INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

Aplicación de criptografía y seguridad (Gpo 302)

Profesores: Alberto F. Martínez

Alejandro Parra Briones

Dr. Mohd Anas Wajid

Reporte Técnico: Evaluación de la Adopción y Salud Criptográfica de DNSSEC en Dominios .MX

Reporte Tecnico.

Integrantes:

Alberto Boughton Reyes A01178500

Valeria Garcia Hernandez A01742811

Facundo Bautista Barbera A01066843

Emiliano Ruiz López A01659693

Daniel Garnelo Martinez A00573086

Monterrey N.L. 2 de diciembre de 2025

Indice

9. Conclusiones Generales

10. Recomendaciones Técnicas

11. Recomendaciones Específicas

- 11.1 Publicación del registro DS en .MX
- 11.2 Rotación y gestión de claves (KSK y ZSK)
- 11.3 Verificación de vigencia de firmas RRSIG
- 11.4 Uso adecuado de NSEC o NSEC3
- 11.5 Implementación de validación DNSSEC en resolvers internos
- 11.6 Auditoría periódica con herramientas automáticas
- 11.7 Recomendaciones específicas por sector

12. Anexos

- 12.1 Comandos utilizados para la validación manual
- 12.2 Elementos de DNSSEC utilizados en el análisis
- 12.3 Ejemplo de salida de DNSSEC correcta
- 12.4 Ejemplo de cadena incompleta
- 12.5 Ejemplo de dominio sin DNSSEC
- 12.6 Archivos generados por el analizador
- 12.7 Flujos de validación utilizados por el analizador
- 12.8 Reproducción completa del análisis

13. Bibliografía

- 13.1 RFCs (Request for Comments)
- 13.2 Documentación de ICANN y NIC México
- 13.3 Herramientas y validadores utilizados
- 13.4 Repositorios y código utilizado
- 13.5 Literatura y fuentes técnicas adicionales

Abstract

Este documento presenta una evaluación técnica sobre la adopción y la salud criptográfica de DNSSEC en dominios bajo el código de país .MX. El análisis se realizó utilizando un sistema automatizado de validación que ejecuta consultas DNS, verifica la cadena de confianza desde la raíz y revisa la conformidad con los estándares definidos en los RFC 4033, 4034 y 4035. Se examinan aspectos como la presencia de registros DNSKEY y DS, firma criptográfica de la zona, algoritmos utilizados, mecanismos de negación autenticada (NSEC/NSEC3) y consistencia operativa. Los resultados muestran una adopción limitada en la muestra analizada, con casos correctos en instituciones gubernamentales y académicas, pero una ausencia casi total en sectores financieros y comerciales. Se presentan conclusiones sobre el estado actual de DNSSEC en México y recomendaciones técnicas para su fortalecimiento.

1. Introducción

El Sistema de Nombres de Dominio (DNS) es una infraestructura distribuida encargada de traducir nombres de dominio a direcciones IP mediante una red jerárquica de servidores raíz, TLD y servidores autoritativos. Su diseño original, establecido en los RFC 1034 y 1035 en 1987, priorizó eficiencia y simplicidad sobre seguridad. Limitaciones como el uso predominante del protocolo UDP y el tamaño reducido de los mensajes facilitaron ataques de suplantación y envenenamiento de caché, evidenciados en incidentes de 1997 y, de manera significativa, en el ataque de Kaminsky en 2008.

Para mitigar estas vulnerabilidades, la IETF desarrolló DNSSEC (DNS Security Extensions), un conjunto de mecanismos criptográficos que permiten verificar la autenticidad e integridad de las respuestas DNS mediante firmas digitales y relaciones de confianza jerárquica. Su versión operativa fue formalizada en los RFC 4033, 4034 y 4035, con extensiones adicionales como NSEC3 en el RFC 5155.

El dominio .MX, gestionado por NIC México, se encuentra firmado y permite validación completa desde la raíz. Sin embargo, la activación de DNSSEC dentro de los dominios bajo .MX depende de cada titular. El presente documento evalúa la adopción real, la validez criptográfica y el cumplimiento operativo de DNSSEC en una muestra representativa de dominios .MX.

2. Fundamentos Técnicos (versión consolidada)

El Sistema de Nombres de Dominio (DNS) es una infraestructura jerárquica y distribuida encargada de traducir nombres legibles por humanos a direcciones IP. La resolución de un nombre involucra componentes como:

- **Servidores raíz (.)**, administrados por ICANN.
- **TLDs genéricos (gTLD, como .com, .org)**.
- **TLDs geográficos (ccTLD, como .mx)**, gestionados por NIC México.
- **Servidores autoritativos**, responsables de zonas específicas.
- **Servidores recursivos**, que realizan la cadena completa de consultas para un usuario final.

Cuando un usuario accede a un dominio, el resolver recursivo consulta la cadena:

Raíz → TLD → dominio → subdominio.

Cada paso devuelve referencias hasta obtener la dirección IP que permite acceder al servicio solicitado.

El DNS fue diseñado en 1987 bajo los RFC 1034 y 1035 con énfasis en eficiencia, no en seguridad. Limitaciones como el uso predominante de UDP y el tamaño reducido de mensajes facilitaron la aparición de ataques como la suplantación de respuestas DNS. Casos relevantes incluyen ataques de manipulación temprana en 1997 y, de forma más notable, el ataque de Kaminsky en 2008, que evidenció la posibilidad de envenenar cachés de manera masiva.

Para mitigar estos riesgos se desarrolló DNSSEC, un conjunto de extensiones basadas en criptografía de clave pública, formalizado en los RFC 4033, 4034 y 4035. DNSSEC introduce:

- **DNSKEY**, claves públicas de la zona.
- **RRSIG**, firmas digitales sobre conjuntos de registros.
- **DS**, vínculos criptográficos entre zona padre e hija.
- **NSEC/NSEC3**, mecanismos autenticados de negación de existencia.

La cadena de confianza se valida desde la raíz hasta el dominio final. Para los dominios bajo .mx, NIC México mantiene el TLD firmado y operativo, permitiendo validar correctamente cualquier dominio cuyo titular haya publicado su registro DS.

3. Metodología

3.1 Enfoque general

El análisis consiste en evaluar la adopción y salud criptográfica de DNSSEC en dominios .mx utilizando exclusivamente consultas públicas (OSINT) desde un servidor recursivo. Se inspeccionan:

- Presencia de DNSKEY, RRSIG, DS.
- Tipo de negación de existencia: NSEC o NSEC3.
- Algoritmos, tamaños de clave y conformidad con prácticas recomendadas.
- Existencia o ruptura de la cadena de confianza.
- Cumplimiento con parámetros definidos en RFCs evaluables.

Los resultados se consolidan en formato Markdown y JSON y posteriormente se comparan con métricas agregadas.

Favor de acceder a las herramientas/versiones/comandos usados para la realización del proyecto en anexos.

3.2 Herramientas

- Python 3 + dnspython para la recolección automatizada.
- dig +dnssec dominio para verificar firmas y claves.
- dig dominio NSEC +dnssec para identificar NSEC.
- dig dominio NSEC3PARAM +dnssec para identificar NSEC3.
- delv dominio.mx para validar la cadena íntegra.
- Validadores externos: DNSViz, Verisign DNSSEC Debugger, SIDN Labs.

4. Criterios de Validación y Lógica del Analizador

4.1 Componentes del analizador

El repositorio contiene los siguientes módulos relevantes:

- generator.py — módulo principal que coordina las consultas DNS, validaciones y generación de reportes. GitHub
- lim_advisor.py — evalúa parámetros criptográficos como algoritmo de clave, tamaño, buenas prácticas. GitHub

- rfc_validator.py — evalúa el cumplimiento contra criterios definidos a partir de los RFC aplicables a DNSSEC. GitHub

Estos componentes trabajan en conjunto para determinar, por cada dominio, su estado DNSSEC y la calidad de su configuración.

4.2 Parámetros y verificaciones que se evalúan

Para cada dominio, el analizador ejecuta las siguientes comprobaciones:

Verificación	Propósito / Qué se revisa
Presencia de DNSKEY	Comprobar que la zona defina claves públicas para firma.
Presencia de RRSIG para RRsets	Verificar que los recursos estén firmados correctamente.
Existencia de DS en la zona padre	Confirmar delegación segura desde .mx hacia el dominio hijo.
Negación de existencia autenticada (NSEC o NSEC3)	Confirmar que la zona use un mecanismo DNSSEC apropiado de negación de existencia.
Cadena de confianza completa (root → TLD → dominio)	Asegurar que la validación se puede hacer desde la raíz hasta la zona, sin eslabones faltantes.
Algoritmo y tamaño de clave aceptables (buenas prácticas)	A través de lim_advisor.py, se evalúa si las claves cumplen parámetros robustos — ej. longitud adecuada, algoritmo recomendable.

Cumplimiento de criterios RFC definidos	Mediante rfc_validator.py, se comprueba conformidad con las reglas definidas para puntuación RFC (p. ej. formato de registros, existencia de campos obligatorios, tiempos de vida, etc.).
Estado general ("Enabled", "Chain Complete/Incomplete/Failed", puntuación RFC)	Resultado agregado que indica si el dominio tiene DNSSEC activo, si su cadena es confiable, y qué tan bien está configurado según los criterios.

4.3 Definiciones usadas por el analizador para estados

La lógica del repo está formada de manera siguiente:

- **DNSSEC Enabled** → hay registros DNSKEY + al menos una firma válida (RRSIG) + delegación DS. GitHub
- **Chain Complete** → la delegación y validación desde la raíz hasta el dominio se puede realizar sin errores: DS presente en TLD, DNSKEY en la zona, firmas válidas. GitHub
- **Chain Incomplete / Disabled** → alguno de los eslabones falla: puede faltar DS, no haber firmas, o haber errores en validación. GitHub
- **RFC Score** → métrica interna calculada por rfc_validator.py, que compara configuración del dominio contra un conjunto de criterios definidos basados en estándares. Un score alto indica mejor conformidad. GitHub
- **Advertencias de configuración** → generadas por lim_advisor.py cuando, aunque DNSSEC esté habilitado, se detectan prácticas no recomendables: claves débiles, algoritmos obsoletos, firmas próximas a expirar, entre otras. GitHub

5. Interpretación de Resultados a la Luz de los Criterios

Al aplicar los criterios anteriores al conjunto de dominios analizados, los resultados indican:

- Dominios con **DNSSEC Enabled + Chain Complete + alto RFC Score** — considerados como configuraciones robustas/completas, con delegación segura y buenas prácticas criptográficas.
- Dominios con **DNSSEC Enabled pero Chain Incomplete** — tienen parte de la configuración (DNSKEY, firmas, tal vez DS) pero falla la cadena de confianza; deben

revisarse DS, delegación, expiración, firma correcta.

- Dominios con **DNSSEC deshabilitado o sin firma** — reputados como no seguros frente a spoofing o suplantación, pues no aprovechan las garantías de autenticidad e integridad.

Además, las advertencias de lim_advisor.py sirven para señalar casos en los que, aunque técnicamente "funcione", la configuración no sigue las mejores prácticas criptográficas (por ejemplo, uso de algoritmos débiles, claves cortas, renovación deficiente), lo cual reduce la confianza a largo plazo.

6. Tabla Comparativa Completa de Dominios Analizados

A continuación se presenta la tabla íntegra (**fig.2**), con todos los dominios analizados, exactamente como fueron clasificados por el analizador (generator.py), ordenados tal como aparecen en el documento de resultados.

Columnas:
DNSSEC Enabled = dominio tiene DNSSEC activo
Chain Complete = validación completa (root → TLD → dominio)
RFC Score = puntaje obtenido según los criterios del validador
RFC % = cumplimiento relativo
Status = estado final detectado
Error = si existió alguna falla de consulta

Tabla de Resultados (fig.2)

Dominio	DNSSEC Enabled	Chain Complete	RFC Score	RFC %	Status	Error
nic.mx	No	No	0/1	0.0%	success	
gob.mx	Yes	Yes	19/21	90.5%	success	
sat.gob.mx	No	No	0/1	0.0%	success	
imss.gob.mx	No	No	0/1	0.0%	success	
sep.gob.mx	Yes	No	13/18	72.2%	success	

segob.gob.mx	No	No	0/1	0.0%	success	
sre.gob.mx	No	No	0/1	0.0%	success	
banxico.gob.mx	No	No	0/1	0.0%	success	
inegi.gob.mx	No	No	0/1	0.0%	success	
conacyt.gob.mx	No	No	0/1	0.0%	success	
shcp.gob.mx	No	No	0/1	0.0%	success	
salud.gob.mx	No	No	0/1	0.0%	success	
economia.gob.mx	No	No	0/1	0.0%	success	
cfe.gob.mx	No	No	0/1	0.0%	success	
pemex.gob.mx	Yes	Yes	21/21	100.0%	success	
unam.mx	Yes	Yes	19/19	100.0%	success	
ipn.mx	Yes	No	9/13	69.2%	success	
itesm.mx	No	No	0/1	0.0%	success	
uag.mx	No	No	0/1	0.0%	success	
uanl.mx	No	No	0/1	0.0%	success	
udg.mx	Yes	No	13/18	72.2%	success	

buap.mx	No	No	0/1	0.0%	success	
uaemex.mx	No	No	0/1	0.0%	success	
uabc.mx	No	No	0/1	0.0%	success	
uach.mx	No	No	0/1	0.0%	success	
bbva.mx	No	No	0/1	0.0%	success	
banorte.com.mx	No	No	0/1	0.0%	success	
santander.com.mx	No	No	0/1	0.0%	success	
hsbc.com.mx	No	No	0/1	0.0%	success	
citibanamex.com.mx	No	No	0/1	0.0%	success	
scotiabank.com.mx	No	No	0/1	0.0%	success	
telmex.com.mx	No	No	0/1	0.0%	success	
telcel.com	No	No	0/1	0.0%	success	
televisa.com.mx	No	No	0/1	0.0%	success	
tv-azteca.com.mx	No	No	0/0	0.0%	error	Domain does not exist
liverpool.com.mx	No	No	0/1	0.0%	success	
cemex.com.mx	No	No	0/1	0.0%	success	

bimbo.com.mx	No	No	0/1	0.0%	success	
femsa.com.mx	No	No	0/1	0.0%	success	
elektra.com.mx	No	No	0/1	0.0%	success	
walmart.com.mx	No	No	0/1	0.0%	success	
coppel.com.mx	No	No	0/1	0.0%	success	
oxxo.com.mx	No	No	0/1	0.0%	success	
eluniversal.com.mx	No	No	0/1	0.0%	success	
reforma.com.mx	No	No	0/1	0.0%	success	
milenio.com	No	No	0/1	0.0%	success	
mercadolibre.com.mx	No	No	0/1	0.0%	success	
amazon.com.mx	No	No	0/1	0.0%	success	

7. Análisis General de Resultados

El conjunto completo de dominios analizados muestra un panorama heterogéneo con baja adopción general de DNSSEC dentro del ecosistema .MX, con algunas excepciones destacables en los sectores gubernamental y educativo.

7.1 Adopción de DNSSEC

A partir de la tabla comparativa:

- **Dominios con DNSSEC Enabled:**
  gob.mx, pemex.gob.mx, unam.mx, ipn.mx, sep.gob.mx, udg.mx
  (6 dominios)

- **Dominios con DNSSEC Disabled:**
  El resto de los dominios evaluados muestran 0/1 en RFC Score y ausencia total de DNSKEY, DS y RRSIG.

Esto indica que solo una fracción menor a la cuarta parte de la muestra implementa DNSSEC.

7.2 Cadena de confianza

La cadena completa (delegación segura desde .mx) se observa únicamente en:

- gob.mx
- pemex.gob.mx
- unam.mx

El resto de los dominios con DNSSEC habilitado presentan **Chain Incomplete**, lo que sugiere:

- DNSKEY presente
- Firmas presentes
- **Ausencia de DS en .mx** (causa más común)

Este patrón es típico cuando la zona está firmada, pero el titular no publica el registro DS con su proveedor o con NIC México, lo que rompe la cadena aunque DNSSEC esté técnicamente en uso.

7.3 Cumplimiento RFC (RFC Score)

Los dominios con mejores prácticas son:

- pemex.gob.mx — **21/21 (100%)**
- unam.mx — **19/19 (100%)**

Ambos casos reflejan:

- DNSKEY completo
- DS publicado
- RRSIG válido

- NSEC/NSEC3 operativo
- Firmas vigentes
- Algoritmos aceptados
- Cadena íntegra

Otros dominios muestran puntuaciones medias por cumplir parcialmente los criterios, normalmente por falta de DS.

7.4 Casos representativos

- **gob.mx**: Alto cumplimiento (19/21) y cadena completa. Configuración estable.
- **pemex.gob.mx**: Ejemplo de implementación correcta y madura.
- **unam.mx**: Caso sobresaliente en el sector educativo.
- **ipn.mx**, **udg.mx**, **sep.gob.mx**: Tienen DNSSEC activo pero sin cadena completa, probablemente por falta de DS.
- Sectores banca, comercio y medios de comunicación: **sin adopción** en toda la muestra.

8. Análisis Sectorial

8.1 Sector Gubernamental (.gob.mx)

Implementación mixta:

- **Con DNSSEC completo o parcial**: gob.mx, pemex.gob.mx, sep.gob.mx
- **Sin DNSSEC**: la mayoría (sat.gob.mx, imss.gob.mx, banxico.gob.mx, segob.gob.mx, etc.)

Aunque existen casos correctos, la adopción general sigue siendo baja considerando el impacto de estas instituciones.

8.2 Sector Educativo (.mx)

Tres instituciones principales aparecen con DNSSEC habilitado:

- **Correcto y completo**: unam.mx

- **Parcial (sin DS)**: ipn.mx, udg.mx
- **Sin DNSSEC**: uanl.mx, buap.mx, uabc.mx, uach.mx, uaemex.mx

Existe avance, pero no de forma uniforme.

8.3 Sector Financiero

Dominios como:

- bbva.mx
- banorte.com.mx
- hsbc.com.mx
- santander.com.mx
- citibanamex.com.mx
- scotiabank.com.mx

Todos aparecen sin DNSSEC.
Esto es relevante, considerando su perfil de riesgo y la criticidad en integridad de DNS.

8.4 Sector Comercial

Empresas como:

- walmart.com.mx
- femsa.com.mx
- bimbo.com.mx
- oxxo.com.mx
- liverpool.com.mx
- amazon.com.mx
- mercadolibre.com.mx

Tampoco muestran adopción de DNSSEC.

9. Conclusiones Generales

1. **La adopción de DNSSEC en la muestra analizada es baja**, con solo unos pocos dominios mostrando configuraciones completas.

2. Los casos de buena implementación confirman que DNSSEC es viable técnicamente y operativo en el ecosistema .mx.

3. La falta de registro DS es el fallo más común entre dominios parcialmente habilitados.

4. Sectores críticos, como finanzas y comercio electrónico, muestran ausencia total de DNSSEC en esta muestra.

5. La presencia de configuraciones completas en entidades como PEMEX, UNAM y el portal de gobierno demuestra que existen buenas prácticas dentro del país, pero no están generalizadas.

10. Recomendaciones Técnicas

Las siguientes recomendaciones se derivan directamente del análisis realizado y están alineadas con las mejores prácticas definidas por la IETF, NIC México y operadores DNS con experiencia en despliegues DNSSEC.

11 Publicación del registro DS en .MX

En todos los dominios que presentan:

- DNSKEY presente
- RRSIG presente
- **Pero Chain Incomplete**

la causa más común es la **ausencia del registro DS en la zona padre .mx**.

La corrección consiste en:

1. Obtener el **DS** correspondiente a la KSK de la zona.
2. Publicarlo en el panel del registrador o integrarlo a través del proveedor DNS.
3. Confirmar la propagación mediante dig +dnssec dominio DS.

Esto restablece la cadena de confianza y permite la validación completa desde la raíz.

11.2 Rotación y gestión de claves (KSK y ZSK)

Las claves deben rotarse periódicamente para evitar debilidades criptográficas y cumplir con prácticas modernas:

- Rotación recomendada de **ZSK**: entre 30 y 90 días.
- Rotación recomendada de **KSK**: entre 6 y 12 meses.
- Mantener ambas claves con algoritmos seguros como:
    - **RSA 2048+**
    - **ECDSA P-256 / P-384**
    - **Ed25519** (altamente recomendado por su eficiencia y robustez)

El uso de RSA 1024 o algoritmos obsoletos debe evitarse.

11.3 Verificación de vigencia de firmas RRSIG

Varias interrupciones en la validación suelen deberse a **firmas caducadas** o con TTLs incorrectos.

Se recomienda:

- Supervisar el tiempo de expiración (RRSIG expiration)
- Automatizar la regeneración de firmas
- Configurar alertas internas cuando falten menos de 3–5 días para expirar

Mantener firmas vigentes es esencial para evitar fallos de validación imprevistos.

11.4 Uso adecuado de NSEC o NSEC3

Para la negación de existencia:

- **NSEC3** con iteraciones bajas y saltos aleatorios suele ser preferible en dominios de mayor visibilidad, ya que dificulta la enumeración de zona.

- **NSEC** es aceptable para zonas públicas sin sensibilidad en nombres.
- Evitar configuraciones sin mecanismo autenticado (NXDOMAIN no firmado).

Revisar los parámetros del hash NSEC3 para evitar reiteraciones excesivas que perjudiquen el rendimiento.

11.5 Implementación de validación DNSSEC en resolvers internos

Incluso si un dominio firma su zona correctamente, la protección real se materializa cuando los resolvers validan.

Se recomienda que instituciones que administran dominios críticos:

- Usen resolvers que validen DNSSEC (Unbound, Knot Resolver, BIND)
- Habiliten val-permissive-mode no
- Distribuyan estos resolvers a usuarios internos

Esto reduce la exposición a ataques de envenenamiento de caché.

11.6 Auditoría periódica con herramientas automáticas

Para mantener configuraciones sanas:

- Ejecutar validadores como DNSViz, Verisign DNSSEC Analyzer y SIDN Labs
- Revisar advertencias sobre TTL, expiraciones, inconsistencias entre servidores NS, etc.
- Programar auditorías trimestrales en dominios gubernamentales, financieros o de alta disponibilidad

El objetivo es prevenir caídas inesperadas por firmas caducadas o malas configuraciones de delegación.

11.7 Recomendaciones específicas por sector

Gobierno

Fortalecer la adopción uniforme de DNSSEC en todas las dependencias, especialmente en servicios críticos como finanzas, identidad y servicios sociales.

Educación

Publicar el DS en los dominios que ya tienen DNSSEC operativo (ej. IPN, UDG), lo que permitiría obtener cadenas completas.

Finanzas

Dado su perfil de riesgo, los bancos deben considerar implementar DNSSEC antes que otros sectores, especialmente para proteger contra ataques de spoofing en subdominios sensibles (login, transacciones).

Comercio electrónico

En sitios de alto tráfico, DNSSEC complementa medidas existentes (HTTPS, HSTS, DNS sobre TLS) aportando integridad contra redirecciones maliciosas en etapa temprana.

12. Anexos

Los siguientes anexos proporcionan material de referencia técnica para comprender y reproducir el análisis DNSSEC realizado, así como para interpretar los resultados obtenidos para cada dominio.

12.1 Comandos utilizados para la validación manual

Estos comandos permiten replicar cualquier parte del análisis de manera independiente al analizador.

Consulta general con DNSSEC

dig +dnssec dominio.mx

Muestra:

- Registros RRSIG si existen
- DNSKEY si están solicitados por implicación
- Indicador de autenticación (ad flag) cuando el resolver valida

Consulta directa de DNSKEY

dig dominio.mx DNSKEY +dnssec

Permite:

- Ver claves públicas
- Identificar KSK y ZSK
- Confirmar algoritmos

Verificación de delegación segura (DS)

dig dominio.mx DS +dnssec

Confirma si el dominio ha publicado su DS en .mx.

Ausencia de DS → cadena incompleta.

Negación de existencia (NSEC / NSEC3)

dig dominio.mx NSEC +dnssec
dig dominio.mx NSEC3PARAM +dnssec

- Respuesta NSEC → listado claro de la vecindad en el espacio de nombres
- Respuesta NSEC3 → negación con hashing

Validación completa de cadena

delv dominio.mx

Este comando realiza validación DNSSEC end-to-end y muestra el motivo exacto de fallas.

12.2 Elementos de DNSSEC utilizados en el análisis

DNSKEY

Contiene claves públicas utilizadas para firmar registros.
Tipos principales:

- **KSK (Key Signing Key)** — firma el DNSKEY RRset
- **ZSK (Zone Signing Key)** — firma el resto de los registros (A, AAAA, MX...)

RRSIG

Firmas digitales aplicadas a cada conjunto de registros.

Permiten verificar integridad y autenticidad.

DS (Delegation Signer)

Ubicado en el TLD.

Vincula criptográficamente el dominio padre con el hijo.

Si falta, la cadena queda incompleta.

NSEC / NSEC3

Mecanismos de *denial of existence*:

- **NSEC** — enumera dominios vecinos
- **NSEC3** — oculta la estructura mediante hashing

Ambos deben estar firmados.

Cadena de confianza

Ruta de validación completa:

Root → .mx → dominio.mx → subdominio

Debe existir:

- Firma de la raíz
- DS en .mx
- DNSKEY y RRSIG válidos en el dominio

12.3 Ejemplo de salida de DNSSEC correcta

Un dominio con DNSSEC completo muestra:

```
;; flags: qr rd ad ; AD = authenticated data
...
dominio.mx.   3600 IN DNSKEY ...
dominio.mx.   3600 IN RRSIG DNSKEY ...
mx.           3600 IN DS <hash>
dominio.mx.   3600 IN RRSIG A ...
dominio.mx.   3600 IN NSEC3 ...
```

Indicadores clave:

- Flag ad activado
- DS presente
- RRSIGs vigentes
- DNSKEY consistente con DS
- NSEC/NSEC3 presente

12.4 Ejemplo de cadena incompleta

Caso típico:

```
dominio.mx.  IN DNSKEY ...
dominio.mx.  IN RRSIG ...
;; NO DS record found for dominio.mx
```

Causa común:

- Zona firmada pero sin DS en .mx
- El analizador marca esto como **Enabled / Chain Incomplete**

12.5 Ejemplo de dominio sin DNSSEC

```
dominio.mx.  IN A ...
;; no DNSKEY
;; no RRSIG
```

Resultado:

- DNSSEC Disabled
- RFC Score mínimo (0/1)

12.6 Archivos generados por el analizador

La ejecución de generator.py produce:

a) Reportes por dominio (.md)

Incluyen:

- DNSKEY
- RRSIG
- DS
- Tipo de NSEC/NSEC3
- Algoritmos
- RFC Score
- Estado final

b) Resumen global (_summary.json)

Para cada dominio contiene:

- dnssec_enabled
- chain_complete
- rfc_score
- rfc_score_max
- status
- nsec_type
- key_algorithms

Este archivo es la base para todas las tablas del reporte.

12.7 Flujos de validación utilizados por el analizador

Validación criptográfica (lim_advisor.py)

Evalúa:

- Algoritmo (RSA/ECDSA/Ed25519)
- Longitud de clave
- Uso correcto de KSK/ZSK
- Señales de clave débil o obsoleta

Validación RFC (rfc_validator.py)

Evalúa criterios como:

- Presencia de RRSIG
- Vigencia de firmas
- Correcta asociación DS ↔ DNSKEY

- Formatos y campos obligatorios
- Existencia de negación de existencia autenticada

12.8 Reproducción completa del análisis

Para duplicar el proceso:

1. Preparar domains.txt
2. Ejecutar:

python3 analyzer/generator.py domains.txt

3. Ver resultados en /output/ o carpeta equivalente:
    - <dominio>.md
    - _summary.json
4. Comparar puntajes y estados según el reporte.

13. Bibliografía

La siguiente bibliografía reúne los documentos técnicos, estándares y fuentes formales utilizados para fundamentar el análisis de DNSSEC, su funcionamiento, las prácticas recomendadas y los criterios aplicados durante la validación de los dominios evaluados.

13.1 RFCs (Request for Comments)

DNS (Base del Sistema de Nombres de Dominio)

- Mockapetris, P. (1987).
  RFC 1034 – Domain Names: Concepts and Facilities.
  Internet Engineering Task Force (IETF).
- Mockapetris, P. (1987).
  RFC 1035 – Domain Names: Implementation and Specification.
  IETF.

DNSSEC (Especificaciones principales)

- Arends, R., et al. (2005).
  RFC 4033 – DNS Security Introduction and Requirements.

- Arends, R., et al. (2005).
  RFC 4034 – Resource Records for DNS Security Extensions.

- Arends, R., et al. (2005).
  RFC 4035 – Protocol Modifications for DNSSEC.

Complementos y actualizaciones relevantes

- Laurie, B., et al. (2008).
  RFC 5155 – DNSSEC Hashed Authenticated Denial of Existence (NSEC3).

- D. J. Bernstein, et al. (2012).
  RFC 5702 – Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG.

- IETF DNSOP Working Group (diversos).
  Documentos de operación recomendada y prácticas contemporáneas.

13.2 Documentación de ICANN y NIC México

- **ICANN – Root DNSSEC Deployment**
  Información técnica sobre la firma de la zona raíz y su operación global.

- **NIC México – DNSSEC en .MX**
  Documentación y lineamientos sobre la administración del ccTLD .MX y su firma DNSSEC.

- **Root Zone Management – Procedures and Key Signing Ceremonies**
  Documentación oficial sobre la gestión de claves y ceremonias criptográficas.

13.3 Herramientas y validadores utilizados

- **DNSViz – DNS Visualization Tool**
  https://dnsviz.net/
  Visualizador gráfico del estado DNSSEC y dependencias entre zonas.

- **Verisign DNSSEC Debugger**
  https://dnssec-debugger.verisignlabs.com/
  Validador diagnóstico para cadenas de confianza.

- **SIDN Labs – DNSSEC Tools**
  https://tools.sidnlabs.nl/
  Herramientas de análisis de firmas, DS, algoritmos y configuración avanzada.

- **delv (Domain Entity Lookup & Validation)**
  Herramienta oficial de validación DNSSEC incluida en BIND 9.

- **dnspython**
  Librería utilizada para consultas programáticas dentro del analizador.

13.4 Repositorios y código utilizado

- **DNSSEC Analyzer – Rama Reportes**
  https://github.com/Facundo-Barbera/DNSSEC-Analyzer/tree/Reportes
  Repositorio utilizado para la ejecución del módulo generator.py y sus dependencias (lim_advisor.py, rfc_validator.py).

- **Scripts y outputs derivados**
  Estructura completa del analizador, incluyendo:

  - analyzer/generator.py
  - analyzer/lim_advisor.py
  - analyzer/rfc_validator.py
  - Reportes generados en .md
  - _summary.json

13.5 Literatura y fuentes técnicas adicionales

- Kaminsky, D. (2008).
  Presentación del ataque de cache poisoning que impulsó la adopción de DNSSEC.

- Crocker, D., et al.
  Publicaciones históricas sobre vulnerabilidades y evolución del DNS.

- Documentos educativos de la IETF y DNSOP relacionados con despliegues DNSSEC modernos.