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

Monterrey N.L. 4 de diciembre de 2025

Reporte Ejecutivo

1. Introducción

El propósito del proyecto fue evaluar qué tán seguros son algunos de los dominios web más importantes en México, refiriéndonos al nivel del sistema de nombres de dominio (DNS), específicamente analizando el uso de DNSSEC, tecnología diseñada para proteger usuarios de ataques como redireccionamientos falsos, suplantación de sitios web y robo de información, etc.

Cuando una persona accede a una página como un banco, una universidad o un portal gubernamental, confía en que realmente está entrando al sitio legítimo, pues supone que estas páginas deben ser seguras y oficiales, sin

embargo, sin DNSSEC, existe el riesgo de que un atacante pueda redirigir al usuario a un sitio falso sin que este lo note. El DNSSEC funciona como una "firma digital" que permite verificar que el sitio es auténtico, y por lo tanto seguro para navegar.

En este trabajo se analizó si los dominios más relevantes de México están utilizando este mecanismo de seguridad correctamente y qué tán seguros se encuentran realmente los usuarios de todas las amenazas.

2. Desarrollo

Para el análisis se seleccionó una muestra representativa de dominios del sector:

- Gobierno
- Educación
- Banca
- Empresas comerciales
- Medios de comunicación

El objetivo fue identificar si:

- El dominio tiene DNSSEC activo.
- La protección está bien configurada.
- La seguridad es completa o parcial.
- El dominio no cuenta con ninguna protección criptográfica.

Se utilizó una aplicación desarrollada por nuestro equipo en Python que consulta múltiples registros técnicos en tiempo real y evalúa si un dominio

cumple con los estándares internacionales definidos por la IETF (organismo que regula DNSSEC).

Además del análisis, se realizaron verificaciones manuales con herramientas reconocidas del sector para confirmar los resultados y asegurar la seguridad de los usuarios y la veracidad del análisis.

El resultado final fue una tabla comparativa que permite observar claramente qué dominios son seguros, cuáles están parcialmente protegidos y cuáles no tienen ninguna protección.

3. Resultados

3.1. Hallazgos generales

El resultado más importante del estudio es que el uso de DNSSEC en México es objetivamente pobre, incluso en sectores que deberían reforzar esta seguridad.

De todos los dominios revisados:

- Solo 6 dominios tenían DNSSEC activado.
- De esos 6, únicamente:
  - gob.mx
  - pemex.gob.mx
  - unam.mx

  tenían una protección completa y correctamente configurada.
- Los demás dominios analizados no contaban con DNSSEC activo o está configurado de manera incorrecta.

3.2. Impacto al usuario final

Cuando un dominio sí tiene DNSSEC completo, el usuario tiene la certeza de que el sitio es real, de esta manera se pueden prevenir ataques de suplantación. Así como es mucho más difícil redirigirlo a una página falsa, dando lugar a transacciones más confiables.

Cuando un dominio no tiene DNSSEC, se vuelve vulnerable a páginas falsas, robo de credenciales, ataques de redireccionamiento y suplantación de identidad. El usuario no tiene forma de verificar autenticidad de las páginas y el riesgo de robo de datos se incrementa especialmente para: Bancos, páginas de gobierno y comercio electrónico.

4. Evaluación por sector

4.1. Gobierno

Algunas instituciones importantes sí implementan DNSSEC correctamente, tales como gob.mx y PEMEX, sin embargo, la mayoría de las dependencias no cuentan con protección activa. Esto es preocupante debido al volumen de trámites importantes, datos personales y operaciones vitales que se manejan en estos sitios.

4.2. Educación

Solo universidades como UNAM tienen la protección completa. Otras instituciones tienen implementaciones incompletas o inexistentes, lo cual pone en riesgo plataformas académicas, correos institucionales y servicios digitales.

4.3. Sector financiero

Todas las entidades bancarias analizadas carecen de DNSSEC. Esto representa uno de los riesgos más importantes del estudio, ya que estos portales

manejan:

- Contraseñas
- Transferencias
- Información personal
- Datos financieros

4.4. Sector comercial y medios

Empresas grandes como supermercados, telecomunicaciones y medios de comunicación tampoco cuentan con protección DNSSEC, exponiendo millones de usuarios diariamente a potenciales ataques.

5. Conclusiones

1. DNSSEC existe en México, pero su adopción es bastante pobre, con sitios que usan datos personales sin protección completa, implicando un gran riesgo a robos y la privacidad.
2. El mayor problema técnico no es instalar DNSSEC, sino terminar correctamente su configuración.
3. La mayoría de los sectores críticos no están protegidos completamente.
4. Los pocos casos exitosos demuestran que sí es posible implementarlo de forma estable, y que podría replicarse em los .
5. La principal vulnerabilidad de los dominios es no activar la cadena de confianza completa.
6. No usar DNSSEC hoy en día equivale a ofrecer servicios digitales sin verificación de identidad.

6. Recomendaciones

A nivel general, nuestras recomendaciones son:

- Promover que DNSSEC sea tan obligatorio como HTTPS.
- Exigir su implementación en sectores de alto riesgo.
- Capacitar a personal técnico.
- Realizar auditorías periódicas.

A nivel técnico

- Completar la cadena de confianza.
- Mantener firmas actualizadas.
- Usar algoritmos modernos.
- Configurar validación DNSSEC en servidores internos.
- Automatizar revisiones.

Por sector

- Gobierno: Establecer una política nacional de DNSSEC.
- Banca: Priorizar DNSSEC como requisito de seguridad.
- Educación: Usar a las universidades ya protegidas como modelo.
- Empresas: Integrar DNSSEC a políticas de ciberseguridad existentes.

7. Reflexión final

México ya tiene la infraestructura para operar DNSSEC. Lo que falta no es la tecnología, sino el compromiso para hacer el cambio y mantener más seguros a los usuarios.

Mientras los atacantes evolucionan, muchos portales siguen sin una verificación básica de autenticidad. DNSSEC debe dejar de verse como algo opcional y convertirse en parte esencial de la seguridad digital del país.

8. 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.