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 Técnico.

Integrantes:
Alberto Boughton Reyes A01178500
Valeria García Hernández A01742811
Facundo Bautista Barbera A01066843
Emiliano Ruiz López A01659693
Daniel Garnelo Martínez A00573086

Socio formador: NIC México
Representante: César Steve Salas Santos

Monterrey N.L. 2 de diciembre de 2025

Índice

Resumen

Este documento presenta una evaluación técnica sobre la adopción y la salud criptográfica de Domain Name System Security Extensions (DNSSEC) en dominios bajo el código de país .mx. El análisis se llevó a cabo con un sistema automatizado de validación que emite consultas Domain Name System (DNS), reconstruye la cadena de confianza desde la raíz y contrasta la operación contra los Request for Comments (RFC) 4033, 4034 y 4035. Se revisaron la presencia de registros Domain Name System Key (DNSKEY) y Delegation Signer (DS), la firma criptográfica de la zona mediante Resource Record Signature (RRSIG), los algoritmos empleados, los mecanismos de negación autenticada Next Secure (NSEC/NSEC3) y la consistencia operativa de cada dominio. La muestra revela una adopción limitada con casos funcionales en instituciones gubernamentales y académicas, mientras que los sectores financiero y comercial prácticamente no exponen DNSSEC activo. Con base en la evidencia recopilada se plantean conclusiones sobre el estado actual de DNSSEC en México y recomendaciones técnicas para fortalecer su despliegue.

1. Introducción

El Sistema de Nombres de Dominio (DNS) es una infraestructura distribuida cuya función es traducir nombres de dominio a direcciones Internet Protocol (IP) a través de capas jerárquicas que incluyen servidores raíz, dominios de nivel superior (TLD) y servidores autoritativos. Su diseño original, descrito en los Request for Comments (RFC) 1034 y 1035, priorizó la eficiencia y la simplicidad, dejando en segundo plano los mecanismos de seguridad (Mockapetris, 1987a, 1987b). El uso predominante de User Datagram Protocol (UDP) y el tamaño reducido de los mensajes facilitaron ataques de suplantación y envenenamiento de caché, visibles desde finales de los noventa y confirmados masivamente con el ataque de Kaminsky en 2008.

Para mitigar estas vulnerabilidades la Internet Engineering Task Force (IETF) desarrolló DNSSEC, un conjunto de extensiones basadas en criptografía de clave pública que permiten verificar la autenticidad e integridad de las respuestas DNS mediante firmas digitales y relaciones de confianza jerárquica. La operación se formalizó en los RFC 4033, 4034 y 4035 (Arends et al., 2005a, 2005b, 2005c), con extensiones posteriores como Next Secure 3 (NSEC3) descritas en el RFC 5155 (Laurie et al., 2008) y la adopción de SHA-2 para DNSKEY plasmada en el RFC 5702 (Bernstein et al., 2012). En el ecosistema mexicano, Network Information Center México (NIC México) administra únicamente el ccTLD `.mx` y mantiene esa zona firmada para habilitar la validación completa desde la raíz; cada país conserva su propio operador para los demás ccTLD. No obstante, la activación final depende de que cada titular publique los registros correspondientes dentro de su zona. Este documento evalúa la adopción real, la validez criptográfica y el cumplimiento operativo de DNSSEC en una muestra representativa de dominios `.mx`.

2. Fundamentos Técnicos

El DNS funciona como una base de datos distribuida en la que los servidores raíz hospedan la referencia de los TLD administrados por la Internet Corporation for Assigned Names and Numbers (ICANN, 2019), estos a su vez delegan la resolución hacia los servidores autoritativos responsables de cada zona, y finalmente los servidores recursivos ejecutan la cadena completa de consultas para los usuarios finales. Cuando un usuario solicita un dominio, el resolver recursivo consulta primero la raíz, recibe la referencia al TLD (.mx en este caso), continúa hacia el servidor autoritativo del dominio y concluye en el subdominio requerido hasta recuperar la dirección IP que habilita el servicio. Cada eslabón suministra la información necesaria para el siguiente paso, lo que permite mantener la estructura jerárquica y distribuir la carga.

El diseño original de 1987 favoreció la eficiencia de los mensajes sobre UDP y no consideró autenticación de respuestas, lo que permitió ataques de suplantación y envenenamiento de caché documentados en 1997 y popularizados por el ataque de Kaminsky. DNSSEC surgió como respuesta mediante la incorporación de registros DNSKEY que contienen las claves públicas de la zona, firmas RRSIG que protegen los conjuntos de registros, enlaces DS que conectan criptográficamente a la zona padre con la hija y mecanismos de negación autenticada como NSEC y NSEC3 (Arends et al., 2005a, 2005b, 2005c; Laurie et al., 2008). Con estos elementos se forma una cadena de confianza que parte de la raíz y permite validar cada respuesta, apoyada en procedimientos formales de manejo de claves documentados por la IANA (IANA, s.f.). Para dominios bajo .mx, NIC México mantiene el TLD firmado, de modo que cualquier dominio hijo puede ser validado siempre que su titular publique el registro DS asociado a su Key Signing Key (KSK) (NIC México, s.f.).

3. Metodología

3.1. Enfoque general

El análisis se basa en consultas públicas realizadas desde un servidor recursivo que actúa como fuente de inteligencia abierta. Para este estudio se utilizó el servidor DNS público de Google (8.8.8.8) como resolutor recursivo. El flujo comienza preparando el entorno con Python 3 y las dependencias incluidas en el repositorio DNSSEC Analyzer disponible en GitHub (ver Sección 14). Tras clonar el repositorio se instalan las bibliotecas descritas, entre ellas `dnspython`, y se verifican utilidades del sistema como `dig` y `delv`. La muestra de dominios se coloca en un archivo de texto plano, por ejemplo `domains.txt`, que sirve como insumo para el módulo principal.

La ejecución se realiza mediante `python3 analyzer/generator.py domains.txt`, comando que lanza el proceso completo de recolección y validación. El script aplica un saneamiento previo de cada dominio (eliminando protocolos, rutas y mayúsculas), ejecuta una verificación *pre-flight* para descartar NXDOMAIN o zonas sin nombres de servidor y, solo cuando la respuesta es positiva, emite las consultas DNSSEC completas. Cada dominio genera un

bloque de evidencia con registros DNSKEY, DS, RRSIG y, en caso de respuestas negativas, NSEC/NSEC3, además de metadatos como códigos de error, tiempos de respuesta y direcciones de los servidores autoritativos a los que se recurrió. Los resultados se almacenan en carpetas individuales en formato Markdown y se consolidan en el archivo `_summary.json`, el cual alimenta las tablas y gráficas del presente reporte.

El módulo `rfc_validator.py` se ejecuta sobre dicho resumen para evaluar criterios concretos de los RFC 4033, 4034, 4035, 5155 y 5702: presencia de firmas, vigencia de las ventanas temporales, correlación DS-DNSKEY, elección de algoritmos y coherencia de los TTL. Cada dominio obtiene una puntuación parcial y una etiqueta de estado que luego se interpreta en las secciones de resultados. Para garantizar la reproducibilidad, cada paso del pipeline queda documentado en la estructura de carpetas del proyecto y se resume visualmente en la Figura 1.

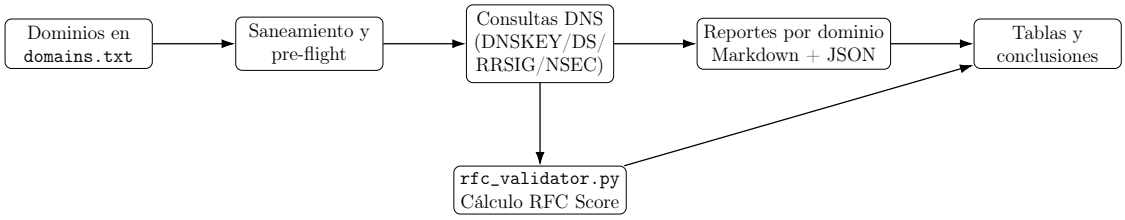

Figura 1: Flujo de procesamiento automatizado empleado para generar la evidencia técnica.

Además de la automatización, se emplean consultas manuales para confirmar hallazgos y comprender el origen de los fallos. La verificación más general se ejecuta con `dig +dnssec dominio.mx` para observar el estado de las firmas. La extracción de claves se realiza con `dig dominio.mx DNSKEY +dnssec`, mientras que la presencia del registro DS en la zona padre se comprueba usando `dig dominio.mx DS +dnssec`. Para determinar el mecanismo de negación autenticada se emplean `dig dominio.mx NSEC +dnssec` y `dig dominio.mx NSEC3PARAM +dnssec`, y para revisar la validación completa desde la raíz se ejecuta `delv dominio.mx`. Los resultados manuales se comparan con los emitidos por el analizador para confirmar que la lógica automatizada refleja el estado real de los dominios.

3.2. Herramientas

El trabajo combina las capacidades de Python 3 y la librería `dnspython`, encargada de emitir las consultas programáticas para cada registro. La utilería `dig` con la opción `+dnssec` permite revisar firmas y claves directamente desde el sistema operativo y sirve como referencia independiente. Las consultas específicas de NSEC y NSEC3PARAM ayudan a diferenciar el mecanismo de negación autenticada implementado en cada dominio. La herramienta `delv`, incluida en Berkeley Internet Name Domain (BIND), ejecuta la validación completa y detalla cualquier ruptura de la cadena de confianza. Para enriquecer el diagnóstico se contrastan los hallazgos con validadores externos como DNSViz, el DNSSEC Debugger de Verisign y los laboratorios de Stichting Internet Domeinregistratie Nederland (SIDN), los cuales ofrecen visualizaciones y advertencias adicionales. Para reproducir el entorno completo también es

necesario contar con Docker Desktop actualizado, ya que la aplicación puede levantarse mediante `docker compose` (ver Anexo 13).

4. Criterios de Validación y Lógica del Analizador

4.1. Componentes del analizador

El repositorio integra dos módulos principales dentro de la carpeta `analyzer`. `generator.py` implementa la clase `DNSSECAnalyzer`, la cual define el resolutor recursivo, maneja cachés para evitar consultas repetidas y ofrece métodos como `check_domain_status()` y `_detect_nsec_from_nxdomai` para caracterizar cada dominio antes y durante la prueba. A partir de ahí coordina las consultas de DNSKEY, DS, RRSIG, NSEC/NSEC3 y genera, para cada conjunto de registros, estructuras JSON con la clave pública, algoritmo, tamaño y vigencias detectadas. También documenta condiciones excepcionales (NXDOMAIN, SERVFAIL, timeouts) y captura los mensajes de advertencia emitidos por los servidores autoritativos.

Por su parte, `rfc_validator.py` consume la salida consolidada y valida los criterios definidos para la puntuación RFC: verifica la alineación DS-DNSKEY, calcula si las firmas expiran dentro de un umbral riesgoso, revisa si existe un mecanismo auténtico de negación de existencia y clasifica los errores más frecuentes. Ambos módulos alimentan los reportes en Markdown y los tabulados que se incluyen en este documento, permitiendo que cada hallazgo traceable tenga su evidencia directa en el repositorio.

4.2. Parámetros y verificaciones que se evalúan

La Tabla 1 resume cada verificación aplicada automáticamente y el propósito puntual que persigue dentro de la evaluación de DNSSEC, lo que permite rastrear los hallazgos descritos en las secciones siguientes.

Cuadro 1: Criterios evaluados por el analizador

Verificación	Propósito / Qué se revisa
Presencia de DNSKEY	Comprobar que la zona defina claves públicas necesarias para la firma DNSSEC.
Presencia de RRSIG para RRsets	Verificar que los conjuntos de registros estén firmados (solo presencia del RRSIG).
Existencia de DS en la zona padre	Confirmar delegación segura desde .mx (u otro TLD) hacia el dominio hijo.
Negación de existencia autenticada (NSEC o NSEC3)	Confirmar que la zona usa un mecanismo DNSSEC válido para respuestas sin existencia.

Verificación	Propósito / Qué se revisa
Cadena de confianza completa (root → TLD → dominio)	Asegurar que la cadena pueda validarse desde la raíz hasta la zona sin eslabones faltantes.
Algoritmo y tamaño de clave (buenas prácticas)	Revisar si las claves usan parámetros adecuados según lo obtenido por `generator.py`.
Cumplimiento de criterios RFC definidos	Mediante `rfc_validator.py`, se comprueba conformidad con las reglas definidas para puntuación RFC (formato de registros, existencia de campos obligatorios, tiempos de vida, etc.).
Estado general	Resultado agregado que resume si el dominio tiene DNSSEC activo, si la cadena es confiable y su puntuación RFC.

4.3. Definiciones usadas por el analizador para estados

Se considera que un dominio tiene *DNSSEC Enabled* cuando publica al menos un conjunto valido de DNSKEY, mantiene al menos una firma RRSIG válida y cuenta con delegación DS en la zona padre. El estado *Chain Complete* aparece cuando la validación puede ejecutarse desde la raíz hasta la zona sin interrupciones, lo que implica DS en .mx, DNSKEY disponible y firmas vigentes. El estado *Chain Incomplete* o *Disabled* refleja fallas en alguno de esos eslabones. La puntuación *RFC Score* es una métrica interna calculada por `rfc_validator.py` que evalúa qué tanto cumple el dominio con los criterios en los RFC relevantes (formato, obligatoriedad de campos, tiempos de vida, etc).

5. Interpretación de Resultados a la Luz de los Criterios

Una configuración robusta se caracteriza por mostrar *DNSSEC Enabled*, *Chain Complete* y una puntuación RFC alta; en ese escenario la delegación está asegurada, las firmas son válidas y no existen prácticas criptográficas cuestionables. Cuando un dominio aparece como *Enabled* pero con *Chain Incomplete*, suele existir DNSKEY y firmas, pero falta el registro DS en .mx o la delegación presenta errores, lo que impide construir la cadena de confianza. Por último, los dominios sin DNSSEC activo mantienen RFC Score mínimos y son vulnerables a ataques de suplantación y manipulación de caché porque no proporcionan garantías de autenticidad.

Las advertencias adicionales indican aspectos a corregir aun cuando el estado general parezca satisfactorio. Claves con tamaños reducidos, algoritmos obsoletos o firmas próximas a expirar disminuyen la ventana de seguridad y pueden provocar rupturas inesperadas. Estos indicadores facilitan la priorización de tareas correctivas sin necesidad de revisar manualmente cada registro.

6. Tabla Comparativa Completa de Dominios Analizados

El repositorio `generator.py` produce un resumen cuyo formato se replica en la Tabla 2. Cada fila corresponde a un dominio y describe si DNSSEC está habilitado, si la cadena se completa, la puntuación RFC alcanzada y cualquier error reportado. Las columnas RFC Score y RFC % muestran la relación entre criterios cumplidos y máximos disponibles, mientras que la columna *Status* refleja el resultado general y *Error* detalla fallas específicas durante la consulta. Esta tabla sirve como referencia directa para los análisis sectoriales descritos posteriormente.

Cuadro 2: Resumen de dominios evaluados

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	–

Dominio	DNSSEC Enabled	Chain Complete	RFC Score	RFC %	Status	Error
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	–
liverpool.com.mx	No	No	0/1	0.0 %	success	–
cemex.com.mx	No	No	0/1	0.0 %	success	Domain does not exist
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

7.1. Panorama de Adopción de DNSSEC

El conjunto total de dominios analizados muestra una adopción heterogénea y, en general, limitada dentro del ecosistema `.mx`. Los datos evidencian que la presencia de DNSSEC es más frecuente en organismos gubernamentales e instituciones académicas, mientras que sectores financieros, comerciales y de medios mantienen configuraciones tradicionales sin firma.

En la muestra analizada, únicamente seis dominios presentan DNSSEC habilitado: `gob.mx`,

pemex.gob.mx, unam.mx, ipn.mx, sep.gob.mx y udg.mx. Todos ellos publican DNSKEY y firmas RRSIG válidas; sin embargo, el resto de los dominios exhiben puntuaciones mínimas en el RFC Score debido a la ausencia de DNSKEY, DS y RRSIG.

7.2. Cadena de Confianza y Cumplimiento RFC

La validación completa de la cadena de confianza solo se observó en gob.mx, pemex.gob.mx y unam.mx, los cuales publican un registro DS correcto en .mx y mantienen firmas vigentes. En contraste, los tres dominios restantes con DNSSEC activo presentan configuración parcial: la zona está firmada pero el DS no está publicado o es inconsistente, lo que deriva en estado *Chain Incomplete*. Este escenario es común cuando el proveedor de hosting o registrador no concluye el proceso de delegación segura.

En cuanto al cumplimiento de las RFC evaluadas, pemex.gob.mx obtuvo 21/21 y unam.mx alcanzó 19/19, lo que evidencia una implementación robusta. gob.mx también registró un puntaje alto (19/21). Por el contrario, ipn.mx, udg.mx y sep.gob.mx presentan configuraciones intermedias debido a la ausencia de DS. Finalmente, la mayoría de los dominios analizados carecen de cualquier configuración DNSSEC, reflejando una brecha significativa en los sectores comercial, bancario y mediático.

8. Análisis Sectorial

Sector Gubernamental (.gob.mx). El sector gubernamental exhibe contrastes. gob.mx y pemex.gob.mx mantienen DNSSEC habilitado con cadena completa, y sep.gob.mx firmó su zona aunque aún carece de DS. En contraste, dependencias como sat.gob.mx, imss.gob.mx, banxico.gob.mx, segob.gob.mx, sre.gob.mx, inegi.gob.mx, conacyt.gob.mx y shcp.gob.mx siguen sin implementar DNSSEC, lo que resulta preocupante dada la criticidad de sus servicios.

Sector Educativo (.mx). Tres instituciones destacan con DNSSEC habilitado. unam.mx opera con cadena completa; ipn.mx y udg.mx mantienen claves y firmas pero no han publicado su DS. El resto de las universidades analizadas: itesm.mx, uag.mx, uanl.mx, buap.mx, uaemex.mx, uabc.mx, uach.mx, continúan sin firmar sus zonas.

Sector Financiero. Los dominios bbva.mx, banorte.com.mx, hsbc.com.mx, santander.com.mx, citibanamex.com.mx y scotiabank.com.mx aparecen con DNSSEC deshabilitado. Dado el alto perfil de riesgo, la ausencia de firmas DNSSEC es notable, pues expone a los usuarios a ataques de suplantación y potencial robo de credenciales.

Sector Comercial. Sitios de gran tráfico como walmart.com.mx, femsa.com.mx, bimbo.com.mx, oxxo.com.mx, liverpool.com.mx, amazon.com.mx y mercadolibre.com.mx mantienen configuraciones sin firma. El mismo patrón aparece en telecomunicaciones y medios: telmex.com.mx,

`telcel.com`, `televisa.com.mx`, `tv-azteca.com.mx`, `eluniversal.com.mx`, `reforma.com.mx`, `milenio.com`, confirmando que DNSSEC aún no es parte de los controles comunes en estos sectores.

9. Conclusiones Generales

La muestra analizada demuestra que DNSSEC todavía es una excepción entre los dominios .mx. Las implementaciones exitosas confirman que la tecnología es viable y puede operar de manera estable dentro del ecosistema nacional, pero los esfuerzos se concentran en unos cuantos organismos. El principal problema técnico detectado en los dominios que sí firmaron su zona es la ausencia del registro DS, lo que rompe la cadena de confianza justo antes de alcanzar al usuario final. Sectores críticos como finanzas y comercio electrónico aún no aprovechan DNSSEC, por lo que continúan expuestos a ataques de spoofing que podrían mitigarse mediante la validación criptográfica. La existencia de configuraciones completas en PEMEX, UNAM y el portal de gobierno evidencia que existen capacidades locales para adoptar y operar DNSSEC, pero también pone de manifiesto la falta de adopción homogénea.

10. Taxonomía de contribuciones

Contributor Roles Taxonomy (CRediT)

Alberto Boughton Reyes
Supervisión general del proyecto, análisis estadístico, redacción de conclusiones.

Valeria García Hernández
Recolección de datos, extracción de DNSKEY/DS, validación con delv.

Facundo Bautista Barbera
Preparación del repositorio, automatización Python, consolidación del JSON.

Emiliano Ruiz López
Clasificación de algoritmos, tamaños de clave y evaluación criptográfica.

Daniel Garnelo Martínez
Redacción técnica, integración de RFCs y elaboración de recomendaciones.

11. Conclusiones particulares

Alberto Boughton Reyes
Integré el análisis, las métricas y la revisión del cumplimiento RFC. Comprendí cómo traducir indicadores criptográficos complejos en hallazgos claros para el socio formador y reforcé la

importancia de documentar cada ruptura de la cadena desde el registro DS hasta la evidencia final.

Valeria García Hernández
Lideré las consultas DNSSEC y la validación con herramientas CLI. Practiqué la reconstrucción manual de la cadena de confianza y el contraste con validadores externos, habilidades esenciales para un ingeniero en ciencia de datos que debe garantizar la integridad de la información que analiza.

Facundo Bautista Barbera
Desarrollé la automatización del pipeline y los procesos de consolidación en JSON. En el camino profundicé en `dnspython`, en el manejo de respuestas NXDOMAIN/NSEC y en la generación de reportes reproducibles que facilitan auditorías masivas en ciberseguridad.

Emiliano Ruiz López
Evalué los algoritmos y tamaños de clave identificados. El ejercicio reforzó los criterios aprendidos en clase para justificar el uso de ED25519, RSA-2048 o ECDSA frente a configuraciones obsoletas, y me permitió explicar esas diferencias con argumentos técnicos sólidos.

Daniel Garnelo Martínez
Redacté la sección de buenas prácticas y el análisis de riesgos. Aprendí a navegar los RFC para sintetizar recomendaciones accionables y a comunicar cómo cada hallazgo del analizador se traduce en controles concretos para proteger la cadena DNSSEC.

12. Recomendaciones Específicas

Las siguientes recomendaciones se derivan de la evidencia obtenida y se alinean con las guías de la IETF, NIC México y operadores con experiencia en despliegues DNSSEC (IETF DNSOP Working Group, s.f.; NIC México, s.f.). Su aplicación ordenada permite cerrar brechas desde la preparación del entorno, la instalación y configuración de las firmas, hasta la operación continua y las auditorías.

12.1. Publicación del registro DS en .mx

Los dominios que ya cuentan con DNSKEY y RRSIG deben completar la cadena publicando el registro DS correspondiente a su KSK en la zona .mx. El procedimiento consiste en extraer el DS desde el administrador DNS, cargarlo en el panel del registrador o proveedor autorizado y confirmar la propagación con una consulta como `dig +dnssec dominio DS`. Este paso, aunque sencillo, restablece la relación de confianza entre la raíz, el TLD y la zona hija.

12.2. Rotación y gestión de claves (KSK y ZSK)

La rotación periódica de claves evita el desgaste criptográfico. Es recomendable renovar la ZSK cada 30 a 90 días y la KSK cada 6 a 12 meses, manteniendo algoritmos seguros como RSA de 2048 bits o superiores, ECDSA P-256/P-384 o ED25519. Claves de 1024 bits o algoritmos obsoletos deben retirarse progresivamente. La documentación automatizada del proceso facilita ejecutar firmados programados sin interrumpir la zona.

12.3. Verificación de vigencia de firmas RRSIG

Muchas interrupciones se originan cuando las firmas expiran o se construyen con Time To Live (TTL) inadecuados. Es conveniente monitorear el campo de expiración de cada RRSIG, automatizar la regeneración y establecer alertas cuando falten entre tres y cinco días para la caducidad. Con ello se evitan fallos repentinos que provoquen respuestas *Server Failure (SERVFAIL)* en los resolvers validadores.

12.4. Uso adecuado de NSEC o NSEC3

La selección del mecanismo de negación depende de la sensibilidad de la zona. NSEC3 con iteraciones bajas y saltos aleatorios reduce la posibilidad de enumeración en dominios de alta visibilidad, mientras que NSEC es suficiente en zonas públicas sin nombres sensibles. Lo crítico es asegurar que el mecanismo exista y esté firmado; Non-Existent Domain (NXDOMAIN) sin protección deja abierta la puerta a ataques de enumeración y suplantación.

12.5. Implementación de validación DNSSEC en resolvers internos

Firmar una zona solo protege a los usuarios que consultan desde resolvers validadores. Instituciones que administran dominios críticos deben habilitar la validación DNSSEC en resolvers como Unbound, Knot Resolver o BIND, desactivando `val-permissive-mode` para forzar el rechazo de respuestas no autenticadas. Distribuir estos resolvers entre los usuarios internos reduce dramáticamente la probabilidad de envenenamiento de caché.

12.6. Auditoría periódica con herramientas automáticas

La revisión continua evita incidentes producidos por expiraciones o configuraciones inconsistentes. Ejecutar validadores como DNSViz, Verisign DNSSEC Debugger y las herramientas de SIDN Labs de manera trimestral permite detectar TTL irregulares, inconsistencias entre servidores Name Server (NS) o firmas desalineadas. Integrar estos pasos en un calendario operativo facilita responder antes de que ocurra una interrupción.

12.7. Recomendaciones específicas por sector

En el gobierno federal conviene establecer una política que obligue a cada dependencia a publicar su DS y a monitorear activamente la vigencia de las firmas, especialmente en dependencias financieras o sociales. En el sector educativo bastaría con que instituciones que ya firmaron, como IPN y UDG, publiquen su DS para cerrar el ciclo y sirvan como referencia para el resto. Las instituciones financieras deberían priorizar DNSSEC al mismo nivel que Hypertext Transfer Protocol Secure (HTTPS) o HTTP Strict Transport Security (HSTS) para proteger portales de autenticación y transferencias, mientras que el comercio electrónico puede integrar DNSSEC como complemento a sus controles existentes para reducir intentos de redireccionamiento malicioso.

13. Anexos

Los anexos consolidan la información necesaria para replicar el análisis completo, comprender los elementos de DNSSEC utilizados y revisar ejemplos concretos de salidas correctas e incorrectas. A continuación se describen los elementos clave:

Comandos utilizados para la validación manual. La consulta `dig +dnssec dominio.mx` muestra los registros relevantes de la zona, incluidos los RRSIG cuando existen, las claves DNSKEY solicitadas por implicación y el indicador `ad` cuando el resolver valida correctamente. Para revisar exclusivamente las claves se emplea `dig dominio.mx DNSKEY +dnssec`, que permite identificar qué registros corresponden a la KSK o a la ZSK y verificar el algoritmo. La delegación segura se inspecciona mediante `dig dominio.mx DS +dnssec`; si la respuesta es nula se confirma que la cadena permanece incompleta. Los mecanismos de negación se distinguen emitiendo `dig dominio.mx NSEC +dnssec` y `dig dominio.mx NSEC3PARAM +dnssec`, lo que facilita determinar si la zona expone listados directos o hashes. Finalmente, `delv dominio.mx` ejecuta la validación completa desde la raíz y explica cualquier ruptura de la cadena.

Elementos de DNSSEC utilizados en el análisis. Los registros DNSKEY contienen las claves públicas que permiten validar las firmas; la KSK firma el conjunto DNSKEY y la ZSK protege el resto de los registros. Las firmas RRSIG garantizan integridad y autenticidad de cada conjunto consultado. Los registros DS, ubicados en la zona padre, forman el vínculo criptográfico entre el dominio y su TLD; sin ellos la cadena se interrumpe. Para negar la existencia de nombres se utilizan NSEC y NSEC3: el primero enumera dominios vecinos mientras que el segundo oculta la estructura mediante hashes, ambos firmados para impedir manipulación. La cadena de confianza completa recorre la raíz, el TLD .mx, el dominio y, en su caso, los subdominios, de modo que cualquier ruptura deja al usuario sin garantía de autenticidad.

Ejemplo de salida de DNSSEC correcta. Un dominio con DNSSEC completo muestra una respuesta similar a la siguiente:

```
;; 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 ...
```

En esta salida el indicador `ad` confirma que la información fue autenticada, el registro DS conecta al dominio con .mx, las firmas RRSIG se encuentran vigentes y el mecanismo NSEC3 documenta la negación de existencia.

Ejemplo de cadena incompleta. Cuando la zona está firmada pero falta el DS en .mx, `dig` reporta las claves y firmas locales pero indica "NO DS record found". El analizador

clasifica este escenario como *Enabled / Chain Incomplete*, lo que explica por qué los resolvers validadores no pueden confiar en la respuesta a pesar de que exista DNSKEY.

Ejemplo de dominio sin DNSSEC. Si la zona no implementa DNSSEC, la respuesta contiene únicamente los registros tradicionales (A, AAAA, MX) y carece de DNSKEY y RRSIG. En ese caso el analizador indica *DNSSEC Disabled* y el RFC Score se reduce al mínimo (0/1).

Archivos generados por el analizador. Cada ejecución de `generator.py` produce reportes por dominio en formato Markdown que incluyen las claves DNSKEY, las firmas RRSIG, el registro DS disponible, el tipo de NSEC o NSEC3, los algoritmos empleados, el RFC Score y el estado final. Paralelamente se genera un archivo `_summary.json` con campos como `dnssec_enabled`, `chain_complete`, `rfc_score`, `rfc_score_max`, `status`, `nsec_type` y `key_algorithms`, que sirve como base para las tablas incluidas en este reporte.

Flujos de validación utilizados por el analizador. El módulo `lim_advisor.py` evalúa cada clave para identificar el algoritmo (RSA, ECDSA, Ed25519), la longitud de la KSK y la ZSK, la correcta separación de roles y señales de uso de claves obsoletas. De forma paralela, `rfc_validator.py` confirma la presencia de RRSIG, revisa las ventanas de vigencia, enlaza los registros DS con las DNSKEY correspondientes, valida los formatos y campos obligatorios y comprueba que exista un mecanismo autenticado de negación de existencia.

Reproducción completa del análisis. Para duplicar el estudio se prepara un archivo con los dominios objetivo (por ejemplo `domains.txt`), se ejecuta `python3 analyzer/generator.py domains.txt` y se revisan los resultados en la carpeta de salida, donde cada dominio tiene su reporte y el archivo `_summary.json` ofrece la consolidación. Comparar estos datos con los descritos en este documento permite verificar que la metodología produce resultados consistentes.

Entorno Docker para despliegue. Cuando se requiere levantar la aplicación completa y verificar la interfaz web local, es necesario contar con Docker Desktop instalado en el equipo (descarga disponible en `https://www.docker.com/products/docker-desktop/`). El proceso recomendado es clonar el repositorio (`git clone https://github.com/Facundo-Barbera/DNSSEC-Ana` abrir Docker Desktop para asegurarse de que el demonio esté activo, ejecutar `docker compose up` dentro de la carpeta del proyecto y acceder finalmente a `http://localhost:5050`. Este flujo permite replicar la experiencia del socio formador y validar que los cambios realizados en el código se reflejen en la plataforma sin necesidad de configurar manualmente todas las dependencias.

14. Repositorios y código utilizado

El análisis se apoya en el repositorio DNSSEC Analyzer disponible en la rama Reportes de `https://github.com/Facundo-Barbera/DNSSEC-Analyzer/tree/Reportes`. La estructura incluye los módulos `analyzer/generator.py`, `analyzer/lim_advisor.py` y `analyzer/rfc_validator.` además de los reportes en Markdown y el archivo `_summary.json` que alimenta las tablas.

15. Bibliografía

1. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005a). *RFC 4033: DNS Security Introduction and Requirements*. Internet Engineering Task Force. `https://datatracker.ietf.org/doc/rfc4033/`

2. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005b). *RFC 4034: Resource Records for DNS Security Extensions*. Internet Engineering Task Force. `https://datatracker.ietf.org/doc/rfc4034/`

3. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005c). *RFC 4035: Protocol Modifications for DNSSEC*. Internet Engineering Task Force. `https://datatracker.ietf.org/doc/rfc4035/`

4. Bernstein, D. J., et al. (2012). *RFC 5702: Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG*. Internet Engineering Task Force. `https://datatracker.ietf.org/doc/rfc5702/`

5. ICANN. (2019). *Root DNSSEC Deployment*. `https://www.icann.org/resources/pages/dnssec-what-is-it-2019-03-05-en`

6. IETF DNSOP Working Group. (s.f.). *Documentos y borradores*. `https://datatracker.ietf.org/wg/dnsop/documents/`

7. Internet Assigned Numbers Authority. (s.f.). *Root Zone Management – Procedures and Key Signing Ceremonies*. `https://www.iana.org/dnssec`

8. Laurie, B., Sisson, G., Arends, R., & Blacka, D. (2008). *RFC 5155: DNSSEC Hashed Authenticated Denial of Existence (NSEC3)*. Internet Engineering Task Force. `https://datatracker.ietf.org/doc/rfc5155/`

9. Mockapetris, P. (1987a). *RFC 1034: Domain Names: Concepts and Facilities*. Internet Engineering Task Force. `https://datatracker.ietf.org/doc/rfc1034/`

10. Mockapetris, P. (1987b). *RFC 1035: Domain Names: Implementation and Specification*. Internet Engineering Task Force. `https://datatracker.ietf.org/doc/rfc1035/`

11. NIC México. (s.f.). *DNSSEC en .MX*. `https://www.nic.mx/es/InformacionGral/DNSSEC`