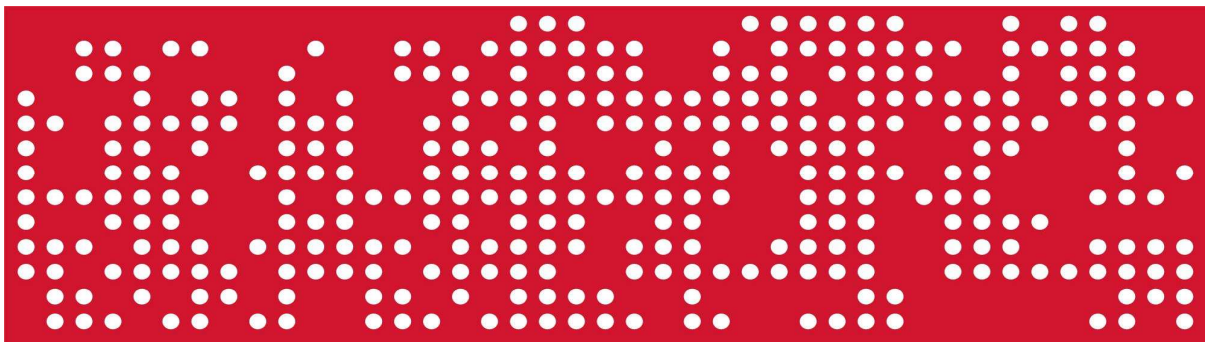
MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es

Declaración de Políticas y Procedimientos para DNSSEC en la zona“.ES”

Red.es



Versión 1.1

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es

Hoja de control documental

Realizado por	Red.es	**Fecha**	11/06/2014
Revisado por		**Fecha**	
Aprobado por		**Fecha**	

Control de versiones

Versión	Fecha	Descripción
1.0	11/06/2014	Primera versión del documento.

Índice

1. INTRODUCCIÓN

Este documento es la *Declaración de Políticas y Procedimientos* ("*DPS*" -"*Policy and Practice Statement*") relativas a *DNSSEC* en Red.es conforme a las indicaciones del *RFC 6851* ("*A Framework for DNSSEC Policies and DNSSEC Practice Statements"*) de la *IETF*.

En este documento se declaran las prácticas y procedimientos que *Red.es* emplea para firmar la zona "*.ES*" y los servicios de distribución que incluyen la generación, administración, cambio y publicación de las claves en el *DNS*.

1.1. RESUMEN

El sistema de nombres de dominio (*DNS*) no fue diseñado originalmente con mecanismos de seguridad fuertes que garanticen la integridad y la autenticidad de los datos.

A través de los años, han sido descubiertas una serie de vulnerabilidades que amenazan la seguridad y confiabilidad de los sistemas *DNS* tradicionales.

Las extensiones de seguridad en *DNS* (*DNSSEC - Domain Name System Security Extensions*) están reflejadas en las siguientes *RFC (Request for Comments) RFC4033, RFC4034, RFC4035* accesibles a través del órgano gestor de las mismas *IETF (Internet Engineering Task Force* - http://www.ietf.org/)

Dichas extensiones, permiten hacer frente a estas vulnerabilidades mediante el uso de criptografía de clave pública lo que facilita la verificación de la autenticación del origen de los datos, la verificación de la integridad de los mismos y negación de existencia autenticada.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

- Título del documento:
  "*Declaración de Políticas y Procedimientos para DNSSEC en la zona .ES*"

1.3. DESTINATARIOS Y APLICACIÓN

Se han identificado las siguientes partes para las que este documento tiene aplicación. La relación entre el Registro y un Agente Registrador está regulada en el contrato de Agente Registrador, que se puede encontrar en su totalidad en: http://www.dominios.es/dominios/sites/default/files/files/es_Contrato%20AR_20130906_con%20marca%20de%20agua%20(espa%C3%B1ol).pdf

1.3.1. Registro

Red.es es el organismo responsable del *ccTLD* "*.ES*" y de la gestión del registro "*.ES", y consecuentemente del registro de nombres de dominio identificados en las zonas bajo la zona .ES. Esto supone que Red.es gestiona, añade, modifica y borra los datos asociados con el nombre de dominio. Asimismo significa que Red.es gestiona y actualiza la infraestructura técnica que asegura el rendimiento y la resiliencia de la zona .ES*

Red.es es responsable de la generación de claves criptográficas*, protegiendo la confidencialidad de la clave privada, y firmando de forma segura los registros DNS en la zona .ES, utilizando DNSSEC y las claves asociadas.*

A su vez, *Red.es es* responsable de la generación, la exportación segura y el mantenimiento de los registros "*DS*" para su firmado y publicación en la zona "*root*". Completando así la cadena de confianza (*trust of chain*).

1.3.2. Agentes registradores

Son entidades responsables de la administración y gestión de nombres de dominios en representación del registro, según los acuerdos establecidos con el "*Registro*" (*Red.es*).

Son responsables del proceso de registro, mantenimiento y gestión de los dominios de los "*Titulares de nombres de dominios*" que adquieran los dominios a través de los "*Agentes registradores*" ya que están acreditados como colaboradores de *Red.es*.

Los agentes registradores tienen la responsabilidad de establecer los mecanismos necesarios para la identificación y autenticación de los "*Titulares de nombres de dominios*", así como de añadir, borrar o actualizar los registros DS específicos de cada dominio a petición del titular del nombre de dominio.

1.3.3. Titulares de un nombre de dominio

Se trata de las personas físicas o entidades legales que adquieren la asignación de un nombre de dominio.

Los titulares de nombres de dominios, son responsables de generar y proteger sus propias claves *DNSSEC* para el firmado de los datos de la zona, así como de registrar y mantener los correspondientes registros DS directamente o a través de un Agente registrador.

Es también responsabilidad del titular realizar el rotado de claves cuando haya indicios de que han sido comprometidas o que se hayan perdido las claves.

1.3.4. Aplicación

Cada titular de nombres de dominios es responsable de establecer un nivel de seguridad para su dominio. El presente DPS aplica exclusivamente al dominio de primer nivel .ES, y describe los procedimientos, controles de seguridad y prácticas empleadas en la gestión de DNSSEC en la zona .ES

1.4. DATOS ADMINISTRATIVOS

1.4.1. Organización

Red.es es una entidad pública empresarial adscrita al *Ministerio de Industria, Energía y Turismo (MINETUR)*, Responsable de la gestión del Registro de nombres de dominio de Internet bajo el código de país ".ES"..

1.4.2. Información de contacto

Entidad Pública Empresarial Red.es – Dominios .es

Edificio Bronce

Plaza Manuel Gómez Moreno, s/n

28020 Madrid

Correo electrónico: info@dominios.es

Teléfonos: 902 010 755 (sólo para llamadas nacionales)

Fax: (+34) 91 212 79 16

1.4.3. Cambios en el Procedimiento

Cualquier modificación del presente documento se informará a través de los medios oficiales de *Red.es*, y se mantendrá la última versión oficial en el repositorio indicado en el apartado Repositorio.

Aquellos cambios efectuados en el *DPS* serán de aplicación inmediata tras su publicación.

Solo será aplicable la última versión *DPS* publicada en los medios oficiales de *Red.es*.

2. PUBLICACIÓN Y REPOSITORIO

2.1. Repositorio

Red.es realizará las publicaciones relativas a la plataforma *DNSSEC* a través de la web oficial. En concreto, las publicaciones relativas al presente documento *DPS* es publicaran en el enlace web de dominios.es:

http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/valores-anadidos/dnssec

2.2. Publicación de las claves públicas de firmado

Red.es publicará sus claves *KSK* a través de los siguientes mecanismos:

- A través de la zona *root* será publicado el registro "*DS*".
- A través de la web oficial de *dominios.es*:

http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/valores-anadidos/dnssec

2.3. Confidencialidad

La siguiente información permanecerá confidencial:

- Componentes privadas de las claves *KSK* y *ZSK*.
- Componentes públicas de las claves *KSK* y *ZSK* antes de su fecha de publicación (claves futuras).
- Identificación de las personas que participan en los procedimientos de generación y firma de las claves generadas.

3. REQUERIMIENTOS OPERACIONALES

3.1. SIGNIFICADO DE LOS NOMBRES DE DOMINIO

Un nombre de dominio es un identificador único, asociado comúnmente con servicios como el alojamiento web o el correo electrónico. Para el propósito de este documento, un nombre de dominio es un nombre registrado bajo el dominio .ES, y correspondiendo la delegación desde la zona .ES, al servidor de nombres operado por el titular de los nombre de dominio o en representación del mismo.

3.2. PROCESO DE ACTIVACIÓN DE DNSSEC PARA ZONAS DELEGADAS BAJO ".ES"

DNSSEC para una zona delegada se activa publicando un registro DS firmado para dicha zona. La inclusión del mismo en el registro .ES para el correspondiente nombre de dominio, establece una cadena de confianza desde la zona .ES hasta la zona delegada.

Red.es asume que los registros "*DS*" provisionados son correctos, y no realizará chequeos o validaciones específicas sobre dichos registros, salvo chequeos básicos de sintaxis. Esto significa, que Red.es no verificará si una zona delegada con DNSSEC habilitado puede ser dada por válida por el registro DS correspondiente.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DEL EMISOR DEL REGISTRO DS DE LA ZONA A FIRMAR

Es responsabilidad de los "*Agentes registradores*" garantizar que los datos asociados a los "*Titulares de nombres de dominios*" son veraces y exactos, de acuerdo a cómo se establece en el contrato entre Red.es y el Agente Registrador.

Aquellos titulares de nombres de dominios que adquieran un dominio directamente a través de *Red.es,* serán identificados y autenticados directamente por dicho organismo, a través de los mecanismos establecidos por Red.es para la gestión de dominios.

3.4. VALIDACIÓN DE LOS REGISTROS DS DE LA ZONA A FIRMAR

Los Agentes Registradores facilitarán los registros DS a través de las herramientas habilitadas por Red.es.
Los titulares de nombres de dominios directamente a través de Red.es, pueden incluir su registro DS vía interfaz web, a través de la herramienta de gestión de nombres de dominios SGND.

3.5. METODOS DE VALIDACION DE PRUEBA DE POSESICON DE LA CLAVE PRIVADA

Red.es, no realiza ninguna comprobación con el objeto de validar el titular como el poseedor de una clave privada. El Agente Registrador es responsable de realizar los chequeos necesarios para asegurar la correcta operación de los nombres de dominio que se ha encargado de registrar.

3.6. ELIMINACION DE REGISTROS DS

Un registro DS puede ser eliminado vía el interfaz EPP, SOA o extranet por el Agente Registrador respectivo o vía el interfaz web por el Titular del dominio. Si todos los registros DS de una zona delegada son eliminados, la validación DNSSEC para esa zona quedará deshabilitada.

3.6.1. ¿Quién puede solicitar la eliminación de los registros DS en la zona ".ES"?

Sólo los titulares del dominio tienen la autoridad para solicitar la eliminación de un registro DS vía un Agente Registrador o directamente a través del interfaz web.

Los Agentes registradores solo pueden eliminar un registro DS en representación del titular.

3.6.2. ¿Cómo se pueden eliminar los registro DS de un dominio?

El titular encargará al Agente Registrador la eliminación de estos registros, o bien lo hará directamente a través de la interfaz web.

El cambio de los datos asociados al dominio quedará reflejado en la siguiente generación del archivo de zona, a partir de la recepción de la solicitud de eliminación por parte de Red.es.

3.6.3. Procedimiento de eliminación de registros DS de emergencia

No hay procedimiento de eliminación de emergencia.

4. INFRAESTRUCTURA, ADMINISTRACIÓN Y CONTROLES OPERACIONALES

4.1. CONTROLES FÍSICOS

4.1.1. Ubicación Física y Controles

Los servicios *DNSSEC* ofrecidos por *Red.es* están distribuidos entre varios centros de procesamiento datos. Esto incluye salas de servidores, racks y un centro de respaldo.

4.1.2. Acceso Físico

Todas las ubicaciones tienen acceso restringido, limitado al personal autorizado

4.1.3. Corriente eléctrica y acondicionamiento climático

Los centros de procesamiento de datos dispuestos por *Red.es* disponen de sistemas de alimentación ininterrumpida (UPS) y sistema de refrigeración. Todas las ubicaciones disponen de sistemas redundantes en el caso de fallo de alimentación.

4.1.4. Protección de inundaciones

Los centros de datos están razonablemente protegidos contra inundaciones y las instalaciones están dotadas de mecanismos de detección de inundación.

4.1.5. Prevención y protección antiincendios

Todas las instalaciones tienen detectores de incendio y extintores.

4.1.6. Almacenamiento de Datos

El almacenamiento se hace de acuerdo a la política de gestión de calidad de Red.es. La clasificación de la información establece las condiciones de almacenamiento, especialmente para los datos confidenciales.

4.1.7. Respaldo Off-site

Todos los datos están respaldados automáticamente en una ubicación remota.

4.2. PROCEDIMIENTOS DE AUDITORÍA

4.2.1. Tipos de Eventos Registrados

Los siguientes eventos son registrados de manera automática por los dispositivos que componen la arquitectura *DNSSEC*:

- Todos los tipos de operaciones relativas las *HSM* como generación de claves, borrado, activación, firmado y acceso a las mismas.
- Accesos remotos permitidos y denegados.
- Operaciones que requieran privilegios administrativos.
- Acceso a las ubicaciones físicas.

4.2.2. Frecuencia de procesamiento de logs

Los logs son continuamente analizados de manera automática y manual. Se realizan inspecciones puntuales de los eventos relativos a la administración de claves, operaciones que requieran elevación de privilegios, reinicio de los equipos o anomalías.

4.2.3. Periodo de retención de los eventos de auditoría

Los eventos de log son almacenados en línea durante un periodo de tiempo al menos de 90 días. Pasado este periodo de tiempo son archivados durante un periodo de tiempo mínimo de 1 año

4.2.4. Procedimientos de copia de seguridad de los eventos de auditoría

Los datos relativos a la información de auditoría son almacenados en una copia de seguridad mensualmente.

4.2.5. Recopilación de eventos de auditoría

Toda la información contenida en los eventos de auditoría es transferida a sistemas de recolección y procesamiento en tiempo real.

4.3. RECUPERACIÓN ANTE COMPROMISO Y DESASTRE

Ante compromiso de las claves *KSK*, *ZSK,* o un desastre, se ejecutará el procedimiento de emergencia de generación de nuevas claves.

Todos los incidentes serán gestionados en base a los procedimientos definidos por *Red.es.*

Red.es dispone de procedimientos definidos para la generación de claves, publicación, firmado de zona, "*rollover*", mantenimiento de zona así como de todo equipamiento físico utilizados en el entorno *DNSSEC* y *HSM*.

Red.es se reserva el derecho proceder a la desactivación de DNSSEC cuando la estabilidad de la zona ".ES" corra algún riesgo.

El presente documento mantendrá su versión oficial en idioma castellano sin perjuicio de traducciones a otros idiomas.

4.4. TERMINACIÓN

Si Red.es debe discontinuar DNSSEC para la zona .es por alguna razón y volver a una zona no firmada, se realizará de forma ordenada con notificación pública.

Si la operación del registro .es se transfiere a un tercero, Red.es tomará parte en la transición para hacerla del mejor modo posible.

5. CONTROLES TÉCNICOS DE SEGURIDAD

5.1. GENERACIÓN DEL PAR DE CLAVES Y SU INSTALACIÓN

5.1.1. Generación del par de Claves

La generación de los pares de claves utilizados por el sistema *DNSSEC* se realizará sobre el módulo criptográfico *HSM* desde el entorno *DNSSEC* mediante protocolos de red seguros (*TLS*).

5.1.2. Distribución de la clave publica

La clave pública de KSK se exporta del sistema de firmado como parte de la ceremonia de generación de claves. Después de exportada es verificada por el RS y el AD. El RS se encarga de la publicación de dicha clave de forma segura, como se indica en la sección 2.2. El AD se encarga de chequear que la clave publicada es la misma que aquella que ha sido exportada y programada para producción, y que está funcionando como se espera.

5.1.3. Parámetros de generación y control de calidad de la clave pública.

Los parámetros de generación de la clave se definen en la política de firmado de zona (ver más abajo) y los controles de calidad incluyen la verificación de la longitud de las claves.

5.1.4. Propósito de uso de la clave

Una clave generada para DNSSEC debe ser usada únicamente para actividades de DNSSEC y nunca debe ser usada fuera de los sistemas de firmado. Una clave debe ser usada únicamente para una zona y no puede ser reutilizada.

5.2. PROTECCIÓN Y CONTROL DE LA CLAVE PRIVADA

Todas las operaciones criptográficas se realizan dentro del HSM.

5.2.1. Controles y estándar del módulo criptográfico

El hardware HSM tiene certificación FIPS 140-2 level 2.

5.2.2. Control Multi-personal de la clave Privada

Un mínimo de 2 a 5 personas se requieren para activar un módulo HSM.

5.2.3. Almacenamiento de las claves Privadas

Las claves privadas no se pueden exportar del HSM.

5.2.4. Respaldo de las claves Privadas

Las claves privadas se almacenarán en dos dispositivos criptográficos sincronizados y en los dispositivos de copia de seguridad dedicados a tal efecto.

Los datos contenidos en el módulo criptográfico *HSM* no son exportables y por lo tanto solo pueden residir en los módulos *HSM* destinados a tal efecto. No obstante

se dispone de módulos criptográficos adicionales destinados exclusivamente a la copia de seguridad de los datos de los *HSM* con medidas de seguridad en el acceso a los datos similares a la de los propios *HSM*.

5.2.5. Método de Activación de las claves Privadas

Las nuevas claves privadas serán activadas por los AD tras autorización expresa de los RS.

5.2.6. Método de Desactivación de las Claves Privadas

Las claves privadas no serán destruidas tras finalizar el periodo de vida útil. Después de su vida útil serán eliminadas del sistema de firmado.

5.3. OTROS ASPECTOS DE LA ADMINISTRACIÓN DE CLAVES.

5.3.1. Archivo Público de Claves

Las claves públicas son respaldadas y archivadas como parte del procedimiento de respaldo de Red.es.

5.3.2. Períodos de Uso de las Claves

Red.es cambiará la clave KSK cuando considere necesario. La clave ZSK se cambiará a los 90 días.

5.4. CONTROLES DE SEGURIDAD DE EQUIPOS.

El acceso a los equipos y sistemas queda registrado en el sistema de logs. El personal con acceso a estos equipos debe usar credenciales individuales.

5.5. CONTROLES DE SEGURIDAD DE REDES

El sistema de *DNSSEC* utilizado para el firmado de la zona ".*ES*" es el único sistema que tiene acceso mediante red a los módulos criptográficos de los *HSM*.

5.6. SINCRONIZACIÓN DE TIEMPO/HORA

Los equipos/sistemas utilizados en el entorno *DNSSEC* son sincronizados periódicamente mediante servicios *NTP*.

5.7. CONTROLES TÉCNICOS EN EL CICLO DE VIDA

Red.es mantendrá un sistema de monitorización constante y ejecutara procedimientos de verificación de los datos como paso previo a la publicación de los datos de zona ".*ES*" con el objetivo de validar los datos publicados.

6. FIRMADO DE LA ZONA ".ES"

El firmado de la zona de ".*ES*" utilizará los parámetros especificados a continuación.

Cualquier cambio a éstos se verá reflejado en el presente documento y será publicado según se establece en el apartado 2.1. Repositorio.

6.1. PERIODO DE VALIDEZ DE LAS CLAVES Y ALGORITMOS

- KSK: 2048 bits, RSASHA256 (algoritmo número 8).
- ZSK: 1024 bits, RSASHA256 (algoritmo número 8).

6.2. DENEGACIÓN DE EXISTENCIA AUTENTICADA.

El registro utilizará NSEC3 con opt-out (RFC 5155)

6.3. FORMATO DE FIRMA

Las firmas utilizarán RSASHA256 (algoritmo número 8).

6.4. ROTACIÓN ("ROLLOVER") DE LA ZSK ("ZONE SIGNING KEY").

Cada ZSK se mantendrá activa durante 3 meses.

6.5. ROTACIÓN ("ROLLOVER") DE LA KSK ("KEY SIGNING KEY").

En el caso de un "rollover" normal, se publicará la clave 3 meses antes de su activación, y se mantendrá por 3 meses después de haber sido desactivada. La duración de esta clave será determinada bajo los criterios que Red.es considere necesarios.

Se utilizará un procedimiento que permita la automatización del "rollover", de acuerdo al RFC 5011.

6.6. CICLO DE VIDA DE LAS FIRMAS Y FRECUENCIA DE REFIRMADO.

Las firmas de la ZSK tendrán una validez de 14 días y se refirmarán en cada zona nueva.

6.7. TIME-TO-LIVE DE LOS RR.

El TTL del DNSKEY será de 3.600 segundos.