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 ejecutiva.

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 Ejecutivo Reto

Introducción:
El propósito de este reto fue el de analizar que tan protegidos o desprotegidos pueden estar algunos de los sitios más importantes en México, esto frente ataques que buscan engañar a usuarios indefensos a través del internet y supuestas páginas oficiales protegidas.

El sistema que nos permite escribir una dirección www.algo.com y nos permite llegar al sitio correcto se llama DNS, no obstante, este sistema fue diseñado con otro propósito, uno no necesariamente seguro, por lo que existen ataques que permiten cambiar direcciones legítimas por falsas sin que el usuario se dé cuenta.

Para solucionar este problema existe el DNSSEC, una tecnología que funciona como un sello de autenticidad digital y su función es confirmar que un sitio web es real y que la información que se recibe no ha sido alterada por atacantes.

Por esto, en este proyecto se evaluó si ciertos dominios mexicanos cuentan con estas tecnologías y mecanismos de protección y si está protegido o tenemos que estar atentos a estas páginas.
.

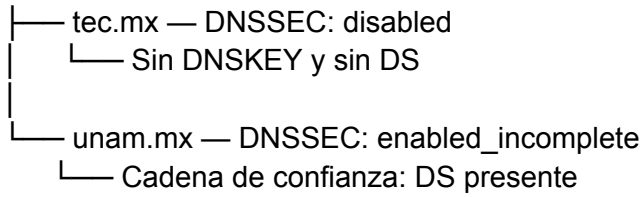
Desarrollo:
Para realizar este análisis se seleccionaron varios dominios importantes en México, específicamente con terminación .mx
Los cuales fueron:

- gob.mx
- ipn.mx
- sat.mx
- tec.mx
- unam.mx

A cada uno de estos se les aplicaron pruebas para ver si cuentan con protección DNSSEC, si su identidad puede ser validada, si existe una cadena de seguridad que confirme su autenticidad o si están configurados de forma completa o parcial.

Asimismo, se construyó un árbol DNS que permite visualizar la relación entre un dominio y sus servidores, mostrando si existe una conexión segura entre ellos.

Árbol DNS:
mx (TLD)
├── gob.mx — DNSSEC: enabled_incomplete
│ └── Cadena de confianza: DS presente
│
├── ipn.mx — DNSSEC: enabled_incomplete
│ └── Cadena de confianza: NO DS → rota
│
├── sat.mx — DNSSEC: disabled
│ └── Sin DNSKEY y sin DS
│



De manera general, el proceso que seguimos fue:
Usuario → Servidor DNS → Verificación de legitimidad → Acceso al sitio

Cuando el DNSSEC está configurado correctamente, el sistema se puede validad dándonos que es auténtico, cuando no lo está podemos ser dirigidos a otras páginas falsas sin notarlo.

En algunos dominios se detectó que el sistema estaba presente, pero mal configurado, lo que significa que la seguridad existe solo en apariencia, pero no en la práctica.

Resultados:
El análisis mostró que no todos los dominios están protegidos adecuadamente, aunque algunos si cuentan con la validación, estos están incompletos, no validan su identidad correctamente o son vulnerables a suplantación.
En este caso, los sitios que sí cuentan con una protección DNSSEC son gob.mx, ipn.mx y unam.mx; sin embargo, estos están incompletos por lo que desde el punto de vista de los usuarios existe una mayor confianza al ingresar datos personales, hay poco riesgo de fraudes, se asegura que el sitio es auténtico y se redicen ataques de redireccionamiento.

Por otro lado, los que no cuentan con DNSSEC para nada son tec.mx y sat.mx que desde el punto de vista del usuario, estos pueden ser engañados fácilmente, existen mayores riesgos de robo de información, no existe garantía de estar en el sitio real y es más fácil de falsificar las páginas.

Un ejemplo podrías ser que un banco protegido por DNSSEC ofrece una mayor protección contra las páginas falsas que busca robar contraseñas o datos personales, mientras que una sin DNSSEC es más vulnerable a cualquier ataque y robo de información.

Evaluación final:
El nivel de implementación de DNSSEC en dominios .mx es limitado e irregular.
Aunque algunas instituciones han comenzado a adoptar esta tecnología, muchas aún no la utilizan o la tienen mal configurada.

Conclusiones:
DNSSEC sí es una solución efectiva para proteger a los usuarios. Aunque no basta con activarlo, debe configurarse correctamente.
La ausencia de DNSSEC representa un riesgo para instituciones y ciudadanos.
La seguridad en línea no depende solo del usuario, sino también de la infraestructura del dominio.

Recomendaciones:

- Implementar DNSSEC como obligación en dominios críticos
- Mejorar auditorías de seguridad periódicas
- Capacitar a personal técnico en protección DNS
- Fomentar su adopción en bancos, universidades y dependencias públicas
- Desarrollar campañas de concientización
- Establecer políticas nacionales de ciberseguridad DNS

Referencias

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