CONCLUSIONES

CONCLUSIONES

En el presente trabajo se puede observar que la seguridad al 100% no existe y ni existirá porque la tecnología cambia día a día y las necesidades de los usuarios también.

Una implementación de medidas de seguridad han sido de años atrás el buscar las extensiones al protocolo de DNS, el no documentar, el no tener fija la meta han logrado que dicha implementación no se logre.

Las extensiones de seguridad a los Servidores de Nombre de Dominio, es lograr la seguridad e integridad mediante el firmado de *Resource Records*.
Y DNSSEC es sólo el firmar los *Resource Records* que no es más que la base de datos que conforman un Servidor de Nombres de Dominio, pero es importante no dejar a un lado a TISG o RNDS que como se vio son también claves de seguridad que se brindan al servidor de nombre de dominio y también son parte de las extensiones de seguridad, por lo que yo considero que todo en conjunto es realmente las extensiones de seguridad a DNS y no sólo DNSSEC como se maneja.

Ya que RNDS sea para la autentificación remota de los servidores, TSIG para la autentificación de servidores de una forma dinámica y DNSSEC para la integridad de la base de datos que contiene se puede, aunque este conjunto de medidas son manejadas por separado.

El protocolo DNSSEC no se ha logrado a su totalidad la implementación dado que se tiene que firmar desde la raíz (.) es decir desde los root servers y empezar a compartir la firma a las diferentes etiquetas como por ejemplo se tiene que www.ingenieria.unam.mx.

En este caso la llave que es generada por los root server y que le asignan a .mx. conocida como ZSK, para después que ésta genere sus llaves privada y pública ésta proporcionara su llave publica a NIC México, para que obtenga

éste la firma de la etiqueta .mx y a su vez comparte ZSK con nic UNAM para que firme la etiqueta unam.mx y a su vez firme todas las dependencias que se encuentran a cargo como es ingenieria.unam.mx.

Todo esto se tiene que realizar para que se concluya en su totalidad pero dado que existe una infinidad de direcciones es laborioso realizar la implementación.
Y tomando en cuenta que se realizó un cambio en la dirección y ahora es www.ingenieria.unam.mx se tiene que hacer todo lo anterior para realizar la firma al registro.

En la Universidad Nacional Autónoma de México se le asigno el segmento de red 132.248 y 132.247 y próximamente a liberar ipv6 se tiene una infinidad de dependencias exteriores a la cual se le brinda servicio, así como interiores como facultades, posgrados, centro de investigación, preparatorias, cch y entre otras, es laborioso realizar dicha implementación.

Lo que yo propondría es que se realice un análisis de las facultades que han tenido problemas de phising, o problemas con sus URLS para generar la llave de DNSSEC para que el usuario que consulta la página conosca realmente la página que está explorando está dentro de la base de datos, es la que realmente se visualiza y esto se logrará mediante la aparición de un candado en la parte superior.

Pero dicha prueba no pudo ser realizada, el visualizar el candado en la parte de la URL, ya que por problemas del equipo que no permitió la configuración debido a que se debe configurar en una red que no contenga firewall ya que no permitía confirmar de la implementación, aunado que se necesita realizar en los DNS que tiene la Universidad Nacional de México con todos los permisos de responder y autorizados por NIC UNAM.

Solo quedaría la seguridad, que el administrador de la red le proporcione a sus cuarto de telecomunicación así como del personal sea el encargado de tenga

las medidas adecuadas del equipo que es asignada la ip, porque solo con DNSSEC se garantizaría que la ip con etiqueta está en la base de datos, pero no se hace responsable del equipo.

DNSSEC es un protocolo funcional que sólo es cuestión de analizar el equipo, Sistema Operativo y que base de datos contendrá

Con esto se reforzaría la transferencia de zonas de los DNS con la utilización de las llaves de encriptación proporcionando una mayor seguridad, garantizando que el conjunto de subdominios que se encuentran bajo unam.mx revisando su autenticidad.