



UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TÍTULO DE INGENIERO EN INFORMÁTICA

Propuesta de implementación de las extensiones de seguridad DNSSEC en los servidores DNS internos de la Universidad Técnica Particular de Loja.

TRABAJO DE TITULACIÓN.

AUTOR: Guanolíque Pereira, César Danilo

DIRECTORA: Enciso Quispe, Liliana, M.Sc. Ph.D.

CENTRO UNIVERSITARIO MACHALA

2016

APROBACIÓN DE LA DIRECTORA DEL TRABAJO DE TITULACIÓN

INGENIERA.

Liliana Enciso Quispe.

DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo de titulación: Propuesta de implementación de las extensiones de seguridad DNSSEC en los servidores DNS internos de la Universidad Técnica Particular de Loja realizado por Guanoliقة Pereira César Danilo, ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, Marzo de 2016

f)

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

“Yo Guanoliqwe Pereira César Danilo declaro ser autor (a) del presente trabajo de titulación: Propuesta de implementación de las extensiones de seguridad DNSSEC en los servidores DNS internos de la universidad técnica particular de Loja, de la Titulación de Ingeniero en Informática, siendo Liliana Enciso Quispe directora del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 88 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”

f)

Autor: Guanoliqwe Pereira César Danilo

Cédula: 0703854539

DEDICATORIA

A todos los que Amo.

AGRADECIMIENTO

Agradezco a Dios sobre todas las cosas por haberme tenido paciencia en esta etapa de mi vida y siempre darme la fuerza necesaria en los momentos de desánimo y flaqueza.

A mis padres por haberme apoyado en cada etapa de mi carrera universitaria, y en especial a mi señora madre por no perder nunca la Fe en mí, gracias mamá.

A todos lo que hicieron posible este trabajo de investigación, ya que sin ellos no se podría ver sustentada toda la información expuesta en este proyecto de tesis.

A todos mis amigos y a todas las personas que moralmente me acompañaron en este proceso de investigación, que con sus palabras de aliento siempre me supieron apoyar.

A la ingeniera Liliana Enciso que ha sido una tutora excepcional, ya que gracias a su capacidad y sabiduría me ha guiado en todo el proceso de desarrollo de este trabajo de investigación.

¡Mil gracias a todos!

ÍNDICE DE CONTENIDOS

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA	i
APROBACIÓN DE LA DIRECTORA DEL TRABAJO DE TITULACIÓN	ii
DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS.....	iii
DEDICATORIA	iv
AGRADECIMIENTO	v
ÍNDICE DE CONTENIDOS	vi
ÍNDICE DE FIGURAS.....	ix
ÍNDICE DE TABLAS	xi
RESUMEN.....	1
ABSTRACT.	2
INTRODUCCIÓN.....	3
ESTADO DEL ARTE.....	6
1 CAPITULO I. Sistema de nombres de dominio (Domain Name System - DNS).....	7
1.1 Historia del DNS.	7
1.2 ¿Qué es el sistema de nombres de dominio (DNS)?	7
1.3 Nombres de dominio.....	8
1.4 Delegación de la autoridad.	9
1.5 Funcionamiento del DNS.....	9
1.5.1 ¿Qué es un servidor de nombres?	9
1.5.2 Interacción entre cliente y servidor DNS.....	10
1.5.3 Zonas de autoridad.....	11
1.5.1 Servicios DNS.....	11
1.5.2 Ubicación del protocolo DNS.	12
1.5.3 Formato del mensaje del DNS.....	12
1.5.4 Empleos de los servidores DNS.	16
1.5.5 Problemas con el servicio de nombres de dominio (DNS).....	17
1.5.6 Principales amenazas del DNS.....	17
2 CAPITULO II. Extensiones DNSSEC.....	19
2.1 ¿Qué es DNSSEC?	19
2.2 ¿Cómo funciona?.....	19

2.3	Tipos de registro de recursos creados para DNSSEC.....	19
2.4	Nuevas banderas “flags”	20
2.5	Claves públicas y privadas - (szk /ksk).....	20
2.6	Algoritmos de encriptación.....	22
2.7	Proceso de firmado de la zona del dominio www.sedes.utpl.edu.ec.....	22
2.8	Cadena de confianza.....	23
2.9	Islas y anclas de confianza.....	24
2.10	Beneficios del DNSSEC.....	25
2.11	Desventajas del DNSSEC.....	25
2.12	Herramientas que ofrecen firmado con DNSSEC.....	25
3	CAPITULO III. DNS y DNSSEC.....	27
3.1	Protección a las diferentes amenazas DNS por parte de DNSSEC	27
3.1.1	Ejemplo de un ataque DNS prevenido por DNSSEC	28
3.2	Criptografía asimétrica de clave pública en DNSSEC	30
3.2.1	Autenticación de datos DNS en el origen.....	30
3.2.2	Integridad de datos.....	30
3.2.3	Denegación de existencia autenticada.....	30
	METODOLOGÍA.....	7
4	CAPITULO IV. Situación actual.....	32
4.1	Infraestructura de la UTPL.....	32
4.2	Esquema parcial de la arquitectura del servicio DNS en UTPL.....	33
4.3	Estado actual DNSSEC de la UTPL.....	34
5	CAPITULO V. Propuesta de implementación del DNSSEC.....	37
5.1	Requerimientos mínimos.....	37
5.2	Escenario de pruebas de DNSSEC.....	38
5.3	Herramientas propuestas para el despliegue DNSSEC en los servidores DNS.....	38
5.4	Herramientas utilizadas en la propuesta para el ambiente de laboratorio.....	39
5.5	Pasos ejecutados en la configuración de los servidores DNS.....	39
5.5.1	Configuración del servicio DNS (principal y esclavo).....	39
5.5.2	Configuración del cliente en Centos.....	40
5.6	Formato del mensaje DNSSEC.....	40
5.7	Configuración DNSSEC Centos.....	41

5.7.1	Configuración de los archivos que intervienen en el despliegue del servidor DNS y de las extensiones de seguridad DNSSEC.....	41
5.7.2	Proceso de introducción DNSSEC.....	42
5.8	Configuración DNSSEC en Windows server 2012 r2.	43
5.8.1	Diagrama de introducción DNSSEC en Windows Server 2012.....	44
5.9	Diferencia entre Centos 7 y Windows Server 2012.	45
RESULTADOS.		32
6	CAPITULO VI. Pruebas.	48
6.1	Centos 7 – bind9.9.4.....	48
6.2	Validación de la configuración en los servidores DNS.	50
6.2.1	Rendimiento del servicio DNS.	50
6.2.2	Tráfico entrante y saliente en el servicio DNS.....	51
6.3	Validación y verificación DNSSEC.	51
6.3.1	Verificación DNSSEC.	51
6.3.2	Validación y verificación de la firma digital DNSSEC.	53
6.3.3	Verificación de la cadena de confianza.	54
6.3.4	Windows server 2012r2.	55
6.4	Tablas de resultados de las herramientas webs.	56
CONCLUSIONES.....		57
RECOMENDACIONES.....		58
REFERENCIAS.....		59
ANEXOS.....		48
ANEXO A. INSTALACIÓN Y CONFIGURACIÓN DE CENTOS 7- BIND 9.....		62
ANEXO B. INSTALACIÓN Y CONFIGURACIÓN DE WINDOWS SERVER 2012.		68

ÍNDICE DE FIGURAS

Figura 1. Árbol parcial inverso de la estructura del sistema de nombre de dominio.	7
Figura 2. Petición de una resolución de nombre al servidor DNS.....	10
Figura 3. Tipos de Registros de Recursos.	16
Figura 4. Registros DNSSEC.....	20
Figura 5. Cadena de confianza formada por las claves públicas y privadas.....	21
Figura 6. Proceso del firmado de zona con algoritmos de encriptación.....	22
Figura 7. Mapa mundial sobre el despliegue DNSSEC.	23
Figura 8. Estado actual del firmado de las zonas con DNSSEC de los diferentes TDLs. .	24
Figura 9. Esquema de dos islas de confianza.	24
Figura 10. Vectores de ataque al DNS.....	27
Figura 11. Protección DNSSEC a los DNS.	28
Figura 12. Ataque de envenenamiento de caché, para obtener datos del usuario.	29
Figura 13. Proceso de validación DNSSEC.	30
Figura 14. Esquema general de la UTPL.	32
Figura 15. Árbol inverso parcial del dominio de UTPL.....	34
Figura 16. Estado del firmado de la zona www.utpl.edu.ec.	35
Figura 17. Equipos que intervendrán en nuestro ambiente de laboratorio.....	38
Figura 18. Estado de nuestra interfaz de red.	64
Figura 19. Ejecución del comando ping para comprobar que exista comunicación entre los servidores.	65
Figura 20. Archivos de zona transferidos.	65
Figura 21. Configuración de cliente Centos 7.	40
Figura 22. Registro DNSSEC.....	41
Figura 23. Diagrama del proceso de introducción de DNSSEC en Centos.	43
Figura 24. Proceso de validación del DNSSEC en Windows server para el dominio sedes.utpl.edu.ec.....	45
Figura 25. Resumen de una petición DNSSEC positiva.	49
Figura 26. Respuesta DNSSEC “flag ad”.....	49
Figura 27. Consulta de servidores DNS.	50
Figura 28. Tiempos de respuesta del servidor DNS de la UTPL.	50
Figura 29. Salida de una consulta a través de DNSstop.	51
Figura 30. Plug-in DNSSEC/TLSA Validator sitio utpl.edu.ec.....	52
Figura 31. Plug-in DNSSEC/TLSA Validator sitio guayacansoft.com	52
Figura 32. Consulta DNSSEC del sitio utpl.edu.ec.....	53
Figura 33. Validación positiva DNSSEC del sitio guayacansoft.com.	54
Figura 34. Mapa DNSSEC del sitio guayacansoft.com.	55
Figura 35. Resumen de una prueba DNSSEC en un cliente Windows 8.....	55
Figura 36. GUI de Centos 7.	62
Figura 37. Archivo de configuración named.conf.	62
Figura 38. Contenido del archivo resolv.conf.	62
Figura 39. Archivo de zona directa.....	63
Figura 40. Archivo de zona inversa.....	63

Figura 41. Configuración de iptables.....	64
Figura 42. Estado del servicio iptables.....	65
Figura 43. Reinicio del servicio iptables.	65
Figura 44. Comando chkconfig.	66
Figura 45. Generación de las llaves privadas.	66
Figura 46. Generación de las llaves públicas.....	66
Figura 47. Vista general de las llaves creadas en el fichero DNSSEC-keys.....	66
Figura 48. Firma de la zona sedes.utpl.edu.ec.	67
Figura 49. Configuración fichero named.conf.....	67
Figura 50. Instalación del servidor DNS.....	68
Figura 51. Configuración del servidor DNS caché.....	68
Figura 52. Anclas o puntos de confianza.	69
Figura 53. Petición de una resolución de nombre DNS master.sedes.utpl.edu.ec.	69

ÍNDICE DE TABLAS

Tabla 1. Dominios territoriales o ccTLDs.....	8
Tabla 2. Dominios genéricos de primer nivel o gTLDs.	9
Tabla 3. Tipos de servidores de acuerdo a su configuración.....	12
Tabla 4. Estructura del mensaje DNS.	13
Tabla 5. Bit del campo parámetro y su significado.	13
Tabla 6. Sección de solicitudes del esquema del mensaje DNS.	14
Tabla 7. Formato de registro de recursos y sus componentes.	14
Tabla 8. Principales tipos de registros de recursos DNS.....	15
Tabla 9. Algoritmos aceptados para DNSSEC.	22
Tabla 10. Direcciones parcial de los hosts que contiene el servidor DNS del dominio utpl.edu.ec.	34
Tabla 11. Zona www.sedes.utpl.edu.ec del escenario propuesto.....	38
Tabla 12. Diferencias Centos 7 y Windows Server 2012.....	45
Tabla 13. Estados del Plug-in DNSSEC/TLSA Validator.....	51
Tabla 14. Registros DNSSEC.....	54
Tabla 15. Validación de las llaves, claves y registros digitales.....	56
Tabla 16. Comandos, testeos y mediciones en servidores DNS.	56

RESUMEN

En la actualidad a través de la implementación de extensiones de seguridad (DNSSEC - Domain Name System Security Extensions) se resolverían algunos de los problemas de los ataques al DNS. Por ejemplo el problema de envenenamiento de caché, el cual fue denunciado por Dam Kaminsky, en donde se describe lo sencillo que es falsificar una petición DNS (Unixwiz.net, 2008). En el presente proyecto se da solución a diferentes tipos de vulnerabilidades en el sistema de nombres de dominio y como las extensiones ayudarán a los servicios DNS de la UTPL a soportar y mitigar la mayoría de estos ataques.

En este proyecto se pretende mostrar y realizar pruebas con herramientas disponibles en la actualidad como por ejemplo BIND9, para que la zona de la Universidad Técnica Particular de Loja (UTPL) "utpl.edu.ec", se encuentre firmada digitalmente con las extensiones DNSSEC, con la finalidad de validar y asegurar con DNSSEC la zona de la UTPL, así como también la correcta administración de las firmas digitales que contienen las claves públicas y privadas de toda la zona.

PALABRAS CLAVES:

DNSSEC, DNS, Seguridad DNS, BIND9, Claves Públicas y Privadas.

ABSTRACT.

Today through the implementation of Security Extensions (DNSSEC - Domain Name System Security Extensions) some of the problems about DNS attacks would be solved. For example the problem of cache poisoning, which was reported by Kaminsky Dam, where it is described how easy is to fake a request. In this project it is given a solution to the different types of vulnerabilities in the system of domain names and how extensions help the UTPL DNS service to withstand and mitigate most of these attacks.

This Project pretends to show and testing with available tools nowadays such as BIND9, so that the area of the Technical University of Loja (UTPL) "utpl.edu.ec" be digitally signed with DNSSEC, in order to validate and secured with DNSSEC the UTPL area, as well as the proper administration of digital signatures containing public and private keys of the whole area.

KEYWORDS:

DNSSEC, DNS, DNS Security, BIND9, Public and private keys.

INTRODUCCIÓN

DNS es un pilar fundamental en el Internet, ya que sin un sistema que realice el intercambio de un nombre de dominio a una dirección IP, sería casi imposible recordar cada una de las direcciones IPs, de la red de redes Internet.

Las DNSSEC, son extensiones de seguridad que contribuyen a que el Internet sea una red más confiable, éstas extensiones se implementan en los DNS para que cada petición de un usuario tenga el mayor grado de confiabilidad, obteniendo un sitio verdadero en vez de uno fraudulento, para entre otras cosas, sustraer información crítica de los usuarios.

Debido a la naturaleza crítica que tiene el servicio DNS para la Universidad, se pretende montar un ambiente de laboratorio, con el fin de configurar y gestionar las extensiones de seguridad al DNS “DNSSEC”, tomando como referencia las configuraciones actuales que tiene la UTPL, así como también los equipos que intervienen en el funcionamiento del DNS. Una vez que se haya visto el funcionamiento de los DNS en la UTPL, se procederá a implementar las DNSSEC en los servidores configurados en el ambiente de laboratorio.

Considerando las diferentes vulnerabilidades en los DNS (envenenamiento de caché, denegación de Servicio, etc.), se presentan las extensiones de seguridad DNSSEC, como una ayuda para asegurar los diferentes servidores DNS, que se encuentran alrededor de todo el mundo; dependiendo de la infraestructura que tenga una empresa, las herramientas que se utilizan para la implementación de las extensiones DNSSEC son diferentes. En nuestro caso hemos optado por tomar la herramienta Bind9, que es uno de los software más utilizados en los DNS, el cual se configura en una distribución Linux-Centos7; también para contrastar utilizaremos otra herramienta como es la que ofrece Windows Server 2012.

Para implementar DNSSEC, se debe contar con personal capacitado y una infraestructura adecuada, así como el manejo adecuado de las claves públicas y privadas, las cuales permitirán que la información de nuestra zona (Resource Record Signature - RRSIG) esté actualizada, protegiéndose además contra ataques de cifrado.

A medida que se adopten las DNSSEC, estaremos contribuyendo para que los sitios, dominios y equipos que forman parte de la red de redes estén más seguros, y puedan soportar los diferentes ataques de personas y software malicioso, afectando de manera significativa a los diferentes servicios que se ofrecen a través de la nube. Es por eso que se deben implementar o adoptar a nivel global

DNSSEC como un esfuerzo de asegurar las redes y mitigar cada vez más las diferentes y nuevas amenazas que se presentan en nuestro entorno globalizado como es el Internet.

Al analizar cómo funcionan las DNSSEC, así como también su introducción en los servidores DNS, contamos con la experiencia necesaria para la correcta implementación de las DNSSEC, ya que al aplicar dicho conocimiento en el ambiente de laboratorio planteado para el despliegue, se observó su correcto funcionamiento. Para demostrar que se puede implementar DNSSEC en un ambiente en producción, se configuró un DNS, para el sitio www.quayacansoft.com, el cual se encuentra actualmente asegurado con las DNSSEC.

El objetivo principal fue demostrar que las DNSSEC, se pueden implementar en un ambiente de laboratorio para obtener un nivel de seguridad adicional en el servicio DNS, y así proponer que todo el procedimiento se traslade al ambiente en producción de la zona de la utpl.edu.ec.

En relación a la UTPL la zona “.ec” en la actualidad no se encuentra firmada, en este enlace (<http://dnssec-debugger.verisignlabs.com/utpl.edu.ec>) se puede verificar que la zona de nivel superior aún no está firmada digitalmente; pero esto no debería detenernos en el despliegue de DNSSEC, ya que se cuenta con la herramienta que nos ofrece el ISC - Internet Systems Consortium, con la cual podemos firmar nuestra zona y generar una isla de confianza para zona UTPL, y así difundir nuestras claves públicas al resto de sitios interesados en comprobar si la zona se encuentra firmada con las DNSSEC. Si el firmado de la zona superior “.ec”, se diera, la UTPL, solo tendría que difundir sus registros de Delegación de firma (Delegation Signer – DS) que son los que contiene información de la claves públicas del firmado DNSSEC, construyéndose así, la cadena de confianza para todo el dominio de la UTPL a nivel global.

El estudio de los componentes de la UTPL, es el primer paso que se da para el análisis, diseño e implementación de DNSSEC en la infraestructura de los DNS, verificando las configuraciones de los diferentes componentes que interfieren en el correcto funcionamiento del servicio DNS, se obtendrá la información relevante para la correcta implementación de DNSSEC.

En la sección I, se describe todo lo referente al protocolo DNS, los servicios que ofrece el sistema DNS, también se detalla cómo funciona explicando cada parte de sus componentes. Se introduce el concepto de las extensiones DNSSEC al DNS, con el objetivo de saber cómo se introducen dentro del DNS.

En la sección II, se detalla la metodología empleada para el despliegue de las extensiones DNSSEC; recogiendo el estudio inicial de la institución, para generar una propuesta de implementación, así

mismo se propone un ambiente de laboratorio para configurar los servidores DNS (Primario y Secundario) e irlos configurando para que se implementen las extensiones de seguridad DNSSEC.

En la sección III, se realizan las pruebas en el ambiente de laboratorio en los sistemas operativos Centos 7 y Windows Server 2012, así mismo se validan las extensiones de seguridad DNSSEC con herramientas webs en los dominios utpl.edu.ec y guayacansoft.com, arrojando resultados de no firmado para la zona utpl.edu.ec y firmado de la zona guayacansoft.com.

Finalmente se concluye que el despliegue de las DNSSEC en la UTPL es factible. La seguridad es un pilar fundamental en cualquier institución, motivo por el cual la UTPL deberá analizar y planificar el despliegue de las DNSSEC dentro de sus servidores DNS, ya que no se requieren múltiples recursos, además que cuenta con personal capacitado e infraestructura dentro de la misma, generando un ambiente óptimo para la implementación de las DNSSEC.

ESTADO DEL ARTE

1 CAPITULO I. Sistema de nombres de dominio (Domain Name System - DNS).

1.1 Historia del DNS.

Cuando no se contaba aún con el protocolo DNS, se tenía un archivo llamado HOST.TXT, el cual contenía información acerca de los diferentes hosts que se encontraban alrededor del mundo, este archivo cada vez se hacía mucho más grande, lo que dificultaba su distribución, y al ser compartido en la red y al llegar al último host, éste ya se volvía obsoleto, debido a la falta de planificación y a la poca visión que se tenía de la expansión de los hosts a través de la Internet.

El Sistema de Nombres de Dominio (DNS) fue desarrollado en noviembre de 1983 por Paul Mockapetris (RFC 882 y RFC 883) y luego revisado en 1987 en las RFC 1034 y 1035.

El DNS tiene un papel importante en la evolución del Internet, sin él no funcionarían lo que conocemos ahora como la Word Wide Web (Mockapetris, 1987).

1.2 ¿Qué es el sistema de nombres de dominio (DNS)?

Es una base de datos distribuida de forma jerárquica (Herrera, 2009), que almacena información asociada a los nombres de dominio que se encuentran en la red, trabaja con el formato cliente (resolver) – servidor (Servidor DNS).

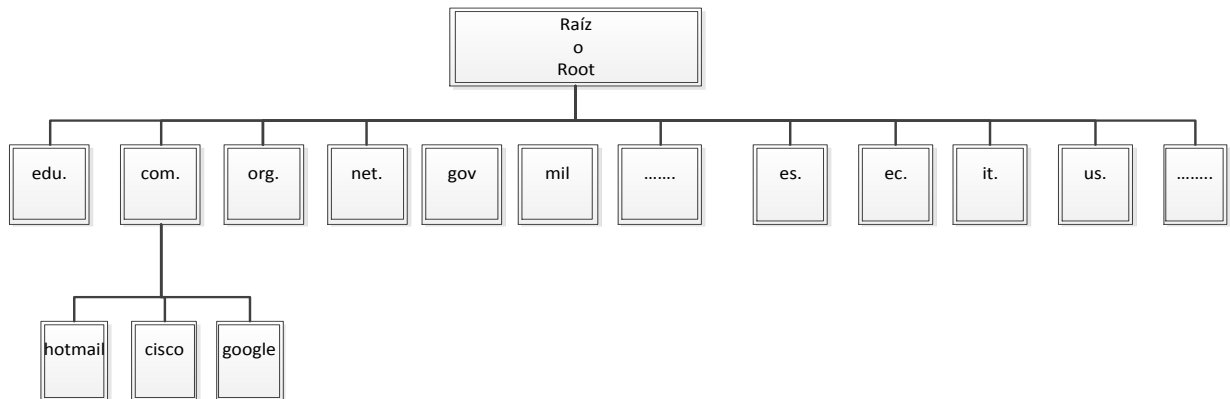


Figura 1. Árbol parcial inverso de la estructura del sistema de nombre de dominio.
Elaborado por: César Guanoliqúe.

En la figura 1, podemos destacar que el sistema de nombre de dominio DNS tiene una estructura de árbol inversa la cual se asemeja a la estructura de directorios de un sistema operativo como Linux o Windows.

Además se aprecia que la raíz no tiene etiqueta, mientras que las etiquetas de las hojas corresponden a un dominio, en el cual puede haber más subdominios.

Los nombres de los dominios de la trayectoria completa o sea del último nodo hacia la raíz, no deben superar los 255 caracteres, y los nombres (los nodos) pueden tener un máximo de 63 caracteres.

1.3 Nombres de dominio.

Los nombres de dominio son etiquetas separadas con un punto “.”, por ejemplo: utpl.edu.ec tiene tres etiquetas, el dominio de nivel inferior es **utpl.edu.ec**, el segundo nivel de dominio es **edu.ec** y el dominio de nivel superior “**ec**”. Aquí se aprecia el nivel jerárquico donde las etiquetas van definiendo el nivel en donde se encuentran.

Los nombres de dominio están divididos en dos grandes grupos de nivel superior: los geográficos o territoriales y los genéricos de tres letras.

Los geográficos también conocidos como ISO 3166-1 alfa 2, son etiquetas de nivel superior correspondientes a los territorios geográficos (ec, fr, us, co, cl, etc.). Con los genéricos se pretende identificar el tipo de organización.

En las tablas 1 y 2, se presentan algunos de los nombres de dominio territorial y genérico respectivamente.

Tabla 1. Dominios territoriales o ccTLDs.

Dominios de primer nivel territoriales	
Extensión	País
.ad	Andorra
.ae	Emiratos Arabes Unidos
.af	Afganistan
.ag	Antigua & Barbuda
.bo	Bolivia
.br	Brasil
.ec	Ecuador
.co	Colombia
.es	España

Elaborado por: César Guanoliقة.

Tabla 2. Dominios genéricos de primer nivel o gTLDs.

Dominios de primer nivel genéricos	
.biz	Negocios
.com	comerciales, es el más utilizado
.edu	Educativos
.gov	Gobierno
.info	Informativos
.int	tratados internacionales
.mil	Militares
.name	Personales
.net	manejo de redes

Elaborado por: César Guanoliqúe.

1.4 Delegación de la autoridad.

La organización que tiene un nombre de dominio como por ejemplo: utpl.edu.ec, es responsable del correcto funcionamiento y mantenimiento de su servicio DNS que traducen sus nombres de dominio.

El administrador tiene a su cargo todo lo referente a las altas, bajas y cambios que puedan ocurrir dentro de su dominio, e inclusive puede delegar a otros parte de los dominios que están bajo su responsabilidad.

1.5 Funcionamiento del DNS.

Cada host de la red tiene una dirección IP por ejemplo 192.168.0.24, la cual identifica de manera única al equipo en la red, los usuario finales están más familiarizados con los nombre de dominio como por ejemplo: www.utpl.edu.ec, que con su dirección IP(Ej.192.168.1.1). Así que para relacionar el nombre del dominio con su respectiva dirección IP, se creó el DNS, que relaciona cada nombre con la dirección IP y viceversa.

También llamamos DNS al protocolo de comunicación entre un cliente (*resolver*) y el servidor DNS. El sistema de nombres de dominios no sirve solamente para transformar nombres en direcciones IP, sino que también permite obtener información acerca de servidores de correo de una empresa en particular.

1.5.1 ¿Qué es un servidor de nombres?

Un servidor de nombres de dominio, es aquel que recibe las peticiones o consulta de los clientes, la consulta puede ser de dos tipos, **recursiva** si el servidor al que se realiza la consulta por lo

general el servidor DNS del ISP, devuelve una respuesta que se ha encontrado o no el nombre de la IP solicitada, e **iterativa**, si el servidor consulta a otros servidores DNS, hasta obtener la respuesta.

1.5.2 Interacción entre cliente y servidor DNS.

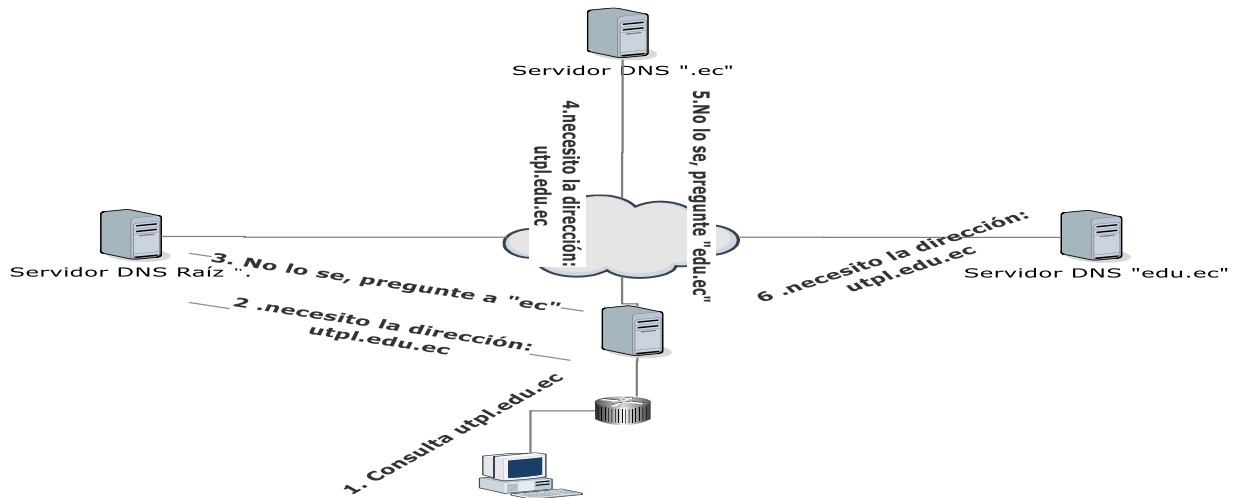


Figura 2. Petición de una resolución de nombre al servidor DNS.
Elaborado por: César Guanoliq.

A modo de ejemplo se describe el proceso de la petición de resolución de nombre www.utpl.edu.ec, al servidor DNS la cual se detalla en la figura 2.

- 1.- Nuestro cliente realiza una pregunta a nuestro servidor local.
- 2.- El servidor local es el responsable de responder a nuestro cliente la pregunta solicitada, que será la petición del sitio web www.utpl.edu.ec, el servidor verifica si tiene en su memoria caché la información solicitada, caso contrario el servidor genera otra pregunta (pregunta iterativa) al servidor DNS Raíz.
- 3.- El servidor DNS Raíz no conoce la dirección IP solicitada, pero el servidor devuelve la dirección de otro servidor DNS "ec".
- 4.-El servidor local reenvía la pregunta iterativa al servidor DNS "ec."
- 5.-El servidor DNS "ec.", tampoco sabe la dirección IP solicitada, pero si conoce la dirección del servidor DNS "edu.ec." por lo que devuelve al servidor local dicha dirección.
- 6.-El servidor local vuelve hacer la misma pregunta al servidor DNS "edu.ec"

7.-El servidor DNS “edu.ec.” si conoce la dirección IP de www.utpl.edu.ec y devuelve la dirección a nuestro servidor local.

8.-El servidor local, ya pudo obtener la información requerida por el cliente y reenvía dicha información. La información es almacenada en la caché del servidor local para posteriores solicitudes.

1.5.3 Zonas de autoridad.

Las zonas de autoridad, son aquellas que contienen una porción de un espacio de nombres de dominio que es responsable un determinado servidor DNS(TANENBAUM, 2003)(Comer, 1996).

La diferencia entre una *zona de autoridad* y un *dominio*, radica en que el primero contiene información y datos de un dominio, mientras que un *dominio* es un nombre que agrupa a otras máquinas y dominios inferiores.

Existen varios tipos de servidores, los cuales se muestran en la tabla 3, pudiendo contar con la función de autoridad los servidores: Primario y Maestro (Servidor autoritativo de la zona), éstos son los que administran todos los registros de recursos y responden a las consultas efectuadas desde otros hosts.

Los servidores autoritativos transfieren las zonas a los servidores secundarios y caché, el cual consiste en transferir toda la información de los registros de recursos de la zona.

1.5.1 Servicios DNS.

El servicio DNS está compuesto por tres partes bien diferenciadas.

- 1.- **Cliente DNS.**- son aquellos que envían las peticiones para la resolución de nombres en direcciones IP.
- 2.- **Servidores DNS.**- Son aquellos que responden las peticiones de los clientes consultando la base de datos propia o de otros servidores DNS.
- 3.- **Servidor de zona autoritativo.**- Almacena los datos de uno o varios servidores DNS.

Tabla 3. Tipos de servidores de acuerdo a su configuración.

Tipo de Servidor	Descripción
Primarios (<i>Primary Name Servers</i>)	Almacenan la información de su zona en una base de datos local. Son responsables de mantener la información actualizada y cualquier cambio debe ser notificado a este servidor
Secundarios (<i>Secondary Name Servers</i>)	Son aquellos que obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona. El proceso de copia de la información se denomina <i>transferencia de zona</i> .
Maestros (<i>Master Name Servers</i>)	Los servidores maestros son los que transfieren las zonas a los servidores secundarios. Cuando un servidor secundario arranca busca un servidor maestro y realiza la transferencia de zona. Un servidor maestro para una zona puede ser a la vez un servidor primario o secundario de esa zona. Estos servidores extraen la información desde el servidor primario de la zona. Así se evita que los servidores secundarios sobrecarguen al servidor primario con transferencias de zonas.
Locales (<i>Caching-only servers</i>)	Los servidores locales o de caché, no tienen autoridad sobre ningún dominio: se limitan a contactar con otros servidores para resolver las peticiones de los clientes DNS. Estos servidores mantienen una <i>memoria caché</i> con las últimas preguntas contestadas. Cada vez que un cliente DNS le formula una pregunta, primero consulta en su memoria caché. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta en su memoria caché y le comunica la respuesta al cliente.

Fuente:(Comer, 1996).

1.5.2 Ubicación del protocolo DNS.

La ubicación del protocolo DNS, se encuentra en la capa de aplicación del modelo TCP/IP, el cual junto a otras aplicaciones interactúan para generar el tráfico en la red.

1.5.3 Formato del mensaje del DNS.

En la tabla 4, se describe el formato de la estructura del mensaje DNS. Un programa cliente realiza una consulta en este caso puede ser nuestro navegador web, el servidor de nombres responde a esta solicitud añadiendo información de la consulta requerida al formato descrito.

Tabla 4. Estructura del mensaje DNS.

Identificación	Parámetro	
Número de solicitudes	Números de respuestas	
Número de autoridad	Número de adicional	
Sección de solicitudes		
Sección de respuestas		
Sección de autoridad		
Sección de información adicional		
0	16	31

Fuente: (Comer, 1996).

Elaborado por: César Guanoliqúe.

A continuación se describe cada uno de los campos que intervienen en una consulta.

IDENTIFICACIÓN: este campo es para hacer corresponder una respuesta con su consulta.

PARÁMETRO: especifica la operación solicitada y el tipo de respuesta. En la tabla 5, se describe los diferentes tipos de parámetros que se pueden recibir y enviar en una consulta:

Tabla 5. Bit del campo parámetro y su significado.

Bit del Campo	Significado
0	Operación: 0 → Solicitud 1 → Respuesta
1-4	Tipo de Solicitud: 0 → Estándar 1 → Inversa 2 → Terminado 1 3 → Terminado 2
5	Activado si se tiene una respuesta autorizada
6	Activado si el manejo esta truncado
7	Activado si se desea recursión
8	Activado si la recursión está disponible

9-11	Reservado
12-15	Tipo de Respuesta: 0 → Sin Error 1 → Error de formato en la solicitud 2 → Falla en el servidor 3 → El nombre no existe

Elaborado por: César Guanoliqúe.

Número de solicitudes: proporcionado en una consulta y en una respuesta.

Número de respuestas: este campo es rellenado por el servidor.

Número de registros de autoridad: proporcionado en una respuesta. La información de los registros de autoridad incluye los nombres de los servidores que contienen los datos de confianza.

Número de registros adicionales: rellenado en la respuesta. La información incluye las direcciones de los servidores de confianza.

En el campo **Sección de solicitudes**, que se representa en la tabla 6, se muestra una solicitud de nombre de dominio, en el cual el cliente solo llena la sección de solicitudes, mientras que el servidor devuelve la solicitud con su respuesta que contiene los campos *Tipo de solicitud* y *Clase de solicitud*.

Tabla 6. Sección de solicitudes del esquema del mensaje DNS.

Solicitud de nombre de dominio(sección de solicitudes)	
Tipo de solicitud	Clase de solicitud
0	31

Elaborado por: César Guanoliqúe.

Cuando se consulta al servidor los campos de las secciones: De respuestas, De autoridad y De información adicional, expuestas en la tabla 4, tienen como resultado, el mismo formato de registro de recursos expuesto en la tabla 7.

Tabla 7. Formato de registro de recursos y sus componentes.

Recurso nombre de dominio	
.....	
Tipo	Clase
Tiempo de límite de duración	Longitud de datos de recurso

Datos de recursos

Elaborado por: César Guanoliqúe.

Estos campos son conocidos como los **Registros de recursos**, para una mejor descripción están representados por 5 tuplas:

Nombre_dominio Tiempo_de_vida Clase Tipo Valor

- EL campo *Nombre_de_dominio* indica el dominio al que pertenece este registro, este campo es la clave primaria para la búsqueda.
- El campo Tiempo de límite de duración (*TTL por sus siglas en ingles*), es la duración que tiene de estabilidad el registro. La información altamente estable recibe un valor de 86,400 segundos, mientras que los no tan importantes reciben un valor de 60 segundos.
- El campo *Clase o Class*, Por lo general y en la mayoría de veces se utiliza el argumento IN que es la utilizada para información de Internet, muy rara veces se utiliza otro tipo de información.
- El campo *Tipo*, indica de qué tipo de registro se está tratando. En la tabla 8, mostramos algunos de los tipos más importantes.

Tabla 8. Principales tipos de registros de recursos DNS.

Tipo	Significado	Valor
SOA	Inicio de autoridad	Parámetros para esta zona
A	Dirección IP de un host	Entero de 32 bits
MX	Intercambio de correo	Prioridad, dominio dispuesto a aceptar correo electrónico
NS	Servidor de nombres	Nombre de un servidor para este dominio
CNAME	Nombre canónico	Nombre de dominio
PTR	Apuntador	Alias de una dirección IP
HINFO	Descripción del host	CPU y SO en ASCII
TXT	Texto	Texto en ASCII no interpretado

Elaborado por: César Guanoliqúe.

- El registro SOA proporciona el nombre de la fuente primaria de información, de la zona del servidor de nombres y la dirección de correo electrónico del administrador.
- El registro A, es el que contiene la dirección IP de 32 bits de algún host, por consiguiente es el registro más importante del registro de recursos.

- El registro *MX* que especifica el nombre de dominio que está disponible para recibir correo electrónico.
 - El registro *NS* especifica servidores de nombres para cada dominio.
 - El registro *CNAME* permite la creación de alias, que permite direccionar la petición a nuestro dominio.
 - El registro *PTR* es un puntero que se usa para asociar un nombre de dominio a una dirección IP con el fin de realizar una búsqueda inversa; es decir que con la correspondiente dirección IP, se puede obtener la dirección web del equipo.
 - El registro *HINFO* nos da información del equipo y del sistema operativo.
 - El registro *TXT* da información arbitraria acerca de los dominios.
- El último campo de nuestra tupla es el llamado *Valor*, este campo puede ser numérico, un nombre de dominio o una cadena de caracteres.

A manera de ejemplo tomaremos la base de datos correspondiente al dominio `sedes.utpl.edu.ec` para observar las tuplas y registros DNS, tal como se muestra en la figura 3.

```

$ORIGIN sedes.utpl.edu.ec.
$TTL 86400
@      IN SOA  masterdns.sedes.utpl.edu.ec.  root.sedes.utpl.edu.ec. (
                                2          ; serial
                                3600       ; refresh
                                1800       ; retry
                                604800    ; expire
                                86400     ) ; minimum

; Nombre de los servidores
@      IN     NS      masterdns.sedes.utpl.edu.ec.
@      IN     NS      slavedns.sedes.utpl.edu.ec.

; Direcciones Ip's de los servidores DNS
@      IN     A       192.168.1.101
@      IN     A       192.168.1.102

;Maquinas y servicios en el Dominio sedes.utpl.edu.ec
@      IN     A       192.168.1.11
@      IN     A       192.168.1.12
masterdns  IN     A       192.168.1.101
slavedns   IN     A       192.168.1.102
pcadmin    IN     A       192.168.1.11
pcsecretaria IN     A       192.168.1.12
moodle     IN     A       192.168.1.172
uio        IN     A       192.168.1.111
gye        IN     A       192.168.1.121

```

Figura 3. Tipos de Registros de Recursos.
Elaborado por: César Guanoliقة.

1.5.4 Empleos de los servidores DNS.

Entre los usos más comunes que prestan los servidores de nombres de dominio tenemos:

Resolución de nombres: Convertir un nombre de host en la dirección IP que le corresponde. Por ejemplo, al nombre de dominio `utpl.edu.ec`, le corresponde la dirección IP `172.30.245.35`.

Resolución inversa de direcciones: Es el mecanismo inverso al anterior, de una dirección IP obtener el nombre de host correspondiente.

Resolución de servidores de correo: Dado un nombre de dominio (por ejemplo gmail.com), obtener el nombre del servidor a través del cual debe realizar la entrega del correo electrónico.

Los servidores DNS también guardan una serie de datos de cada dominio, conocidos como DNS Record, incluyen información del propietario, fecha de creación, vencimiento, etc.

1.5.5 Problemas con el servicio de nombres de dominio (DNS).

El DNS es un punto crítico en una empresa, el cual debe seguir respondiendo las consultas que están dirigidas a los servidores DNS aún, cuando estén bajo ataque. Si nuestro servidor externo cae nuestra empresa estaría desconectada de Internet.

(Infoblox, 2013) Solamente en el último año (2014), los ataques de DNS aumentaron en más del 200%. Los atacantes buscan los enlaces más débiles de la red, y el protocolo DNS es fácil de atacar. En consecuencia, los ataques diseñados para desconectar los servidores y consumir el ancho de banda de la red, y para interferir o cerrar aplicaciones de TI críticas como el correo electrónico, sitios web, VoIP y software como un servicio (SaaS), están en auge.

1.5.6 Principales amenazas del DNS.

El 9 de Junio del 2008 fue reportada una vulnerabilidad en el protocolo DNS por DAN KAMINSKY, la cual afectaba tanto al diseño del propio protocolo como a la implementación del mismo, por los fabricantes de dispositivos, estamos hablando del **envenenamiento de la caché al DNS** o también llamado Caché Poisoning (Stewart, 2003).

Entre algunas de las amenazas descritas en el RFC 3833 y según Atkins & Austein (2004) tenemos los de mayor frecuencia al DNS.

Los ataques específicos de DNS, atacan vulnerabilidades en el software de DNS.

Los ataques de amplificación de DNS directos, congestionan el ancho de banda de salida enviando una gran cantidad de consultas de DNS que están creadas específicamente para generar una respuesta masiva.

Los ataques de reflexión, utilizan un servidor DNS de terceros (normalmente un servidor de nombres recursivo abierto) en Internet para propagar un ataque de DoS o DDoS enviando consultas a ese servidor recursivo, que procesará consultas desde cualquier dirección IP. El

atacante incluye la dirección IP de la víctima como IP fuente de la consulta, de modo que el servidor de nombres envía todas las respuestas a la dirección IP de la víctima y posiblemente lo hará congestionar y a su vez evitara que preste sus servicios (Handley & Rescorla, 2006).

Las congestiones de TCP, UDP e ICMP, explotan el Protocolo de Control de Transferencia (TCP), el Protocolo de Datagramas de Usuario (UDP) y el Protocolo de Mensajes de Control de Internet (ICMP) para consumir el ancho de banda de la red y los recursos con grandes volúmenes de paquetes.

El envenenamiento de la caché de DNS (DNS Poisoning), consiste en insertar un registro de dirección falso de un dominio de Internet en una consulta de DNS. Si el servidor DNS acepta el registro, se responde a las solicitudes posteriores con la dirección de un servidor controlado por el atacante y las solicitudes web y correos electrónicos entrantes van a la dirección del atacante (Fall, 2008).

Las anomalías de protocolo envían paquetes de DNS con estructura incorrecta al servidor objetivo y provocan un bucle infinito en el subproceso del servidor o hacen que éste deje de responder.

Los dispositivos de reconocimiento no son ataques, son intentos de obtener información sobre el entorno de red antes de lanzar un gran ataque DDoS o de otro tipo.

La tunelización de DNS implica la tunelización de otro protocolo a través del puerto 53 de DNS, que normalmente está autorizado por el firewall para transportar tráfico que no es de DNS. Estos ataques se utilizan para la filtración de datos.

2 CAPITULO II. Extensiones DNSSEC.

En vista a las diferentes vulnerabilidades al protocolo DNS, se ha venido trabajando con diferentes mecanismos de seguridad, dando como resultado las extensiones de seguridad al protocolo DNS (DNSSEC por sus siglas en inglés). Podemos destacar lo que nos dice Daniel Karrenberg (Karrenberg, 2010) de cómo la comunidad de Internet viene trabajando en el despliegue de DNSSEC.

2.1 ¿Qué es DNSSEC?

Un conjunto de extensiones de seguridad que se implementa al protocolo DNS, éstas extensiones crean una capa adicional de seguridad que protege al DNS contra diferentes tipos de ataques (por Ej: DNS-Caché poisoning), con el fin de que los datos obtenidos sean válidos para los distintos clientes que generan diferentes tipos de consultas.

2.2 ¿Cómo funciona?

DNSSEC permite firmar criptográficamente una zona haciendo que los datos pedidos por el cliente sean autenticados por éste, a través de una clave pública siguiendo algoritmos y procesos de encriptación que puedan validar su contenido.

Cuando un cliente hace una consulta al servidor DNS, el servidor devuelve las firmas digitales, además de los *recursos de registros* solicitados.

Un cliente u otro servidor, pueden obtener la clave pública, del par de claves pública o privada del servidor consultado, y validarlas para saber que los datos no han sido manipulados, para lo cual el **cliente** o el **servidor** deben configurarse con un ancla de confianza para la zona firmada por el servidor de la zona superior. Por consiguiente DNSSEC proporciona integridad y autenticidad de los datos, pero no garantiza la confidencialidad de los datos.

2.3 Tipos de registro de recursos creados para DNSSEC.

A la estructura actual del DNS se han incrementado algunos nuevos registros para la operatividad de DNSSEC.

- RRSIG (Resource Record Signature).- Registro de la firma, contiene información del RRSet (Resource Record Set) con firma digital, establecida por la ZSK (Zone Signing Key).
- DNSKEY (DNS public key).- Es la firma pública, sirve para verificar las firmas de los registros RRSIG.

- NSEC (Next Secure). Nos permite verificar un registro no existente a través de la firma digital de su RRSIG. Este registro fue reemplazado por NSEC3, debido al comportamiento del mismo y la vulnerabilidad que presentaba.
- DS (Delegation Signer). Contiene un Hash de la clave pública de la zona y a su vez es entregado a la zona superior con el objetivo de que los datos no han sido manipulados y este a su vez genera un RRSIG con un hash con la clave pública del mismo, este proceso se genera hasta en nodo raíz generando una cadena de confianza.

DNSSEC firma una tupla de registro de recursos **RR** es decir hace un **RRSet** que comparte:

Clase, Tipo, Nombre. Por ejemplo:

- www 86000 IN A 192.168.1.101.

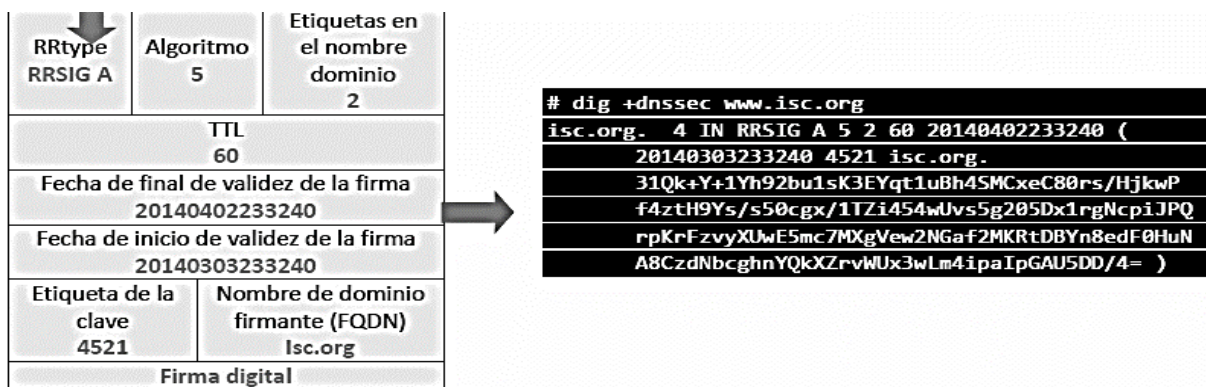


Figura 4. Registros DNSSEC.
Fuente: (Padilla, 2013).

En la figura 4, se puede observar el formato de un mensaje DNSSEC, que contiene información de la zona isc.org, así como también la información correspondiente al firmado del conjunto de registros de recursos RRSet.

2.4 Nuevas banderas “flags”.

AD (Authenticated Data).- Con esta bandera podemos identificar que la respuesta está autenticada.

CD (Checking Disabled). Muestra al usuario que el chequeo DNSSEC no se ha efectuado.

2.5 Claves públicas y privadas - (szk /ksk).

Las claves ZSK (Zone Signing Key) y KSK (Key Signing Key), son las encargadas de generar las claves para la correspondiente firma de cada zona, a través de un registro tipo DS (firmante de

la delegación) que se encarga de firmar las zonas inferiores, las cuales tendrían ahora sus propios registros DNSKEY y DS.

La figura 5 explica cómo se lleva a cabo el proceso de firmado, todo comienza con la firma de la zona raíz, la cual se firma de manera offline, para que su proceso de firmado no quede expuesto al levantar el servidor raíz, una vez hecho esto el servidor cuenta con los registros DNSKEY y DS, los cuales a través de un proceso de delegación de clave se genera comienza el firmado hasta la zonas inferiores, formándose la cadena de confianza en todo el árbol.

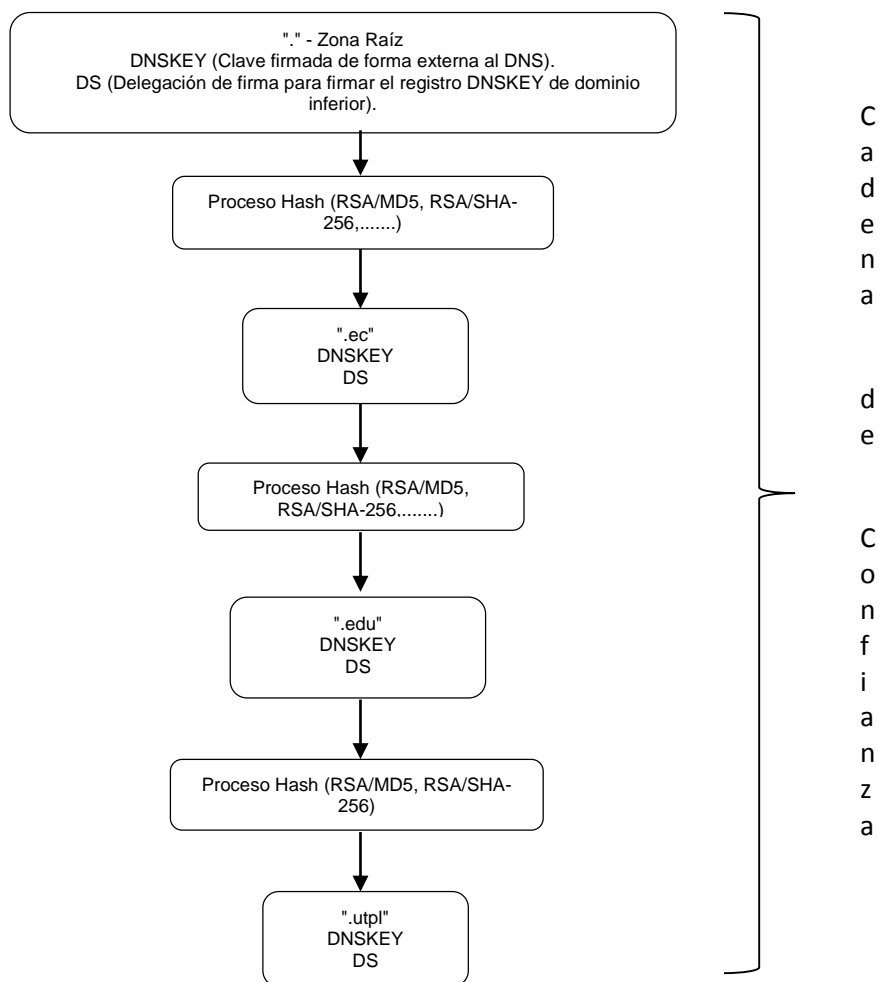


Figura 5. Cadena de confianza formada por las claves públicas y privadas.
Elaborado por: César Guanoliقة.

2.6 Algoritmos de encriptación.

Existen algunos tipos de algoritmos de encriptación validados para DNSSEC, no podemos decir que estos algoritmos estarán libres de ataques, para eso DNSSEC admitirá nuevas versiones de los algoritmos compatibles con los anteriores. En la tabla 9, se detalla los principales algoritmos aceptados para DNSSEC.

Tabla 9. Algoritmos aceptados para DNSSEC.

Campo del algoritmo	Algoritmo	Fuente
0	Reservado	<u>RFC 4034</u>
1	<u>RSA/MD5</u>	
3	<u>DSA/SHA-1</u>	
5	RSA/SHA-1	
7	RSASHA1-NSEC3-SHA1	<u>RFC 5155</u>
8	RSA/SHA-256	<u>RFC 5702</u>
10	RSA/SHA-512	
12	<u>GOST R 34.10-2001</u>	<u>RFC 5933</u>

Elaborado por: César Guanoliqúe.

2.7 Proceso de firmado de la zona del dominio www.sedes.utpl.edu.ec

Para firmar una zona de un dominio en particular, se debe contar con las herramientas necesarias para el firmado de una zona, de acuerdo a la herramienta o software que se esté utilizando en el servidor DNS de la institución.

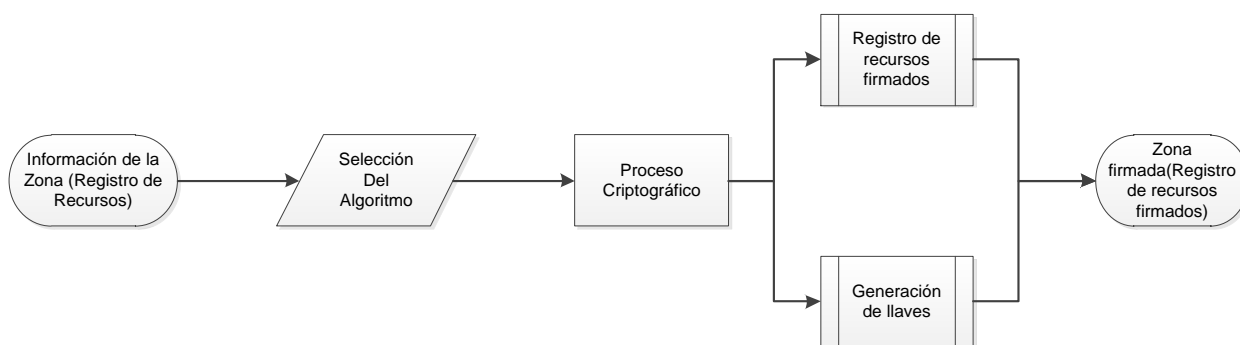


Figura 6. Proceso del firmado de zona con algoritmos de encriptación.

Elaborado por: César Guanoliqúe.

La figura 6 explica cómo se desarrolla el proceso de firmado de una zona, que en nuestro caso es la zona, [sedes.utpl.edu.ec](http://www.sedes.utpl.edu.ec), en primer lugar se obtiene la ubicación de archivo donde contiene los registros de recursos para la zona, después se debe seleccionar un algoritmo de encriptación descritos en la tabla 9, luego a través de comandos se procede a la aplicación del algoritmo al

fichero que contiene los registros de recursos, dándonos como resultado un par de llaves (KSK y ZSK), así como también los registros firmados digitalmente, ya podemos decir que nuestra zona se encuentra firmada digitalmente con DNSSEC.

2.8 Cadena de confianza.

Una cadena de confianza comienza desde la zona raíz a través de su firma digital, es decir primero se debe firmar la zona raíz para que los dominios de nivel superior (ccTLD y gTLD) y subdominios de cada estructura puedan firmarse en base a su clave pública, tal como se muestra en la figura 5. Debido a que algunas partes de los dominios de nivel superior no están firmados, los administradores de dominios inferiores pueden crear sus propias cadenas de confianza.

La cadena de confianza tiene un importante impacto para el despliegue de DNSSEC, ya que nos proporciona un punto de partida para firmar nuestras zonas o dominios inferiores.

Otro dato que hay que aportar es que hasta la actualidad el dominio de nivel superior (ccTLD) “.ec”, no está firmado por consiguiente no cuenta con registros DS y DNSKEY. En la figura 6, se muestra en qué estado se encuentra el despliegue de DNSSEC en el mundo, mientras que en la figura 7, se visualiza el estado actual de cada uno de los dominios de primer nivel con respecto al firmado de su zona con DNSSEC.

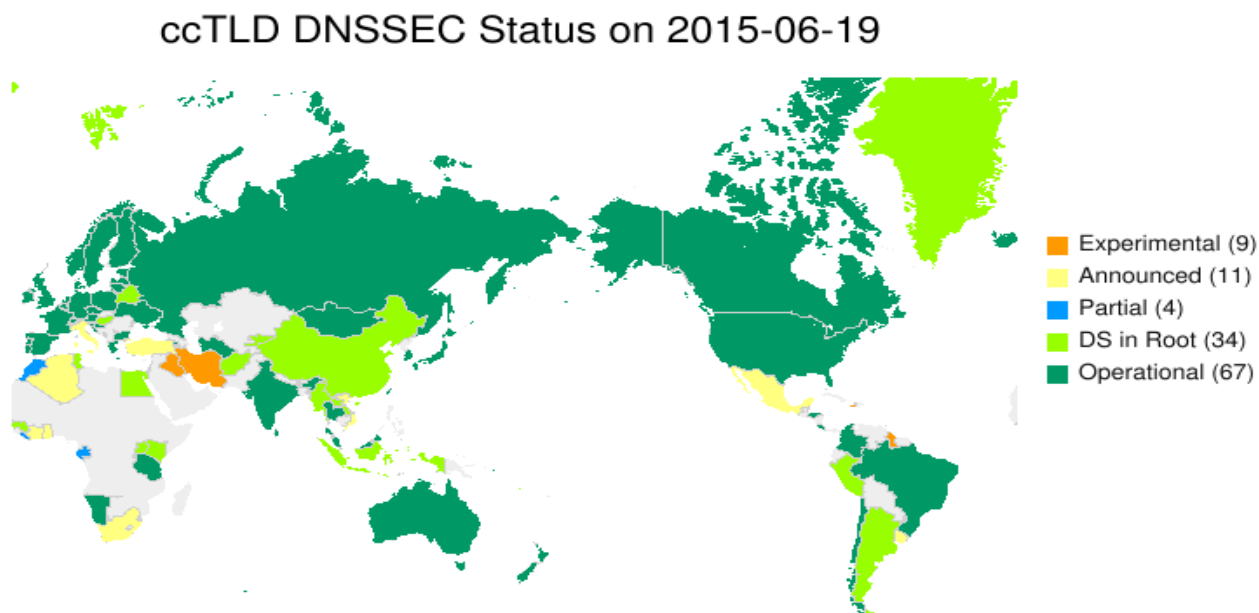


Figura 7. Mapa mundial sobre el despliegue DNSSEC.
Fuente:("DNSSEC Deployment Maps | Deploy360 Programme," 2015.).

2.9 Islas y anclas de confianza.

En las figuras 7 y 8, se puede evidenciar que el ccTLD “.ec”, ni siquiera se encuentra en fase experimental en lo que se refiere al despliegue DNSSEC, por consiguiente la zona no se encuentra firmada.

TLD DNSSEC Report (2016-01-25 00:02:30) Summary

- 1205 TLDs in the root zone in total
- 1042 TLDs are signed;
- 1034 TLDs have trust anchors published as DS records in the root zone;
- 5 TLDs have trust anchors published in the ISC DLV Repository.



TLD	Signed?	DS in Root?	ISC DLV?
eat.	YES	YES	NO
ec.	NO	NO	NO
edeka.	YES	YES	NO
edu.	YES	YES	NO
education.	YES	YES	NO

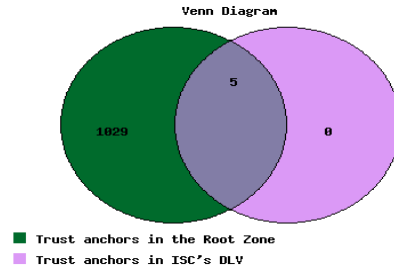


Figura 8. Estado actual del firmado de las zonas con DNSSEC de los diferentes TDLs.
Fuente: ("ICANN Research - TLD DNSSEC Report," 2016.).

Las *Islas de Confianza* vendrán a ser el dominio asegurado con DNSSEC, es decir que una isla de confianza se forma a través de firmar nuestro dominio utpl.edu.ec, a través de un ancla de confianza, con el cual se genera una clave pública, para que ésta pueda ser usada como comienzo de la cadena de confianza, y también para que los demás sitios validen DNSSEC.

En la figura 9, se muestra como se podrán generar islas de confianza con DNSSEC, así no se encuentren firmados aún el dominio de nivel superior.

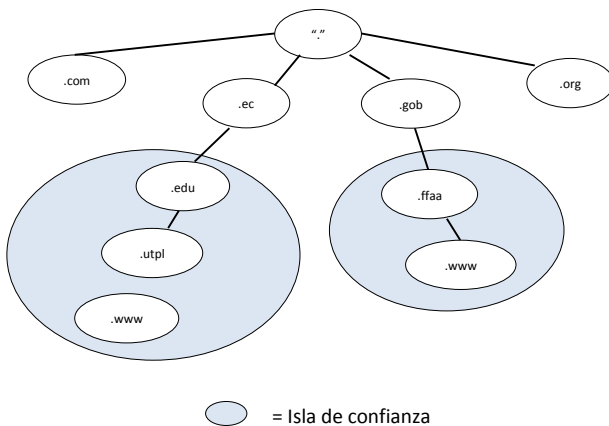


Figura 9. Esquema de dos islas de confianza.
Elaborado por: César Guanoliقة.

El ancla de confianza no es más que la *clave pública* de nuestra zona que permite generar a nuestra cadena de confianza en nuestro dominio. Es decir es el punto de partida para ir firmando nuestros subdominios a pesar que el dominio de nivel superior no se encuentre firmado aún.

2.10 Beneficios del DNSSEC.

Cuando se trata de obtener información de Internet o de un sitio web que conocemos, esperamos que toda la información que estamos solicitando sea verídica, por tal motivo las DNSSEC tratan de resolver o de acabar con las vulnerabilidades al DNS.

A través de los RFC 4033, 4034, 4035, nos dan la pauta de cómo estas extensiones beneficiarían al usuario y a los administradores de servidores de nombres de dominio a que sus datos sean los que corresponda a cada sitio o dominio web.

En consecuencia no sólo los clientes y servidores DNS se beneficiarían de estas extensiones de seguridad sino que también las diferentes aplicaciones y protocolos que funcionan en la capa de aplicación del modelo TCP/IP.

Se puede citar las palabras de Elspeth Wales (Wales, 2000), que expresa que a través de estas extensiones se protege contra hackers que secuestran el tráfico Web y redirigen a sitios falsos.

2.11 Desventajas del DNSSEC.

Entre los puntos negativos de las extensiones de seguridad del DNS, tenemos: son complejos gestionar, y que las transferencias de las zonas entre los servidores primario y secundario son de gran tamaño. Como nos explica Casey Deccio (Deccio, 2012) en su artículo, en el cual nos habla sobre lo tedioso que implica implementar DNSSEC en nuestros servidores DNS.

Las extensiones no garantizan la confidencialidad de los datos, ya que las peticiones no son encriptadas, tampoco protege contra los Ataques de Denegación de Servicio.

Otro problema es quién será la persona que estará a cargo de la administración de las claves, las cuales deben ser actualizadas periódicamente para garantiza la seguridad de las mismas. El proceso para el despliegue de DNSSEC, conlleva a mucha configuración manual, lo que incrementa la posibilidad de error humano en el proceso de configuración.

2.12 Herramientas que ofrecen firmado con DNSSEC.

Existen en la actualidad diversas herramientas o distribuciones que permiten el firmado DNSSEC en los servicios DNS, entre las más utilizadas tenemos:

- **OpenDNSSEC.** Es un software de código abierto que se encuentra en fase de pruebas, así que aún no se lo debe usar en producción, está diseñado para implementar todas las extensiones de seguridad del DNS.
- **BIND9.** Es el servidor de nombres de dominios más utilizado en el mundo, está diseñado para que trabaje con las extensiones de seguridad DNSSEC, y más comúnmente utilizado en sistemas operativos como UNIX/LINUX, a pesar que también existen versiones para Windows, muy poco usadas.
- **UNBOUND.** Servidor de nombre de dominio DNS, es amigable con DNSSEC, ya que este ha sido el punto de partida para su desarrollo, está bajo una licencia BSD, es mantenido por los laboratorios NLnet Labs, organización sin fines de lucro.
- **WINDOWS SERVER.** Es el software de la empresa Microsoft para servidores de dominio DNS, y todos sus productos Windows, tiene soporte para DNSSEC, y cuenta con una instalación en líneas de comandos, como una interfaz gráfica de usuario.

3 CAPITULO III. DNS y DNSSEC.

DNSSEC no es un protocolo que viene a reemplazar al protocolo DNS, sino que son extensiones de seguridad que se introducen en el protocolo DNS para asegurar la información del mensaje DNS, así obtener una respuesta verídica del sitio al cual estamos visitando, es decir que el dominio al cual estamos consultando es legítimo.

3.1 Protección a las diferentes amenazas DNS por parte de DNSSEC

Los puntos o vectores de ataques al flujo de datos empleados en el servicio DNS que se representan en la figura 10, con los cuales vamos a describir como las DNSSEC ayudan a mitigar algunos de estos problemas.

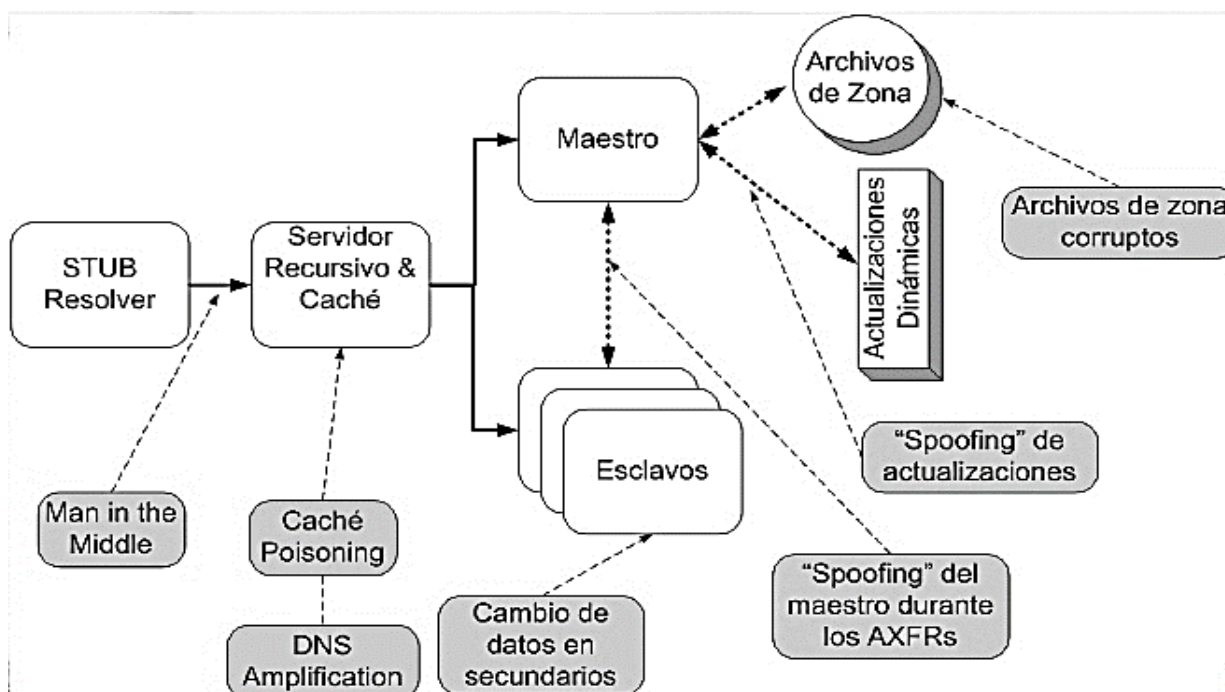


Figura 10. Vectores de ataque al DNS.
Fuente: (Martínez-Cagnazzo, 2011).

En la figura 10, se describen varios vectores de ataques a los DNS y los distintos puntos donde los atacantes pueden introducir información corrupta o a su vez capturar la información para después manipularla, con el objetivo de hacer daño a los servicios y usuarios. Es aquí donde DNSSEC actúa protegiendo de las vulnerabilidades que tienen los DNS, proporcionando una verificación de los datos de las zonas, en el caso de los servidores DNS o la verificación de los datos devueltos a los clientes o usuarios.

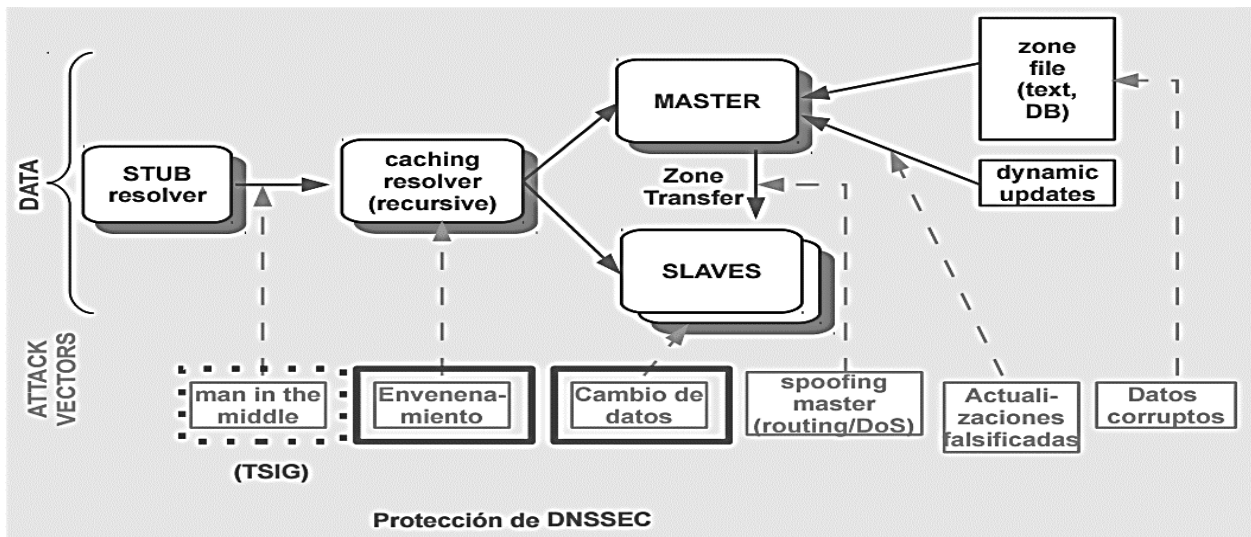


Figura 11. Protección DNSSEC a los DNS.
Fuente: (Network Startup Resource Center, 2015).

La figura 11 muestra donde DNSSEC actúa para proteger a los DNS, dando soporte de verificación a los clientes de extremo a extremo.

El despliegue DNSSEC en los servidores DNS, requieren de un análisis completo de cómo y cuándo se debería implementar los DNSSEC, elaborándose estrategias de configuración y actualización de software (BIND9).

Se debe realizar un proceso de verificación de costos y tiempo que llevaría el despliegue de las extensiones de seguridad DNSSEC, así como el personal capacitado.

3.1.1 Ejemplo de un ataque DNS prevenido por DNSSEC

Vamos a presentar un ejemplo claro de cómo DNSSEC nos ayuda a prevenir un ataque que se llama envenenamiento de caché (Cache Poisoning/Spoofing).

Si un usuario o estudiante de la UTPL, tiene la necesidad de realizar su pago de matrícula en línea y debe visitar la dirección correspondiente a los pagos, pagosutpl.edu.ec, el ataque de envenenamiento de caché se produce cuando un atacante inyecta datos corruptos al servidor DNS y redirecciona el tráfico DNS a un servidor web del atacante. En la figura 12, se describe gráficamente el proceso del ataque de envenenamiento de caché con la finalidad de obtener datos del usuario.

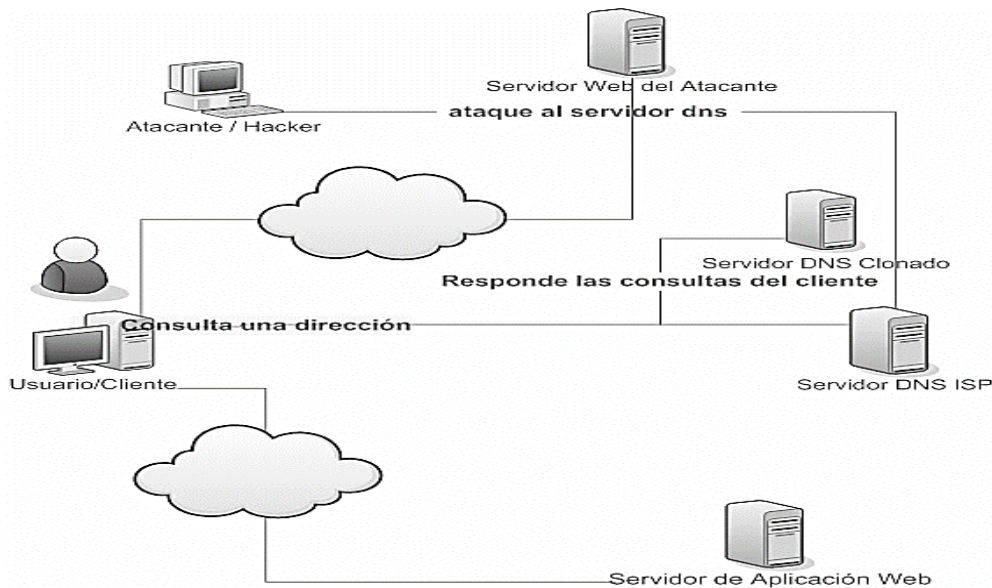


Figura 12. Ataque de envenenamiento de caché, para obtener datos del usuario.
Elaborado por: César Guanolíque.

Una vez obtenido los datos del servidor DNS, el atacante puede crear copias de las páginas que más se visita por ejemplo: pagos.utpl.edu.ec, el atacante genera una página similar a la cual redirecciona al cliente al momento de hacer una consulta a dicha página y aprovecha para sustraer la información del usuario y después de obtenida la información el atacante redirecciona al sitio original.

Este proceso sucede sin que el usuario final se dé cuenta, ya que al final de la transacción él usuario será redirigido al sitio que originalmente ingreso.

Aquí es donde intervienen las extensiones de seguridad DNSSEC, ya que dichas extensiones proporcionan un mecanismo para verificar que los datos proporcionados son enviados por el servidor DNS autorizado.

En la figura 13, se muestra el proceso de validación que se efectúa con criptografía en el cual se crea una firma digital de los registros de recursos, así tanto el emisor como el receptor verifican la autenticidad de los datos, como la integridad y a su vez la no existencia de registros. Con esto el usuario está protegido y tiene la seguridad que el sitio que está visitando es el correcto, ya que si es llevado a un sitio fraudulento DNSSEC, advertirá al usuario que el sitio no es el que se está consultando.

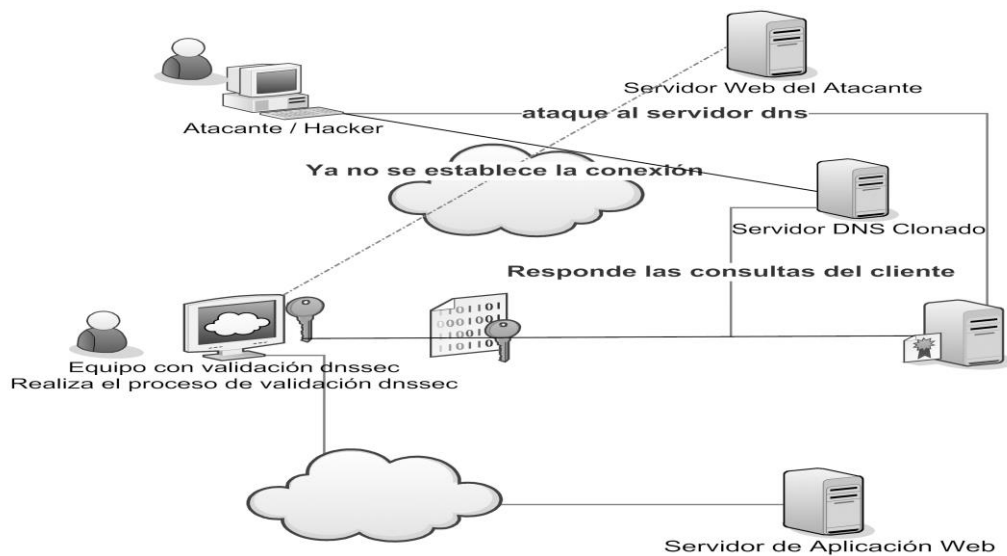


Figura 13. Proceso de validación DNSSEC.
Elaborado por: César Guanoliqúe.

3.2 Criptografía asimétrica de clave pública en DNSSEC

La utilización de criptografía es fundamental en las extensiones DNSSEC, sin esta no se podría realizar el firmado de los registros de recursos y no se garantizaría los siguientes aspectos:

3.2.1 Autenticación de datos DNS en el origen.

Las DNSSEC permiten comprobar a través de diferentes técnicas de comprobación (función Hash-algoritmos de encriptación) que los datos recibidos son enviados por el emisor original.

3.2.2 Integridad de datos.

Así mismo DNSSEC ayuda a que la integridad del mensaje recibido no ha sido alterada en el transcurso de la transmisión, el cual no da la seguridad de que los registros contenidos son los que se enviaron.

3.2.3 Denegación de existencia autenticada.

DNSSEC utilizará para comprobar la denegación de existencia autenticada de los nuevos registros de recursos NSEC/NSEC3, los cuales nos ayudan a establecer si un registro se encuentra o no, dándonos diferentes respuestas:

- NXDOMAIN indica que un nombre no existe,
- NOERROR, si la respuesta está vacía,

Por lo tanto el NSEC comprueba que el tipo de dominio no existe.

METODOLOGÍA.

4 CAPITULO IV. Situación actual.

La UTPL, maneja sus propios servicios DNS, motivo por el cual se plantea esta tesis con el tema de la propuesta de implementación de las DNSSEC dentro de los DNS de la UTPL, a través de herramientas preestablecidas, las cuales se integran al servicio DNS, dando como resultado una capa adicional de seguridad a los servidores DNS de la UTPL.

Inicialmente el servicio DNS de la UTPL se encuentra operando con normalidad, pero éste no está exento de ataques a sus servicios por lo cual las DNSSEC, aportarán a que su estructura esté protegida y asegurada al proporcionar sus servicios.

4.1 Infraestructura de la UTPL.

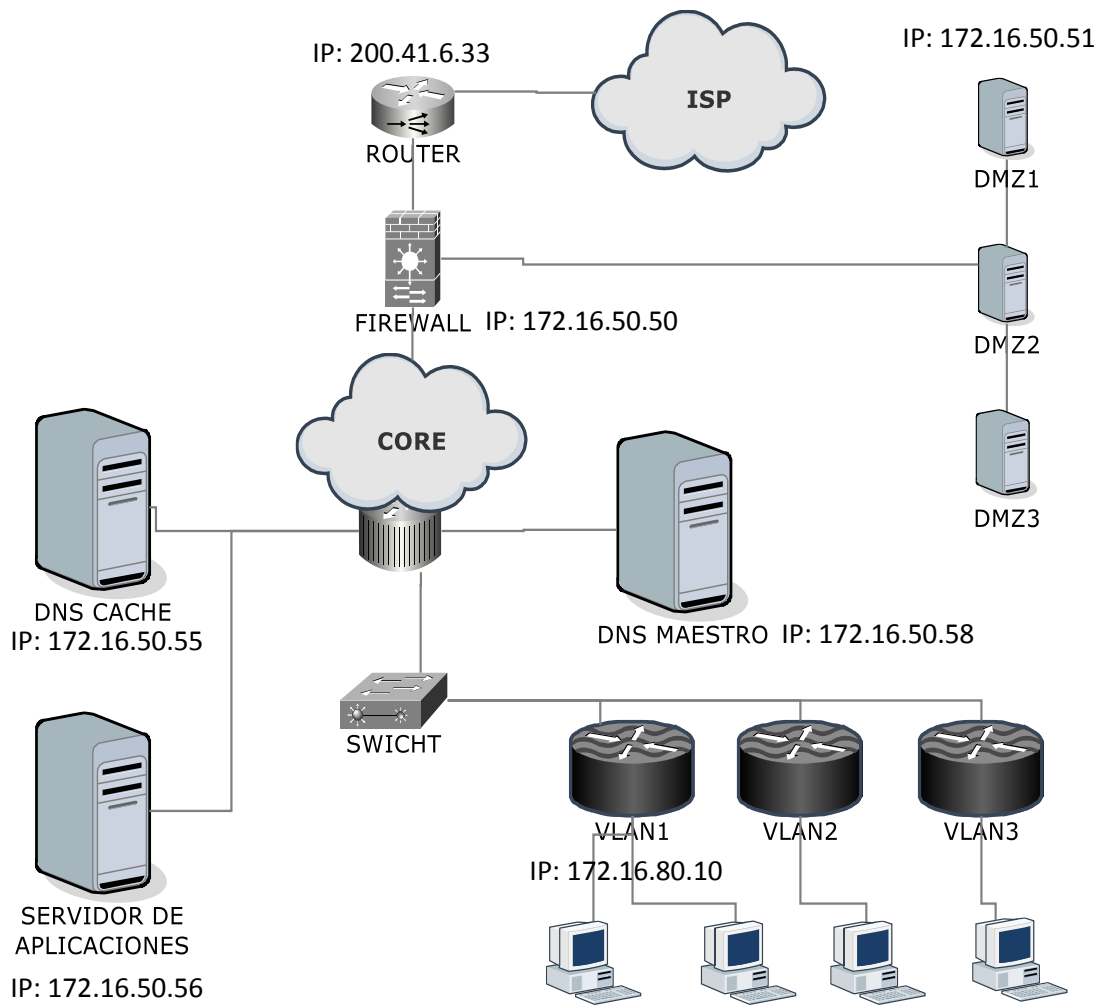


Figura 14. Esquema general de la UTPL.
Elaborado por: César Guanoliq.

En la figura 14, se muestran los equipos que intervienen en la infraestructura de la UTPL:

- Servicio ISP
- Router
- Firewall
- Zona desmilitarizada (DMZ)
- Core
- Servidor de aplicaciones
- Switch
- Vlans
- Estaciones de trabajo

En lo referente a los servicios DNS están:

- Servidor interno (Caché), encargado de responder internamente todas las peticiones de los estudiantes, personal docente y administrativo.
 - Software Ubuntu 12.04
 - Software DNS: Bind 9.2.4-16.EL4
 - Memoria ram 2 GB
 - Disco duro de 80 GB
 - CPU 2,4 MHz
- Servidor externo (Maestro). Servidor autoritativo, es el encargado de administrar toda la zona utpl.edu.ec.
 - Software Ubuntu 14.04
 - Software DNS: Bind 9.3.6-P1
 - Memoria ram 4 GB
 - Disco duro de 360 GB
 - CPU 2,8 MHz

4.2 Esquema parcial de la arquitectura del servicio DNS en UTPL.

Para una mejor comprensión de la infraestructura de la UTPL, vamos a tomar una parte de su estructura, la cual está designada en servicios (Sub-dominios), y no comúnmente dentro del mismo dominio de la UTPL.

La tabla 10 presenta parcialmente la infraestructura del servicio DNS de la UTPL, en el cual se describe el servicio, dirección y su descripción.

Tabla 10. Direcciones parcial de los hosts que contiene el servidor DNS del dominio utpl.edu.ec.

DOMINIO utpl.edu.ec		
Servicio o sub-dominio	Dirección	Descripción
eva1.utpl.edu.ec	107.23.95.101	Entorno Virtual de aprendizaje
biblioteca.utpl.edu.ec	172.16.80.14	Biblioteca Benjamín Carrión
tramites.utpl.edu.ec	172.16.80.37	Trámites académicos
srv-si-001-utpl.edu.ec	172.16.95.14	Pagos en línea
investigacion.utpl.edu.ec	200.41.6.33	Investigaciones de la UTPL
educ.utpl.edu.ec	200.41.6.33	Educación continua

Elaborado por: César Guanolíque.

En la figura 15, se visualiza la estructura jerárquica del dominio utpl.edu.ec, desde la raíz hasta el dominio inferior, contando con servicios adicionales y a su vez subdominios por ejemplo: eva.utpl.edu.ec, biblioteca.utpl.edu.ec, entre otros.

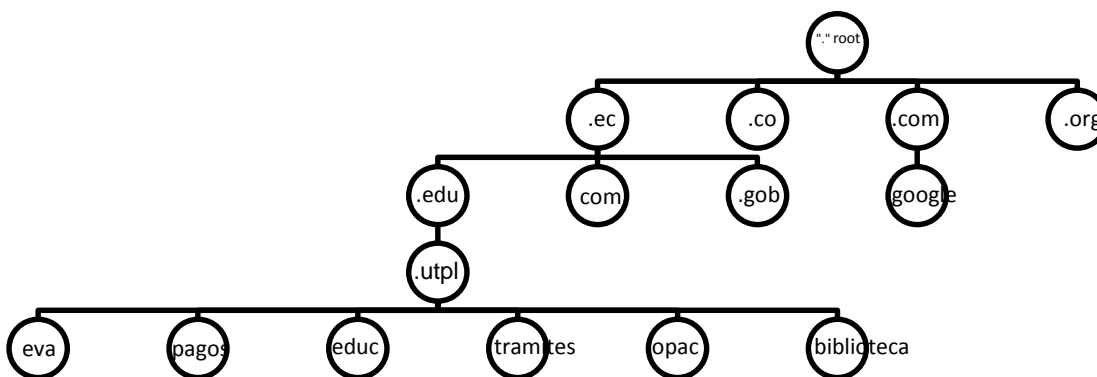


Figura 15. Árbol inverso parcial del dominio de UTPL.

Elaborado por: César Guanolíque.

4.3 Estado actual DNSSEC de la UTPL.

Se comprobó el estado actual del firmado DNSSEC de la zona utpl.edu.ec, la cual se puede observar en la figura 16, que no se encuentra firmada digitalmente.

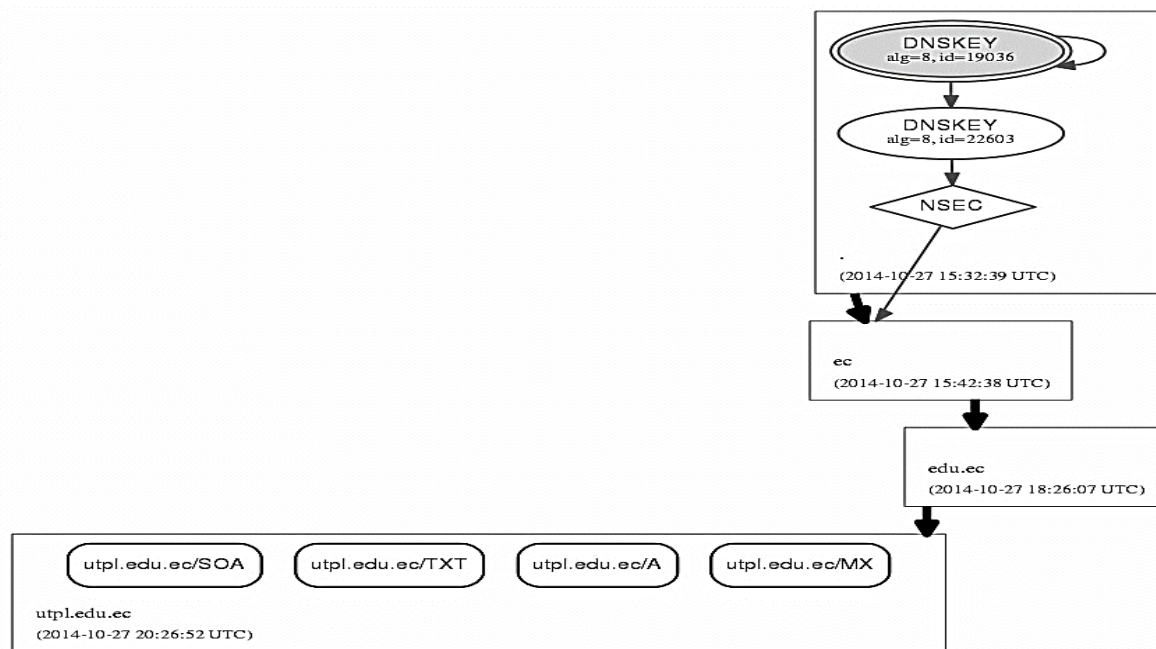


Figura 16. Estado del firmado de la zona `www.utpl.edu.ec`.
Fuente: 1("DNSViz," 2014).

5 CAPITULO V. Propuesta de implementación del DNSSEC.

Para la validación de nuestra propuesta se creó un escenario de laboratorio para el uso e implementación de DNSSEC, así demostrar la hipótesis de que el despliegue en un ambiente en producción se lo puede llevar a cabo de manera eficiente y responsable. Se tomará un subdominio de la UTPL para fines de pruebas y a través de DNSSEC asegurar los servidores DNS en el ambiente de laboratorio.

5.1 Requerimientos mínimos.

Para el despliegue de DNSSEC es necesario revisar la estructura que se encuentra en la organización y con qué equipos cuenta como sus respectivas características, ya que el despliegue DNSSEC conlleva realizar cambios en la configuración de los DNS, tanto a nivel de software como de hardware, como la actualización del firmware de los equipos en caso de ser necesario.

En el despliegue de las extensiones de seguridad DNS (DNSSEC), se necesita firmar digitalmente nuestras zonas para lo cual se debe tener en cuenta dos partes, por un lado la gestión de software DNS y por el otro lado la gestión de los algoritmos de encriptación, que hace referencia a los procedimientos, políticas y manejos de las claves públicas y privadas, así como también la futura actualización de la clave pública para mayor seguridad

En la implementación de las DNSSEC en el ambiente de laboratorio, se levantarán dos servidores DNS, uno que será el servidor principal y el otro será el servidor caché que simularán a los servicios DNS de la UTPL. También se configurará un equipo cliente para las respectivas peticiones y respuestas a los servidores DNS.

Para nuestras pruebas se validaron dos herramientas las cuales son las más utilizadas al momento de establecer un servidor de infraestructura: Microsoft Windows Server y Linux. Todas las características se verán reflejadas en las dos herramientas, consideradas para la evaluación y correcto funcionamiento de las extensiones de seguridad DNSSEC.

Se tomará un sub dominio para representar el dominio de la UTPL, el cual será `sedes.utpl.edu.ec`. En la tabla 11, se muestra las direcciones y los nombres de los equipos que serán agregados en el archivo de zona de `sedes.utpl.edu.ec`.

Tabla 11. Zona www.sedes.utpl.edu.ec del escenario propuesto.

ZONA sedes.utpl.edu.ec		
Servicio o sub-dominio	Dirección	Descripción
quito.sedes.utpl.edu.ec	192.168.1.111	Sede de la ciudad de Quito
guayaquil.sedes.utpl.edu.ec	192.168.1.121	Sede de la ciudad de Guayaquil
cuenca.sedes.utpl.edu.ec	192.168.1.131	Sede de la ciudad de Cuenca
loja.sedes.utpl.edu.ec	192.168.1.141	Sede de la ciudad de Loja
stodomingo.sedes.utpl.edu.ec	192.168.1.151	Sede de Sto. Domingo
moodle.sedes.utpl.edu.ec	192.168.1.161	Entorno virtual de aprendizaje

Elaborado por: César Guanoliqúe.

5.2 Escenario de pruebas de DNSSEC.

En la UTPL se, tiene un servidor DNS maestro y uno de caché para la resoluciones externas e internas respectivamente, tomando en cuenta ese detalle se configurarán nuestros servidores DNS en el ambiente de laboratorio. En la figura 17, se muestra el esquema que vamos a utilizar para configurarlos y firmarlos con DNSSEC.

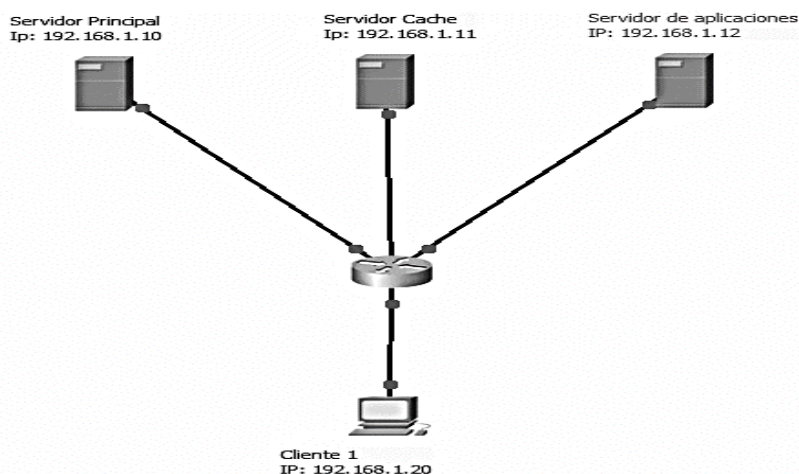


Figura 17. Equipos que intervendrán en nuestro ambiente de laboratorio.
Elaborado por: César Guanoliqúe.

5.3 Herramientas propuestas para el despliegue DNSSEC en los servidores DNS.

Las herramientas utilizadas en la actualidad por la UTPL en sus servidores DNS, son: una distribución Linux Ubuntu y el software DNS BIND9, en la cual esta soportada toda la infraestructura DNS de la institución.

Como ya hemos comentado el ambiente de laboratorio contempla un esquema similar manejado por la UTPL para dar el servicio DNS, con el objetivo de contar con toda la información necesaria

para implementar DNSSEC en los servidores DNS en producción. Este ambiente simula los requerimientos empleados por los DNS como son: envío de correo electrónico, solicitudes de páginas web, despliegue de servicios, etc.

5.4 Herramientas utilizadas en la propuesta para el ambiente de laboratorio.

Las versiones utilizadas para fines de pruebas en el ambiente de laboratorio de nuestra zona sedes.utpl.edu.ec, en el caso de Microsoft Windows Server fueron: Windows Server 2012 versión r2, y en el caso de Linux: Centos 7- con el software bind9 versión 9.9.4.

Se ha tomado el software Virtual Box de Oracle, para la virtualización e instalación de las diferentes distribuciones que están destinadas para la experimentación y despliegue de las DNSSEC en el ambiente de laboratorio.

5.5 Pasos ejecutados en la configuración de los servidores DNS.

- Instalación del servidor en este caso una distribución de LINUX Centos versión 7, destinada a servidores de infraestructura.
- Instalación y configuración del software DNS en este caso BIN9 dentro de Centos.
- Instalación y configuración de un cliente Centos para las peticiones.
- Instalación de Windows Server 2012 r2.
- Configuración de los servicios DNS en el servidor

5.5.1 Configuración del servicio DNS (principal y esclavo).

La instalación del servicio DNS en el servidor primario y caché, es la misma en ambos caso, la diferencia radica en la denominación o servicio que prestará el servidor.

Para mayor entendimiento y explicación se escogió la interfaz GUI de Centos 7, más el software BIN9 que viene integrada a la distribución.

Archivos que serán modificados para el arranque del servicio DNS:

- /etc/named.conf: Encargado del arranque del servicio DNS.
- /etc/resolv.conf: Encargado de establecer el nombre del servidor del dominio.
- /var/named/sedes.zone: Encaragado de contener los registros de recursos de la zona.
- /var/named/sedes.inv.zone: Encargado de contener los registro de recursos de la zona inversa.

5.5.2 Configuración del cliente en Centos.

El cliente se lo configura dentro del dominio sedes.utpl.edu.ec, para luego efectuar las consultas o peticiones DNSSEC con el comando “dig”.

Archivos que serán modificados para que el cliente trabaje en el dominio sedes.utpl.edu.ec:

- /etc/resolv.conf: Encargado de establecer el nombre del servidor del dominio.
- /etc/sysconfig/network-scripts/ifc-fg-enp0s3: Configuración de la tarjeta de red.
- /etc/host.conf: configuración de servidores DNS
- /etc/hosts

En la figura 18, se visualiza parte de la configuración de un cliente Centos dentro del dominio sedes.utpl.edu.ec, desde cual se puede consultar los registros DNSSEC que tienen otros equipos a través del comando “dig”.

```
clientecentos@localhost:/home/clientecentos
Archivo Editar Ver Buscar Terminal Ayuda
clientecentos@localhost ~]$ su
Contraseña:
root@localhost clientecentos]# nano /etc/sysconfig/network-scripts/i
root@localhost clientecentos]# nano /etc/resolv.conf
root@localhost clientecentos]# nano /etc/hosts
hosts hosts.allow hosts.deny
root@localhost clientecentos]# nano /etc/host
host.conf hostname hosts hosts.allow hosts.deny
root@localhost clientecentos]# nano /etc/host.conf
root@localhost clientecentos]# nano /etc/hosts
root@localhost clientecentos]# ping www.moodle.sedes.utpl.edu.ec
```

Figura 18. Configuración de cliente Centos 7.
Elaborado por: César Guanoliq.

5.6 Formato del mensaje DNSSEC.

La figura 19 muestra cómo se estructura un mensaje de respuesta DNSSEC por parte del servidor DNS, se aprecia una tupla sin firmar y otra con su respectiva firma DNSSEC del dominio sedes.utpl.edu.ec, se pueden apreciar algunos de los registros nuevos, así como las nuevas banderas –flags, el Registros RRSIG, que lleva el firmado digital, así como el número de algoritmo utilizado.

```
[root@localhost maestro]# dig +dnssec +multi sedes.utpl.edu.ec
; <<>> DiG 9.9.4-RedHat-9.9.4-18.el7_1.3 <<>> +dnssec +multi sedes.utpl.edu.ec
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 56875
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;sedes.utpl.edu.ec.      IN A

;; ANSWER SECTION:
sedes.utpl.edu.ec.      86400 IN A 192.168.1.101
sedes.utpl.edu.ec.      86400 IN RRSIG A 5 4 86400 (
    20150922015211 20150823015211 48393 sedes.utpl.edu.ec.
    lqqlmyf0+tLC5hx9kwacNEm3M95Q2VT1z1o0+tRv/rxs
    sBAKVkw5cIryfgJb4TEaX9zq+jrtHSWU0+jzLuq1X9F8
    uVmJjbHM/TWedfNAZF96PHK1nN21LF/QbK0VEmprIVD
    nsicA7uS9Tjy2m8asGI8b7M5viRUbtWw9MC4/NP1UtcJ
    7bTRBmGX87S4CybKurebTU0ZMyLZoyhi2JvKXX/75EPB
    CAc7sJiwXtR04akmzpKdX+pejLSEgh9bw71LueNutJ89
    P3Uz0c5tWQr/xdnLQ5q9XLQYvC4XGpaiC7kY/gkHkCch
    0m2V0LS7u0/cBP68MnrZM3SBEVLz+7c9LA== )
```

Figura 19. Registro DNSSEC.
Elaborado por: César Guanolíque.

En las extensiones de seguridad DNSSEC se identificaron tres tipos de servicios los cuales son fueron considerados para el firmado y la construcción de la cadena de confianza de la zona sedes.utpl.edu.ec:

- **Distribución de las llaves (key distribution).**- Mediante un proceso de criptografía, las llaves son distribuidas a través del árbol de jerarquía DNS hasta su raíz, es decir, la zona raíz (“.” ROOT).
- **Autenticación del origen de las llaves (Data Origin Authentication).**- Con el proceso de Hash las llaves son comprobadas para saber si no han sido manipuladas por terceros, así se establece una cadena de confianza.
- **Autenticación de transacciones y pedidos (DNS Transaction and Request Authentication).**- Permite autenticar los mensajes DNS a través de sus cabeceras, ésta genera una respuesta afirmativa en caso de ser correcta. La seguridad que impera en una transacción asegura a ambas partes que se ha realizado con éxito desde servidor que se esperaba la respuesta, lo cual permite que las actualizaciones dinámicas entre servidores se dé sin ningún contratiempo.

5.7 Configuración DNSSEC Centos.

5.7.1 Configuración de los archivos que intervienen en el despliegue del servidor DNS y de las extensiones de seguridad DNSSEC.

La configuración de DNSSEC en Centos, implica configurar un servidor DNS normal y agregar las configuraciones necesarias para que DNSSEC empiecen a operar; los archivos que intervienen en la configuración son:

- /etc/named.conf – configuración del archivo de ejecución del servicio DNS- DNSSEC.
- /etc/resolv.conf – configuración de los dominios que intervienen en la zona.
- /var/named/sedes.zone – Zona directa de los registros de recursos a firmar.
- /var/named/sedes.inv.zone – Zona inversa de los registros de recursos a firmar.
- /var/named/iptables – Configuración del firewall.

La explicación detallada sobre los archivos de configuración se encuentra en el anexo A página 63, donde se muestran los registros de recursos que intervienen en la configuración del servidor DNS, su estructura es similar en ambas distribuciones (Centos y Windows), la diferencia solo radica en el procedimiento de firmado.

Al configurar las extensiones de seguridad DNSSEC se deben generar las llaves KSK y PSK privadas y públicas respectivamente, y también escoger el tipo de algoritmo de encriptación para la generación de las diferentes llaves.

Una vez generadas se procede a distribuir las diferentes firmas a través de los diferentes servidores internos y externos de la institución formando la cadena de confianza entre las zonas.

5.7.2 Proceso de introducción DNSSEC en Centos.

La figura 20 describe un diagrama del proceso del firmado DNSSEC dentro del servidor DNS, para su mejor comprensión del firmado.

El proceso de introducción de DNSSEC comienza en la instalación de las herramientas que se van ocupar en el firmado de la zona, comenzamos con la instalación de la distribución Linux – Centos, luego las herramientas “dnstools”, así como también el software BIND9.

Una vez levantado el servicio DNS, se comienza la configuración de DNSSEC a través de las herramientas “dnstools”, las herramientas ayudan con la generación de las llaves, así como la generación del registro DS, una vez obtenido las llaves, se procede a la configuración del archivo named.conf, el cual contiene la información de los archivos de zona, en el cual se hace referencia al nuevo archivo generado con la firma digital de la zona.

A su vez se hacen las pruebas correspondiente para verificar si están firmado los registros de recursos, y si es así se procede a transferir la zona con sus respectivas clave pública.

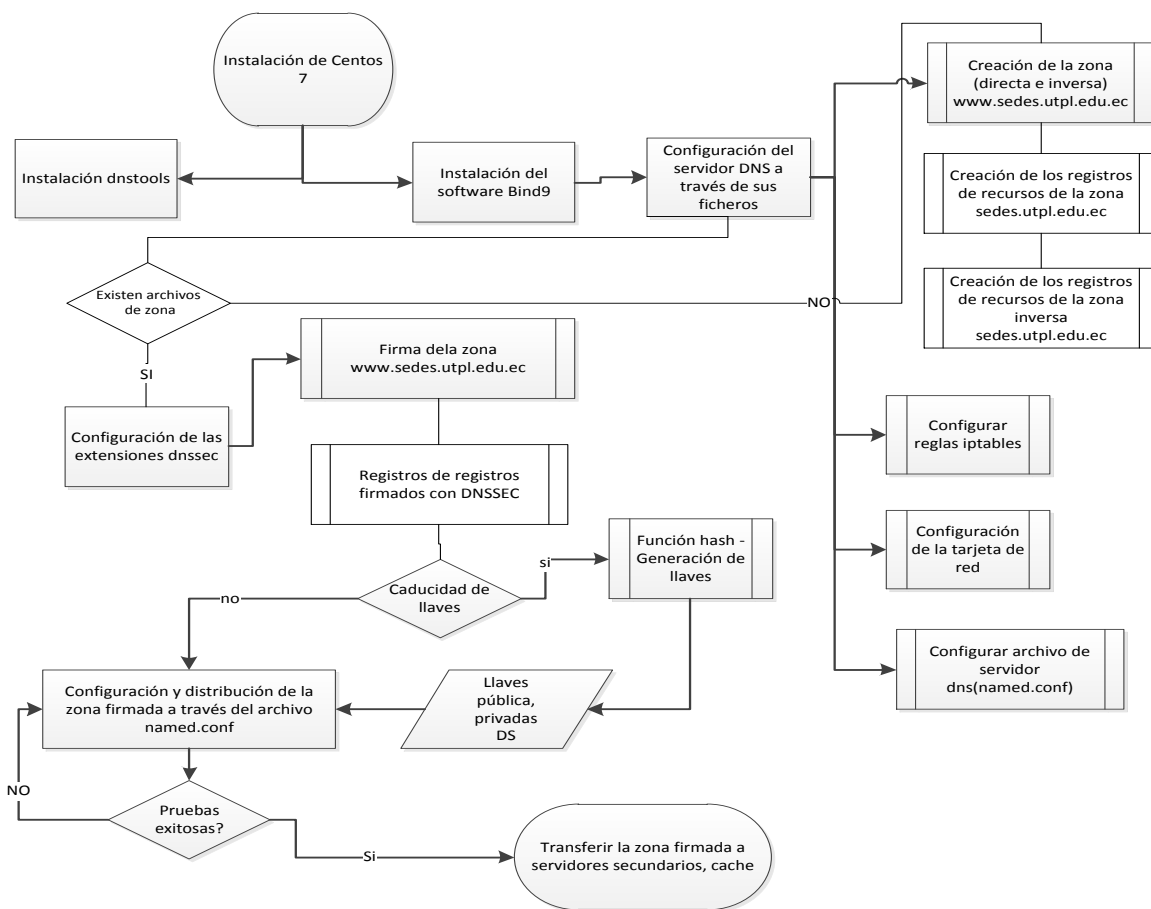


Figura 20. Diagrama del proceso de introducción de DNSSEC en Centos. Elaborado por: César Guanoliqúe.

5.8 Configuración DNSSEC en Windows server 2012 r2.

En Windows server 2012 la configuración de servidores DNS es diferente a la distribución Linux Centos 7, ya que en Windows 2012 utilizamos las herramientas preestablecidas, siendo el manejo de ellas más intuitivas por su entorno gráfico, claro que si no se tiene ningún conocimiento se puede tornar en una situación compleja.

Para la configuración del servidor DNS propuesto en el ambiente de laboratorio, se tomó como referencia la guía (Microsoft-TechNet, 2015), configurando de esta manera el servidor DNS y controladores de dominio con el fin de establecer un acceso seguro a todos los usuarios y a los administradores de los servicios.

Ya establecido la configuración de la zona en el servidor DNS maestro como la configuración adicional de un controlador de dominio Active Directory, así como la transferencia de zona al servidor DNS secundario (DNS caché), este último contendrá todas las solicitudes DNS previstas

por los usuarios de la red interna, así como la configuración de recursividad en caso de no conocer una en particular.

Con respecto a la configuración de los clientes, se establecieron las direcciones IP manualmente ya que en el esquema no se cuenta con un servidor DHCP; se configuró también para que pertenezcan al dominio sedes.utpl.edu.ec.

5.8.1 Diagrama de introducción DNSSEC en Windows Server 2012

En la figura 21, se observa como es el proceso de introducción DNSSEC en la distribución Windows Server, la cual comienza con su instalación, en la cual se incluyen todas las herramientas necesarias para el firmado de la zona con DNSSEC, luego se empieza con la configuración del servidor para que corresponda al dominio de la UTPL. Adicional a la configuración DNS, Windows Server instala un controlador de dominio, el cual crea un punto de acceso al servidor DNS principal, con respecto a los demás servidores DNS instalados en la red, en la cual configuramos la zona.

La firma de la zona, se la realiza con los comandos ya preestablecidos en Windows, en el cual generamos el ancla de confianza, las llaves KSK ZSK, y finalmente se establece reglas de validación DNSSEC, que son las difusión de las llaves ya que en el servidor secundario se transmite la zona firmada digitalmente. Después se generan las pruebas de validación, para así transferir la zona firmada.

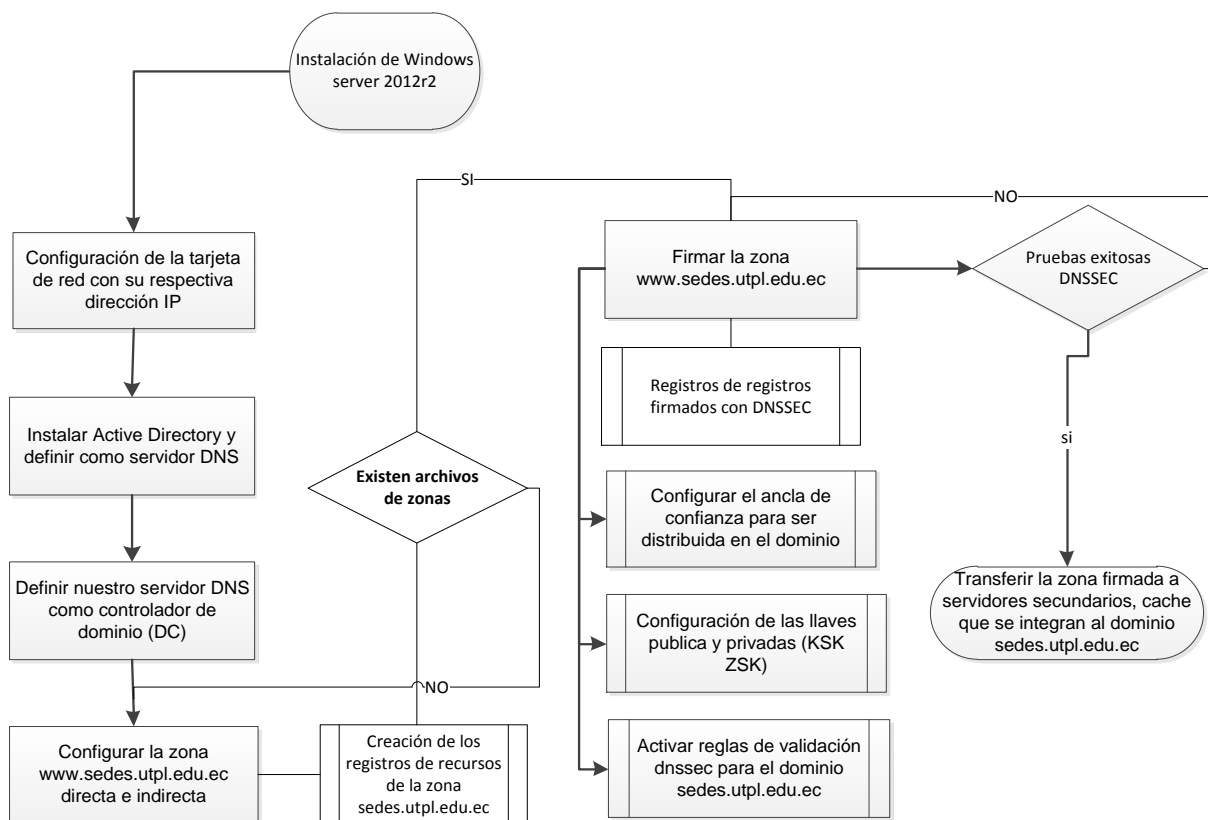


Figura 21. Proceso de validación del DNSSEC en Windows server para el dominio sedes.utpl.edu.ec. Elaborado por: César Guanoliq.

5.9 Diferencia entre Centos 7 y Windows Server 2012.

Entre las diferencias que podemos encontrar entre estas dos herramientas tenemos:

Tabla 12. Diferencias Centos 7 y Windows Server 2012.

Centos 7	Windows Server 2012
Licencia gratuita	Licencia de paga
No existencia de interfaz gráfica (GUI) en servidores de infraestructura.	Existencia de interfaz gráfica.
Instalación de herramientas externa para el firmado DNSSEC	Herramientas de firmado incluidas en la distribución.
Conocimientos mayores en servidores de infraestructura.	Ayuda de manera más amigable a la configuración del servidor gracias a su GUI.
Abundante información	Abundante información
Soporte técnico a cargo del administrador	Soporte Técnico especializado

Elaborado por: César Guanoliq.

En la tabla 12, se detalla las diferencias más importantes que existen entre las distribuciones Centos 7 y Windows Server 2012, se puede observar que la licencia de Centos 7 es gratuita, mientras que la de Windows Server 2012 es de paga, con la diferencia que radica que el soporte técnico lo brinda Windows, mientras que el soporte es Centos corre por parte del administrador del sistema, es decir este tendrá que recurrir a los foros especializados para resolver algún problema que se le presente con respecto a la configuración y administración del servidor.

La interfaz gráfica (GUI) que ofrece Windows Server 2012 es muy completa e intuitiva, facilitando y ofreciendo a los administradores herramientas para el firmado DNSSEC y configuración del servidor DNS; mientras que en Centos, se deben instalar herramientas externas para el firmado DNSSEC, habiendo variedad de ellas, lo cual implica un mayor grado de conocimiento por parte del administrador, para que éste pueda integrar una acorde a sus necesidades y requerimientos.

RESULTADOS.

6 CAPITULO VI. Pruebas.

Para que nuestro servidor DNS funcione adecuadamente se debe monitorear el servicio a través de herramientas de diagnóstico y supervisión, para tomar a futuro cualquier decisión de mejora y optimización del servicio DNS.

Con respecto a las extensiones de seguridad DNSSEC, la implementación no demanda de recursos de hardware y software excesivos, así que el rendimiento de nuestro servidor DNS no se verá afectado de manera significativa, estas extensiones suponen la validación de nuestro sitio a través de técnicas de verificación de firmas y de cadenas de confiabilidad, así que la demanda por parte de los usuarios en respuesta a sus peticiones no son mayores de lo habitual en una petición sin validación DNSSEC.

Las pruebas realizadas en ambas distribuciones tanto en Centos 7 como en Windows Server 2012, fueron exitosas en el ambiente de laboratorio, exitosas desde el punto de vista de que se logró validar el firmado digital con DNSSEC de la zona, esto demuestra que la implementación no demanda recursos ni tiempos excesivos de configuración, lo que sí podría complicar el firmado de la zona, es la caducidad de las claves de seguridad (KSK y PKI), cuando éstas no son renovadas en el tiempo establecido al momento de firmar la zona. Esto demuestra que no hay excusa para **no implementar DNSSEC** en nuestros servidores DNS, todo depende de una administración basado en políticas establecidas por la institución.

6.1 Centos 7 – bind9.9.4.

Como se ha mencionado anteriormente, no se cuenta con el firmado de la zona de nivel superior “.ec”, motivo por el cual se trabajó con un ancla de confianza que lo ofrece la ISC, para las respectivas pruebas con el objetivo de crear una isla de confianza en la zona sedes.utpl.edu.ec. A través de esta ancla, se puede tener firmada toda la zona, así estar preparado para el momento en que se firme la zona superior y se produzca una cadena de confianza en toda la jerarquía del DNS.

En la figura 22, se muestra una consulta DNSSEC positiva a través del servidor maestro del dominio sedes.utpl.edu.ec., con el comando “dig” desde una terminal.

```
[root@localhost dnsmaster]# dig +dnssec -x 192.168.1.12 +multi

;<<>> DiG 9.9.4-RedHat-9.9.4-14.el7 <<>> +dnssec -x 192.168.1.12 +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41181
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
; DNSSEC OK
```

Figura 22. Resumen de una petición DNSSEC positiva.
Elaborado por: César Guanoliقة.

```
maestro@localhost:/home/maestro
Archivo Editar Ver Buscar Terminal Ayuda
<<>> DiG 9.9.4-RedHat-9.9.4-18.el7_1.3 <<>> +dnssec +multi pc2.moodle.sedes.utpl.edu.ec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60367
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
; pc2.moodle.sedes.utpl.edu.ec. IN A

;; ANSWER SECTION:
pc2.moodle.sedes.utpl.edu.ec. 86400 IN A 192.168.1.21
pc2.moodle.sedes.utpl.edu.ec. 86400 IN RRSIG A 5 6 86400 (
20150921014036 20150822014036 20463 moodle.sedes.utpl.edu.
ac.
q3u0iurw2MvEmDycOt7lWMf64NTmnAQtxRMIXNPPs5Do
3tLmp98uNGkoc48RI6spId6EcvVwCcClcYw1hGHcX1j
Nh+Rjb4fV81WLf0EyxJxuz9WcCiqSbDcxnczK8xw2W5
LU4Vah5B+geKURNzJX1f10CaYccSFV0tHw9VVs rEPY0X
OpUWWEQhIfbJU/NoHBI fQBcm3Evd4kJsic8vKtIzvenf
jybV.iYJt8QxJ1uPhG05UVYp72Nv0stYg3G6n1PLJCPKQ
xTp6wCqNtHlphbRRN9Je5KQHJHQFAL0BbZdP75T2iweY
psyukJgpHjV3dkPqiYmGci+FV816UhCnDA== )
```

Figura 23. Respuesta DNSSEC “flag ad”.
Elaborado por: César Guanoliقة.

La figura 23 visualiza la consulta a través del servidor maestro al dominio de nivel inferior moodle.sedes.utpl.edu.ec, nótese que en este caso nos devuelve la solicitud positiva a través de la bandera “ad” o “flag ad”, el cual nos está indicando que los datos están autenticados y validados con DNSSEC.

Para validar nuestra propuesta en el ambiente de laboratorio y comprobar que la metodología empleada en el firmado con DNSSEC de la zona “sedes.utpl.edu.ec” tuvieron los resultados esperados, como es la validación DNSSEC de la zona, se realizó el firmado de la zona guayacansoft.com, en un ambiente en producción, en el cual se tuvo acceso a la información de la zona, a las configuraciones y además que no se comprometían sus datos, considerando que es un dominio nuevo.

6.2 Validación de la configuración en los servidores DNS.

Entre algunas herramientas para monitorización de un servidor DNS, tenemos algunas que funcionan a nivel de distribución y otras externas como software para monitorear las actividades DNS.

6.2.1 Rendimiento del servicio DNS.

Para evaluar el rendimiento del servicio DNS, se utilizó esta herramienta, la cual nos permite analizar y verificar el comportamiento de los diferentes servidores DNS, con esto se pudo establecer el rendimiento actual del servicio DNS de la UTPL, así como también su seguridad y velocidad al momento de consultar sus bases de datos.

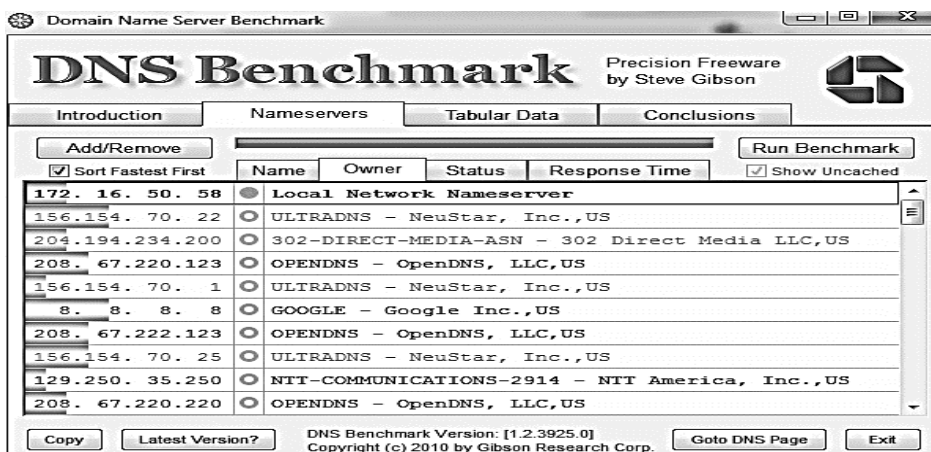


Figura 24. Consulta de servidores DNS.
Elaborado por: César Guanoliq.

En la figura 24, se muestra la consulta realizada a diversos servidores DNS, que responde a una solicitud, en el cual el servidor DNS de la UTPL (IP:172.16.50.58), nos da una referencia de su comportamiento, en cuanto a su saturación y su velocidad de respuesta, entre otras características.

En la figura 25, se observa tiempos de respuesta del servidor DNS de la UTPL, el cual indica que está respondiendo primero a la consulta:

```

172. 16. 50. 58 | Min | Avg | Max |Std.Dev|Reliab%|
+-----+-----+-----+-----+-----+
+ Cached Name   | 0,003 | 0,062 | 0,185 | 0,044 | 100,0 |
+ Uncached Name | 0,104 | 0,223 | 0,572 | 0,113 | 97,9 |
+ DotCom Lookup | 0,132 | 0,829 | 2,294 | 0,935 | 97,9 |
+-----+-----+-----+-----+-----+
                                gdr5.utpl.edu.ec
                                Local Network Nameserver

```

Figura 25. Tiempos de respuesta del servidor DNS de la UTPL.
Elaborado por: César Guanoliq.

6.2.2 Tráfico entrante y saliente en el servicio DNS.

Se comprobó el tráfico entrante y saliente que ofrece el servicio DNS de la UTPL, se empleó la herramienta DNSStop, con el fin de medir las consultas de los hosts de nuestra LAN a nuestros servidores DNS, así como también que equipos están generando mayor demanda de recursos y todas las solicitudes de los clientes en un determinado servidor DNS, tal como se muestra en la figura 26.

```
Queries: 0 new, 641 total      Tue Jul 1
Query Name      Count      %
-----
com             602       93.9
net             34         5.3
us              5          0.8
```

Figura 26. Salida de una consulta a través de DNSstop.
Elaborado por: César Guanoliqúe.



6.3 Validación y verificación DNSSEC.



Las primeras pruebas se hicieron utilizando el Plug-in para navegadores webs “DNSSEC/TLSA Validator”, así como también los sitios webs de VeriSign (<http://DNSSEC-debugger.verisignlabs.com/>), el cual nos dió un detalle de nuestra zona firmada con los parámetros más relevantes de DNSSEC, mientras que el sitio <http://DNSviz.net/>, también nos detalló la situación DNSSEC de nuestra zona.

6.3.1 Verificación DNSSEC.

Con el plugin DNSSEC/TLSA Validator se realizó la verificación del sitio de la UTPL “utpl.edu.ec”, dándonos como resultado que el dominio no cuenta con las extensiones de seguridad DNSSEC. Así mismo se validó el firmado digital de la zona de guayacansoft.com con DNSSEC. En la tabla 13, se describe los estados más importantes del Plugin, con sus respectivos significados.

Tabla 13. Estados del Plug-in DNSSEC/TLSA Validator.

Estado del plugin	Descripción
	Significa que la IP de nuestro sitio, concuerda con el nombre de dominio, ya que ha fue validado por DNSSEC, y por ende se está protegido contra ataques de suplantación de nombres de dominio.
	Significa que el sitio está garantizado por DNSSEC, pero se ha detectado una firma de nombre de dominio no válido. Puede señalar un intento de suplantación del nombre de dominio.

	<p>Señala que el nombre de dominio no está garantizado por DNSSEC, no es posible validar los datos obtenidos del DNS, y el sitio está expuesto a ataques de suplantación.</p>
	<p>Nos indica que la dirección IP utilizada por el navegador, no es la obtenida por DNSSEC. Puede ser un ataque de suplantación al DNS.</p>

Fuente: (Cz.nic, 2015)

Elaborado por: César Guanoliقة.

En la figura 27, se puede observar que en el Plugin se visualiza icono en forma de llave de color gris con un indicador rojo, que nos dice que el sitio no se encuentra asegurado con DNSSEC, y no es posible validar los datos obtenidos del DNS, en consecuencia el sitio está expuesto a ataques de suplantación de dominio.

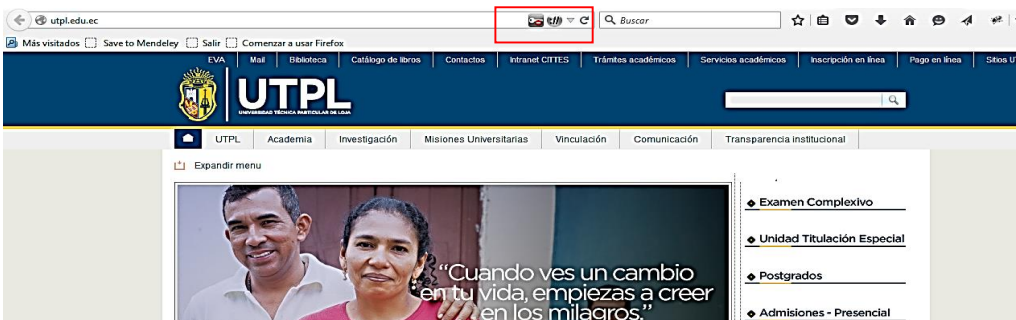


Figura 27. Plugin DNSSEC/TLSA Validator sitio utpl.edu.ec.

Elaborado por: César Guanoliقة.



Figura 28. Plug-in DNSSEC/TLSA Validator sitio guayacansoft.com

Elaborado por: César Guanoliقة.

En la figura 28, observamos que el Plugin DNSSEC Validator se encuentra con una llave de color verde, el cual nos indica que el sitio guayacansoft.com se encuentra asegurado contra ataques de suplantación de nombres de dominio.

6.3.2 Validación y verificación de la firma digital DNSSEC.

Otra herramienta web con la que se probó la validación DNSSEC, tanto para la zona utpl.edu.ec como la de la zona guayacansoft.com, es la proporcionada por VeriSign con esta herramienta se pudo evidenciar si el sitio se encuentra firmado digitalmente por DNSSEC, o no, para lo cual digitando la dirección de la zona utpl.edu.ec o guayacansoft.com, se consulta si existen registros DNSSEC en su estructura DNS y a su vez si existe la cadena de confianza desde el nivel inferior hasta el nivel superior (la raíz “.”). Es decir que toda la jerarquía DNS se encuentre firmado con DNSSEC.

Con esta herramienta se realizó la consulta, para conocer el estado de la zona utpl.edu.ec con respecto a las DNSSEC, así mismo para saber si la zona cuenta con registros DNSSEC. En la figura 29, se observa que no existe ninguna firma digital DNSSEC, y por consiguiente ningún registro RRSig ni DS. También podemos observar que no existe ningún registro para la verificación y validación de DNSSEC desde nivel superior “.ec” hasta el dominio de nivel inferior utpl.edu.ec, solamente en la raíz “.”, se puede observar que existen registros RRSIG, DS, y DNSKEY.

Zone	Results
.	<ul style="list-style-type: none"> ✔ Found 2 DNSKEY records for . ✔ DS=19036/SHA-1 verifies DNSKEY=19036/SEP ✔ Found 1 RRSIGs over DNSKEY RRset ✔ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
ec	<ul style="list-style-type: none"> ✘ No DS records found for ec in the . zone ✘ No DNSKEY records found ⚠ Query to n1.nic.ec/200.12.198.1 for edu.ec/NS timed out or failed
edu.ec	<ul style="list-style-type: none"> ✘ No DS records found for edu.ec in the ec zone ✘ No DNSKEY records found
utpl.edu.ec	<ul style="list-style-type: none"> ✘ No DS records found for utpl.edu.ec in the edu.ec zone ✘ No DNSKEY records found ✔ utpl.edu.ec A RR has value 200.41.6.33 ✘ No RRSIGs found

Figura 29. Consulta DNSSEC del sitio utpl.edu.ec.
Elaborado por: César Guanolique.

	<ul style="list-style-type: none"> Found 2 DNSKEY records for . DS=19036/SHA-1 verifies DNSKEY=19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
com	<ul style="list-style-type: none"> Found 1 DS records for com in the . zone Found 1 RRSIGs over DS RRset RRSIG=1518 and DNSKEY=1518 verifies the DS RRset Found 2 DNSKEY records for com DS=30909/SHA-256 verifies DNSKEY=30909/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=30909 and DNSKEY=30909/SEP verifies the DNSKEY RRset
guayacansoft.com	<ul style="list-style-type: none"> Found 2 DS records for guayacansoft.com in the com zone Found 1 RRSIGs over DS RRset RRSIG=35864 and DNSKEY=35864 verifies the DS RRset Found 2 DNSKEY records for guayacansoft.com DS=64174/SHA-1 verifies DNSKEY=64174/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=29640 and DNSKEY=29640 verifies the DNSKEY RRset dnsserver.guayacansoft.com serial (2015051301) differs from ns2.digitalocean.com serial (1440364721) guayacansoft.com A RR has value 45.55.240.164

Figura 30. Validación positiva DNSSEC del sitio guayacansoft.com.
Elaborado por: César Guanoliq.

La Figura 30, muestra la cadena de confianza que existe entre el dominio guayacansoft.com hasta la raíz “.”, comprobándose que existen los registros DNSKEY, DS y RRSIG; que tienen información del nivel inferior hasta el superior.

Tabla 14. Registros DNSSEC.

Dominio	DNSKEY	Registro DS	Registro RRSIG
utpl.edu.ec	No	No	No
Guayacansoft.com	Si	Si	Si

Elaborado por: César Guanoliq.

La tabla 14, explica que los registros DNSKEY, DS, RRSIG, no se encuentran en la zona utpl.edu.ec, por lo cual el sitio no puede responder a consultas DNSSEC. Por lo contrario la zona guayacansoft.com si cuenta con los registros para la validación de DNSSEC.

6.3.3 Verificación de la cadena de confianza.

La herramienta web que nos ofrece el sitio dnsviz.net, es una herramienta gráfica que nos permite ver el estado DNSSEC de nuestro dominio en toda la jerarquía DNS, a diferencia de la herramienta de VeriSign se puede observar la cadena de confianza, así como también los registros que intervienen en su construcción.

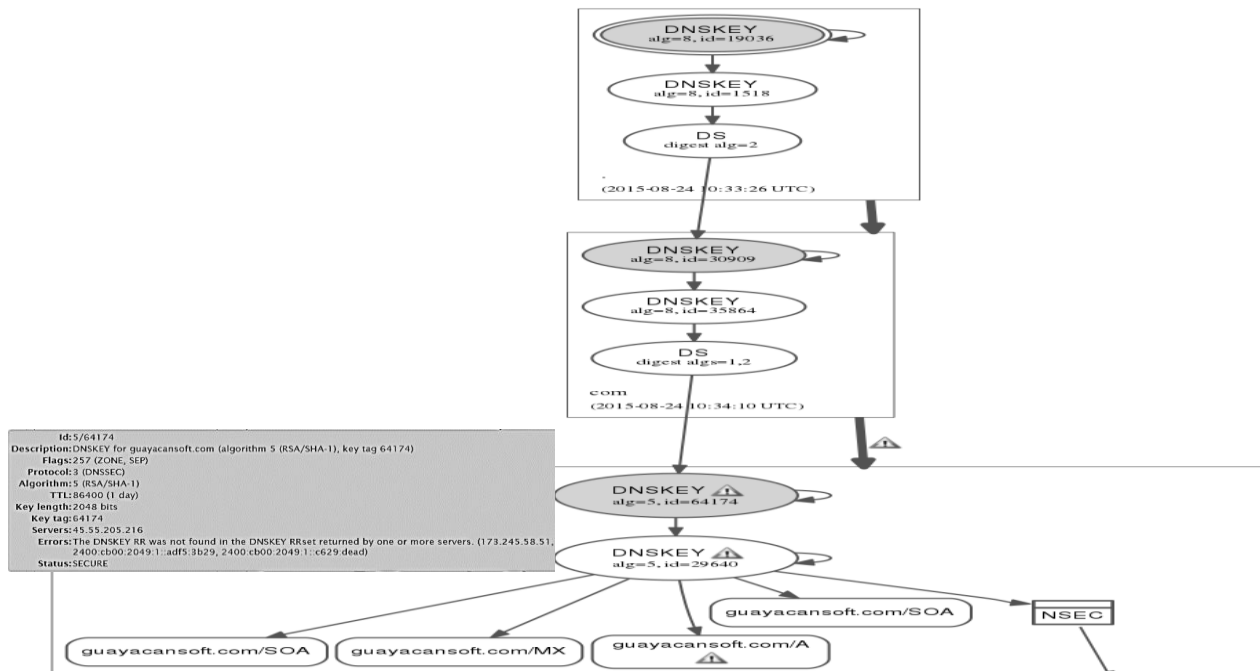


Figura 31. Mapa DNSSEC del sitio guayacansoft.com.
Elaborado por: César Guanoliqúe.

En la figura 31, se describe la información DNSSEC de la zona guayacansoft.com, en la cual se puede observar estado DNSSEC del dominio de nivel inferior guayacansoft.com hasta la raíz “.”.

6.3.4 Windows server 2012r2.

En la figura 32, se muestra la respuesta DNSSEC, a la consulta de un host de zona sedes.utpl.edu.ec, a través del comando Resolve-DnsName.

```
PS C:\> Resolve-DnsName dc1master.sec.sedes.utpl.edu.ec -server dns1cache -dnssecok

Name                                     Type    TTL    Section  IPAddress
----
dc1master.sec.sedes.utpl.edu.ec         A       3599   Answer   192.168.1.103

Name           : dc1master.sec.sedes.utpl.edu.ec
QueryType     : RRSIG
TTL           : 3599
Section       : Answer
TypeCovered   : A
Algorithm     : 8
LabelCount   : 6
OriginalTtl   : 3600
Expiration   : 02/02/2015 23:29:14
Signed        : 23/01/2015 22:29:14
Signer        : sec.sedes.utpl.edu.ec
Signature     : {142, 1, 211, 121...}

Name           : -
QueryType     : OPT
TTL           : 32768
Section       : Additional
Data          : {}
```

Figura 32. Resumen de una prueba DNSSEC en un cliente Windows 8.
Elaborado por: César Guanoliqúe.

6.4 Tablas de resultados de las herramientas webs.

En la tabla 15, mostramos los resultados de la validación de las herramientas webs en la cual se indican los registros de firmas digitales DNSSEC que sirven para la validación de la información del firmado de la zona sedes.utpl.edu.ec.

Las herramientas VERISIGN y DNSVIZ, muestran en detalle las llaves y registros firmados digitalmente, mientras que el Plugin DNSSEC/TLSA VALIDATOR solo muestra el estado de la zona a través de indicadores de estado.

Tabla 15. Validación de las llaves, claves y registros digitales.

Nombre	Tipo	Registros	Keys	Firma
DNSSEC/TLSA VALIDATOR	Plugin	No	No	Si
VERISIGN	Reporte	Si	Si	Si
DNSVIZ.NET	Reporte visual	Si	Si	Si

Elaborado por: César Guanolíque.

En la tabla 16, se muestra los diferentes comandos que se utilizó para las diferentes herramientas, para obtener los resultados a las consultas DNSSEC a nivel de servidores DNS.

Tabla 16. Comandos, testeos y mediciones en servidores DNS.

Comando	S.O. Distribución	IP	Keys/ Claves	Firma DNSSEC	Registros RRSIG
Dig	Linux	Si	Si	Si	SI
DNSstop	Windows/Linux	No	No	No	NO
Resolve-Dnsname	Windows	Si	Si	Si	SI
Nslookup	Windows/Linux	No	No	No	NO

Elaborado por: César Guanolíque.

Como se observa en las tablas 15 y 16, se utilizó diferentes herramientas con el objetivo de diagnosticar, verificar y validar que el servicio DNS de la UTPL opera eficazmente, así mismo se utilizaron estas herramientas y comandos en ambiente de laboratorio y en producción con respecto al servidor de la zona sedes.utpl.edu.ec que sirvieron para comprobar el correcto despliegue y funcionamiento de DNSSEC en ambos ambientes.

CONCLUSIONES

- Las DNSSEC son indispensables para la seguridad interna de los servicios DNS de las empresas e instituciones de toda índole, se presentan como una solución efectiva a algunas de las vulnerabilidades del protocolo DNS. En el caso de la UTPL, los DNSSEC otorgarían mayor seguridad en sus áreas más críticas, como es el área financiera y el área académica, colocando una capa adicional de seguridad, contra ataques no deseados y a su vez dándole un grado más de confiabilidad a sus usuarios.
- Validar herramientas, a fin de establecer cuál es la que mejor se adapta con respecto a la seguridad de sus servicios DNS, puede ser una estrategia que permite ahorrar recursos a la institución. En el caso de la UTPL la herramienta que más se acopló a sus necesidades fue la de distribución en Linux- Centos.
- Las configuraciones en el ambiente de laboratorio, tanto la distribución de Linux como Windows, cuentan con todas las facilidades para desplegar e implementar DNSSEC para los servicios DNS, en el caso particular de UTPL, si se quiere hacer una migración por ejemplo de Linux a Windows se debería evaluar el impacto de su implementación.
- Implementar nuevos recursos de registros (RR) con DNSSEC permite una integración con el servicio DNS, no elimina ninguna de las capacidades de DNS, solo amplía el nivel de seguridad a dicho protocolo.
- Con las DNSSEC, se observa un Internet más seguro para los usuarios, así que no tomar o no invertir en el despliegue de las extensiones de seguridad DNSSEC, será colocar a nuestro sitio como un potencial punto de ataque. Por lo que se debería adoptar una cultura de seguridad para que así los ataques a los diferentes servicios DNS, tengan un impacto mínimo o a su vez nulo al intentar explotar las vulnerabilidades del protocolo DNS, protegiendo así a los usuarios y las instituciones en ambos extremos de las conexiones.
- Se puede firmar la zona utpl.edu.ec, a través de un ancla de confianza, el hecho de que la zona de primer nivel TLD's ".ec" no se encuentra firmada con DNSSEC, no es excusa para no implementar DNSSEC en los servidores DNS de la UTPL.

RECOMENDACIONES

Revisar las versiones del software que se tiene en los equipos DNS, en el caso de la UTPL, la versión de la distribución de Linux, como también el software BIND9 que tienen instaladas las versiones 9.2.4 y 9.3.6, las cuales deberían actualizarse para aprovechar todas las ventajas actuales de las extensiones de seguridad.

Efectuar un mecanismo para el firmado automático de los registros a través de las llaves KSK y ZSK, ya que cada cierto tiempo caducan sus claves criptográficas. En la actualidad ya existen script que efectúan el firmado automático de los registros, solo se deberá monitorear que el proceso se haya efectuado en los tiempos establecidos.

Optar por una capacitación constante sobre las DNSSEC, para ir revisando las mejoras y actualizaciones disponibles que existen, para mejorar la seguridad en los diferentes vectores de ataques que tiene DNS.

REFERENCIAS

- Arends, R. Austein, R. Larson, M. Massey, D. and Rose, S. (2005). DNS Security Introduction and Requirements. RFC 4033 (Proposed Standard). <http://www.ietf.org/rfc/rfc4033.txt>.
- Arends, R. Austein, R. Larson, M. Massey, D. and Rose, S. (2005). Protocol Modifications for the DNS Security Extensions. RFC 4035 (Proposed Standard), <http://www.ietf.org/rfc/rfc4035.txt>, (Updated by RFC4470).
- Deccio, C. (2012). Maintenance, mishaps and mending in deployments of the domain name system security extensions (DNSSEC), *International Journal of Critical Infrastructure Protection*, Volume 5, Issue 2, Pages 98-103, ISSN 1874-5482, <http://dx.doi.org/10.1016/j.ijcip.2012.05.002>(<http://www.sciencedirect.com/science/article/pii/S1874548212000212>).
- Hollenbeck, S. (2005). Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP). RFC 4310 (Proposed Standard), <http://www.ietf.org/rfc/rfc4310.txt>.
- Huston, G. (2006). DNSSEC The Practice. The ISOC ISP column, <http://ispcolumn.isoc.org/2006-09/DNSSEC2.html>.
- Karrenberg, D. (2010). DNSSEC: Securing the global infrastructure of the Internet, *Network Security*, Volume 2010, Issue 6, Pages 4-6, ISSN 1353-4858, [http://dx.doi.org/10.1016/S1353-4858\(10\)70080-5](http://dx.doi.org/10.1016/S1353-4858(10)70080-5). (<http://www.sciencedirect.com/science/article/pii/S1353485810700805>)
- Kolkman, O. Schlyter, J. and Lewis, E. (2004). Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag. RFC 3757(roposed Standard), <http://www.ietf.org/rfc/rfc3757.txt>, (Obsoleted by RFCs 4033, 4034, 4035).
- Atkins, D., & Austein, R. (2004). Threat Analysis of the Domain Name System (DNS), 16. Retrieved from <https://tools.ietf.org/html/rfc3833>
- Comer, D. E. (1996). *REDES GLOBALES DE INFORMACION CON INTERNET Y TCP/IP*.
- Cz.nic. (2015). DNSSEC/TLSA Validator. Retrieved September 30, 2015, from <https://www.dnssec-validator.cz/pages/documentation.html>
- Deccio, C. (2012). Maintenance, mishaps and mending in deployments of the domain name system security extensions (DNSSEC). *International Journal of Critical Infrastructure Protection*, 5(2), 98–103. <http://doi.org/10.1016/j.ijcip.2012.05.002>
- DNSViz. (2014). Retrieved October 28, 2014, from <http://dnsviz.net/d/utpl.edu.ec/dnssec/>
- Fall. (2008). *Incident Response Guide to the Kaminsky DNS Cache Poison Exploit - kaminsky-cache-poison-ir.pdf*. Retrieved from <https://www.team-cymru.com/ReadingRoom/Whitepapers/2008/kaminsky-cache-poison-ir.pdf>
- Handley, M. J., & Rescorla, E. (2006). Internet Denial-of-Service Considerations, 38. Retrieved from <https://tools.ietf.org/html/rfc4732>
- Herrera, J. F. (2009). Las vulnerabilidades de seguridad de DNS. *Inventum*, 34-44(6), 34–44.

- Infoblox. (2013). *infoblox-whitepaper-prepare-withstand-dns-attacks.pdf*. U.S. Retrieved from <http://www.infoblox.es/sites/infobloxcom/files/es/resources/infoblox-whitepaper-prepare-withstand-dns-attacks.pdf>
- Karrenberg, D. (2010). DNSSEC: Securing the global infrastructure of the Internet. *Network Security*, 2010(6), 4–6. [http://doi.org/10.1016/S1353-4858\(10\)70080-5](http://doi.org/10.1016/S1353-4858(10)70080-5)
- Martínez-Cagnazzo, C. (2011). Conceptos generales de DNSSEC. Retrieved October 6, 2015, from <http://www.labs.lacnic.net/site/sites/default/files/dnssec-citel-generalidades-ES-01.pdf>
- Microsoft-TechNet. (2015). Paso a paso: demostración de DNSSEC en un laboratorio de pruebas. Retrieved December 19, 2014, from <http://technet.microsoft.com/es-es/library/hh831411.aspx>
- Mockapetris, P. (1987). *RFC-1034*. Retrieved from <http://www.rfc-es.org/rfc/rfc1034-es.txt>
- Network Startup Resource Center. (2015). DNSSEC Introduction Principles Deployment. Retrieved October 6, 2015, from <https://nsrc.org/workshops/2015/apricot2015/raw-attachment/wiki/Track2Agenda/03-dnssec-tutorial.pdf>
- Padilla, A. L. (2013). Autor Antonio López Padilla Coordinación, 73.
- Stewart, J. (2003). DNS cache poisoning—the next generation. *Com/Research/Articles/Dns-Cache-Poisoning*, 13. Retrieved from <http://www.ouah.org/DNScp.htm>
- TANENBAUM, A. S. (2003). *Redes de computadoras* (Cuarta edi).
- Unixwiz.net. (2008). An Illustrated Guide to the Kaminsky DNS Vulnerability. Retrieved September 17, 2014, from <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>
- Wales, E. (2000). Health Care Industry Debate: Electronic Versus Digital Signatures. *Network Security*, 2000(12), 5. [http://doi.org/10.1016/S1353-4858\(00\)12013-6](http://doi.org/10.1016/S1353-4858(00)12013-6)

ANEXOS

ANEXO A. INSTALACIÓN Y CONFIGURACIÓN DE CENTOS 7- BIND 9

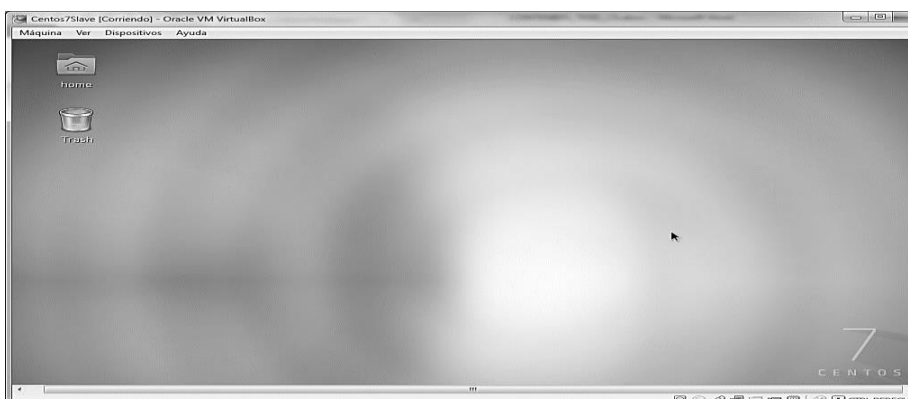


Figura 33. GUI de Centos 7.
Elaborado por: César Guanoliقة.

En la figura 33, se observa la interfaz gráfica de la distribución Linux –Centos 7, el entorno gráfico (GUI), cuenta con herramientas para la administración y configuración del servicio DNS.



Figura 34. Archivo de configuración named.conf.
Elaborado por: César Guanoliقة.

En la figura 34, se muestra el contenido parcial del archivo de configuración del software DNS - BIND9, donde se encuentra todos los archivos que intervienen para el arranque del servicio.

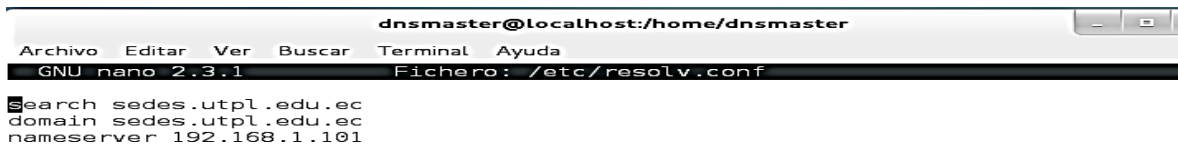


Figura 35. Contenido del archivo resolv.conf.
Elaborado por: César Guanoliقة.

En la Figura 35, se muestra el contenido del archivo resolv.conf, éste archivo es el encargado de establecer en que dominio se encuentra trabajando el servidor DNS, así como también se especifica su dirección IP, para que al momento de ser consultarlo responda con la dirección IP del servidor DNS.

```

dnsmaster@localhost:/home/dnsmaster
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.3.1 Fichero: /var/named/sedes.zone
$ORIGIN sedes.utpl.edu.ec.
$TTL 86400
@ IN SOA masterdns.sedes.utpl.edu.ec. root.sedes.utpl.edu.ec. (
    1 ; serial
    3600 ; refresh
    1800 ; retry
    604800 ; expire
    86400 ) ; minimum

; Nombre de los servidores
@ IN NS masterdns.sedes.utpl.edu.ec.
@ IN NS slavedns.sedes.utpl.edu.ec.

; Direcciones Ip's de los servidores DNS
@ IN A 192.168.1.101
@ IN A 192.168.1.102

;Maquinas y servicios en el Dominio sedes.utpl.edu.ec
@ IN A 192.168.1.11
@ IN A 192.168.1.12
masterdns IN A 192.168.1.101
slavedns IN A 192.168.1.102
pcadmin IN A 192.168.1.11
pcsecretaria IN A 192.168.1.12

```

Figura 36. Archivo de zona directa.
Elaborado por: César Guanoliقة.

En la figura 36, se observa el contenido parcial del archivo de zona directa, en el cual se forman las tuplas de todos los registros de recursos que contiene la zona sedes.utpl.edu.ec.

```

dnsmaster@localhost:/home/dnsmaster
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.3.1 Fichero: /var/named/sedes.inv.zone
$ORIGIN 1.168.192.in-addr.arpa.
$TTL 86400
@ SOA masterdns.sedes.inv.utpl.edu.ec. root.sedes.utpl.edu.ec. (
    2 ; serial
    3600 ; refresh
    1800 ; retry
    604800 ; expire
    86400 ) ; minimum

; Nombre de los servidores DNS
@ IN NS masterdns.sedes.utpl.edu.ec.
@ IN NS slavedns.sedes.utpl.edu.ec.
;@ IN PTR sedes.utpl.edu.ec.

;Ip's de los serviodres DNS.
masterdns IN A 192.168.1.101
slavedns IN A 192.168.1.102

;maquinas o servicios del dominio sedes.utpl.edu.ec.
pcadmin IN A 192.168.1.11
pcsecretaria IN A 192.168.1.12
101 IN PTR masterdns.sedes.utpl.edu.ec.
102 IN PTR slavedns.sedes.utpl.edu.ec.
11 IN PTR pcadmin.sedes.utpl.edu.ec.
12 IN PTR pcsecretaria.sedes.utpl.edu.ec.

```

Figura 37. Archivo de zona inversa.
Elaborado por: César Guanoliقة.

En la figura 37, se visualiza el archivo de zona inversa, que es el encargado de almacenar todos los registros de recursos que apuntan a un host determinado, con el fin de resolver las consultas a través de la dirección IP que requieran saber el nombre del host al que corresponda.

```

[root@localhost named]# iptables -t filter -I INPUT 7 -s 192.168.1.0/24 -p tcp -
n tcp --dport 53 -j ACCEPT
[root@localhost named]# iptables -t filter -I INPUT 8 -s 192.168.1.0/24 -p udp -
n udp --dport 53 -j ACCEPT
[root@localhost named]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[root@localhost named]# service named restart
Redirecting to /bin/systemctl restart named.service
[root@localhost named]# service iptables restart
Redirecting to /bin/systemctl restart iptables.service
[root@localhost named]# █

```

Figura 38. Configuración de iptables.

Elaborado por: César Guanoliqúe.

En la figura 38, se muestra como se realiza el ingreso de las reglas iptables para la configuración del firewall en nuestro equipo, éstas iptables crean reglas de acceso para permitir o denegar el tráfico a un determinado puerto o puertos.

Configuración de las reglas para que el firewall permita comunicarse por medio del puerto 53, a través del protocolo UDP y TCP, así resolver todas las consultas y actualizaciones de zona que se realicen en los servidores DNS. Por ejemplo tenemos un comando iptables:

- iptables -I INPUT -p udp/tcp --dport 53 -m state --state NEW -j ACCEPT

El cual introduce una regla para que el puerto 53 soporte el tráfico que se genera a través de los protocolos TCP y UDP.

Comprobamos si la tarjeta de red está configurada de acuerdo a nuestro esquema de red. En la figura 39, se muestra un fragmento de la configuración de la tarjeta de red en el servidor maestro.

- Ifconfig – muestra la interfaz de red que tiene nuestro equipo que en este caso es enp0s3.

```

[root@localhost dnsmaster]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fe62:a48d prefixlen 64 scopeid 0x20<link>
ether 08:00:27:62:a4:8d txqueuelen 1000 (Ethernet)
RX packets 47 bytes 5738 (5.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 67 bytes 9077 (8.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 523 bytes 40718 (39.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 523 bytes 40718 (39.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura 39. Estado de nuestra interfaz de red.

Elaborado por: César Guanoliqúe.

Si no estuviera configurada la tarjeta de red, se aplica los comandos:

- Nano /etc/sysconfig/network-scripts/ifcfg-enp0s3
- IPADDR= 192.168.1.101 en el maestro y IPADDR= 192.168.1.102 en el esclavo
- NETMASK=255.255.255.0

Luego se levanta el servicio a través del siguiente comando:

- Service network restart

Y para tener la certeza de que las máquinas DNSMaster y DNSSlave están comunicándose se realiza las pruebas con el comando “ping”. En la figura 40 detalla un ping desde el servidor DNSMaster hacia el servidor DNSSlave.

```
[root@localhost dnsmaster]# ping 192.168.1.102 -c 2
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data:
64 bytes from 192.168.1.102: icmp_seq=1 ttl=64 time=0.381 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=64 time=0.413 ms
--- 192.168.1.102 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.381/0.397/0.413/0.016 ms
[root@localhost dnsmaster]#
```

Figura 40. Ejecución del comando ping para comprobar que exista comunicación entre los servidores.
Elaborado por: César Guanoliقة.

```
[root@localhost slaves]# cd /var/named/slaves/
[root@localhost slaves]# ls -l
total 8
-rw-r--r--. 1 named named 806 dic  2 12:15 sedes.inv.zone
-rw-r--r--. 1 named named 521 dic  2 12:23 sedes.zone
[root@localhost slaves]#
```

Figura 41. Archivos de zona transferidos.
Elaborado por: César Guanoliقة.

En la figura 41, se muestra la transferencia de los dos archivos de las zonas creadas en el servidor maestro, de acuerdo a la configuración que se hizo en el archivo named.conf del servidor maestro, los archivos que se hacen referencia son: sedes.zone y sedes.inv.zone

```
hint: some times were ellipsized, use -t to show in full.
[root@localhost dnsmaster]# service iptables status
Redirecting to /bin/systemctl status iptables.service
iptables.service - IPv4 firewall with iptables
Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled)
Active: inactive (dead)
```

Figura 42. Estado del servicio iptables.
Elaborado por: César Guanoliقة.

En la figura 42, se observa el comando que se utiliza para saber si nuestro firewalld está habilitado y funcionando, en éste caso se puede observar que a través del comando service iptables status el firewall se encuentra deshabilitado.

```
[root@localhost dnsmaster]# service iptables restart
Redirecting to /bin/systemctl restart iptables.service
```

Figura 43. Reinicio del servicio iptables.
Elaborado por: César Guanoliقة.

En la figura 43, se describe el comando para reiniciar el servicio iptables, el cual es: service iptables restart, éste comando se lo utiliza para que se establezca una nueva regla en el firewall ingresada con anterioridad.

```
[root@localhost dnsmaster]# chkconfig iptables on
Nota: Reenviando petición a 'systemctl enable iptables.service'.
ln -s '/usr/lib/systemd/system/iptables.service' '/etc/systemd/system/basic.target.wants/iptables.service'
```

Figura 44. Comando chkconfig.
Elaborado por: César Guanoliq.

En la figura 44, se visualiza la ejecución del comando “chkconfig iptables on”, con el objetivo de establecer el arranque automático de firewalld, este comando permitirá que se inicie el servicio cada vez que nuestro servidor este en funcionamiento.

```
[root@localhost dnssec-keys]# dnssec-keygen -a NSEC3RSASHA1 -b 2048 -n ZONE sede
s.zone
Generating key pair.....
.....+++ .....+++
Ksedes.zone.+007+45575
[root@localhost dnssec-keys]#
```

Figura 45. Generación de las llaves privadas.
Elaborado por: César Guanoliq.

En la figura 45, observamos el comando “dnssec -keygen” en donde se agregan los atributos para la generación de las llaves públicas y privadas, así como también con que argumentos son creadas. En esta ocasión, se generan las llaves privadas.

```
[root@localhost dnssec-keys]# dnssec-keygen -r /dev/urandom -a RSASHA1 -b 4096 -
n ZONE -f KSK sedes.zone
Generating key pair.....
.....++ .....
.....++
Ksedes.zone.+005+42733
[root@localhost dnssec-keys]#
```

Figura 46. Generación de las llaves públicas.
Elaborado por: César Guanoliq.

En la figura 46, se describe el proceso de generación de las llaves públicas, a través del comando “dnssec-keygen” y sus atributos se crean las llaves públicas.

```
[root@localhost dnssec-keys]# ls -l
total 16
-rw-r--r--. 1 root root 949 dic 2 16:23 Ksedes.zone.+005+42733.key
-rw-----. 1 root root 3314 dic 2 16:23 Ksedes.zone.+005+42733.private
-rw-r--r--. 1 root root 604 dic 2 16:10 Ksedes.zone.+007+45575.key
-rw-----. 1 root root 1779 dic 2 16:10 Ksedes.zone.+007+45575.private
[root@localhost dnssec-keys]#
```

Figura 47. Vista general de las llaves creadas en el fichero DNSSEC-keys.
Elaborado por: César Guanoliq.

La figura 47 muestra el directorio donde se generaron las diferentes llaves públicas y privadas con las cuales se procederán al firmado de los diferentes registros de recursos que se encuentra en los archivos de zona, tanto directa como inversa.

```
[root@localhost named]# dnssec-signzone -S -K /etc/pki/dnssec-keys -e +3024000
o sedes.utpl.edu.ec -t sedes.zone
Verifying the zone using the following algorithms: NSEC3RSASHA1.
Zone fully signed:
Algorithm: NSEC3RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked
                        ZSKs: 1 active, 0 stand-by, 0 revoked

sedes.zone.signed
Signatures generated:          14
Signatures retained:           0
Signatures dropped:             0
Signatures successfully verified: 0
Signatures unsuccessfully verified: 0
Signing time in seconds:        0.030
Signatures per second:         458.010
Runtime in seconds:             0.206
[root@localhost named]# █
```

Figura 48. Firma de la zona sedes.utpl.edu.ec.
Elaborado por: César Guanoliq.

En la figura 48, se observa el procedimiento para el firmado de la zona sedes.utpl.edu.ec, a través del comando “dnssec-signzone”, el cual por medio de varios atributos se establece con que algoritmos de encriptación se va a firmar, así como las llaves públicas y privadas que se utilizan.

```
#editando la zona sedes.utpl.edu.ec
zone "sedes.utpl.edu.ec" IN {
    type master;
    file "sedes.zone.signed";
    allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "sedes.inv.zone";
    allow-update { none; };
};
```

Figura 49. Configuración fichero named.conf.
Elaborado por: César Guanoliq.

En la figura 49, se visualiza la modificación del fichero “named.conf”, ya que se debe agregar la ruta de los nuevos ficheros de zona, tanto directa como inversa, los cuales fueron firmados digitalmente con DNSSEC.

ANEXO B. INSTALACIÓN Y CONFIGURACIÓN DE WINDOWS SERVER 2012.

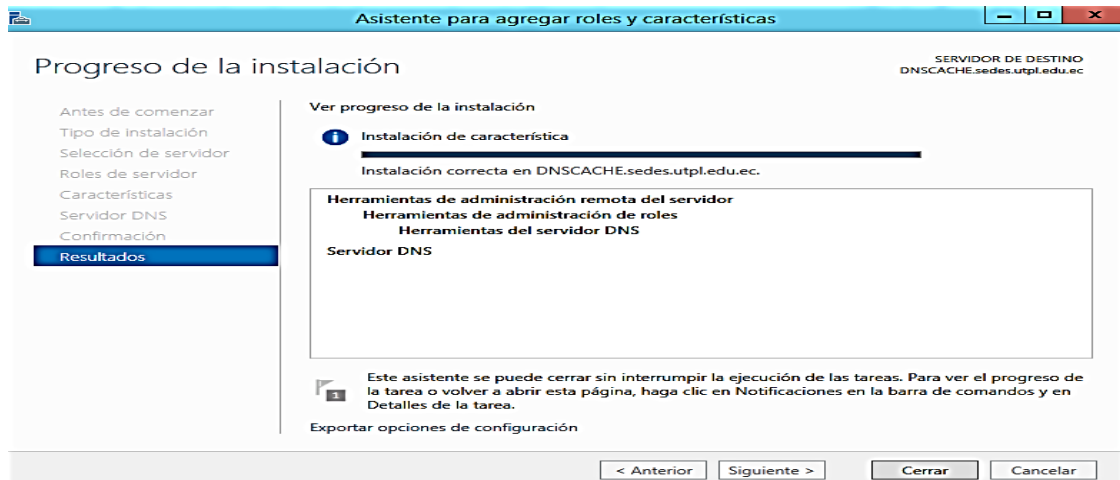


Figura 50. Instalación del servidor DNS.
Elaborado por: César Guanoliq.

La figura 50 muestra el proceso de instalación y configuración del servicio DNS en Windows Server, en esta ocasión se está configurando o instalando el servidor DNS caché.

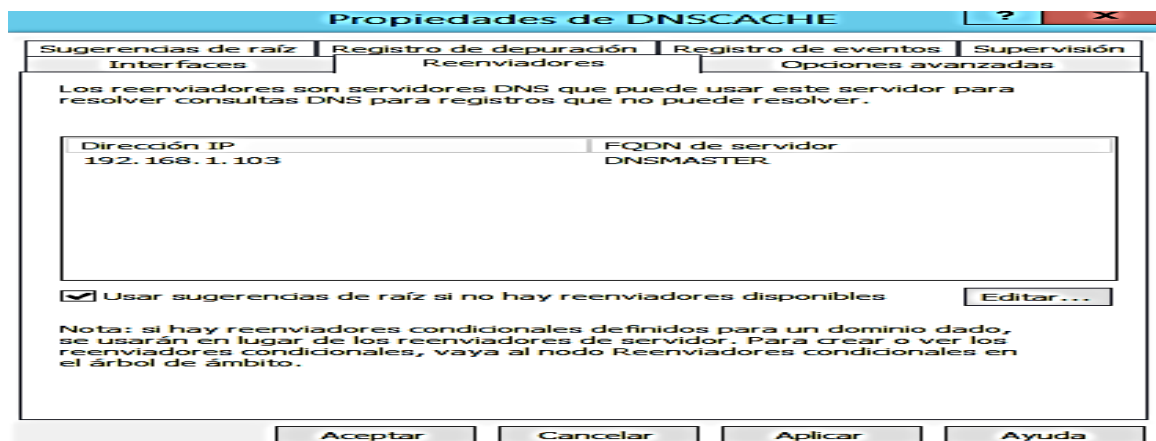


Figura 51. Configuración del servidor DNS caché.
Elaborado por: César Guanoliq.

En la figura 51, se observa la configuración del servidor DNS Caché (Servidor secundario), en la cual se puede observar la dirección del servidor maestro, del cual va a recibir todas las consultas DNS externas y actualizaciones.

```

Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\user1> resolve-dnsname -name sec.sedes.utpl.edu.ec.trustanchors -type dnskey -server dnscache

Name                                     Type      TTL      Section  Flags  Protocol Algorithm  Key
-----
sec.sedes.utpl.edu.ec.trustanchors      DNSKEY 3600    Answer   257    DNSSEC  8                {3, 1, 0, 1...}
sec.sedes.utpl.edu.ec.trustanchors      DNSKEY 3600    Answer   257    DNSSEC  8                {3, 1, 0, 1...}

PS C:\Users\user1> resolve-dnsname -name sec.sedes.utpl.edu.ec.trustanchors -type dnskey -server dnscache

```

Figura 52. Anclas o puntos de confianza.
Elaborado por: César Guanoliqúe.

En la figura 52, se puede visualizar los puntos de confianza (Anclas de confianza) de la zona secundaria sec.sedes.utpl.edu.ec (sub dominio), que genera el servidor Windows para el dominio sedes.utpl.edu.ec.

```

PS C:\> Resolve-DnsName dnsmaster.sedes.utpl.edu.ec -server dnscache -dnssecok

Name                                     Type      TTL      Section  IPAddress
-----
dnsmaster.sedes.utpl.edu.ec             A          2608    Answer   192.168.1.103

Name      :
QueryType : OPT
TTL       : 32768
Section   : Additional
Data      : {}

```

Figura 53. Petición de una resolución de nombre DNS master.sedes.utpl.edu.ec.
Elaborado por: César Guanoliqúe.

En la figura 53, se observa una consulta DNS al servidor maestro desde el servidor secundario, con el comando “Resolve-DnsName”, el cual genera una respuesta por partes del servidor principal.