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

DNSSEC compliance de dominios bajo .mx

Versión Tecnica.

Integrantes:

Alberto Boughton Reyes A01178500

Valeria Garcia Hernandez A01742811

Facundo Bautista Barbera A01066843

Emiliano Ruiz López A01659693

Daniel Garnelo Martinez A00573086

Monterrey N.L. 25 de noviembre de 2025

Reporte Técnico Reto

Introducción:

Objetivos del reto:

- Se busca evaluar el estado de implementación y conformidad de DNSSEC en un conjunto de dominios usando escáneres automatizados.
- Verificar la presencia y propiedades de DNSKEY, RRSIG, DS, NSEC/NSEC3, parametros NSEC3PARAM y elementos de la cadena de confianza padre hijo.
- Detectar problemas operativos como claves con tamaños sospechosos, firmas caducadas, ausencia de DS en los padres, uso de NSEC3 opt-out, o una ausencia directa de DNSSEC
- Generar reportes legibles (markdown + json) y un árbol DNS que demuestre la jerarquía y dominios con un DNSSEC válido.

Activos involucrados:

- Dominios de la lista
- Resolver DNS empleado
- Máquina por la que se ejecutó el script, red y librería
- Archivos de salida como Markdown por dominio con todo el conjunto

Alcance de las pruebas realizadas:

- El análisis es no intrusivo debido a que únicamente realiza consultas DNS estándar (SOA, A, AAAA, MX, DNSKEY, NS, SD, NSEC/NSEC3/NSEC3PARAM)
- Alcance: Revisa metadatos relevantes como algoritmos, tamaños de clave, existencia de DS, expiración de firmas y tipo de negación de existencia de registros.
- Limitaciones: No realiza una validación criptográfica completa ni pruebas paralelas masivas.

Semblanza técnica de DNS y DNSSEC:

- DNS: Sistema de resolución de nombres que mapea nombres legibles a recursos. La jerarquía ba desde la raiz a TDL al dominio
- DNSSEC: Extensión DNS que añade firmas digitales y claves públicas, registros DS que enlazan las claves hijo con la cadena de confianza. Provee autenticidad e integridad de respuestas DNS. Para negar existencias se usan NSEC o NSEC3.

Desarrollo: Cómo generaron su entorno de pruebas, qué pruebas
hicieron, cómo recopilaron la información

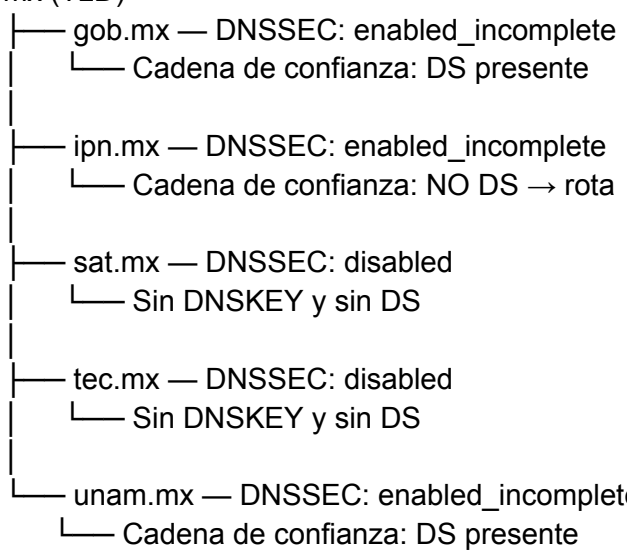
Entorno de pruebas:

- Entorno mínimo: máquina Linux o Windows con Python versiones 3.8+, librería dnspython instalada (pip install dnspython)
- Archivo domains_file.txt con la lista de dominios proporcionado en el GitHub
- Script dnssec_analizador.py configurado con:
    - nameserver: IP del resolver la cual es 8.8.8.8 por defecto
    - delay_seconds: Espera definida para evitar rate-limits
    - timeout: tiempo máximo por consulta

Resultados:

Dominio	DNSSEC Habilitado	DNSKEY	DS en padre	RRSIG	NSEC/NSEC3	Algoritmos	Validación
gob.mx	Sí	2	Sí	NA	NINGUNO (solo NSEC3PARAM)	RSA/SHA-256	enabled_incomplete
ipn.mx	Sí	2	NA	NA	NINGUNO (solo NSEC3PARAM)	RSA/SHA-512	enabled_incomplete
sat.mx	NA	0	NA	NA	NINGUNO	—	disabled
tec.mx	NA	0	NA	NA	NINGUNO	—	disabled
unam.mx	Sí	2	Sí	NA	NSEC	ECDSA-P256	enabled_incomplete

Árbol DNS:



Análisis por dominio:

- gob.mx

Estado: enabled_incomplete

Fortalezas	Problemas encontrados	Evaluacion IETF
Tiene DNSKEY (KSK RSA 2080 bits, ZSK RSA 1056 bits). Tiene DS en el TLD (.mx) → la cadena de confianza existe. Usa RSA/SHA-256, permitido por IETF.	NO existen RRSIG → la zona no está firmando los RRsets actualmente. No hay NSEC ni NSEC3, solo un NSEC3PARAM, lo cual es inconsistente: Tener NSEC3PARAM sugiere zona NSEC3, pero no existe ningún registro NSEC3 → zona no firmada o firma interrumpida.	Algoritmos: aceptables. Firmas activas: incumple. Cadena completa: sí existe. Negación de existencia: ausencia. Gestión de claves: KSK/ZSK separados correctamente.

Conclusion: La zona tiene DNSSEX configurado sin embarglo las firmas estan deshabilitadas o han caducado, por lo que la validacion es incompleta.

- ipn.mx

Estado: enabled_incomplete

Fortalezas	Problemas encontrados	Evaluacion IETF
DNSKEY presente (RSA/SHA-512 con KSK+ZSK). Algoritmo fuerte y permitido por IETF.	Sin DS en .mx → cadena de confianza rota. Sin RRSIG → zona no firmada. Solo presenta NSEC3PARAM pero no NSEC/NSEC3 → configuración incompleta.	Algoritmos: fuerte (RSA/SHA-512). Cadena: rota. Firmas activas: ausentes. Negación de existencia: no implementada.

Conclusion: La zona parece haber tenido DNSSEC anteriormente sin embargo, actualmente no firma y no tiene DS, por loq ue no se puede autentificar.

- sat.mx

Estado: disabled

Hallazgos

No tiene DNSKEY. No tiene DS. No tiene RRSIG. No tiene NSEC/NSEC3.

Conclusion: El SAT no cuenta con DNSSEC en absoluto

- tec.mx

Estado: disabled

Fortalezas
Sin DNSKEY Sin DS Sin RRSIG Sin NSEC/NSEC3

Conclusiones:El tec tampoco implementa con DNSSEC en absoluto

- unam.mx

Estado: enabled_incomplete

Fortalezas	Problemas encontrados	Evaluacion IETF
Tiene DNSKEY con ECDSA-P256, moderno y eficiente. Tiene DS en .mx → cadena existente. Presenta NSEC, que cumple negación de existencia.	RRSIG ausentes → zona no firmada actualmente. Esto es crítico: aunque hay DNSKEY y DS, sin RRSIG no existe protección criptográfica del contenido.	Algoritmos: recomendados. Cadena: completa. Firmas: ausentes. Negación de existencia: con NSEC. Gestión de claves: correcta separación KSK/ZSK.

Conclusiones: La UNAM tiene una configuración completa, sin embargo, la ausencia de RRSIG implica que el DNSSEC no esta completamente operativo.

Conclusiones de los resultados:
En este caso los dominios de gob.mx y unam.mx si funcionan, pues tienen DNSKEY y DS así como una estructura correcta aunque no firman o que no tiene RRSIG, por otro lado, ipn.mx tiene buenas claves, pero cadena rota y zonas sin firmar.

Los dominios que en general no funcionan son sat.mx y tec.mx, ya que directamente no implementan DNSSEC, aparte en todos los dominios con DNSSEC activado les falta el RRSIG, lo cual significa que ningún dominio está totalmente protegido.

Recomendaciones técnicas:

Para dominios con DNSSEC incompleto: gob.mx, ipn.mx, unam.mx

1. Regenerar y publicar RRSIG para activar la firma real
2. Revisar la automatización del signer
3. Validad que las claves KSK y ZSK están activas y bien publicadas.
4. Probar las zonas con herramientas externas como verisign DNSSEC Analyzer o dnsviz.net
5. En específico ipn.mx se puede publicar el DS en .mx

Para dominios sin DNSSEC como sat.mx y tec.mx

1. Implementar DNSSEC desde cero siguiendo el RFC 4033 - 4035
2. Generar el KSK/ZSK y configurar la política de rotación
3. Publicar el DS en el TLD

Referencias

Anexos:
https://github.com/Facundo-Barbera/cripto-5to