otro lado, las DNSSEC agregan un nivel determinado de complejidad adicional a la infraestructura y operaciones existentes del DNS. Por lo tanto, mantener la documentación actualizada es crucial para garantizar que se disponga de un panorama claro del sistema existente como referencia. Esto también permite la continuidad operativa en caso de cambios en el personal o actualización de la infraestructura.

Recomendamos que la documentación resuma dos aspectos principales: las políticas de gobernanza del ccTLD y los aspectos operativos y técnicos del servicio.

Asimismo, es aconsejable que el documento contenga la máxima información posible, y que omita cualquier dato sensible o confidencial, como nombres de usuario y contraseñas, que puedan utilizarse para realizar ataques contra el registro.

Los aspectos de gobernanza del documento podrían abarcar los siguientes temas:

- Descripción general y estructura del ccTLD
- Modelo(s) de registración: 3R (registro, registrador y registratario), 2R (solo registro y registratario) u otros modelos
- Contactos técnicos y administrativos del registro
- Recursos humanos, funciones, responsabilidades y contactos de las personas que participan en el proceso de toma de decisiones técnicas del registro
- Una lista de registradores con sus respectivos datos de contacto

Los aspectos técnicos y operativos del documento podrían abarcar los siguientes temas:

- Número de servidores de nombres (NS) autoritativos primarios y secundarios con sus respectivas direcciones IP, información de contacto del TLD (teléfono y direcciones de correo electrónico), protocolos en uso entre el registro y los registradores, como el Protocolo de Aprovisionamiento Extensible (EPP), el software y el hardware que implementa las funciones del registro, incluida la base de datos del registro, el Protocolo de Acceso a los Datos de Registración (RDAP) y/o los servidores de WHOIS (entre otros elementos de información técnica)
- El acceso de los usuarios y el inventario de privilegios solo deben estar disponibles para un número limitado de personas autorizadas
- Copias de seguridad y procedimientos de restauración
- Seguridad: acceso físico, gestión de registros, controles de acceso, gestión de contraseñas, cortafuegos, integridad de los archivos de zona y seguridad de la transferencia de zonas (por nombrar algunos aspectos)
- Sistemas de monitoreo: hardware, software, sincronización de zonas (entre NS)
- Estrategia de mantenimiento
- Plan de continuidad de operaciones y de recuperación ante desastres

3.2 Auditoría de la infraestructura existente

Como se ha señalado anteriormente, la implementación de las DNSSEC agrega un nivel de complejidad a la infraestructura y las operaciones existentes del DNS. Por lo tanto, una práctica recomendada y segura sería realizar una auditoría de la infraestructura, las operaciones y los procesos actuales del sistema, ya sea a través de una parte externa o interna que posea las capacidades y la autonomía necesarias para identificar y compartir sus conclusiones y cualquier carencia existente. Es esencial solucionar cualquier deficiencia del sistema actual antes de la firma de la zona. Al hacerlo, se reduce el riesgo de que las cosas se vuelvan inmanejables tras la implementación de las DNSSEC.

3.3 Redactar una política y declaraciones de prácticas de DNSSEC

3.3.1 ¿Qué es una Política de DNSSEC y una Declaración de Prácticas de DNSSEC?

Hay varias consideraciones que hay que tener en cuenta y parámetros que hay que definir a la hora de firmar un dominio, por ejemplo, los algoritmos de firma de las DNSSEC, el tamaño de las claves, el periodo de validez de la firma y la frecuencia de actualización de la firma. En el caso de una zona con muchas delegaciones, una práctica recomendada es documentar completamente y mantener actualizados los conjuntos de parámetros aplicables a la zona y hacerlos públicos. Por lo tanto, hay que tener en cuenta dos conceptos:

- La **Política de DNSSEC** (DP): establece los requisitos y normas de seguridad que deben aplicarse a una zona firmada con las DNSSEC. La DP constituye una base para una auditoría, una acreditación o una evaluación de una entidad, por ejemplo, un registro. Cada entidad puede ser evaluada con respecto a una o varias DP que afirme implementar. En resumen, la DP establece lo que debe hacerse.
- La **Declaración de Prácticas de DNSSEC** (DPS): se trata de un documento de divulgación de prácticas operativas que puede ser un documento respaldatorio y complementario de la Política de DNSSEC (si la hubiere). Establece las generalidades de cómo un operador de zona y sus socios en la gestión de una zona, si los hay, implementan procedimientos y controles para cumplir los requisitos de la DP aplicable. A diferencia de una DP, la DPS establece lo que se hace realmente.

Una DP proporciona principios generales, mientras que una DPS ofrece una descripción de los procedimientos y controles, por lo que es más detallada que una DP. Por otra parte, la política suele ser redactada por una autoridad política (administrador de TLD o autoridad reguladora) y puede ser aplicable a una o más zonas en la jerarquía del DNS, mientras que una declaración de prácticas específica para una sola zona es redactada por el operador de la zona, que describe cómo cumple los requisitos de una política concreta o de un conjunto de políticas.

Por ejemplo, en el contexto en el que tanto el contacto administrativo como el contacto técnico de un ccTLD son entidades diferentes, el contacto administrativo podría publicar una política en la que se describan las normas y los requisitos a seguir, al tiempo que se exige al contacto técnico que publique una declaración de prácticas en la que se detalle cómo se cumplirán dichas normas y requisitos.

Como alternativa, un operador o administrador de zona que no se rija por ninguna política externa puede publicar una DPS.

La publicación de una DPS es más relevante para las entidades que operan una zona que contiene un número significativo de delegaciones, como un TLD. La publicación de una DPS ayuda a proporcionar un nivel de transparencia que aumenta la confianza de la comunidad en las operaciones del TLD pero, como se ha señalado anteriormente, una DPS no debe contener información operativa sensible.

El documento RFC 6841, *Un marco para las políticas de DNSSEC y las declaraciones de prácticas de las DNSSEC*, es un documento que explica en detalle una lista exhaustiva de temas que un operador de TLD debe considerar al definir una DP y una DPS, respectivamente.

3.3.2 Cómo redactar una DP y una DPS

La redacción de una DPS es un paso importante en el camino hacia la firma de un ccTLD. La DPS puede ser breve y sencilla o extensa y compleja, pero debe ayudar a las personas a entender el marco de operaciones de las DNSSEC y cómo pueden confiar en el proceso de firma del ccTLD.

La siguiente tabla es un resumen del conjunto de disposiciones que comprenden ocho componentes, indicados en el documento RFC 6841, que podrían tenerse en cuenta al redactar una DP o una DPS. No es obligatorio implementar todos los componentes del documento RFC 6841 y, por lo tanto, tiene la libertad de elegir aquellos (sub)componentes que se adapten a sus necesidades.

Título	Descripción	Subcomponentes
Introducción	Identifica e introduce el conjunto de disposiciones, e indica los tipos de entidades y aplicaciones a los que se dirige la política o la declaración de prácticas.	● Reseña ● Nombre e identificación del documento ● Comunidad y aplicabilidad ● Administración de la especificación
Publicación y repositorios	Describe los requisitos para que una entidad publique la información relativa a sus prácticas, las claves públicas y el estado actual de dichas claves, junto con los detalles relativos a los repositorios en los que se conserva la información.	● Repositorios ● Publicación de claves públicas
Requisitos operativos	Describe los requisitos operativos al operar una zona firmada por las DNSSEC.	● Significado de los nombres de dominio ● Identificación y autenticación de un administrador de zona secundaria ● Registración de registros de recursos de DS ● Métodos para demostrar la posesión y propiedad de una clave privada ● Eliminación de registros de recursos de DS

Controles de las instalaciones, la gestión y el funcionamiento	Describe los controles de seguridad no técnicos, es decir, físicos, de procedimiento y de personal para realizar de forma segura las funciones relacionadas con las DNSSEC. Estos controles incluyen el acceso físico, la gestión de claves, la recuperación ante desastres, las auditorías y el almacenamiento en archivo. Estos controles de seguridad no técnicos son fundamentales para confiar en las firmas generadas por las DNSSEC.	● Controles físicos ● Controles de procedimiento ● Controles de personal ● Procedimientos de registro de auditorías ● Compromiso y recuperación ante desastres ● Cese de la entidad
Controles técnicos de seguridad	Define las medidas de seguridad adoptadas para gestionar las claves criptográficas y los datos de activación, por ejemplo, números de PIN, contraseñas o participaciones en claves mantenidas manualmente, relevantes para las operaciones de las DNSSEC.	● Generación e instalación de pares de claves ● Protección de la clave privada y controles de ingeniería del módulo criptográfico ● Datos de activación
Firma de zonas	Cubre todos los aspectos de la firma de zonas, incluida la especificación criptográfica que rodea a las claves de firma, el esquema de firma, la metodología para el traspaso de claves y la firma de zona. Las zonas secundarias y otros actores afines pueden depender de la información de esta sección para entender los datos esperados en la zona firmada y determinar su propio comportamiento.	● Longitudes, tipos y algoritmos de las claves ● Denegación de existencia autenticada ● Formato de la firma ● Traspaso de clave ● Duración de la firma y frecuencia para volver a firmar
Auditoría de cumplimiento	Describe cómo el operador de zona y, posiblemente, otras entidades implicadas deben realizar las auditorías.	● La frecuencia de una auditoría de cumplimiento de la entidad ● La identidad/cualificación del auditor ● Temas que abarca la auditoría ● Acciones posteriores a la auditoría
Asuntos jurídicos	Indica bajo qué jurisdicción se opera el registro y proporciona referencias	● Mención de la jurisdicción aplicable

	a cualquier acuerdo asociado que esté en vigencia. La sección de Asuntos Jurídicos puede informar sobre cualquier implicación identificada en la protección de la información privada de identificación personal.	• Obligaciones contractuales y cumplimiento de leyes y normativas nacionales, transnacionales o internacionales • Protección de datos y tratamiento de la información de identificación personal

Se pueden agregar otros componentes en este marco para abordar las necesidades específicas del ccTLD. En el Anexo A de esta guía, se incluyen ejemplos de declaraciones de prácticas de DNSSEC.

3.3.3 Selección de algoritmos criptográficos para una zona

El campo de la criptografía evoluciona continuamente. Los algoritmos más nuevos sustituyen a los existentes cuando se descubre que son menos seguros de lo que se creía. Por lo tanto, los requisitos de implementación de los algoritmos y las directrices de uso se actualizan de forma periódica para reflejar las nuevas realidades.

La implementación de las DNSSEC requiere la elección de un algoritmo criptográfico adecuado. Al momento de la publicación de esta guía, el documento RFC 8624, *Requisitos para la implementación de algoritmos y guía de uso para las DNSSEC* proporciona tanto directrices de implementación de algoritmos como requisitos de parámetros de firma pertinentes para las DNSSEC.

La siguiente tabla incluye una lista (no exhaustiva) de algunas recomendaciones extraídas del documento RFC 8624. Es probable que los operadores individuales tengan requisitos específicos y deseen realizar las adaptaciones correspondientes.

Elemento	**Recomendación**
Algoritmo DNSKEY	El **algoritmo 13 (ECDSAP256SHA256)** proporciona solidez criptográfica y actualmente se recomienda su uso en las nuevas implementaciones de las DNSSEC debido a sus claves más cortas y al tamaño de la firma, lo que da lugar a paquetes del DNS más pequeños. Sin embargo, el **algoritmo 8 (RSASHA256)** también se puede utilizar porque está ampliamente implementado y ha sido el algoritmo predeterminado durante varios años debido a su solidez criptográfica.

Algoritmos del firmante de la delegación (DS)	SHA-256 es ampliamente utilizado y es un algoritmo de autenticación (hash) sólido y, por lo tanto, se recomienda para las implementaciones nuevas y existentes para el DS.
Algoritmo de seguridad de DNSSEC (compuesto por el algoritmo criptográfico y el algoritmo de autenticación o hash)	La recomendación actual es el algoritmo 13 (ECDSAP256SHA256). En caso contrario, también podría utilizarse el algoritmo 8 (RSASHA256).
Tamaño de la clave para la firma de la zona (ZSK) y de la clave para la firma de la llave (KSK)	El algoritmo 13 (ECDSAP256SHA256) siempre generará claves de 256 bits. El tamaño de la clave del algoritmo 8 (RSASHA256) puede establecerse entre 2048 y 4096 bits.
Periodo de efectividad de la ZSK y la KSK	No existe una forma correcta de estimar las necesidades individuales, dado que los operadores ajustan los periodos de efectividad de las claves en función de sus experiencias previas. Varios operadores han utilizado una ZSK de uno a tres meses y una KSK de uno a cinco años antes de realizar un traspaso.
Almacenamiento de claves privadas	Máquinas fuera de línea, no conectadas a la red y físicamente seguras, como los módulos de seguridad de hardware (HSM).

Nota: las claves más grandes aumentarán el tamaño de los registros de RRSIG y DNSKEY y, por lo tanto, aumentarán la posibilidad de sobrecarga de paquetes UDP del DNS. Además, el tiempo que se tarda en validar y crear firmas de registros de recursos (RRSIG) aumenta con claves más grandes, por lo que hay que evitar aumentar innecesariamente el tamaño de las claves.

3.3.4 Denegación de existencia: NSEC o NSEC3

La denegación de existencia o prueba de que algo no existe es un mecanismo que informa a un resolutor que un determinado nombre de dominio no existe (NXDOMAIN). A la inversa, un nombre de dominio existe pero no tiene el registro de recursos específico (NODATA) que se solicita. La denegación de existencia autenticada utiliza la criptografía para firmar una respuesta negativa. En las DNSSEC, esto se logra mediante el uso de NSEC (Next Secure) o NSEC3 (Next Secure v3), respectivamente.

NSEC se utiliza para describir un intervalo entre nombres. Indica indirectamente a un resolutor qué nombres no existen en una zona proporcionando en orden canónico el nombre anterior y el nombre posterior. Este mecanismo implementado en NSEC constituye la base de la denegación de existencia autenticada en las DNSSEC y se enfrenta a dos problemas:

- Los registros NSEC son susceptibles de ataques de enumeración de zona (zone walking) y esta debilidad puede permitir a un atacante recorrer todos los nombres de

una zona. Por ende, es posible reconstruir toda la zona y, por lo tanto, derrotar cualquier intento de bloquear administrativamente las transferencias de zona.

- El segundo problema para NSEC en una zona centrada en la delegación, como un TLD, es que cada nombre de esa zona recibe un registro NSEC y su RRSIG asociada. Una vez que una zona está firmada, esto tiene un impacto adverso y conlleva un aumento de su tamaño. Los gastos generales generados por este aumento podrían tener un impacto negativo en el rendimiento de los servidores autoritativos del DNS, como la limitación de los recursos de almacenamiento de hardware o la prolongación de la duración para realizar las transferencias de zona.

NSEC3, por el contrario, mitiga el problema de los ataques de enumeración de zona (zone walking) en NSEC, mediante el uso del algoritmo de autenticación (hash) en los nombres de dominio con la posibilidad de consolidarlos utilizando una función de Salt. Además, gracias a una función específica denominada "opt-out" (no participar), los nombres de dominio no firmados delegados en una zona (delegaciones inseguras) no requieren un registro de NSEC3. Esto implica que cuando se activa la función “no participar” (opt-out) en una zona de TLD, NSEC3 no puede probar o negar la existencia de los dominios no firmados registrados en ese TLD. No obstante, un escollo que presenta NSEC3 es que las respuestas del DNS son mayores que las de NSEC.

No hay una única respuesta adecuada a la hora de elegir entre NSEC y NSEC3. Si se prefiere utilizar NSEC3 para evitar la enumeración de zona (zone walking), generalmente se recomienda implementar NSEC3 sin iteraciones adicionales y con el valor de Salt vacío. Sin embargo, para las zonas más pequeñas, no se recomienda el uso de registros de NSEC3 con la función “no participar” (opt-out). Para zonas muy grandes y escasamente firmadas, en las que la mayoría de los registros son delegaciones inseguras, podría utilizarse la función “no participar” (opt-out) de NSEC3. Aparte de estas consideraciones mencionadas, la solución de problemas en NSEC es más fácil que en NSEC3.

3.4 Participación de los registradores

Es muy recomendable la participación de los registradores en las etapas preliminares de la firma de un ccTLD. No solo porque son el intermediario entre el registro y los registratarios, sino porque la implementación de las DNSSEC a nivel de ccTLD es el punto de partida para asegurar el espacio de nombres de ese ccTLD. Una vez firmado el ccTLD, los titulares de dominios de segundo nivel pueden empezar a asegurar sus respectivos dominios. Esto requerirá que los registradores sean capaces de recopilar y enviar un nuevo tipo de registro de esos titulares de dominios de segundo nivel o posteriores al registro. Este nuevo tipo de registro se denomina Firmante de Delegación (DS).

En términos técnicos, el DS es un hash de la clave para la firma de la llave de la zona raíz (KSK) y ayuda a establecer la cadena de confianza entre una zona principal y una zona secundaria en el espacio de nombres del DNS. Tener el registro de DS en la zona principal crea un vínculo seguro que un atacante externo tendría que superar para falsificar el material clave en la zona secundaria.

Normalmente, el ccTLD comparte su registro de DS con la Autoridad de Números Asignados en Internet (IANA) para su publicación en la zona raíz. Los registratarios y administradores de

nombres de dominios bajo el ccTLD comparten sus registros de DS con el ccTLD directamente o a través de un registrador. Los registradores tienen dos funciones importantes que desempeñar aquí:

- **Proporcionar una interfaz o un mecanismo seguro y confiable para recopilar los registros de DS** de los registratarios; si dicha interfaz o mecanismo aún no existe, los registradores que estén dispuestos a ofrecer compatibilidad con las DNSSEC a sus registratarios deben trabajar lo antes posible para implementarlo. No existe una forma estandarizada de trasladar el registro de DS del cliente al registrador. Los distintos registradores tienen diferentes mecanismos, que van desde simples interfaces web hasta diversas API.
- **Enviar el DS al registro**. Se recomienda una solución automatizada de publicación del DS en la zona principal en lugar de la intervención manual. En el modelo registro-registrador, es posible utilizar las extensiones de las DNSSEC para el EPP para la transferencia de conjuntos de registros de recursos de DS (RRset) y, opcionalmente, de RRset de DNSKEY. En cualquier caso, deberían realizarse pruebas entre el operador de ccTLD y los registradores para garantizar que las nuevas transacciones sean viables utilizando la infraestructura existente.

Otro mecanismo para que una zona secundaria gestione automáticamente el DS con su zona principal es utilizar un RRset de CDS (DS secundario) o de CDNSKEY (DNSKEY secundario) si la zona principal tiene una política de aceptación para estos registros. Pueden utilizarse para los tres casos de uso siguientes:

- Una publicación inicial de DS
- Un traspaso de clave
- Volver al estado inseguro

En pocas palabras, el CDS/CDNSKEY es una instrucción a la zona principal para modificar el RRset del recurso de DS si el CDS/CDNSKEY y el DS difieren. El documento RFC 8078, *Gestión de registros de DS desde la zona principal a través de CDS/CDNSKey* explica en detalle la gestión automatizada de registros de DS entre las zonas secundaria y principal.

Por último, la participación de los registradores en una fase inicial del proceso también les permite beneficiarse de la formación y los programas prácticos sobre las DNSSEC que imparte la ICANN junto con sus entidades asociadas en la comunidad de Internet.

4 Cronograma

No existen plazos específicos para la implementación de las DNSSEC. La duración puede variar desde unas pocas semanas hasta meses o años, en función de diversos factores. No obstante, tenga en cuenta las siguientes sugerencias para evitar grandes retrasos:

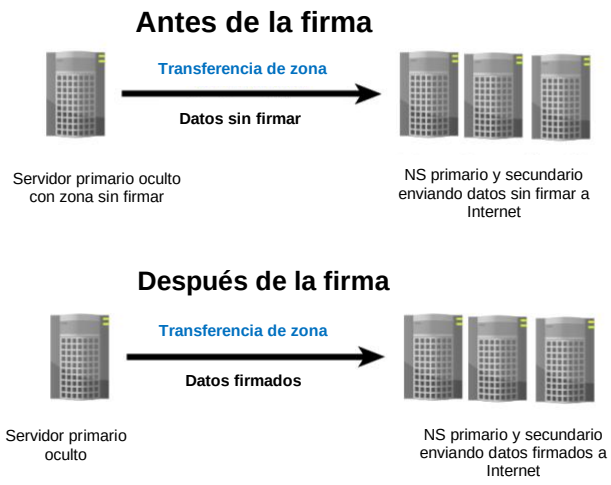
- Defina el proceso como un proyecto con una fecha de inicio clara, una fecha de finalización prevista e hitos a alcanzar. Además, asigne un gerente de proyecto o un líder técnico que cuente con los recursos adecuados.
- Defina, gestione e interactúe con las partes interesadas, las cuales comprenden, entre otras, a los entes reguladores, los registradores, los actores técnicos y administrativos, los contratistas y los operadores de backend. También es necesario abordar la comunicación entre las diferentes partes interesadas del ccTLD.
- Identifique y gestione adecuadamente los riesgos.

5 Escenarios de implementación de las DNSSEC

Tanto si decide gestionar la zona únicamente con sus propios recursos e infraestructura o a través de la contratación de un proveedor, como un operador de backend, es probable que la arquitectura de implementación técnica siga uno de los dos escenarios principales que se describen a continuación.

5.1 Servidor primario para firmas en línea (primario oculto)

En este escenario de configuración, un servidor de nombres primario oculto, normalmente desconocido en Internet, funciona en la zona para un conjunto de servidores autoritativos del DNS, normalmente para un primario público y una serie de servidores secundarios. Un servidor de nombres primario oculto no es un requisito específico de las DNSSEC, sino una práctica recomendada de operación del DNS que sugiere tener un servidor de nombres autoritativo fuera de banda que sea inaccesible y desconocido para el público y donde se puedan realizar todas las actualizaciones de zona. Este servidor también debería implementar procedimientos de seguridad y auditoría más estrictos. La arquitectura se asemeja a la figura siguiente:

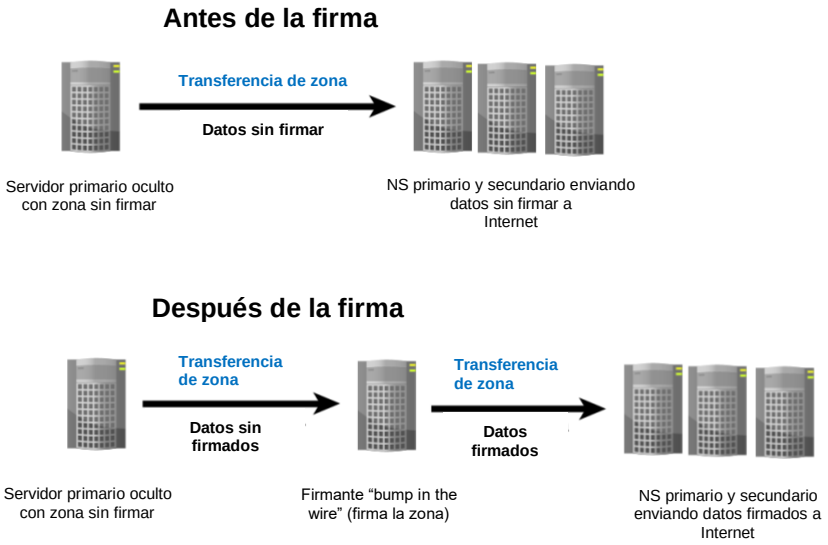


Este servidor primario oculto estará configurado para reconocer las claves creadas, y utilizarlas para generar y ejecutar una zona firmada, siguiendo el proceso proporcionado por el software del DNS que ejecuta. Al finalizar, la versión firmada del archivo de zona se transferirá y se mantendrá sincronizada con todos los servidores de nombres autoritativos visibles públicamente.

A excepción de los cambios de configuración en el servidor de nombres primario oculto, no hay más cambios de configuración o de software adicionales que realizar en esta arquitectura.

5.2 Firma en línea “bump-in-the-wire”

En este escenario de configuración, se inserta un nuevo servidor de nombres, el firmante, en la arquitectura existente, y se coloca entre el servidor primario oculto y los servidores de nombres públicos que funcionan en la zona para Internet. Este nuevo servidor actúa como un dispositivo "bump-in-the-wire" (BITW). Toma el archivo de zona sin firmar del primario oculto, firma los datos y envía el archivo de zona firmado para distribuirlo a los servidores de nombres públicos del dominio.



Para ello, se pueden tener en cuenta los siguientes pasos:

1. El primario oculto no debe figurar en el conjunto de recursos del servidor de nombres (NS) del dominio para evitar obtener respuestas conflictivas, es decir, respuestas no firmadas del primario oculto y respuestas firmadas de los demás servidores de nombres.
2. La configuración del servidor primario oculto debe actualizarse para que solo el firmante pueda realizar una transferencia de zona.
3. El firmante utiliza el archivo de zona sin firmar recibido del servidor primario oculto y una clave privada para firmar los registros de recursos. Por último, distribuye el archivo de zona firmado a los servidores de nombres primario y secundario utilizando mecanismos de transferencia de zona.
4. La configuración de los servidores de nombres también debe actualizarse en consecuencia para recibir la transferencia de zona únicamente del firmante.

Independientemente del escenario de implementación, se recomienda verificar la zona firmada antes de distribuirla entre todos los servidores. Este ejercicio de verificación puede realizarse en el nombre de dominio, utilizando herramientas en línea como las que se describen en la Sección 10 del presente documento. También es una práctica recomendada ejecutar varias consultas buscando las firmas de los registros de recursos de las DNSSEC y las fechas de caducidad de las firmas, entre otros parámetros, en cada una de las zonas que se administran. Incluya estas ejecuciones de prueba como parte de la validación de su implementación.

En resumen, comparemos los pasos de la cadena de producción de zonas entre el DNS normal y las DNSSEC:

- **DNS normal**: Crear → Validar → Publicar → Monitorear
- **Con DNSSEC**: Crear → Validar → Firmar → Validar → Publicar → Monitorear

6 Firma de un TLD

Como en el caso de cualquier otro cambio importante, es muy recomendable realizar una fase de pruebas exhaustivas antes de planificar una implementación en el sistema de producción. Resulta aún más necesario en el caso de las DNSSEC, porque se introducen nuevos cambios en la zona. Los pasos que se describen a continuación ofrecen un resumen general para la firma de una zona de TLD pero, en función de su entorno y de sus requisitos específicos, es posible que deba ajustarlos.
En algunos casos, firmar todo el archivo de zona a la vez no sería apropiado para los ccTLD de gran tamaño; en cambio, sería más seguro establecer un enfoque progresivo para firmar la zona. Otros ccTLD también pueden optar por firmar primero una zona secundaria en un banco de pruebas, antes de agregar un registro de DS en la zona principal. Se trata de una prueba preparatoria antes de firmar la zona del ccTLD real.

En cualquier caso, para completar con éxito el proceso de firma, sería prudente proceder con cautela adoptando planes de implementación y prueba adecuados que estén acompañados de una metodología de validación rigurosa.

1. Despliegue y configure un entorno de plataforma de prueba de las DNSSEC. En función del modelo de implementación, la plataforma de prueba podría contener los siguientes elementos:
   - Un servidor de firma de prueba, un servidor de nombres (NS de prueba), que sea capaz de firmar un archivo de zona. El servidor debe ser capaz de generar las claves de firma o recibir claves generadas desde otro servidor o desde un Módulo de Seguridad de Hardware (HSM), firmar la zona y distribuir el archivo de zona firmado, entre otras funciones.
   - Un servidor de nombres secundario autoritativo de prueba recibirá la zona firmada y la servirá.
   - Un resolutor de prueba debe estar configurado para realizar validaciones de DNSSEC localmente para la zona firmada.
2. Copie el archivo de zona sin firmar del servidor primario oculto en el servidor de firma de prueba. La distribución del archivo de zona sin firmar en el sistema de firma de prueba podría automatizarse más adelante en la fase de pruebas.
3. Genere las claves KSK y ZSK. Se recomienda generar las claves fuera del sistema de firma. Almacene la KSK en un HSM o fuera de línea y utilícela solo para firmar los registros de recursos DNSKEY.
4. Firme la zona y publíquela en el servidor o servidores de nombres secundarios de prueba.
5. Genere e importe el DS como claves de confianza al resolutor de prueba. En situaciones reales, los administradores de TLD no distribuirán el DS en los resolutores recursivos de todo el mundo directamente, sino que lo enviarán a la IANA para que lo publique en la zona raíz. Cualquier resolutor recursivo de validación en cualquier parte del mundo obtendrá entonces el DS correspondiente a ese TLD desde la zona raíz.
6. Realice algunas pruebas mediante las pruebas de aceptación de usuarios (UAT) basadas en casos de prueba definidos. Las pruebas deben abarcar temas como la

recuperación de las claves y las firmas, la comprobación de la caducidad de las firmas, el tiempo de respuesta de la consulta y el tamaño. Realice la validación de las DNSSEC entre otras tareas.

7. Si el proceso de firma de prueba está automatizado, observe la caducidad de las firmas y la generación automática de nuevas firmas. En caso contrario, deberá realizar renovaciones manuales hasta que el proceso de firma de prueba esté automatizado.
8. Realice el traspaso de la ZSK y el traspaso de la KSK. Para un traspaso de la KSK, genere el nuevo DS y simule que lo comparte con la zona principal agregándolo al resolutor de prueba para su validación local. En función de varios parámetros de tiempo, como el período de validez de la clave en el entorno de prueba, tendrá que eliminar el antiguo DS del resolutor de prueba y la antigua KSK de la zona para completar el traspaso de la KSK.
9. Realice nuevas pruebas de forma iterativa y perfeccione los pasos 1 a 8.
10. Una vez que tenga confianza en la metodología de pruebas, concéntrese en la puesta en marcha y en la elección del entorno y el escenario de implementación adecuados: firma primaria oculta en línea o BITW. Realice una nueva Prueba de Aceptación de Usuarios (UAT) para confirmar que todos los servidores de nombres autoritativos del dominio sirven correctamente a la zona y sus correspondientes registros de recursos de las DNSSEC.
11. Por último, publique el DS en la zona raíz siguiendo las pautas de gestión de delegaciones para los TLD definidas por la IANA en https://www.iana.org/domains/root/manage. Una vez agregado a la zona raíz, anuncia al mundo que el ccTLD está firmado con las DNSSEC y que cualquier resolutor de seguridad debe realizar la validación de las DNSSEC frente a los registros del DNS que se originan en esa zona. Se recomienda encarecidamente utilizar una herramienta como https://dnsviz.net/ (ver la Sección 10 para más detalles) para validar realmente la cadena de confianza de las DNSSEC para la zona.
12. Una vez que el ccTLD esté "oficialmente firmado", planifique abrir el acceso para que los registradores publiquen los registros de DS de los registratarios en el registro y así la cadena de confianza sea efectiva.

7 Traspaso de claves y algoritmos

Cuando una zona está asegurada con las DNSSEC, el administrador de la zona debe estar preparado para reemplazar (o "traspasar") las claves utilizadas para asegurar la zona, tanto si se hace de forma periódica por seguridad como por cuestiones operativas o en caso de emergencia. Para implementar un traspaso de claves o algoritmos, es necesario introducir nuevas claves y descartar las antiguas de la zona. Es fundamental tener en cuenta que los datos publicados para una zona se encuentran en varias cachés de resolución. Ignorar los datos que pueden estar en las cachés podría llevar a la pérdida de servicio para los clientes. Por ejemplo, considere los datos de zona firmados con una clave antigua, que están siendo validados por un resolutor que no tiene la clave de zona antigua en su caché. Si la clave antigua ya no está presente en la zona actual, la validación fallará y los datos de zona correspondientes se marcarán como falsos.

Por otro lado, si un resolutor intenta validar datos firmados con una nueva clave mientras la clave antigua todavía está en la caché del resolutor, también se marcarán los datos como falsos. Existen varios tipos de técnicas de traspaso de claves y algoritmos, como las descritas en el documento RFC 6781, *Prácticas operativas de las DNSSEC, Versión 2*, así como en el

documento RFC 7583, *Consideraciones de plazos para el traspaso de claves de las DNSSEC*. Ejemplos de estas técnicas son la *prepublicación*, el *traspaso de ZSK de doble RRSIG*, *la doble KSK, el doble DS y el doble RRset,* por nombrar algunos.

En el caso concreto de que se requiera un traspaso de clave de emergencia porque se sospecha que un par de claves ZSK o KSK está comprometido, es aconsejable tener ya un procedimiento documentado.

7.1 Traspaso de la ZSK

Durante un traspaso de la ZSK, es esencial asegurarse de que cualquier validador de caché que tenga acceso a una firma concreta también tenga acceso a la ZSK válida correspondiente. El RFC 6781, *Prácticas operativas de las DNSSEC, Versión 2*, documenta tres métodos para llevar a cabo un traspaso de ZSK: prepublicación, doble firma y doble RRSIG.

En este documento, describiremos solo el método de prepublicación, dado que mantiene el tamaño de las zonas y las respuestas al mínimo durante todo el proceso de traspaso. En este método, la nueva ZSK se introduce en el RRset de DNSKEY y después de que haya transcurrido el tiempo suficiente para garantizar que cualquier RRset de DNSKEY en caché contenga ambas claves. A continuación, se firma la zona con la nueva ZSK y se eliminan las firmas antiguas. Por último, cuando todas las firmas creadas con la ZSK antigua han caducado en las cachés, se elimina la clave antigua. Los pasos siguientes describen el proceso.

1. La nueva ZSK A se introduce en la zona y aparece en el RRset de DNSKEY, pero aún no se utilizará para firmar registros en la zona. Las KSK activas actuales renuncian al RRset de DNSKEY, que se vuelve a firmar con las KSK actualmente activas. En esta etapa, se dice que la nueva ZSK está publicada.
2. Después de un cierto período de tiempo, la ZSK A está lista para firmar registros en la zona. Este periodo corresponde al retraso de propagación de la zona más el tiempo de vida de los registros de DNSKEY de la zona. En otras palabras, es el tiempo máximo que tardan los registros de DNSKEY existentes en caducar en las cachés. La ZSK A se activa y empieza a firmar registros para la zona.
3. La ZSK A continuará firmando y actualizando registros para la zona hasta un momento en que sea necesario publicar una nueva ZSK B. El tiempo de publicación de la clave B depende del tiempo de activación de la clave A y del tiempo de vida de la ZSK establecido para la zona en la política de gestión de claves. La ZSK B se prepara y puede utilizarse para firmar registros, pero la ZSK A sigue activa.
4. Cuando se alcanza el tiempo de vida de la ZSK para la clave A, ésta se retira. La clave B se activa y se utiliza para firmar la zona. Sin embargo, la clave retirada debe conservarse en la zona durante algún tiempo (durante un "intervalo de retirada") para permitir que la RRSIG que se genere utilizando esa clave siga siendo validada por los resolutores. El intervalo de retirada corresponde al tiempo necesario para que todos los RRset existentes se vuelvan a firmar con la clave B, más el retraso de propagación de la zona, y el TTL máximo de todas las RRSIG creadas con la clave antigua en la zona.
5. Después de un cierto período de tiempo, las firmas creadas con la clave retirada desaparecen de las cachés del resolutor, y se dice que la clave antigua está muerta.
6. Una vez que la clave antigua está muerta, puede eliminarse del RRset de DNSKEY, que debe volver a firmarse con las KSK de la zona actual. En esta etapa, se declara la eliminación de la clave A.
7. Pasado cierto tiempo, se publicará una nueva clave y se repetirá todo el proceso.

7.2 Traspaso de la KSK

En un traspaso de KSK, el principal desafío consiste en garantizar que exista una KSK de confianza para la zona en todo momento, incluso durante el proceso de traspaso. El documento RFC 6781, *Prácticas operativas de las DNSSEC, Versión 2*, también detalla tres métodos para llevar a cabo un traspaso de la KSK: doble KSK, doble DS y doble RRset. El método de doble RRset es el más eficiente, dado que tanto los nuevos registros de DS como los RRset de DNSKEY se propagan en paralelo.

En este método, los nuevos registros de DNSKEY y de DS se publican simultáneamente en las zonas correspondientes. Una vez que ha transcurrido el tiempo suficiente para que los antiguos RRset de DNSKEY y de DS caduquen en las cachés, se eliminan de sus respectivas zonas. Las etapas del traspaso se describen a continuación:

1. Los registros de DS y de DNSKEY están presentes en sus respectivas zonas. Su correspondiente KSK A está activa y asegura la zona.
2. Una vez que está por concluir el tiempo de vida de la KSK A actual, se introduce una nueva KSK B en la zona y se la utiliza para firmar el RRset de DNSKEY. El DS de la KSK B se envía al principal para su publicación en la zona principal.
3. El principal podría proceder a verificar el nuevo DS y luego publicarlo en la zona principal.
4. Transcurrido un tiempo determinado, el nuevo DS o DNSKEY ya se ha propagado en las cachés de los resolutores de validación. Al mismo tiempo, la ZSK A se elimina de la zona.
5. Posteriormente, también se eliminan los registros de DS y DNSKEY asociados a la ZSK A.
6. Pasado cierto tiempo, se publicará una nueva clave y se repetirá todo el proceso.

8 Otras consideraciones para las zonas firmadas

Cabe tener en cuenta los siguientes elementos en la preparación de una estrategia de implementación de las DNSSEC:

- **Definir un programa de capacitación:** identifique y participe en talleres, seminarios web, formaciones prácticas y cualquier otra actividad de desarrollo de capacidades que pueda ayudar a aumentar los conocimientos y desarrollar nuevas habilidades en las operaciones de las DNSSEC. El departamento de Participación Técnica de la ICANN imparte este tipo de formación, incluidos los talleres sobre las DNSSEC, que suelen tener lugar durante las reuniones de la ICANN.
  - Además de la ICANN, el Centro de Recursos de Inicio de Redes (NSRC), la Internet Society y los registros regionales de Internet (RIR) también ofrecen actividades de difusión relacionadas con las DNSSEC.
  - Por último, participar en foros, seminarios web y talleres en los que tanto los operadores experimentados como los nuevos miembros se reúnen, realizan presentaciones y debaten sobre las implementaciones actuales y futuras de las DNSSEC puede mejorar en gran medida sus conocimientos sobre las prácticas operativas de las DNSSEC.

- **Suscribirse a las listas de correo de los NOG**: estos son foros en los que las personas debaten y comparten sus experiencias y conocimientos técnicos, además de buscar apoyo y asistencia en cuestiones técnicas. Considérelos una comunidad que puede ayudarlo cuando lo necesite.
- **Generación y gestión de claves:** los módulos de seguridad de hardware (HSM) suelen ser una buena opción para generar y almacenar claves privadas. Sin embargo, hay que tener en cuenta los costos de compra, seguridad y mantenimiento de los HSM. En función de sus características, los costos de los HSM pueden variar desde unos pocos cientos hasta miles de dólares. Los HSM también pueden agregar gastos de capacitación, dado que el aprendizaje de cualquier hardware nuevo conlleva sus dificultades. La utilización de los HSM es una práctica recomendada, pero no es el único método para generar claves. Otra posibilidad que vale la pena considerar es generar, almacenar y utilizar las claves privadas en una máquina fuera de línea, no conectada a la red y físicamente segura. El documento RFC 6781, *Prácticas operativas de las DNSSEC, Versión 2* proporciona más detalles sobre la generación y gestión de claves.
- **Consideraciones de tiempo**: las DNSSEC introducen la noción de tiempo absoluto en el DNS. Las firmas en las DNSSEC tienen un periodo de validez desde su fecha de inicio hasta su fecha de caducidad, después de la cual la firma se marca como no válida y los datos firmados se consideran falsos. Es fundamental asegurarse de que el tiempo se gestione adecuadamente para que las firmas se generen con el período de validez correcto. Imagínese una zona firmada cuyo período de validez de la firma haya transcurrido; esto hará que la validación falle en el resolutor. Por lo tanto, se recomienda encarecidamente configurar el servidor del protocolo de horario de red (NTP) para mantener la hora exacta. También existen otras consideraciones como el tiempo de vida útil (TTL) mínimo y máximo de la zona, el período de publicación de la firma y el período de validez de la firma, tal y como se describe en el documento RFC 6781, *Prácticas operativas de las DNSSEC, Versión 2*.
- **Requisitos de software, hardware y red**: actualmente se admiten implementaciones de las DNSSEC tanto de código abierto como comerciales, entre las cuales se incluye el Dominio de Nombres de Internet de Berkeley (BIND), PowerDNS, Name Server Daemon (NSD) de NLnet Labs y Knot DNS, por nombrar algunas. OpenDNSSEC es una solución de firma que sigue siendo muy utilizada, dado que automatiza el proceso de seguimiento de las claves de las DNSSEC y la firma de las zonas. Si su plan es implementar las DNSSEC en un servidor autoritativo, tendrá que generar las claves de firmas criptográficas en el sistema. El tiempo necesario para generar las claves depende de la fuente de aleatoriedad (entropía) del sistema. Los sistemas como las máquinas virtuales con insuficiente entropía pueden tardar mucho más tiempo en generar las claves.
  - Los recursos de hardware, como la CPU, el almacenamiento del sistema y la memoria, también son áreas que vale la pena considerar para posibles optimizaciones. Esto se debe a que la activación de las DNSSEC aumenta el almacenamiento del sistema, el uso de la memoria y la carga de la CPU en parte debido a la generación de claves y la firma. Una zona firmada siempre va acompañada de un aumento considerable del archivo de zona.
  - En cuanto a las políticas de seguridad de la red, verifique que las reglas del cortafuegos y de las ACL, por ejemplo, permitan tanto los paquetes UDP del DNS de gran tamaño como el DNS sobre TCP en el puerto 53. Además, es necesario activar el Mecanismo de Extensión para DNS (EDNS0) tanto en los servidores del DNS como en la configuración de la red, respectivamente.

9 Anular la firma del TLD si es necesario

Las DNSSEC, como muchas cosas en este mundo, no están exentas de problemas. Al agregar mayor complejidad al DNS, aumenta la probabilidad de que las cosas se dañen o salgan mal. Por ejemplo, la KSK o la ZSK, o ambas, pueden perderse o verse afectadas. Un problema imprevisto de hardware o software podría impedir que una zona sea firmada y distribuida, lo cual afectaría, por lo tanto, el correcto servicio de una zona.

En el peor de los casos, es posible que prefiera anular la firma de la zona para solucionar cualquier problema o error antes de volver a firmarla. Sin embargo, anular la firma de un dominio conlleva el costo de volver a llevarlo a un estado inseguro.

El mundo sabe si una zona está firmada o no por la presencia de un registro de DS en la zona principal. Si no existe ningún registro de DS, la cadena de confianza no está asegurada. Por lo tanto, volver a un estado sin firma es técnicamente tan fácil como eliminar todos los registros de DS de la zona principal. En el caso de un ccTLD, esto implica solicitar a la IANA que elimine los registros de DS correspondientes de la zona raíz.

Una vez resueltos todos los problemas, el operador del TLD debe considerar la posibilidad de generar nuevas claves y volver a firmar la zona. Además, el operador debe asegurarse de que la zona recién firmada esté bien distribuida y disponible en todos los servidores de nombres antes de publicar un nuevo registro de DS en la zona raíz. Una vez que la IANA publica el DS, toda Internet sabe que la zona del TLD ha sido firmada de nuevo y que cualquier resolutor de validación verificará todos los registros de recursos para los cuales la zona brinda servicio.

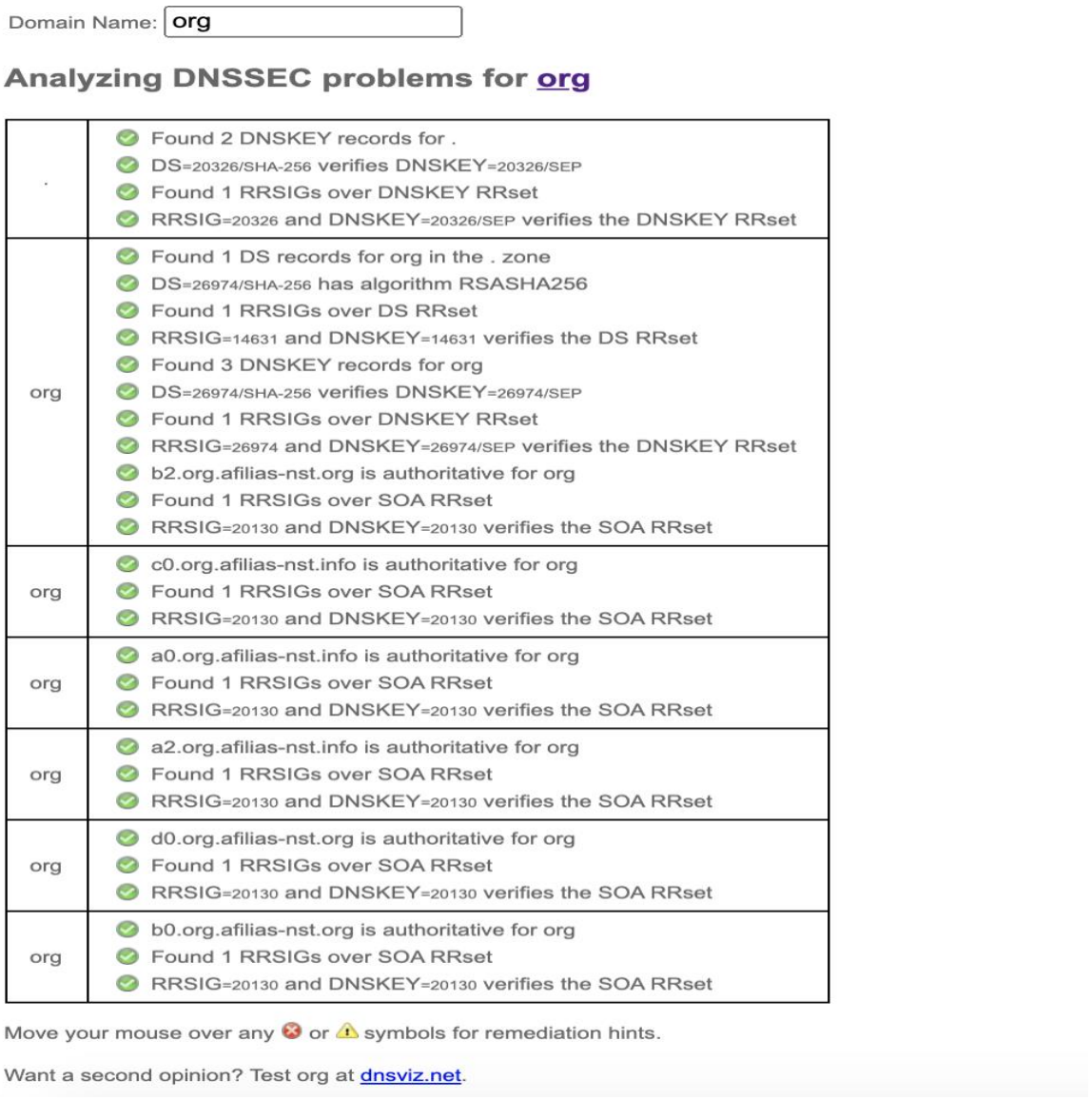
10 Herramientas útiles para implementar las DNSSEC

Las siguientes herramientas pueden resultar útiles para solucionar problemas con las DNSSEC.

10.1 Depurador para DNSSEC de Verisign

Este depurador de DNSSEC, que se encuentra en https://dnssec-debugger.verisignlabs.com/, es una herramienta basada en la web, que ayuda a garantizar que la "*cadena de confianza*" está intacta para un nombre de dominio particular habilitado para DNSSEC. Muestra una validación paso a paso de un determinado nombre de dominio y resalta cualquier problema que se encuentre.

A continuación, se muestra un ejemplo del resultado:



Domain Name: org

Analyzing DNSSEC problems for org

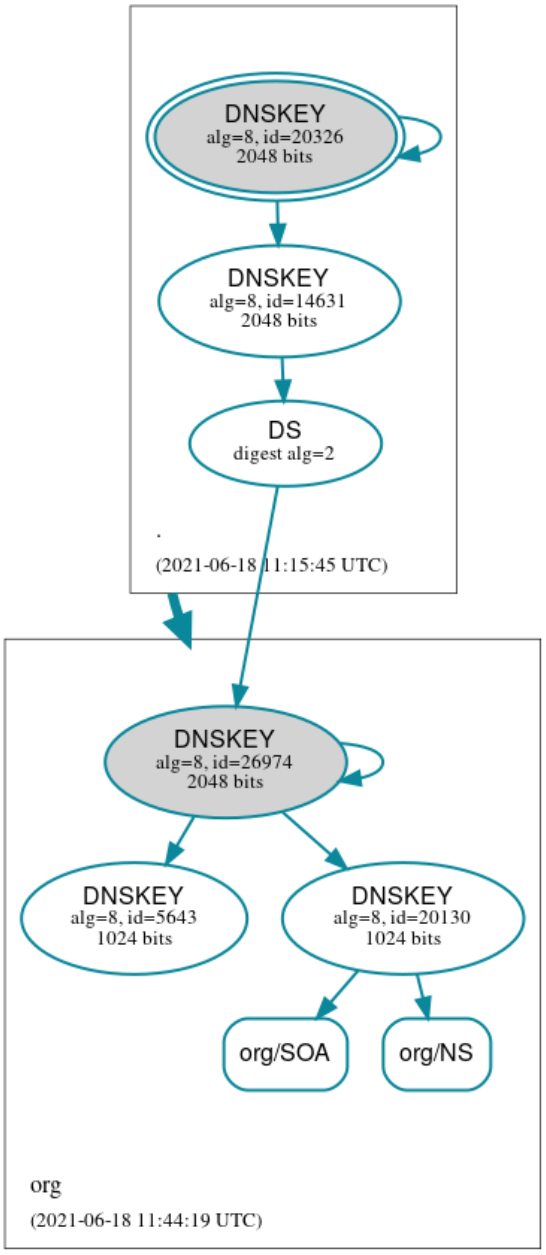
.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
org	Found 1 DS records for org in the . zone DS=26974/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=14631 and DNSKEY=14631 verifies the DS RRset Found 3 DNSKEY records for org DS=26974/SHA-256 verifies DNSKEY=26974/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=26974 and DNSKEY=26974/SEP verifies the DNSKEY RRset b2.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	c0.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	a0.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	a2.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	d0.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	b0.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

Want a second opinion? Test org at dnsviz.net.

10.2 DNSVIZ

DNSViz (https://dnsviz.net) es una herramienta para visualizar el estado de una zona del DNS. Proporciona un análisis visual de la cadena de autenticación de las DNSSEC para un nombre de dominio y su ruta de resolución en el espacio de nombres del DNS. También enumera los errores de configuración detectados por la herramienta. A continuación, se muestra una visualización de la zona de .ORG:



11 Conclusión

Las DNSSEC son un protocolo sólido que proporciona autenticación e integridad a los datos del DNS. Firmar un nombre de dominio con las DNSSEC cambia muchas cosas a nivel operativo al introducir nuevos conceptos y tareas que no existían con el DNS normal.

Este documento es una guía para ayudar a los operadores de registro de ccTLD, y a quienes lo necesiten, a entender lo que constituye la firma de un ccTLD. Hay mucho que mencionar sobre

las DNSSEC. Este documento abarca algunos de los aspectos más importantes de su implementación.

Al igual que cualquier otra solución de seguridad, es aconsejable seguir un proceso adecuado y prepararse para evitar que las cosas dejen de funcionar. Todos los actores deben evaluar su propio entorno, junto con las amenazas y vulnerabilidades asociadas, para determinar el nivel de riesgo que están dispuestos a aceptar al confiar en las DNSSEC para proteger su zona y los dominios que se encuentran en ella.

Esencialmente, los esfuerzos coordinados y la colaboración activa de todas las partes interesadas siguen siendo clave para el éxito de la implementación de las DNSSEC.

A Ejemplo de políticas de DNSSEC y declaraciones de prácticas de DNSSEC

- Marco de políticas y declaraciones de prácticas de DNSSEC del ZACR, versión 001, septiembre de 2016, ZACR: https://www.registry.net.za/downloads/u/zacr-dps-signed.pdf
- Declaración de prácticas de DNSSEC para .fr, versión 1.2, junio de 2013, Afnic: https://www.afnic.fr/wp-media/uploads/2020/12/dps-english-fr.pdf
- Declaración de prácticas de DNSSEC de la CIRA para .CA, versión 1.5, agosto de 2016, CIRA: https://www.cira.ca/cira-dnssec-practice-statement-ca
- Declaración de prácticas de DNSSEC para la zona de JP (JP DPS), versión 1.4, octubre de 2015, JPRS: https://jprs.jp/doc/dnssec/jp-dps-eng.v1.4.html
- Declaración de prácticas de DNSSEC de Verisign para la zona de TLD/GTLD, versión 1.8, dic. 2019, Verisign Inc.: https://www.verisign.com/assets/20191111_CTLD_VerisignDNSSECPracticeStatement_v1.8_finalized.pdf. La lista de las zonas a las que se aplica este documento se encuentra en https://www.verisign.com/assets/20190430-Verisign-Operated-TLD-GTLD-Zones-v1.04-Converted.pdf

B Ejemplo de zona sin firmar y firmada

B.1 Zona sin firmar

```
example.                  86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                2017072300 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                2419200    ; expire (4 weeks)
                300        ; minimum (5 minutes)
                )

example.                  86400  IN     NS     a.nic.dns.blablabla.
example.                  86400  IN     NS     b.nic.dns.blablabla.
example.                  86400  IN     NS     d.nic.dns.blablabla.
```

```
example.                    86400  IN     NS     e.nic.dns.blablabla.
example.                    86400  IN     NS     f.nic.dns.blablabla.
aaa.example.                86400  IN     NS     ns1.reg.zzzz.
aaa.example.                86400  IN     NS     ns2.reg.zzzz.
bbb.example.                86400  IN     NS     ns1.reg.zzzz.
bbb.example.                86400  IN     NS     ns2.reg.zzzz.
ccc.example.                86400  IN     NS     ns1.reg.zzzz.
ccc.example.                86400  IN     NS     ns2.reg.zzzz.
ddd.example.                86400  IN     NS     ns3-l2.nic.zzzz.
```

B.2 Zona firmada

```
example.                    86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                2017072305 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                2419200    ; expire (4 weeks)
                300        ; minimum (5 minutes)
                )

example.                    86400  IN     RRSIG  SOA 8 1 86400 20170724231821
20170618015310 660 example. nQ8H8StSRDoQgzwBNQ0k9+E1LGrV0tsCinoB6KxcyuHfGT4ehWsj5JI6
N01WpXqy/q1S/XlhqtjVoiti4zSOwIjFlSloug3W09eJnH9biwmb6U8B
JQoHf3edGvZtWNZdtcOKY1CFBI2ApceFn8KOYvT0qzpygOlF5lMrJvnO J5c=
example.                    86400  IN     NS     a.nic.dns.blablabla.
example.                    86400  IN     NS     b.nic.dns.blablabla.
example.                    86400  IN     NS     d.nic.dns.blablabla.
example.                    86400  IN     NS     e.nic.dns.blablabla.
example.                    86400  IN     NS     f.nic.dns.blablabla.
example.                    86400  IN     RRSIG  NS 8 1 86400 20170730192856
20170617025305 660 example. KNaF2jTPuCGq5FIzspbJL+TDBx/6z01E7+tkkzYRNh0xAKDnutcfb1It
D7XrNWPEbXsaafFyZ/M5DaDGzTzsVNm1h9h3md6o0vZNH07q8nmm+fYX
do8sx9aFxCgl9NsmG0cyrBbVnyrPKxDlAx69HJCh0kBb7PFKhr1hpnYY xGA=
example.                    86400  IN     DNSKEY 256 3 8
AwEAAasHjitdDurpevNLojD4Sp3609P+C9uOTR42DJel0NSSva/x38Ba
7gs0b4Q+tmKPI5cmxDhECiUfdzaRRA8vxPZK8x5LL/V1WZ5q6egFmH4x
eLxWaxlftFotev/T8kVe7jZUk7Hh3x7LPgGLajpjNNFELj42Xe6XBkkN 9FY1lQkB
example.                    86400  IN     DNSKEY 257 3 8
AwEAAY6HLDY5M5kjlrjVV9HQyWUkkrYZ2eB8KeJjUMN9qDM6FsA57pbS
5tmbGV1zxxqGon0pO7HYV06GZIgFOLBqDvgGsnKDQ5A2iktYNuSmTh+w
fd8ixgbYigtoBMBnNeqFozMK58c1yf7amui2cCOg9ibGZMpLQvjKOSyV
Jnlh0l8e3OE7Ul1GEa39XpVez2wkjImhsG0e7KAZPlFjEUpvwie8HEQV
jz3PK7Zr6SZVLLyet0rnN3prCHfvhNh6DycN/rt6/PopLvPQM8SaW+u8
zn6Z4S4AoTPTxKm5udzb7mWf7lT83PAbOvLu/WIRY6nqye+4SkJsrmjI xnLdk/Q54E8=
example.                    86400  IN     RRSIG  DNSKEY 8 1 86400 20170703000000
20170613000000 54322 example. B2riGYos+/q5RqXVBQKrrkVUuruDBH8ANNa8J6sMHUjf0MPZOuICd2kZ
PlAGMpZpp8LoaRoG2zaTVILZ8Vhi90FsyLsZVpPooAvmKlTFOrWoJoPo
XScLhb3ISRLOzKEnyLt5Ds3TxuabHLPlf8jpTXaHMFZCzYYtTJJQb+M3
BLeK+Lx4uCwU1pvxNkuR9StKa5tJquByIZCWZsSx5nKWPyrsGLtFJKrg
DXe8XlA8LxeER69OQgSZ1VXvK8Kd4p3wyvzUHCcsPYZzebxHXPqDrYB7
BU7eqsDUjCfThqbkC0Ju7koHROYRjGdoY/4f6nDOJEOICIFEgEDHJg2t w1nENQ==
example.                    0      IN     NSEC3PARAM 1 0 3 00FF
example.                    0      IN     RRSIG  NSEC3PARAM 8 1 0 20170716213640
20170606005304 660 example. a6Mp1NjW2/nnn+5i98AWzVrOX0yUvu/urP1cqY6zZjISReZOSLx6aorJ
```

```
lM9Nnx1fNVr2COtD71UVJI7kFUC5jVbmAitWdHHH/zyzK6WyyaN5Nsaf
cKW0Su8lLkctCHiqpKmuhOhnK1Dqmigx8YhyhPbN5nCzoST6lcnNjtV0 TwQ=
aaa.example.        86400  IN     NS     ns1.reg.zzzz.
aaa.example.        86400  IN     NS     ns2.reg.zzzz.
bbb.example.        86400  IN     NS     ns1.reg.zzzz.
bbb.example.        86400  IN     NS     ns2.reg.zzzz.
ccc.example.        86400  IN     NS     ns1.reg.zzzz.
ccc.example.        86400  IN     NS     ns2.reg.zzzz.
ddd.example.        86400  IN     NS     ns3-l2.nic.zzzz.
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN      NSEC3 1 1 3 00FF
464L7A368JEOCPKU9G34B9RQADEPKA14 NS DS RRSIG
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170703210235 20170602012306 660 example.
H+qdaHqnAgUa66VSKmMmfKWopeZQM0ridMUN2YN4rncHeWD8b0yA6O6N
hLF/ojpZoGrQN+G+p4SWJVb/pj2CkLk00E2AhloXXV0KaQIzUwPVNm7p
J9es7ohi5ErGtM1ClLpGggz05qNWboejbrXtS8TFdoTtn6Z2Omk4RNmj hG0=
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN      NSEC3 1 1 3 00FF
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA NS DS RRSIG
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170715005821 20170610062309 660 example.
dk6WScB3zmJYig0w8LxFXoc9vj1leqFRBlET4YAVVmeAwcGf0ixa41T+
pKKcMHbXDsw+PHYZHaRLmA9lEgs+4lJMdA3fRroNSXyV2usHMdFaKUoG
UZKehVGdgrBRx4vx+o4w1ztdumY6MsD0ART6IrhUbr+cvGHAlxNSviCI BbE=
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN      NSEC3 1 1 3 00FF
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7 NS SOA RRSIG DNSKEY NSEC3PARAM
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170706043605 20170604225320 660 example.
Ndq6p+Y8ztlgNN1vH12o5rxxh7QM8GLY3E1FPCX4h7N4RtnuoPpvEpsl
/K4XQ1p/8Uehe6Izg0BpvQ7A256/+UW3lkwlonR7UaOX/+gkEdxuxlC/
41nX5fI9G5QFrV7H8B7ezlVF/uLz4nXyH4mzz496x4iTMEoHfoAdMinL C7A=
example.                  86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. 2017072305 86400 14400 2592000 3600
```

C Lista de verificación para la implementación de las DNSSEC

C.1 Inicio y preparación

- ❑ Definir el despliegue de las DNSSEC como un proyecto

  Gestionar todo el proceso como un proyecto con una fecha de inicio, una fecha de finalización prevista y resultados claros utilizando un enfoque de gestión de proyectos
- ❑ Documentar el sistema existente

  Documentación actualizada que describa el sistema y los procesos en uso
- ❑ Auditar la infraestructura existente

  Solucionar las deficiencias del sistema actual antes de la implementación de las DNSSEC
- ❑ Implicar a las partes interesadas

  Procurar su comprensión y buena disposición para la implementación de las DNSSEC

- ❏ Definir y seguir un plan de capacitación

  Proporcionar al personal y a las partes interesadas los conocimientos y habilidades necesarios para la implementación de las DNSSEC

C.2 Implementación y monitoreo

- ❏ Redactar una DP o una DPS

  Publicar el marco de operaciones de las DNSSEC aplicable en la zona
- ❏ Redactar un plan de implementación de las DNSSEC

  Documentar los pasos y la estrategia global de implementación. En este documento, se pueden abordar varios puntos de la lista de verificación.
- ❏ Redactar y validar los procesos y procedimientos operativos de las DNSSEC

  Documentar los procedimientos para sus requisitos y su entorno
- ❏ Elegir un escenario de implementación de las DNSSEC

  Identificar el modelo de implementación de las DNSSEC
- ❏ Identificar y comprar materiales y equipos nuevos

  Adquirir nuevos equipos y materiales
- ❏ Seleccionar los parámetros de firma de las DNSSEC

  Asignar valores a un conjunto de parámetros de las DNSSEC
- ❏ Crear un banco de pruebas para las DNSSEC

  Redactar, ejecutar y validar casos de prueba para la firma de zonas para familiarizarse con los procesos y operaciones de las DNSSEC
- ❏ Planificar la puesta en marcha y preparar un procedimiento de respaldo

  Preparar y documentar la puesta en marcha en el entorno de producción, así como el monitoreo y los procedimientos de respaldo.
- ❏ Puesta en marcha y monitoreo

  Implementar y monitorear la firma de las DNSSEC en el entorno de producción
- ❏ Planificar la publicación del DS de los registratarios

Promoción de las DNSSEC, preparación para recibir y procesar los registros de DS de los subdominios

- ❏ Publicar el DS de los registratarios

  Anunciar el DS de subdominios en la zona del ccTLD
- ❏ Documentar las lecciones aprendidas

  Recopilar las lecciones y experiencias de aprendizaje en cada etapa del proceso

D Más información

- *Principales interrupciones y fallos en la validación de las DNSSEC*, IANIX: https://ianix.com/pub/dnssec-outages.html
- *DNSSEC: el largo y accidentado camino del despliegue de algoritmos*, APNIC, https://blog.apnic.net/2020/12/01/dnssec-the-long-and-bumpy-road-of-algorithm-deployment/
- *Marco de auditoría de la infraestructura de las DNSSEC*, NLnet Labs, https://nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf
- *Información sobre las DNSSEC de la raíz*, IANA, https://www.iana.org/dnssec
- *Preguntas frecuentes sobre las DNSSEC*, SIDN, https://www.sidn.nl/en/faq/dnssec
- RFC 6781, *Prácticas operativas de las DNSSEC v2,* https://www.rfc-editor.org/rfc/rfc6781.html

1. RFC 6841, *Un marco para las políticas de las DNSSEC y las declaraciones de prácticas de las DNSSEC,* https://www.rfc-editor.org/rfc/rfc6841.html

2. RFC 8078, *Administración de registros de DS del principal mediante CDS/CDNSKey,* https://www.rfc-editor.org/rfc/rfc8078.html
3. RFC 8624, *Requisitos para la implementación de algoritmos y guía de uso para las DNSSEC,* https://www.rfc-editor.org/rfc/rfc8624.html