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

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. 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, con extensiones posteriores como Next Secure 3 (NSEC3) descritas en el RFC 5155. El dominio .MX, administrado por Network Information Center México (NIC México), se encuentra firmado y permite validación completa desde la raíz; 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), 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. Con estos elementos se forma una cadena de confianza que parte de la raíz y permite validar cada respuesta. 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).

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 NOTA:AÑADIR SERVIDOR RECURSIVO QUE SE UTILIZO. El flujo comienza preparando el entorno con Python 3 y las dependencias incluidas en el repositorio DNSSEC Analyzer disponible en GitHub (ver Subsección 13.4). 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 genera para cada dominio las consultas DNSSEC pertinentes, traduce los resultados a reportes en Markdown y consolida los indicadores en archivos JavaScript Object Notation (JSON). Con esta información se determinan los estados DNSSEC y las puntuaciones RFC nota:falta añadir que las puntaciones rfc se validan usnado el otro script dns validator. Para garantizar la reproducibilidad, cada paso del pipeline se documenta y se conserva en la estructura de carpetas del proyecto.

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 mecanis-

mo 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.

4. Criterios de Validación y Lógica del Analizador

4.1. Componentes del analizador

nota: no incluir lim advisor .py El repositorio integra tres módulos principales. `generator.py` coordina las consultas DNS, reúne los registros, llama a los módulos de evaluación y construye los reportes finales. `lim_advisor.py` revisa los parámetros criptográficos de cada clave, como el algoritmo utilizado, el tamaño de la KSK o Zone Signing Key (ZSK) y la proximidad de expiración, emitiendo advertencias cuando detecta prácticas débiles. Finalmente, `rfc_validator.py` compara la configuración del dominio contra criterios derivados de los RFC relevantes y calcula la puntuación que aparece en la tabla de resultados. El trabajo en conjunto de estos componentes permite determinar si un dominio tiene DNSSEC activo, si la cadena de confianza es verificable y qué tan apegada a los estándares es su configuración.

4.2. Parámetros y verificaciones que se evalúan

nota: coregir tabla y quitar lim advisor

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.

Verificación	Propósito / Qué se revisa
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)	Mediante `lim_advisor.py`, se evalúa si las claves cumplen parámetros robustos, por ejemplo longitud adecuada o algoritmo recomendable.
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 ("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

nota: esta seccion hay que validar que sea correcto lo que se dice y quitar lim advisor Se considera que un dominio tiene *DNSSEC Enabled* cuando publica registros DNSKEY, mantiene al menos una firma RRSIG válida y cuenta con delegación DS en la zona padre. La marca *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 indica qué tanto cumple el dominio con los criterios establecidos, mientras que las advertencias emitidas por `lim_advisor.py` alertan sobre claves débiles, algoritmos obsoletos o firmas próximas a expirar.

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.

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	–

Dominio	DNSSEC Enabled	Chain Complete	RFC Score	RFC %	Status	Error
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	–
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

nota mejorar el formato para que no tenga secciones pequeñas y poner el dato de cuantos dominios en el mundo tiene dnssec, incluir referencia El conjunto completo de dominios revela una adopción heterogénea y, en general, limitada dentro del ecosistema .MX. Los datos confirman que la presencia de DNSSEC es mayor en organismos gubernamentales y algunas instituciones académicas, mientras que los sectores financiero y comercial mantienen configuraciones tradicionales sin firma.

7.1. Adopción de DNSSEC

Solo seis dominios aparecen con DNSSEC habilitado: `gob.mx`, `pemex.gob.mx`, `unam.mx`, `ipn.mx`, `sep.gob.mx` y `udg.mx`. Cada uno muestra registros DNSKEY, firmas RRSIG y elementos mínimos para operar la zona firmada. El resto de la muestra presenta valores 0/1 en el RFC Score, lo que evidencia la ausencia de DNSKEY, DS y RRSIG; en conjunto, estos casos constituyen la gran mayoría del universo analizado.

7.2. Cadena de confianza

La validación completa solo se logró en `gob.mx`, `pemex.gob.mx` y `unam.mx`. Estos dominios publican el registro DS en .mx y mantienen firmas vigentes. En los tres casos restantes con DNSSEC activo el registro DS no está presente o resulta inconsistente, por lo que el estado cambia a *Chain Incomplete*. Este patrón es típico cuando la zona fue firmada pero el proveedor o el registrador no publica la delegación segura en el TLD.

7.3. Cumplimiento RFC (RFC Score)

`pemex.gob.mx` alcanzó 21/21 y `unam.mx` obtuvo 19/19, lo que indica adherencia plena a los criterios evaluados. El portal `gob.mx` registró 19/21, también con una configuración sólida. Los dominios `ipn.mx`, `udg.mx` y `sep.gob.mx` lograron puntajes intermedios porque carecen de DS, aunque mantienen firmas válidas. Los demás dominios permanecen con puntajes mínimos debido a la falta total de DNSSEC.

7.4. Casos representativos

`gob.mx` se presenta como un despliegue estable con cadena completa y alto cumplimiento. `pemex.gob.mx` demuestra una implementación madura y sirve como referencia para otros organismos. `unam.mx` destaca como ejemplo en el sector educativo, mientras que `ipn.mx`, `udg.mx` y `sep.gob.mx` muestran el esfuerzo parcial que se queda a un paso de la delegación segura. La ausencia total de DNSSEC en banca, comercio y medios evidencia una brecha significativa frente a los sectores más críticos.

8. Análisis Sectorial

nota escribir bonito sin tantas subsecciones

8.1. 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. 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` continúan sin implementar DNSSEC. Tomando en cuenta la criticidad de estos servicios, la adopción sigue siendo baja.

8.2. 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 consideradas en la muestra (`itesm.mx`, `uag.mx`, `uanl.mx`, `buap.mx`, `uaemex.mx`, `uabc.mx` y `uach.mx`) continúan sin firmar sus zonas.

8.3. 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. La falta de adopción en entidades de alto perfil de riesgo es relevante porque las suplantaciones de DNS pueden afectar la confianza de los clientes y exponer credenciales.

8.4. Sector Comercial

Sitios de gran tráfico y presencia internacional 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 comportamiento se observa en empresas enfocadas en telecomunicaciones y medios como `telmex.com.mx`, `telcel.com`, `televisa.com.mx`, `tv-azteca.com.mx`, `eluniversal.com.mx`, `reforma.com.mx` y `milenio.com`. La ausencia generalizada confirma que DNSSEC aún no forma parte de los controles típicos en este sector.

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. Recomendaciones Técnicas

nota combinar seccion 10 y 11 nota MX cambiarlo por mx 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. 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.

11. Recomendaciones Específicas

11.1. 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.

11.2. 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.

11.3. Verificación de vigencia de firmas RRSIG

nota; revisar que es valido lo que se dice aqui 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.

11.4. 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.

11.5. 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.

11.6. 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.

11.7. 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.

12. Anexos

hacer un anexo de manera mas formal 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.

12.1. 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.

12.2. 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.

12.3. Ejemplo de salida de DNSSEC correcta

Un dominio con DNSSEC completo muestra una salida 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 respuesta 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.

12.4. 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.

12.5. 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).

12.6. 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.

12.7. 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.

12.8. 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.

13. Bibliografía

La bibliografía reúne los documentos técnicos, estándares y fuentes formales utilizados para contextualizar DNSSEC, definir los criterios de evaluación y referenciar el código empleado durante el análisis.

13.1. RFCs (Request for Comments)

La base del DNS se describe en los RFC 1034 y 1035 publicados por Paul Mockapetris en 1987, mientras que la especificación de DNSSEC se formaliza en los RFC 4033, 4034 y 4035 de 2005 redactados por Roy Arends y colaboradores. Como complemento se utilizan el RFC 5155 sobre NSEC3, el RFC 5702 que habilita Secure Hash Algorithm 2 (SHA-2) en DNSKEY y las notas publicadas por el grupo DNS Operations (DNSOP) de la IETF que documentan las prácticas operativas recomendadas.

13.2. Documentación de ICANN y NIC México

ICANN mantiene documentación sobre el despliegue de DNSSEC en la zona raíz y los procedimientos de ceremonias de firma, mientras que NIC México describe los lineamientos específicos para el country code top-level domain (ccTLD) .MX y la administración de sus claves. Las referencias a Root Zone Management detallan los procesos formales asociados a la gestión de claves y respaldan la validez de la cadena de confianza utilizada en este estudio.

13.3. Herramientas y validadores utilizados

DNSViz, el DNSSEC Debugger de Verisign y las herramientas de SIDN Labs se emplean como validadores externos para visualizar cadenas de confianza y detectar inconsistencias. La herramienta `delv`, incluida en BIND 9, se utiliza para validar manualmente dominios, mientras que `dnspython` habilita las consultas programáticas integradas al analizador.

13.4. 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.

13.5. Literatura y fuentes técnicas adicionales

El trabajo de Dan Kaminsky sobre *cache poisoning* en 2008 se toma como antecedente clave para comprender la urgencia de desplegar DNSSEC. Se consultaron también publicaciones de Dave Crocker y documentos educativos publicados por la IETF y el grupo DNSOP que abordan vulnerabilidades históricas y los lineamientos para despliegues modernos.