



**Tecnológico
de Monterrey**



**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 Ejecutivo

Integrantes:

Alberto Boughton Reyes A01178500

Valeria Garcia Hernandez A01742811

Facundo Bautista Barbera A01066843

Emiliano Ruiz López A01659693

Daniel Garnelo Martinez A00573086

Socio formador: NIC México

Representante: César Steve Salas Santos

Monterrey N.L. 4 de diciembre de 2025

Reporte Ejecutivo

1. Introducción

El proyecto evaluó el nivel de protección que ofrecen los dominios web más relevantes de México al operar en el sistema de nombres de dominio (DNS). El foco se encontró en DNSSEC, tecnología que firma digitalmente las respuestas y que, bien implementada, impide redireccionamientos falsos, suplantación de sitios y robo de información (Arends et al., 2005a, 2005b, 2005c). Para una ciudadanía que realiza trámites, operaciones financieras y gestiones académicas en línea, la ausencia de esta protección permite que un atacante redirija al usuario a un portal falso sin levantar sospechas, por lo que la confianza del país en sus servicios digitales depende de manera directa de la correcta adopción de DNSSEC. Además, el ecosistema `.mx` está firmado por NIC México, por lo que cada entidad nacional puede sumarse a la cadena de confianza publicando su registro DS (NIC México, s.f.). La Figura 1 resume la cadena de confianza evaluada y permite relacionar cada hallazgo con los eslabones que lo originan.

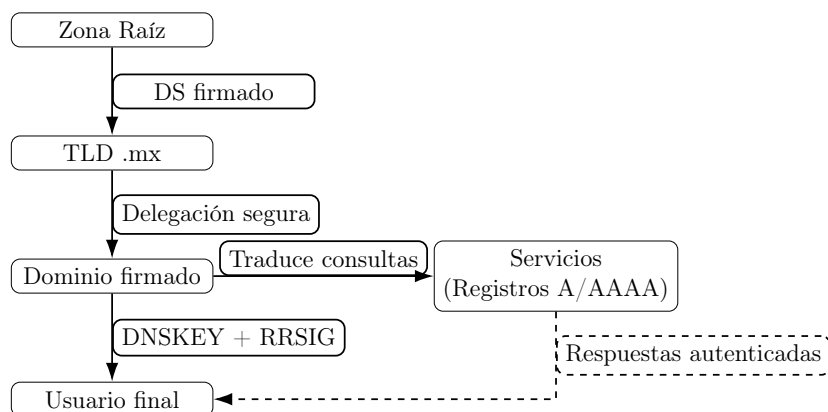


Figura 1: Árbol resumido del DNS y cadena de confianza revisada para cada dominio `.mx`.

2. Desarrollo

Se construyó un panorama ejecutivo de los principales sectores del país (gobierno, educación, banca, empresas comerciales y medios) mediante una herramienta propia que consulta registros DNS en tiempo real, verifica el cumplimiento de las mejores prácticas internacionales y contrasta los hallazgos con verificaciones manuales. La evidencia recabada permite responder tres preguntas clave para el socio formador:

- En qué punto de la cadena DNS (raíz, TLD, dominio) ocurre la ruptura ilustrada en la Figura 1.
- Qué tan extendida se encuentra la activación de DNSSEC entre los sectores estratégicos (Figura 2).
- Qué riesgos enfrentan los usuarios cuando la cadena se rompe y cómo priorizar su corrección.

Al presentar estos resultados en juntas ejecutivas, NIC México puede mostrar de forma inmediata qué dependencias gubernamentales o instituciones financieras requieren acompañamiento para publicar su registro DS, cuál es el beneficio de escalar la herramienta a otros dominios y cómo la automatización acelera auditorías regionales sin depender de revisiones manuales extensas.

3. Resultados

3.1. Hallazgos generales

El uso de DNSSEC en México sigue siendo limitado: de todos los dominios evaluados solo seis muestran la tecnología activada y, de ellos, únicamente gob.mx, pemex.gob.mx y unam.mx ofrecen una configuración completa y coherente con los estándares. El resto carece totalmente de DNSSEC o bien mantiene implementaciones incompletas que no alcanzan a proteger al usuario final. La Figura 2 contrasta la magnitud de la brecha y facilita priorizar acciones para cada sector.

3.2. Impacto al usuario final

Un dominio protegido con DNSSEC confirma su autenticidad y reduce con claridad la probabilidad de fraudes, transacciones inconclusas o suplantaciones. En la situación actual, millones de mexicanos interactúan diariamente con portales que no brindan esa garantía, lo que se traduce en un riesgo mayor de robo de credenciales, interceptación de operaciones financieras y manipulación de comunicaciones oficiales. Los sectores bancario, gubernamental y de comercio electrónico son los más expuestos por la criticidad de los datos que administran.

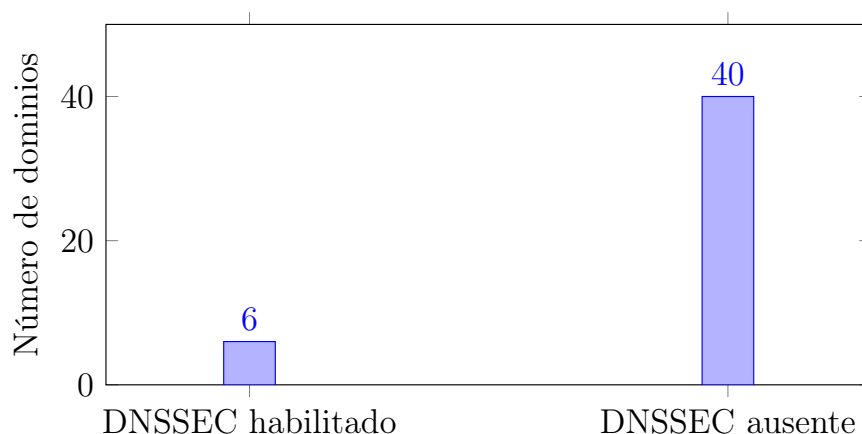


Figura 2: Porcentaje de dominios con DNSSEC habilitado frente al total de la muestra.

4. Evaluación por sector

Gobierno. Aunque gob.mx y PEMEX exhiben una implementación ejemplar de DNSSEC, la mayoría de las dependencias federales y estatales continúan con la cadena de confianza abierta o inexistente. Esta situación expone expedientes sensibles, trámites digitales y sistemas de recaudo, por lo que el rezago gubernamental debe convertirse en prioridad nacional.

Educación. La UNAM es el referente positivo y demuestra que la firma de la zona .mx es viable dentro del ecosistema académico. Sin embargo, ins-

tituciones como IPN, UDG y la mayor parte de las universidades privadas siguen sin publicar su DS o ni siquiera han iniciado el proceso, de modo que plataformas escolares, correos y servicios de pago permanecen vulnerables a manipulación.

Sector financiero. Ninguno de los bancos analizados cuenta con DNSSEC habilitado, lo que convierte a esta industria en la más expuesta para la ciudadanía. La ausencia de firmas digitales facilita ataques de redireccionamiento que pueden derivar en robo de credenciales, transferencias fraudulentas o interrupciones en los canales de banca en línea.

Sector comercial y medios. Telecomunicaciones, supermercados y conglomerados mediáticos operan sin la protección criptográfica, por lo que cada campaña de marketing, portal de compras o sitio de noticias se convierte en un vector de phishing altamente verosímil. Esta brecha impacta directamente al consumidor final, que interactúa con estos servicios de manera cotidiana sin verificación de identidad.

5. Conclusiones

La adopción de DNSSEC en México existe, pero sigue siendo marginal y se concentra en muy pocos casos de éxito. La dificultad no reside en instalar la tecnología sino en cerrar adecuadamente la cadena de confianza y mantenerla vigente, tarea que hoy la mayoría de los operadores no ha logrado. Mientras los sectores críticos carezcan de esta protección, los datos personales y financieros de la población continuarán expuestos, a pesar de que ya se demostró que la implementación estable es factible y replicable. En consecuencia, ofrecer un servicio digital sin DNSSEC equivale a renunciar a una capa básica de verificación de identidad.

6. 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.

7. Conclusiones particulares

Alberto Boughton Reyes

Integré el análisis y las métricas que respaldan cada conclusión. Este trabajo me permitió enlazar los conceptos de criptografía vistos en clase con la redacción de hallazgos ejecutivos, entendiendo por qué un registro DS ausente invalida todo el esfuerzo de firma y cómo eso se traduce en riesgo para los usuarios.

Valeria García Hernández

Lideré las consultas DNSSEC y la validación con herramientas de línea de comandos. Aprendí a diagnosticar paso a paso la cadena de confianza y a comparar las respuestas autenticadas con lo observado en los validadores externos, habilidades que fortalecen mi perfil de ingeniería en ciencia de datos con una base sólida de operaciones seguras.

Facundo Bautista Barbera

Desarrollé la automatización del pipeline y los procesamientos en JSON. Esto me dio práctica en la instrumentación de `dnspython` y en la trazabilidad de fallos criptográficos, demostrando cómo la programación aplicada simplifica auditorías de gran escala en contextos de ciberseguridad.

Emiliano Ruiz López

Analicé los algoritmos y tamaños de clave detectados. La experiencia reforzó mi comprensión de por qué ED25519 o RSA de 2048 bits representan un equilibrio entre rendimiento y resistencia criptográfica, y cómo justificarlos ante un socio formador que busca decisiones técnicas basadas en evidencia.

Daniel Garnelo Martínez

Redacté las buenas prácticas y el análisis de riesgos con base en los RFC relevantes. Practiqué la traducción de requisitos técnicos a recomendaciones ejecutivas, algo indispensable para comunicar proyectos de ciberseguridad a perfiles no técnicos dentro y fuera del aula.

8. Recomendaciones

El país necesita una estrategia nacional que coloque a DNSSEC al mismo nivel que HTTPS en los reglamentos de seguridad digital. Resulta prioritario establecer lineamientos obligatorios para sectores de alto riesgo, acompañados de programas de capacitación y auditorías periódicas que aseguren la continuidad operativa de las firmas, siguiendo las mejores prácticas publicadas por la IETF y operadores como ICANN (ICANN, 2019; IETF DNSOP Working Group, s.f.). Desde lo técnico, cada organización debe completar la cadena de confianza, mantener las firmas actualizadas, favorecer algoritmos modernos, habilitar validación interna y automatizar revisiones para detectar desalineaciones antes de que impacten al usuario. Por último, se recomienda que el gobierno lidere una política de adopción gradual, que la banca incluya DNSSEC en sus requisitos regulatorios, que las universidades repliquen los modelos exitosos existentes y que las empresas integren esta medida a sus marcos de ciberseguridad corporativos.

9. Reflexión final

México cuenta con la infraestructura y el talento necesarios para operar DNSSEC a gran escala; lo que falta es el compromiso sostenido de las organizaciones para cerrar la brecha. Mientras los atacantes perfeccionan sus tácticas,

muchos portales continúan sin una verificación básica de autenticidad. El país debe considerar a DNSSEC como un requisito esencial para garantizar el desarrollo seguro de la economía digital.

10. 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.

11. 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. ICANN. (2019). *Root DNSSEC Deployment*. <https://www.icann.org/resources/pages/dnssec-what-is-it-2019-03-05-en>
5. IETF DNSOP Working Group. (s.f.). *Documentos y borradores*. <https://datatracker.ietf.org/wg/dnsop/documents/>
6. NIC México. (s.f.). *DNSSEC en .MX*. <https://www.nic.mx/es/InformacionGral/DNSSEC>