UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicadas en comunidades virtuales de aprendizaje de las instituciones de Educación Superior"

"Tesis previa a la Obtención del título de Ingeniero en Sistemas"

Autora: Gabriela Paulina Espinoza Ami

Director: Ing. Luis Antonio Chamba Eras, Mg.Sc

LOJA-ECUADOR
2014

Certificación del Director

Ing. Luis Antonio Chamba Eras, Mg.Sc.

DOCENTE DE LA CARRERA DE INGENIERÌA EN SISTEMAS

CERTIFICA:

Que la egresada Gabriela Paulina Espinoza Ami autora del presente trabajo de titulación, cuyo tema versa sobre "EXTENSIONES DE SEGURIDAD PARA EL SISTEMA DE NOMBRES DE DOMINIO APLICADAS EN COMUNIDADES VIRTUALES DE APRENDIZAJE DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR", ha sido dirigido, orientado y discutido bajo mi asesoramiento y reúne a satisfacción los requisitos exigidos en una investigación de este nivel por lo cual autorizo su presentación y sustentación.

Loja, Mayo de 2014

Ing. Luis Antonio Chamba Eras, Mg.Sc.

DIRECTOR DEL TRABAJO DE TITULACIÒN

Autoría

Yo Gabriela Paulina Espinoza Ami declaro ser autora del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional-Biblioteca Virtual.

Autora: Gabriela Paulina Espinoza Ami.

Firma: 

Cédula: 1105139453

Fecha: 14 de mayo de 2014

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo Gabriela Paulina Espinoza Ami declaro ser autora de la tesis titulada: "EXTENSIONES DE SEGURIDAD PARA EL SISTEMA DE NOMBRES DE DOMINIO APLICADAS EN COMUNIDADES VIRTUALES DE APRENDIZAJE DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR", como requisito para optar al grado de: Ingeniera en Sistemas; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los catorce días del mes de mayo del dos mil catorce, firma la autora.

Firma: 

Autora: Gabriela Paulina Espinoza Ami.

Cédula: 1105139453.

Dirección: Córdova y Río de Janeiro. Correo Electrónico: gpespinozaa@unl.edu.ec

Teléfono: 2614360. Celular: 0985847804.

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Luis Antonio Chamba Eras, Mg.Sc.

Tribunal de Grado: Ing. Hernán Leonardo Torres Carrión, Mg.Sc.

Ing. Edwin René Guamán Quinche, Mg.Sc.

Ing. Pablo Fernando Ordóñez Ordóñez, Mg.Sc.

Agradecimiento

A mi madre y padre por su apoyo al brindarme la posibilidad de concretar una carrera profesional.

Al Ing. Luis Chamba quien con su experiencia y conocimiento fue mi guía en la elaboración y desarrollo del trabajo de titulación.

A los docentes por los conocimientos impartidos en mi formación académica.

Dedicatoria

A mi madre, Hilda.

A mi padre, Gerardo.

A mis hermanos, José Luis y Francis.

Cesión de Derechos

Gabriela Paulina Espinoza Ami autora principal del presente trabajo de titulación, autoriza a la Universidad Nacional de Loja, al Área de la Energía, las Industrias y los Recursos Naturales No Renovables y por ende a la Carrera de Ingeniería en Sistemas hacer uso del mismo en lo que estime sea conveniente.

a. Título

“Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicadas en comunidades virtuales de aprendizaje de las instituciones de Educación Superior”.

b. Resumen

Las instituciones de educación superior almacenan gran cantidad de información sensible y se mantienen activas en línea en las comunidades virtuales de aprendizaje cuyo acceso debe ser restringido, los ataques DNS resultan en contraseñas robadas, e-mail alterado, la exposición al malware, y otros problemas; por lo que el presente trabajo de titulación corresponde a un estudio sobre las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) aplicado en comunidades virtuales de aprendizaje de las instituciones de educación superior, para validar la autenticidad y la integridad de los datos del Sistema de Nombres de Dominio (DNS).

Para lo cual se realizó una serie de pasos sucesivos y ordenados llegando a la aplicación de métodos respectivos para establecer el tema a investigar, determinar objetivos, estructurar el estado del arte y plantear soluciones al problema trazado. Además, se empleó una metodología de resolución de problemas que reveló qué hacer con el problema planteado.

Asimismo se analizó el estado del arte del DNS de las instituciones de educación superior a nivel internacional, nacional y local. Igualmente se desarrolló una simulación virtualizada de los servidores DNS de las universidades, en los que se realizó las configuraciones para el funcionamiento de DNSSEC, a través del proceso de firma de las zonas DNS mediante las claves públicas y privadas que establecen una cadena de confianza. Así también, se configuró un servidor de nombres recursivo que almacenó las claves públicas de los dominios firmados creando de esta forma anclas de confianza para validar las respuestas por parte de los usuarios. Como resultado de estos procedimientos se establecieron islas de confianza a los dominios firmados que a su vez crearon un archipiélago de confianza entre los mismos.

Además se efectuó el proceso de renovación de claves donde una de las claves en la zona se sustituyó por otra. También se realizó la generación de un secreto compartido de Transacciones Firmadas (TSIG) utilizado para firmar el contenido de cada paquete DNS, con lo que se aseguró la transferencia de zona que garantizó la comunicación entre los servidores. Como medios de validación en el navegador de la máquina del usuario se instaló el plugin DNSSEC Validator que verificó que los dominios están asegurados con DNSSEC y se realizó un ataque DNS como es el redireccionamiento DNS que comprobó que los dominios asegurados no sufren de esta vulnerabilidad.

Summary

Institutions of higher education store large amounts of sensitive information and these stay active online in virtual learning communities which access should be restricted, the DNS attacks result in stolen passwords, e-mail altered, exposure to malware, and other issues; therefore the present work of titling corresponds to a study on the Security Extensions Domain Name System (DNSSEC) applied to virtual learning communities of institutions of higher education, to validate the authenticity and integrity of Domain Name System (DNS) data.

For thus a series of successive and ordered steps was performed coming to the implementation of respective methods for the research topic, setting goals, structuring the state of art and propose solutions to the problem. In addition a methodology troubleshooting was used that revealed what to do with the problem.

Also an analysis of the state of the art of DNS of institutions of higher education was made to international, national and local level. Equally a virtualized simulation of DNS servers of universities was developed, in which the necessary configurations for the operation of DNSSEC was performed, through the process of signing DNS zones using public and private keys that establish a chain of trust. So also a recursive name server that stored the public key of the signed domains was configured, creating this form of trust anchors to validate responses from users. As a result of these procedures were established as islands of trust signed domains that in turn created an archipelago of trust between them.

Besides the rolling key process in which a key was replaced by another key was made. Also the generating of a shared secret of Transaction Signature (TSIG) used to sign the content of each DNS packet was performed, whereby the zone transfer that ensured communication between servers was sure. As a means of validation DNSSEC Validator plugin was installed on the browser of the user's machine to verify that the domains are secured with DNSSEC and a DNS attack was performed as is the DNS redirection that verified that domains insured does not suffer from this vulnerability.

Índice de Contenidos

Índice General

Índice de Figuras

Índice de Tablas

c. Introducción

Las instituciones de educación superior representan un microcosmos de la Internet como un todo, repleto de ataques cibernéticos, algunos de los cuales podrían ser impedidos por una combinación de firma y validación DNSSEC; en la parte académica, DNSSEC se suma a la autenticidad del producto del trabajo académico [1].

Las comunidades virtuales de aprendizaje proporcionan el ambiente idóneo para que el alumno se inicie en la comunicación virtual con otros congéneres con los cuales comparte información [2], en donde la utilización de DNSSEC puede contribuir a combatir los ataques de suplantación de identidad, ataques contra la integridad de la información y el riesgo de que los usuarios sean redirigidos hacia cualquier sitio web inseguro o no deseado.

DNSSEC es un conjunto de especificaciones técnicas para salvaguardar ciertos tipos de información proporcionada por el DNS, que pretende proteger a los usuarios de las comunidades virtuales de aprendizaje contra cierto tipo de riesgos y ataques maliciosos mediante la firma digital de la información usando algoritmos de cifrado criptográficos de clave pública/privada, esto significa que la información es cifrada con la clave privada y validada con la clave pública, tal y como lo realizan los procesos de cifrado de clave pública/privada; con lo que el usuario puede tener certeza acerca de su validez [3].

Con la implementación de la actualización técnica, DNSSEC señalará automáticamente que los usuarios han sido dirigidos a comunidades virtuales de aprendizaje reales que pretendían visitar, mitigando el riesgo de que sean inconscientemente raptados o erróneamente dirigidos a sitios falsos que pudieran poner en riesgo su seguridad; con lo que se podrá establecer una cadena de confianza en las comunidades virtuales de aprendizaje de cada institución de educación superior, en donde se podrá garantizar la procedencia de contenidos creados en este tipo de ambientes de aprendizaje [4].

Los riesgos derivados del DNS y los beneficios de implementar DNSSEC tienen un significado especial para la educación superior. Se espera que las universidades sean “buenos ciudadanos de Internet” y den ejemplo en los esfuerzos para mejorar el bienestar público. Dado que los usuarios tienden a confiar en determinados ámbitos como el dominio .edu, más que otros, las expectativas para la fiabilidad de los sitios

web de la universidad son altas. En la medida en que las instituciones de educación superior dependen de su reputación, DNSSEC es una vía para evitar algunos de los tipos de incidentes que pueden dañar el prestigio de una universidad.

En términos más concretos, las instituciones de educación superior almacenan enormes cantidades de información sensible (incluyendo la información personal y financiera para los estudiantes y otras personas, información médica y datos de investigación), y se mantienen activos en línea en las comunidades virtuales de aprendizaje cuyo acceso debe ser restringido efectivamente. Los ataques DNS resultan en contraseñas robadas, e-mail alterado (que a menudo es el canal para las comunicaciones oficiales), la exposición al malware, y otros problemas; por lo que DNSSEC puede ser una parte importante de una estrategia de seguridad cibernética de base amplia [5].

Razones por las cuales se ha realizado un estudio para la implementación de DNSSEC en comunidades virtuales de aprendizaje de las instituciones de educación superior, utilizando un ambiente virtualizado donde se simula los servidores DNS de las universidades y se realiza el aseguramiento de las zonas DNS, así como también un servidor de nombres recursivo que valida las respuestas efectuadas por los usuarios; además se efectúa el proceso de renovación de claves para alternar las mismas cuando caduquen, y se realiza el aseguramiento de la transferencia de zona como medio para garantizar la comunicación entre los servidores a través de la creación de un secreto compartido de Transacciones Firmadas (TSIG); así también se emplea como herramienta de validación el plugin DNSSEC Validator que comprueba la existencia de DNSSEC en las zonas aseguradas, y se efectúa un redireccionamiento DNS como un tipo de ataque DNS que comprueba que los dominios asegurados no se sufren de esta vulnerabilidad.

Actividades realizadas con la finalidad de dar cumplimiento a los objetivos planteados como son: analizar el estado del arte del Sistema de Nombres de Dominio de las instituciones de educación superior, para determinar los requerimientos de implementación de DNSSEC, proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de educación superior, y asegurar la comunicación entre servidores de las mismas.

La estructura del presente informe consta de la Revisión de Literatura que comprende la temática del DNS donde se detalla la infraestructura, el funcionamiento, los

componentes y la inseguridad; y la temática de DNSSEC que consta de la definición, lo que no es, la necesidad, el funcionamiento, la seguridad, cadena de confianza, islas de confianza, y los registros de recursos. Así también, la sección de Materiales y Métodos que abarca en detalle los recursos materiales, métodos científicos y técnicas de recolección de información utilizadas y la metodología para el cumplimiento de las fases del trabajo. El apartado de Resultados incluye el desarrollo de los procedimientos aplicados en el trabajo, donde constan todas las configuraciones realizadas para el funcionamiento de DNSSEC. En la parte de Discusión se presenta los principios, relaciones y generalizaciones de los resultados obtenidos. La sección de Conclusiones expone las deducciones de las experiencias obtenidas durante el cumplimiento de los objetivos. Y el apartado de Recomendaciones contiene sugerencias que pueden llevarse a cabo durante el despliegue de DNSSEC en las instituciones de educación superior.

d. Revisión de Literatura

1. Sistema de Nombres de Dominio (DNS).

El sistema de nombres de dominio (DNS) es un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se emplea en redes TCP/IP, como Internet, para buscar equipos y servicios mediante nombres descriptivos [6].

Este sistema proporciona un esquema jerárquico de nombres basado en dominios y una base de datos distribuida para implementar este esquema. Su función principal es la de relacionar direcciones de host y servicios de red con sus direcciones IP correspondientes y viceversa [7].

1.1. Funcionamiento del DNS.

Cuando un servidor recibe una consulta para resolver un nombre (por ejemplo unl.edu.ec) (ver Figura 1):

1. Comprueba si el nombre pertenece a alguno de los dominios que sirve. Si es así, busca en su "mapa" y devuelve la IP correspondiente.
2. Si no, pregunta a un servidor del dominio raíz, que le contestará con la IP de un servidor del dominio "ec".
3. Luego pregunta a ése, obteniendo la IP de un servidor del dominio edu.ec.
4. Ahora se pregunta al último, que ya tiene en su mapa la IP buscada [8].

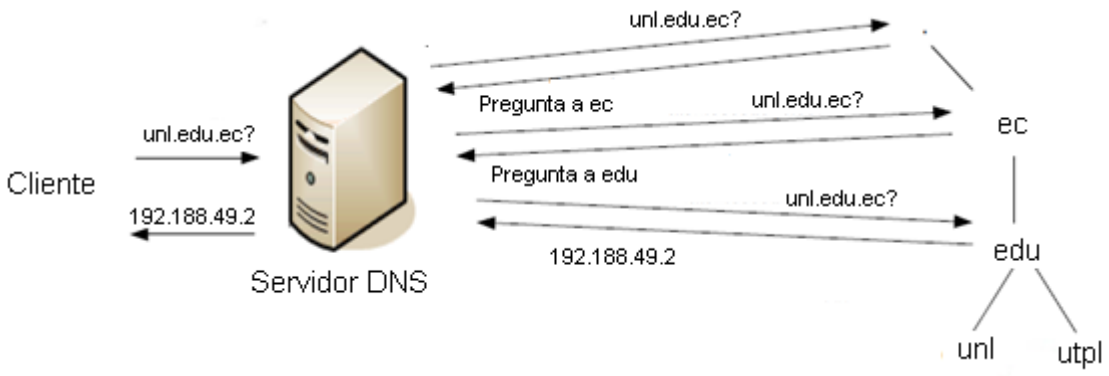

Figura 1. Funcionamiento del DNS.

Si el servidor tiene la respuesta, nos la proporcionará, indicándonos además si es autoritativa, es decir, dicho servidor tiene autoridad en dicho dominio. En caso de que no lo conozca, hay dos maneras de proceder Recursiva e Iterativa [9].

1.1.1. Resolución recursiva.

En las resoluciones recursivas, el servidor no tiene la información en sus datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta [10].

1.1.2. Resolución iterativa.

Las resoluciones iterativas consisten en la respuesta completa que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados. El servidor encargado de hacer la resolución realiza iterativamente preguntas a los diferentes DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la máquina que contiene la zona autoritativa para el nombre que se desea resolver [10].

1.2. Inseguridad del DNS.

El sistema DNS puede ser explotado por un atacante de múltiples formas. En sus vertientes más benignas puede ser utilizado como una valiosa fuente de información para ataques posteriores. Pero los mayores peligros vienen de la capacidad de explotar fallos en el protocolo o la implementación del mismo en clientes y servidores para conseguir modificar fraudulentamente las resoluciones de DNS, con el propósito de desviar las conexiones de sus destinatarios reales [11].

Hay varias clases diferentes de amenazas al DNS, la mayoría de los cuales son casos relacionados con los problemas más generales del DNS, pero algunas de las cuales son específicas a las particularidades del protocolo DNS [12].

1.2.1. La interceptación de paquetes.

Una de las formas de interceptación de paquetes son los ataques man-in-the-middle y dentro de este tipo de ataques se encuentra el redireccionamiento DNS, el cual se llevó a cabo en el trabajo de titulación como medio para verificar que los dominios firmados con DNSSEC no sufren de esta vulnerabilidad.

2. Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC).

DNSSEC es una especificación de una extensión para el DNS a través de la definición de los Registros de Recursos DNS adicionales que pueden ser utilizados por los clientes DNS para validar la autenticidad de una respuesta DNS, y donde la respuesta indica que tal dominio o tipo de recurso no existe, esta información negativa también puede ser autenticado. En otras palabras, si un atacante intenta crear una respuesta de DNS que ha sido alterada a partir de la autenticación original, y el atacante luego intenta pasar la respuesta como una respuesta auténtica, entonces un cliente DNSSEC debe ser capaz para detectar el hecho de que la respuesta ha sido alterada y que la respuesta no se corresponde con la información DNS con autoridad para esa zona. Es decir, DNSSEC está destinado a proteger a los clientes DNS de datos DNS falsos. Esta protección no elimina el potencial para inyectar datos falsos en una operación de resolución de DNS, pero se añade información adicional a las respuestas DNS para permitir que un cliente pueda comprobar si la respuesta es auténtica y completa [13].

2.1. Funcionamiento de DNSSEC.

Mediante el uso de DNSSEC, se está construyendo una cadena de confianza. La cadena se crea al permitir que un padre firme la clave pública de un hijo. Las cadenas se inician con una clave que es conocida para un dispositivo de resolución. Lo ideal sería que esta clave fuese la clave de los servidores raíz de Internet. Esta clave puede ser publicada en un diario de circulación nacional y en un sitio web, para que todo el que quiera pueda comprobar la exactitud de las llaves de su padre.

Si un resolutor confía en un TLD, por tener esa clave preconfigurada, ese punto en el árbol de DNSSEC se llama un punto de entrada de seguridad. En el caso ideal sólo hay un punto de entrada de seguridad, los servidores raíz (".").

Si un resolutor encuentra una firma con una clave que no conoce, esta subirá por la cadena para buscar una llave que lo sepa. Los resolutores eventualmente encuentran una clave de confianza o no la encuentran. En el primer caso los resultados pueden ser validados, y, o bien se encuentran protegidos o no protegidos, en el último caso los resultados se consideran malos. Para evitar que se produzcan bucles, BIND9 sólo

permite claves subsiguientes de las zonas por encima de la zona actual, por lo que pondrá fin a una búsqueda de una clave no existente en el "." [14].

2.2. Seguridad basada en cifrado.

La seguridad que DNSSEC proporciona esta basada en la firma de información usando algoritmos de cifrado criptográficos de clave pública/privada, esto significa que la información es cifrada con la clave privada y validada con la clave pública, tal y como lo realizan los procesos de cifrado de clave pública/privada. DNSSEC es implementado en una zona o nivel dentro de la estructura de DNS, y es la zona completa la que es firmada con los certificados digitales.

Una característica importante de DNSSEC es que el proceso de firma es realizado offline y sería imposible realizar el proceso de firma digital en “tiempo real”. Por lo tanto DNSSEC firma las zonas en el proceso de implementación del servicio antes de ponerlo en funcionamiento, con lo que las zonas firmadas son almacenadas y tiene que ser servidas por un servidor DNS que soporte DNSSEC.

Al proporcionar estas zonas firmadas, DNSSEC ofrece respuestas autenticadas a las consultas DNS recibidas. Un servidor de almacenamiento de caché de nombres de dominio o incluso un cliente puede validar las respuestas recibidas por el servidor DNS, comprobando la firma de la respuesta recibida contra la clave pública apropiada. Es importante tener en cuenta que DNSSEC no proporciona confidencialidad. DNSSEC sólo demuestra que una respuesta es correcta [15].

2.3. Cadena de confianza.

DNSSEC usa pares de claves asimétricos, esto es, pares de claves públicas y privadas. Este sistema de dos elementos fue desarrollado por arquitectos de la IETF (Internet Engineering Task Force).

Dentro de una zona, basta con conocer la KSK pública para validar la ZSK y luego los RRs. Entre una zona y su padre, DNSSEC usa un DS-RR (Delegation Signer RR). En lo alto de la cadena de confianza hay una KSK, que define el SEP, o Anclaje de Confianza, y designa como región segura la jerarquía de la zona por debajo de ella [16].

2.4. Islas de confianza.

Debido a que las zonas ec. y edu.ec. aún no están firmadas, cualquier dominio que tenga como su zona padre a uno de ellos y despliegue DNSSEC formará una isla de confianza como se muestra en la figura 2.

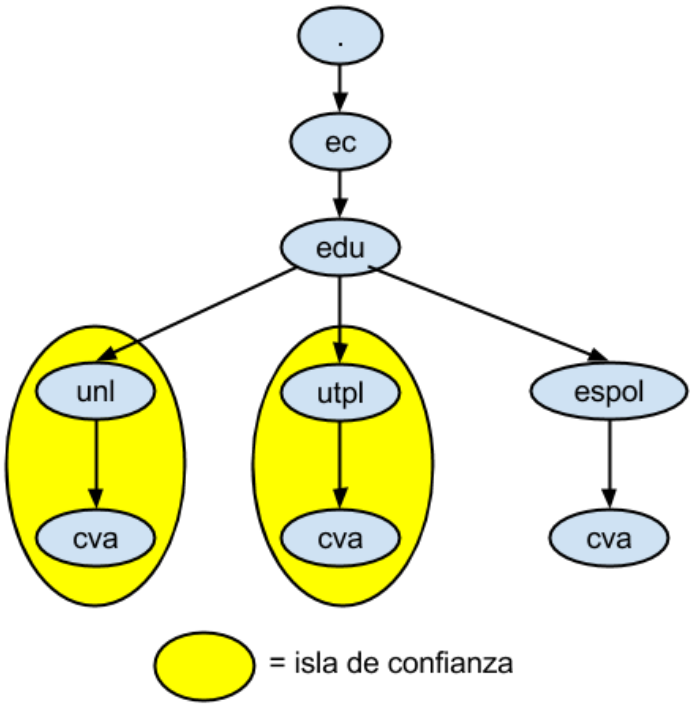

Figura 2. Islas de confianza.

Para crear una “isla” de confianza se firmó las zonas y se distribuyó los “puntos de entrada seguros” al servidor de nombres recursivo [17]. Después de la creación de los pares de claves utilizados para la firma y validación se firmó los datos de la zona para las propias instituciones y se configuró los promotores de almacenamiento en caché en la red de la organización para validar los datos con la clave pública de la institución.

Como puede pasar algún tiempo antes de que esas zonas se firmen se establecen "archipiélagos" de confianza, donde se almacenan las “anclas” de confianza para un grupo de islas de confianza como se ilustra en la figura 3.

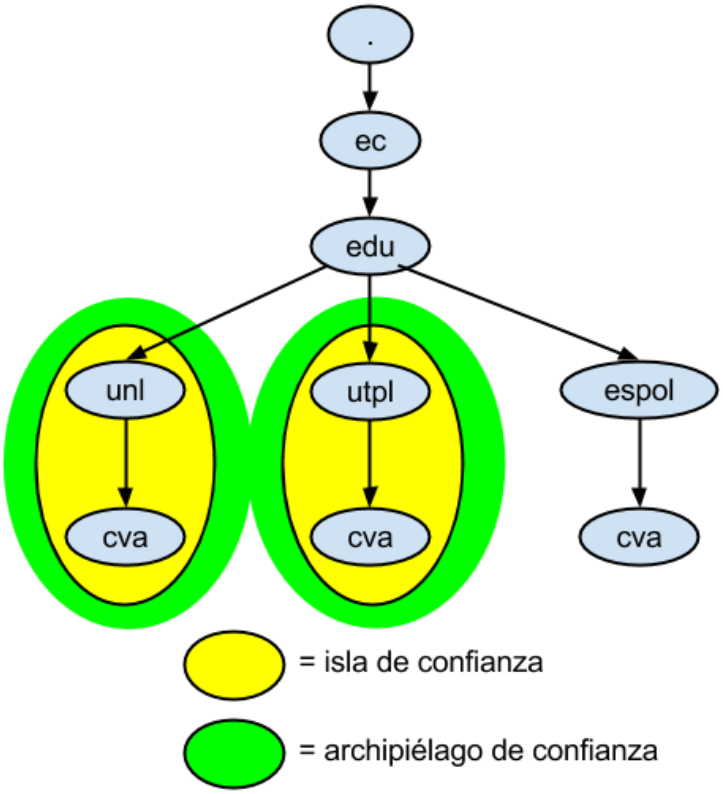

Figura 3. Archipiélago de confianza.

Donde las islas de confianza de la Universidad Nacional de Loja y Universidad Técnica Particular de Loja forman el archipiélago de confianza que permite que los resolvedores puedan confiar en estos dominios.

2.5. Registros de Recursos (RR) DNSSEC.

Las Extensiones de Seguridad DNS (DNSSEC) introducen cuatro nuevos tipos de registros de recursos DNS: Clave Pública DNS (DNSKEY), Registro del Recurso Firma (RRSIG), Siguiente Seguro (NSEC) y Delegación Firmante (DS) [18].

2.5.1. DNSKEY.

DNSSEC utiliza criptografía de clave pública para firmar y autenticar conjuntos de registros de recursos DNS (RRsets). Las claves públicas se almacenan en registros de recursos DNSKEY y se utilizan en el proceso de autenticación de DNSSEC descrito en [19]: Una zona firma sus RRsets autorizados mediante el uso de una clave privada y almacena la clave pública correspondiente en un RR DNSKEY. Un resolvedor puede entonces utilizar la clave pública para validar las firmas que cubren los RRsets en la zona, y por lo tanto para autenticarlos.

El RR DNSKEY no pretende ser un registro para almacenar claves públicas arbitrarias y NO DEBE ser usado para almacenar los certificados o claves públicas que no se refieran directamente a la infraestructura DNS [18].

2.5.1.1. Ejemplo de un RR DNSKEY.

El siguiente RR DNSKEY almacena una clave de zona DNS para unl.edu.ec.:

```
unl.edu.ec. 604800 IN DNSKEY 256 3 5 (
                    AwEAAcgYN103j/QcJhzOJw8DEfJ86weSxvvl8Cnrgyw4
                    SOVBw8S1/BWf7eDKkWzChTfeYPcMoCfsnUA4WPabJ7kE
                    mhd6PJ25Ig9B3BcPH4aVgDjolItzTbkBKIAwkDQFfYW8
                    q+I1nMV98sgUz3T5jnizKhhKvWP6dxGct1C9keW5sgqJ)
```

Los primeros cuatro campos de texto especifican el nombre del propietario, TTL, clase y tipo del RR (DNSKEY). El valor 256 indica el bit de la clave de la zona. El valor 3 es el valor fijo del Protocolo. El valor 5 indica la clave pública del algoritmo. El texto restante es una codificación en Base64 de la clave pública [18].

2.5.2. RRSIG.

DNSSEC utiliza criptografía de clave pública para firmar y autenticar conjuntos de registros de recursos DNS (RRsets). Las firmas digitales se almacenan en registros de recursos RRSIG y se utilizan en el proceso de autenticación de DNSSEC descrito en [19]: Un validador puede utilizar estos RRs RRSIG para autenticar RRsets de la zona. El RR RRSIG sólo se DEBE utilizar para transportar material de verificación (firma digital) que se utiliza para asegurar las operaciones del DNS.

Un registro RRSIG contiene la firma de un RRset con un determinado nombre, clase y tipo. El RR RRSIG especifica un intervalo de validez de la firma y utiliza el algoritmo, el nombre del firmante, y la llave de la etiqueta para identificar el RR DNSKEY que contiene la clave pública que un validador puede usar para verificar la firma.

Debido a que cada autoridad RRset en una zona debe ser protegida por una firma digital, los RRs RRSIG deben estar presentes para los nombres que contienen un RR CNAME. Esto se trata de un cambio en la especificación tradicional del DNS [20], que establecía que si un CNAME está presente para un nombre, este es el único tipo permitido en ese nombre. Un RRSIG y NSEC (véase la sección 2.5.3) DEBEN existir

para el mismo nombre como un registro de recursos CNAME en una zona firmada [18].

2.5.2.1. Ejemplo de un RR RRSIG.

El siguiente RR RRSIG almacena la firma para un RRset de cva.unl.edu.ec.:

```
cva.unl.edu.ec. 604800 IN RRSIG A 5 4 604800 20140115184625 (
                          20131216184625 38691 cva.unl.edu.ec.
                          SLEtSCjuyKA6oVvfxtSYKMio5RmkfE6sxf8iJq7JqY/3
                          T6kmdSDrFFEUyKzy4D1BLT1eSI9mAmkdicBZoUgenYDX
                          nC2/eT6f3e9n2Ge6XoUk3DS3fSBYbc39GCK807tOQTg4
                          iXYGKWi4gGPj4NOUj3DnFz9h6FykPrXZQcyLHDc=)
```

Los primeros cuatro campos especifican el nombre del propietario, TTL, clase y tipo del RR (RRSIG). La "A" representa el tipo de terreno cubierto. El valor 5 identifica el algoritmo utilizado (RSA/SHA1) para crear la firma. El valor 4 es el número de etiquetas en el nombre del dueño original. El valor 604800 en el RDATA del RRSIG es el TTL original para la cubierta de un RRset. 20140115184625 y 20131216184625 son el vencimiento y fechas de creación, respectivamente. 38691 es la llave de la etiqueta, y cva.unl.edu.ec. es el nombre del firmante. El texto restante es una codificación en Base64 de la firma [18].

2.5.3. NSEC.

El registro de recursos NSEC enumera dos cosas distintas: el nombre próximo del propietario (en el orden canónico de la zona) que contiene datos de autoridad o un punto de delegación RRset NS, y el conjunto de tipos de RR presentes en el nombre del propietario del RR NSEC [21]. El conjunto completo de RR NSEC en una zona indica que existen RRsets autorizados en una zona y también forman una cadena de nombres de propietario autorizada en la zona. Esta información se utiliza para proporcionar la negación autenticada de la existencia de datos del DNS, como se describe en [19].

Debido a que cada autoridad de nombres en una zona debe ser parte de la cadena NSEC, los RRs NSEC deben estar presentes para los nombres que contienen un RR CNAME. Esto se trata de un cambio en la especificación tradicional del DNS [20], que establecía que si un CNAME está presente para un nombre, este es el único tipo

permitido en ese nombre. Un RRSIG (véase la sección 2.5.2) y NSEC DEBEN existir para el mismo nombre como un registro de recursos CNAME en una zona firmada [18].

2.5.3.1. Ejemplo de un RR NSEC.

El siguiente RR NSEC identifica los RRsets asociados con utpl.edu.ec. e identifica el siguiente nombre de autoridad después utpl.edu.ec.

utpl.edu.ec. 604800 IN NSEC cva.utpl.edu.ec. (
A NS SOA RRSIG NSEC DNSKEY)

Los primeros cuatro campos de texto especifican el nombre, TTL, clase y tipo del RR (NSEC). La entrada de cva.utpl.edu.ec. es el siguiente nombre de autoridad después de utpl.edu.ec. en orden canónico. La A, NS, SOA, RRSIG, NSEC y DNSKEY mnemotécnicos indican que hay A, NS, SOA, RRSIG, NSEC y DNSKEY RRsets asociados con el nombre utpl.edu.ec. [18].

2.5.4. DS.

El registro de recursos DS se refiere a un RR DNSKEY y se utiliza en el proceso de autenticación de DNSKEY del DNS. Un RR DS hace referencia a un RR DNSKEY mediante el almacenamiento de la etiqueta de la llave, el número de algoritmo, y un resumen del RR DNSKEY. Tenga en cuenta que mientras que el resumen debe ser suficiente para identificar la clave pública, el almacenamiento de la etiqueta de la llave y el algoritmo de clave ayuda a que el proceso de identificación sea más eficiente. Mediante la autenticación del registro DS, una resolución puede autenticar el RR DNSKEY a la que apunta el registro DS. El proceso de autenticación de clave se describe en [19].

El RR DS y su correspondiente RR DNSKEY tienen el mismo nombre del propietario, pero se almacenan en diferentes ubicaciones. El RR DS aparece sólo en el lado superior (los padres) de una delegación, y es autoridad de datos en la zona de los padres. Por ejemplo, el RR DS para "example.com" se almacena en la zona de "com" (la zona de los padres) en lugar de en la zona de "example.com" (la zona secundaria). El correspondiente RR DNSKEY se almacena en la zona de "example.com" (la zona secundaria). Esto simplifica la gestión de las zonas DNS y la zona de la firma, pero

introduce requisitos especiales de procesamiento de respuesta para el RR DS, los cuales se describen en [19] [18].

2.5.4.1. Ejemplo de un RR DS.

El siguiente ejemplo muestra un RR DNSKEY y su correspondiente RR DS.

```
dskey.example.com. 86400 IN DNSKEY 256 3 5 (
                                AQOeiiR0GOMYkDshWoSKz9Xz
                                fwJr1AYtsmx3TGkJaNXVbfi/
                                2pHm822aJ5iI9BMzNXxeYCmZ
                                DRD99WYwYqUSdjMmmAphXdvx
                                egXd/M5+X7OrzKBaMbCVdFLU
                                Uh6DhweJBjEVv5f2wwjM9Xzc
                                nOf+EPbtG9DMBmADjFDc2w/r
                                ljwvFw==
                                ) ; key id = 60485
dskey.example.com. 86400 IN DS 60485 5 1 (
                                2BB183AF5F22588179A53B0A
                                98631FAD1A292118 )
```

Los primeros cuatro campos de texto especifican el nombre, TTL, clase y tipo del RR (DS). El valor 60485 es la etiqueta de la llave para el correspondiente "dskey.example.com." El RR DNSKEY, y el valor 5 denotan el algoritmo utilizado por este "dskey.example.com." en el RR DNSKEY. El valor 1 es el algoritmo usado para construir el resumen, y el resto del texto RDATA es el resumen en hexadecimal [18].

e. Materiales y Métodos

El desarrollo del presente trabajo implicó la realización de una serie de pasos sucesivos y ordenados llegando a la aplicación de métodos respectivos siendo esta la base principal para establecer el tema a investigar, determinar objetivos, estructurar el marco teórico, plantear soluciones al problema trazado, además de poner en práctica los conocimientos obtenidos durante la formación académica, para lo cual se hizo uso de métodos y técnicas de investigación científica, así como una metodología de resolución de problemas descritos a continuación.

1. Métodos.

1.1. Método deductivo.

Con este método se determinó el tema a investigar en base a todo lo referente teórico, puesto que dicho método parte de un marco general de referencia que en este caso son los conocimientos generales e información recopilada, para determinar un caso en particular como lo es el estudio de las Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicado en comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

1.2. Método inductivo.

Mediante este método, que es el razonamiento que partiendo de casos particulares, se eleva a conocimientos generales; se lo utilizó para estructurar el marco teórico, buscando información relacionada con el tema en material bibliográfico.

1.3. Método científico.

Con este método se obtuvo, analizó y sintetizó los conceptos teóricos de la temática y a su vez la creación del estado del arte que da fundamento teórico al proceso investigativo.

2. Técnicas.

2.1. Entrevista.

Esta técnica se la aplicó a los encargados del servicio DNS de la Universidad Nacional de Loja y Universidad Técnica Particular de Loja, para obtener información referente a la administración del servicio DNS, con lo que se examinó las principales

vulnerabilidades del mismo; que sirvieron para determinar la situación problemática y el problema del trabajo, de los cuales se partió para ejecutar la mejor solución posible.

3. Metodología.

El desarrollo del actual trabajo involucró el abordaje de dos tipos de investigaciones cualitativas, las mismas que se exponen a continuación, con el propósito de examinar y detallar la realidad de la tecnología DNSSEC; asimismo se puso en práctica una metodología de resolución de problemas [22] que permitió develar qué hacer con el problema planteado, de forma tal de asegurar calidad y realización.

3.1. Investigación exploratoria.

Mediante esta investigación se indagó sobre el estado del arte del mecanismo DNSSEC, lo cual permitió familiarizarse y obtener una visión correcta del mismo para determinar los procedimientos a efectuarse en su implementación.

3.2. Investigación diagnóstica.

A través de esta investigación se realizó un análisis de las causas que originaron el problema de investigación planteado, con lo que se adquirió la información pertinente para su resolución.

3.3. Metodología de resolución de problemas.

Esta metodología se centra en tres objetivos: la comprensión del problema, la creación de una estrategia de resolución o intervención y el logro del mejoramiento o la solución al problema. Para ello, la metodología se organiza en siete etapas descritas a continuación:

3.3.1. Etapa 1: Identificar el problema.

En esta etapa se visualizó el problema de investigación (ver Anexo 30 sección B subsección 2), el mismo que se refiere a la comprobación de la seguridad en el protocolo DNS en cuanto a la validación de la autenticidad y la integridad de los datos transferidos en las comunidades virtuales de aprendizaje de las instituciones de educación superior.

3.3.2. Etapa 2: Explicar el problema.

Durante esta etapa se indagó el estado del arte del Sistema de Nombres de Dominio de las instituciones de educación superior (ver sección Resultados subsección Fase 1), partiendo de la recogida de información tanto a nivel internacional, nacional y local, de forma específica en la Universidad Nacional de Loja y Universidad Técnica Particular de Loja; con el propósito de determinar las principales vulnerabilidades del DNS, lo que permitió avanzar en un consenso más firme y extendido sobre la naturaleza del problema.

3.3.3. Etapa 3: Idear las estrategias alternativas de intervención.

En tanto esta etapa se propuso las soluciones en cuanto a la manera de proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje y la forma adecuada de asegurar la comunicación entre servidores de las instituciones de educación superior (ver sección Resultados subsección Fase 2 y Fase 3), con lo cual se obtuvo las opciones factibles de aplicación.

3.3.4. Etapa 4: Decidir la estrategia.

Partiendo de las estrategias abordadas en la etapa anterior, esta fase afirmó la mejor solución que permitió analizar el estado del arte del Sistema de Nombres de Dominio de las universidades (ver sección Resultados subsección Fase 1), proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje (ver sección Resultados subsección Fase 2), y asegurar la comunicación entre servidores de las instituciones de educación superior (ver sección Resultados subsección Fase 3); con lo que se logró aportar seguridad en la autenticación y procedencia de datos en las comunidades virtuales de aprendizaje transferidos por el protocolo DNS.

3.3.5. Etapa 5: Diseñar la intervención.

En esta etapa se estableció las acciones, plazos y recursos, para la realización de una serie de actividades y tareas concernientes al análisis del estado del arte del DNS, la protección de los datos DNS de las comunidades virtuales de aprendizaje y el aseguramiento de la comunicación entre servidores de las universidades.

3.3.6. Etapa 6: Desarrollar la intervención.

Durante esta fase se realizó la revisión del estado del arte del sistema DNS (ver sección Resultados subsección Fase 1) en las universidades y las configuraciones y validaciones necesarias para la protección de los datos DNS (ver sección Resultados subsección Fase 2) que se transfieren en las comunidades virtuales de aprendizaje y el aseguramiento de la comunicación entre servidores (ver sección Resultados subsección Fase 3) de las instituciones.

3.3.7. Etapa 7: Evaluar los logros.

Finalmente en esta etapa se analizó los resultados obtenidos durante el proceso de implementación, con lo que se determinó la eficiencia de los beneficios aportados por la tecnología DNSSEC en las comunidades virtuales de aprendizaje de la universidad, que se redactan en el apartado de discusión.

f. Resultados

En este apartado se plasma el estudio efectuado sobre la tecnología DNSSEC, el mismo que se llevó a cabo de acuerdo a los objetivos planteados estableciendo una fase de desarrollo por cada uno de ellos.

En la fase 1 se efectúa un análisis del estado del arte del DNS de las instituciones de educación superior a nivel internacional, nacional y local como medio para determinar los requerimientos de implementación de DNSSEC.

En la fase 2 se ejecuta la protección de los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de educación superior, desarrollando configuraciones para el funcionamiento de DNSSEC en un ambiente virtualizado.

En la fase 3 se realiza el aseguramiento de la comunicación entre servidores de las instituciones de educación superior, generando secretos compartidos de transacciones firmadas para la protección de la transferencia de zona.

Fase 1: Analizar el estado del arte del Sistema de Nombres de Dominio de las instituciones de Educación Superior, para determinar los requerimientos de implementación de DNSSEC.

Durante esta fase se realizó la recogida de información a nivel internacional, nacional y local de instituciones de educación superior que hayan implementado DNSSEC; en el ámbito internacional se indagó sobre cualquier institución fuera de Ecuador que haya efectuado el despliegue de esta tecnología, en el ambiente nacional se investigó sobre la implementación de DNSSEC en el proveedor de servicios de internet TELCONET S.A., así como en las instituciones existentes en el país; y a nivel local se desarrolló una entrevista estructurada a los encargados del servicio DNS de la Universidad Nacional de Loja y la Universidad Técnica Particular de Loja para efectuar un análisis de la administración del servicio DNS y examinar las principales vulnerabilidades del mismo.

1. Búsqueda bibliográfica sobre casos de éxito de DNSSEC en instituciones de Educación Superior.

1.1. Recogida de información a nivel internacional.

Las instituciones de educación superior de todo el mundo han sido los principales defensores de las tecnologías de Internet. La gTLD del dominio .EDU se encuentra firmada, sin embargo, una reciente encuesta de nombres .EDU muestra que sólo el uno por ciento están firmados.

Las universidades representan un microcosmos de la Internet como un todo, repleto de ataques cibernéticos, algunos de los cuales podrían ser impedidos por una combinación de firma y validación DNSSEC. En la parte académica, DNSSEC se suma a la autenticidad del producto del trabajo académico.

De acuerdo a la iniciativa DNSSEC Deployment [1], entre las principales instituciones de educación superior que han implementado DNSSEC, se encuentran:

- Colegio Técnico Acadiana (acadiana.edu)
- Colegio Baker (baker.edu)
- Universidad Berkeley de California (berkeley.edu)
- Universidad Bucknell (bucknell.edu)

- Colegio de Comunidad Técnica Central de Louisiana (cltc.edu)
- Universidad Carnegie Mellon (carnegiemellon.edu, cmu.edu)
- Universidad de Colorado Mesa (coloradomesa.edu, mesa.edu)
- Universidad Cal Poly Pomona (csupomona.edu)
- Universidad China de Hong Kong (cuhk.edu)
- Universidad DeSales (desales.edu)
- Universidad Estatal de Fort Hays (fhsu.edu)
- Colegio Técnico Flint Hills (fhtc.edu)
- Colegio Técnico Gateway (gtc.edu)
- Academia Nacional de Diseño de Karlsruhe (hfg.edu)
- Colegio Georgia Highlands (highlands.edu)
- Universidad de Indiana (indiana.edu, iu.edu)
- Colegio Técnico de Indiana (indianatech.edu)
- Universidad de Indiana Bloomington (iub.edu)
- Universidad de Indiana - Universidad de Purdue Indianápolis (iupui.edu)
- Laboratorio de Física Aplicada de la Universidad Johns Hopkins (jhuapl.edu)
- Instituto Kestrel (kestrel.edu)
- Comunidad de Luisiana y Sistema de Colegios Técnicos (lctcs.edu)
- Universidad Estatal de Luisiana (lsu.edu)
- Colegio Técnico de Luisiana (ltc.edu)
- Universidad Estatal de Westfield (ma.edu)
- Universidad de Millikin (millikin.edu)
- Comunidad Estatal de Minnesota y Colegio Técnico (minnesota.edu)
- Universidad de Monmouth (monmouth.edu)
- Universidad de Missouri de Ciencia y Tecnología (mst.edu)
- Universidad del Norte de Arizona (nau.edu)
- Colegio de Comunidad Técnica de Northshore (northshorecollege.edu)
- Colegio Técnico del Noroeste de Louisiana (nwltc.edu)
- Universidad de Oxford (oxford-university.edu)
- Universidad del Pacífico (pacificu.edu)
- Universidad de Pensilvania (penn.edu, upenn.edu)
- Centro de Supercomputación de Pittsburgh (psc.edu)
- Colegio Comunitario de Richland (richland.edu)
- Universidad Rockefeller (rockefeller.edu)

- Colegio Técnico Sur Central de Luisiana (scl.edu)
- Escuela de Minas y Tecnología de Dakota del Sur (sdsmt.edu)
- Universidad Adventista del Sur (southern.edu)
- Universidad del Sur de Utah (suu.edu)
- Universidad de Tilburg (tilburguniversity.edu)
- Instituto Tata de Ciencias Sociales (tiss.edu)
- Universidad Estatal de Truman (truman.edu)
- Universidad de Arkansas en Little Rock (ualr.edu)
- Corporación Universitaria para el Desarrollo de Internet Avanzado (ucaid.edu)
- Universidad Riverside de California (ucr.edu)
- Universidad de Iowa (uiowa.edu)
- Universidad del Condado de Maryland Baltimore (umbc.edu)
- Universidad de Stuttgart (uni-stuttgart.edu)
- Universidad Pompeu Fabra (upf.edu)
- Universidad de Valencia (valencia.edu)
- Colegio Washington & Jefferson (washjeff.edu)
- Universidad Estatal de Weber (weber.edu)

En Portugal, conforme a la asociación DNSSEC .PT [23] algunas instituciones de educación superior han firmado sus dominios con DNSSEC, mejorando así la seguridad de sus sitios mediante la aplicación de las mejores prácticas. Estas instituciones son:

- Instituto Politécnico de Bragança (www.ipb.pt)
- Instituto Politécnico de Cávado y Ave (www.ipca.pt)
- Instituto de Estudios Superiores de Fafe (www.iesfafe.pt)
- Instituto Tecnológico y Nuclear (www.itn.pt)
- Universidad Abierta (www.uaberta.pt)
- Universidad Autónoma de Lisboa (www.universidade-autonoma.pt)
- Universidad del Atlántico (www.uatlantica.pt)
- Universidad de Évora (www.uevora.pt)
- Universidad de Madeira (www.uma.pt)
- Universidad de Lisboa (www.ul.pt)

1.1.1. Caso de éxito: Universidad de Pensilvania.

La división de los Sistemas de Información y Computación (ISC) de la Universidad de Pensilvania ha anunciado su implementación exitosa en toda la institución de la tecnología de Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC). La zona DNS upenn.edu se firmó con DNSSEC a principios de agosto del 2009. Penn es parte de Internet2 y Educause, una comunidad de los primeros en adoptar la tecnología DNSSEC y es la primera universidad de los EE.UU. en implementarlo en toda la institución.

DNSSEC aborda muchas vulnerabilidades de seguridad en el Sistema de Nombres de Dominio (DNS), la parte de Internet que traduce los nombres descriptivos, como www.upenn.edu, en numéricos de direcciones de red necesarios para proporcionar información en Internet. Estas vulnerabilidades han adquirido mayor importancia en los últimos años dado que partidos maliciosos han encontrado cada vez más formas de explotar las vulnerabilidades, utilizándose para distribuir información de DNS falsificada, redirigiendo a los usuarios de Internet con el propósito de fraude y otras actividades criminales. DNSSEC ofrece la posibilidad de incorporar la firma digital de los nombres en el DNS, los cuales pueden ser usados para verificar su autenticidad, y así frustrar estos ataques. Además, DNSSEC permite nuevas capacidades de las aplicaciones de red que les permite publicar de forma segura una variedad de material de claves de cifrado en el DNS.

Algunas universidades de Estados Unidos han implementado DNSSEC en algunas partes de su infraestructura (bancos de pruebas, los departamentos de investigación, u otras subdivisiones). Pero Penn se cree que es el primero que ha completado el despliegue de DNSSEC en un campus de gran escala. De hecho, la experiencia de Penn con DNSSEC se remonta mucho más allá. En 2006, también desplegó DNSSEC en MAGPI (Mid-Atlantic GigaPOP de Internet2), una red regional de investigación y educación que funciona como parte del proyecto Internet2, y que sirve para la mayoría de las universidades y colegios en el este de Pensilvania, Nueva Jersey, y regiones de Delaware.

Además, Penn está trabajando con Educause sobre sus planes para implementar DNSSEC en el nivel superior EDU del dominio DNS, que Educause y Verisign operan bajo un acuerdo de cooperación con el Departamento de Comercio de EE.UU. Penn es uno de los primeros participantes en el banco de pruebas de DNSSEC EDU, ya en

curso. Cuando se termine el proyecto, las instituciones educativas de todo el país tendrán la posibilidad de publicar una firma digital para sus nombres de dominio EDU.

Shumon Huque, un Director Técnico de TI en Redes y Telecomunicaciones de la organización del ISC, está liderando los esfuerzos de implementación de DNSSEC de Penn y su participación en el banco de pruebas de Educause. "La educación superior puede tener un papel de liderazgo en la obtención de los DNS", dijo Huque. "Si algunas universidades de la comunidad de redes avanzadas pueden desplegar plenamente DNSSEC y compartir experiencias, podemos hacer un amplio despliegue más sencillo para la comunidad en general".

En cualquier momento/lugar el acceso a Internet es fundamental para la capacidad de la educación superior para realizar negocios.

"La Universidad de Pensilvania y el ISC nos sentimos honrados de tener la oportunidad de contribuir a la mejora de la seguridad en Internet. Esperamos que el trabajo que nosotros y nuestros colegas en la Universidad Estatal de Luisiana, UC Berkeley, Cambridge, y otros están haciendo a este proyecto producir nuevos conocimientos valiosos que en última instancia será útil para otras organizaciones de educación de todo el mundo y que también se traducen en información útil que pueda ser utilizada por las empresas y la industria, lo que hace que Internet sea un lugar mejor y más seguro para todos nosotros", dijo el vicepresidente de Sistemas de Información y Computación de Penn, Robin Beck. "Tener un seguro de Internet es absolutamente fundamental para la comunidad Penn, que depende de la tecnología basada en la web para una gran variedad de funciones y servicios esenciales, entre ellos nuestro sistema para Admisiones de Pregrado, Servicios Financieros Estudiantiles, Registro de Cursos, y la presentación y adjudicación de becas de investigación, por nombrar sólo unos pocos" [24].

1.1.2. Caso de éxito: Universidad Pompeu Fabra.

La Universidad Pompeu Fabra disponía de una arquitectura DNS obsoleta, tanto a nivel de Hardware como de Software. Se procedió a valorar la actualización de esta arquitectura y la posterior implementación de DNSSEC cuando Educause publicó la intención de firmar el dominio .edu a principios de agosto del 2010.

En un estudio realizado por el grupo de Computer Science de la Universidad de los Angeles (UCLA) la implantación de DNSSEC ha visto un aumento considerable este último año, que suponemos que ha sido a raíz de las firmas de los dominios org y edu.

El proceso de actualización de la arquitectura se realiza en dos fases como se muestra en la figura 4, una primera fase en la que se actualizó el hardware, los servidores, y una segunda fase en la que se actualizó el software, en esta fase se aprovechó para implementar el sistema DNSSEC en los dominios upf.edu y upf.cat.

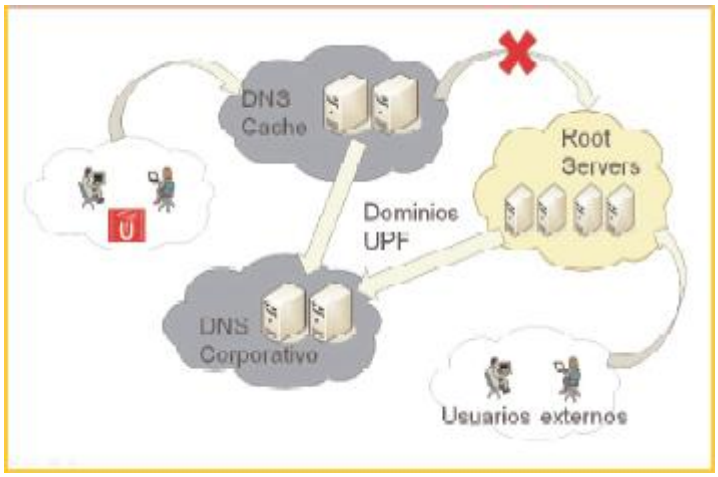

Figura 4. Estado actual [25].

Se optó por servidores virtuales, creando dos servidores cachés, dónde se concentran todas las peticiones de los usuarios y dos servidores autoritativos, donde reside la información principal de los dominios gestionados desde la Universidad Pompeu Fabra.

Para conseguir una mayor seguridad e integridad de los sistemas, los servidores autoritativos se configuraron para que no pudieran hacer consultas DNS recursivas, es decir, si alguien hace una consulta a estos servidores de un dominio que no sea de la Universidad no dará ninguna respuesta.

Una vez se implantó la nueva arquitectura, se implementó DNSSEC para los dominios upf.edu y upf.cat. Se deben generar dos claves, una KSK (Key-signing key y una ZSK (Zone signing key) de la siguiente manera:

- dnssec-keygen –r/dev/random –f KSK –a RSASHA1 –b 2048 –n ZONE upf.edu
- dnssec-keygen –r/dev/random –a RSASHA1 –b 2048 –n ZONE upf.edu

Una vez tenemos las claves, se añaden al final del documento del fichero de la zona, de esta manera se propaga la clave a través de los root servers. Es necesario esperar a que se propague la información, este tiempo es el TTL configurado para cada zona.

Se firma la zona con ambas claves, esto genera un fichero con extensión signed

- dnssec-signzone -o upf.edu –k Kupf.edu.actual.key upf.edu.hosts Kupf.edu.actual.key

Cambiamos la configuración del servidor indicando que el fichero con la información de la zona es el fichero con extensión signed.

Se añaden los datos en el registrador de dominio y se verifica que resuelva correctamente.

En el caso de realizar una actualización de las claves, se añaden las nuevas claves en el fichero, además de las antiguas, y se espera a que se propague la información. Una vez haya pasado el TTL de la zona, se firma con la nueva clave y se hace la revocación de la antigua.

Al actualizar las claves, hay que tener en cuenta que si nos equivocamos a la hora de publicar las claves y firmamos la zona con otra clave que no sea la que se ha publicado, la resolución de nombres dejará de funcionar al no poder validarla. Es importante habilitar que los paquetes DNS puedan tener un tamaño mayor a 512 bytes en los equipos de la red, sobre todo en los Firewalls.

Con el plugin DNSSEC Validator instalado en Mozilla (ver figura 5) se puede comprobar que URLs están securizadas mediante DNSSEC. También se puede verificar con el comando dig o en diferentes web como dnscheck.iis.se [25].

Figura 5. Resultado [25].

1.2. Recogida de información a nivel nacional.

Actualmente en el Ecuador ninguna institución de educación superior ha realizado el firmado de las zonas DNS con DNSSEC, con lo cual podrían enfrentarse a los riesgos derivados del DNS, debido a que las instituciones de educación superior almacenan enormes cantidades de información sensible y se mantienen activos en línea en las comunidades virtuales de aprendizaje cuyo acceso debe ser restringido efectivamente. Los ataques DNS resultan en contraseñas robadas, e-mail alterado, la exposición al malware, y otros problemas.

Por lo que se debería considerar importante la implantación de esta tecnología dado que los usuarios tienden a confiar en determinados ámbitos, como el dominio .edu, más que otros, las expectativas para la fiabilidad de los sitios web de la universidad son altas. En la medida en que las instituciones de educación superior dependen de su reputación, DNSSEC es una vía para evitar algunos de los tipos de incidentes que pueden dañar el prestigio de una institución de educación superior [5].

1.2.1. Recogida de información sobre TELCONET S.A.

La empresa privada TELCONET, operadora de comunicaciones corporativas y proveedora de servicios de internet en Ecuador, según los reportes de los laboratorios

del Registro Regional de Internet para la región de Asia Pacífico (APNIC), no provee resolutores de validación DNSSEC [26]; es decir que no ha habilitado DNSSEC en sus servidores de nombres recursivos por lo que no permite que sus usuarios puedan verificar la autenticidad de las respuestas que otorga la zona.

Debido a que la Red Académica Avanzada del Ecuador (Red CEDIA) opera sobre la Red Nacional NGN de TELCONET, uniendo las principales universidades, escuelas politécnicas, organizaciones de ciencia y tecnología del país; es de fundamental importancia realizar la implementación de DNSSEC, ya que al implementarlo puede proteger mejor a sus clientes, reforzar su reputación como líder en la protección de clientes y la seguridad de internet, además de diferenciarse de sus competidores. También puede ser capaz de influir en el desarrollo de productos y servicios (y otras iniciativas de la industria) que respalden y beneficien a su empresa.

Si agrega esta capa importante de forma proactiva, TELCONET puede:

- Ayudar a reducir el riesgo de que sus clientes sean víctimas de crímenes informáticos.
- Contribuir a proteger y desarrollar su propia marca y reputación.
- Mantener la lealtad y confianza de sus clientes.
- Ofrecer una experiencia de internet más segura como parte de la propuesta de valor que realiza a sus clientes.
- Atraer y retener clientes que dan prioridad a la seguridad.
- Proteger sus negocios principales a través de un aumento de la confianza en internet.
- Ejercer su liderazgo e influencia para moldear el futuro de DNSSEC [27].

1.3. Recogida de información a nivel local.

1.3.1. Recogida de información en la Universidad Nacional de Loja.

1.3.1.1. Entrevistar al encargado del servidor DNS.

Para obtener información detallada acerca del servidor DNS se ha procedido a realizar una entrevista estructurada (Ver Anexo 2) al jefe de la Unidad de Redes de la Unidad de Telecomunicaciones e Información (UTI), el mismo que dio a conocer la manera como se efectúa la administración del servicio y aseguró que no se ha realizado la implementación de DNSSEC en la universidad.

Con lo cual supo expresar que resultaría conveniente implementar DNSSEC, ya que los usuarios del dominio de la universidad que se encuentran fuera de la ciudad como en Zapotepamba y la Quinta Experimental “El Padmi” podrían intercambiar información confidencial teniendo seguridad de que es la real; además en el caso de la Modalidad de Estudios a Distancia (MED) se tendrá la confianza de la información en cuanto a pagos bancarios que deben realizar.

1.3.1.2. Analizar la administración del servicio DNS.

La administración del servicio DNS se realiza conforme a las políticas existentes en la Unidad de Telecomunicaciones e Información, de acuerdo a ello el administrador del servidor es la única persona autorizada para acceder al mismo, el cual abarca un alto número de usuarios que corresponden a todos aquellos que hacen uso del servicio; por lo cual se considera una situación grave si el servicio llegase a fallar, debido a que no se tendría acceso a ciertos dominios en la red, las direcciones de cierto dominio se podrían reconocer como no válidas y con ello no se podrían realizar las actividades diarias, provocando pérdidas y molestias en los usuarios.

El servicio DNS interactúa con otros servicios existentes en la universidad, como es el caso de los servicios Web, Webmail y EVA, los cuales se encuentran a disposición de todos los usuarios; para lo que el servidor cuenta con algunos tipos de seguridad lógica como son las iptables, SSH y el firewall.

En la actualidad no se realiza el monitoreo del tráfico de red en el servidor DNS, pero se tiene aprobado un trabajo de titulación en el que se plantea la implementación de un sistema para la monitorización del tráfico de red que servirá para el análisis de los paquetes de datos que se transmiten en los diferentes servidores de la universidad.

1.3.1.3. Examinar las principales vulnerabilidades del servicio DNS.

La vulnerabilidad más sobresaliente que se ha detectado en el servidor DNS ha sido un ataque correspondiente a la interceptación de paquetes DNS, ya que en el servidor de correo se han hackeado las cuentas y suplantaron la identidad de algunos usuarios a través de la IP pública de la universidad, lo cual se realizó al servidor de la Área de la Energía el mismo que no se maneja en la UTI.

Este ataque hubiese sido prevenido mediante DNSSEC, debido a que este mecanismo elimina ciertos tipos de ataques DNS para aumentar en gran medida la confianza en las transacciones por parte del negocio y los consumidores, específicamente:

- Envenenamiento de caché DNS
- Hombre en medio de los ataques
- Interceptación de paquetes DNS
- Redirección DNS/Suplantación DNS [28]

Con lo que los ataques pueden causar pérdidas financieras a partes inocentes y pueden resultar en la pérdida de confianza de la universidad con instituciones de educación superior externas al país.

1.3.2. Recogida de información en la Universidad Técnica Particular de Loja.

1.3.2.1. Entrevistar al encargado del servidor DNS.

Para obtener información detallada acerca del servidor DNS se ha procedido a realizar una entrevista estructurada (Ver Anexo 3) al jefe de la Unidad de Redes de la Unidad de Proyectos y Sistemas Informáticos, el mismo que dio a conocer la manera como se efectúa la administración del servicio y aseguró que no se ha realizado la implementación de DNSSEC en la universidad.

Consecuentemente afirmó que sería conveniente realizar la implementación de DNSSEC, porque permitiría dar una solución integral a los ataques concernientes al DNS, y podría formar parte del proyecto de seguridad perimetral que se está llevando a cabo en la universidad.

1.3.2.2. Analizar la administración del servicio DNS.

La administración del servicio DNS se realiza conforme a las políticas existentes en la Unidad de Proyectos y Sistemas Informáticos, de acuerdo a ello el administrador del servidor es la única persona autorizada para acceder al mismo, el cual abarca un alto número de usuarios que corresponden a todos aquellos que hacen uso del servicio; por lo cual se considera una situación grave si el servicio llegase a fallar, porque se produciría un colapso total de los demás servicios de la universidad, como por ejemplo el Entorno Virtual de Aprendizaje (EVA) y el registro académico, aparte de que desde el exterior no se podrían resolver los nombres de Dominio.

El servicio DNS interactúa con otros servicios existentes en la universidad, como es el caso de los servicios Web, Webmail y Sistema de Gestión Académica, los cuales se encuentran a disposición de todos los usuarios; para lo que el servidor cuenta con algunos tipos de seguridad lógica como son SSH y el firewall.

En la actualidad el monitoreo del tráfico de red en el servidor DNS se realiza constantemente por parte de un sistema de monitorización de red que se encarga de buscar problemas causados por servidores sobrecargados y/o caídos, conexiones de red, u otros dispositivos y en caso de existir algún problema, este notifica al administrador de la red; razón por la cual solo se revisa el historial cuando se produce algún incidente.

1.3.2.3. Examinar las principales vulnerabilidades del servicio DNS.

La vulnerabilidad más sobresaliente que se ha detectado en el servidor DNS ha sido un ataque correspondiente a la falsificación de la página de la universidad, el mismo que hubiese sido impedido mediante la implementación de DNSSEC.

Debido a que la universidad permite efectuar pagos en línea, para lo cual se exige más seguridad de la que tienen ahora. Actualmente un usuario (1) va al sitio web de la universidad, (2) se conecta y (3) lleva a cabo algunas acciones. La banca en línea ha recorrido un largo camino para asegurar el paso 2. Están utilizando el cifrado a través de HTTP y el usuario tiene almohadillas de contraseña para asegurar el log en el paso 1. Sin embargo, no está seguro; un usuario nunca puede estar seguro de que él/ella está visitando el sitio correcto. No importa lo bueno que se lleva a cabo el paso 2, si falla el paso 1, el paso 2 no le garantiza una mayor seguridad [29].

Aquí es donde entra en juego DNSSEC. Con DNSSEC el paso 1 se puede asegurar (o por lo menos ahora es posible detectar que el usuario está visitando un sitio equivocado), es así que la universidad obtendrá confianza por parte de los usuarios que realicen sus pagos en línea.

Fase 2: Proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

En esta fase se planteó un laboratorio que simula los servidores DNS de la Universidad Nacional de Loja y la Universidad Técnica Particular de Loja, así como sus comunidades virtuales de aprendizaje, en los que se realizó las configuraciones necesarias para el funcionamiento de DNSSEC, también se simuló el servidor DNS de la Escuela Superior Politécnica del Litoral y su comunidad virtual de aprendizaje pero en estos no se configuró DNSSEC; para lo mencionado se utilizó el servidor DNS de código abierto BIND9 [30] y sus paquetes dependientes, lo cual se efectuó a través de la consola del sistema operativo Debian 7, en la tabla I se especifica la información de los servidores.

TABLA I. INFORMACIÓN DE SERVIDORES.

Servidor		Dirección IP	Nombre	Dominio	Sistema Operativo	Software
Universidad Nacional de Loja	Sitio web	192.168.1.30	unl	unl.edu.ec	Debian 7	Joomla
	Comunidad virtual de aprendizaje	192.168.1.35	cvaunl	cva.unl.edu.ec	Debian 7	Moodle
Universidad Técnica Particular de Loja	Sitio web	192.168.1.40	utpl	utpl.edu.ec	Debian 7	Joomla
	Comunidad virtual de aprendizaje	192.168.1.45	cvautpl	cva.utpl.edu.ec	Debian 7	Moodle
Escuela Superior Politécnica del Litoral	Sitio web	192.168.1.50	espol	espol.edu.ec	Debian 7	Joomla
	Comunidad virtual de aprendizaje	192.168.1.55	cvaespol	cva.espol.edu.ec	Debian 7	Moodle
Resolvedor		192.168.1.60	resolver		Debian 7	
Usuario		192.168.1.xx	usuario		Debian 7	Ettercap

1. Instalación y configuración de los servidores DNS.

Las configuraciones que se establecieron para los servidores de las universidades se muestran de manera gráfica en la figura 6, las mismas que son las que se definen en la TABLA I.

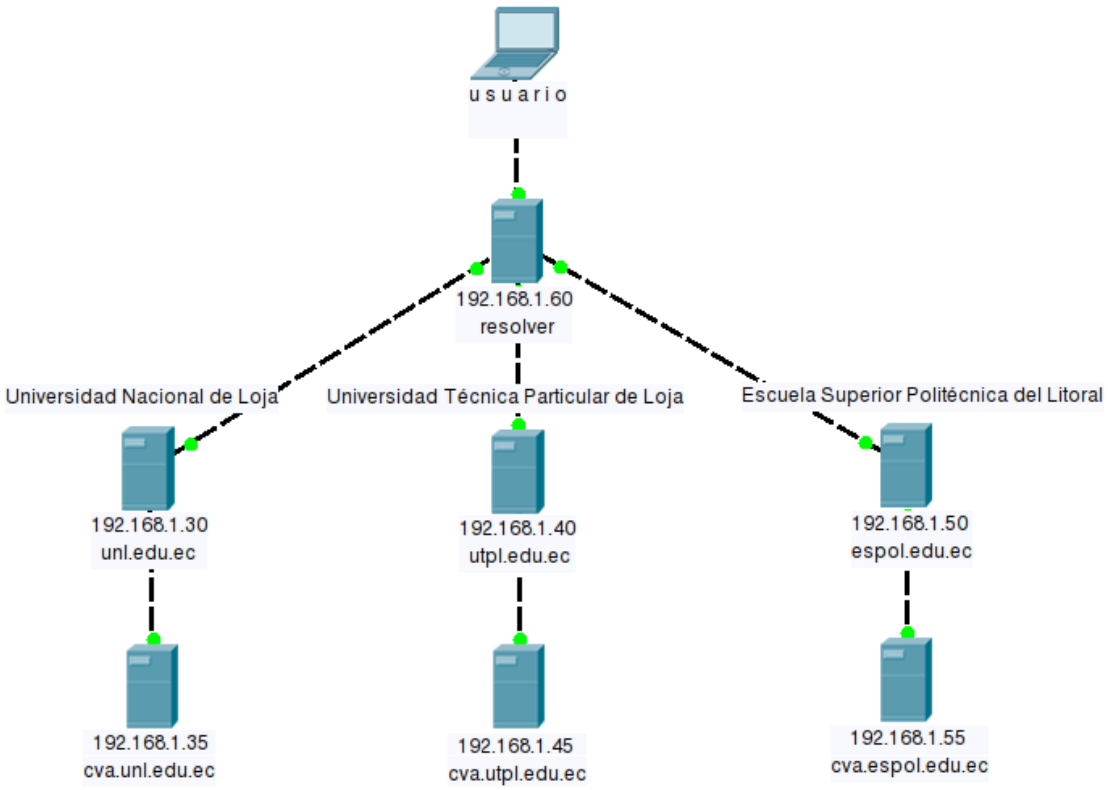

Figura 6. Esquema DNS.

La instalación y configuración de los servidores DNS están basadas en la documentación presentada en [31, 32].

1.1. Servidores Universidad Nacional de Loja.

1.1.1. Sitio web.

Los pasos para instalar y configurar Bind en el servidor del sitio web se especifican en el Anexo 4.

1.1.2. Comunidad virtual de aprendizaje.

Los pasos para instalar y configurar Bind en el servidor de la comunidad virtual de aprendizaje se detallan en el Anexo 5.

1.2. Servidores Universidad Técnica Particular de Loja.

1.2.1. Sitio web.

Los pasos para instalar y configurar Bind en el servidor del sitio web se especifican en el Anexo 6.

1.2.2. Comunidad virtual de aprendizaje.

Los pasos para instalar y configurar Bind en el servidor de la comunidad virtual de aprendizaje se detallan en el Anexo 7.

1.3. Servidores Escuela Superior Politécnica del Litoral.

1.3.1. Sitio web.

Los pasos para instalar y configurar Bind en el servidor del sitio web se especifican en el Anexo 8.

1.3.2. Comunidad virtual de aprendizaje.

Los pasos para instalar y configurar Bind en el servidor de la comunidad virtual de aprendizaje se detallan en el Anexo 9.

2. Aseguramiento de la zona DNS.

Si una zona ha sido firmada y su clave se ha configurado en un servidor de nombres recursivo validador por lo general se refieren a él como una “isla de seguridad”. Al parecer no tiene un padre asegurado y se encuentra solo en el mar de otros dominios sin garantía. Por lo general, la creación de una “isla de seguridad” es el primer paso para convertirse en parte de los DNS seguro. La “isla de seguridad” seguirá siendo “insegura” para los resolvedores que no tienen un ancla de confianza configurada para el dominio [17].

Con lo que el aseguramiento de las zonas DNS de las instituciones de educación superior quedaría como se ilustra en la figura 7.

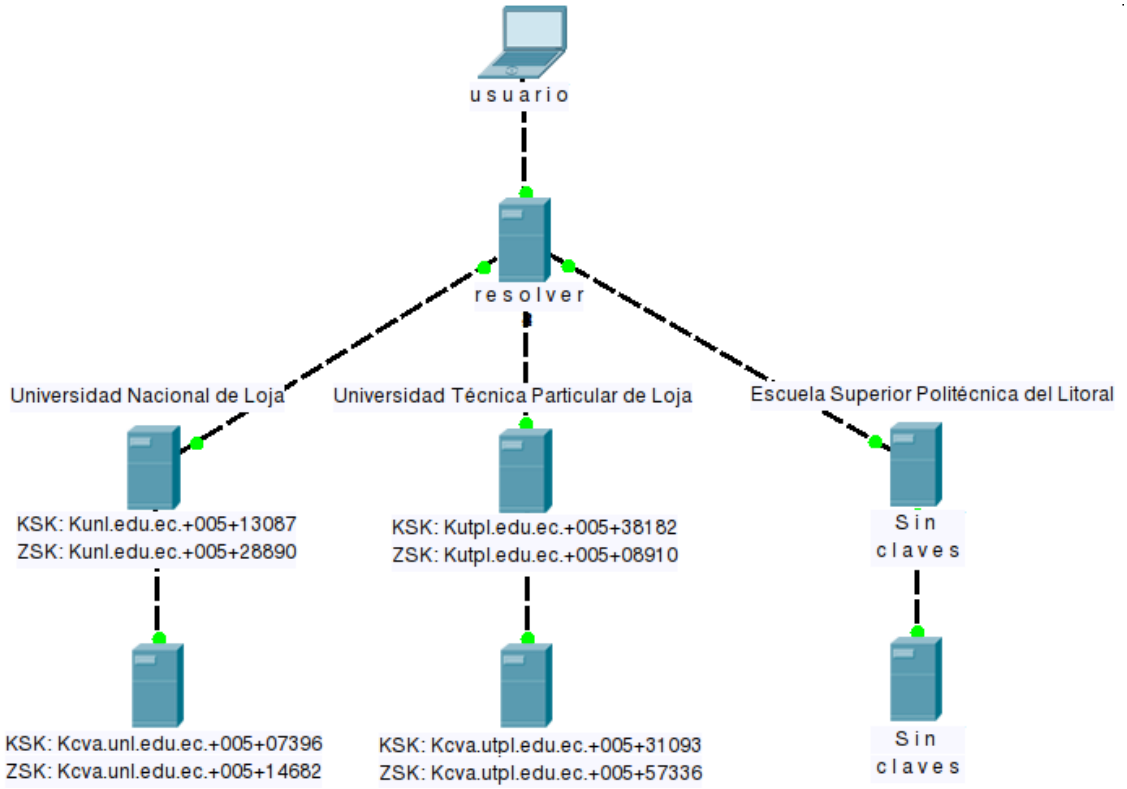

Figura 7. Esquema del aseguramiento de las zonas DNS.

El aseguramiento de las zonas DNS está fundamentado en la documentación indicada en [17, 33].

2.1. Servidores Universidad Nacional de Loja.

2.1.1. Sitio web.

El aseguramiento de la zona DNS del sitio web se especifica en el Anexo 10.

2.1.2. Comunidad virtual de aprendizaje.

El aseguramiento de la zona DNS de la comunidad virtual de aprendizaje se especifica en el Anexo 11.

2.2. Servidores Universidad Técnica Particular de Loja.

2.2.1. Sitio web.

El aseguramiento de la zona DNS del sitio web se especifica en el Anexo 12.

2.2.2. Comunidad virtual de aprendizaje.

El aseguramiento de la zona DNS de la comunidad virtual de aprendizaje se especifica en el Anexo 13.

2.3. Servidores Escuela Superior Politécnica del Litoral.

En los presentes servidores no se configuró el aseguramiento de las zonas DNS (espol.edu.ec, cva.espol.edu.ec), para de esta manera poder identificar las diferencias que existen al momento que un usuario realiza una consulta DNS a un servidor habilitado con DNSSEC (unl.edu.ec, cva.unl.edu.ec, utpl.edu.ec, cva.utpl.edu.ec) y a un servidor inseguro (espol.edu.ec, cva.espol.edu.ec).

3. Configuración de un servidor de nombres recursivo para validar las respuestas.

Se planeó configurar un servidor de nombres recursivo para validar los datos que el mismo recibe. Los usuarios que utilizan este servidor de nombres recursivo como su resolvedor, sólo recibirán los datos que son ya sea seguros y validados o inseguros. Como resultado, la información segura que no supere la validación, no va a encontrar su camino a los usuarios. Tener un servidor de nombres recursivo validador protege a todos aquellos que lo utilizan como un promotor contra la recepción de datos DNS falsificados.

Mediante la configuración de una clave pública para una zona específica, se le dice al promotor de almacenamiento en caché que todos los datos procedentes de esa zona deben estar firmados con la clave privada correspondiente. La zona actúa como un punto de entrada seguro en el árbol DNS y la clave configurada en el servidor de nombres recursivos actúa como el inicio de una cadena de confianza [17].

En el servidor de nombres recursivo se almacenan las claves KSK (claves públicas) de las zonas firmadas con DNSSEC como se muestra en la figura 8, para de esta manera crear anclas de confianza.

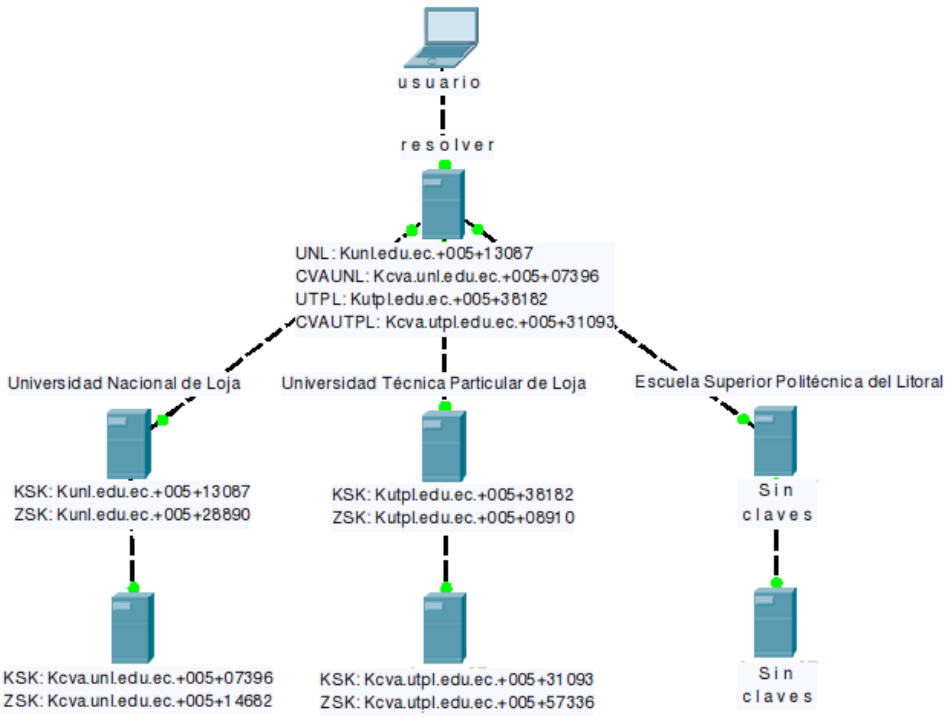

Figura 8. Esquema del servidor de nombres recursivo con claves KSK.

La configuración de un servidor de nombres recursivo para validar las respuestas está estipulada en la documentación demostrada en [17, 31 - 35].

3.1. Configuración del promotor de almacenamiento en caché.

La configuración del promotor de almacenamiento en caché se detalla en el Anexo 14.

4. Delegación de la autoridad de firma.

Se ha cubierto cómo implementar DNSSEC en una sola zona. Ahora se debe construir una cadena de confianza, por lo que una vez que un cliente ha obtenido seguramente una clave pública de alto nivel en la jerarquía DNS, se puede seguir la cadena para validar los datos en la propia zona o en la zona de los hijos.

Durante el proceso de validación un resolvedor iniciará a partir de un ancla de confianza configurada. Esta se utilizará para validar que el conjunto de claves en la cúspide de la zona. Una vez que el conjunto de claves ha sido validado las claves en ese conjunto de claves se pueden utilizar para validar cualquier otro dato en una zona, tales como A, AAAA y registros de recursos PTR. Para confiar en una zona secundaria el validador seguirá un puntero, almacenado en el registro de recursos DS, que apunta a una clave en el conjunto de claves del hijo que se utilizará para validar las claves en esa zona. Ese RR DS está firmado por la ZSK del padre y señala a la KSK del hijo [17].

4.1. Problemas.

Debido a que las zonas padres (ec., edu.ec.) aún no son seguras se requiere gesticular con un registro DLV para que terceras partes puedan hacer uso de la seguridad que el dominio proporciona. El registro DLV que permite mayor facilidad para realizar la validación lookaside es el ISC DLV (Internet Systems Consortium DNSSEC Look-aside Validation) [34], ya que permite servir como un repositorio de confianza de los puntos de entrada a través del cual las claves se pueden recuperar de forma segura por el sistema de resolución cuando se las necesite.

Para ello se añaden las zonas (unl.edu.ec, utpl.edu.ec) al registro DLV y se carga la clave KSK generada para cada zona, pero se presenta un error de servidores inaccesibles (Servers Unreachable) como se muestra en la figura 9.

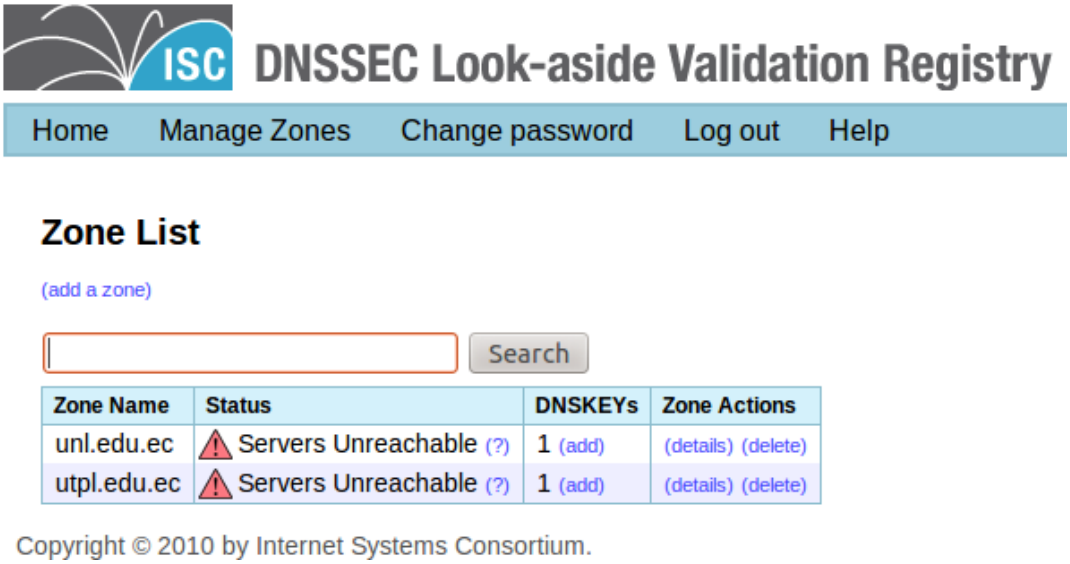

Figura 9. Error Servers Unreachable.

Donde se revisa el log de las medidas de verificación realizadas sobre los registros DNSKEY, como medio para diagnosticar los fallos como se observa en la figura 10.

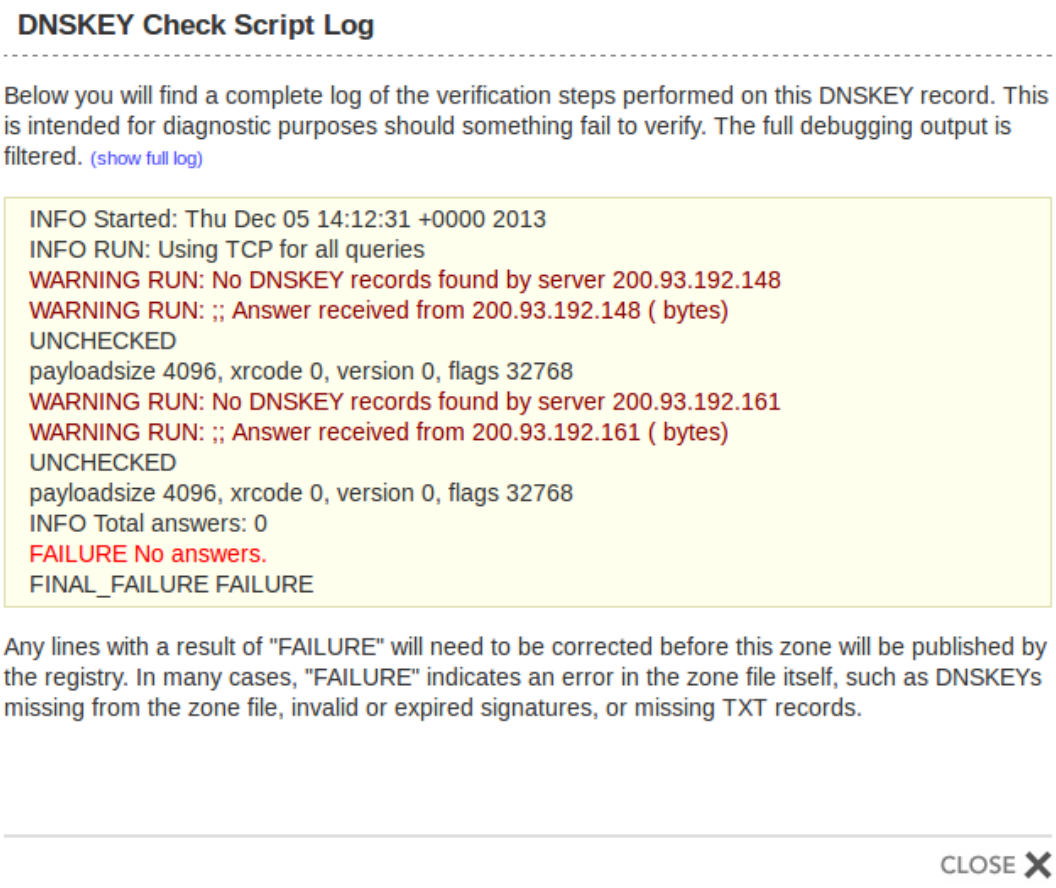

Figura 10. Log.

Con lo que se derivan dos problemas que se describen a continuación.

1.1.1. Dominio.

El registro DLV valida la propiedad de los dominios unl.edu.ec y utpl.edu.ec, pero debido a que la implementación de DNSSEC no se la ha realizado en los servidores reales no se puede utilizar estos dominios, es por ello que al momento de consultar la existencia de los registros DNSKEY en los servidores DNS de TELCONET e IMPSAT respectivamente no se los encuentra; como se observa en las figuras 11 y 12.

```
3.630:DEBUG RUN: Found answer from 200.93.192.148
3.630:WARNING RUN: No DNSKEY records found by server 200.93.192.148
3.630:WARNING RUN: ;; Answer received from 200.93.192.148 ( bytes)
;;;
;; Security Level : UNCHECKED
;; HEADER SECTION:
;; id = 40190:
;; qr = true opcode = Query aa = true tc = false rd = false:
;; ra = false ad = false cd = false rcode = NOERROR:
;; qdcount = 1 ancount = 0 nscount = 1 arcount = 1:
:
OPT pseudo-record : payloadsize 4096, xrcode 0, version 0, flags 32768
:
;; QUESTION SECTION (1 record):
;; unl.edu.ec. IN DNSKEY:
:
;; AUTHORITY SECTION (1 record):
unl.edu.ec. 300 IN SOA srv1.telconet.net. hostmaster.unl.edu.ec. 2011051718 3600 250
1209600 300:
```

Figura 11. Negación de registros DNSKEY en la zona unl.edu.ec.

```
77.248:DEBUG RUN: Found answer from 200.0.31.155
77.248:WARNING RUN: No DNSKEY records found by server 200.0.31.155
77.248:WARNING RUN: ;; Answer received from 200.0.31.155 ( bytes)
;;;
;; Security Level : UNCHECKED
;; HEADER SECTION:
;; id = 49538:
;; qr = true opcode = Query aa = true tc = false rd = false:
;; ra = false ad = false cd = false rcode = NOERROR:
;; qdcount = 1 ancount = 0 nscount = 1 arcount = 1:
:
OPT pseudo-record : payloadsize 4096, xrcode 0, version 0, flags 32768
:
;; QUESTION SECTION (1 record):
;; utpl.edu.ec. IN DNSKEY:
:
;; AUTHORITY SECTION (1 record):
utpl.edu.ec. 5500 IN SOA gdr2.utpl.edu.ec. root.utpl.edu.ec. 2013112001 3600 7200
1209600 5500:
```

Figura 12. Negación de registros DNSKEY en la zona utpl.edu.ec.

Por ello se decidió comprar dos dominios en el registro de dominios NIC.EC que tengan como zona padre a edu.ec., pero para obtener este tipo de dominios se necesita ser una persona jurídica que posee RUC, por lo que no se pudo realizar dicha compra.

1.1.2. Proveedor de servicios de internet.

Debido a que los dominios de la Universidad Nacional de Loja y Universidad Técnica Particular de Loja se encuentran almacenados en los servidores DNS de TELCONET e IMPSAT respectivamente (ver figuras 13 y 14), es necesario que estos proveedores hayan desplegado DNSSEC en sus zonas, situación que actualmente no se ha efectuado.

```
1.601:DEBUG RUN: Got activity for 1, from 200.12.198.1
1.601:DEBUG RUN: Got referral
1.603:DEBUG RUN: unl.edu.ec. 129600 IN NS srv1.telconet.net.
1.603:DEBUG RUN: unl.edu.ec. 129600 IN NS srv2.telconet.net.
```

Figura 13. Dominio unl.edu.ec en servidores de TELCONET.

```
1.457:DEBUG RUN: Got activity for 1, from 200.12.198.1
1.457:DEBUG RUN: Got referral
1.460:DEBUG RUN: utpl.edu.ec. 129600 IN NS gdr2.utpl.edu.ec.
1.460:DEBUG RUN: utpl.edu.ec. 129600 IN NS ns1.impsat.net.ec.
1.460:DEBUG RUN: utpl.edu.ec. 129600 IN NS gye.impsat.net.ec.
```

Figura 14. Dominio utpl.edu.ec en servidores de IMPSAT.

Es importante que los proveedores tengan esta capacidad ya que para construir una cadena de confianza se deben otorgar los registros DNSKEY a los proveedores para que ellos a su vez los registren en los servidores recursivos que funcionan como validadores de DNSSEC; y de esta manera todos los usuarios que realicen una consulta DNS sobre estos dominios tengan la seguridad de que la información se encuentra autenticada.

5. Renovación de claves.

Una renovación es el proceso en el que una de las claves en una zona se sustituye por otra de las claves. Puesto que las claves tienen una vida útil limitada resulta necesario cambiarlas de vez en cuando. Se necesita tener cuidado de que las cadenas de confianza existentes no se rompan durante la renovación.

La renovación se define por el momento en que la claves generadas con la “nueva” clave privada son introducidas por primera vez en la zona. El par de claves se puede generar con antelación y la clave pública también se puede hacer pública de antemano.

Si la renovación ha sido planeada hace referencia a una renovación programada. Si la renovación es el resultado de un (presunto) peligro o pérdida de la clave privada se llama una renovación de clave no programada o de emergencia.

Hay dos tipos de renovación de clave programados. Las renovaciones de las claves KSK y las renovaciones de las claves ZSK [17].

5.1. Renovaciones “Pre-Publicación” y “Doble Firma”.

Durante una renovación de pre-publicación, la clave pública es introducida en el conjunto de RR de DNSKEY mucho antes que los RRSIG sean hechos con la parte privada de la clave. Las “nuevas” claves públicas están entonces disponibles en caché cuando los RRSIG de los datos aparecen en los servidores de nombres autoritativos y servidores de nombres recursivos.

Durante una renovación de doble firma, el nuevo par de claves es introducido y las firmas se generan con la nueva y la vieja clave. Ambas claves públicas se publican en el DNS. Después del período que se necesita para que estos datos se propaguen a través del DNS, se retira la clave vieja y sólo la nueva clave se publica y se utiliza para la firma [17].

5.2. Renovación Zone-Signing Key (ZSK).

Durante una renovación de clave ZSK se utiliza un esquema de “pre-publicación”, para lo cual se debe preparar, renovar y limpiar la clave ZSK como se ilustra en las figuras 15, 16 y 17 respectivamente.

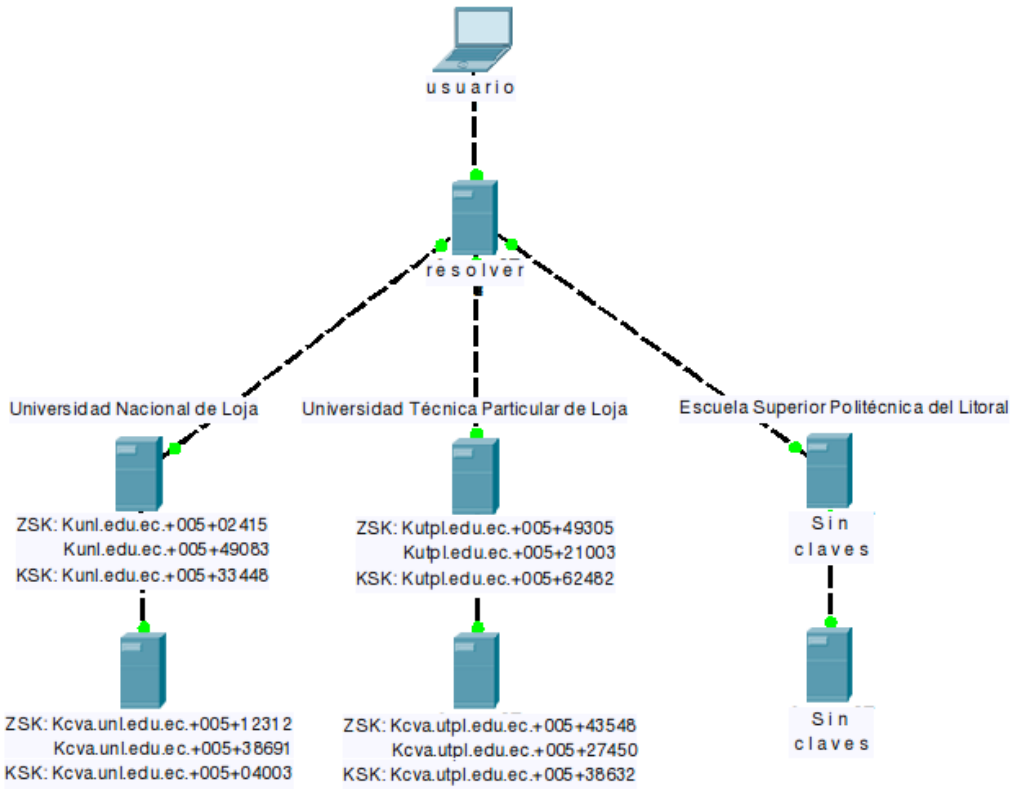

Figura 15. Preparar ZSK.

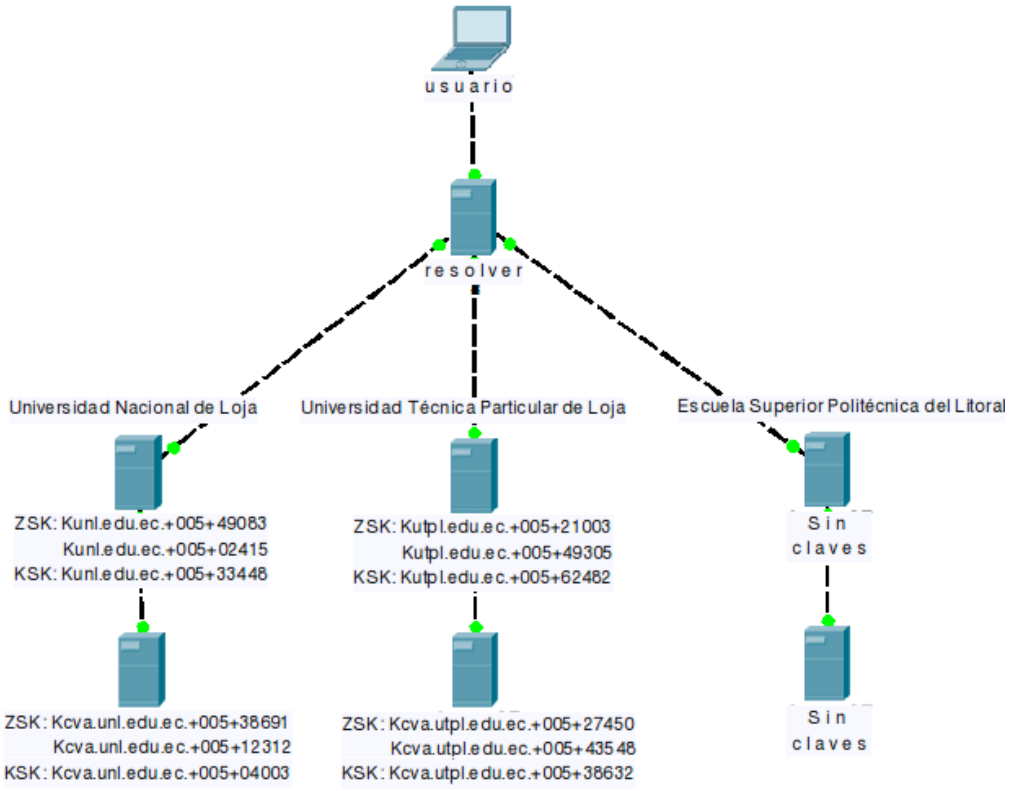

Figura 16. Renovar ZSK.

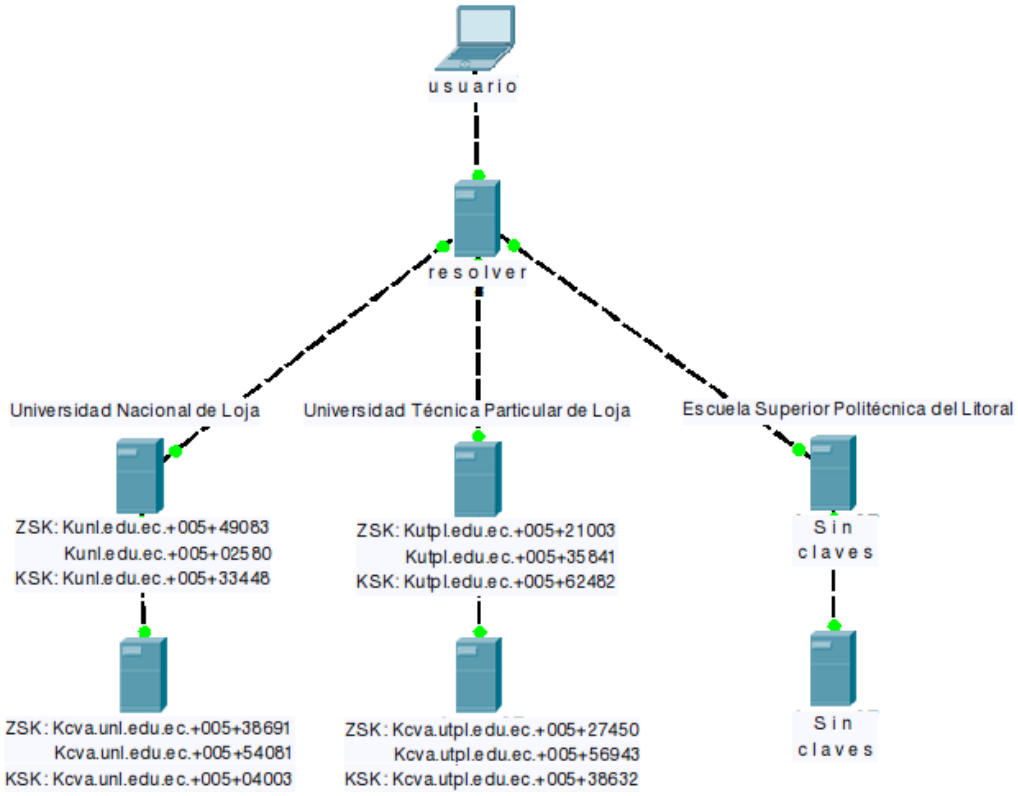

Figura 17. Limpiar ZSK.

La renovación de la clave ZSK está determinada en la documentación manifestada en [17, 33].

5.2.1. Servidores Universidad Nacional de Loja.

5.2.1.1. Sitio web.

La renovación de la clave ZSK del sito web se detalla en el Anexo 15.

5.2.1.2. Comunidad virtual de aprendizaje.

La renovación de la clave ZSK de la comunidad virtual de aprendizaje se detalla en el Anexo 16.

5.2.2. Servidores Universidad Técnica Particular de Loja.

5.2.2.1. Sitio web.

La renovación de la clave ZSK del sito web se detalla en el Anexo 17.

5.2.2.2. Comunidad virtual de aprendizaje.

La renovación de la clave ZSK de la comunidad virtual de aprendizaje se detalla en el Anexo 18.

5.3. Renovación Key-Signing Key (KSK).

Durante una renovación de clave KSK se utiliza un esquema de “doble firma”, para lo que se necesita preparar, renovar y limpiar la clave KSK como se muestra en las figuras 18, 19 y 20 respectivamente.

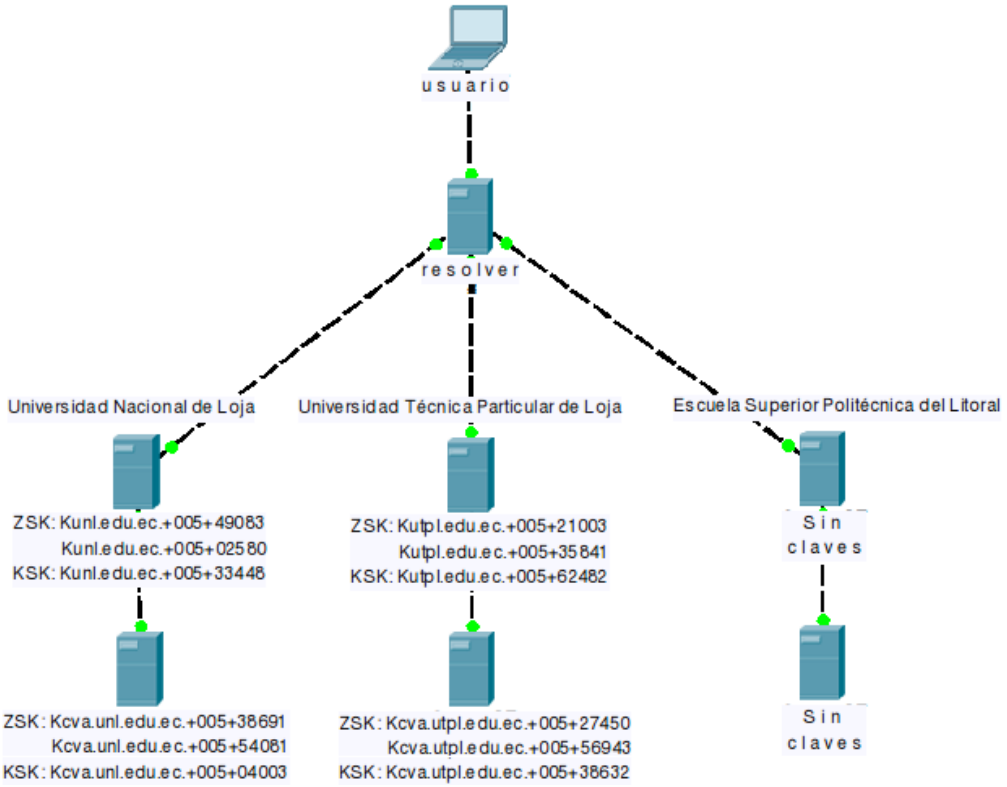

Figura 18. Preparar KSK.

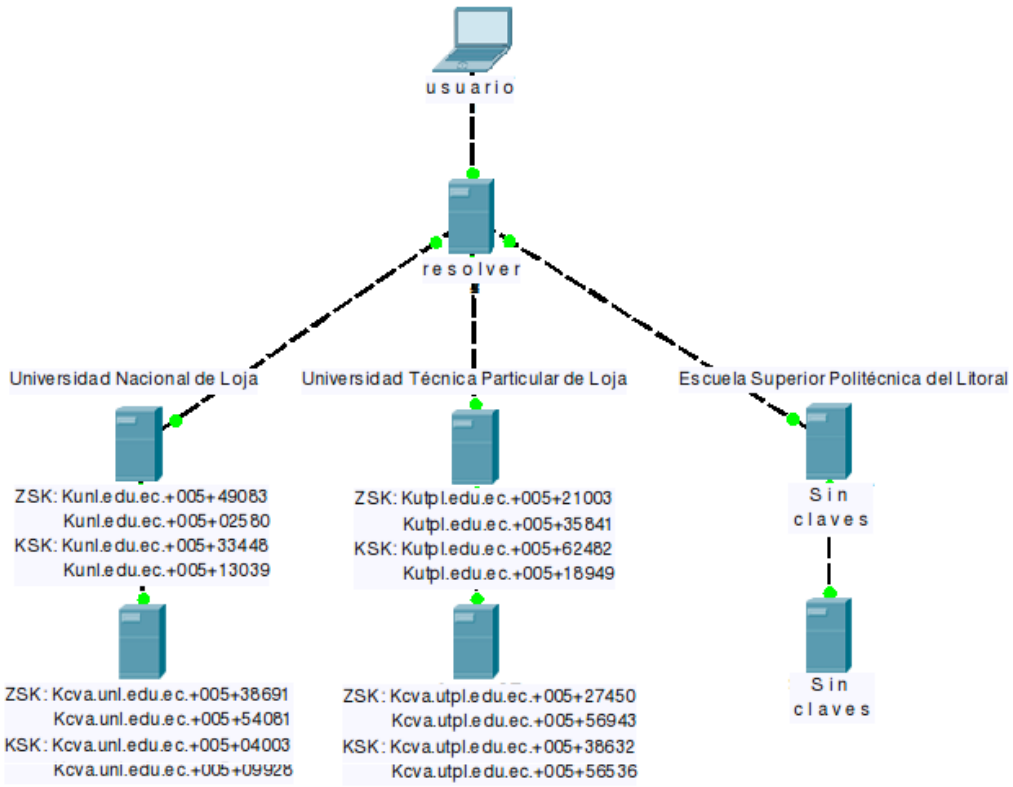

Figura 19. Renovar KSK.

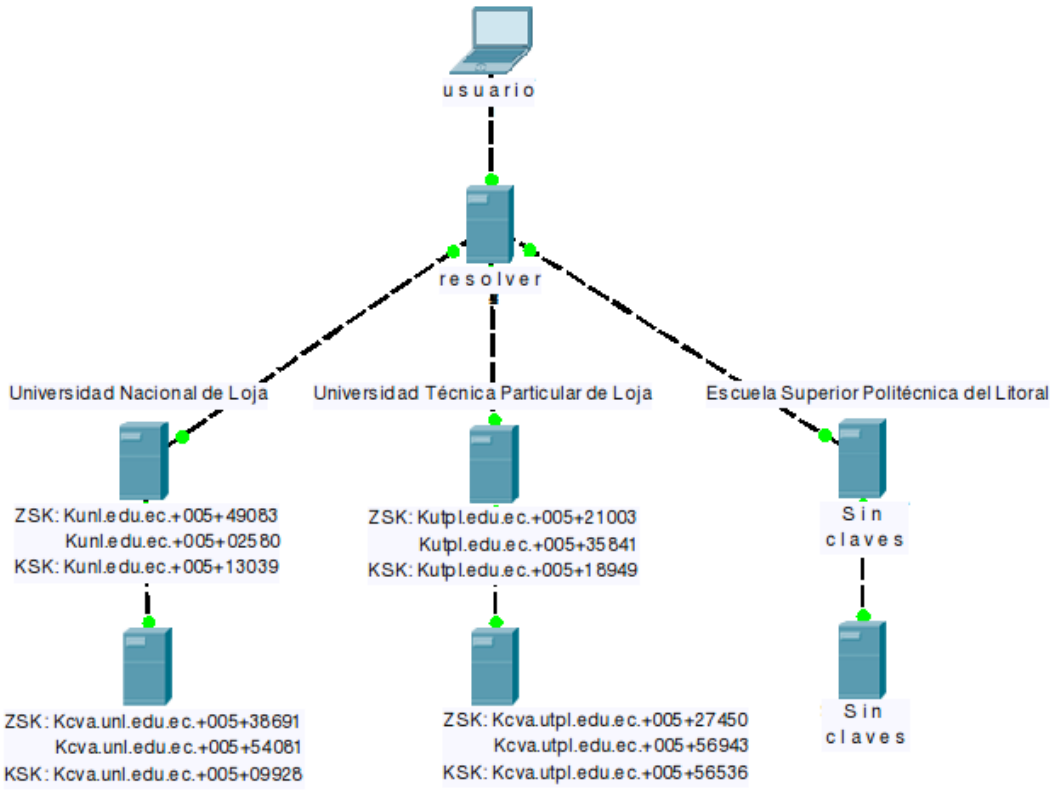

Figura 20. Limpiar KSK.

La renovación de la clave KSK está determinada en la documentación manifestada en [17, 33].

5.3.1. Servidores Universidad Nacional de Loja.

5.3.1.1. Sitio web.

La renovación de la clave KSK del sitio web se detalla en el Anexo 19.

5.3.1.2. Comunidad virtual de aprendizaje.

La renovación de la clave KSK de la comunidad virtual de aprendizaje se detalla en el Anexo 20.

5.3.2. Servidores Universidad Técnica Particular de Loja.

5.3.2.1. Sitio web.

La renovación de la clave KSK del sitio web se detalla en el Anexo 21.

5.3.2.2. Comunidad virtual de aprendizaje.

La renovación de la clave KSK de la comunidad virtual de aprendizaje se detalla en el Anexo 22.

Fase 3: Asegurar la comunicación entre servidores de las instituciones de Educación Superior.

En esta fase se desarrolló un laboratorio que simula los servidores DNS de la Universidad Nacional de Loja y la Universidad Técnica Particular de Loja, así como sus comunidades virtuales de aprendizaje, en los que se generó un secreto compartido de TSIG [36], lo cual se efectuó a través de la consola del sistema operativo Debian 7.

Para la validación de DNSSEC se usó el plugin DNSSEC Validator [37] que permitió verificar la existencia de esta tecnología en los sitios web de las instituciones educativas en los que se empleó el sistema de gestión de contenidos Joomla y en las comunidades virtuales de aprendizaje donde se utilizó el sistema de gestión de aprendizaje Moodle, además se realizó un redireccionamiento DNS como un ejemplo de ataque DNS que evidencia que los dominios asegurados no se sufren de esta inseguridad.

1. Aseguramiento de la transferencia de zona.

La comunicación entre los hosts se puede asegurar (autenticado y cifrado) mediante un esquema basado en la criptografía simétrica. Al compartir una clave los administradores de dos servidores pueden estar seguros de que los datos DNS sólo se ha intercambiado entre esas dos cajas y que los datos no han sido alterados en el tránsito.

El mecanismo más conocido usado para permitir esto se conoce como TSIG y se basa en un secreto compartido. El secreto compartido se utiliza para firmar el contenido de cada paquete DNS. La firma puede ser utilizada tanto para la autenticación y para la comprobación de la integridad de los datos. Con el fin de impedir que un tercero malicioso retransmita datos capturados (ataque de reproducción) una marca de tiempo se incluye en los datos. El mecanismo TSIG también se puede utilizar para prevenir las transferencias de zonas no autorizadas; sólo los propietarios de la clave secreta son capaces de hacer una transferencia de zona [17].

Por lo que el aseguramiento de la transferencia de zona de las instituciones de educación superior quedaría como se ilustra en la figura 21.

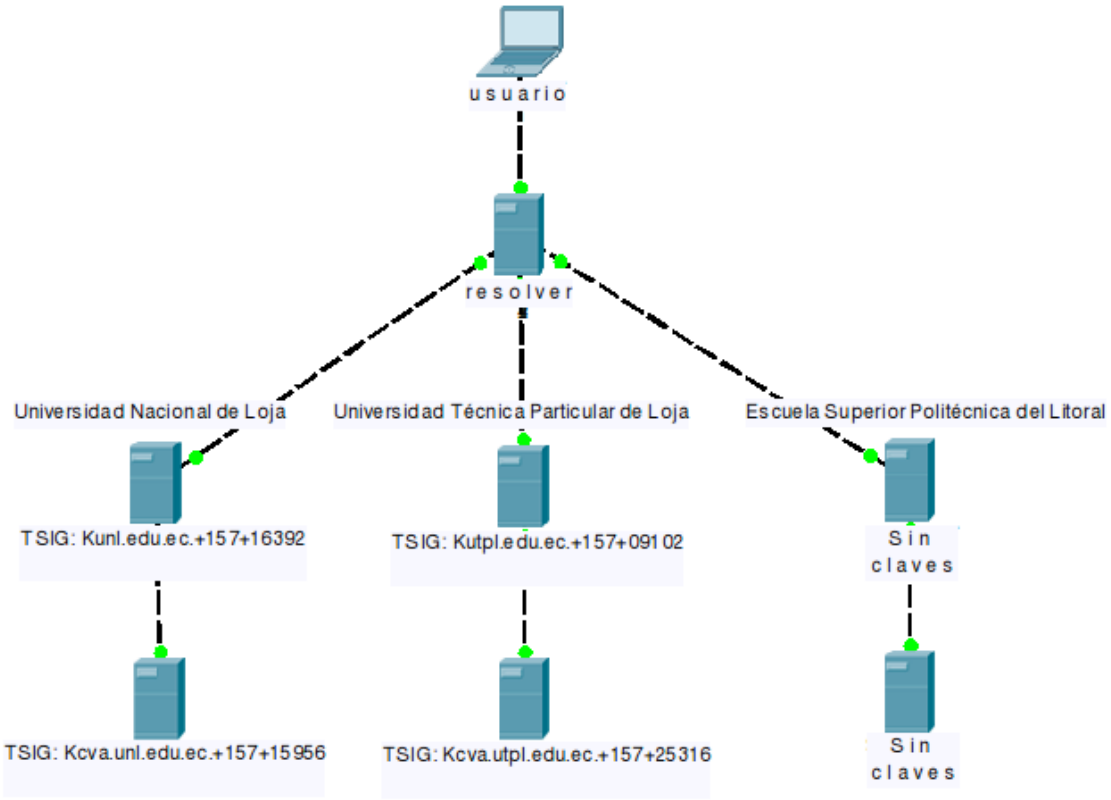

Figura 21. Esquema de claves TSIG.

El aseguramiento de la transferencia de zona está explicado en la documentación presentada en [17, 36].

1.1. Servidores Universidad Nacional de Loja.

1.1.1. Sitio web.

El aseguramiento de la transferencia de zona del sitio web se precisa en el Anexo 23.

1.1.2. Comunidad virtual de aprendizaje.

El aseguramiento de la transferencia de zona de la comunidad virtual de aprendizaje se define en el Anexo 24.

1.2. Servidores Universidad Técnica Particular de Loja.

1.2.1. Sitio web.

El aseguramiento de la transferencia de zona del sitio web se precisa en el Anexo 25.

1.2.2. Comunidad virtual de aprendizaje.

El aseguramiento de la transferencia de zona de la comunidad virtual de aprendizaje se puntualiza en el Anexo 26.

2. Validación de DNSSEC.

2.1. DNSSEC Validator.

DNSSEC Validator es un complemento para navegadores web que permite comprobar la existencia y validez de los registros de las extensiones de seguridad del DNS (DNSSEC) relativos a los nombres de dominio en la barra de direcciones del navegador. Los resultados de estas comprobaciones se muestran con iconos y textos de información en la barra de direcciones o barra de herramientas de la página. Actualmente, en los navegadores web Internet Explorer (IE), Mozilla Firefox (MF) y Google Chrome (GC) es soportado [37].

2.1.1. Servidores Universidad Nacional de Loja.

Con el plugin DNSSEC Validator instalado en el navegador web Mozilla Firefox se comprobó que los dominios unl.edu.ec y cva.unl.edu.ec están asegurados mediante DNSSEC, como se muestra en la figura 22 y 23 respectivamente.

Figura 22. Validación del dominio unl.edu.ec.

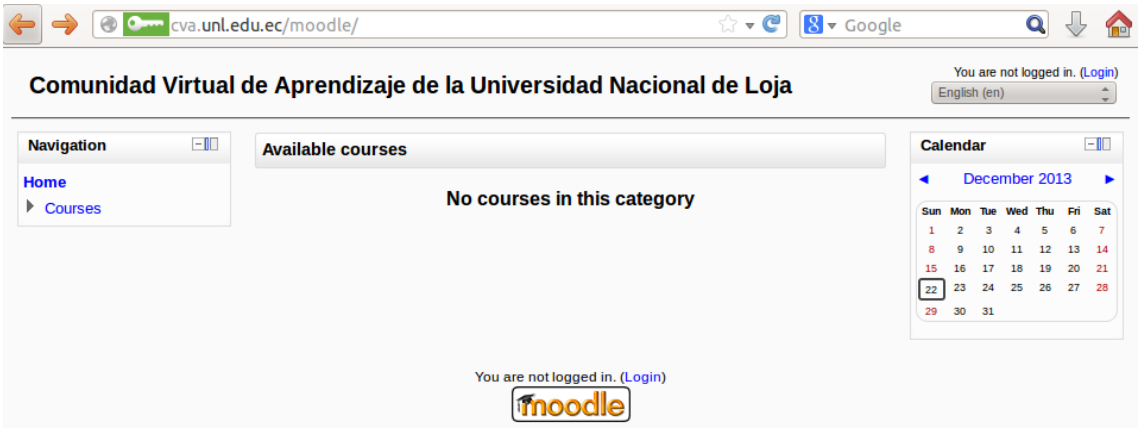

Figura 23. Validación del dominio cva.unl.edu.ec.

2.1.2. Servidores Universidad Técnica Particular de Loja.

Mediante el plugin DNSSEC Validator instalado en el navegador web Mozilla Firefox se validó que los dominios utpl.edu.ec y cva.utpl.edu.ec están asegurados mediante DNSSEC, como se muestra en la figura 24 y 25 correspondientemente.

Figura 24. Validación del dominio utpl.edu.ec.

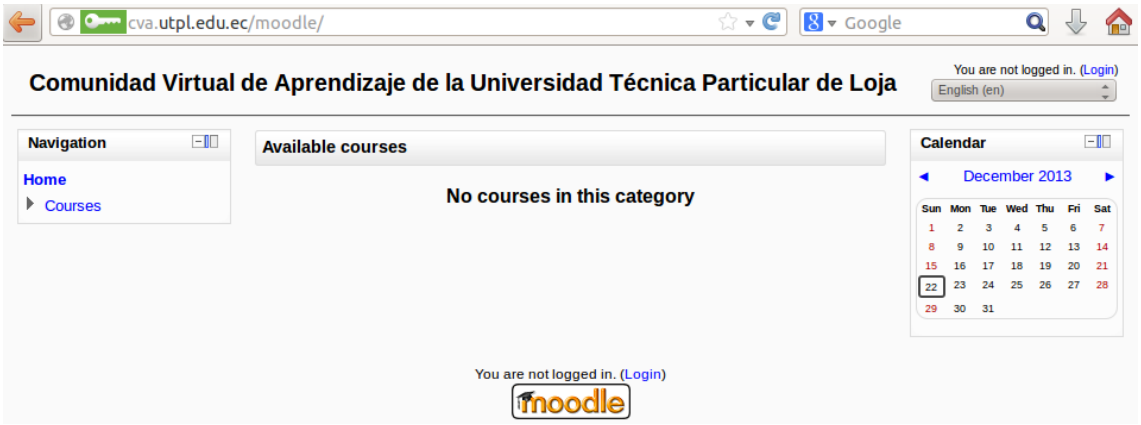

Figura 25. Validación del dominio cva.utpl.edu.ec.

2.1.3. Servidores Escuela Superior Politécnica del Litoral.

A través del plugin DNSSEC Validator instalado en el navegador web Mozilla Firefox se evidenció que los dominios espol.edu.ec y cva.espol.edu.ec no están asegurados mediante DNSSEC, como se muestra en la figura 26 y 27 concernientemente.

Figura 26. Validación del dominio espol.edu.ec.

Figura 27. Validación del dominio cva.espol.edu.ec.

Como se puede observar en las figuras anteriores, el plugin permite saber si el dominio se encuentra firmado con DNSSEC al mostrar un icono en color verde, como es el caso de los dominios unl.edu.ec, cva.unl.edu.ec, utpl.edu.ec y cva.utpl.edu.ec; mientras que para los dominios espol.edu.ec y cva.espol.edu.ec el icono se muestra con un símbolo en color rojo.

2.2. Redirección DNS.

Uno de los ataques que DNSSEC elimina es el redireccionamiento de dominio, por lo que se utilizó el sniffer Ettercap [38] para crear un ataque de este tipo y comprobar que mediante la implementación de DNSSEC resulta imposible llevarlo a cabo.

Para realizar este ataque se editó el archivo /etc/ettercap/etter.dns como se muestra en la figura 28.

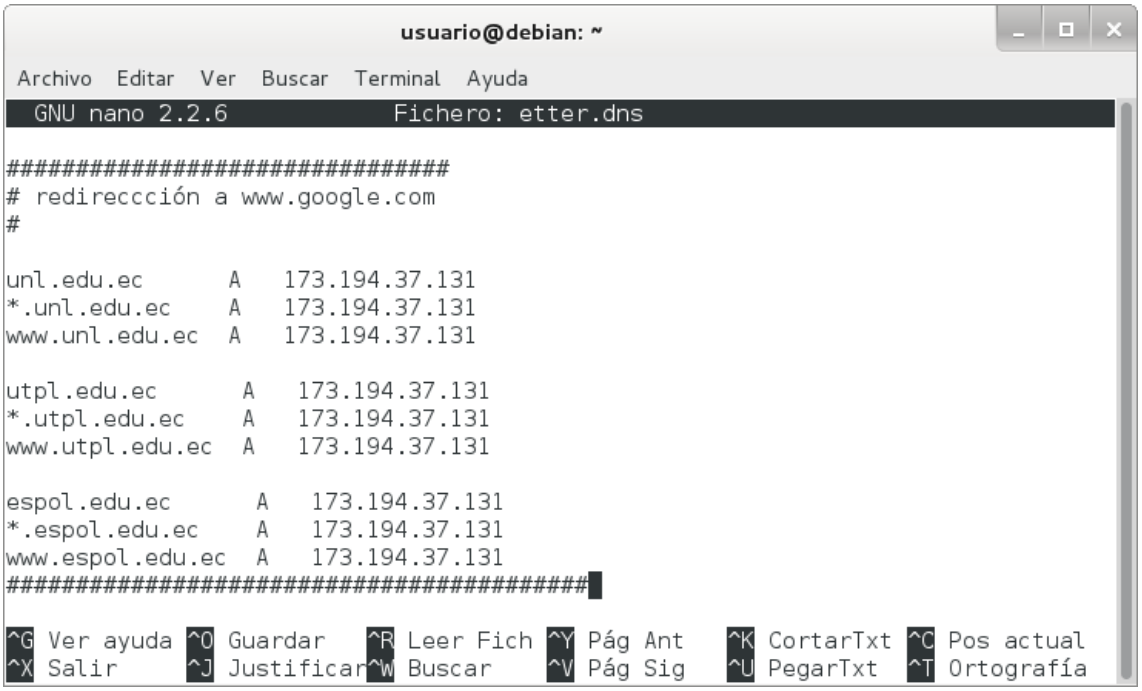

Figura 28. Archivo etter.dns.

En el que se especificó los dominios de las universidades que serán redireccionados a la dirección IP del dominio de Google (173.194.37.131).

Posteriormente se inició Ettercap mediante el siguiente comando:

#ettercap -T -q -i eth0 -P dns_spoof -M arp // //

Y se observa el redireccionamiento que se efectúa.

2.2.1. Servidores Universidad Nacional de Loja.

Debido a que los dominios del sitio web y de la comunidad virtual de aprendizaje de la universidad están asegurados con DNSSEC, el redireccionamiento no se produce tal como se muestra en la figura 29 y 30 respectivamente.

Figura 29. No existe redireccionamiento del dominio unl.edu.ec.

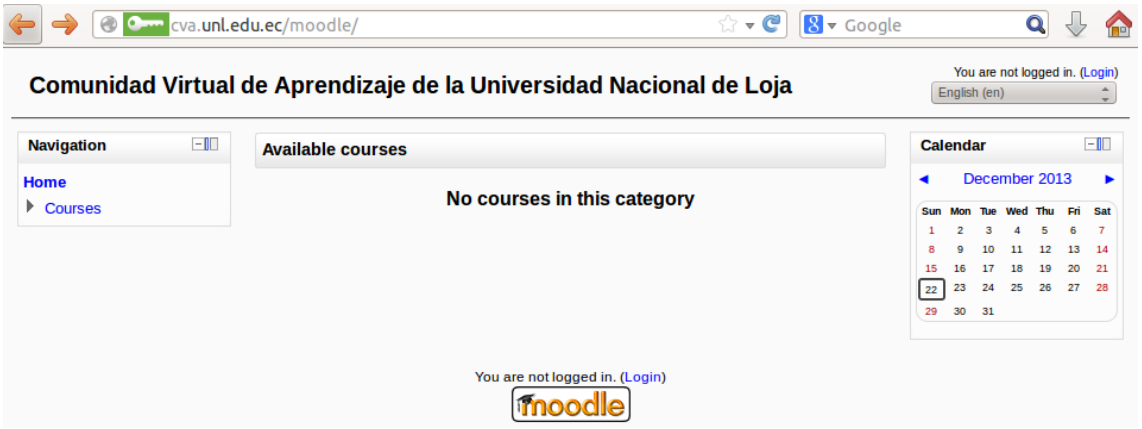

Figura 30. No existe redireccionamiento del dominio cva.unl.edu.ec.

2.2.2. Servidores Universidad Técnica Particular de Loja.

Debido a que los dominios del sitio web y de la comunidad virtual de aprendizaje de la universidad están asegurados con DNSSEC, el redireccionamiento no se produce tal como se muestra en la figura 31 y 32 correspondientemente.

Figura 31. No existe redireccionamiento del dominio utpl.edu.ec.

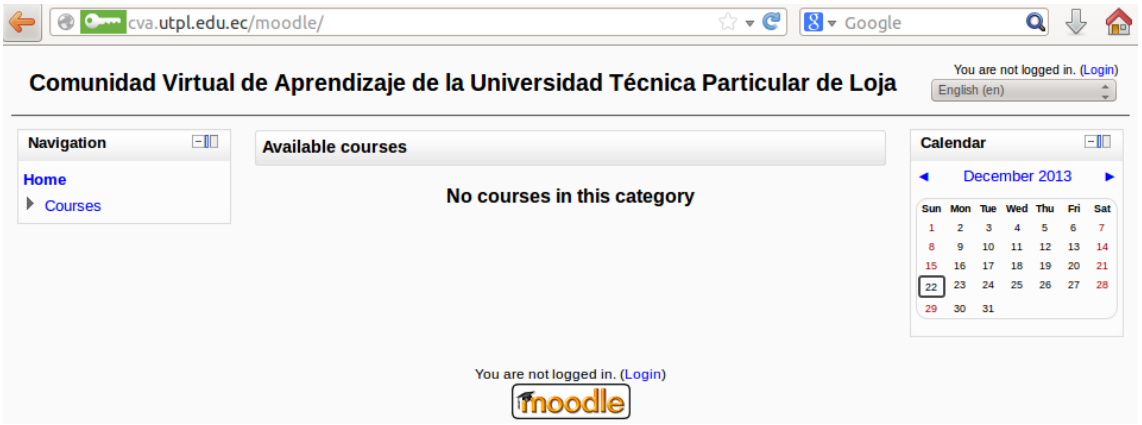

Figura 32. No existe redireccionamiento del dominio cva.utpl.edu.ec.

2.2.3. Servidores Escuela Superior Politécnica del Litoral.

Debido a que los dominios del sitio web y de la comunidad virtual de aprendizaje de la universidad no están asegurados con DNSSEC, el redireccionamiento si tiene efecto tal como se muestra en la figura 33 y 34 concernientemente.

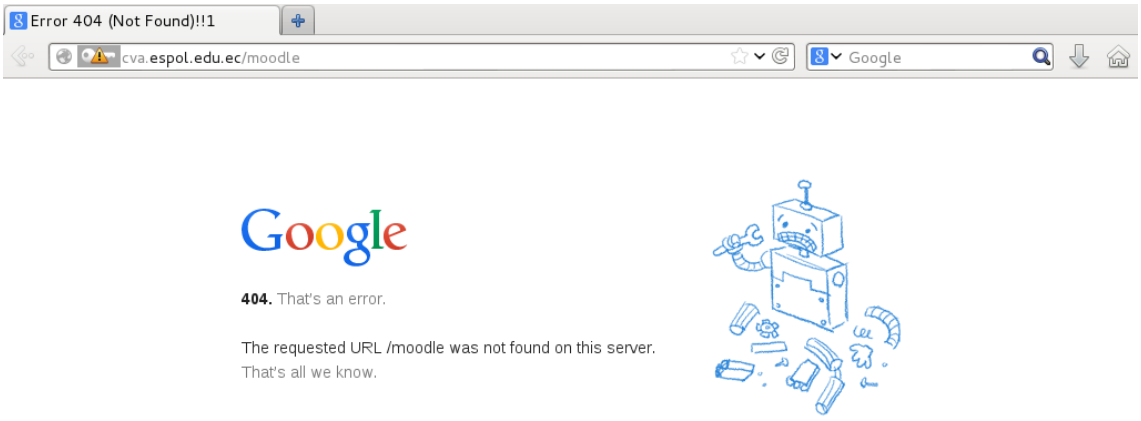

Figura 33. Redireccionamiento del dominio espol.edu.ec.

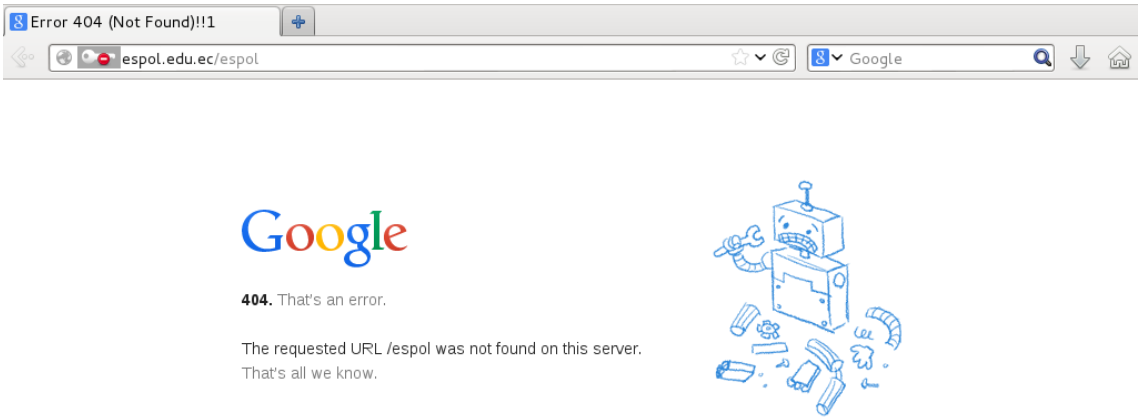

Figura 34. Redireccionamiento del dominio cva.espol.edu.ec.

g. Discusión

La implementación de DNSSEC en las instituciones de educación superior fortalece la infraestructura de ambientes de aprendizaje autenticando el origen de los datos y verificando su integridad, así mismo ofrece protección contra los datos provenientes de DNS falsos usando criptografía de clave pública/privada para firmar digitalmente información de dominio; mediante lo cual la suplantación de identidad resulta más difícil y el envenenamiento de caché deja de ser una amenaza.

El presente trabajo de titulación es de carácter investigativo cuyo propósito es promover la implementación de seguridad para el DNS en las instituciones de educación superior del país, para lo mencionado se asistió a un curso sobre artículos científicos dictado en el aula magna del Área de la Energía, las Industrias y los Recursos Naturales no Renovables, culminando con la exposición del artículo acerca del presente proyecto ante el instructor del curso y los profesores del área; es así que mediante este curso se obtuvo el conocimiento para elaborar dos artículos que fueron aceptados para ser presentados en el IX Congreso de Ciencia y Tecnología ESPE 2014 (ver Anexo 28) y la Convocatoria TICAL 2014 (ver Anexo 29).

1. Desarrollo de la propuesta alternativa.

Objetivo 1: Analizar el estado del arte del Sistema de Nombres de Dominio de las instituciones de Educación Superior, para determinar los requerimientos de implementación de DNSSEC.

El cumplimiento de este objetivo se efectuó mediante una búsqueda bibliográfica sobre casos de éxito relativos a la implementación de DNSSEC en instituciones de educación superior (ver sección Resultados subsección Fase 1 apartado 1), realizando una recogida de información a nivel internacional, nacional y local, en cuanto al ámbito nacional (ver sección Resultados subsección Fase 1 apartado 1.2) se adquirió información sobre el proveedor de servicios de internet TELCONET S.A., vislumbrando que no ha realizado el despliegue de DNSSEC en sus zonas; y en el ambiente local (ver sección Resultados subsección Fase 1 apartado 1.3) se obtuvo información acerca de la administración del servicio DNS de la Universidad Nacional de Loja y la Universidad Técnica Particular de Loja, descubriendo que no se ha efectuado la implementación de DNSSEC.

Objetivo 2: Proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

La ejecución de este objetivo se llevó a cabo a través de la instalación de servidores DNS y configuración de ellos (ver sección Resultados subsección Fase 2 apartado 1) para el funcionamiento de DNSSEC en máquinas virtuales que simulan los servidores DNS de instituciones de educación superior como son Universidad Nacional de Loja (ver sección Resultados subsección Fase 2 apartado 1.1), Universidad Técnica Particular de Loja (ver sección Resultados subsección Fase 2 apartado 1.2) y Escuela Superior Politécnica del Litoral (ver sección Resultados subsección Fase 2 apartado 1.3), así como sus respectivas comunidades virtuales de aprendizaje, lo cual permitió verificar el aseguramiento de los datos DNS que se transfieren en las mismas; para lo cual se realizó el aseguramiento de las zonas DNS (ver sección Resultados subsección Fase 2 apartado 2) a través de la generación de pares de claves KSK y ZSK empleadas para firmar las zonas y la configuración de un servidor de nombres recursivo (ver sección Resultados subsección Fase 2 apartado 3) que almacena las claves KSK (claves públicas) de los dominios firmados creando de esta forma anclas de confianza para validar las respuestas por parte de los usuarios. A partir de estos procedimientos realizados se establecieron islas de confianza formadas por los dominios de las universidades firmadas, que a su vez crearon un archipiélago de confianza entre ellas.

Conjuntamente, se desarrolló el proceso de renovación de claves (ver sección Resultados subsección Fase 2 apartado 5) en el que una de las claves en una zona se sustituyó por otra de las claves, tanto para la clave ZSK (ver sección Resultados subsección Fase 2 apartado 5.2) donde se utilizó un esquema de pre-publicación, para lo cual se preparó, renovó y limpió la clave; como para la clave KSK (ver sección Resultados subsección Fase 2 apartado 5.3) en el cual se aplicó un esquema de doble firma, para lo que se preparó, renovó y limpió la clave; lo cual funciona como medida de seguridad ya que si el servidor ha sufrido algún tipo de ataque las nuevas claves firmarán nuevamente la información de la zona y no podrá ser falsificada.

Objetivo 3: Asegurar la comunicación entre servidores de las instituciones de Educación Superior.

La realización de este objetivo se cumplió a través del aseguramiento de la transferencia de zona (ver sección Resultados subsección Fase 3 apartado 1) en los

servidores simulados de la Universidad Nacional de Loja y la Universidad Técnica Particular de Loja que garantizó la comunicación entre los servidores, mediante la generación de un secreto compartido de Transacciones Firmadas (TSIG) utilizado para firmar el contenido de cada paquete DNS.

Para validar el desempeño de DNSSEC (ver sección Resultados subsección Fase 3 apartado 2) en el navegador Mozilla Firefox de la máquina virtualizada del usuario se instaló el plugin DNSSEC Validator (ver sección Resultados subsección Fase 3 apartado 2.1) que permitió demostrar que los dominios están asegurados con DNSSEC, así también se produjo un redireccionamiento DNS (ver sección Resultados subsección Fase 3 apartado 2.2) en función de un ataque DNS que comprobó que los dominios asegurados no son víctimas de este tipo de vulnerabilidad.

2. Valoración técnica económica ambiental.

El desarrollo del presente trabajo implicó una inversión económica, puesto que exige recursos que se dedicaron, en la medida que se requirieron, para alcanzar los objetivos plasmados, los cuales se materializaron a través de acciones basadas en un plan lógico, el cual correspondió con los costos que se especifican a continuación:

TABLA II. RECURSO HUMANO.

Equipo de trabajo	**Horas**	**Precio/hora**	**Valor total**
Gabriela Espinoza	960	$5,00	$4.800,00
Director	15	$15,00	$225,00
SUBTOTAL			**$5.025,00**

TABLA III. RECURSOS MATERIALES.

Descripción	Cantidad	Depreciación			Valor Total
		V. Real	T. de util/año	V. Rec.	
Hardware					
Portátil Dell Core i5	1	$1.300,00	5	$300	$200,00
Impresora	1	$60,00	5	$12	$9,60
Subtotal					**$209,60**
Software					
Sistema Operativo Debian	8				$0,00
Sistema Operativo Windows 7	1				$149,00
Oracle VM VirtualBox	1				$0,00
Ettercap	1				$0,00
DNSSEC Validator	1				$0,00
Subtotal					**$149,00**
TOTAL					**$358,60**

TABLA IV. RECURSOS DE SERVICIOS.

Descripción	Cantidad	Valor Unitario	Valor Total
Internet	400	$0,70	$280,00
Llamadas telefónicas	5	$0,20 x min	$1,00
Bus	150	$0,25	$37,50
Taxi	10	$1,00	$10,00
SUBTOTAL			**$328,50**

TABLA V. COSTE GENERAL DE RECURSOS.

Descripción	Total
Recurso humano	$5.025,00
Recursos materiales	$358,60
Recursos de servicios	$328,50
Subtotal	$5.712,10
Imprevistos (10%)	$571,21
Total	**$6.283,31**

El desarrollo del presente proyecto se estima factible, debido a que el coste general corresponde con el tiempo de ejecución del mismo que fue de cuatro meses, además se utilizó herramientas de licencia libre para reducir el coste de recursos materiales; cabe mencionar que el costo económico se adjudicó por la autora del trabajo debido a que esta investigación se considera de carácter formativo y que permitirá la obtención del título profesional, exceptuando el costo del recurso humano del director del proyecto que fue adjudicado por la universidad.

h. Conclusiones

- El uno porciento de las instituciones de educación superior a nivel mundial han firmado sus zonas con DNSSEC, en el ámbito nacional ninguna institución académica a efectuado el despliegue de esta tecnología, siendo el mismo caso el del proveedor de servicios de internet TELCONET S.A. lo cual no proporciona confianza en los usuarios al momento de mantenerse en línea en sitios web no asegurados. En Latinoamérica, los países de Brasil, Chile, Colombia y Guyane han firmado sus dominios de nivel superior de código de país con DNSSEC.

- El despliegue de DNSSEC en comunidades virtuales de aprendizaje de las instituciones de educación superior garantiza la procedencia de contenidos creados en este tipo de ambientes de aprendizaje y permite mantener comunicaciones digitales fidedignas y confiables para el aprendizaje y la investigación.

- La generación de secretos compartidos de Transacciones Firmadas permite que exclusivamente las partes que integran el secreto puedan realizar transacciones de zona, con lo que se asegura la comunicación entre los servidores de las instituciones de educación superior.

- No se registra información de un plan para realizar el despliegue de las extensiones de seguridad en los dominios .ec y .edu.ec, por lo que, las instituciones que deseen implementar DNSSEC en sus entornos DNS pueden hacer uso del DNSSEC Look-aside Validation provisto por la Internet Systems Consortium.

i. Recomendaciones

- Los proveedores de servicios de internet deben realizar la implementación de DNSSEC en sus zonas para reducir el riesgo de que sus clientes sean víctimas de ataques DNS y proteger la información de las universidades, escuelas politécnicas, organizaciones de ciencia y tecnología del mundo.

- Las instituciones de educación superior deben adoptar planes sobre la implementación de DNSSEC, para que la información que se produzca en ellas conste de integridad para el personal académico que haga uso de la misma, además la implementación de esta tecnología fortalece la reputación de la institución y la confianza por parte de usuarios externos.

- Debido a que DNSSEC no es un mecanismo que resuelve todos los problemas concernientes al DNS, se recomienda que su implementación se desarrolle conjuntamente con otras técnicas como el protocolo DNScurve para proteger las consultas entre un cliente y un servidor mediante la encriptación de los paquetes DNS, el conjunto de protocolos IPsec para asegurar las comunicaciones sobre el Protocolo de Internet (IP) cifrando cada paquete IP en un flujo de datos; y el protocolo SSL o TLS para proveer autenticación y privacidad de la información entre las partes extremas mediante el uso de criptografía.

j. Bibliografía

Referencias Bibliográficas

[1] DNSSEC Deployment. ***DNSSEC in Higher Education — 1% is not enough***. [En línea] link: https://www.dnssec-deployment.org/index.php/2012/03/dnssec-in-higher-education-1-isnt-enough/. Consulta realizada 10-Feb-2014.

[2] Edilia Bautista Acosta, Rodolfo Sánchez Reyes. ***Las comunidades virtuales de aprendizaje en la educación presencial como medio para fomentar el uso de las TIC en los estudiantes de nivel medio superior (Propuesta)***. [En línea] link: http://www.comie.org.mx/congreso/memoriaelectronica/v10/pdf/area_tematica_07/ponencias/1101-F.pdf. Consulta realizada 10-Feb-2014.

[3] Miguel Morillo Iruela. ***DNSSEC (DNS Security Extensions)***. Universidad de Castilla-La Mancha. [En línea] link: http://www.dns-sec.es/wp-content/uploads/2010/12/DNSSEC_mmi.pdf. Consulta realizada 11-Feb-2014.

[4] .CO Internet S.A.S. ***Una introducción a DNSSEC***. [En línea] link: http://www.cointernet.com.co/sites/default/files/documents/DNSSEC_Informacion_Mar2012_ES.pdf. Consulta realizada 12-Feb-2014.

[5] Educause. ***Things you should know about DNSSEC***. [En línea] link: http://net.educause.edu/ir/library/pdf/est1001.pdf. Consulta realizada 05-Nov-2013.

[6] Microsoft. ***Introducción a DNS.*** [En línea] link: http://technet.microsoft.com/es-es/library/cc730775.aspx. Consulta realizada 13-Feb-2014.

[7] Tanenbaum, A.S. ***Redes de computadoras.*** Editorial Alhambra S. A. (SP). 2003. [En línea] link: http://books.google.com.ec/books?id=WWD-4oF9hjEC. Consulta realizada 13-Feb-2014.

[8] Jesús Moreno León, Alberto Molina Coballes. ***DNS: Domain Name System.*** Consejería de Educación. [En línea] link: http://www.josedomingo.org/web/mod/resource/view.php?id=2187. Consulta realizada 14-Feb-2014.

[9] Alfredo Barrainkua Zallo. ***DNS Domain Name Service.*** Instituto de Iurreta. [En línea] link: http://www1.iurreta-institutua.net/infortxostenak/sarezerlinux/ServiciosRedLinux-DNS-v1.0-ES.pdf. Consulta realizada 14-Feb-2014.

[10] John Deivis Tabares Tobón, Luis Fernando Ramirez. ***DNS Domain Name System Sistema de Nombres de Dominio.*** Servicio Nacional de Aprendizaje. [En línea]

link: http://redesjdeivis.files.wordpress.com/2011/10/servidor-dns-windows-server2.pdf. Consulta realizada 15-Feb-2014.

[11] Miguel Ángel Hernández Vallejos. ***Riesgos en el sistema de DNS.*** Revista SIC (Seguridad en Informática y Comunicaciones), Febrero 2006, Nº 68. [En línea] link: http://www.geocities.ws/lowis00/hwct/foros/local/pag15.pdf. Consulta realizada 15-Feb-2014.

[12] D. Atkins. ***Threat Analysis of the Domain Name System (DNS)***. Request for Comments 3833, Internet Engineering Task Force, Agosto 2004. [En línea] link: http://tools.ietf.org/html/rfc3833. Consulta realizada 16-Feb-2014.

[13] Geoff Huston. ***DNSSEC - The Theory.*** Internet Society. The ISP Column. [En línea] link: http://www.cse.iitd.ernet.in/~siy117527/sil765/readings/dnssec.pdf. Consulta realizada 16-Feb-2014.

[14] R. Gieben. ***Chain of Trust.*** NLnet Labs. [En línea] link: http://www.nlnetlabs.nl/downloads/publications/CSI-report.pdf. Consulta realizada 16-Feb-2014.

[15] Miguel Morillo Iruela. ***DNSSEC (DNS Security Extensions).*** Universidad de Castilla-La Mancha. [En línea] link: http://www.dns-sec.es/wp-content/uploads/2010/12/DNSSEC_mmi.pdf. Consulta realizada 16-Feb-2014.

[16] Eric Amberg. ***Cadena de Confianza.*** Revista Linux Magazine, Nº 41. [En línea] link: http://www.linux-magazine.es/issue/41/058-064DNSSECLM41.pdf. Consulta realizada 16-Feb-2014.

[17] Olaf Kolkman. ***DNSSEC HOWTO, a tutorial in disguise.*** [En línea] link: http://www.nlnetlabs.nl/publications/dnssec_howto/dnssec_howto.pdf. Consulta realizada 17-Feb-2014.

[18] R. Arends. ***Resource Records for the DNS Security Extensions.*** Request for Comments 4034, Internet Engineering Task Force, Marzo 2005. Obsoletos RFC 2535, 3008, 3090, 3445, 3655, 3658, 3755, 3757, 3845; Actualizado por 1034, 1035, 2136, 2181, 2308, 3225, 3007, 3597, 3226. [En línea] link: http://tools.ietf.org/html/rfc4034. Consulta realizada 18-Feb-2014.

[19] R. Arends. ***Protocol Modifications for the DNS Security Extensions.*** Request for Comments 4035, Internet Engineering Task Force, Marzo 2005. Obsoletos RFC 2535, 3008, 3090, 3445, 3655, 3658, 3755, 3757, 3845; Actualizado por RFC 1034, 1035, 2136, 2181, 2308, 3225, 3007, 3597, 3226. [En línea] link: http://tools.ietf.org/html/rfc4035. Consulta realizada 18-Feb-2014.

[20] P. Mockapetris. ***Domain names – concepts and facilities.*** Request for Comments 1034, Internet Engineering Task Force, Noviembre 1987. Obsoletos RFC 0973; Actualizado por RFC 1101. [En línea] link: http://tools.ietf.org/html/rfc1034. Consulta realizada 19-Feb-2014.

[21] J. Schlyter, Ed. ***DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format.*** Request for Comments 3845, Internet Engineering Task Force, Agosto 2004. Actualizado por RFC 3755, 2535. [En línea] link: http://tools.ietf.org/html/rfc3845. Consulta realizada 19-Feb-2014.

[22] Instituto Internacional de Planeamiento de la Educación (IIPE Buenos Aires). ***Resolución de problemas.*** Ministerio de Educación de la Nación. Argentina. [En línea] link: http://187.174.84.106/siise/procap/ktml2/files/uploads/modulo07.pdf. Consulta realizada 20-Feb-2014.

[23] DNSSEC.PT. ***Higher education institutions and R&D sign their domains with DNSSEC.*** [En línea] link: http://www.dnssec.pt/index.php?lang=en. Consulta realizada 20-Feb-2014..

[24] Shirley Ross. ***University of Pennsylvania Becomes First U.S. University to Deploy DNSSEC (DNS Security).*** Information Systems and Computing. [En línea] link: http://www.upenn.edu/computing/home/news/2009/1101dnssec.html. Consulta realizada 20-Feb-2014.

[25] Joao Damas, José. M Femenia, Antoni Santos Cutando, Silvia Onsurbe Martínez. ***Despliegues DNSSEC.*** Information Systems and Computing, Universidad de Valencia, Universidad Pompeu Fabra. [En línea] link: http://www.rediris.es/difusion/publicaciones/boletin/90/ponencia11.A.pdf. Consulta realizada 20-Feb-2014.

[26] APNIC. ***Resolvers by as.*** Laboratorios APNIC. [En línea] link: http://labs.apnic.net/dnssec/resolvers_by_as.txt. Consulta realizada 21-Feb-2014.

[27] Verisign. ***Beneficios para proveedores de Internet.*** [En línea] link: http://www.verisigninc.com/es_LA/why-verisign/innovation-initiatives/dnssec/benefits/index.xhtml?target=isps. Consulta realizada 21-Feb-2014.

[28] A10 Networks, Inc. ***Domain Name System Security Extensions (DNSSEC): Preparing the Network.*** [En línea] link: http://www.a10networks.com.cn/resources/files/WP_DNSSEC_98768755098.pdf. Consulta realizada 21-Feb-2014.

[29] R. Gieben. ***DNSSEC in NL.*** NLnet Labs. [En línea] link: http://www.nlnetlabs.nl/downloads/publications/dnssec/dnssecnl/secreg-report.pdf. Consulta realizada 22-Feb-2014.

[30] Internet Systems Consortium. ***BIND 9 Administrator Reference Manual.*** [En línea] link: http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.pdf. Consulta realizada 22-Feb-2014.

[31] Nicolai Langfeldt, Jamie Norrish & Co. ***DNS HOWTO.*** [En línea] link: http://www.tldp.org/HOWTO/pdf/DNS-HOWTO.pdf. Consulta realizada 22-Feb-2014.

[32] LinuxConfig.com. ***Linux DNS server BIND configuration.*** [En línea] link: http://linuxconfig.org/linux-dns-server-bind-configuration. Consulta realizada 22-Feb-2014.

[33] VeriSign. ***Tool guide series in DNSSEC.*** [En línea] link: https://net.educause.edu/ir/library/pdf/CSD5928.pdf. Consulta realizada 23-Feb-2014.

[34] Internet Systems Consortium. ***DNSSEC Look-aside Validation Registry.*** [En línea] link: https://dlv.isc.org/about/using. Consulta realizada 23-Feb-2014.

[35] Roland van Rijswijk- Deij. ***Deploying DNSSEC. Validation on recursive caching name servers.*** Surf Net. Agosto 2012. [En línea] link: http://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_Deploying_DNSSEC_v20.pdf. Consulta realizada 23-Feb-2014.

[36] P. Vixie, O. Gudmundsson, D. Eastlake 3rd, B. Wellington. ***Secret Key Transaction Authentication for DNS (TSIG).*** RFC 2845 (Estándar Propuesto), May 2000. Actualizado por RFC 3645. [En línea] link: http://www.ietf.org/rfc/rfc2845.txt. Consulta realizada 23-Feb-2014.

[37] Martin Straka, Karel Slaný, Ondřej Surý, Ondřej Filip. ***DNSSEC Validator***. CZ.NIC. [En línea] link: https://www.dnssec-validator.cz/. Consulta realizada 23-Feb-2014.

[38] Alberto Ornaghi, Marco Valleri, Emilio Escobar, Eric Milam. ***Ettercap***. [En línea] link: http://ettercap.sourceforge.net. Consulta realizada 23-Feb-2014.

k. Anexos

Anexo 1: Certificación de traducción.

Lic. Susana Mabel González Salinas
LICENCIADA EN CIENCIAS DE LA EDUCACIÓN EN LA ESPECIALIDAD DE IDIOMA INGLÉS

CERTIFICA:

Que la traducción del resumen del presente trabajo de titulación, cuyo tema versa sobre **"EXTENSIONES DE SEGURIDAD PARA EL SISTEMA DE NOMBRES DE DOMINIO APLICADAS EN COMUNIDADES VIRTUALES DE APRENDIZAJE DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR"**, de la autora Gabriela Paulina Espinoza Ami, ha sido realizado por mi persona por lo cual autorizo su presentación.

Loja, Marzo del 2014

……..

Lic. Susana Mabel González Salinas

Anexo 2: Entrevista al encargado del servidor DNS de la Universidad Nacional de Loja.

UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Carrera de Ingeniería en Sistemas

La presente entrevista está dirigida al encargado del servidor DNS de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, con el objetivo de recolectar información relevante y actualizada acerca del servidor/servicio DNS para el análisis de su administración y nivel de seguridad lógica.

Datos

Nombre: Ing. Juan Pablo Ramón

Cargo: Jefe de la Unidad de Redes

Fecha: 04 de Noviembre del 2013

Preguntas

1. ¿Quién tiene acceso al servidor?

El administrador del servidor DNS.

2. ¿Cuál es el número de usuarios del servicio?

Alto (X) Medio ( ) Bajo ( )

3. ¿Cuál es el nivel de importancia/impacto si el servidor/servicio falla?

Grave (X) Medio ( ) Leve ( )

¿Por qué?

Si este servicio falla no se tendría acceso a ciertos dominios en la red, las direcciones de cierto dominio se podrían reconocer como no válidas y con ello no se podrían realizar las actividades diarias, provocando pérdidas y molestias en los usuarios.

4. ¿El servicio DNS interactúa con otros servicios? ¿Con cuáles?

El servicio DNS interactúa con otros servicios, como es el caso de los servicios Web, Webmail y EVA.

5. ¿El servidor cuenta con seguridad lógica? ¿Con qué tipo?

Los tipos de seguridades lógicas con las que cuenta el servidor DNS son las iptables, SSH y el firewall.

6. ¿Se monitorea el tráfico que recibe el servidor? ¿Con qué frecuencia?

En la actualidad no se realiza el monitoreo del tráfico de red en el servidor DNS.

7. ¿Se ha detectado alguno de los siguientes ataques al servidor?

Suplantación del dominio	( )
Redirección del dominio	( )
Falsificación de la página	( )
Interceptación de paquetes DNS	(X)
Denegación del servicio	( )

8. ¿Cree conveniente la implementación de DNSSEC? ¿Por qué?

Resultaría conveniente implementar DNSSEC, ya que los usuarios del dominio de la universidad que se encuentran fuera de la ciudad como en Zapotepamba y la Quinta Experimental “El Padmi” podrían intercambiar información confidencial teniendo seguridad de que es la real; además en el caso de la Modalidad de Estudios a Distancia (MED) se tendrá la confianza de la información en cuanto a pagos bancarios que deben realizar.

Anexo 3: Entrevista al encargado del servidor DNS de la Universidad Técnica Particular de Loja.

UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Carrera de Ingeniería en Sistemas

La presente entrevista está dirigida al encargado del servidor DNS de la Unidad de Proyectos y Sistemas Informáticos de la Universidad Técnica Particular de Loja, con el objetivo de recolectar información relevante y actualizada acerca del servidor/servicio DNS para el análisis de su administración y nivel de seguridad lógica.

Datos

Nombre: Ing. Byron Jaramillo

Cargo: Jefe de la Unidad de Redes

Fecha: 04 de Noviembre del 2013

Preguntas

1. ¿Quién tiene acceso al servidor?

El administrador del servidor DNS.

2. ¿Cuál es el número de usuarios del servicio DNS?

Alto (X) Medio ( ) Bajo ( )

3. ¿Cuál es el nivel de importancia/impacto si el servidor/servicio falla?

Grave (X) Medio ( ) Leve ( )

¿Por qué?

Porque se produciría un colapso total de los demás servicios de la universidad, como por ejemplo el Entorno Virtual de Aprendizaje (EVA) y el registro académico, aparte de que desde el exterior no se podrían resolver los nombres de Dominio.

4. ¿El servicio DNS interactúa con otros servicios? ¿Con cuáles?

El servicio DNS interactúa con otros servicios, como es el caso de los servicios Web, Webmail y Sistema de Gestión Académica.

5. ¿El servidor cuenta con seguridad lógica? ¿Con qué tipo?

Los tipos de seguridades lógicas con las que cuenta el servidor DNS son SSH y el firewall.

6. ¿Se monitorea el tráfico que recibe el servidor? ¿Con qué frecuencia?

El monitoreo del tráfico de red del servidor DNS se realiza constantemente, pero solo se revisa el historial cuando se produce algún incidente.

7. ¿Se ha detectado alguno de los siguientes ataques al servidor?

Suplantación del dominio	( )
Redirección del dominio	( )
Falsificación de la página	(X)
Interceptación de paquetes DNS	( )
Denegación del servicio	( )

8. ¿Cree conveniente la implementación de DNSSEC? ¿Por qué?

Por supuesto, porque permitiría dar una solución integral a los ataques concernientes al DNS, y podría formar parte del proyecto de seguridad perimetral que se está llevando a cabo en la universidad.

Anexo 4: Instalación y configuración del servidor DNS del sitio web de la Universidad Nacional de Loja.

Los pasos para instalar y configurar Bind fueron los siguientes:

1. Instalar el servidor DNS Bind9:

   # apt-get install bind9

Mediante este comando se puede observar la información en modo texto sobre los paquetes extra que serán instalados, los paquetes sugeridos para la instalación, los paquetes nuevos y las actualizaciones que serán realizadas en los paquetes existentes, tal como se muestra en la figura 35.

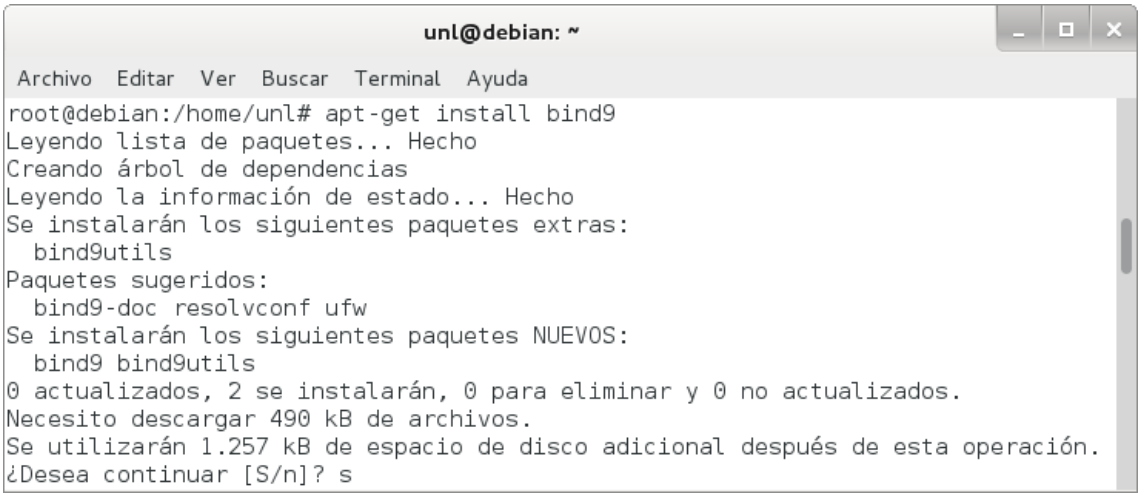

Figura 35. Instalación de Bind.

2. Modificar el archivo */etc/resolv.conf* para que el servidor resuelva las peticiones DNS:

   # nano /etc/resolv.conf

Donde se establece la dirección IP del servidor en el parámetro *nameserver,* como se muestra en la figura 36.

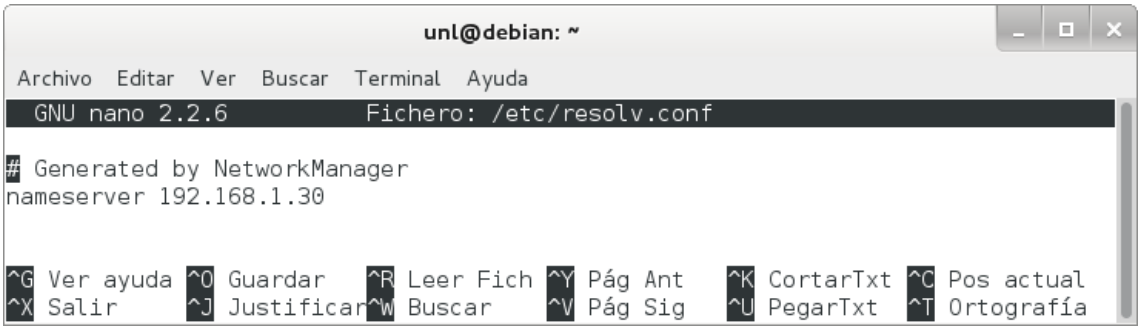

Figura 36. Archivo resolv.conf.

3. Editar el archivo */etc/bind/named.conf.local*:

 # nano /etc/bind/named.conf.local

Donde se asigna las zonas y el fichero en el que se encuentran, como se observa en la figura 37.

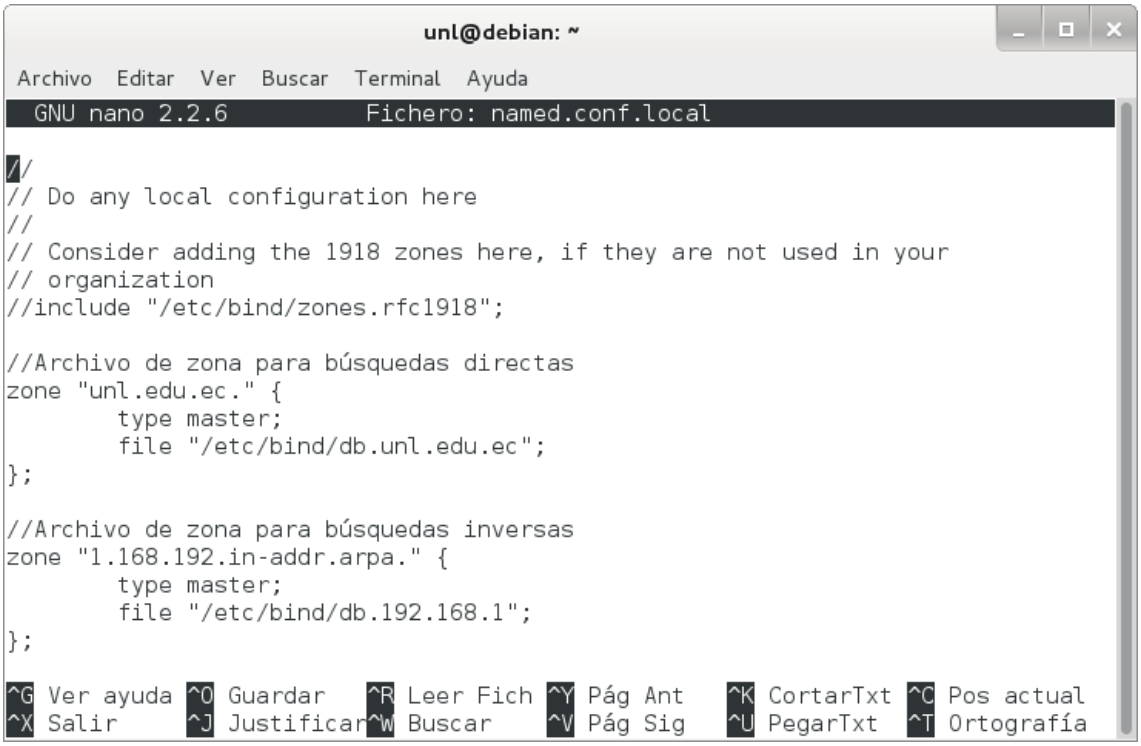

Figura 37. Archivo named.conf.local.

4. Para comprobar la sintaxis de los archivos de configuración ejecutamos el siguiente comando:

   # *named-checkconf*

Si no aparece nada, la sintaxis de los archivos de configuración es correcta, como se muestra en la figura 38.

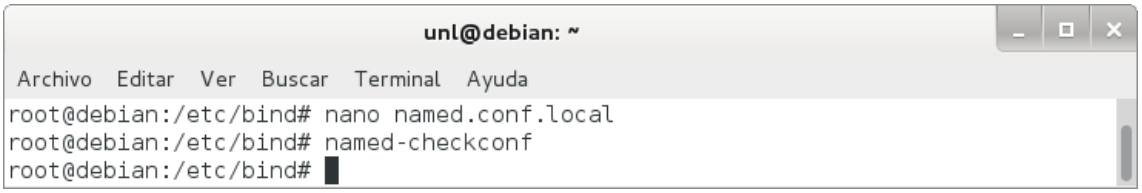

Figura 38. Ejecución de named-checkconf sin errores.

5. Crear el archivo */etc/bind/db.unl.edu.ec*:

   # *nano /etc/bind/db.unl.edu.ec*

Donde se configura la zona directa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 39.

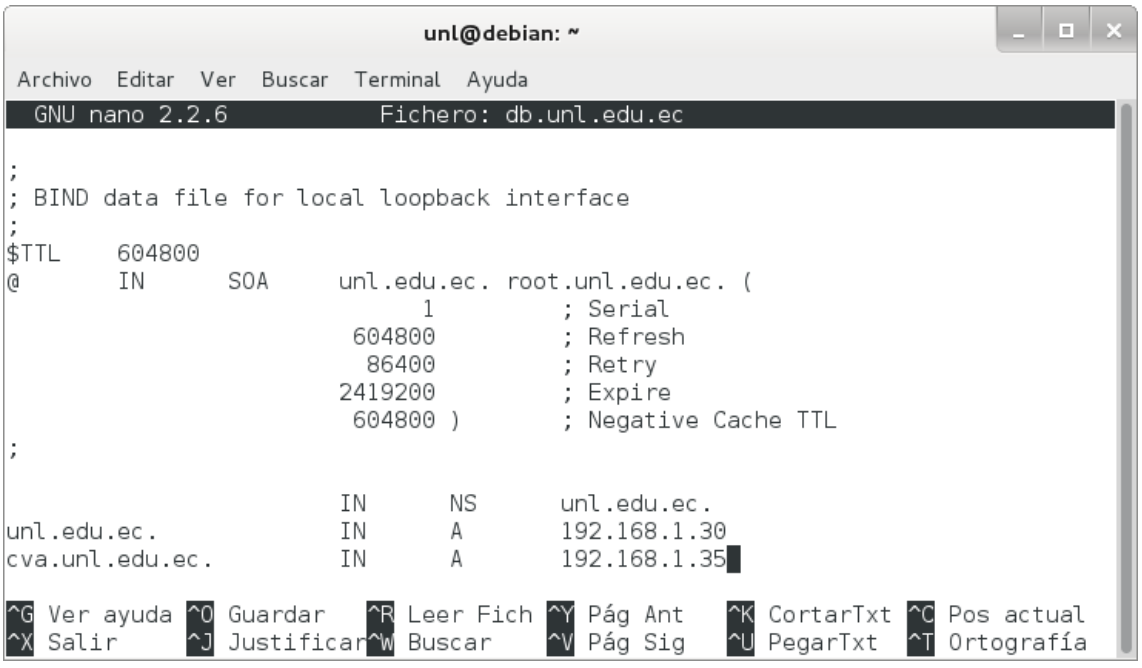

Figura 39. Archivo db.unl.edu.ec.

6. Comprobar la zona que se creó (*unl.edu.ec*):

 # named-checkzone unl.edu.ec. db.unl.edu.ec

Con lo que se comprueba que la zona está correctamente configurada, como se observa en la figura 40.

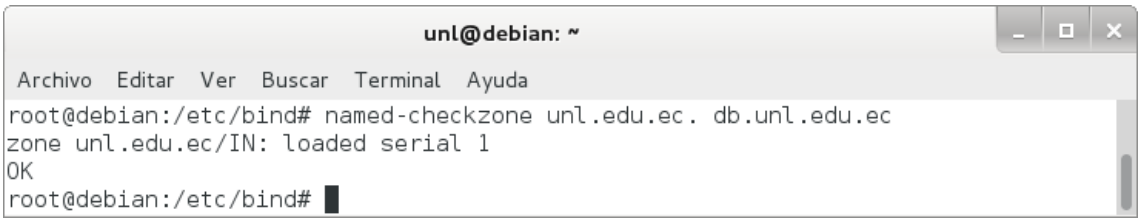

Figura 40. Ejecución de named-checkzone sin errores.

7. Crear el archivo */etc/bind/db.192.168.1*:

 # nano /etc/bind/db.192.168.1

Donde se configura la zona inversa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 41.

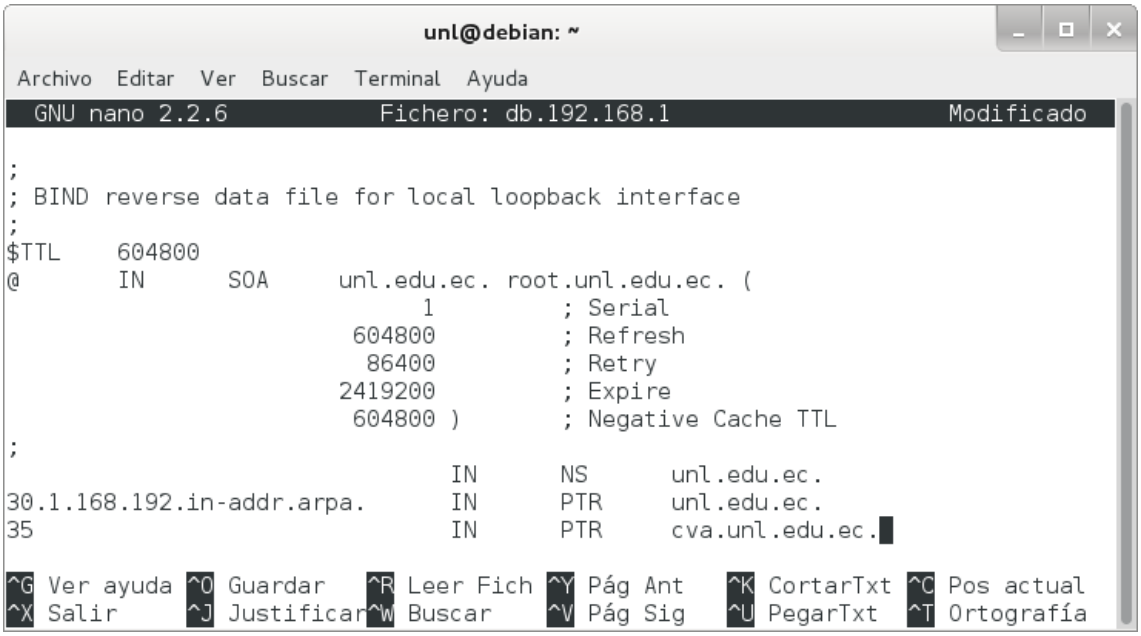

Figura 41. Archivo db.192.168.1.

8. Comprobar la zona inversa que se creó:

 # named-checkzone 1.168.192.in-addr.arpa db.192.168.1

Con lo que se comprueba que la zona inversa está correctamente configurada, como se observa en la figura 42.

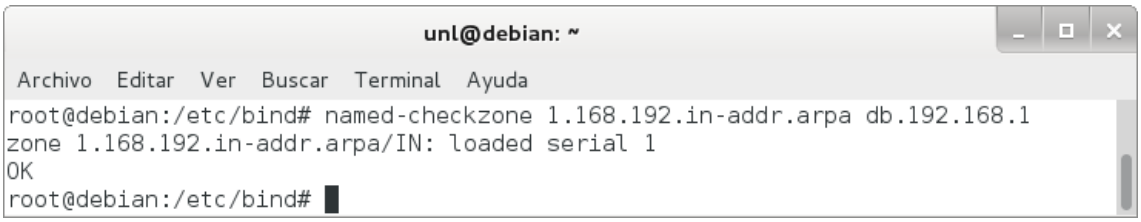

Figura 42. Ejecución de named-checkzone sin errores.

9. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 43.

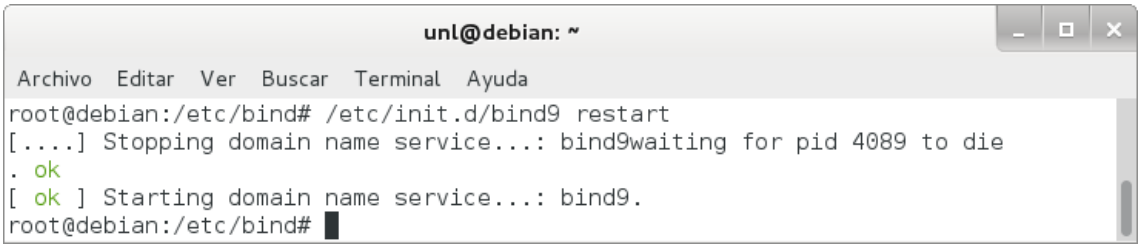

Figura 43. Reinicio del servicio.

10. Probar el servidor de nombres:

 # dig unl.edu.ec

La respuesta será parecida a como se muestra en la figura 44.

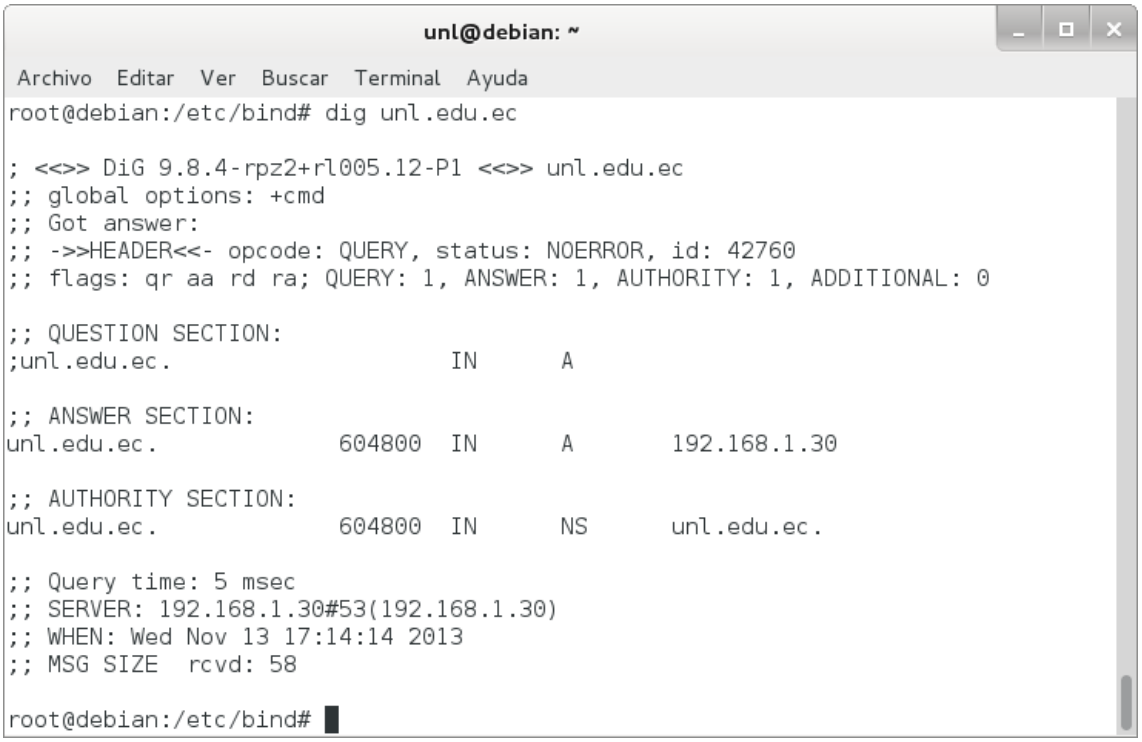

Figura 44. Ejecución de dig unl.edu.ec.

11. Probar la resolución inversa:

 # dig -x 192.168.1.30

La respuesta será parecida a como se muestra en la figura 45.

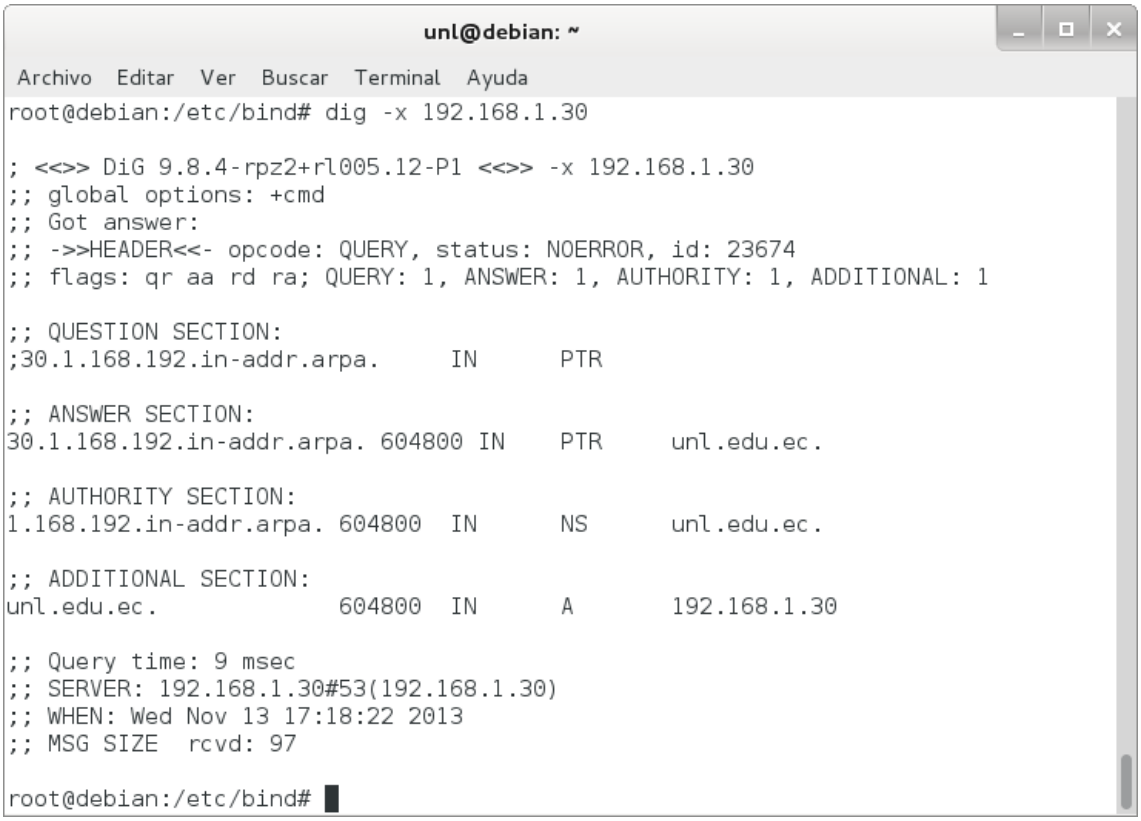

Figura 45. Ejecución de dig -x 192.168.1.30.

Anexo 5: Instalación y configuración del servidor DNS de la comunidad virtual de aprendizaje de la Universidad Nacional de Loja.

Los pasos para instalar y configurar Bind fueron los siguientes:

1. Instalar el servidor DNS Bind9:

   # apt-get install bind9

Mediante este comando se puede observar la información en modo texto sobre los paquetes extra que serán instalados, los paquetes sugeridos para la instalación, los paquetes nuevos y las actualizaciones que serán realizadas en los paquetes existentes, tal como se muestra en la figura 46.

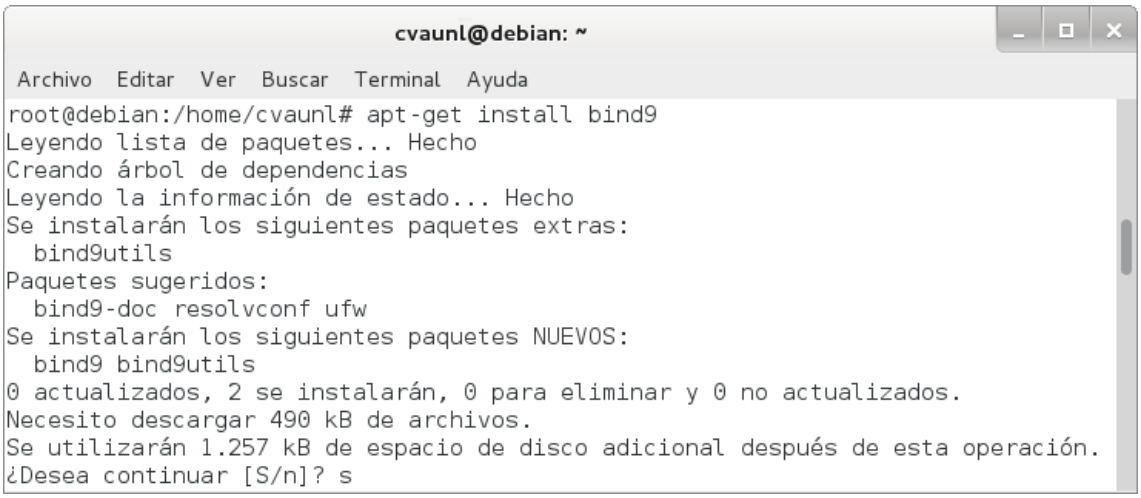

Figura 46. Instalación de Bind.

2. Modificar el archivo /etc/resolv.conf para que el servidor resuelva las peticiones DNS:

   # nano /etc/resolv.conf

Donde se establece la dirección IP del servidor en el parámetro nameserver, como se muestra en la figura 47.

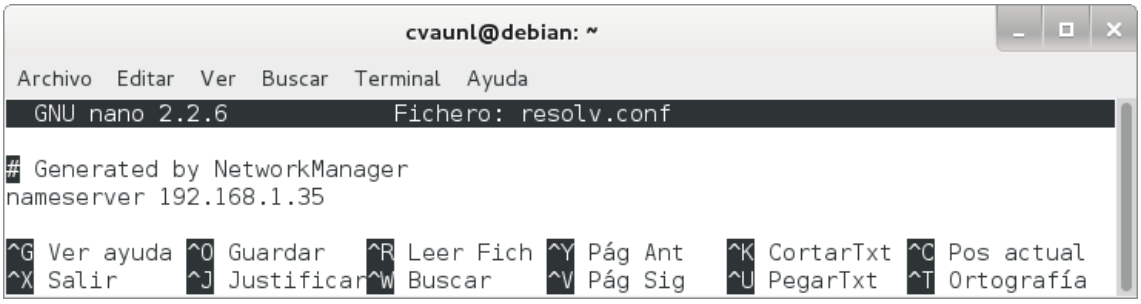

Figura 47. Archivo resolv.conf.

3. Editar el archivo /etc/bind/named.conf.local:

 # nano /etc/bind/named.conf.local

Donde se asigna las zonas y el fichero en el que se encuentran, como se observa en la figura 48.

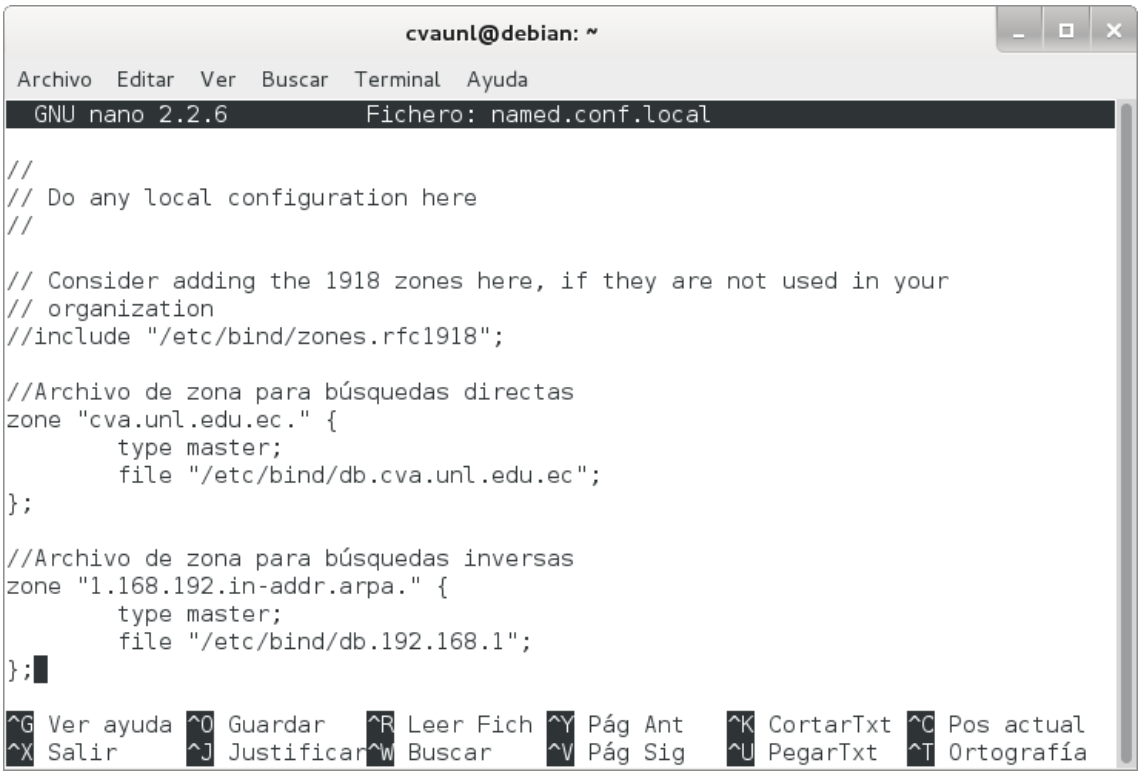

Figura 48. Archivo named.conf.local.

4. Para comprobar la sintaxis de los archivos de configuración ejecutamos el siguiente comando:

   # named-checkconf

Si no aparece nada, la sintaxis de los archivos de configuración es correcta, como se muestra en la figura 49.

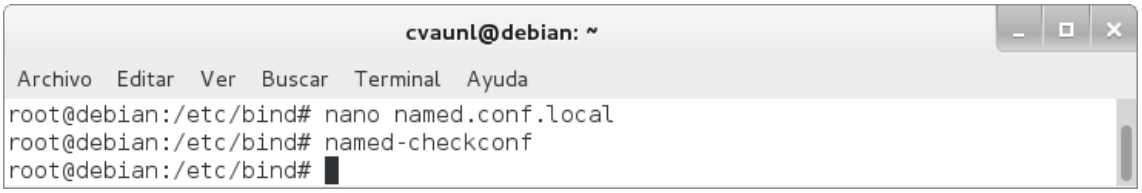

Figura 49. Ejecución de named-checkconf sin errores.

5. Crear el archivo /etc/bind/db.cva.unl.edu.ec:

   # nano /etc/bind/db.cva.unl.edu.ec

Donde se configura la zona directa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 50.

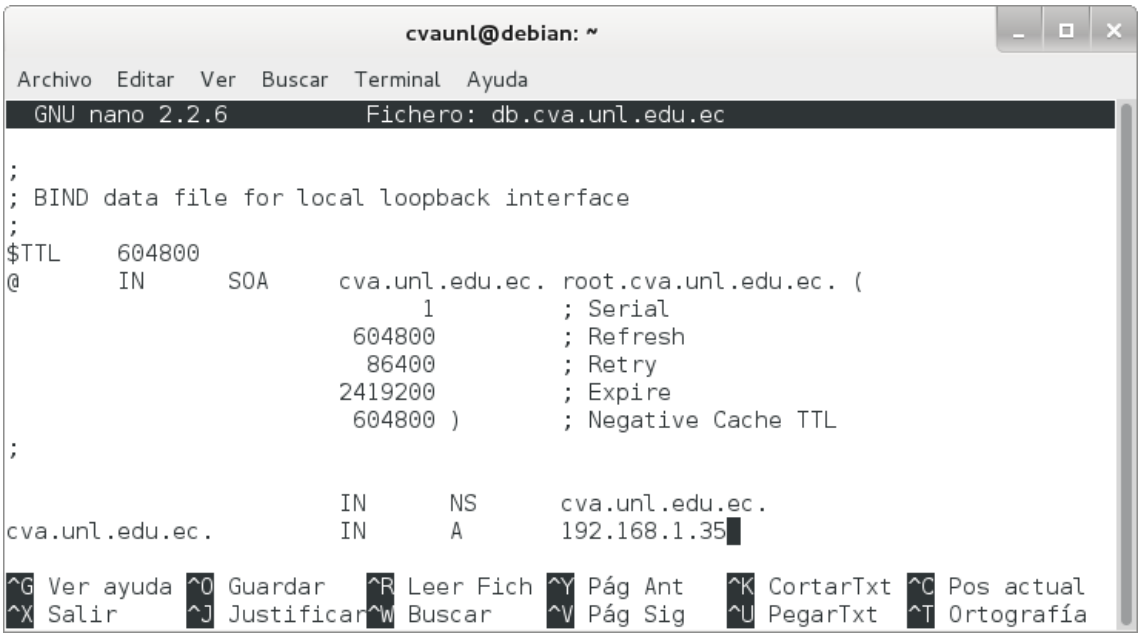

Figura 50. Archivo db.cva.unl.edu.ec.

6. Comprobar la zona que se creó (cva.unl.edu.ec):

 # named-checkzone cva.unl.edu.ec. db.cva.unl.edu.ec

Con lo que se comprueba que la zona está correctamente configurada, como se observa en la figura 51.

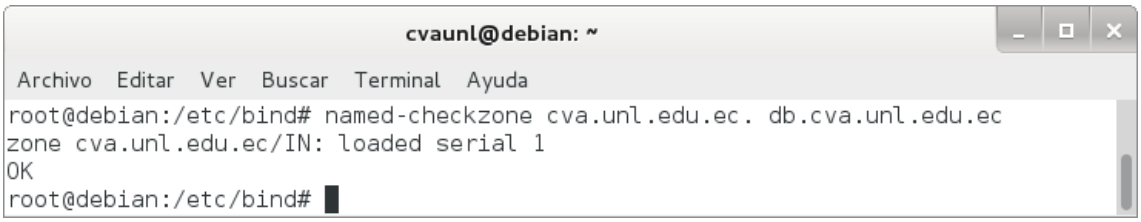

Figura 51. Ejecución de named-checkzone sin errores.

7. Crear el archivo /etc/bind/db.192.168.1:

 # nano /etc/bind/db.192.168.1

Donde se configura la zona inversa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 52.

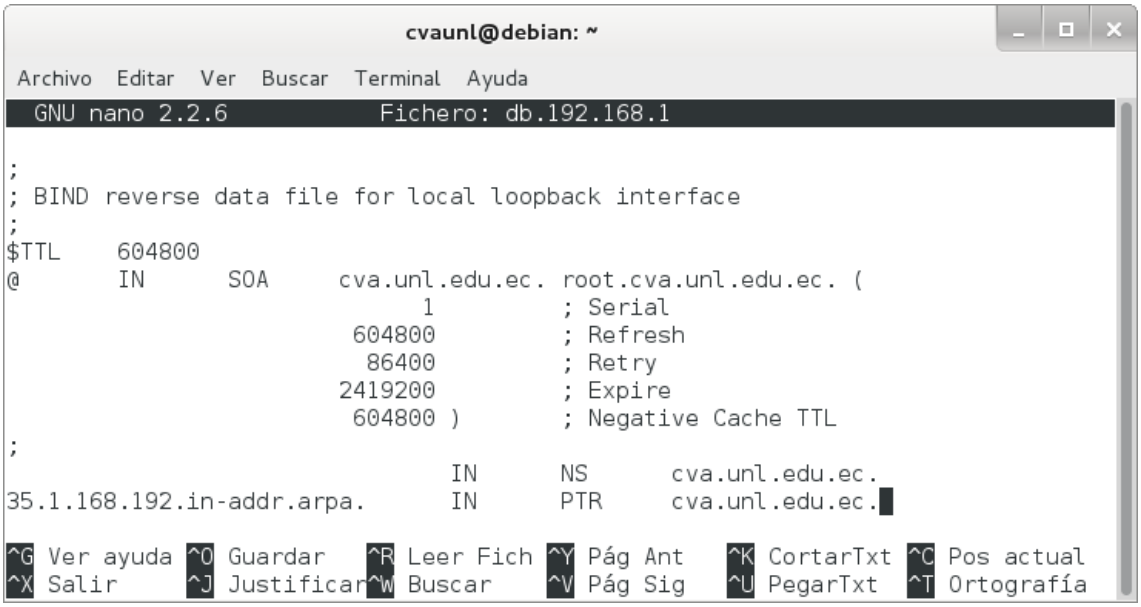

Figura 52. Archivo db.192.168.1.

8. Comprobar la zona inversa que se creó:

 # named-checkzone 1.168.192.in-addr.arpa db.192.168.1

Con lo que se comprueba que la zona inversa está correctamente configurada, como se observa en la figura 53.

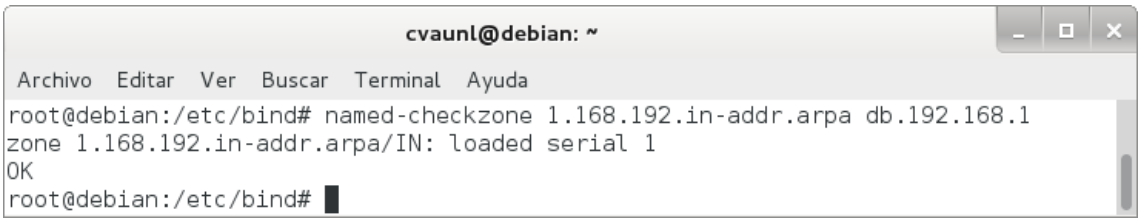

Figura 53. Ejecución de named-checkzone sin errores.

9. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 54.

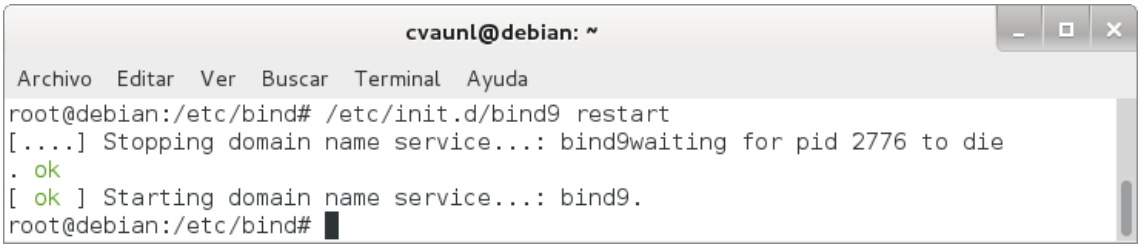

Figura 54. Reinicio del servicio.

10. Probar el servidor de nombres:

 # dig cva.unl.edu.ec

La respuesta será parecida a como se muestra en la figura 55.

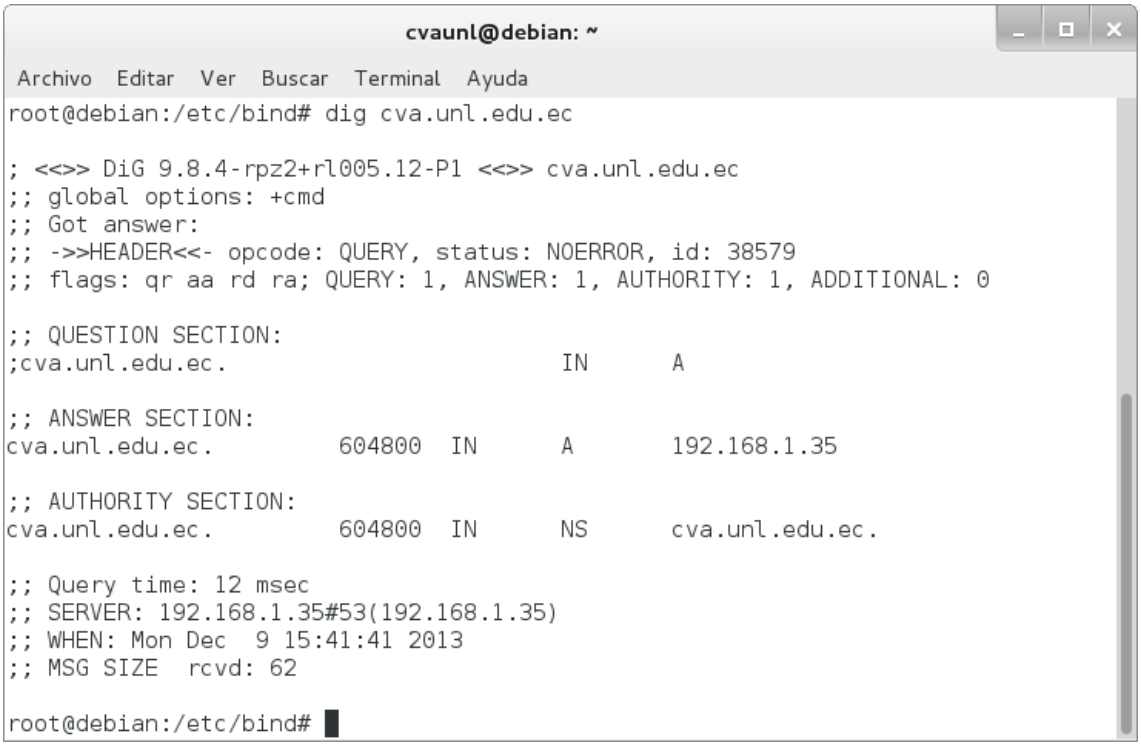

Figura 55. Ejecución de dig cva.unl.edu.ec.

11. Probar la resolución inversa:

    # dig -x 192.168.1.35

La respuesta será parecida a como se muestra en la figura 56.

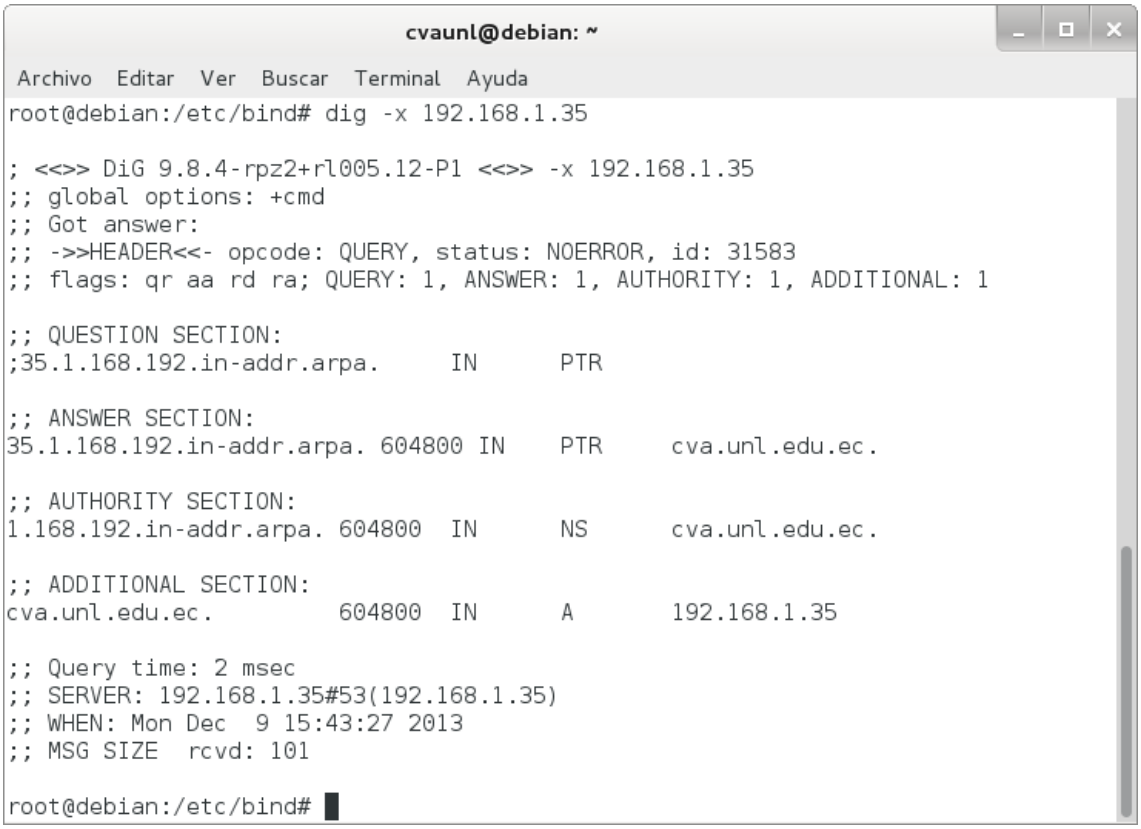

Figura 56. Ejecución de dig -x 192.168.1.35.

Anexo 6: Instalación y configuración del servidor DNS del sitio web de la Universidad Técnica Particular de Loja.

Los pasos para instalar y configurar Bind fueron los siguientes:

1. Instalar el servidor DNS Bind9:

   # apt-get install bind9

Mediante este comando se puede observar la información en modo texto sobre los paquetes extra que serán instalados, los paquetes sugeridos para la instalación, los paquetes nuevos y las actualizaciones que serán realizadas en los paquetes existentes, tal como se muestra en la figura 57.

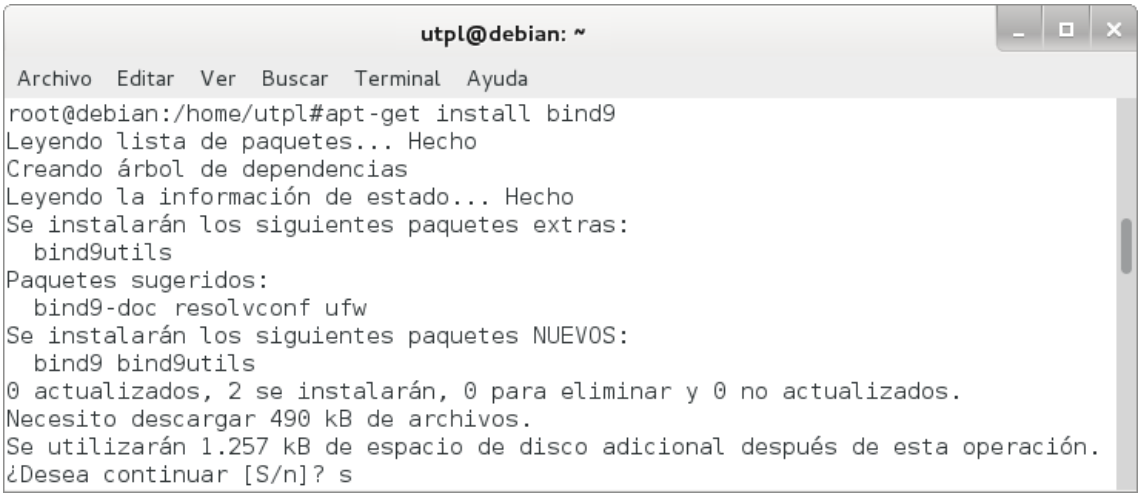

Figura 57. Instalación de Bind.

2. Modificar el archivo /etc/resolv.conf para que el servidor resuelva las peticiones DNS:

   # nano /etc/resolv.conf

Donde se establece la dirección IP del servidor en el parámetro nameserver, como se muestra en la figura 58.

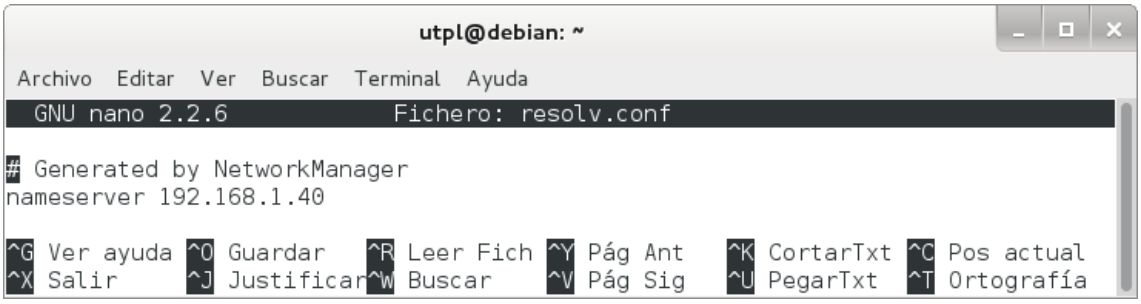

Figura 58. Archivo resolv.conf.

3. Editar el archivo /etc/bind/named.conf.local:

 # nano /etc/bind/named.conf.local

Donde se asigna las zonas y el fichero en el que se encuentran, como se observa en la figura 59.

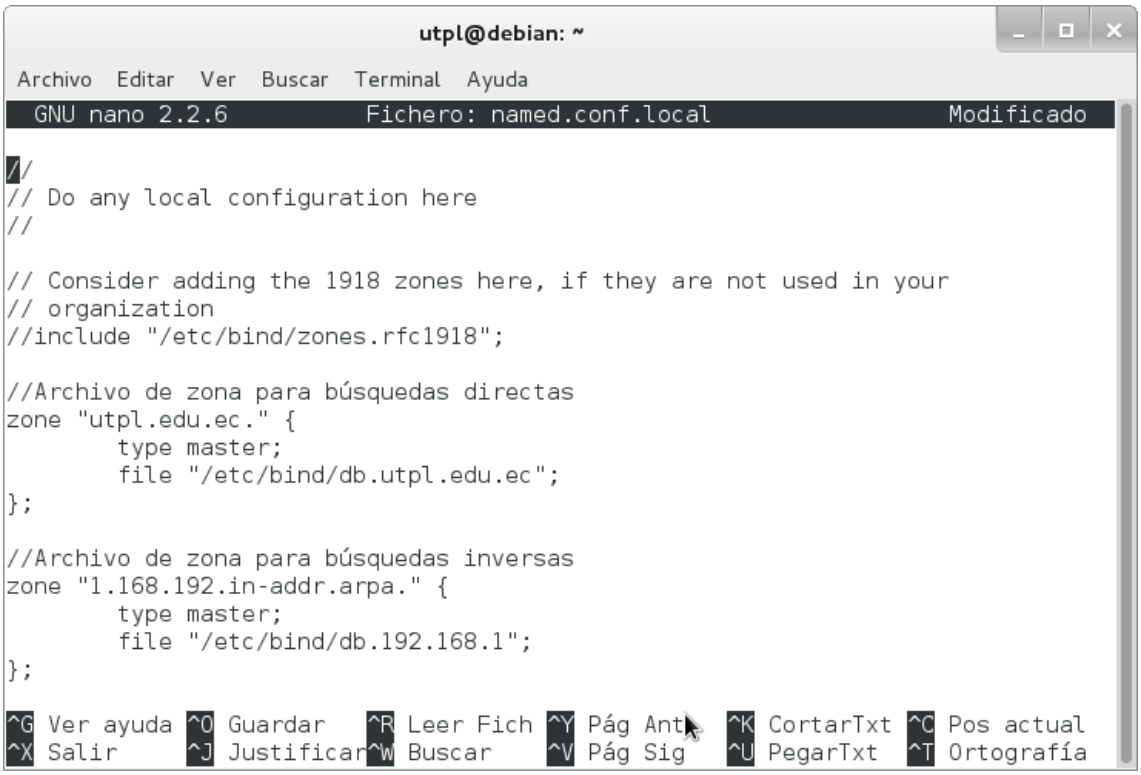

Figura 59. Archivo named.conf.local.

4. Para comprobar la sintaxis de los archivos de configuración ejecutamos el siguiente comando:

   # named-checkconf

Si no aparece nada, la sintaxis de los archivos de configuración es correcta, como se muestra en la figura 60.

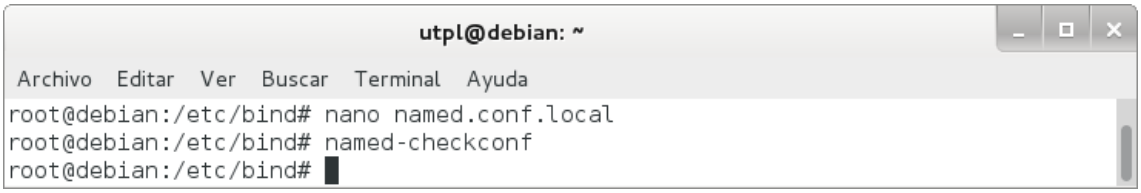

Figura 60. Ejecución de named-checkconf sin errores.

5. Crear el archivo /etc/bind/db.utpl.edu.ec:

   # nano /etc/bind/db.utpl.edu.ec

Donde se configura la zona directa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 61.

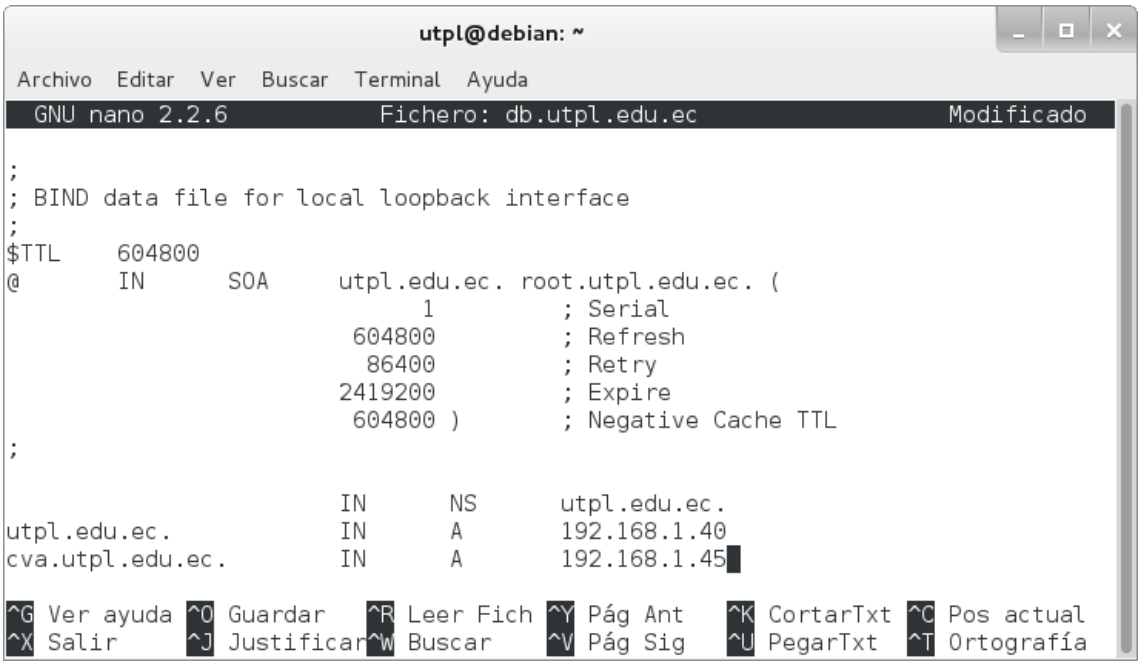

Figura 61. Archivo db.utpl.edu.ec.

6. Comprobar la zona que se creó (utpl.edu.ec):

 # named-checkzone utpl.edu.ec. db.utpl.edu.ec

Con lo que se comprueba que la zona está correctamente configurada, como se observa en la figura 62.

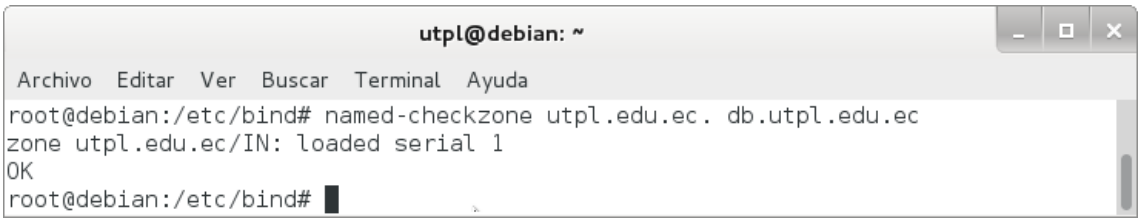

Figura 62. Ejecución de named-checkzone sin errores.

7. Crear el archivo /etc/bind/db.192.168.1:

 # nano /etc/bind/db.192.168.1

Donde se configura la zona inversa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 63.

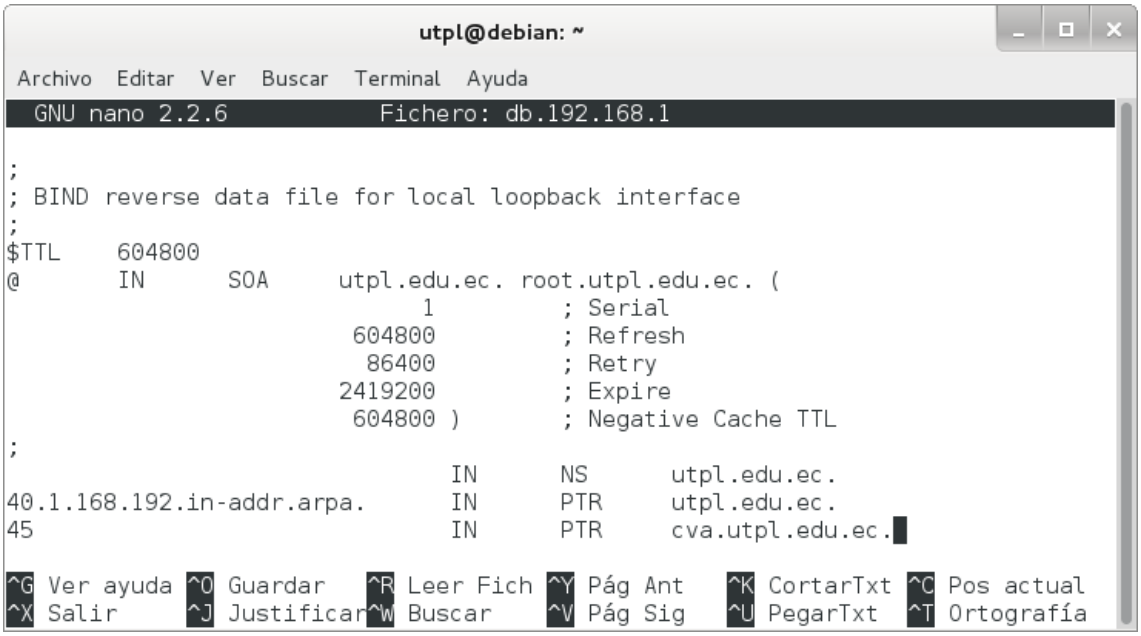

Figura 63. Archivo db.192.168.1.

8. Comprobar la zona inversa que se creó:

 # named-checkzone 1.168.192.in-addr.arpa db.192.168.1

Con lo que se comprueba que la zona inversa está correctamente configurada, como se observa en la figura 64.

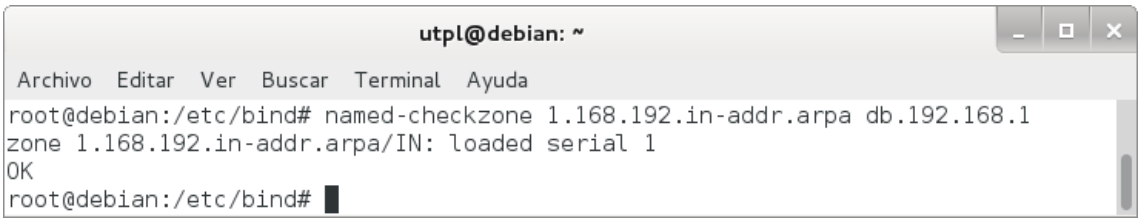

Figura 64. Ejecución de named-checkzone sin errores.

9. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 65.

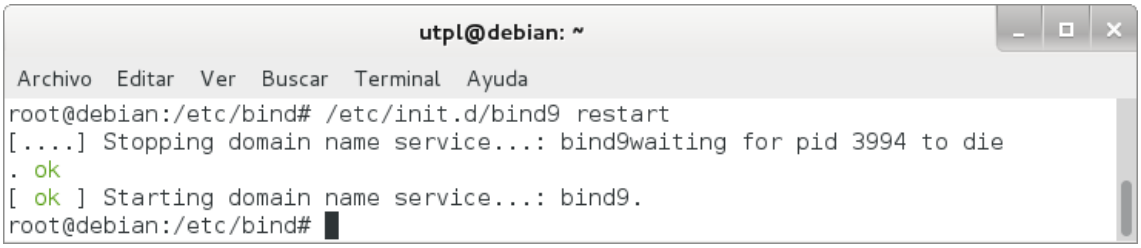

Figura 65. Reinicio del servicio.

10. Probar el servidor de nombres:

 # dig utpl.edu.ec

La respuesta será parecida a como se muestra en la figura 66.

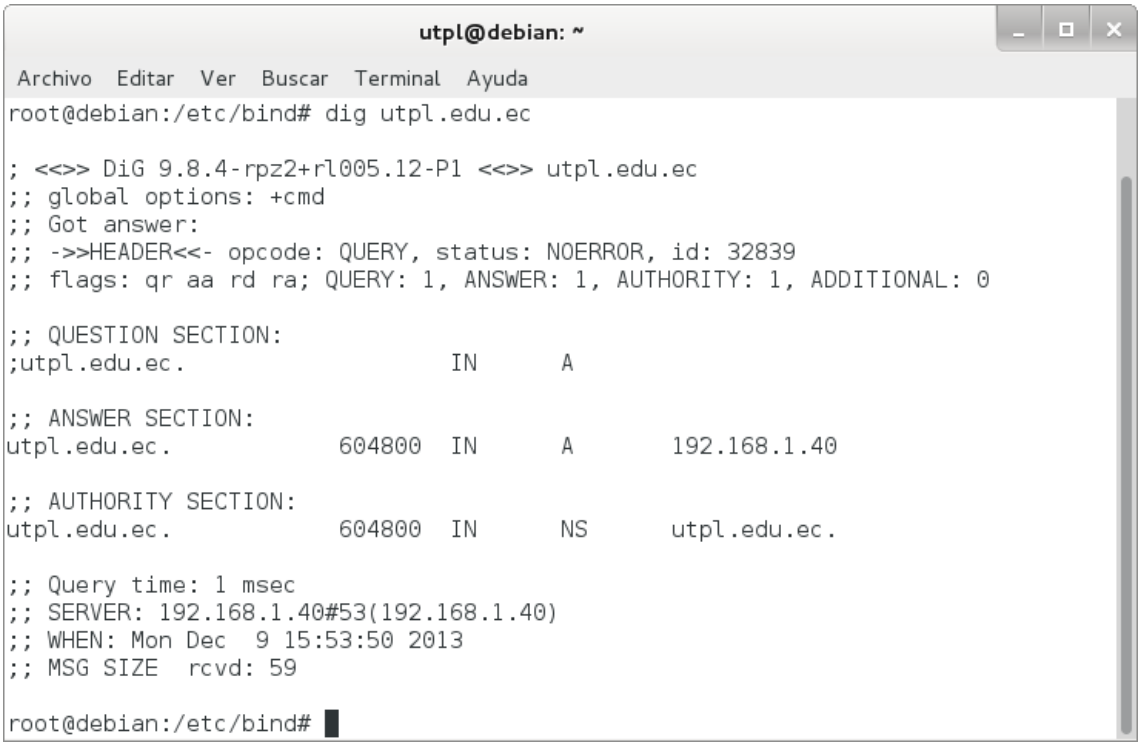

Figura 66. Ejecución de dig utpl.edu.ec.

11. Probar la resolución inversa:

    # dig -x 192.168.1.40

La respuesta será parecida a como se muestra en la figura 67.

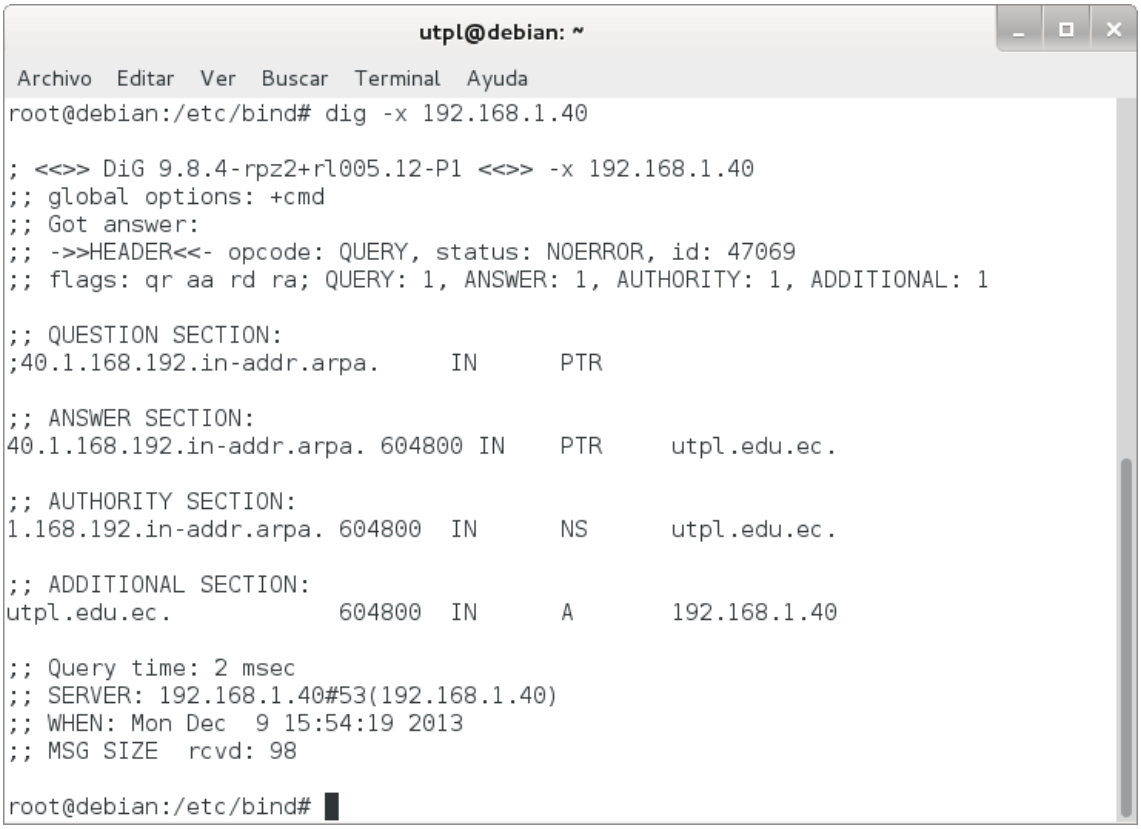

Figura 67. Ejecución de dig -x 192.168.1.40.

Anexo 7: Instalación y configuración del servidor DNS de la comunidad virtual de aprendizaje de la Universidad Técnica Particular de Loja.

Los pasos para instalar y configurar Bind fueron los siguientes:

1. Instalar el servidor DNS Bind9:

   # apt-get install bind9

Mediante este comando se puede observar la información en modo texto sobre los paquetes extra que serán instalados, los paquetes sugeridos para la instalación, los paquetes nuevos y las actualizaciones que serán realizadas en los paquetes existentes, tal como se muestra en la figura 68.

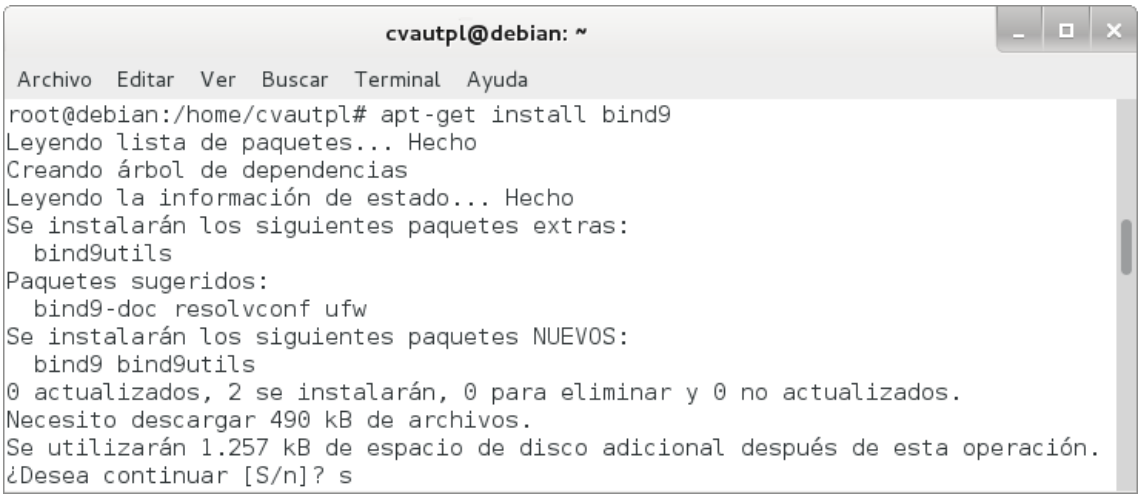

Figura 68. Instalación de Bind.

2. Modificar el archivo /etc/resolv.conf para que el servidor resuelva las peticiones DNS:

   # nano /etc/resolv.conf

Donde se establece la dirección IP del servidor en el parámetro nameserver, como se muestra en la figura 69.

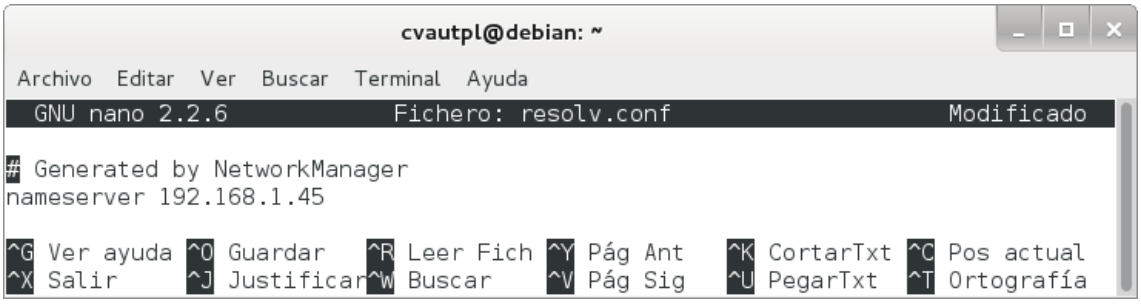

Figura 69. Archivo resolv.conf.

3. Editar el archivo /etc/bind/named.conf.local:

 # nano /etc/bind/named.conf.local

Donde se asigna las zonas y el fichero en el que se encuentran, como se observa en la figura 70.

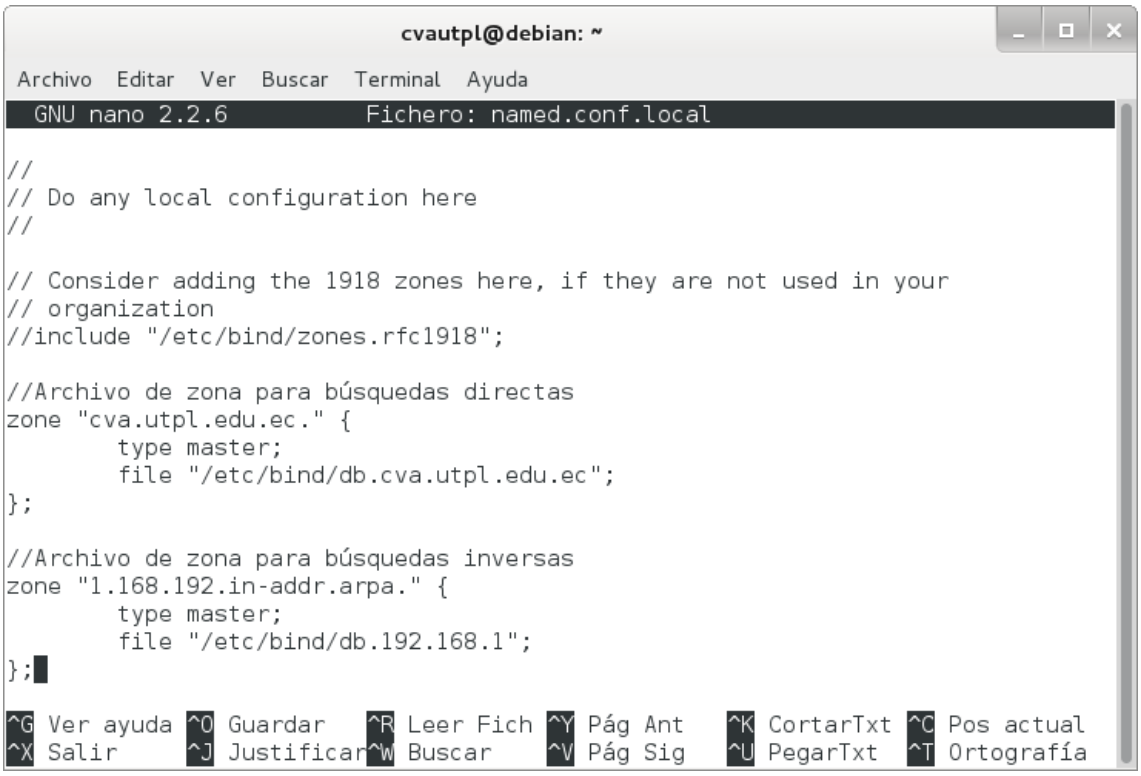

Figura 70. Archivo named.conf.local.

4. Para comprobar la sintaxis de los archivos de configuración ejecutamos el siguiente comando:

   # named-checkconf

Si no aparece nada, la sintaxis de los archivos de configuración es correcta, como se muestra en la figura 71.

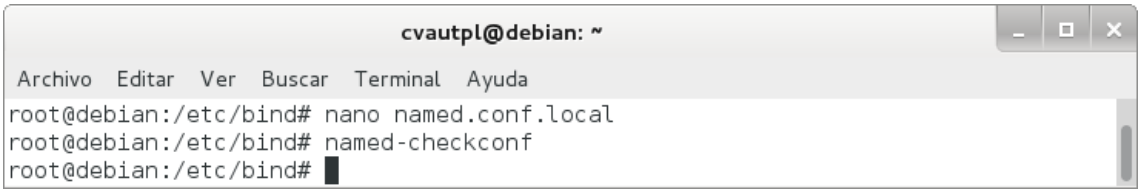

Figura 71. Ejecución de named-checkconf sin errores.

5. Crear el archivo /etc/bind/db.cva.utpl.edu.ec:

   # nano /etc/bind/db.cva.utpl.edu.ec

Donde se configura la zona directa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 72.

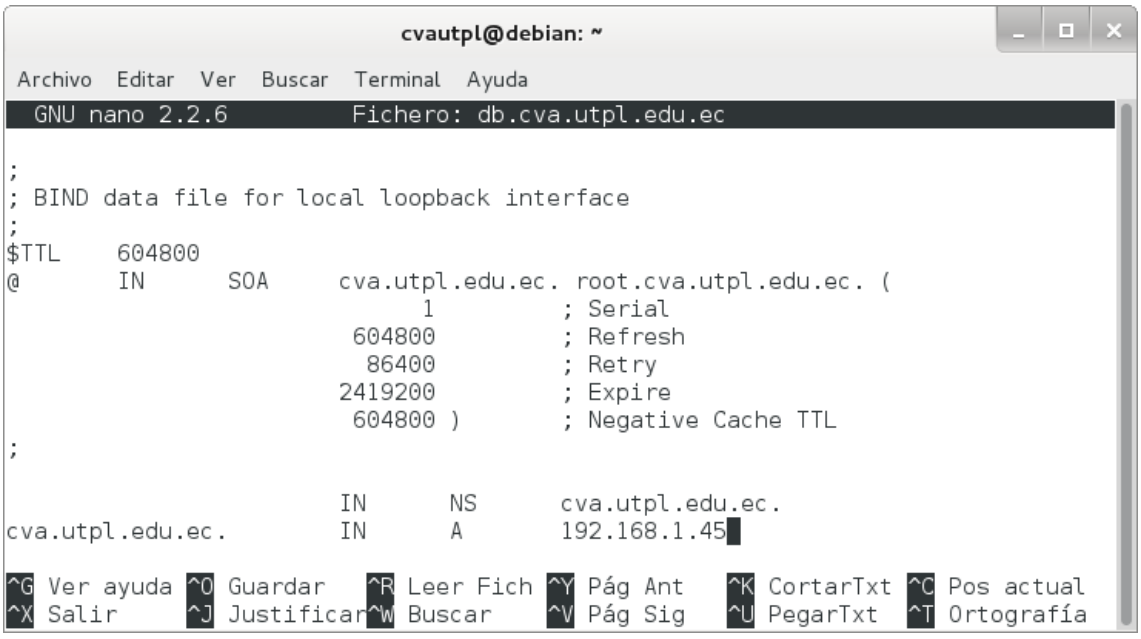

Figura 72. Archivo db.cva.utpl.edu.ec.

6. Comprobar la zona que se creó (cva.utpl.edu.ec):

 # named-checkzone cva.utpl.edu.ec. cva.db.utpl.edu.ec

Con lo que se comprueba que la zona está correctamente configurada, como se observa en la figura 73.

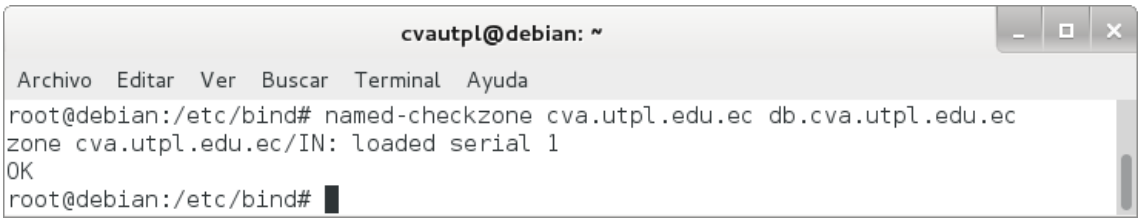

Figura 73. Ejecución de named-checkzone sin errores.

7. Crear el archivo /etc/bind/db.192.168.1:

 # nano /etc/bind/db.192.168.1

Donde se configura la zona inversa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 74.

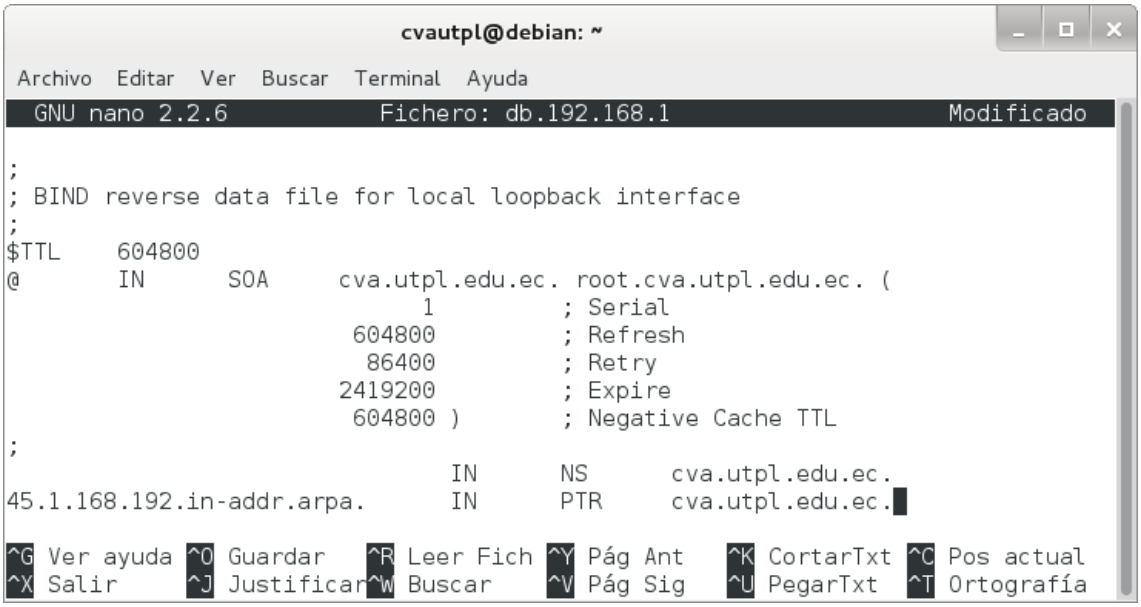

Figura 74. Archivo db.192.168.1.

8. Comprobar la zona inversa que se creó:

 # named-checkzone 1.168.192.in-addr.arpa db.192.168.1

Con lo que se comprueba que la zona inversa está correctamente configurada, como se observa en la figura 75.

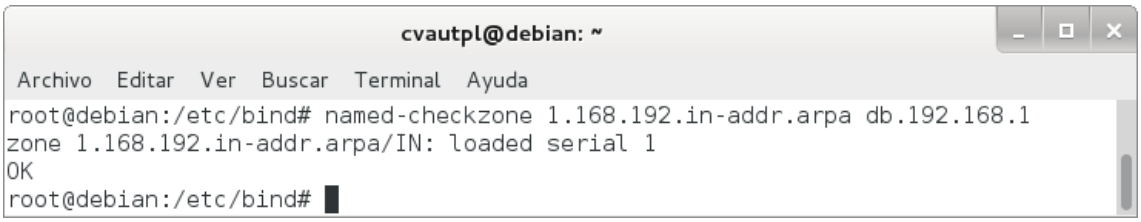

Figura 75. Ejecución de named-checkzone sin errores.

9. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 76.

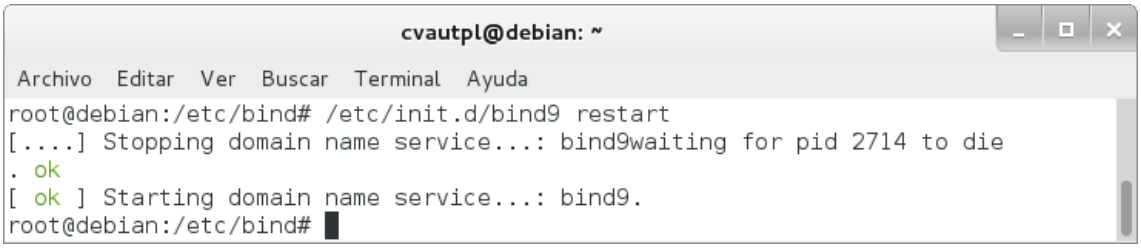

Figura 76. Reinicio del servicio.

10. Probar el servidor de nombres:

 # dig cva.utpl.edu.ec

La respuesta será parecida a como se muestra en la figura 77.

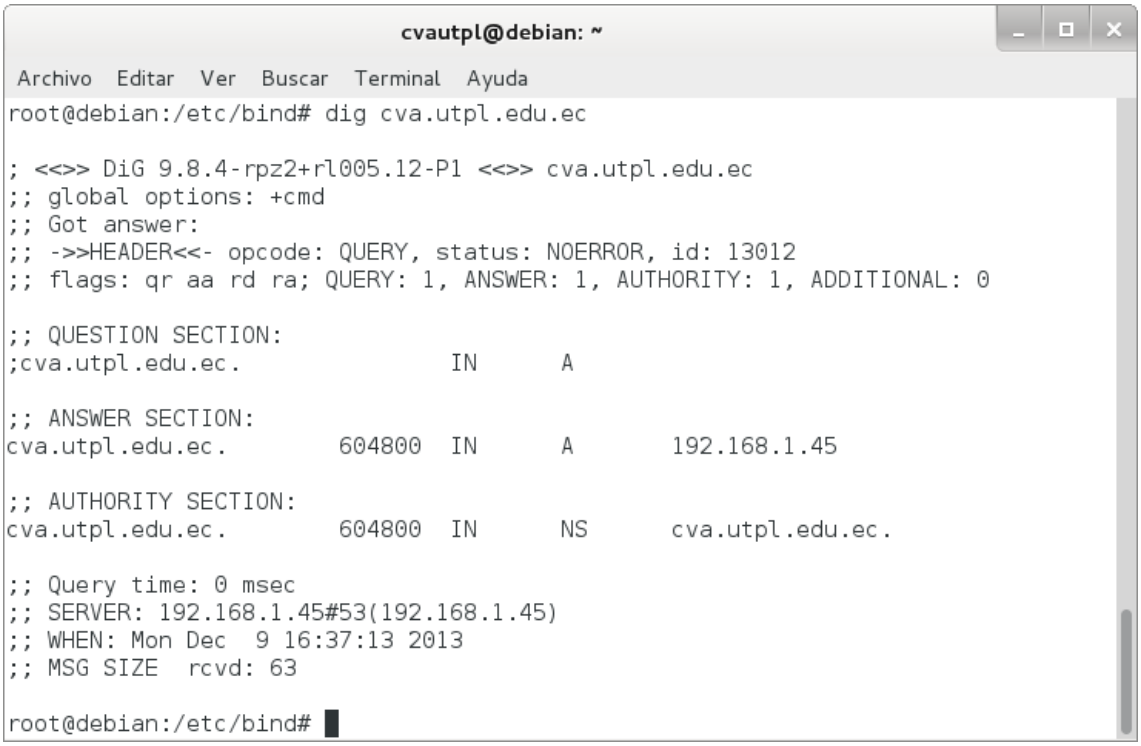

Figura 77. Ejecución de dig cva.utpl.edu.ec.

11. Probar la resolución inversa:

    # dig -x 192.168.1.45

La respuesta será parecida a como se muestra en la figura 78.

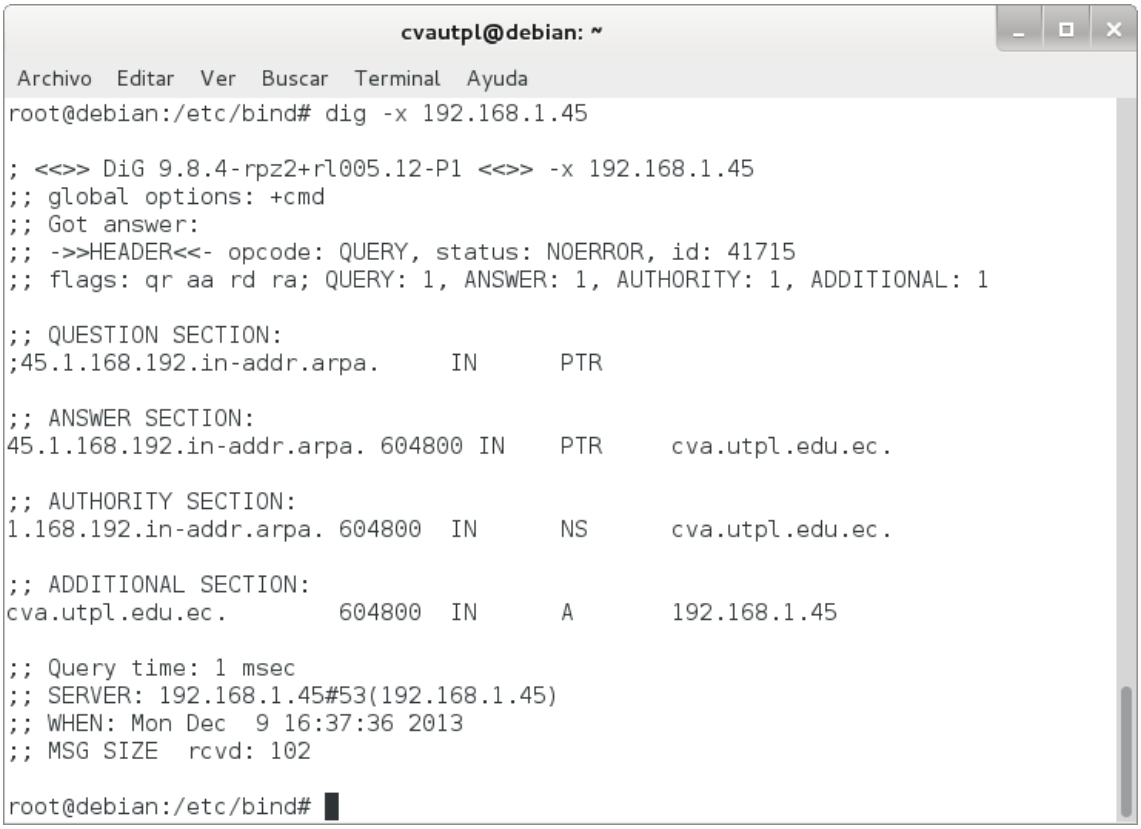

Figura 78. Ejecución de dig -x 192.168.1.45.

Anexo 8: Instalación y configuración del servidor DNS del sitio web de la Escuela Superior Politécnica del Litoral.

Los pasos para instalar y configurar Bind fueron los siguientes:

1. Instalar el servidor DNS Bind9:

   # apt-get install bind9

Mediante este comando se puede observar la información en modo texto sobre los paquetes extra que serán instalados, los paquetes sugeridos para la instalación, los paquetes nuevos y las actualizaciones que serán realizadas en los paquetes existentes, tal como se muestra en la figura 79.

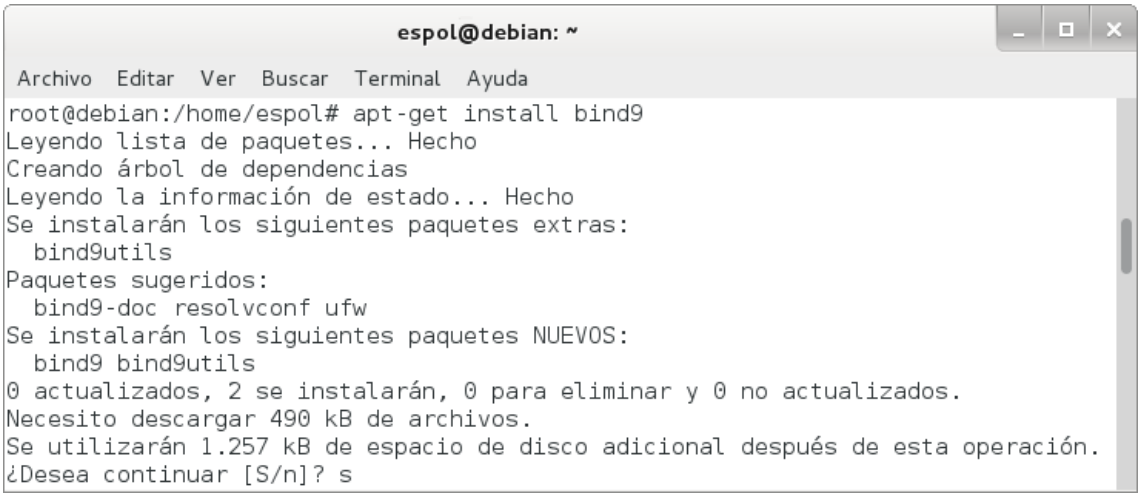

Figura 79. Instalación de Bind.

2. Modificar el archivo /etc/resolv.conf para que el servidor resuelva las peticiones DNS:

   # nano /etc/resolv.conf

Donde se establece la dirección IP del servidor en el parámetro nameserver, como se muestra en la figura 80.

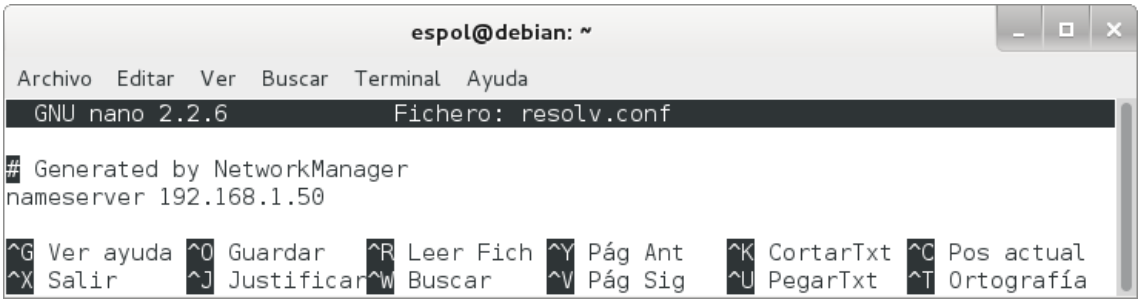

Figura 80. Archivo resolv.conf.

3. Editar el archivo /etc/bind/named.conf.local:

 # nano /etc/bind/named.conf.local

Donde se asigna las zonas y el fichero en el que se encuentran, como se observa en la figura 81.

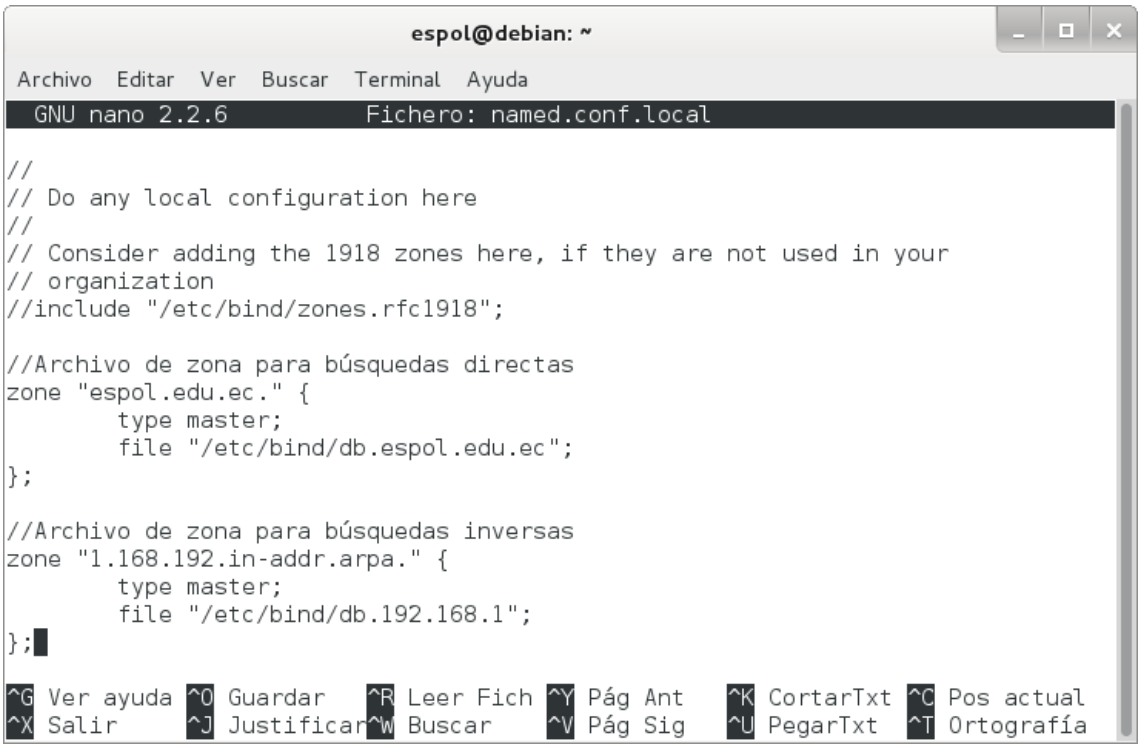

Figura 81. Archivo named.conf.local.

4. Para comprobar la sintaxis de los archivos de configuración ejecutamos el siguiente comando:

   # named-checkconf

Si no aparece nada, la sintaxis de los archivos de configuración es correcta, como se muestra en la figura 82.

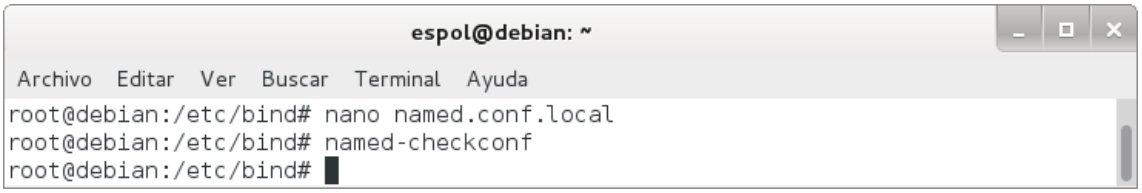

Figura 82. Ejecución de named-checkconf sin errores.

5. Crear el archivo /etc/bind/db.espol.edu.ec:

   # nano /etc/bind/db.espol.edu.ec

Donde se configura la zona directa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 83.

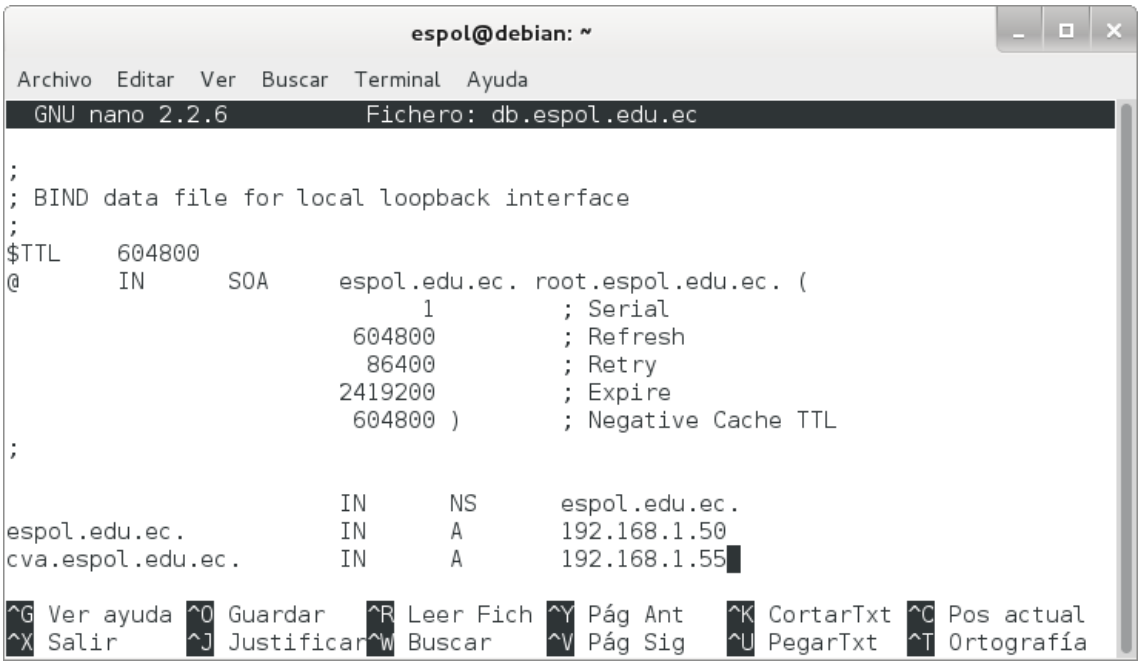

Figura 83. Archivo db.espol.edu.ec.

6. Comprobar la zona que se creó (espol.edu.ec):

 # named-checkzone espol.edu.ec. db.espol.edu.ec

Con lo que se comprueba que la zona está correctamente configurada, como se observa en la figura 84.

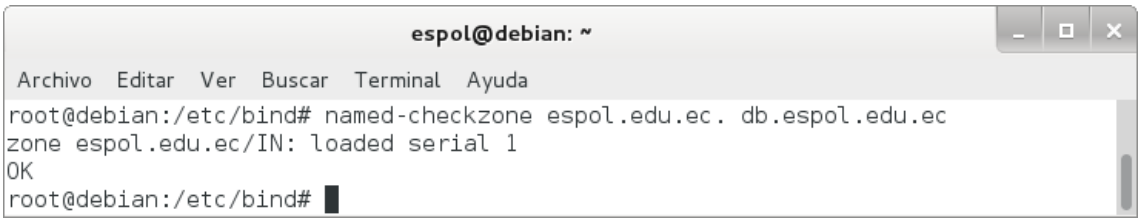

Figura 84. Ejecución de named-checkzone sin errores.

7. Crear el archivo /etc/bind/db.192.168.1:

 # nano /etc/bind/db.192.168.1

Donde se configura la zona inversa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 85.

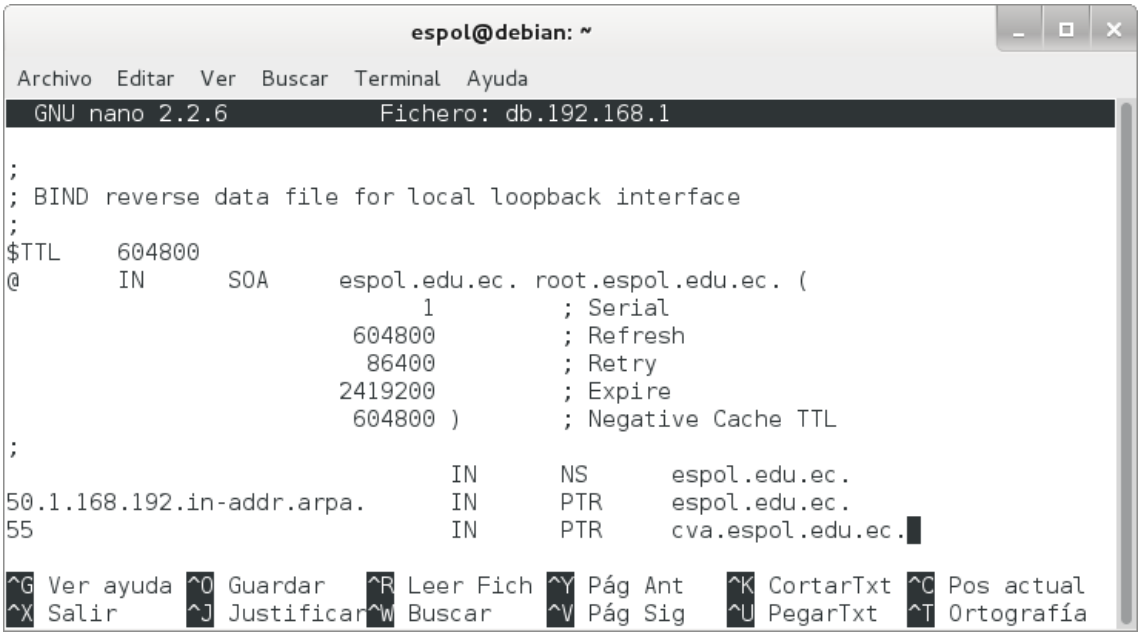

Figura 85. Archivo db.192.168.1.

8. Comprobar la zona inversa que se creó:

 # named-checkzone 1.168.192.in-addr.arpa db.192.168.1

Con lo que se comprueba que la zona inversa está correctamente configurada, como se observa en la figura 86.

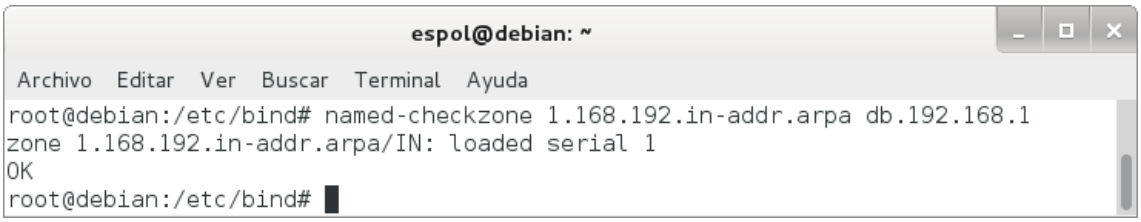

Figura 86. Ejecución de named-checkzone sin errores.

9. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 87.

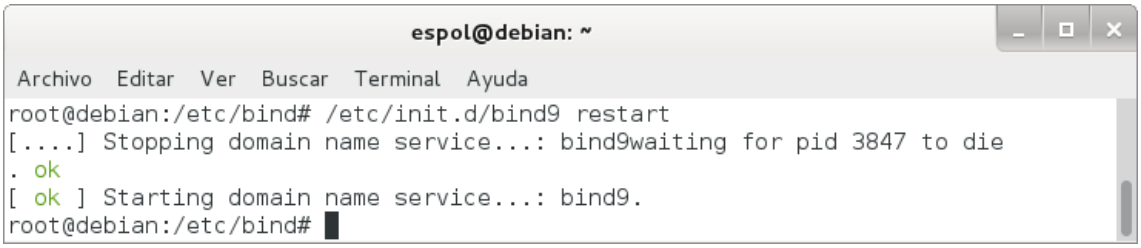

Figura 87. Reinicio del servicio.

10. Probar el servidor de nombres:

 # dig espol.edu.ec

La respuesta será parecida a como se muestra en la figura 88.

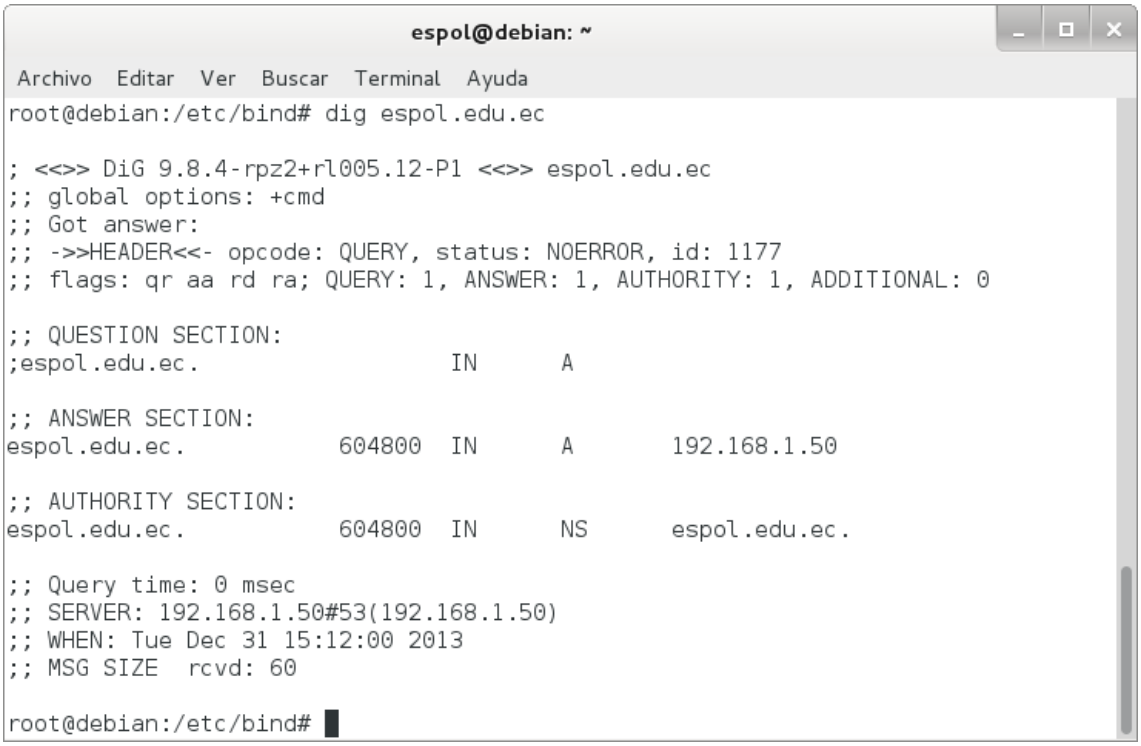

Figura 88. Ejecución de dig espol.edu.ec.

11. Probar la resolución inversa:

    # dig -x 192.168.1.50

La respuesta será parecida a como se muestra en la figura 89.

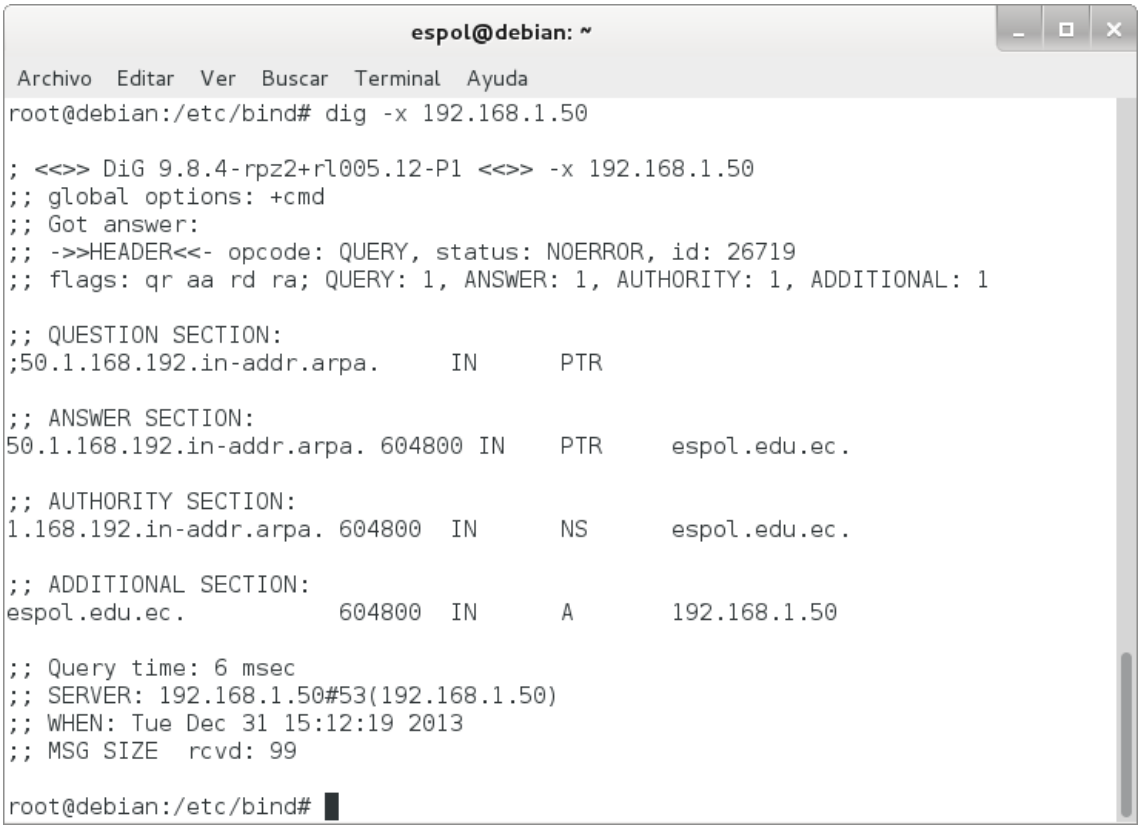

Figura 89. Ejecución de dig -x 192.168.1.50.

Anexo 9: Instalación y configuración del servidor DNS de la comunidad virtual de aprendizaje de la Escuela Superior Politécnica del Litoral.

Los pasos para instalar y configurar Bind fueron los siguientes:

1. Instalar el servidor DNS Bind9:

   # apt-get install bind9

Mediante este comando se puede observar la información en modo texto sobre los paquetes extra que serán instalados, los paquetes sugeridos para la instalación, los paquetes nuevos y las actualizaciones que serán realizadas en los paquetes existentes, tal como se muestra en la figura 90.

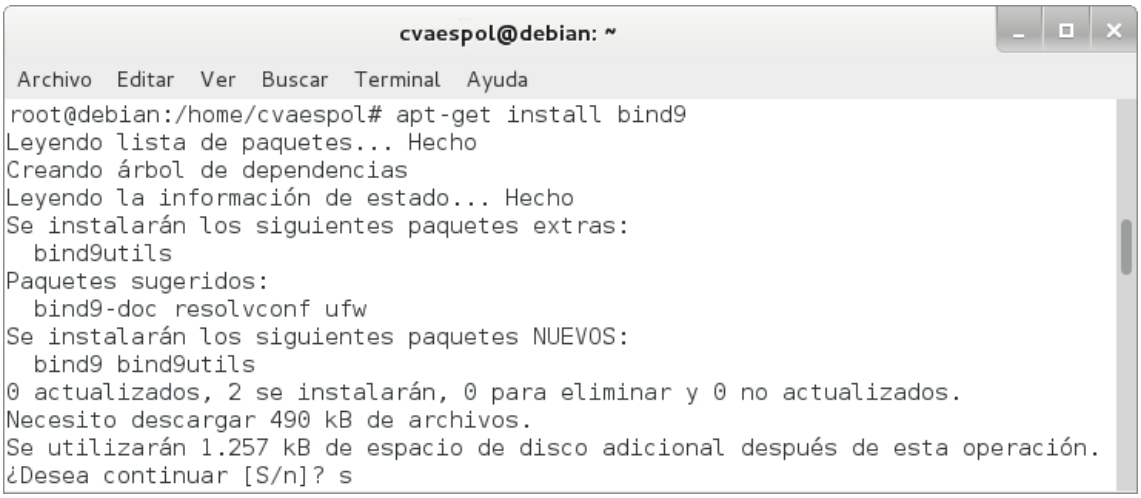

Figura 90. Instalación de Bind.

2. Modificar el archivo /etc/resolv.conf para que el servidor resuelva las peticiones DNS:

   # nano /etc/resolv.conf

Donde se establece la dirección IP del servidor en el parámetro nameserver, como se muestra en la figura 91.

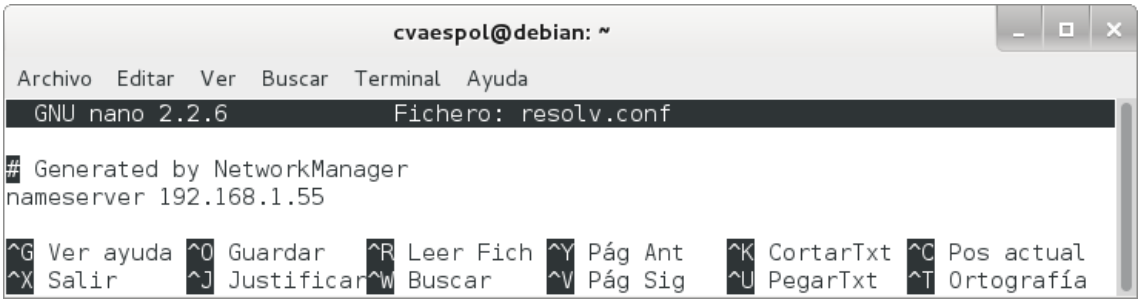

Figura 91. Archivo resolv.conf.

3. Editar el archivo /etc/bind/named.conf.local:

 # nano /etc/bind/named.conf.local

Donde se asigna las zonas y el fichero en el que se encuentran, como se observa en la figura 92.

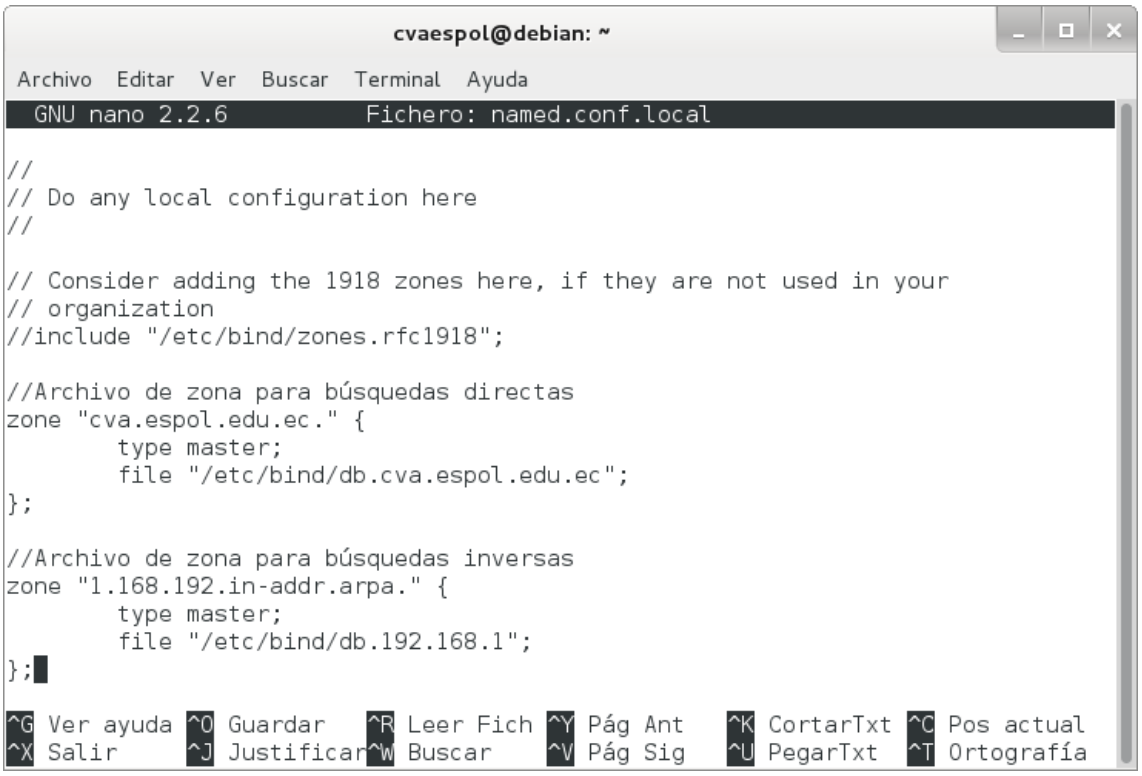

Figura 92. Archivo named.conf.local.

4. Para comprobar la sintaxis de los archivos de configuración ejecutamos el siguiente comando:

   # named-checkconf

Si no aparece nada, la sintaxis de los archivos de configuración es correcta, como se muestra en la figura 93.

Figura 93. Ejecución de named-checkconf sin errores.

5. Crear el archivo /etc/bind/db.cva.espol.edu.ec:

   # nano /etc/bind/db.cva.espol.edu.ec

Donde se configura la zona directa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 94.

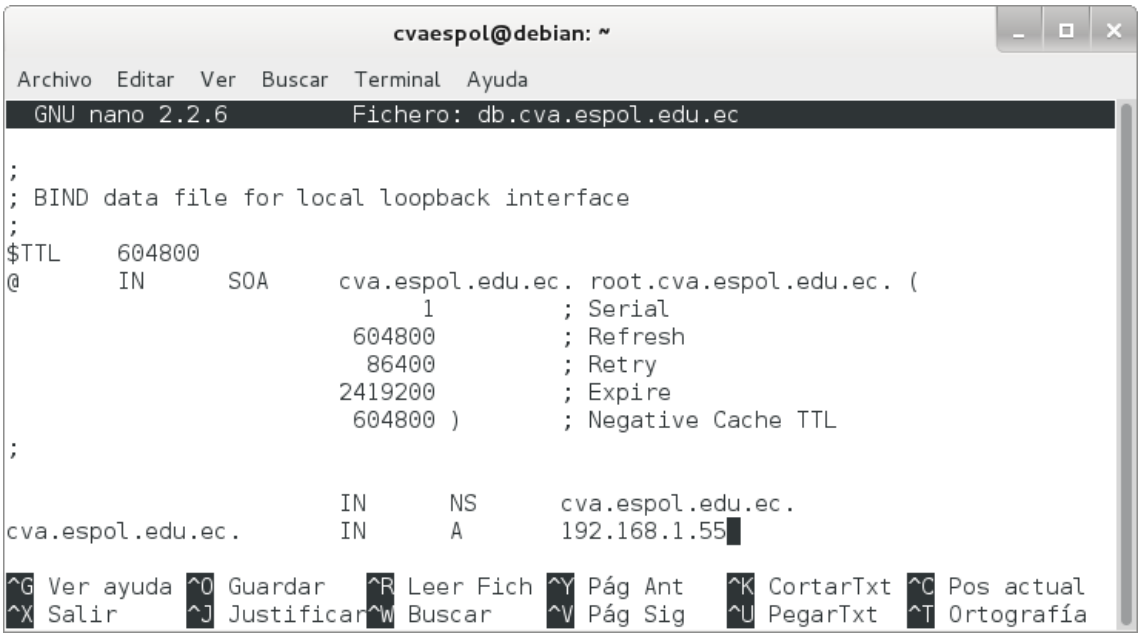

Figura 94. Archivo db.cva.espol.edu.ec.

6. Comprobar la zona que se creó (cva.espol.edu.ec):

 # named-checkzone cva.espol.edu.ec. db.cva.espol.edu.ec

Con lo que se comprueba que la zona está correctamente configurada, como se observa en la figura 95.

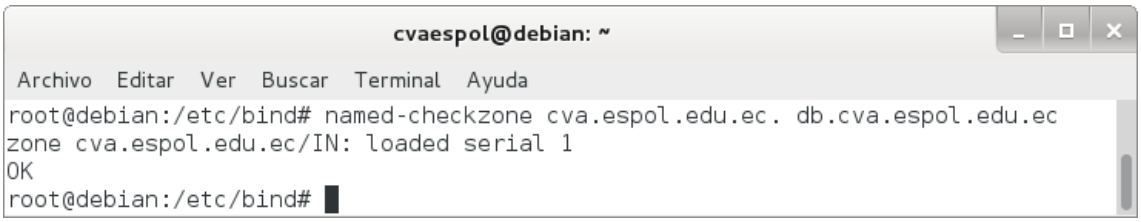

Figura 95. Ejecución de named-checkzone sin errores.

7. Crear el archivo /etc/bind/db.192.168.1:

 # nano /etc/bind/db.192.168.1

Donde se configura la zona inversa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs; tal como se observa en la figura 96.

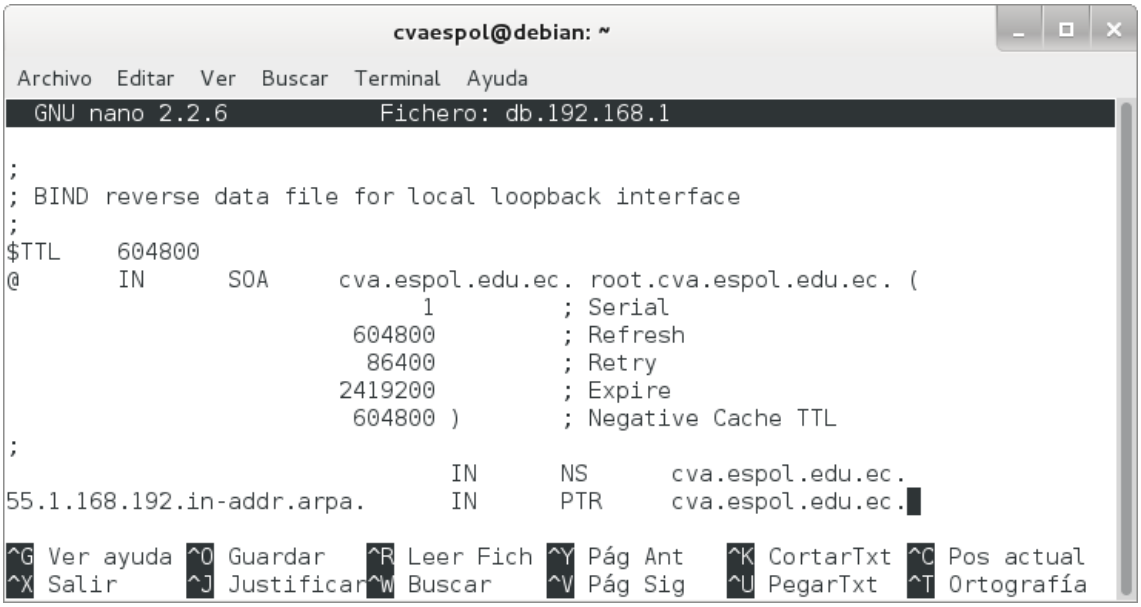

Figura 96. Archivo db.192.168.1.

8. Comprobar la zona inversa que se creó:

 # named-checkzone 1.168.192.in-addr.arpa db.192.168.1

Con lo que se comprueba que la zona inversa está correctamente configurada, como se observa en la figura 97.

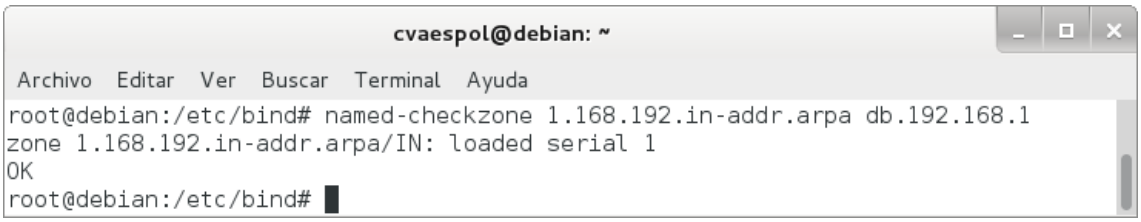

Figura 97. Ejecución de named-checkzone sin errores.

9. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 98.

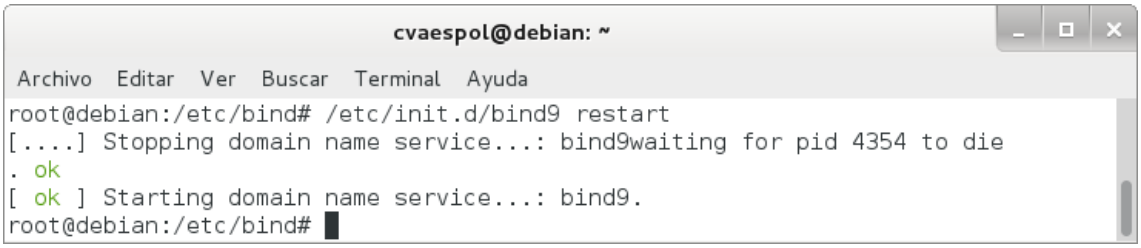

Figura 98. Reinicio del servicio.

10. Probar el servidor de nombres:

 # dig cva.espol.edu.ec

La respuesta será parecida a como se muestra en la figura 99.

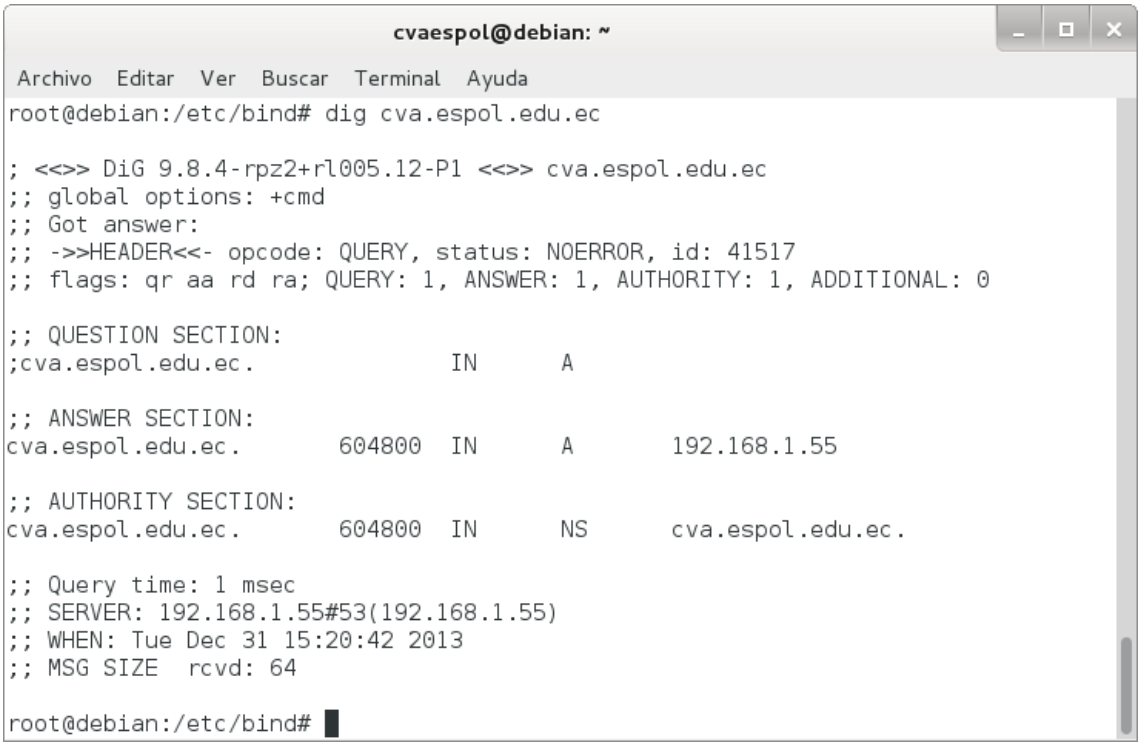

Figura 99. Ejecución de dig cva.espol.edu.ec.

11. Probar la resolución inversa:

    # dig -x 192.168.1.55

La respuesta será parecida a como se muestra en la figura 100.

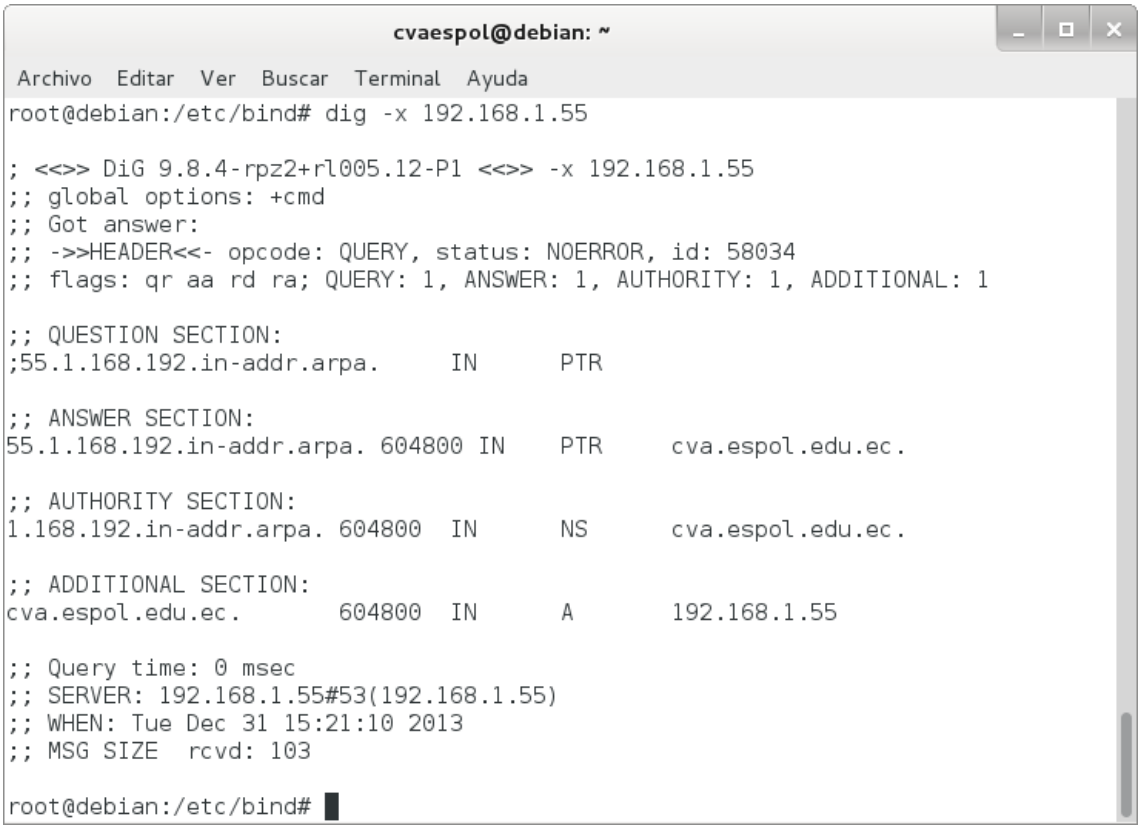

Figura 100. Ejecución de dig -x 192.168.1.55.

Anexo 10: Aseguramiento de la zona DNS del sitio web de la Universidad Nacional de Loja.

1. Configurar servidor autoritativo.

El servidor autoritativo se configuró para soportar DNSSEC. Los pasos esenciales son:

1. Revisar que Bind esté compilado con OpenSSL:

 # named -V

Donde se puede observar la versión de OpenSSL que se está usando, tal como en la figura 101.

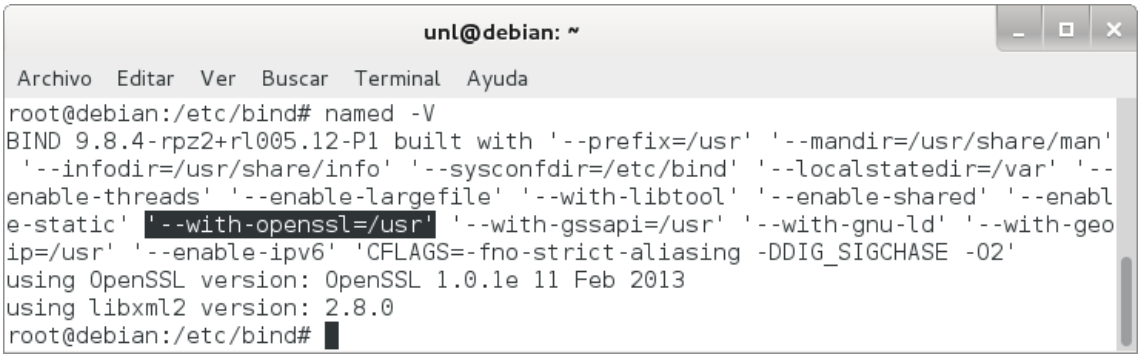

Figura 101. Compilación de Bind.

2. Habilitar DNSSEC en el archivo /etc/bind/named.conf.options:

```
options {
        dnssec-enable yes;
        dnssec-validation auto;
        dnssec-lookaside auto;
};
```

Con lo que se permite la habilitación, validación y lookaside de DNSSEC, como se muestra en la figura 102.

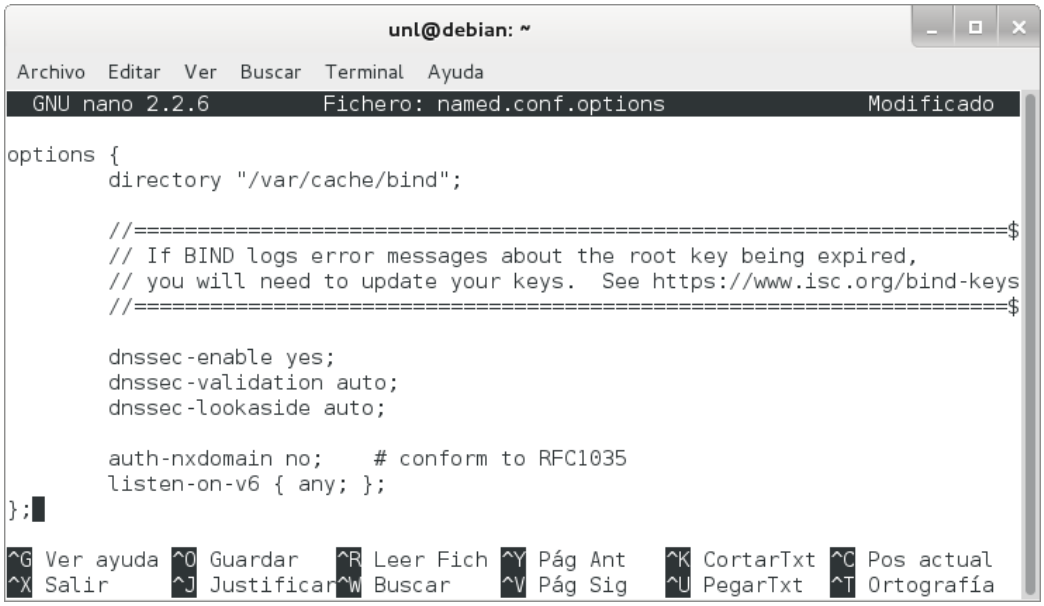

Figura 102. Habilitación de DNSSEC.

3. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 103.

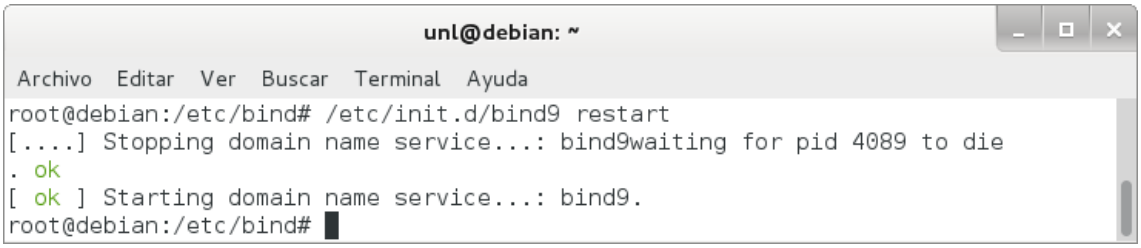

Figura 103. Reinicio del servicio.

2. Crear pares de claves.

Es necesario crear una KSK (Key Signing Key) inicial y ZSK (Zone Signing Key) para cada zona para estar asegurado. Las partes privadas deben mantenerse en privado y seguras [34].

La salida se puede encontrar en dos archivos. El nombre de los archivos contiene información relevante:

Knombre_dominio+id_algoritmo+id_clave.extension

El nombre_dominio es el nombre especificado en la línea de comandos. Es utilizado por otras herramientas de BIND de DNSSEC. El id_algoritmo identifica el algoritmo utilizado: 1 para RSAMD5, 3 de DSA, 5 para RSASHA1 y 54 de HMAC-MD5. El id_clave es un identificador para el contenido de la clave. Este id_clave es utilizado por el registro de recurso RRSIG. La extension es cualquier key o private, la primera es la clave pública y la segunda es la clave privada [17].

Los pasos para crear las claves son:

1. Crear la KSK:

   # dnssec-keygen -r /dev/random -f KSK -a RSASHA1 -b 1280 -n ZONE unl.edu.ec

Donde se crea un par de KSK con el tipo de algoritmo RSASHA1, tamaño de la clave 1280 y unl.edu.ec como el nombre de la zona, tal como se observa en la figura 104.

Figura 104. KSK.

Mediante este comando se generan dos archivos, cuyos contenidos se muestran en las figuras 105 y 106.

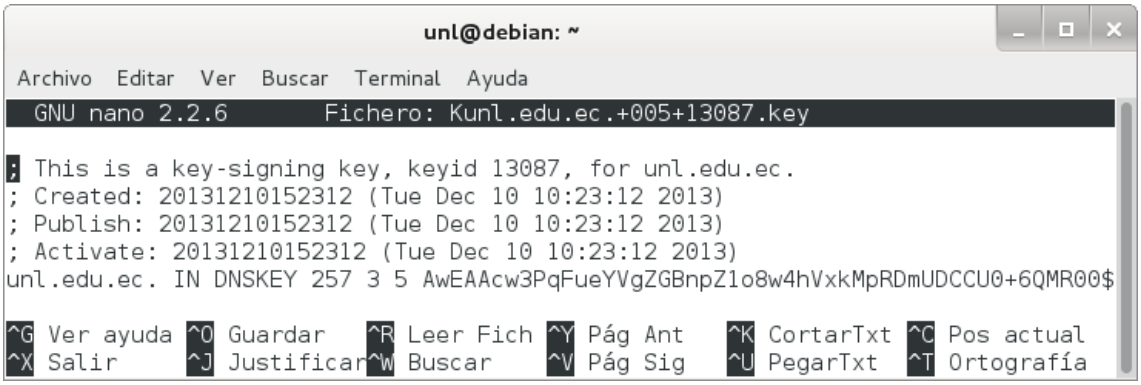

Figura 105. Archivo Kunl.edu.ec.+005+13087.key.

Donde la clave pública (extensión .key) es tal y como aparece en el archivo de zona. Tenga en cuenta que no se especifica el valor TTL. Esta clave tiene un valor "bandera" de 257. Dado que este valor es un número impar, la clave está marcada como una clave SEP y no se debe utilizar para la zona de firma.

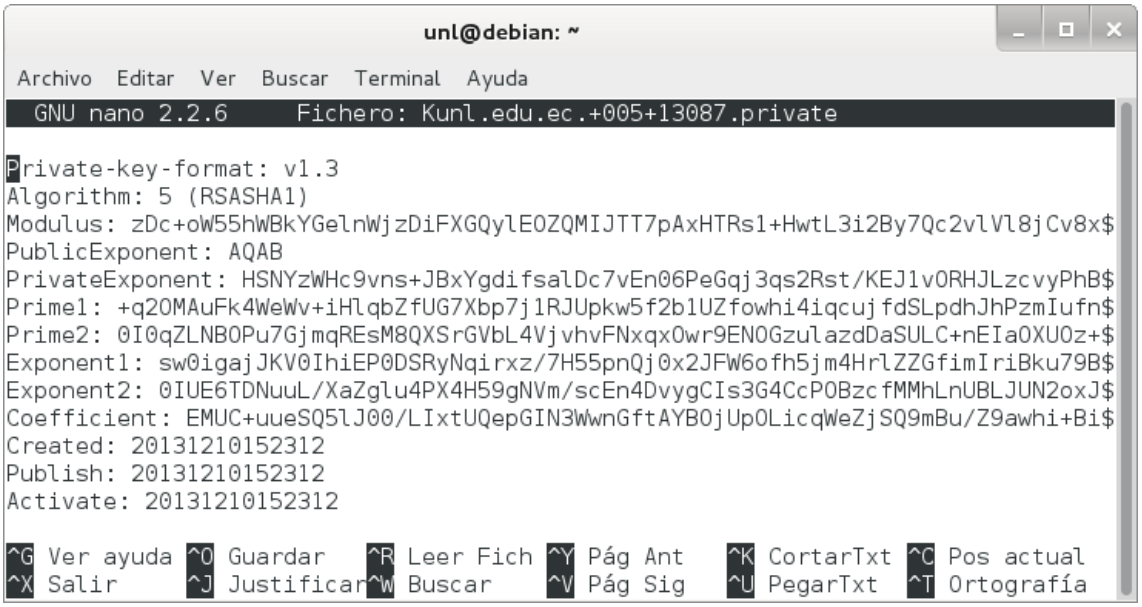

Figura 106. Archivo Kunl.edu.ec.+005+13087.private.

Donde la clave privada (extensión .private) contiene todos los parámetros que hacen a una clave privada RSASHA1. La clave privada de una clave RSA contiene diferentes parámetros para DSA.

2. Crear la ZSK:

 # dnssec-keygen -r /dev/random -a RSASHA1 -b 1024 -n ZONE unl.edu.ec

Donde se crea un par de ZSK con el tipo de algoritmo RSASHA1, tamaño de la clave 1024 y unl.edu.ec como el nombre de la zona, tal como se observa en la figura 107.

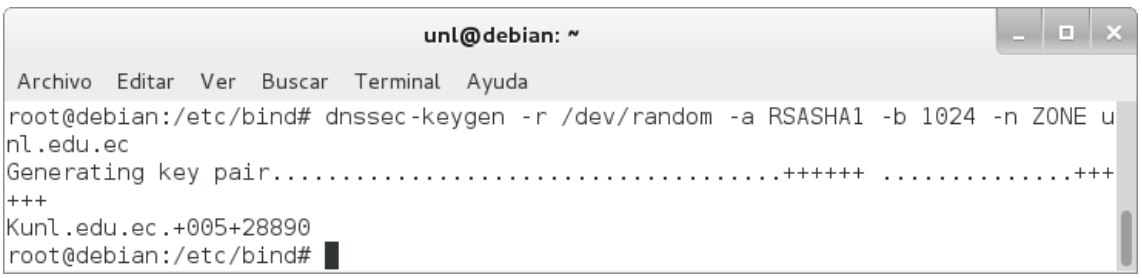

Figura 107. ZSK.

Mediante este comando se generan dos archivos, cuyos contenidos se muestran en las figuras 108 y 109.

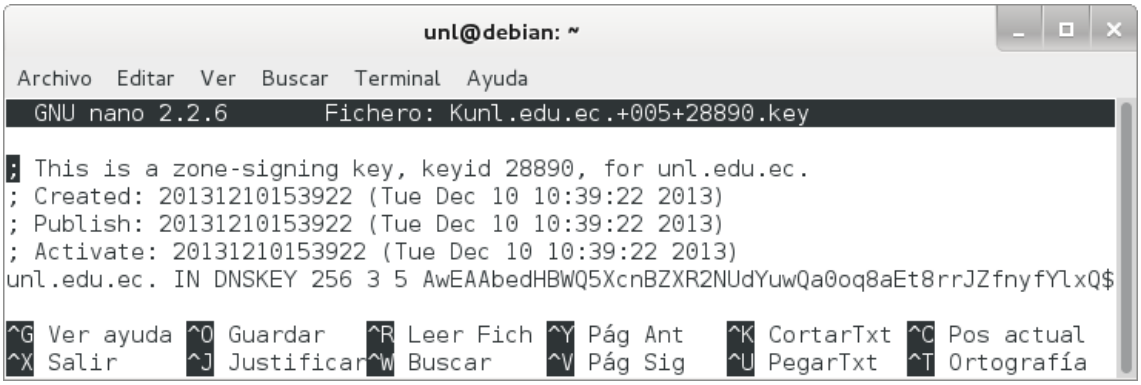

Figura 108. Archivo Kunl.edu.ec.+005+28890.key.

Donde la clave pública (extensión .key) es tal y como aparece en el archivo de zona. Tenga en cuenta que no se especifica el valor TTL. Esta clave tiene un valor “bandera” de 256. Dado que este valor es un número par, la clave no está marcada como una clave SEP y se debe utilizar para la zona de firma.

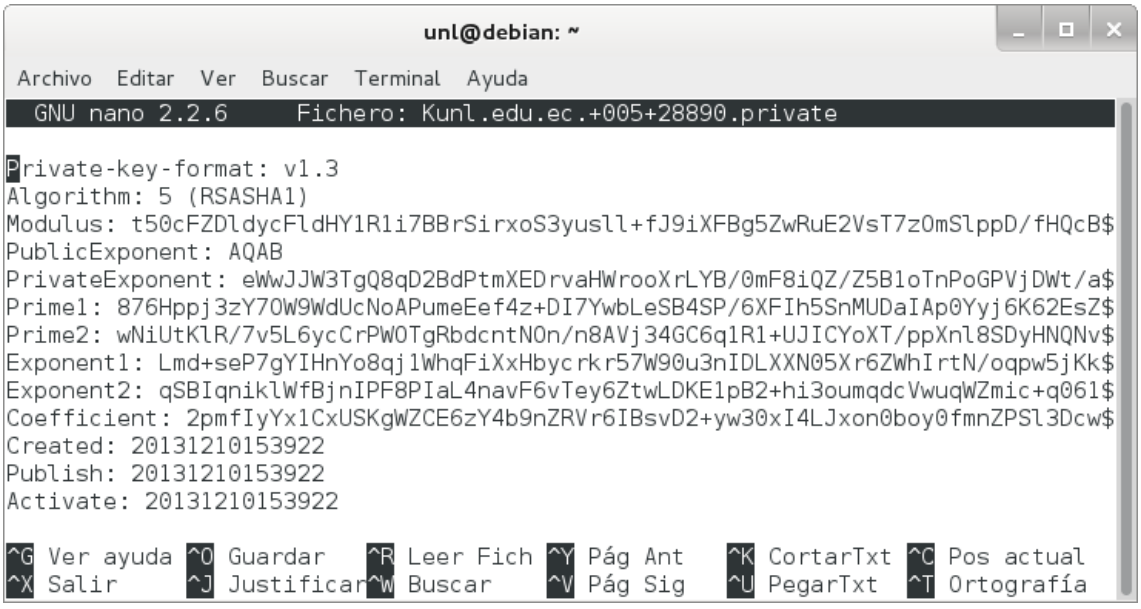

Figura 109. Archivo Kunl.edu.ec.+005+28890.private.

Donde la clave privada (extensión .private) contiene todos los parámetros que hacen a una clave privada RSASHA1. La clave privada de una clave RSA contiene diferentes parámetros para DSA.

3. Insertar las claves de la zona.

Al crear pares de claves, estas se las incluyó en su archivo de zona.

Para incluir las claves en la zona se debe:

1. Añadir la directiva $INCLUDE en el archivo /etc/bind/db.unl.edu.ec:

   $INCLUDE Kunl.edu.ec.+005+13087.key

   $INCLUDE Kunl.edu.ec.+005+28890.key

Observe la figura 110, donde se utiliza la directiva $INCLUDE para incluir las claves.

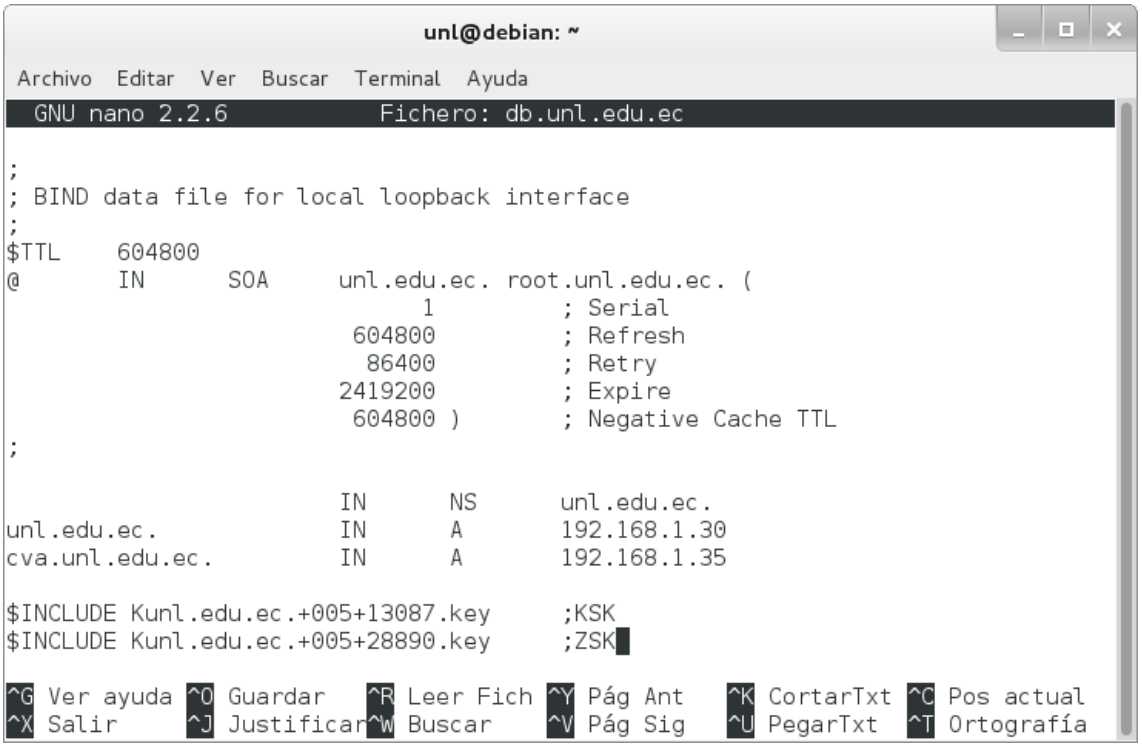

Figura 110. Inserción de las claves de la zona.

4. Firmar la zona.

Una vez que las claves han sido incluidas en el archivo de zona, se prosiguió a firmar la zona, para lo cual se utilizó la herramienta dnssec-signzone.

Para firmar la zona se realizó lo siguiente:

1. Emplear la herramienta dnssec-signzone:

 # dnssec-signzone -o unl.edu.ec -k Kunl.edu.ec.+005+13087.key db.unl.edu.ec Kunl.edu.ec.+005+28890.key

Donde se especifica a unl.edu.ec como el origen de la zona, por defecto el origen se deduce del nombre del archivo de zona; se especifica qué clave se va a utilizar como KSK, la cual sólo firmará el conjunto DNSKEY RR en el vértice de la zona, la clave que se encuentra como argumento al final del comando se utiliza para firmar todos los datos de RR para los que la zona es autoritativa. Si no especifican las claves, BIND usará aquellas para las que las claves públicas están incluidas en la zona y usa la bandera SEP para distinguir entre las claves y las ZSK.

Las firmas se crean con un tiempo de vida por defecto de 30 días desde el momento de la firma. Una vez que las firmas han expirado los datos no pueden ser validados y su zona se marcará como 'falsa'. Por lo tanto, se tendrá que volver a firmar la zona dentro de los 30 días [17].

La zona firmada se almacena en el archivo db.unl.edu.ec.signed, como se muestra en la figura 111.

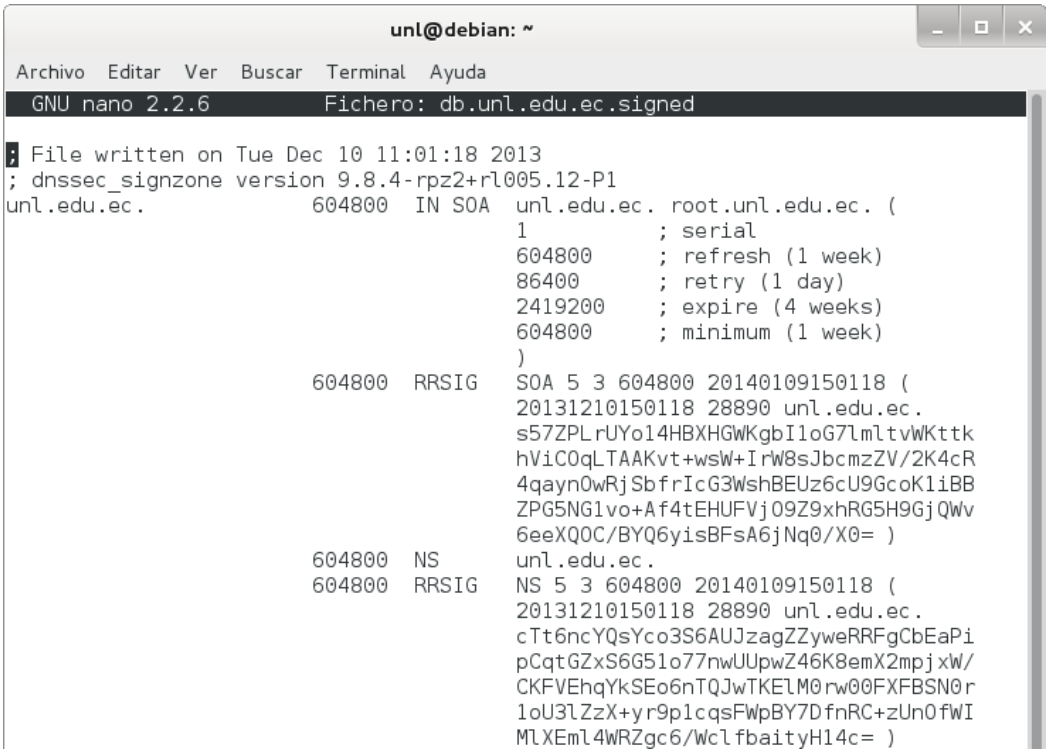

Figura 111. Archivo db.unl.edu.ec.signed.

Figura 111. Archivo db.unl.edu.ec.signed (continuación).

2. Comprobar si el archivo de zona db.unl.edu.ec.signed fue generado:

   # named-checkzone unl.edu.ec. db.unl.edu.ec.signed

Con lo que se comprueba que la zona ha sido firmada, como se observa en la figura 112.

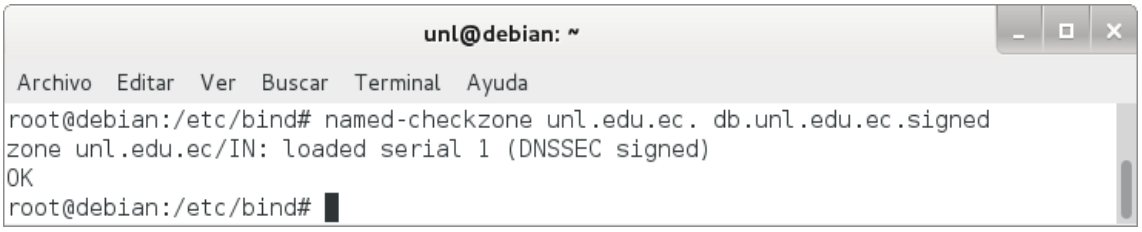

Figura 112. Ejecución de named-checkzone sin errores.

3. Cambiar en el archivo de configuración named.conf.local, el nombre del archivo de zona para el nuevo nombre que contiene la zona unl.edu.ec ya firmada:

```
zone "unl.edu.ec." {
        type master;
        file "/etc/bind/db.unl.edu.ec.signed";
};
```

Quedando como se muestra en la figura 113.

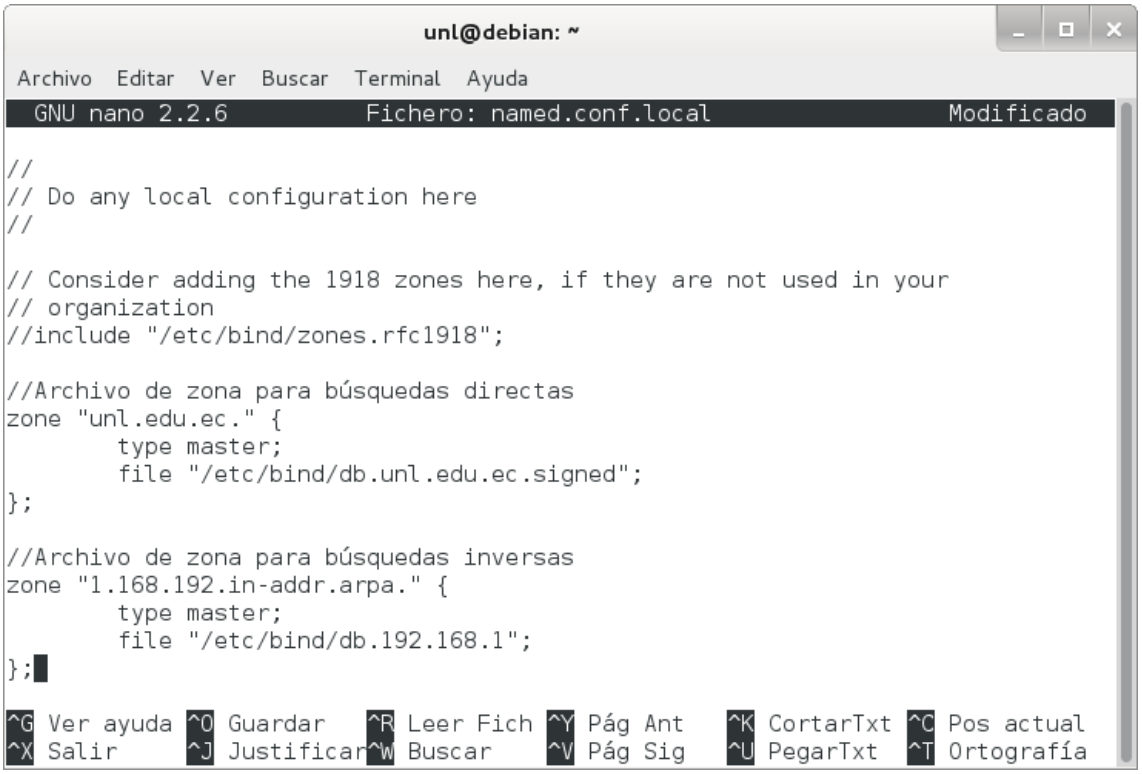

Figura 113. Archivo named.conf.local.

4. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 114.

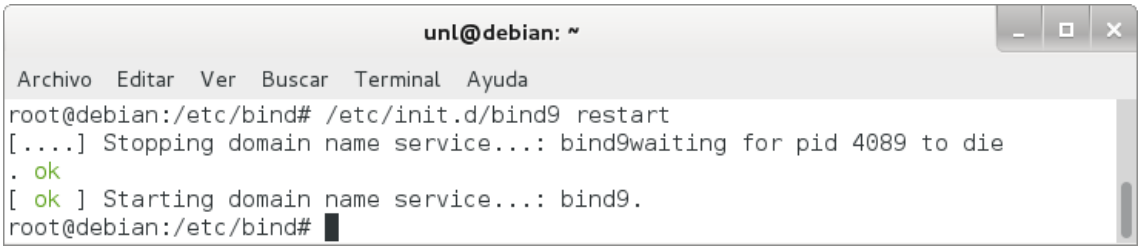

Figura 114. Reinicio del servicio.

5. Realizar pruebas.

Se comprobó si el servidor de nombres emite respuestas y si estas respuestas contienen información DNSSEC.

Para ello se realizó lo siguiente:

1. Emplear el comando dig:

 # dig @localhost unl.edu.ec SOA +dnssec +multiline

Con lo que el resultado de la zona unl.edu.ec configurada correctamente quedaría como se muestra en la figura 115.

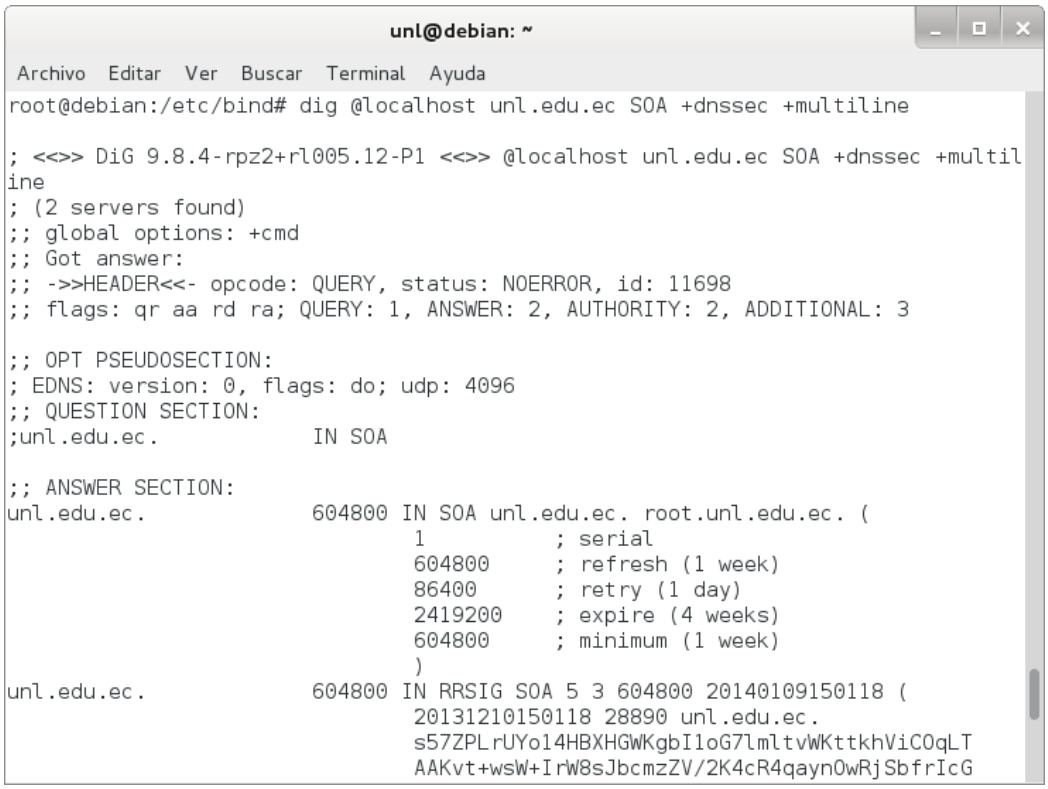

Figura 115. Ejecución correcta de dig.

Anexo 11: Aseguramiento de la zona DNS de la comunidad virtual de aprendizaje de la Universidad Nacional de Loja.

1. Configurar servidor autoritativo.

El servidor autoritativo se configuró para soportar DNSSEC. Los pasos esenciales fueron:

1. Revisar que Bind esté compilado con OpenSSL:

   # named -V

Donde se puede observar la versión de OpenSSL que se está usando, tal como en la figura 116.

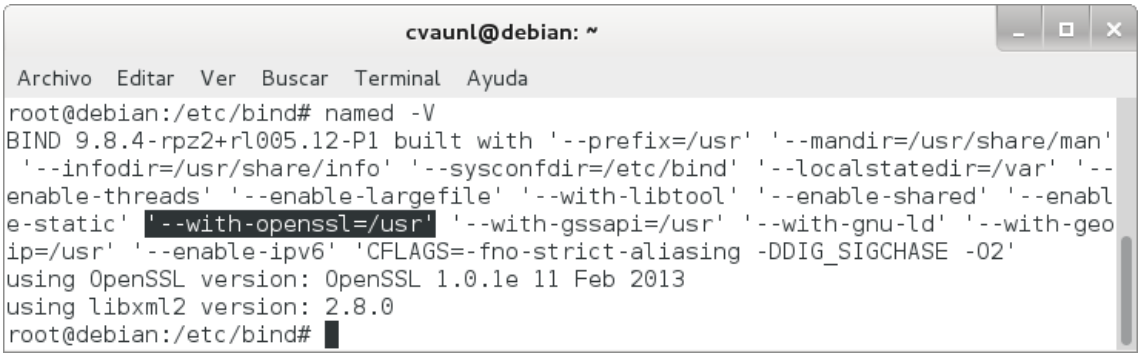

Figura 116. Compilación de Bind.

2. Habilitar DNSSEC en el archivo /etc/bind/named.conf.options:

```
options {
        dnssec-enable yes;
        dnssec-validation auto;
        dnssec-lookaside auto;
};
```

Con lo que se permite la habilitación, validación y lookaside de DNSSEC, como se muestra en la figura 117.

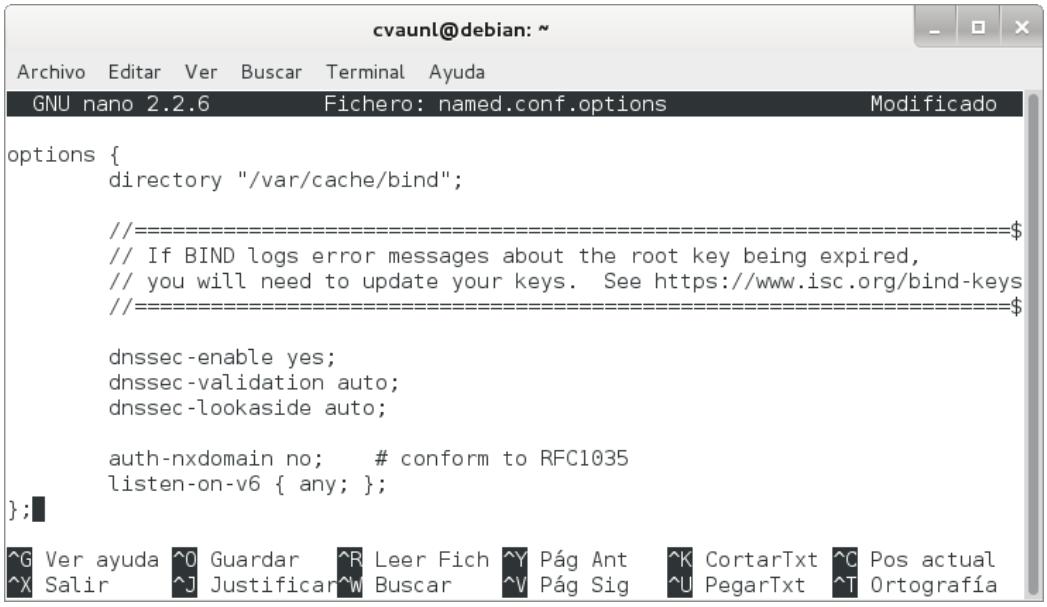

Figura 117. Habilitación de DNSSEC.

3. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 118.

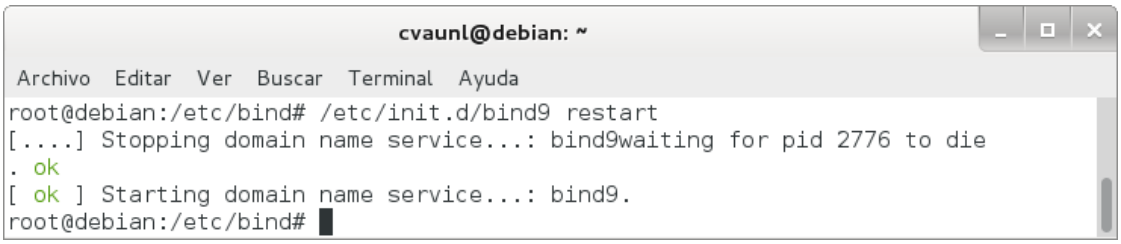

Figura 118. Reinicio del servicio.

2. Crear pares de claves.

Es necesario crear una KSK (Key Signing Key) inicial y ZSK (Zone Signing Key) para cada zona para estar asegurado. Las partes privadas deben mantenerse en privado y seguras [34].

La salida se puede encontrar en dos archivos. El nombre de los archivos contiene información relevante:

Knombre_dominio+id_algoritmo+id_clave.extension

El nombre_dominio es el nombre especificado en la línea de comandos. Es utilizado por otras herramientas de BIND de DNSSEC. El id_algoritmo identifica el algoritmo utilizado: 1 para RSAMD5, 3 de DSA, 5 para RSASHA1 y 54 de HMAC-MD5. El id_clave es un identificador para el contenido de la clave. Este id_clave es utilizado por el registro de recurso RRSIG. La extension es cualquier key o private, la primera es la clave pública y la segunda es la clave privada [17].

Los pasos para crear las claves fueron:

1. Crear la KSK:

   # dnssec-keygen -r /dev/random -f KSK -a RSASHA1 -b 1280 -n ZONE cva.unl.edu.ec

Donde se crea un par de KSK con el tipo de algoritmo RSASHA1, tamaño de la clave 1280 y cva.unl.edu.ec como el nombre de la zona, tal como se observa en la figura 119.

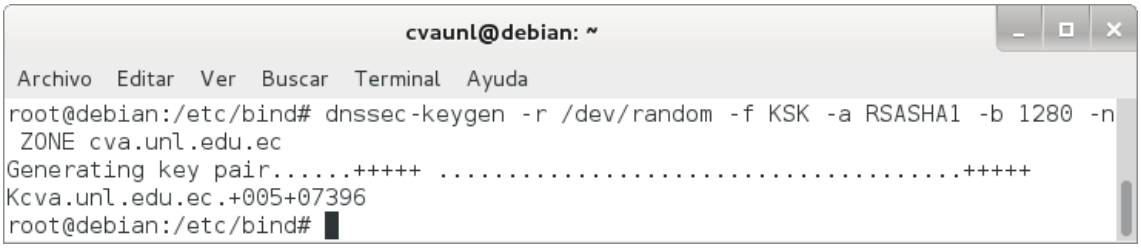

Figura 119. KSK.

Mediante este comando se generan dos archivos, cuyos contenidos se muestran en las figuras 120 y 121.

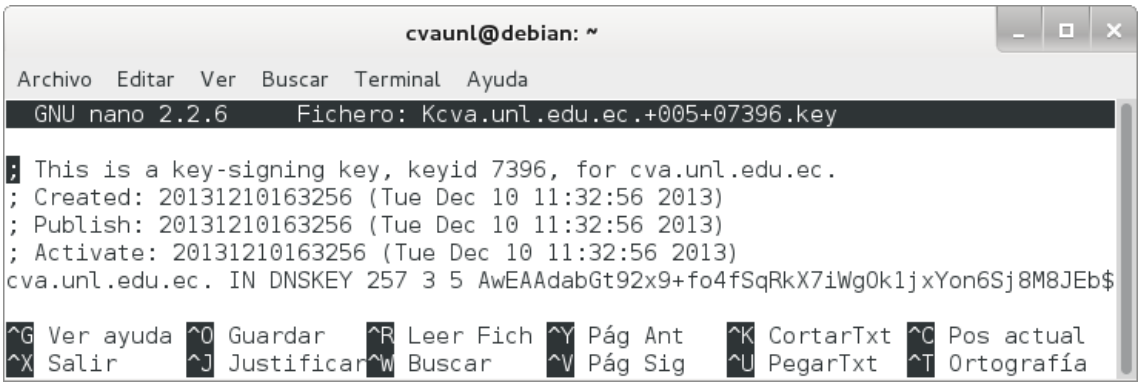

Figura 120. Archivo Kcva.unl.edu.ec.+005+07396.key.

Donde la clave pública (extensión .key) es tal y como aparece en el archivo de zona. Tenga en cuenta que no se especifica el valor TTL. Esta clave tiene un valor "bandera" de 257. Dado que este valor es un número impar, la clave está marcada como una clave SEP y no se debe utilizar para la zona de firma.

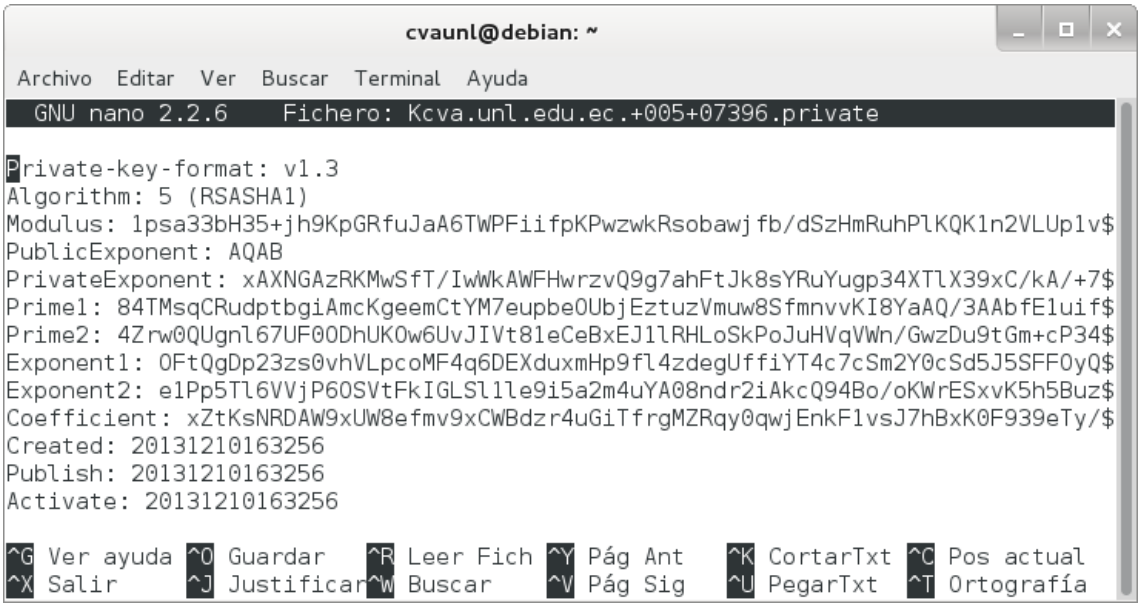

Figura 121. Archivo Kcva.unl.edu.ec.+005+07396.private.

Donde la clave privada (extensión .private) contiene todos los parámetros que hacen a una clave privada RSASHA1. La clave privada de una clave RSA contiene diferentes parámetros para DSA.

2. Crear la ZSK:

 # dnssec-keygen -r /dev/random -a RSASHA1 -b 1024 -n ZONE cva.unl.edu.ec

Donde se crea un par de ZSK con el tipo de algoritmo RSASHA1, tamaño de la clave 1024 y cva.unl.edu.ec como el nombre de la zona, tal como se observa en la figura 122.

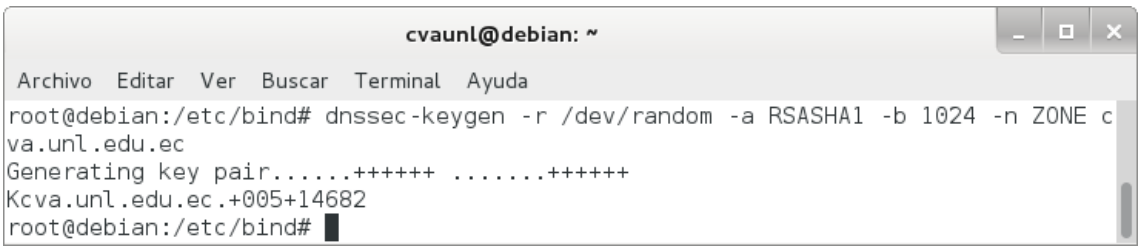

Figura 122. ZSK.

Mediante este comando se generan dos archivos, cuyos contenidos se muestran en las figuras 123 y 124.

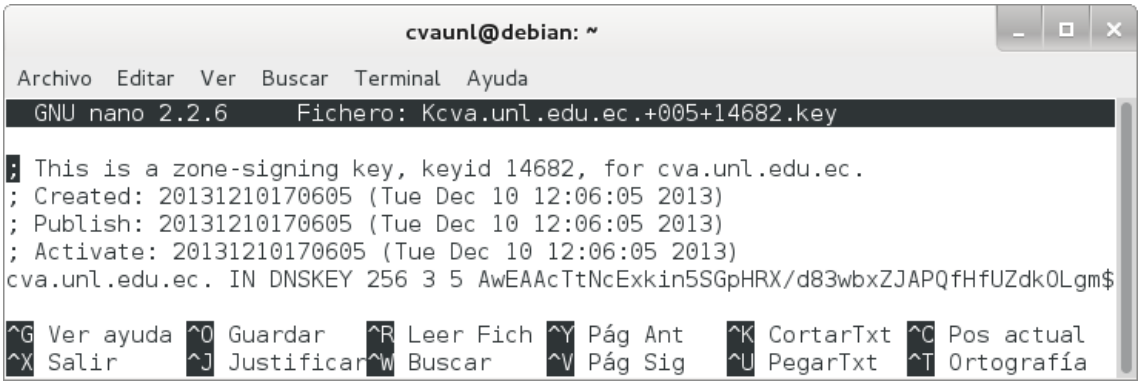

Figura 123. Archivo Kcva.unl.edu.ec.+005+14682.key.

Donde la clave pública (extensión .key) es tal y como aparece en el archivo de zona. Tenga en cuenta que no se especifica el valor TTL. Esta clave tiene un valor “bandera” de 256. Dado que este valor es un número par, la clave no está marcada como una clave SEP y se debe utilizar para la zona de firma.

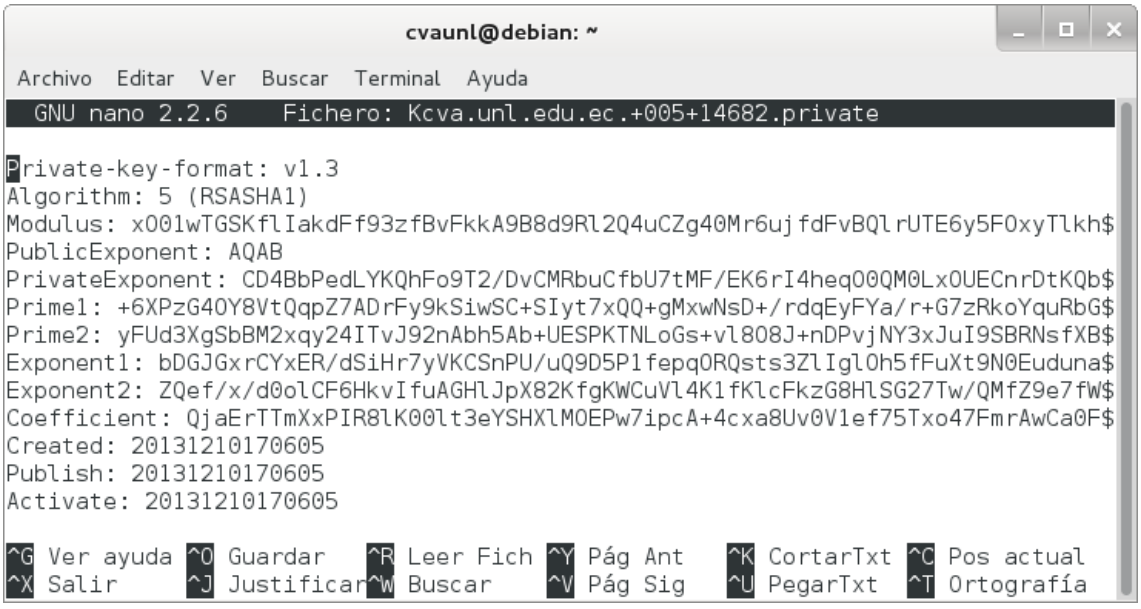

Figura 124. Archivo Kcva.unl.edu.ec.+005+14682.private.

Donde la clave privada (extensión .private) contiene todos los parámetros que hacen a una clave privada RSASHA1. La clave privada de una clave RSA contiene diferentes parámetros para DSA.

3. Insertar las claves de la zona.

Al crear pares de claves, estas se las incluyó en su archivo de zona.

Para incluir las claves en la zona se debe:

1. Añadir la directiva $INCLUDE en el archivo /etc/bind/db.cva.unl.edu.ec:

   $INCLUDE Kcva.unl.edu.ec.+005+07396.key

   $INCLUDE Kcva.unl.edu.ec.+005+14682.key

Observe la figura 125, donde se utiliza la directiva $INCLUDE para incluir las claves.

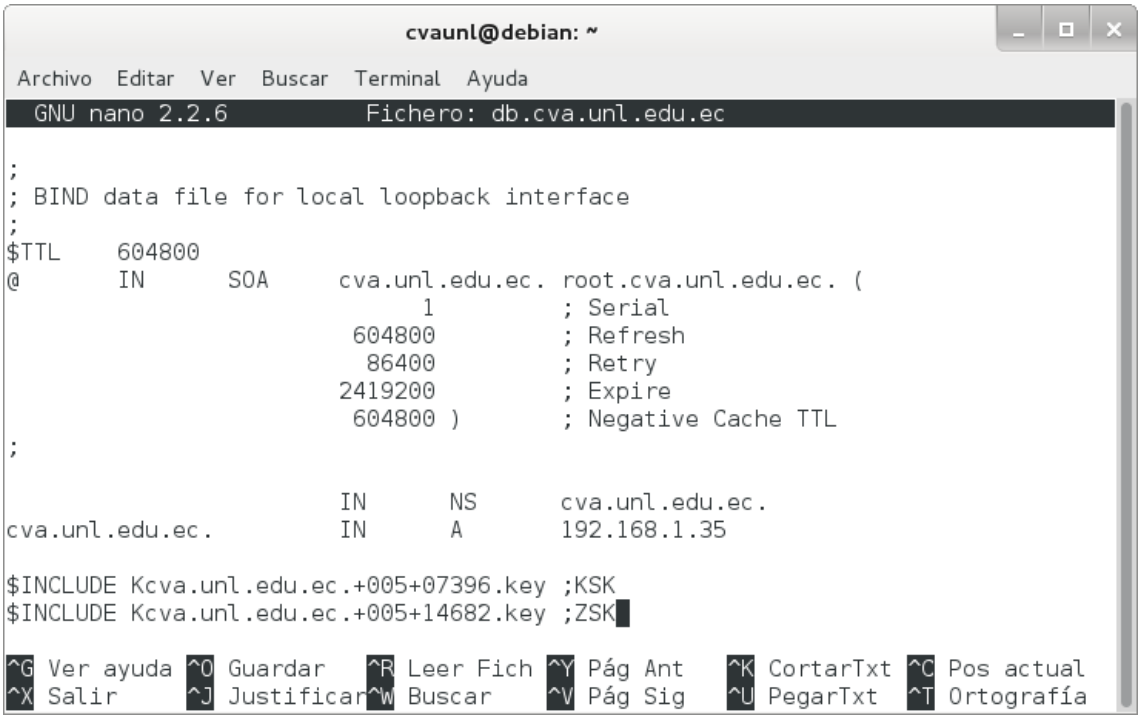

Figura 125. Inserción de las claves de la zona.

4. Firmar la zona.

Una vez que las claves han sido incluidas en el archivo de zona, se prosiguió a firmar la zona, para lo cual se utilizó la herramienta dnssec-signzone.

Para firmar la zona se realizó lo siguiente:

1. Emplear la herramienta dnssec-signzone:

 # dnssec-signzone -o cva.unl.edu.ec -k Kcva.unl.edu.ec.+005+26923.key db.cva.unl.edu.ec Kcva.unl.edu.ec.+005+30528.key

Donde se especifica a cva.unl.edu.ec como el origen de la zona, por defecto el origen se deduce del nombre del archivo de zona; se especifica qué clave se va a utilizar como KSK, la cual sólo firmará el conjunto DNSKEY RR en el vértice de la zona, la clave que se encuentra como argumento al final del comando se utiliza para firmar todos los datos de RR para los que la zona es autoritativa. Si no especifican las claves, BIND usará aquellas para las que las claves públicas están incluidas en la zona y usa la bandera SEP para distinguir entre las claves y las ZSK.

Las firmas se crean con un tiempo de vida por defecto de 30 días desde el momento de la firma. Una vez que las firmas han expirado los datos no pueden ser validados y su zona se marcará como 'falsa'. Por lo tanto, se tendrá que volver a firmar la zona dentro de los 30 días [17].

La zona firmada se almacena en el archivo db.cva.unl.edu.ec.signed, como se muestra en la figura 126.

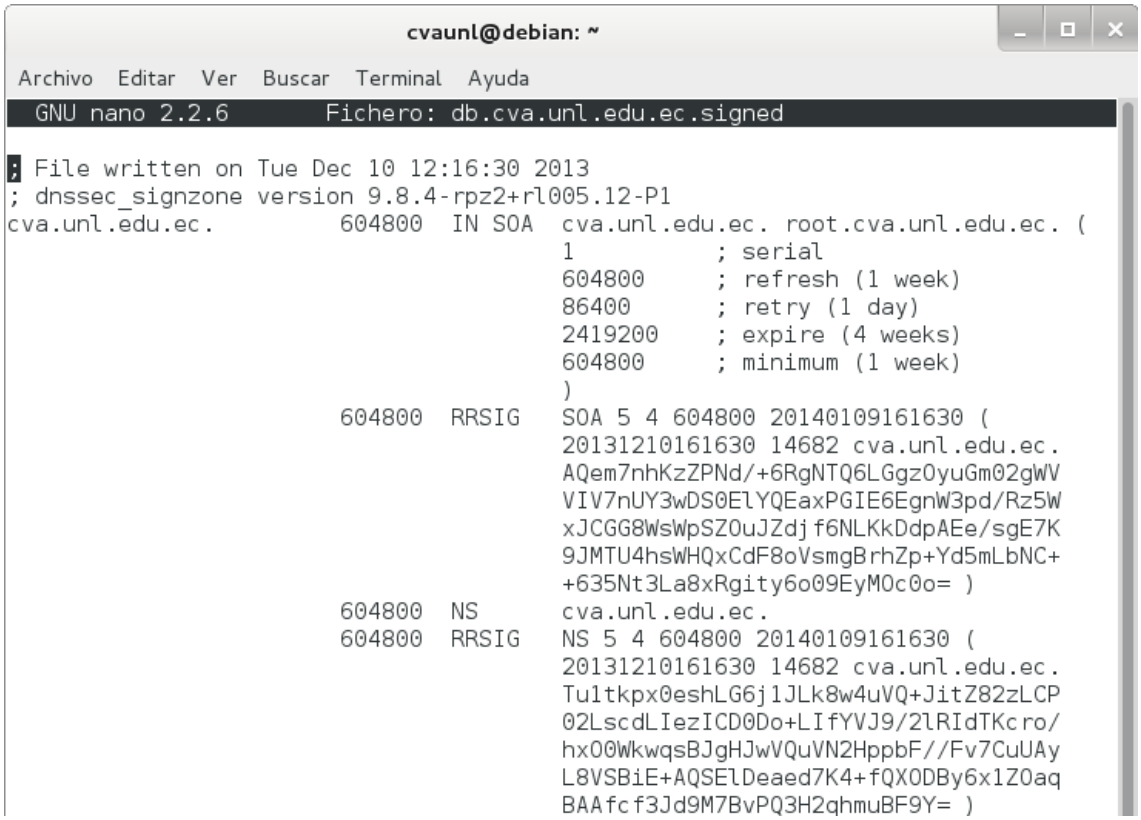

Figura 126. Archivo db.cva.unl.edu.ec.signed.

Figura 126. Archivo db.cva.unl.edu.ec.signed (continuación).

2. Comprobar si el archivo de zona db.cva.unl.edu.ec.signed fue generado:

 # named-checkzone cva.unl.edu.ec. db.cva.unl.edu.ec.signed

Con lo que se comprueba que la zona ha sido firmada, como se observa en la figura 127.

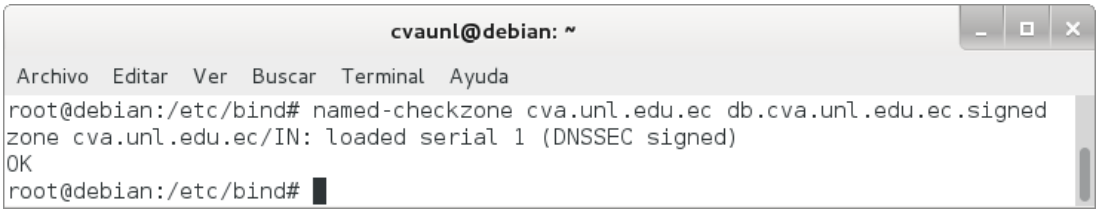

Figura 127. Ejecución de named-checkzone sin errores.

3. Cambiar en el archivo de configuración named.conf.local, el nombre del archivo de zona para el nuevo nombre que contiene la zona cva.unl.edu.ec ya firmada:

zone "cva.unl.edu.ec." {
type master;
file "/etc/bind/db.cva.unl.edu.ec.signed";
};

Quedando como se muestra en la figura 128.

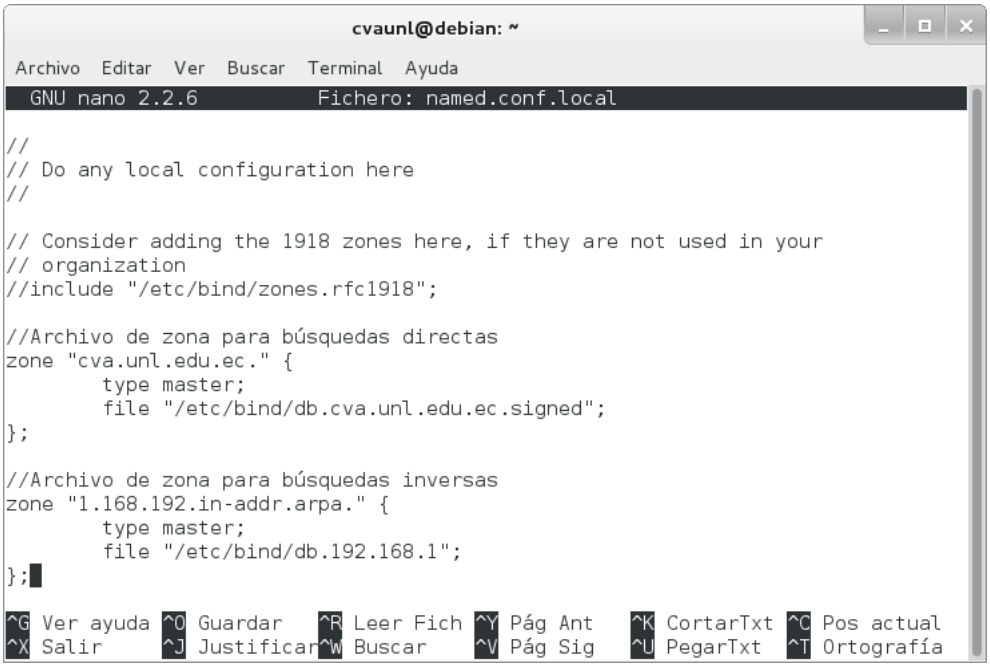

Figura 128. Archivo named.conf.local.

4. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 129.

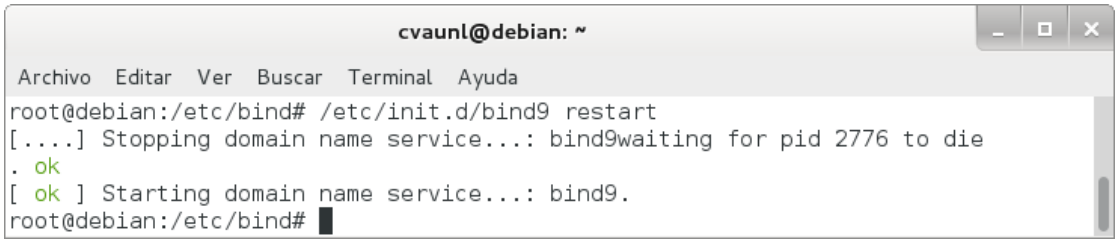

Figura 129. Reinicio del servicio.

5. Realizar pruebas.

Se comprobó si el servidor de nombres emite respuestas y si estas respuestas contienen información DNSSEC.

Para ello se realizó lo siguiente:

1. Emplear el comando dig:

 # dig @localhost cva.unl.edu.ec SOA +dnssec +multiline

Con lo que el resultado de la zona cva.unl.edu.ec configurada correctamente quedaría como se muestra en la figura 130.

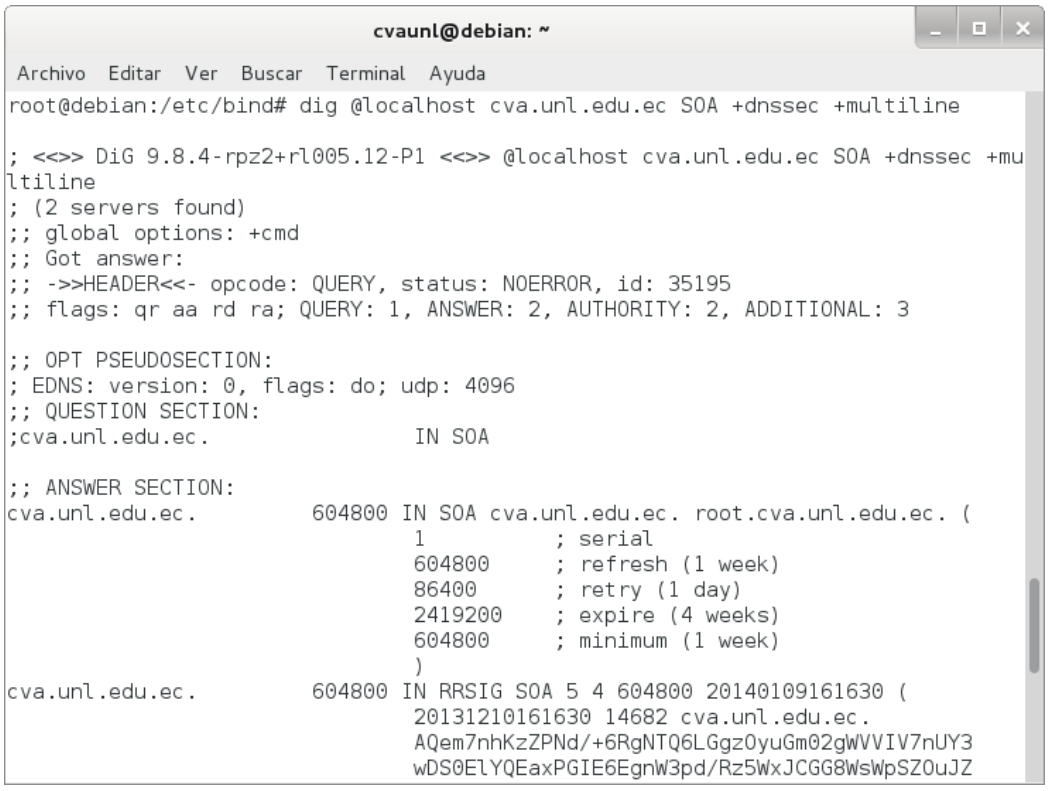

Figura 130. Ejecución correcta de dig.

Anexo 12: Aseguramiento de la zona DNS del sitio web de la Universidad Técnica Particular de Loja.

1. Configurar servidor autoritativo.

El servidor autoritativo se configuró para soportar DNSSEC. Los pasos esenciales fueron:

1. Revisar que Bind esté compilado con OpenSSL:

 # named -V

Donde se puede observar la versión de OpenSSL que se está usando, tal como en la figura 131.

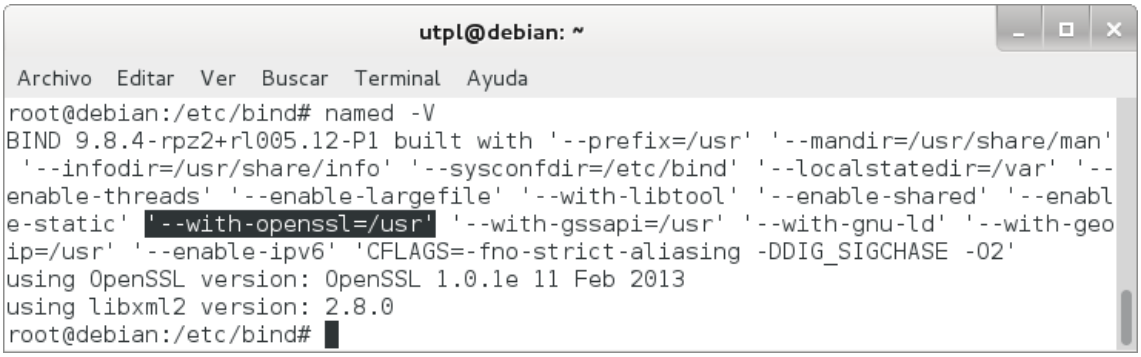

Figura 131. Compilación de Bind.

2. Habilitar DNSSEC en el archivo /etc/bind/named.conf.options:

```
options {
        dnssec-enable yes;
        dnssec-validation auto;
        dnssec-lookaside auto;
};
```

Con lo que se permite la habilitación, validación y lookaside de DNSSEC, como se muestra en la figura 132.

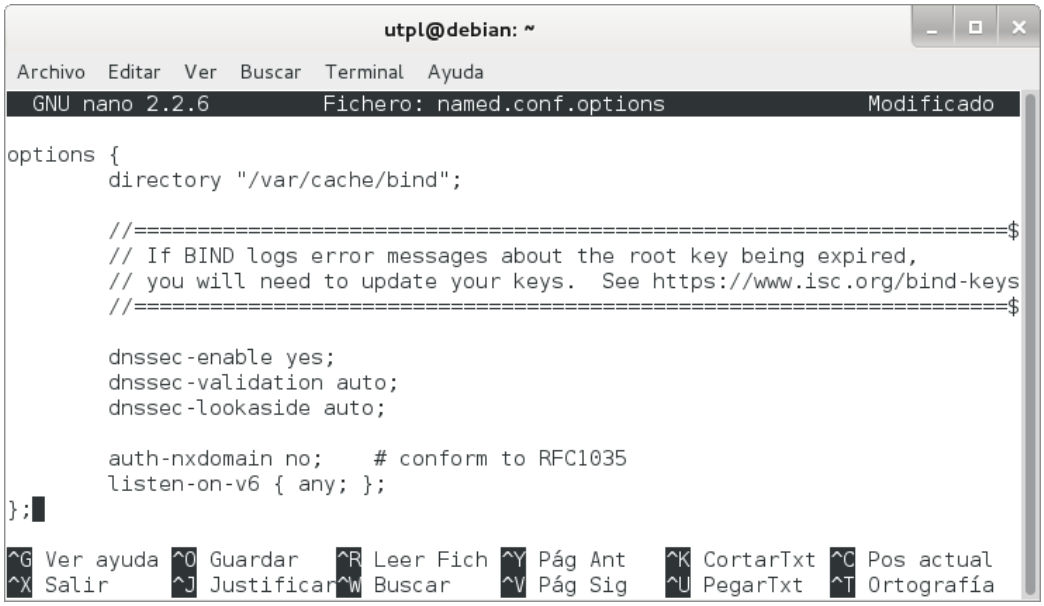

Figura 132. Habilitación de DNSSEC.

3. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 133.

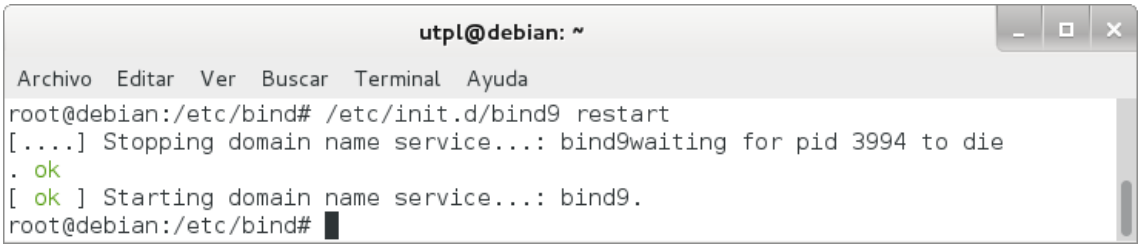

Figura 133. Reinicio del servicio.

2. Crear pares de claves.

Es necesario crear una KSK (Key Signing Key) inicial y ZSK (Zone Signing Key) para cada zona para estar asegurado. Las partes privadas deben mantenerse en privado y seguras [34].

La salida se puede encontrar en dos archivos. El nombre de los archivos contienen información relevante:

Knombre_dominio+id_algoritmo+id_clave.extension

El nombre_dominio es el nombre especificado en la línea de comandos. Es utilizado por otras herramientas de BIND de DNSSEC. El id_algoritmo identifica el algoritmo utilizado: 1 para RSAMD5, 3 de DSA, 5 para RSASHA1 y 54 de HMAC-MD5. El id_clave es un identificador para el contenido de la clave. Este id_clave es utilizado por el registro de recurso RRSIG. La extension es cualquier key o private, la primera es la clave pública y la segunda es la clave privada [17].

Los pasos para crear las claves fueron:

1. Crear la KSK:

   # dnssec-keygen -r /dev/random -f KSK -a RSASHA1 -b 1280 -n ZONE utpl.edu.ec

Donde se crea un par de KSK con el tipo de algoritmo RSASHA1, tamaño de la clave 1280 y utpl.edu.ec como el nombre de la zona, tal como se observa en la figura 134.

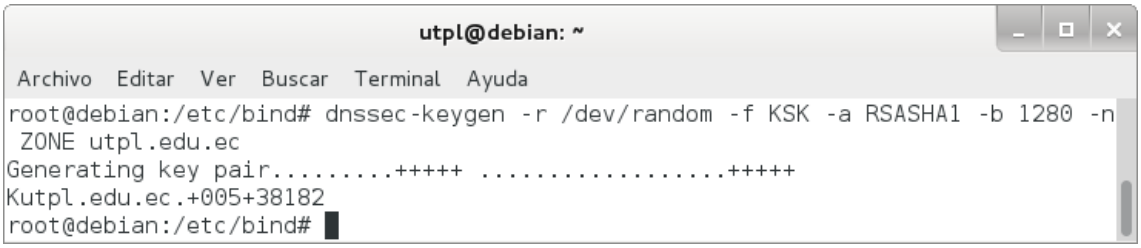

Figura 134. KSK.

Mediante este comando se generan dos archivos, cuyos contenidos se muestran en las figuras 135 y 136.

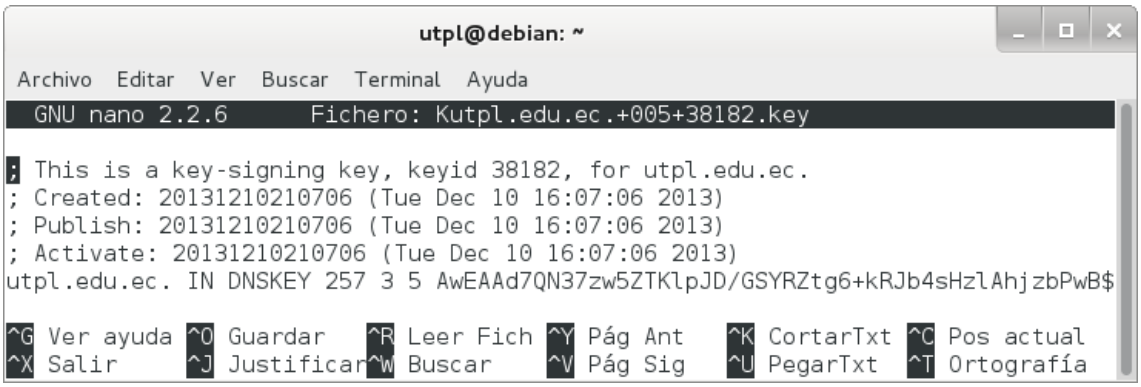

Figura 135. Archivo Kutpl.edu.ec.+005+38182.key.

Donde la clave pública (extensión .key) es tal y como aparece en el archivo de zona. Tenga en cuenta que no se especifica el valor TTL. Esta clave tiene un valor "bandera" de 257. Dado que este valor es un número impar, la clave está marcada como una clave SEP y no se debe utilizar para la zona de firma.

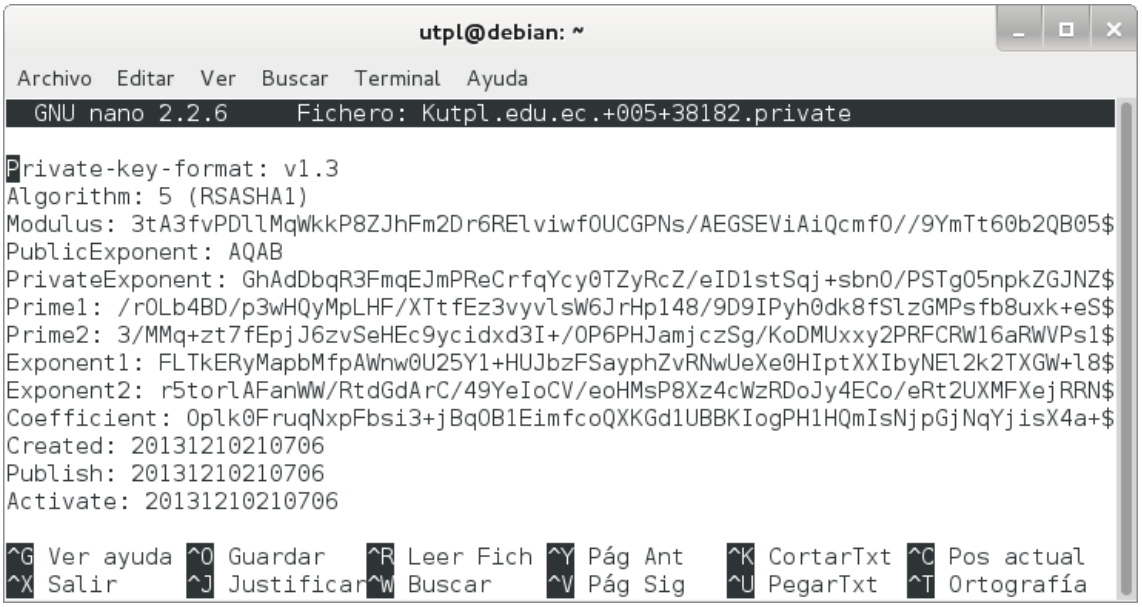

Figura 136. Archivo Kutpl.edu.ec.+005+38182.private.

Donde la clave privada (extensión .private) contiene todos los parámetros que hacen a una clave privada RSASHA1. La clave privada de una clave RSA contiene diferentes parámetros para DSA.

2. Crear la ZSK:

 # dnssec-keygen -r /dev/random -a RSASHA1 -b 1024 -n ZONE utpl.edu.ec

Donde se crea un par de ZSK con el tipo de algoritmo RSASHA1, tamaño de la clave 1024 y utpl.edu.ec como el nombre de la zona, tal como se observa en la figura 137.

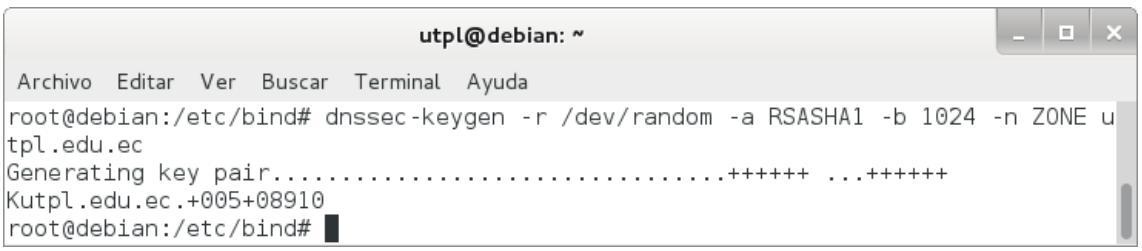

Figura 137. ZSK.

Mediante este comando se generan dos archivos, cuyos contenidos se muestran en las figuras 138 y 139.

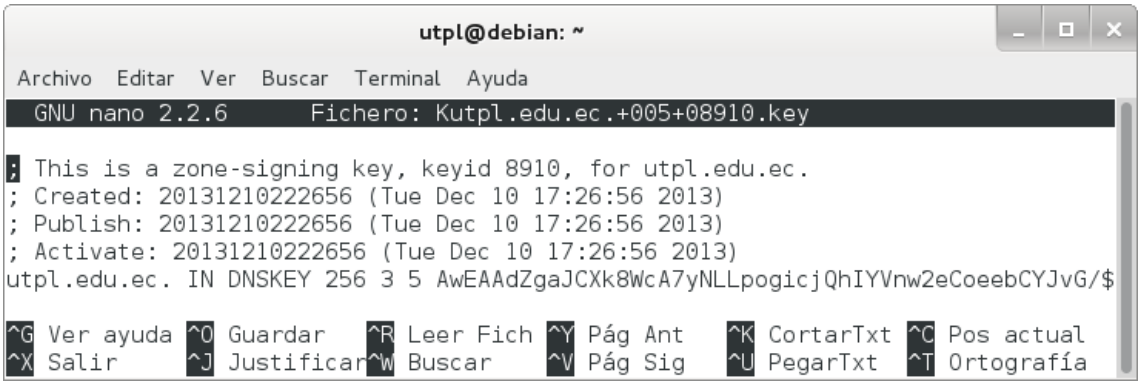

Figura 138. Archivo Kutpl.edu.ec.+005+08910.key.

Donde la clave pública (extensión .key) es tal y como aparece en el archivo de zona. Tenga en cuenta que no se especifica el valor TTL. Esta clave tiene un valor “bandera” de 256. Dado que este valor es un número par, la clave no está marcada como una clave SEP y se debe utilizar para la zona de firma.

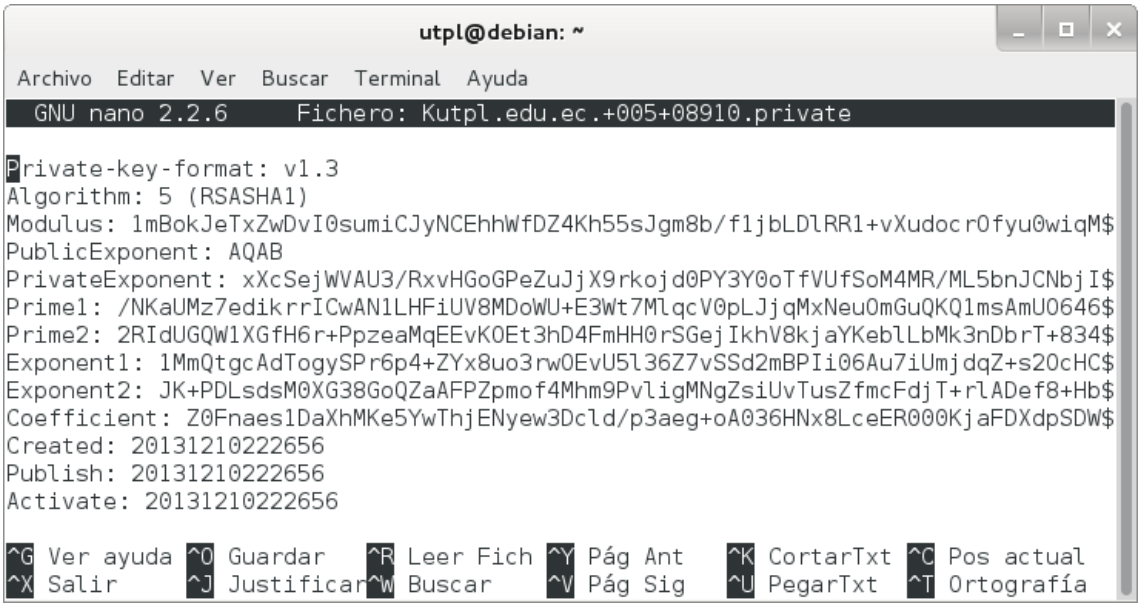

Figura 139. Archivo Kutpl.edu.ec.+005+08910.private.

Donde la clave privada (extensión .private) contiene todos los parámetros que hacen a una clave privada RSASHA1. La clave privada de una clave RSA contiene diferentes parámetros para DSA.

3. Insertar las claves de la zona.

Al crear pares de claves, estas se las incluyó en su archivo de zona.

Para incluir las claves en la zona se debe:

1. Añadir la directiva $INCLUDE en el archivo /etc/bind/db.utpl.edu.ec:

   $INCLUDE Kutpl.edu.ec.+005+38182.key

   $INCLUDE Kutpl.edu.ec.+005+08910.key

Observe la figura 140, donde se utiliza la directiva $INCLUDE para incluir las claves.

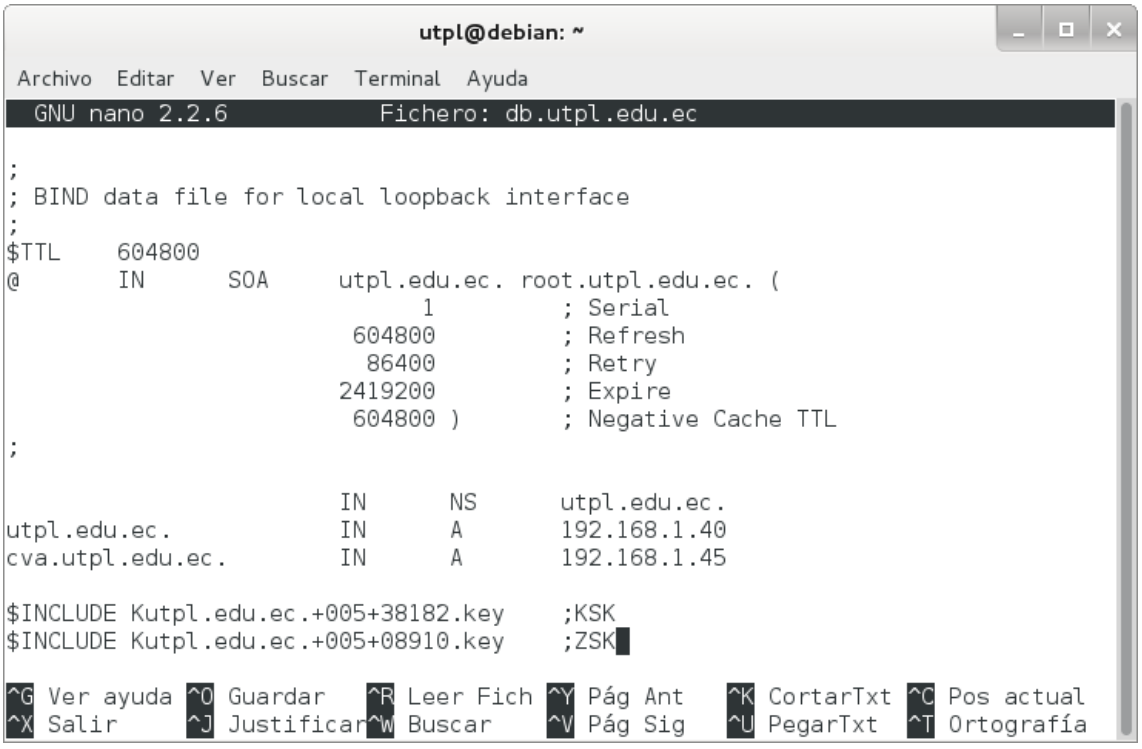

Figura 140. Inserción de las claves de la zona.

4. Firmar la zona.

Una vez que las claves han sido incluidas en el archivo de zona, se prosiguió a firmar la zona, para lo cual se utilizó la herramienta dnssec-signzone.

Para firmar la zona se realizó lo siguiente:

1. Emplear la herramienta dnssec-signzone:

 # dnssec-signzone -o utpl.edu.ec -k Kutpl.edu.ec.+005+59911.key db.utpl.edu.ec Kutpl.edu.ec.+005+31113.key

Donde se especifica a utpl.edu.ec como el origen de la zona, por defecto el origen se deduce del nombre del archivo de zona; se especifica qué clave se va a utilizar como KSK, la cual sólo firmará el conjunto DNSKEY RR en el vértice de la zona, la clave que se encuentra como argumento al final del comando se utiliza para firmar todos los datos de RR para los que la zona es autoritativa. Si no especifican las claves, BIND usará aquellas para las que las claves públicas están incluidas en la zona y usa la bandera SEP para distinguir entre las claves y las ZSK.

Las firmas se crean con un tiempo de vida por defecto de 30 días desde el momento de la firma. Una vez que las firmas han expirado los datos no pueden ser validados y su zona se marcará como 'falsa'. Por lo tanto, se tendrá que volver a firmar la zona dentro de los 30 días [17].

La zona firmada se almacena en el archivo db.utpl.edu.ec.signed, como se muestra en la figura 141.

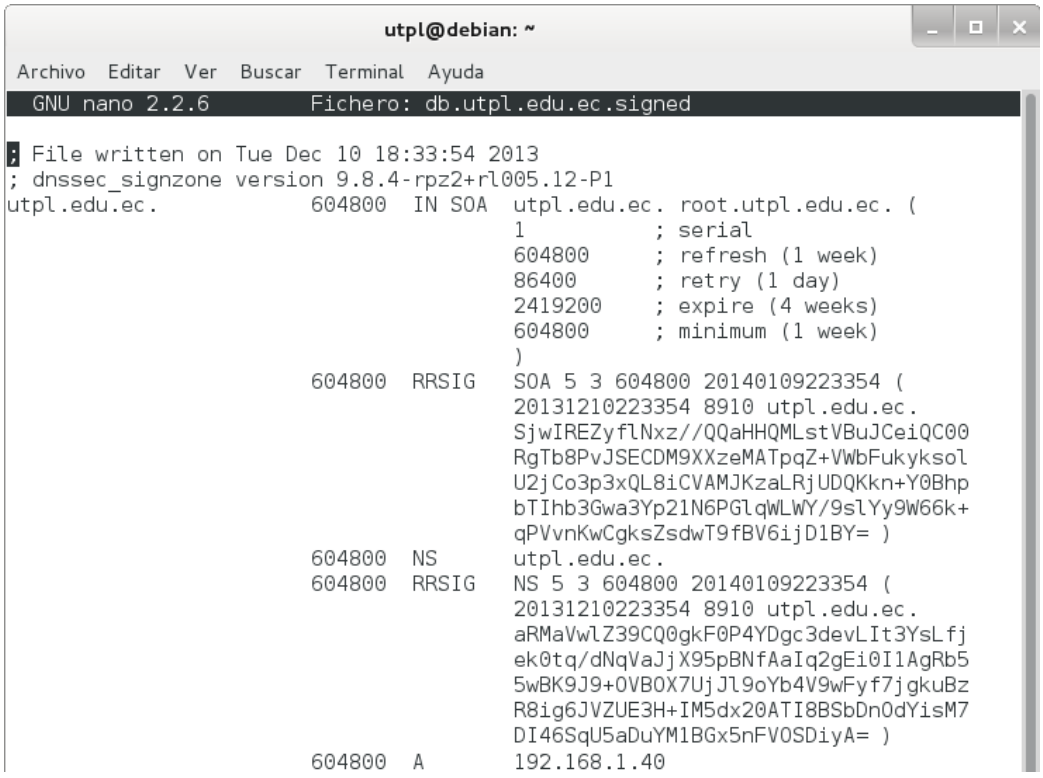

Figura 141. Archivo db.utpl.edu.ec.signed.

```
                        604800  RRSIG   A 5 3 604800 20140109223354 (
                                        20131210223354 8910 utpl.edu.ec.
                                        jG3V+l8LEB0iqobh0jbnD84XU0STXwlL+6vx
                                        i0p5vRXuCL0mEYeoviH1bnf+iaaZhOSc73nm
                                        4GxKmMe79jn6R5EuQczRW2NJEDGeWDuoMKwo
                                        NoO61bZeEM2+NN9uL8HeVujWD+ICGJ0o7jS3
                                        ELXfLV9kkZy9bmRW7bNrxc5naZg= )
                        604800  NSEC    cva.utpl.edu.ec. A NS SOA RRSIG NSEC DN$
                        604800  RRSIG   NSEC 5 3 604800 20140109223354 (
                                        20131210223354 8910 utpl.edu.ec.
                                        wI1vg/iDjG/fl2hg85my1vZkXQKEcv1DTPAL
                                        8ZNBkm3wVIbdc4YxL0i0WXJvwXgJNhuc/gol
                                        oMpfLJj5uPSeUMb79MhcY3TZOvDmxQOTcSjB
                                        O4x9xEG5rhwQ6dQnqWsoPB0Wlsunq1DR4yK1
                                        bpb0YPqvPS7z920wxpze0FT0FHU= )
                        604800  DNSKEY  256 3 5 (
                                        AwEAAdZgaJCXk8WcA7yNLLpogicjQhIYVnw2
                                        eCoeebCYJvG/39Y2yw5UUdfr17naHKzn8rtM
                                        IqjAhQQFtw15pzUCPH0GelifenAlGxU+s54+
                                        3jGShWqJHJEbPlhB8KREOQ4MSe0HcwYk51XQ
                                        8fMu4pA7VcBLOBoz9XemiQulCEjmcj13
                                        ) ; key id = 8910
                        604800  DNSKEY  257 3 5 (
                                        AwEAAd7QN37zw5ZTKlpJD/GSYRZtg6+kRJb4
                                        sHzlAhjzbPwBBkhFYgIkHJnzv//WJk7etG9k
                                        Ad0UwZ+pr9sILxGa/3pvTuSEAtJMYvhb2RCr
                                        go3EeIDtfnqzkev/VMaATriaq87XQbwsWQ9j
                                        ClV4ocmEaAxewGonUxorG6pMTk1pCKMEVVXq
                                        dFXXVBNxOzOsr01MCKYsl7Y9DhQgJCGBsAec
                                        qmM=
                                        ) ; key id = 38182
                        604800  RRSIG   DNSKEY 5 3 604800 20140109223354 (
                                        20131210223354 8910 utpl.edu.ec.
                                        i0zbugvmPCfDEDvIvp7j5oahzskAnOtgOTSg
                                        9mzxijOzTvDKnAiLNEoJ9myfHARe6wZ+xfEU
                                        c3LVzbxIoOjfd0sSVUt6836n0xxNYXoicWwi
                                        BpZThSPgs6x9avRBaJxTm/kKcgIj8NPDud6x
                                        hK8t8m84znkdmrUG7Gz4D+BU0/M= )
                        604800  RRSIG   DNSKEY 5 3 604800 20140109223354 (
                                        20131210223354 38182 utpl.edu.ec.
                                        tkyjXHSrdlf/tVg3wAjLdCfbzLtqSkxam6ZO
                                        f7FciYt7ymFkM8yyA5XI+w746XK9nSH28vh/
                                        cNpe5DwTULw0w2n/q1UdCHU054fOBLQmv2te
                                        4XB/f54HuOBDQ4GwxXlVkdjE9Q3CGeevA9OQ
                                        iH2SD7oOcqnjDZLwFEL+AVgaV21XnVvzTnaQ
                                        NiOjDgNYc5w2mTzAmHFU8qiJ+MNYgJyR6g== )
cva.utpl.edu.ec.        604800  IN A   192.168.1.45
                        604800  RRSIG   A 5 4 604800 20140109223354 (
                                        20131210223354 8910 utpl.edu.ec.
                                        bhSnKd/J4u3EGHzHFs6Wg1NIesP3um/j6gkP
                                        apRvVI+xcxVE4tzLOfTOTrrpGn1L6Bl86ll7
                                        UQKHohjXq5oGoHv+a4of5x6voEJ6Ln5ZWUZv
                                        yduoo6+ysKl3Uyd+fopoSeWD4lOwANAp194u
                                        kt01vnERNljxoRHW3ekKVtvJjsA= )
                        604800  NSEC    utpl.edu.ec. A RRSIG NSEC
                        604800  RRSIG   NSEC 5 4 604800 20140109223354 (
                                        20131210223354 8910 utpl.edu.ec.
                                        wfk4Tv3e5dR6pgnKAM/0fSV5RRXmi7khP+FB
                                        iVstZa5eRd533w2Y1Bei2Ldl3qslfgdyOe6f
                                        Yd8xXylt35voqQ0cazW+WIn3n8KKNM5fA4om
                                        NESbZ2rH49Byno9iIFjSMuPnIJ3ffdDgHcsK
                                        4V0DD6qxuIt9OXLzzhs6bFnEYzo= )

^G Ver ayuda ^O Guardar   ^R Leer Fich ^Y Pág Ant   ^K CortarTxt ^C Pos actual
^X Salir     ^J Justificar^W Buscar    ^V Pág Sig   ^U PegarTxt  ^T Ortografía
```

Figura 141. Archivo db.utpl.edu.ec.signed (continuación).

2. Comprobar si el archivo de zona db.utpl.edu.ec.signed fue generado:

   # *named-checkzone utpl.edu.ec. db.utpl.edu.ec.signed*

Con lo que se comprueba que la zona ha sido firmada, como se observa en la figura 142.

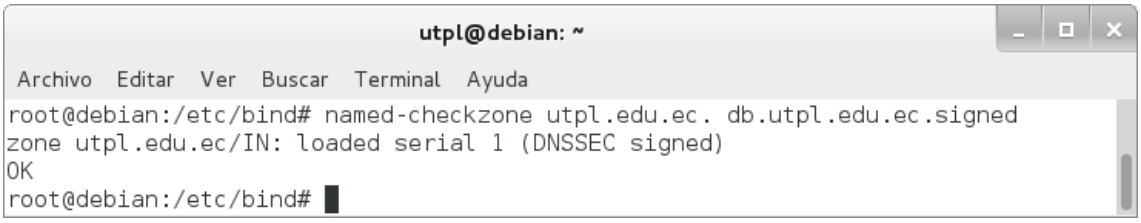

Figura 142. Ejecución de named-checkzone sin errores.

3. Cambiar en el archivo de configuración named.conf.local, el nombre del archivo de zona para el nuevo nombre que contiene la zona utpl.edu.ec ya firmada:

   zone "utpl.edu.ec." {
   type master;
   file "/etc/bind/db.utpl.edu.ec.signed";
   };

Quedando como se muestra en la figura 143.

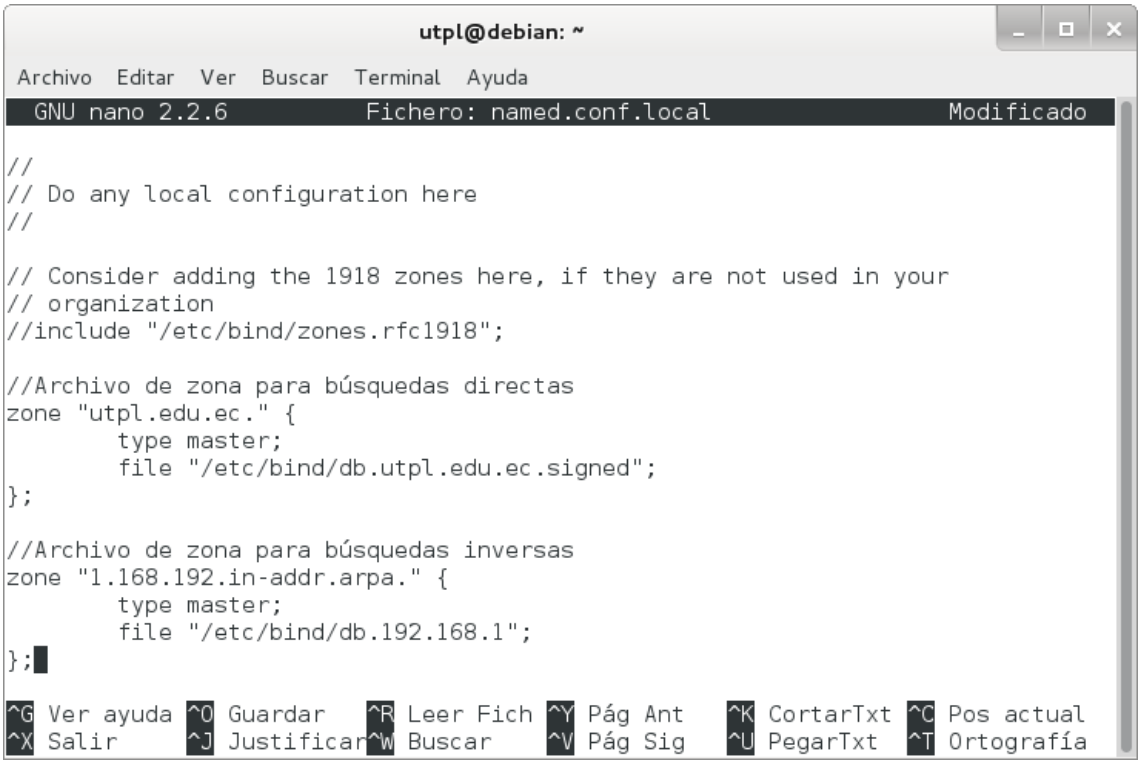

Figura 143. Archivo named.conf.local.

4. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 144.

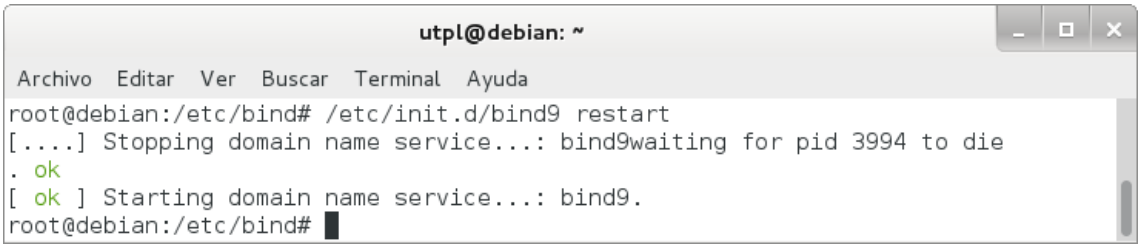

Figura 144. Reinicio del servicio.

5. Realizar pruebas.

Se comprobó si el servidor de nombres emite respuestas y si estas respuestas contienen información DNSSEC.

Para ello se realizó lo siguiente:

1. Emplear el comando dig:

 # dig @localhost utpl.edu.ec SOA +dnssec +multiline

Con lo que el resultado de la zona utpl.edu.ec configurada correctamente quedaría como se muestra en la figura 145.

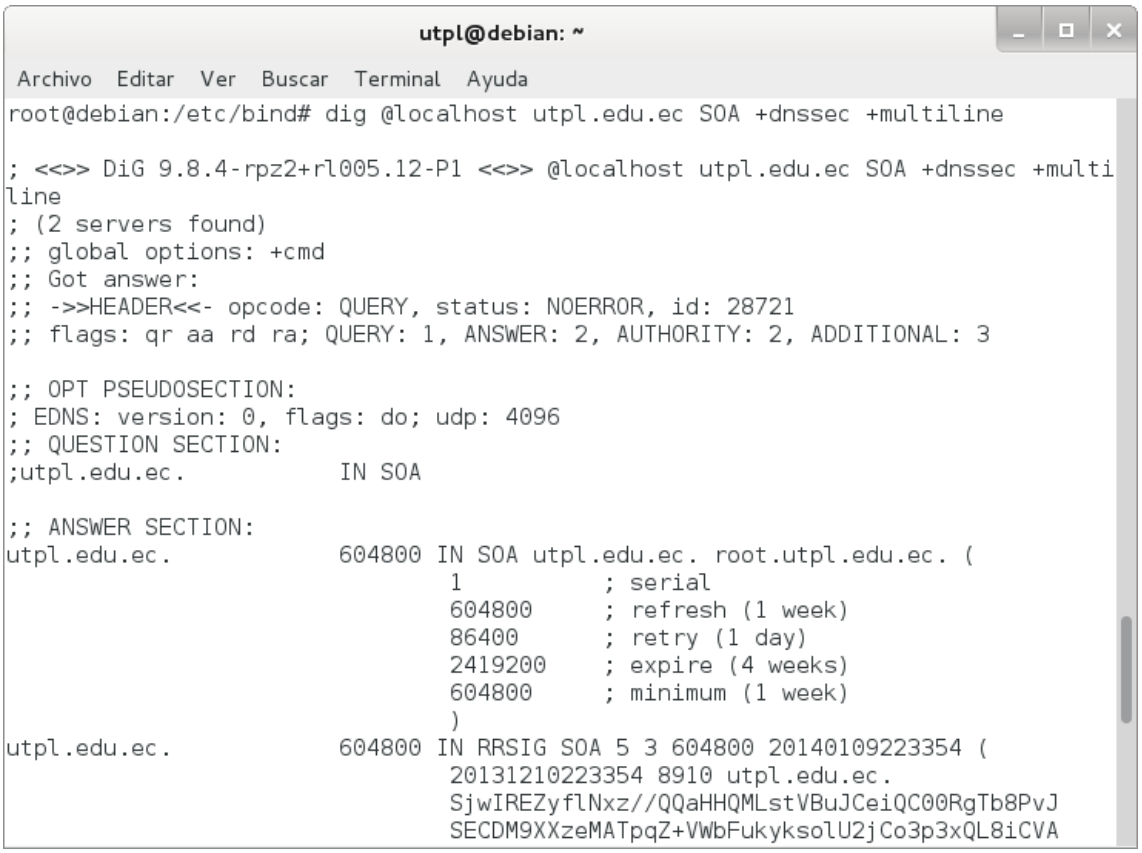

Figura 145. Ejecución correcta de dig.

Anexo 13: Aseguramiento de la zona DNS de la comunidad virtual de aprendizaje de la Universidad Técnica Particular de Loja.

1. Configurar servidor autoritativo.

El servidor autoritativo se configuró para soportar DNSSEC. Los pasos esenciales fueron:

1. Revisar que Bind esté compilado con OpenSSL:

 # named -V

Donde se puede observar la versión de OpenSSL que se está usando, tal como en la figura 146.

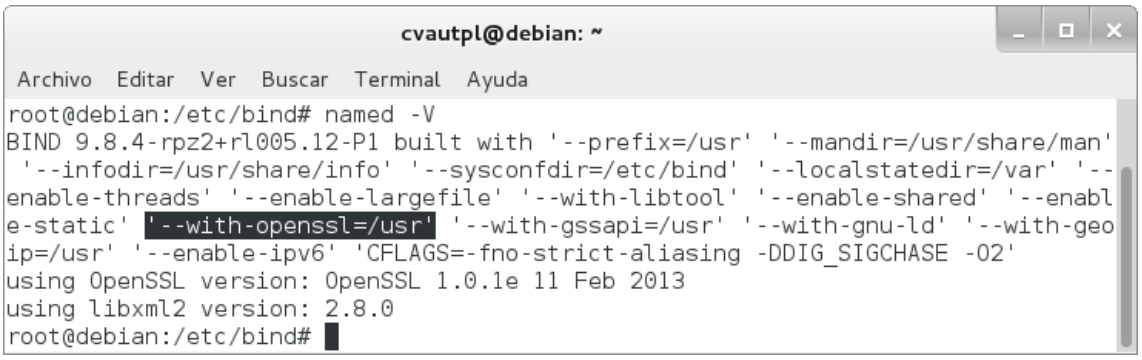

Figura 146. Compilación de Bind.

2. Habilitar DNSSEC en el archivo /etc/bind/named.conf.options:

```
options {
        dnssec-enable yes;
        dnssec-validation auto;
        dnssec-lookaside auto;
};
```

Con lo que se permite la habilitación, validación y lookaside de DNSSEC, como se muestra en la figura 147.

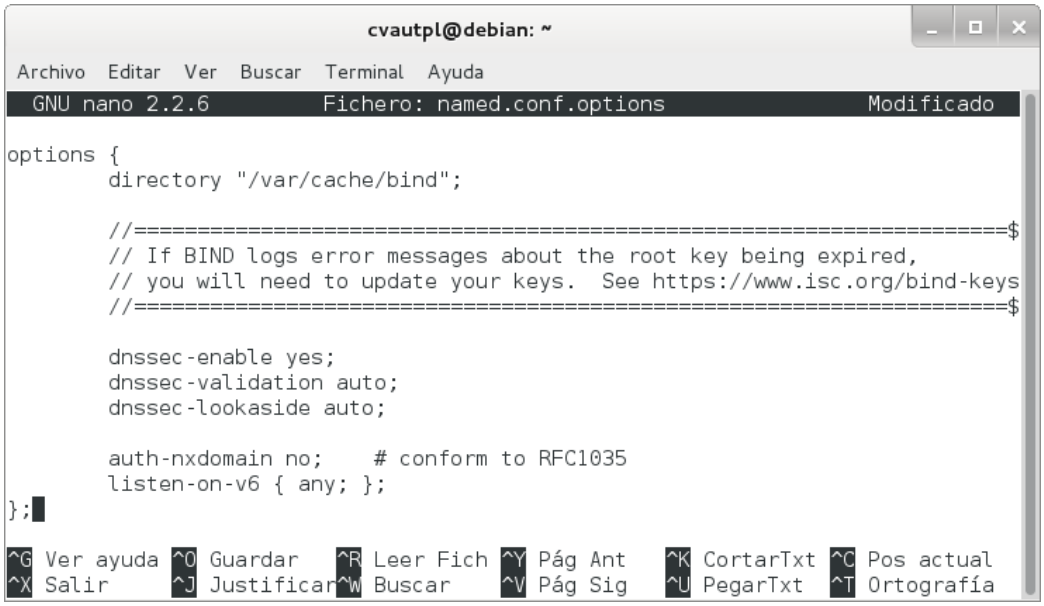

Figura 147. Habilitación de DNSSEC.

3. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 148.

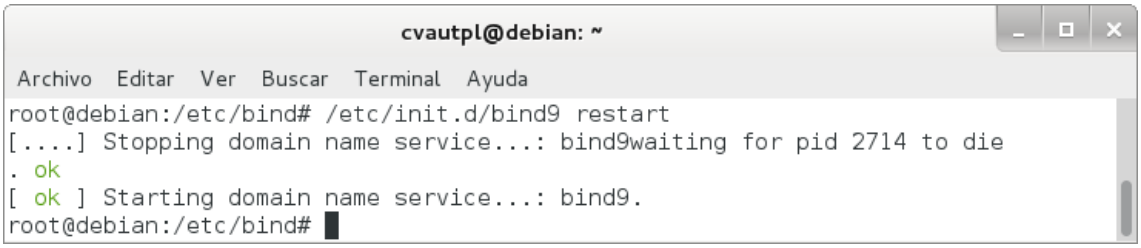

Figura 148. Reinicio del servicio.

2. Crear pares de claves.

Es necesario crear una KSK (Key Signing Key) inicial y ZSK (Zone Signing Key) para cada zona para estar asegurado. Las partes privadas deben mantenerse en privado y seguras [34].

La salida se puede encontrar en dos archivos. El nombre de los archivos contienen información relevante:

Knombre_dominio+id_algoritmo+id_clave.extension

El nombre_dominio es el nombre especificado en la línea de comandos. Es utilizado por otras herramientas de BIND de DNSSEC. El id_algoritmo identifica el algoritmo utilizado: 1 para RSAMD5, 3 de DSA, 5 para RSASHA1 y 54 de HMAC-MD5. El id_clave es un identificador para el contenido de la clave. Este id_clave es utilizado por el registro de recurso RRSIG. La extension es cualquier key o private, la primera es la clave pública y la segunda es la clave privada [17].

Los pasos para crear las claves fueron:

1. Crear la KSK:

   # dnssec-keygen -r /dev/random -f KSK -a RSASHA1 -b 1280 -n ZONE cva.utpl.edu.ec

Donde se crea un par de KSK con el tipo de algoritmo RSASHA1, tamaño de la clave 1280 y cva.utpl.edu.ec como el nombre de la zona, tal como se observa en la figura 149.

Figura 149. KSK.

Mediante este comando se generan dos archivos, cuyos contenidos se muestran en las figuras 150 y 151.

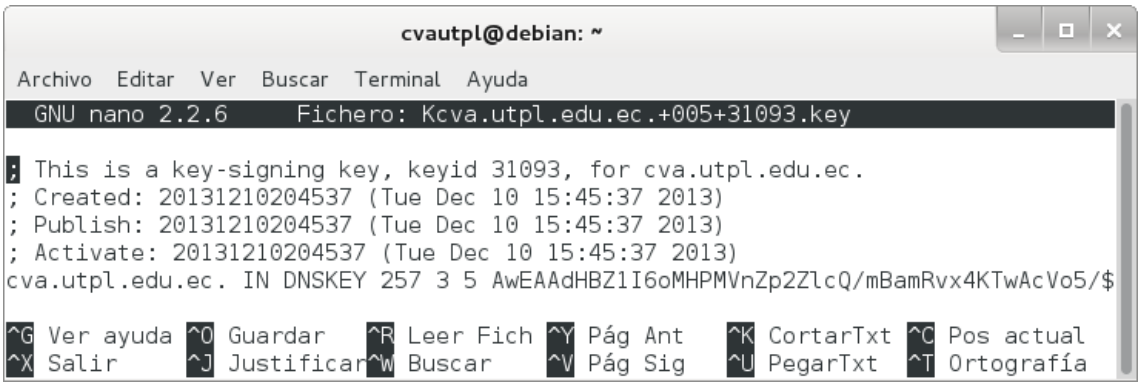

Figura 150. Archivo Kcva.utpl.edu.ec.+005+31093.key.

Donde la clave pública (extensión .key) es tal y como aparece en el archivo de zona. Tenga en cuenta que no se especifica el valor TTL. Esta clave tiene un valor "bandera" de 257. Dado que este valor es un número impar, la clave está marcada como una clave SEP y no se debe utilizar para la zona de firma.

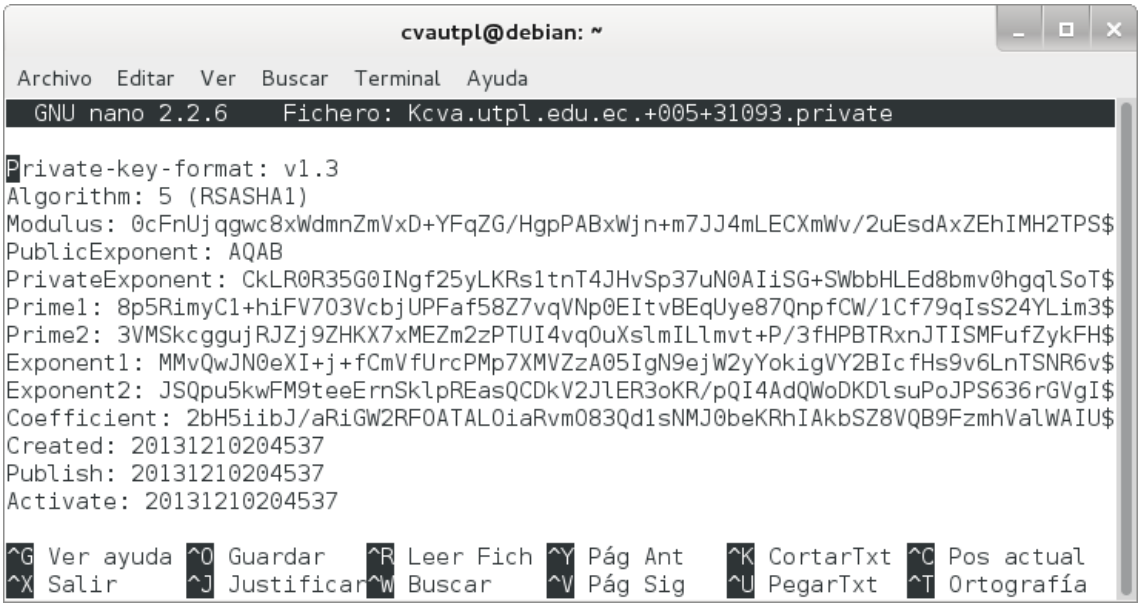

Figura 151. Archivo Kcva.utpl.edu.ec.+005+31093.private.

Donde la clave privada (extensión .private) contiene todos los parámetros que hacen a una clave privada RSASHA1. La clave privada de una clave RSA contiene diferentes parámetros para DSA.

2. Crear la ZSK:

 # dnssec-keygen -r /dev/random -a RSASHA1 -b 1024 -n ZONE cva.utpl.edu.ec

Donde se crea un par de ZSK con el tipo de algoritmo RSASHA1, tamaño de la clave 1024 y cva.utpl.edu.ec como el nombre de la zona, tal como se observa en la figura 152.

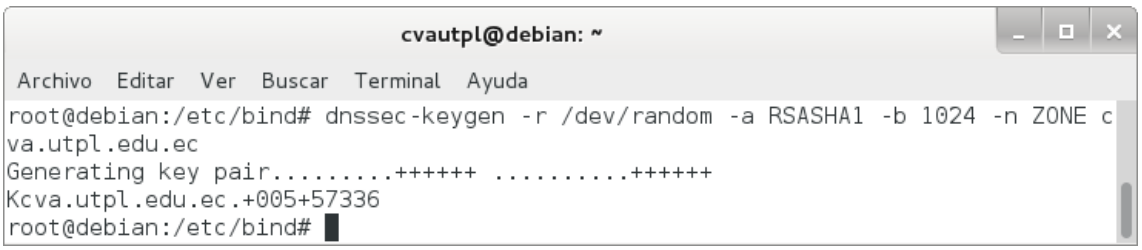

Figura 152. ZSK.

Mediante este comando se generan dos archivos, cuyos contenidos se muestran en las figuras 153 y 154.

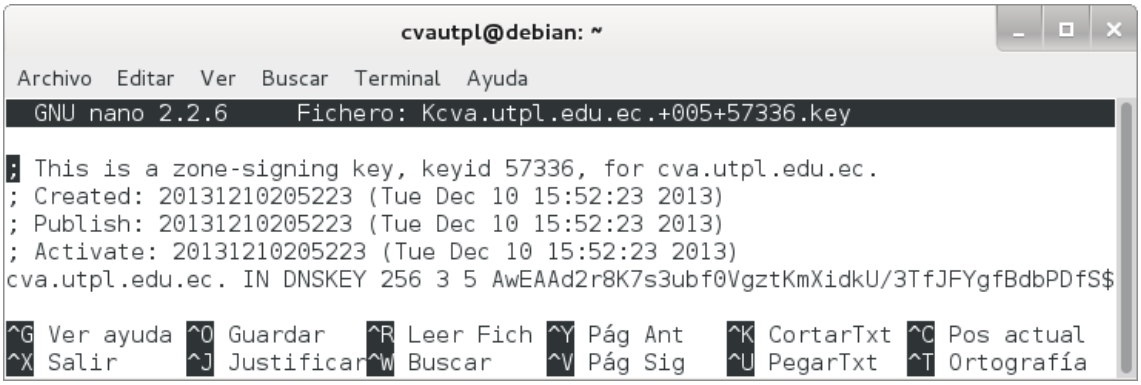

Figura 153. Archivo Kcva.utpl.edu.ec.+005+57336.key.

Donde la clave pública (extensión .key) es tal y como aparece en el archivo de zona. Tenga en cuenta que no se especifica el valor TTL. Esta clave tiene un valor “bandera” de 256. Dado que este valor es un número par, la clave no está marcada como una clave SEP y se debe utilizar para la zona de firma.

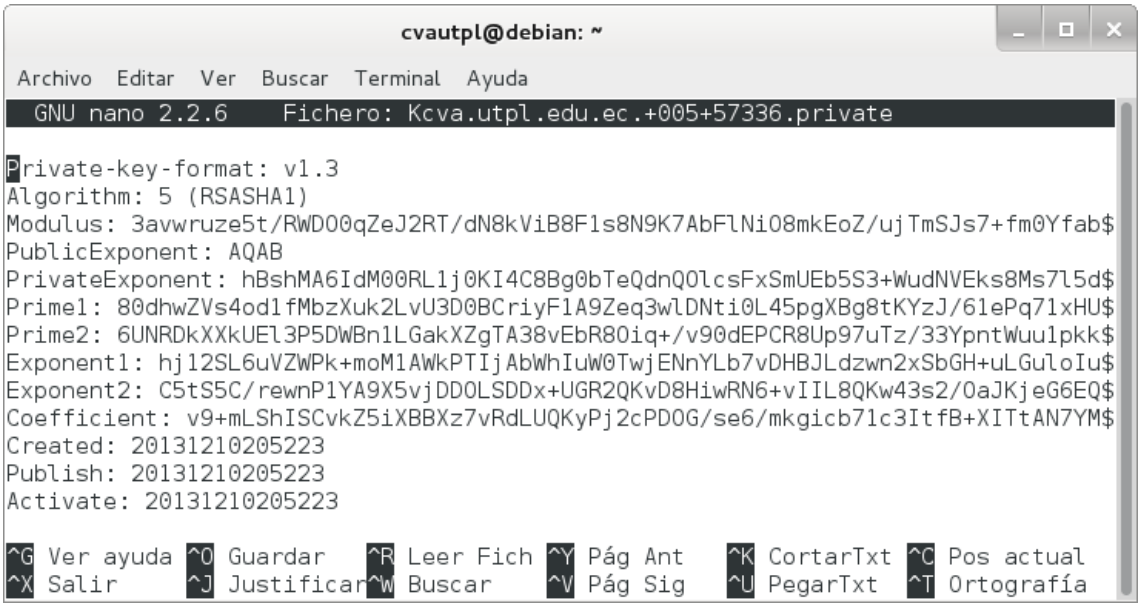

Figura 154. Archivo Kcva.utpl.edu.ec.+005+57336.private.

Donde la clave privada (extensión .private) contiene todos los parámetros que hacen a una clave privada RSASHA1. La clave privada de una clave RSA contiene diferentes parámetros para DSA.

3. Insertar las claves de la zona.

Al crear pares de claves, estas se las incluyó en su archivo de zona.

Para incluir las claves en la zona se debe:

1. Añadir la directiva $INCLUDE en el archivo /etc/bind/db.cva.utpl.edu.ec:

   $INCLUDE Kcva.utpl.edu.ec.+005+.31093.key

   $INCLUDE Kcva.utpl.edu.ec.+005+57336.key

Observe la figura 155, donde se utiliza la directiva $INCLUDE para incluir las claves.

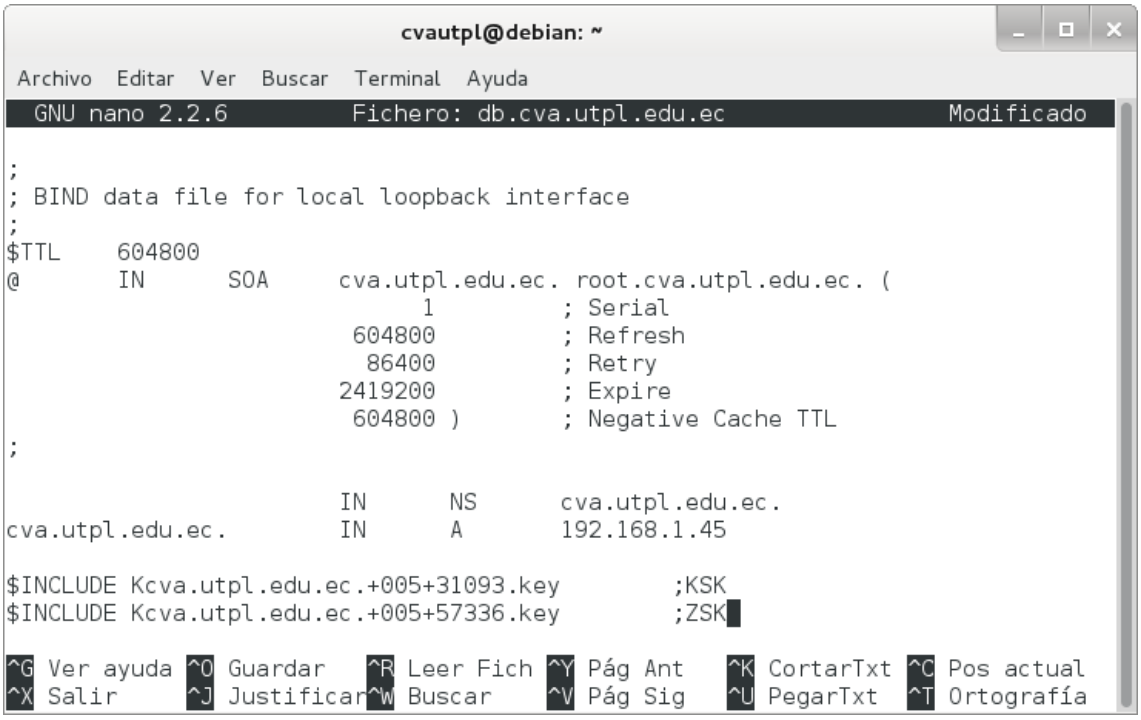

Figura 155. Inserción de las claves de la zona.

4. Firmar la zona.

Una vez que las claves han sido incluidas en el archivo de zona, se prosiguió a firmar la zona, para lo cual se utilizó la herramienta dnssec-signzone.

Para firmar la zona se realizó lo siguiente:

1. Emplear la herramienta dnssec-signzone:

 # dnssec-signzone -o cva.utpl.edu.ec -k Kcva.utpl.edu.ec.+005+59911.key db.cva.utpl.edu.ec Kcva.utpl.edu.ec.+005+31113.key

Donde se especifica a cva.utpl.edu.ec como el origen de la zona, por defecto el origen se deduce del nombre del archivo de zona; se especifica qué clave se va a utilizar como KSK, la cual sólo firmará el conjunto DNSKEY RR en el vértice de la zona, la clave que se encuentra como argumento al final del comando se utiliza para firmar todos los datos de RR para los que la zona es autoritativa. Si no especifican las claves, BIND usará aquellas para las que las claves públicas están incluidas en la zona y usa la bandera SEP para distinguir entre las claves y las ZSK.

Las firmas se crean con un tiempo de vida por defecto de 30 días desde el momento de la firma. Una vez que las firmas han expirado los datos no pueden ser validados y su zona se marcará como 'falsa'. Por lo tanto, se tendrá que volver a firmar la zona dentro de los 30 días [17].

La zona firmada se almacena en el archivo db.cva.utpl.edu.ec.signed, como se muestra en la figura 156.

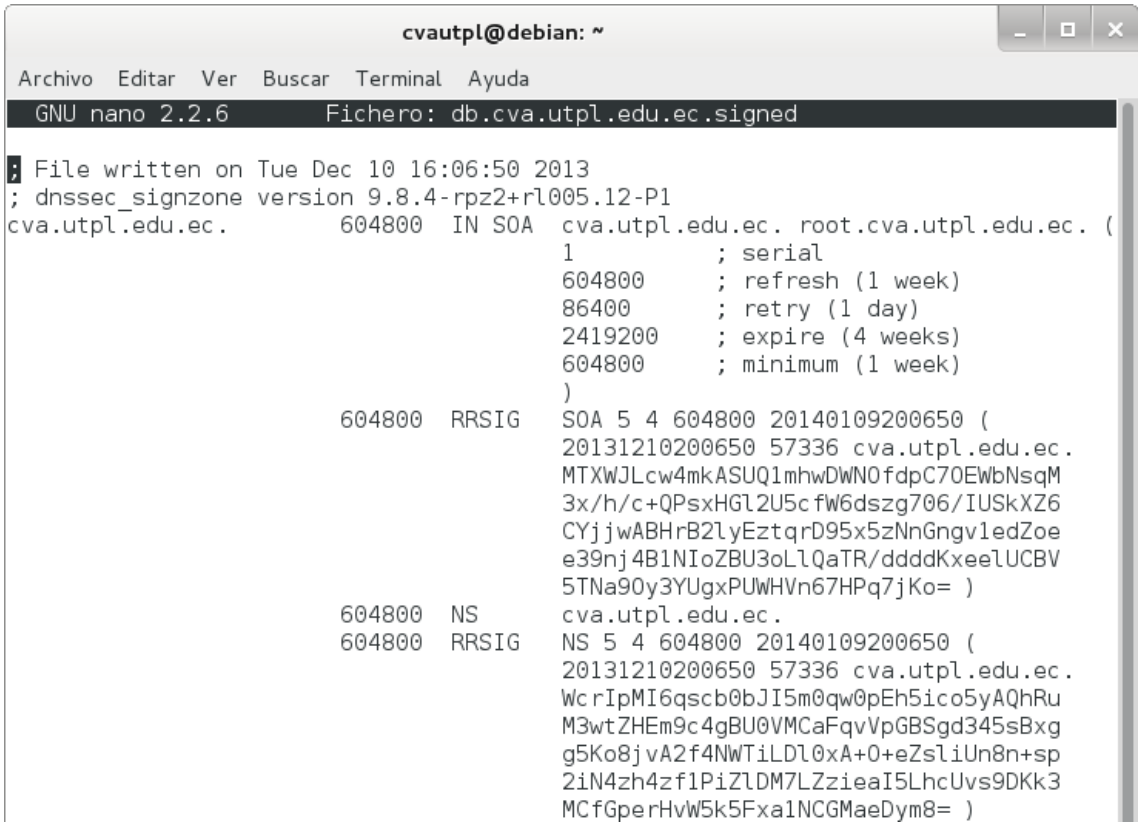

Figura 156. Archivo db.cva.utpl.edu.ec.signed.

Figura 156. Archivo db.cva.utpl.edu.ec.signed (continuación).

2. Comprobar si el archivo de zona db.cva.utpl.edu.ec.signed fue generado:

 # named-checkzone cva.utpl.edu.ec. db.cva.utpl.edu.ec.signed

Con lo que se comprueba que la zona ha sido firmada, como se observa en la figura 157.

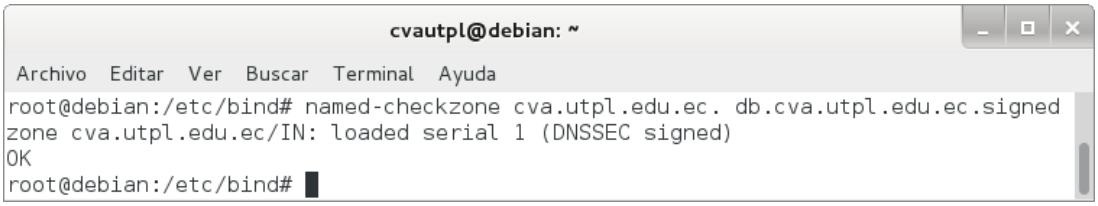

Figura 157. Ejecución de named-checkzone sin errores.

3. Cambiar en el archivo de configuración named.conf.local, el nombre del archivo de zona para el nuevo nombre que contiene la zona cva.utpl.edu.ec ya firmada:

zone "cva.utpl.edu.ec." {

type master;

file "/etc/bind/db.cva.utpl.edu.ec.signed";

};

Quedando como se muestra en la figura 158.

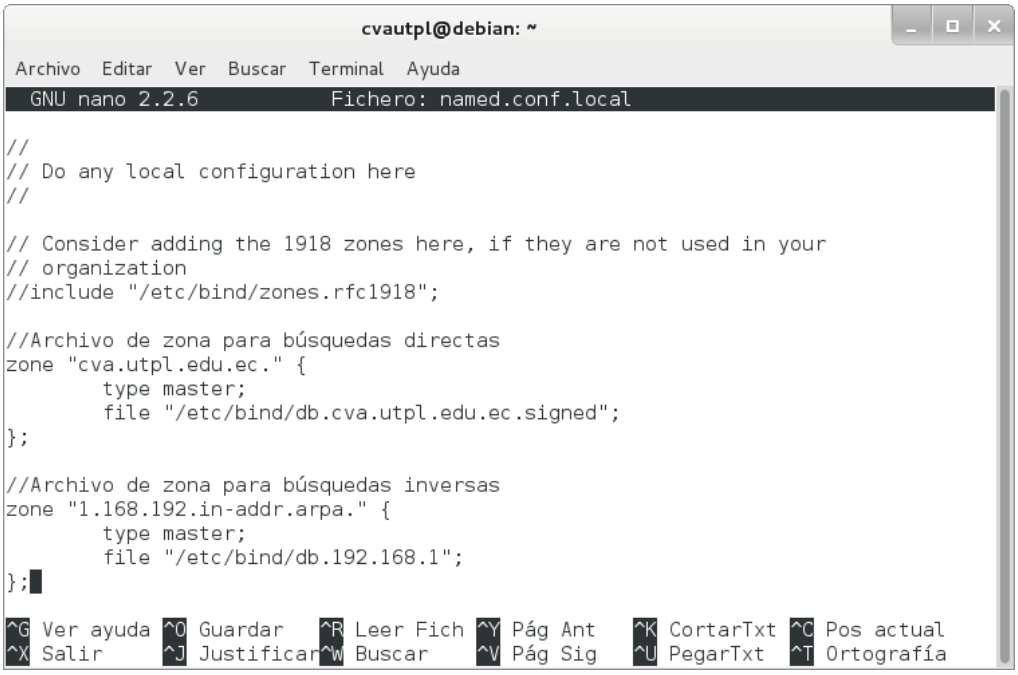

Figura 158. Archivo named.conf.local.

4. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 159.

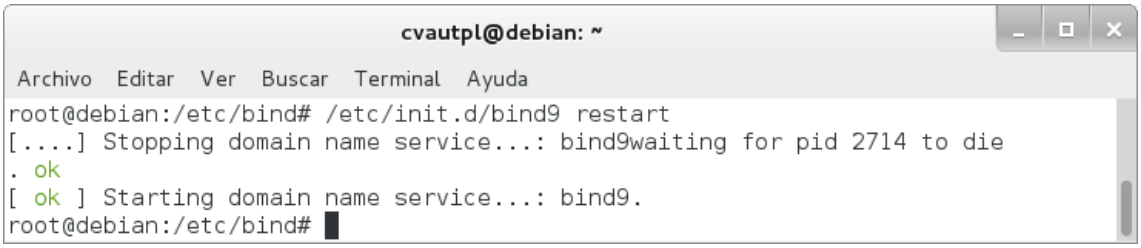

Figura 159. Reinicio del servicio.

5. Realizar pruebas.

Se comprobó si el servidor de nombres emite respuestas y si estas respuestas contienen información DNSSEC.

Para ello se realizó lo siguiente:

1. Emplear el comando dig:

 # dig @localhost cva.utpl.edu.ec SOA +dnssec +multiline

Con lo que el resultado de la zona cva.utpl.edu.ec configurada correctamente quedaría como se muestra en la figura 160.

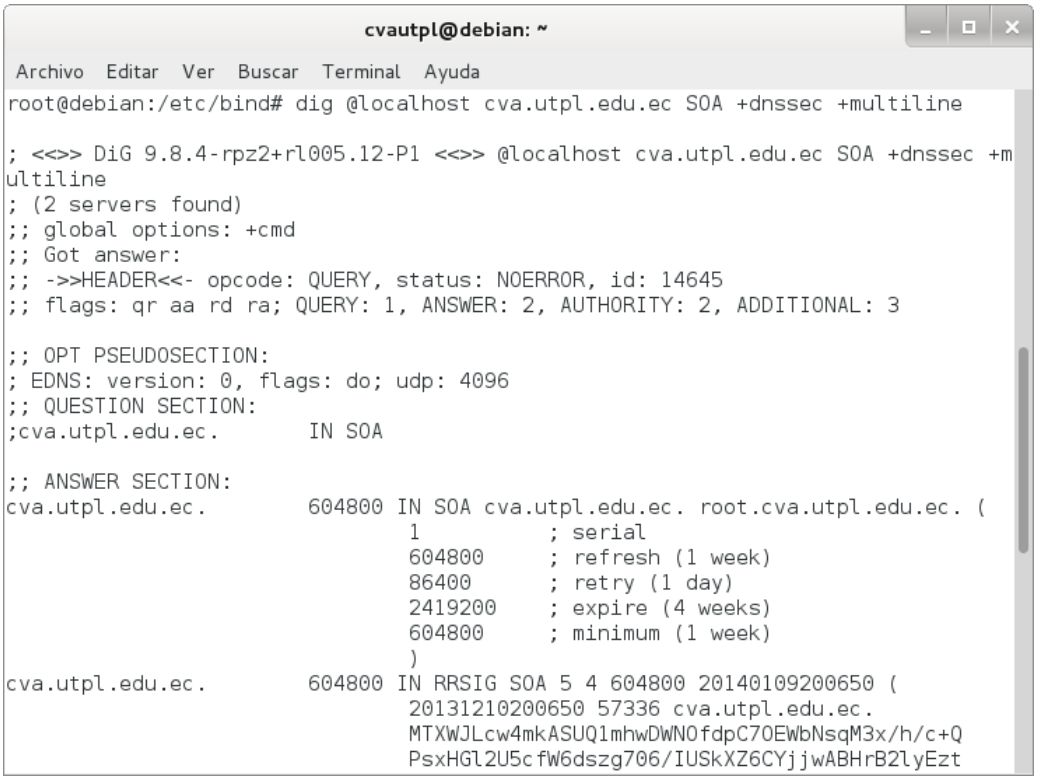

Figura 160. Ejecución correcta de dig.

Anexo 14: Configuración del promotor de almacenamiento en caché.

1. Instalación y configuración del servidor.

La configuración que se estableció para el servidor se muestra de manera gráfica en la figura 6, la misma que es la siguiente:

- **Promotor de almacenamiento en caché**
  - Dirección IP del servidor: **192.168.1.60**
  - Nombre del servidor: **resolver**

Para instalar y configurar el servidor se siguieron los siguientes pasos:

1. Instalar BIND 9 con OpenSSL:

 # apt-get install bind9

Mediante este comando se puede observar la información en modo texto sobre los paquetes extra que serán instalados, los paquetes sugeridos para la instalación, los paquetes nuevos y las actualizaciones que serán realizadas en los paquetes existentes, tal como se muestra en la figura 161.

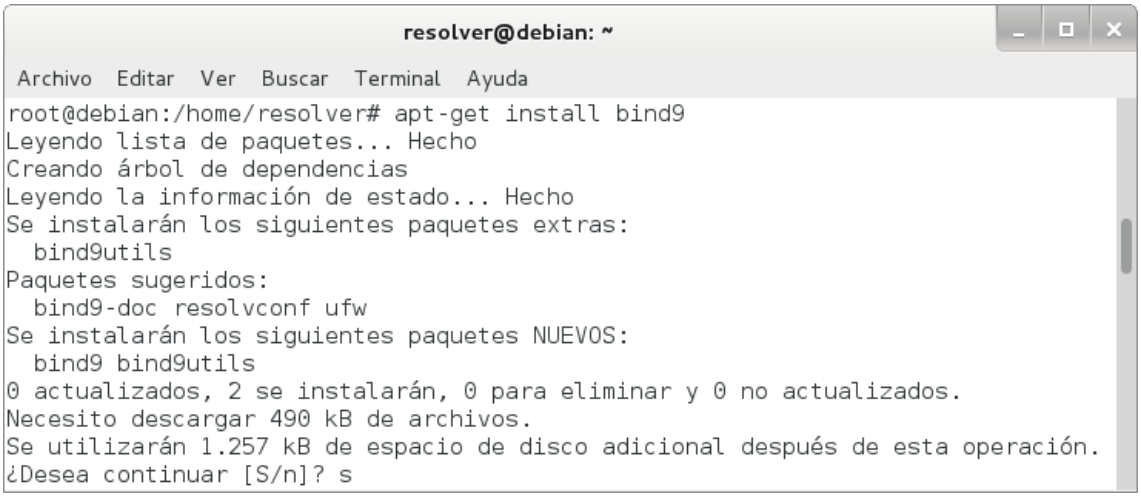

Figura 161. Instalación de Bind.

2. Revisar que Bind esté compilado con OpenSSL:

 # named -V

Donde se puede observar la versión de OpenSSL que se está usando, tal como en la figura 162.

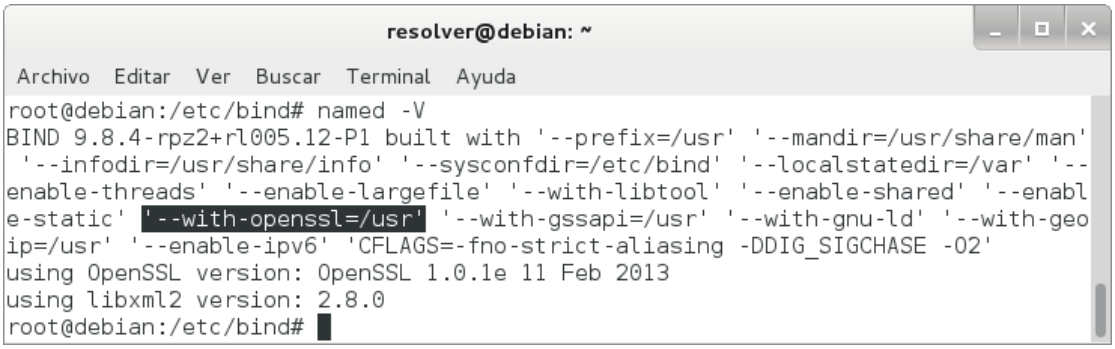

Figura 162. Compilación de Bind.

3. Habilitar DNSSEC en el archivo /etc/bind/named.conf.options:

```
options {
        dnssec-enable yes;
        dnssec-validation auto;
        dnssec-lookaside auto;
};
```

Con lo que se permite la habilitación, validación y lookaside de DNSSEC, como se muestra en la figura 163.

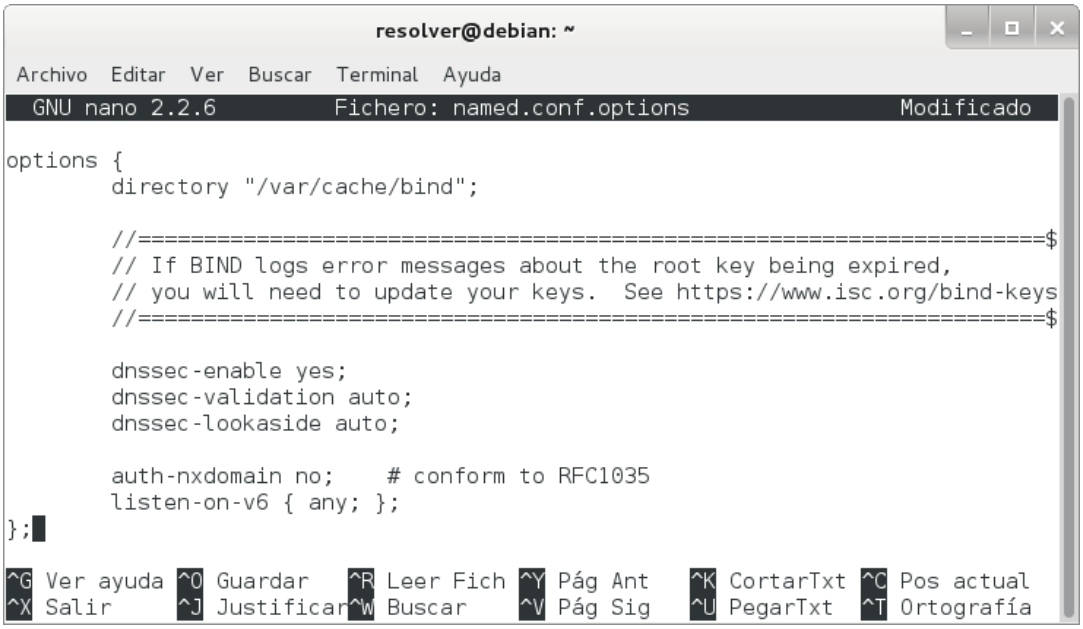

Figura 163. Habilitación de DNSSEC.

4. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 164.

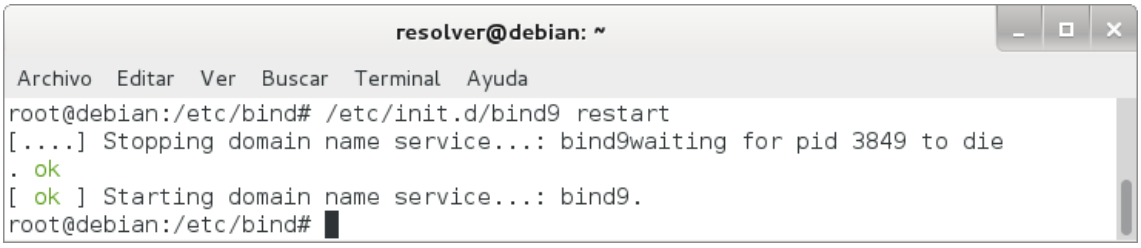

Figura 164. Reinicio del servicio.

2. Configurar un ancla de confianza.

Un ancla de confianza es una clave pública que se configura como el punto de entrada para una cadena de autoridad. En el caso ideal (donde la zona raíz se encuentre firmada y las cadenas de confianza se puedan construir a partir de los dominios de alto nivel hasta los nodos finales) los servidores de nombres validadores sólo necesitarán una de estas anclas de confianza para ser configurados [17]. Pero debido a que las zonas padres (ec., edu.ec.) aún no están firmadas se debe configurar múltiples anclas de confianza.

Para configurar un ancla de confianza en el servidor recursivo se hizo:

1. Crear el archivo /etc/bind/named.conf.keys:

 # nano /etc/bind/named.conf.keys

Donde se añade la sección managed-keys que incluye la clave pública (clave KSK) de las zonas unl.edu.ec, cva.unl.edu.ec, utpl.edu.ec y cva.utpl.edu.ec, como se muestra en la figura 165; siendo esta clave la ancla de confianza, después de que los registros DS se han cargado al registrador, esta ancla de confianza ya no es necesaria porque se tiene la clave de zona raíz en la configuración.

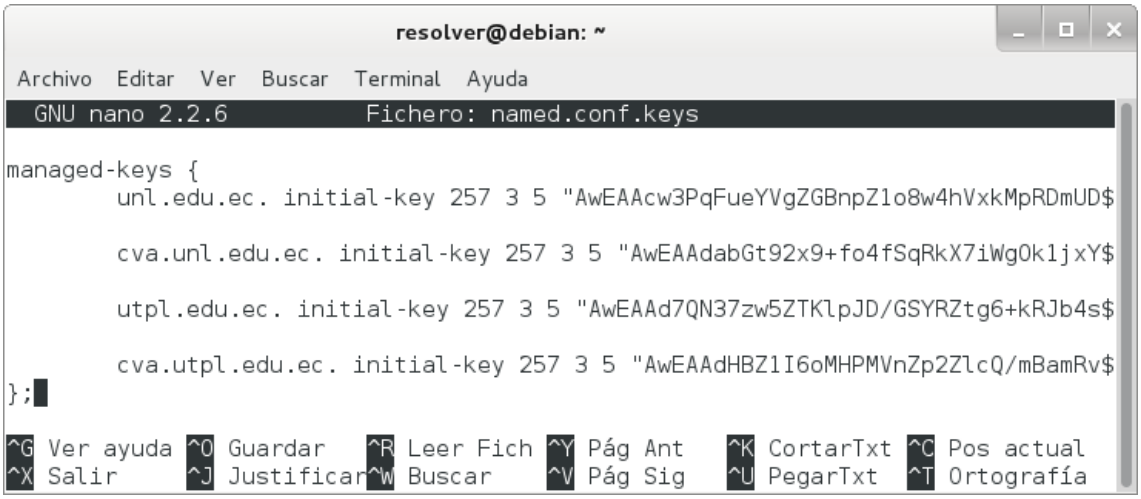

Figura 165. Archivo named.conf.keys.

2. Incluir el archivo /etc/bind/named.conf.keys en el archivo /etc/bind/named.conf:

include "/etc/bind/named.conf.keys";

Observe la figura 166, donde se incluye el archivo /etc/bind/named.conf.keys.

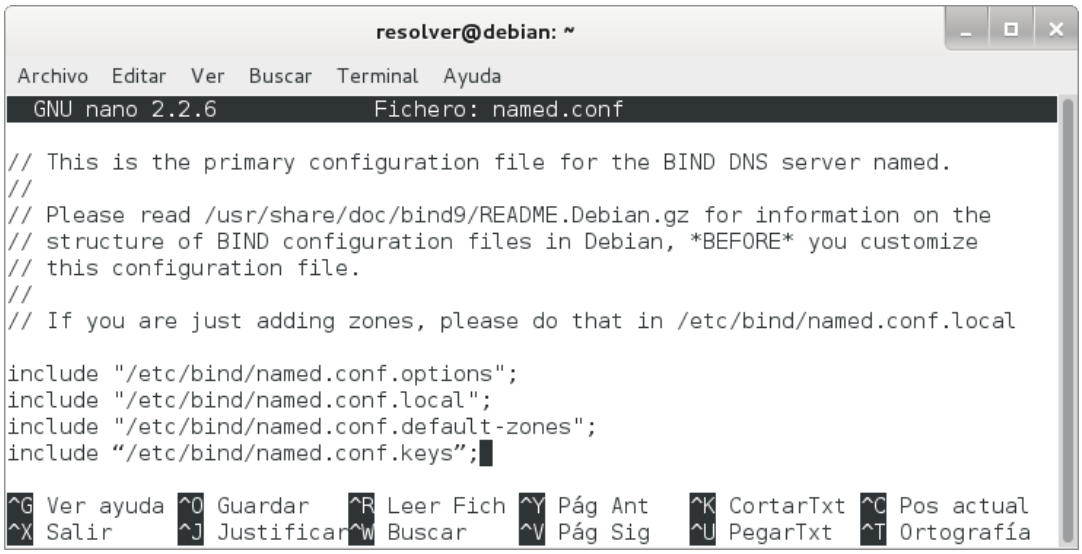

Figura 166. Inserción del archivo named.conf.keys.

3. Modificar el archivo /etc/bind/named.conf.options:

 # nano /etc/bind/named.conf.options

Donde se agregan las direcciones IP de los servidores maestros en la sección forwarders, como se observa en la figura 167.

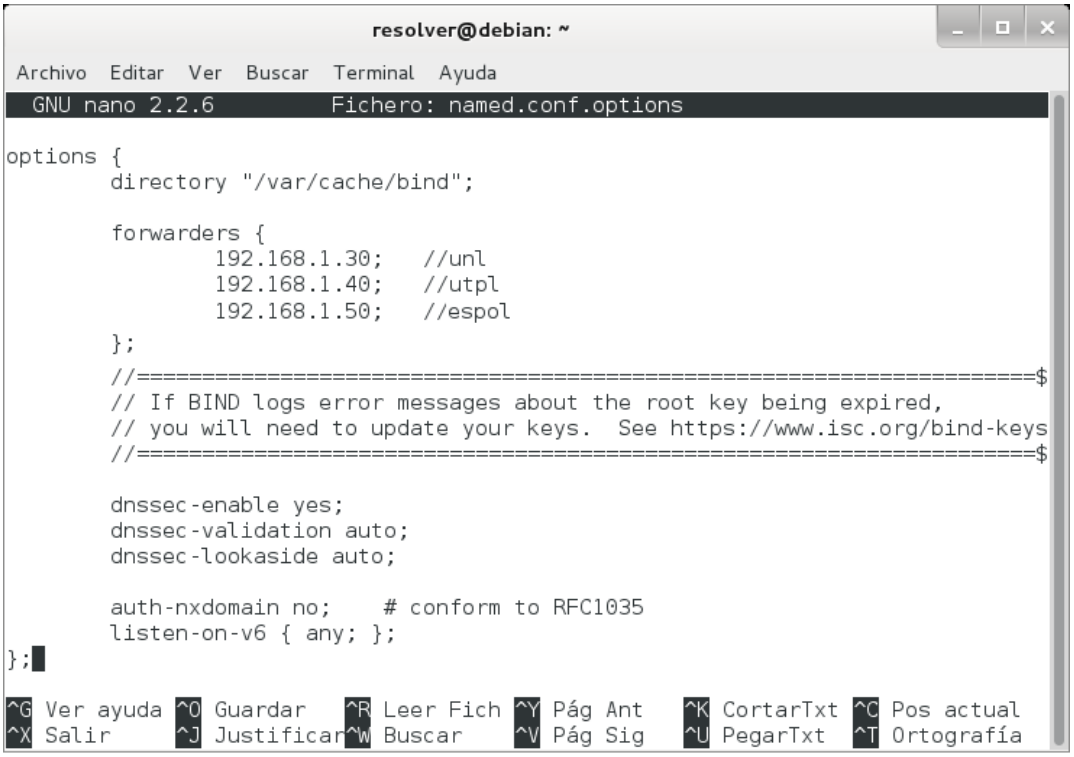

Figura 167. Archivo named.conf.options.

4. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 168.

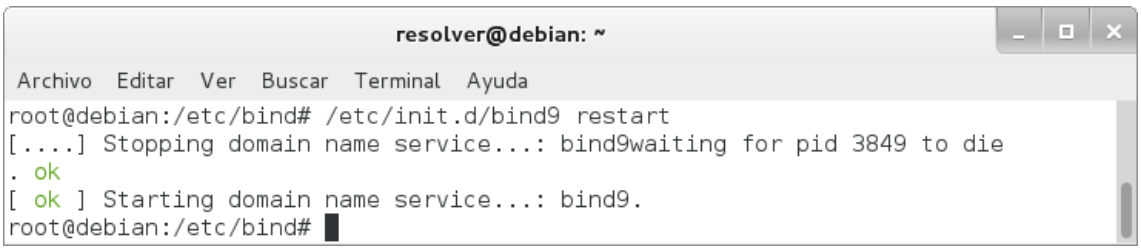

Figura 168. Reinicio del servicio.

3. Configurar el registro.

Es importante que se compruebe que la validación está funcionando correctamente. Esto se puede hacer mediante el uso de las facilidades del registro de BIND en la máquina que está configurado como servidor de nombres recursivo validador.

En BIND los mensajes de una determinada categoría se pueden registrar en canales separados. Los canales determinan dónde los mensajes van y qué nivel de gravedad tendrán para ser reportados. La categoría pertinente para la validación DNSSEC es dnssec. Con el fin de seguir el proceso de validación del canal tiene que iniciar al menos severidad de depuración 3 [17].

Para configurar el registro se debe:

1. Crear el archivo /var/log/dnssec.log:

   # nano /var/log/dnssec.log

2. Crear el archivo /etc/bind/named.conf.logging:

   # nano /etc/bind/named.conf.logging

Donde se especifica el canal de registro de DNSSEC, la marca de tiempo de las entradas, se agrega el nombre de la categoría de las entradas, se añade el nivel de gravedad de las entradas y se imprime el mensaje de depuración; tal como se muestra en la figura 169.

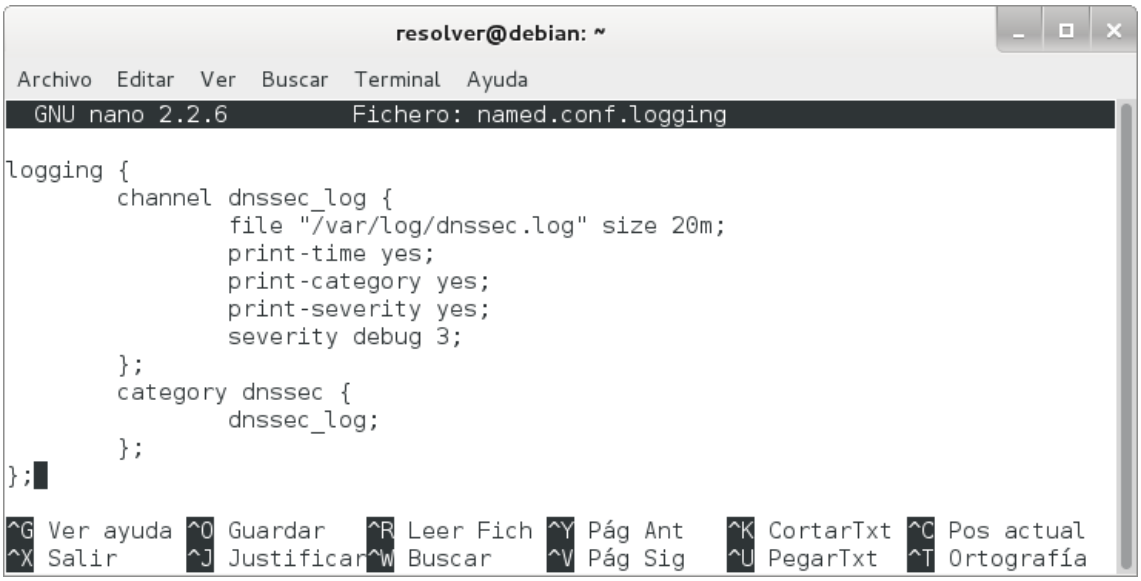

Figura 169. Archivo named.conf.logging.

3. Incluir el archivo /etc/bind/named.conf.logging en el archivo /etc/bind/named.conf:

   include "/etc/bind/named.conf.logging";

Observe la figura 170, donde se incluye el archivo /etc/bind/named.conf.logging.

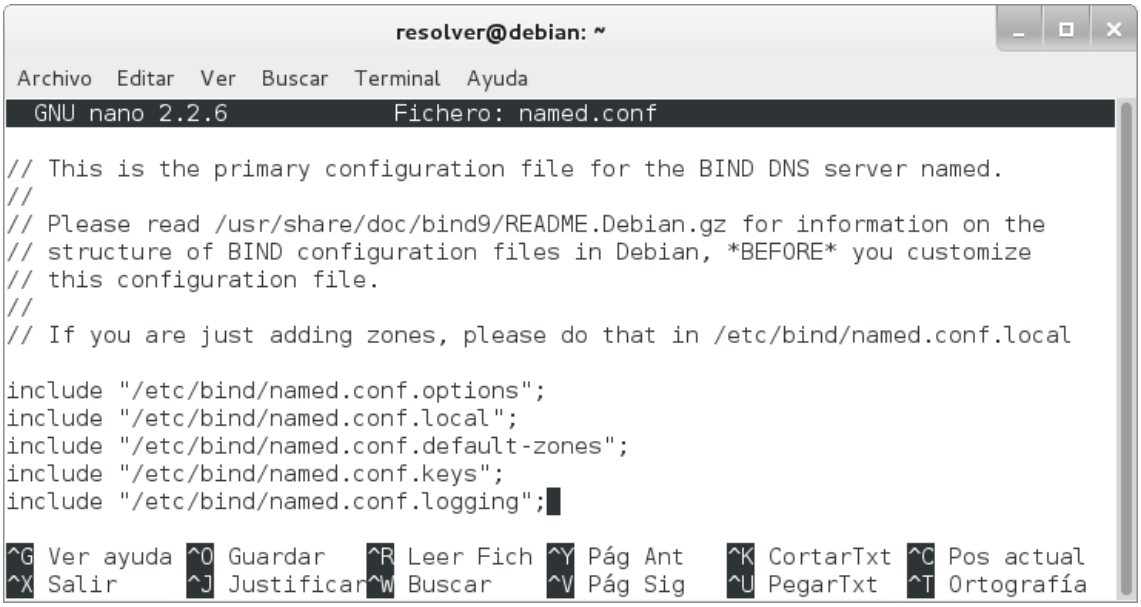

Figura 170. Inserción del archivo named.conf.logging.

4. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 171.

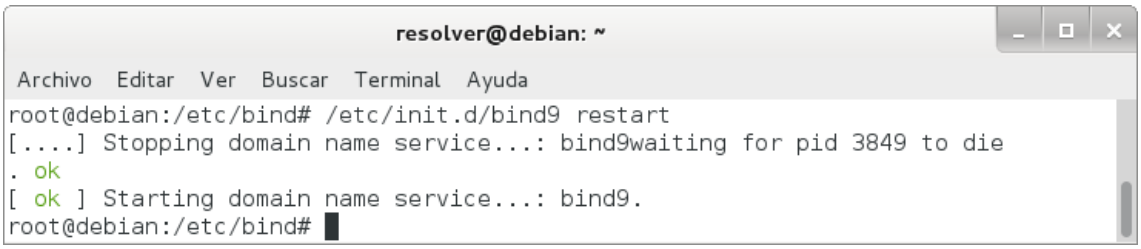

Figura 171. Reinicio del servicio.

4. Realizar pruebas.

Tan pronto como una clave de confianza se ha configurado, los datos de esa zona o de sus sub zonas serán validados por el promotor de almacenamiento en caché. Se puede probar esto al consultar al servidor. Si los datos son validados por el promotor de almacenamiento en caché el bit ad (authenticated data) será fijado por el servidor de nombres [17].

4.1. Servidores Universidad Nacional de Loja.

4.1.1. Sitio web.

Para lo cual se realizó lo siguiente:

1. Utilizar el comando dig:

 # dig +dnssec unl.edu.ec

Con lo que se comprueba que la información de la zona unl.edu.ec se encuentra autenticada, ya que se fija la bandera ad como se muestra en la figura 172.

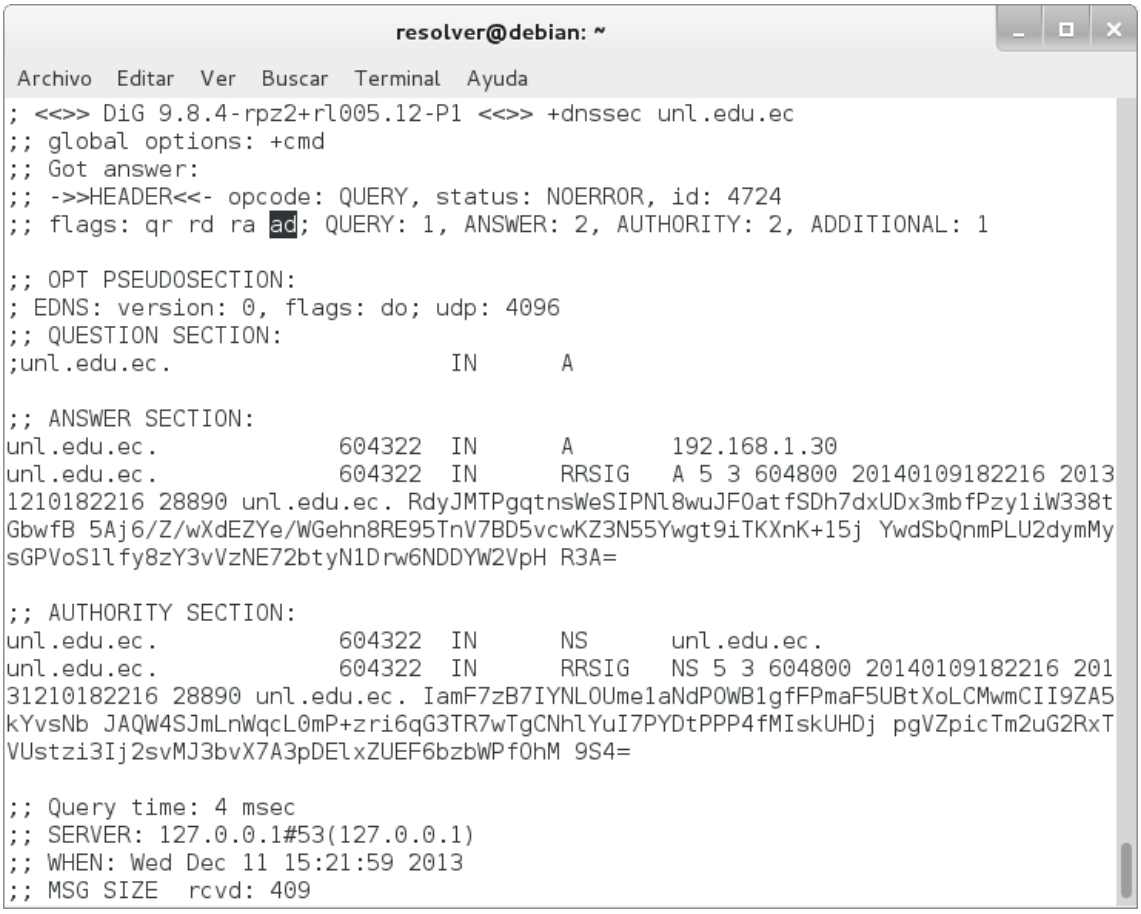

Figura 172. Ejecución correcta de dig.

2. Revisar el registro:

 # nano /var/log/dnssec.log

Donde se muestra cómo el validador trata de demostrar que el conjunto de RR es de confianza, siguiendo la cadena de confianza hasta el punto de entrada de seguridad

apropiado. La cadena de confianza comienza por la validación de una firma sobre un conjunto RR de DNSKEY, luego estas claves se utilizan para validar el conjunto RR de DS que apuntan al RR de DNSKEY en una zona secundaria, o los DNSKEY se pueden utilizar para validar los datos que se consultan. El registro refleja la actividad del validador siguiendo la cadena de confianza, como se muestra en la figura 173.

```
validating @0xb8f188a0: unl.edu.ec DNSKEY: starting
validating @0xb8f188a0: unl.edu.ec DNSKEY: attempting positive response validation
validating @0xb8f188a0: unl.edu.ec DNSKEY: verify rdataset (keyid=26923): success
validating @0xb8f188a0: unl.edu.ec DNSKEY: signed by trusted key; marking as secure
validator @0xb8f188a0: dns_validator_destroy
validating @0xb8ed0d48: unl.edu.ec A: in fetch_callback_validator
validating @0xb8ed0d48: unl.edu.ec A: keyset with trust 8
validating @0xb8ed0d48: unl.edu.ec A: resuming validate
validating @0xb8ed0d48: unl.edu.ec A: verify rdataset (keyid=30528): success
validating @0xb8ed0d48: unl.edu.ec A: marking as secure, noqname proof not needed
validator @0xb8ed0d48: dns_validator_destroy
```

Figura 173. Registro del validador.

4.1.2. Comunidad virtual de aprendizaje.

Para lo cual se realizó lo siguiente:

1. Utilizar el comando dig:

   # dig +dnssec cva.unl.edu.ec

Con lo que se comprueba que la información de la zona cva.unl.edu.ec se encuentra autenticada, ya que se fija la bandera ad como se muestra en la figura 174.

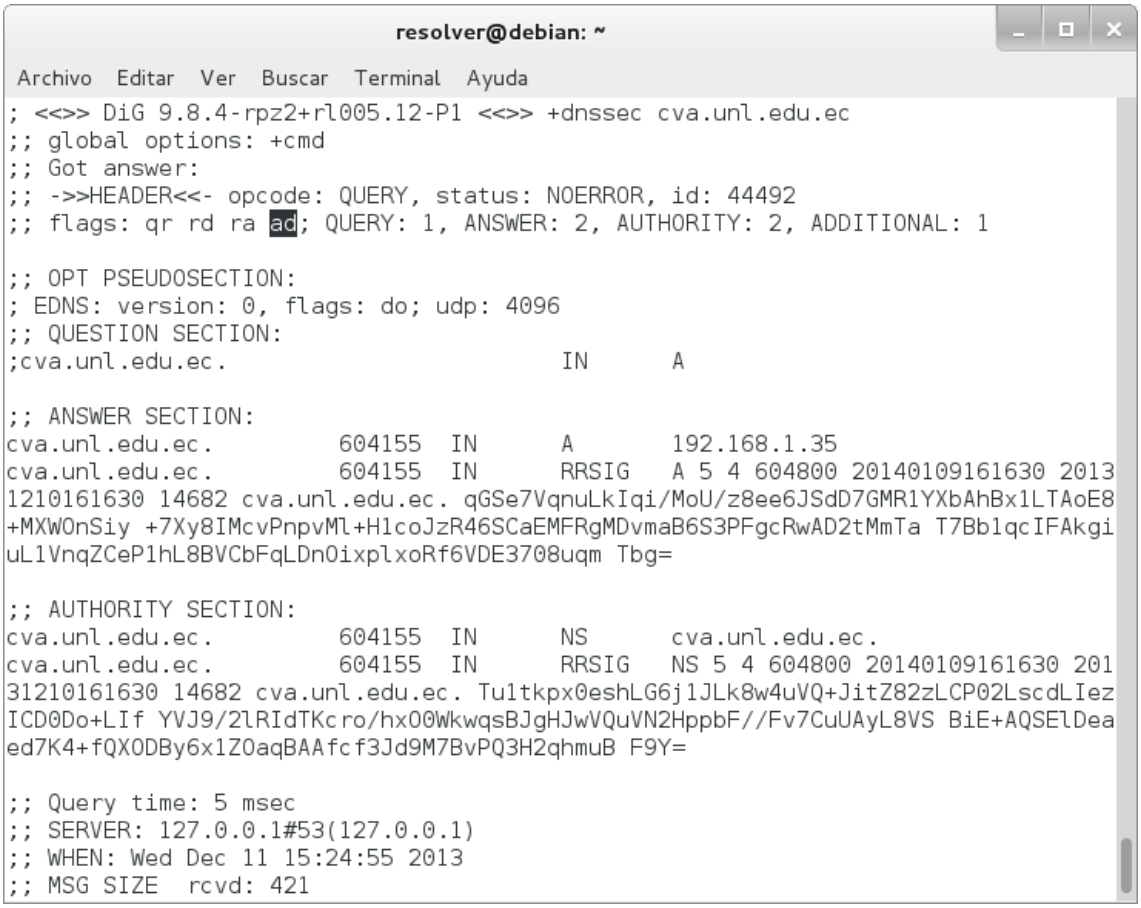

Figura 174. Ejecución correcta de dig.

2. Revisar el registro:

 # nano /var/log/dnssec.log

Donde se muestra cómo el validador trata de demostrar que el conjunto de RR es de confianza, siguiendo la cadena de confianza hasta el punto de entrada de seguridad apropiado. La cadena de confianza comienza por la validación de una firma sobre un conjunto RR de DNSKEY, luego estas claves se utilizan para validar el conjunto RR de DS que apuntan al RR de DNSKEY en una zona secundaria, o los DNSKEY se pueden utilizar para validar los datos que se consultan. El registro refleja la actividad del validador siguiendo la cadena de confianza, como se muestra en la figura 175.

```
validating @0xb8860c78: cva.unl.edu.ec A: starting
validating @0xb8860c78: cva.unl.edu.ec A: attempting positive response validation
validating @0xb88a88a0: cva.unl.edu.ec DNSKEY: starting
validating @0xb88a88a0: cva.unl.edu.ec DNSKEY: attempting positive response validation
validating @0xb88a88a0: cva.unl.edu.ec DNSKEY: verify rdataset (keyid=7396): success
validating @0xb88a88a0: cva.unl.edu.ec DNSKEY: signed by trusted key; marking as secure
validator @0xb88a88a0: dns_validator_destroy
validating @0xb8860c78: cva.unl.edu.ec A: in fetch_callback_validator
validating @0xb8860c78: cva.unl.edu.ec A: keyset with trust 8
validating @0xb8860c78: cva.unl.edu.ec A: resuming validate
validating @0xb8860c78: cva.unl.edu.ec A: verify rdataset (keyid=14682): success
validating @0xb8860c78: cva.unl.edu.ec A: marking as secure, noqname proof not needed
validator @0xb8860c78: dns_validator_destroy
```

Figura 175. Registro del validador.

4.2. Servidores Universidad Técnica Particular de Loja.

4.2.1. Sitio web.

Para lo cual se realizó lo siguiente:

1. Utilizar el comando dig:

   # dig +dnssec utpl.edu.ec

Con lo que se comprueba que la información de la zona utpl.edu.ec se encuentra autenticada, ya que se fija la bandera ad como se muestra en la figura 176.

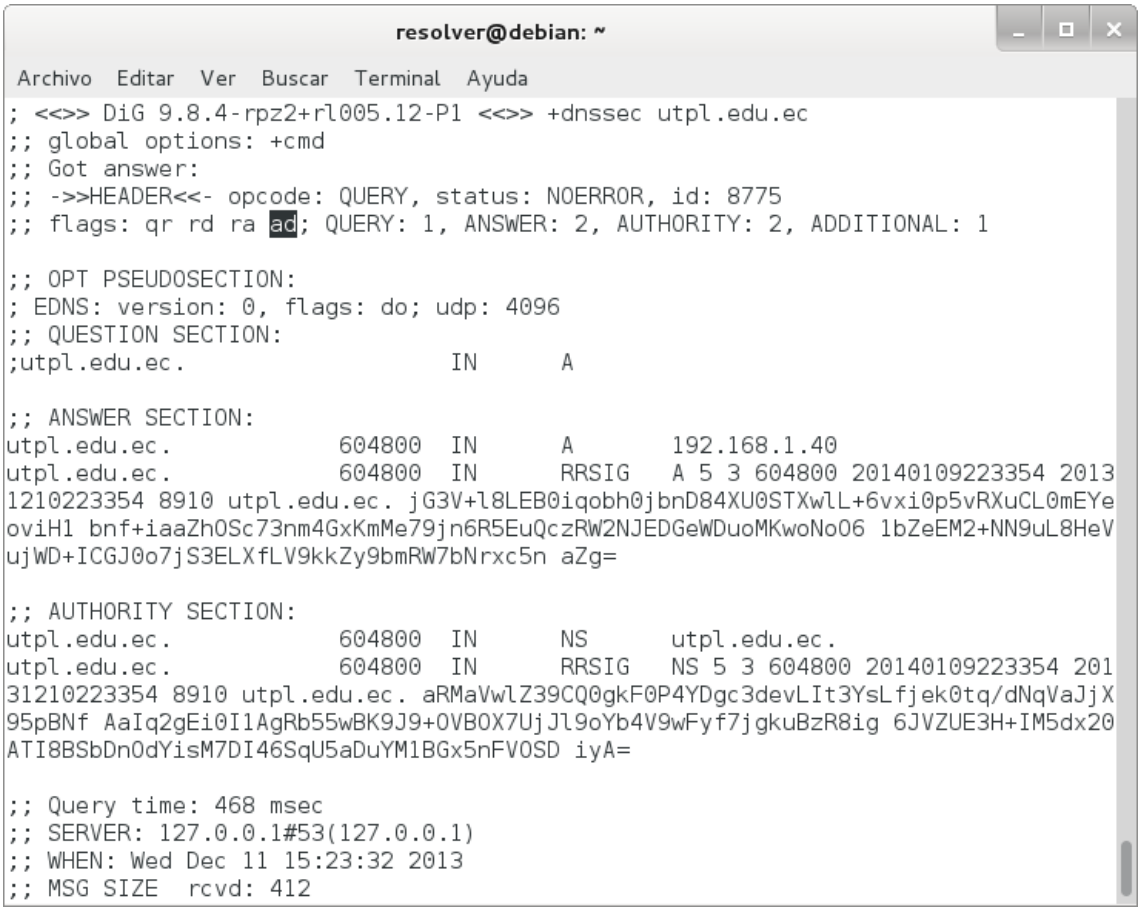

Figura 176. Ejecución correcta de dig.

2. Revisar el registro:

 # nano /var/log/dnssec.log

Donde se muestra cómo el validador trata de demostrar que el conjunto de RR es de confianza, siguiendo la cadena de confianza hasta el punto de entrada de seguridad apropiado. La cadena de confianza comienza por la validación de una firma sobre un conjunto RR de DNSKEY, luego estas claves se utilizan para validar el conjunto RR de DS que apuntan al RR de DNSKEY en una zona secundaria, o los DNSKEY se pueden utilizar para validar los datos que se consultan. El registro refleja la actividad del validador siguiendo la cadena de confianza, como se muestra en la figura 177.

```
validating @0xb9152230: utpl.edu.ec DNSKEY: starting
validating @0xb9152230: utpl.edu.ec DNSKEY: attempting positive response validation
validating @0xb9152230: utpl.edu.ec DNSKEY: verify rdataset (keyid=59911): success
validating @0xb9152230: utpl.edu.ec DNSKEY: signed by trusted key; marking as secure
validator @0xb8f188a0: dns_validator_destroy
validator @0xb9152230: dns_validator_destroy
validating @0xb8ed0d48: utpl.edu.ec A: in fetch_callback_validator
validating @0xb8ed0d48: utpl.edu.ec A: keyset with trust 8
validating @0xb8ed0d48: utpl.edu.ec A: resuming validate
validating @0xb8ed0d48: utpl.edu.ec A: verify rdataset (keyid=31113): success
validating @0xb8ed0d48: utpl.edu.ec A: marking as secure, noqname proof not needed
validator @0xb8ed0d48: dns_validator_destroy
```

Figura 177. Registro del validador.

4.2.2. Comunidad virtual de aprendizaje.

Para lo cual se realizó lo siguiente:

1. Utilizar el comando dig:

   # dig +dnssec cva.utpl.edu.ec

Con lo que se comprueba que la información de la zona cva.utpl.edu.ec se encuentra autenticada, ya que se fija la bandera ad como se muestra en la figura 178.

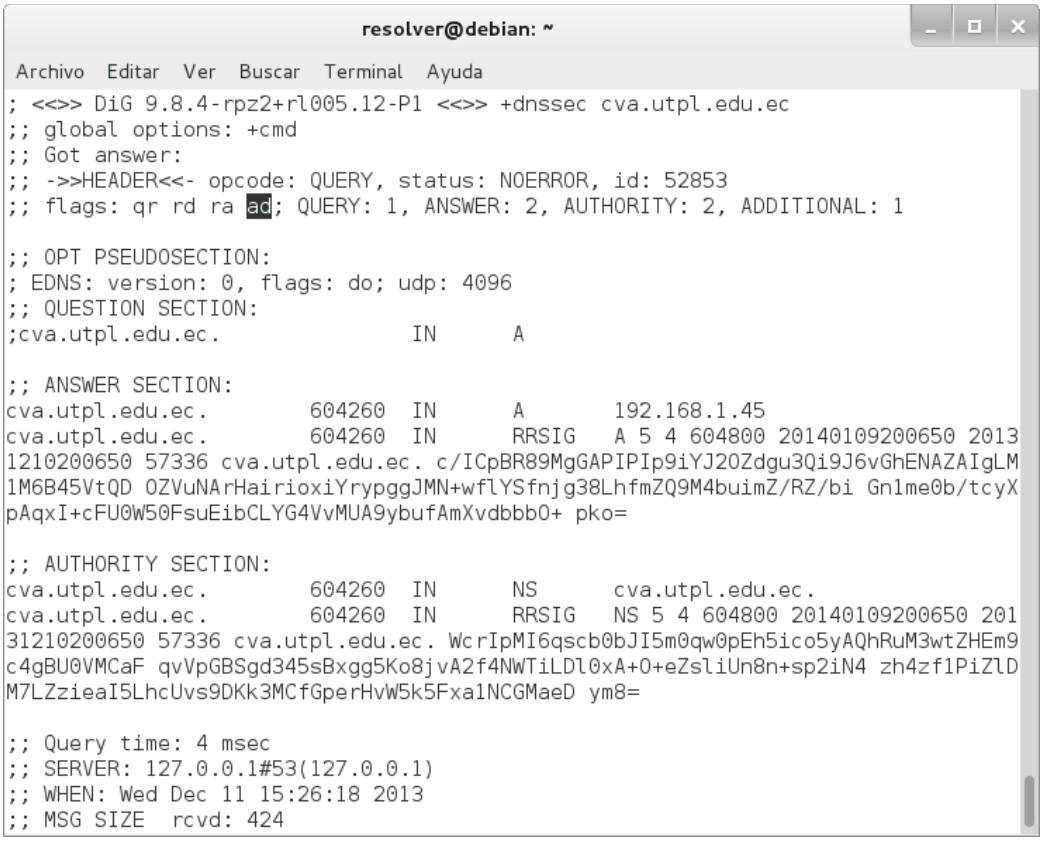

Figura 178. Ejecución correcta de dig.

2. Revisar el registro:

 # nano /var/log/dnssec.log

Donde se muestra cómo el validador trata de demostrar que el conjunto de RR es de confianza, siguiendo la cadena de confianza hasta el punto de entrada de seguridad apropiado. La cadena de confianza comienza por la validación de una firma sobre un conjunto RR de DNSKEY, luego estas claves se utilizan para validar el conjunto RR de DS que apuntan al RR de DNSKEY en una zona secundaria, o los DNSKEY se pueden utilizar para validar los datos que se consultan. El registro refleja la actividad del validador siguiendo la cadena de confianza, como se muestra en la figura 179.

```
validating @0xb89ac8a0: cva.utpl.edu.ec DNSKEY: starting
validating @0xb89ac8a0: cva.utpl.edu.ec DNSKEY: attempting positive response validation
validating @0xb89ac8a0: cva.utpl.edu.ec DNSKEY: verify rdataset (keyid=31093): success
validating @0xb89ac8a0: cva.utpl.edu.ec DNSKEY: signed by trusted key; marking as secure
validator @0xb89ac8a0: dns_validator_destroy
validating @0xb8964c78: cva.utpl.edu.ec A: in fetch_callback_validator
validating @0xb8964c78: cva.utpl.edu.ec A: keyset with trust 8
validating @0xb8964c78: cva.utpl.edu.ec A: resuming validate
validating @0xb8964c78: cva.utpl.edu.ec A: verify rdataset (keyid=57336): success
validating @0xb8964c78: cva.utpl.edu.ec A: marking as secure, noqname proof not needed
validator @0xb8964c78: dns_validator_destroy
```

Figura 179. Registro del validador.

Anexo 15: Renovación de la clave ZSK del sitio web de la Universidad Nacional de Loja.

1. Preparar ZSK (fase de producción).

Para lo cual se siguieron los siguientes pasos:

1. Generar dos claves ZSK y una clave KSK:

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE unl.edu.ec

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE unl.edu.ec

   # dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE unl.edu.ec

Con lo que se observa en la figura 180 que la clave 02415 se utilizará como la activa y la clave 49083 como la ZSK pasiva. Ambas claves estarán disponibles a través del conjunto de claves, pero sólo la clave activa se utiliza para firmar.

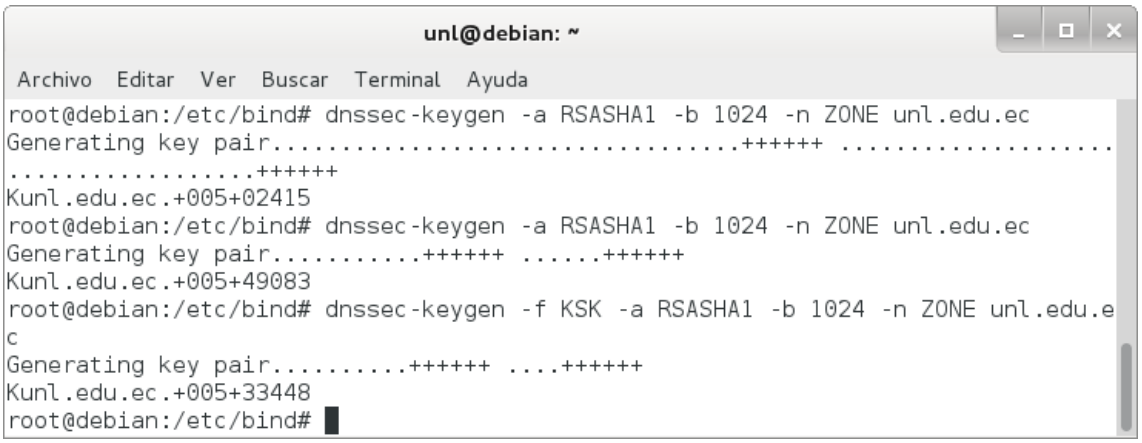

Figura 180. Claves ZSK y KSK.

2. Incluir las claves en la zona añadiendo la directiva $INCLUDE al archivo /etc/bind/db.unl.edu.ec:

   ;ZSK
   $INCLUDE Kunl.edu.ec.+005+02415.key
   $INCLUDE Kunl.edu.ec.+005+49083.key

   ;KSK
   $INCLUDE Kunl.edu.ec.+005+33448.key

Observe la figura 181, donde se utiliza la directiva $INCLUDE para incluir las claves.

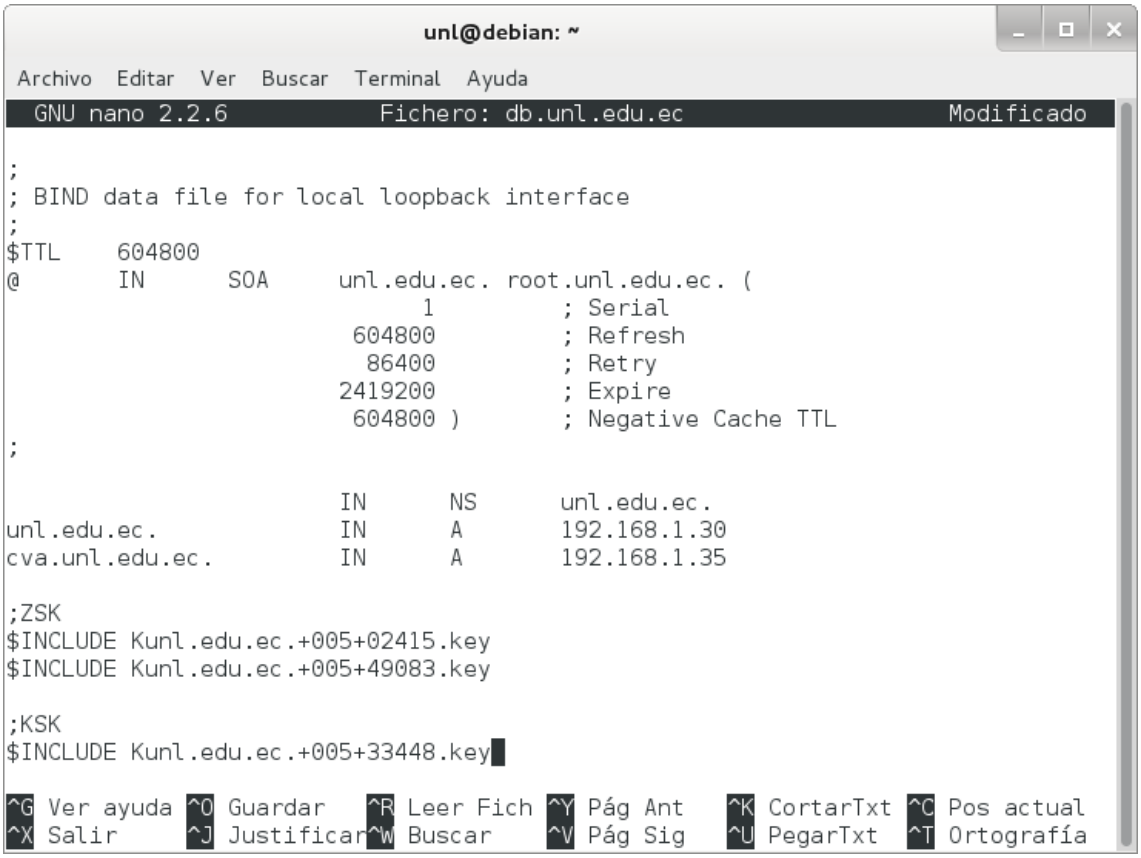

Figura 181. Inserción de las claves en la zona.

3. Firmar la zona:

 # dnssec-signzone -o unl.edu.ec -k Kunl.edu.ec.+005+33448.key db.unl.edu.ec Kunl.edu.ec.+005+02415.key

2. Renovar ZSK (fase 1).

En el momento de la renovación se tuvo que:

1. Hacer activa la clave pasiva actual (49083) y pasiva la clave activa actual (02415).
2. Re-firmar la zona utilizando la nueva clave activa:

 # dnssec-signzone -o unl.edu.ec -k Kunl.edu.ec.+005+33448.key db.unl.edu.ec Kunl.edu.ec.+005+49083.key

3. Limpiar ZSK (fase 2).

Se tuvo que reemplazar la clave ZSK pasiva (02415) por una nueva clave pasiva, para lo cual se hizo:

1. Generar la nueva clave ZSK pasiva:

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE unl.edu.ec

2. Incluir la nueva clave pasiva (02580) en el archivo /etc/bind/db.unl.edu.ec y remover la anterior clave pasiva de la zona:

   ;ZSK
   $INCLUDE Kunl.edu.ec.+005+49083.key
   $INCLUDE Kunl.edu.ec.+005+02580.key

   ;KSK
   $INCLUDE Kunl.edu.ec.+005+33448.key

Observe la figura 182, donde se utiliza la directiva $INCLUDE para incluir las claves.

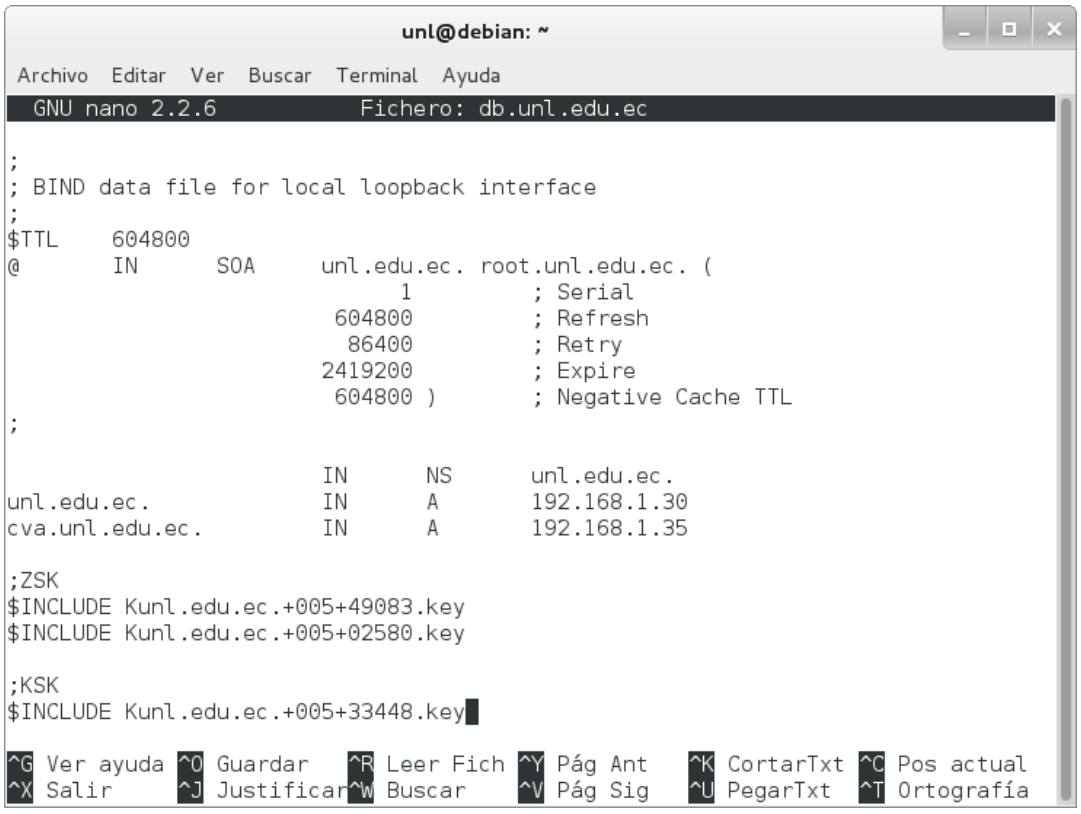

Figura 182. Inserción de las claves en la zona.

3. Re-firmar la zona utilizando la misma clave activa de la fase 1:

   # dnssec-signzone -o unl.edu.ec -k Kunl.edu.ec.+005+33448.key db.unl.edu.ec Kunl.edu.ec.+005+49083.key

4. Borrar la anterior clave pasiva (02415):

 # rm Kunl.edu.ec.+005+02415.key

Anexo 16: Renovación de la clave ZSK de la comunidad virtual de aprendizaje de la Universidad Nacional de Loja.

1. Preparar ZSK (fase de producción).

Para lo cual se siguieron los siguientes pasos:

1. Generar dos claves ZSK y una clave KSK:

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE cva.unl.edu.ec

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE cva.unl.edu.ec

   # dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE cva.unl.edu.ec

Con lo que se observa en la figura 183 que la clave 12312 se utilizará como la activa y la clave 38691 como la ZSK pasiva. Ambas claves estarán disponibles a través del conjunto de claves, pero sólo la clave activa se utiliza para firmar.

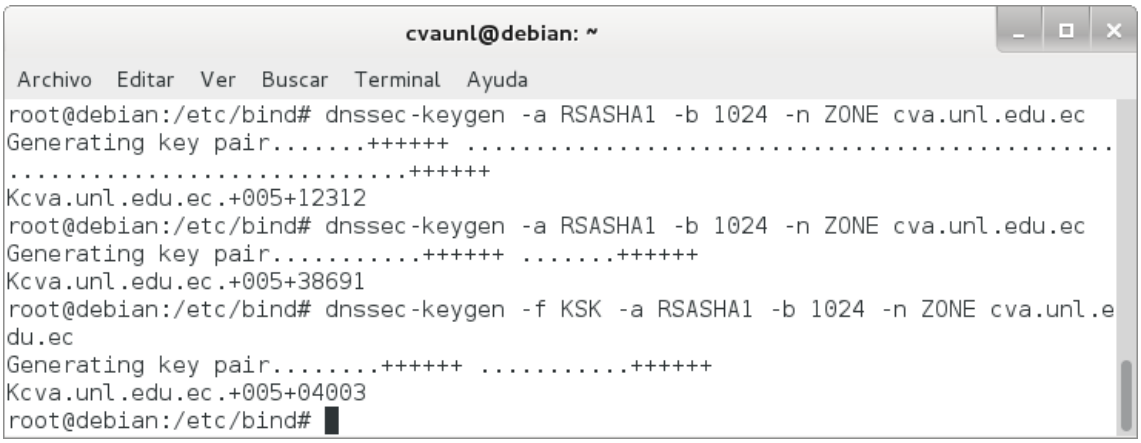

Figura 183. Claves ZSK y KSK.

2. Incluir las claves en la zona añadiendo la directiva $INCLUDE al archivo /etc/bind/db.cva.unl.edu.ec:

   ;ZSK
   $INCLUDE Kcva.unl.edu.ec.+005+12312.key
   $INCLUDE Kcva.unl.edu.ec.+005+38691.key

   ;KSK
   $INCLUDE Kcva.unl.edu.ec.+005+04003.key

Observe la figura 201, donde se utiliza la directiva $INCLUDE para incluir las claves.

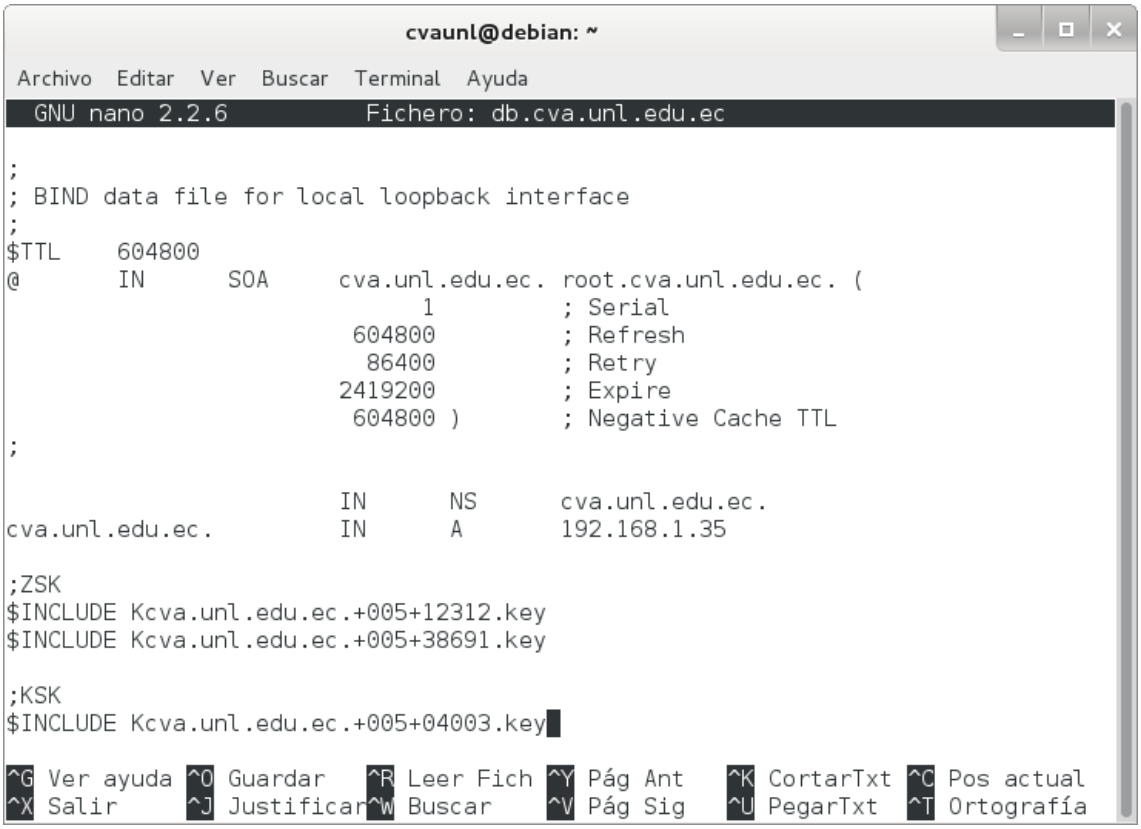

Figura 184. Inserción de las claves en la zona.

3. Firmar la zona:

 # dnssec-signzone -o cva.unl.edu.ec -k Kcva.unl.edu.ec.+005+04003.key db.cva.unl.edu.ec Kcva.unl.edu.ec.+005+12312.key

2. Renovar ZSK (fase 1).

En el momento de la renovación se tuvo que:

1. Hacer activa la clave pasiva actual (38691) y pasiva la clave activa actual (12312).
2. Re-firmar la zona utilizando la nueva clave activa:

 # dnssec-signzone -o cva.unl.edu.ec -k Kcva.unl.edu.ec.+005+04003.key db.cva.unl.edu.ec Kcva.unl.edu.ec.+005+38691.key

3. Limpiar ZSK (fase 2).

Se tuvo que reemplazar la clave ZSK pasiva (12312) por una nueva clave pasiva, para lo cual se hizo:

1. Generar la nueva clave ZSK pasiva:

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE cva.unl.edu.ec

2. Incluir la nueva clave pasiva (54081) en el archivo /etc/bind/db.cva.unl.edu.ec y remover la anterior clave pasiva de la zona:

   ;ZSK
   $INCLUDE Kcva.unl.edu.ec.+005+38691.key
   $INCLUDE Kcva.unl.edu.ec.+005+54081.key

   ;KSK
   $INCLUDE Kcva.unl.edu.ec.+005+04003.key

Observe la figura 185, donde se utiliza la directiva $INCLUDE para incluir las claves.

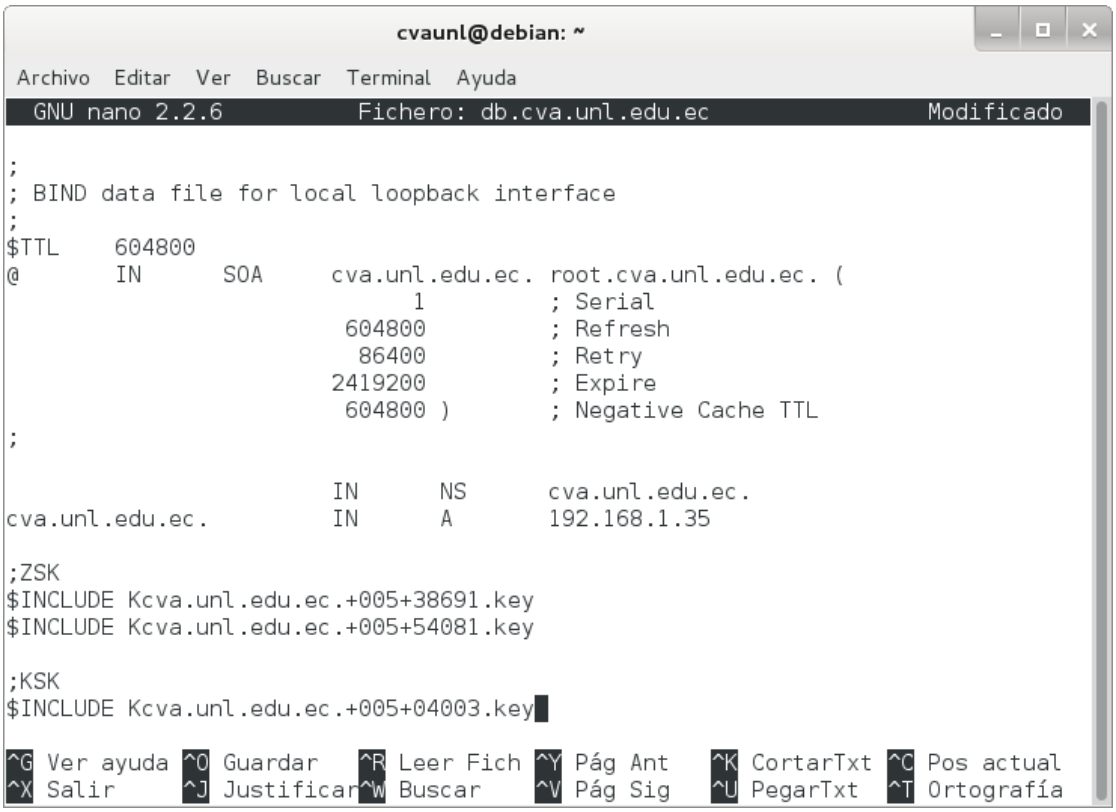

Figura 185. Inserción de las claves en la zona.

3. Re-firmar la zona utilizando la misma clave activa de la fase 1:

   # *dnssec-signzone -o cva.unl.edu.ec -k Kcva.unl.edu.ec.+005+04003.key db.cva.unl.edu.ec Kcva.unl.edu.ec.+005+38691.key*

4. Borrar la anterior clave pasiva (12312):

   # *rm Kcva.unl.edu.ec.+005+12312.key*

Anexo 17: Renovación de la clave ZSK del sitio web de la Universidad Técnica Particular de Loja.

1. Preparar ZSK (fase de producción).

Para lo cual se siguieron los siguientes pasos:

1. Generar dos claves ZSK y una clave KSK:

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE utpl.edu.ec

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE utpl.edu.ec

   # dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE utpl.edu.ec

Con lo que se observa en la figura 186 que la clave 49305 se utilizará como la activa y la clave 21003 como la ZSK pasiva. Ambas claves estarán disponibles a través del conjunto de claves, pero sólo la clave activa se utiliza para firmar.

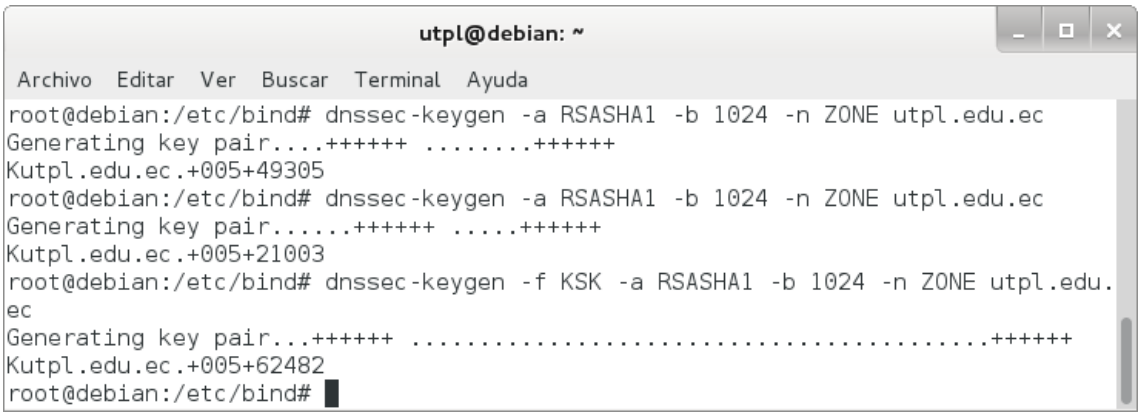

Figura 186. Claves ZSK y KSK.

2. Incluir las claves en la zona añadiendo la directiva $INCLUDE al archivo /etc/bind/db.utpl.edu.ec:

   ;ZSK
   $INCLUDE Kutpl.edu.ec.+005+49305.key
   $INCLUDE Kutpl.edu.ec.+005+21003.key

   ;KSK
   $INCLUDE Kutpl.edu.ec.+005+62482.key

Observe la figura 187, donde se utiliza la directiva $INCLUDE para incluir las claves.

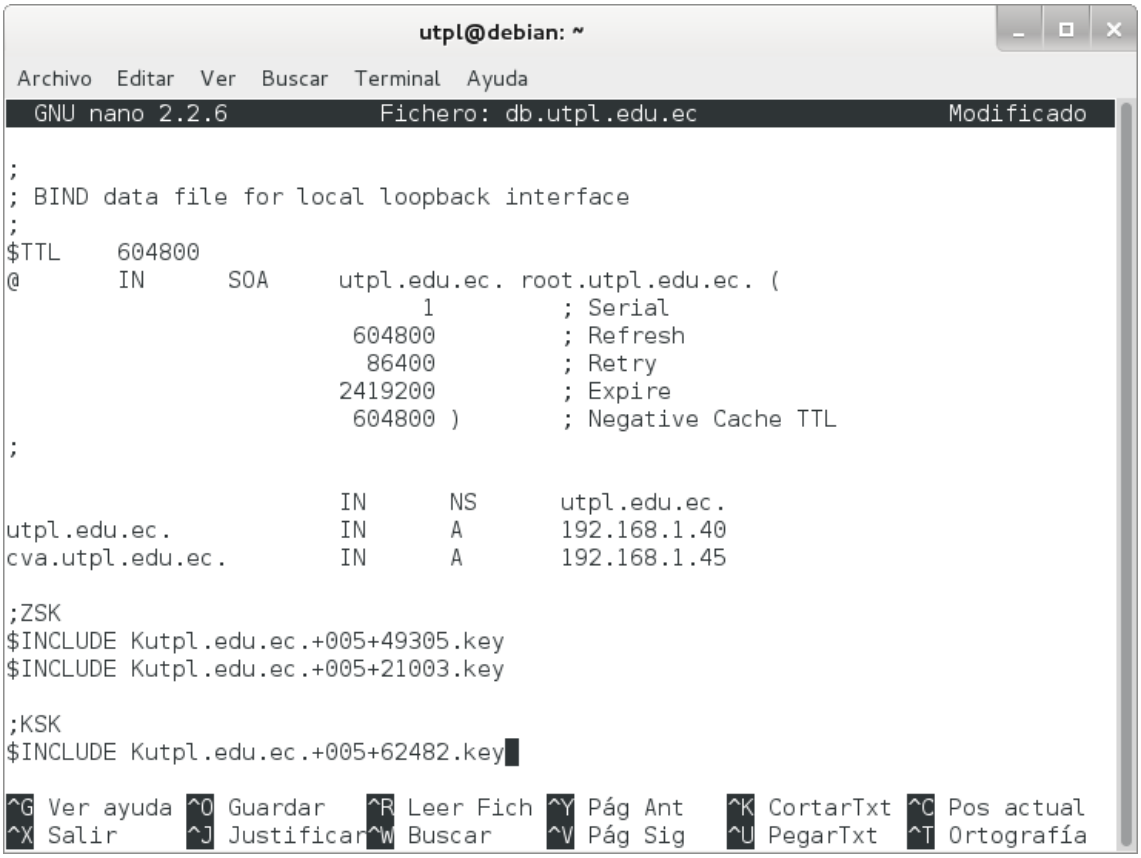

Figura 187. Inserción de las claves en la zona.

3. Firmar la zona:

 # dnssec-signzone -o utpl.edu.ec -k Kutpl.edu.ec.+005+62482.key db.utpl.edu.ec Kutpl.edu.ec.+005+49305.key

2. Renovar ZSK (fase 1).

En el momento de la renovación se tuvo que:

1. Hacer activa la clave pasiva actual (21003) y pasiva la clave activa actual (49305).
2. Re-firmar la zona utilizando la nueva clave activa:

 # dnssec-signzone -o utpl.edu.ec -k Kutpl.edu.ec.+005+62482.key db.utpl.edu.ec Kutpl.edu.ec.+005+21003.key

3. Limpiar ZSK (fase 2).

Se tuvo que reemplazar la clave ZSK pasiva (49305) por una nueva clave pasiva, para lo cual se hizo:

1. Generar la nueva clave ZSK pasiva:

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE utpl.edu.ec

2. Incluir la nueva clave pasiva (35841) en el archivo /etc/bind/db.utpl.edu.ec y remover la anterior clave pasiva de la zona:

   ;ZSK
   $INCLUDE Kutpl.edu.ec.+005+21003.key
   $INCLUDE Kutpl.edu.ec.+005+35841.key

   ;KSK
   $INCLUDE Kutpl.edu.ec.+005+62482.key

Observe la figura 188, donde se utiliza la directiva $INCLUDE para incluir las claves.

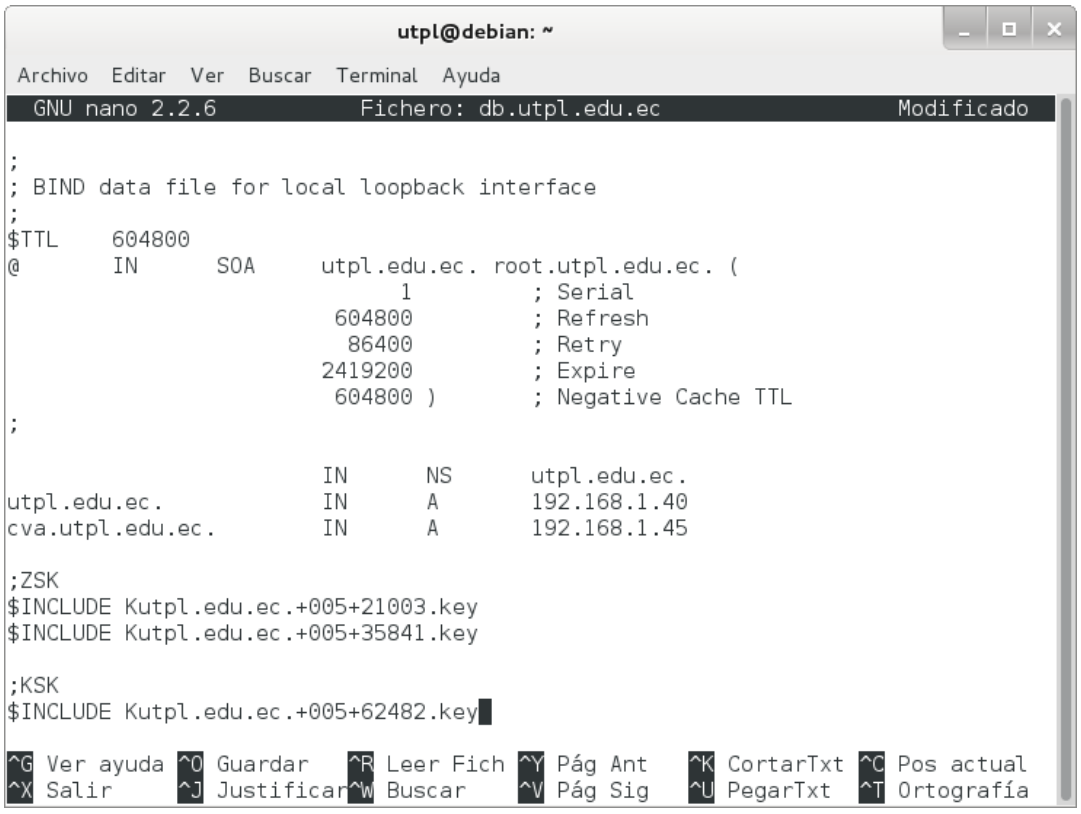

Figura 188. Inserción de las claves en la zona.

3. Re-firmar la zona utilizando la misma clave activa de la fase 1:

   # dnssec-signzone -o utpl.edu.ec -k Kutpl.edu.ec.+005+62482.key db.utpl.edu.ec Kutpl.edu.ec.+005+21003.key

4. Borrar la anterior clave pasiva (49305):

   # rm Kutpl.edu.ec.+005+49305.key

Anexo 18: Renovación de la clave ZSK de la comunidad virtual de aprendizaje de la Universidad Técnica Particular de Loja.

1. Preparar ZSK (fase de producción).

Para lo cual se siguieron los siguientes pasos:

1. Generar dos claves ZSK y una clave KSK:

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE cva.utpl.edu.ec

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE cva.utpl.edu.ec

   # dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE cva.utpl.edu.ec

Con lo que se observa que la clave 43548 se utilizará como la activa y la clave 27450 como la ZSK pasiva. Ambas claves estarán disponibles a través del conjunto de claves, pero sólo la clave activa se utiliza para firmar, como se muestra en la figura 189.

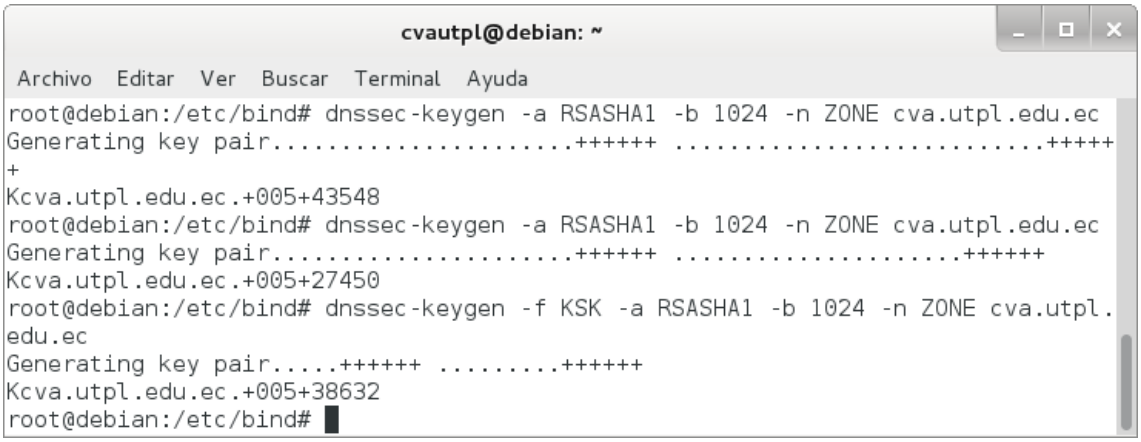

Figura 189. Claves ZSK y KSK.

2. Incluir las claves en la zona añadiendo la directiva $INCLUDE al archivo /etc/bind/db.cva.utpl.edu.ec:

   ;ZSK
   $INCLUDE Kcva.utpl.edu.ec.+005+43548.key
   $INCLUDE Kcva.utpl.edu.ec.+005+27450.key

;KSK

$INCLUDE Kcva.utpl.edu.ec.+005+38632.key

Observe la figura 190, donde se utiliza la directiva $INCLUDE para incluir las claves.

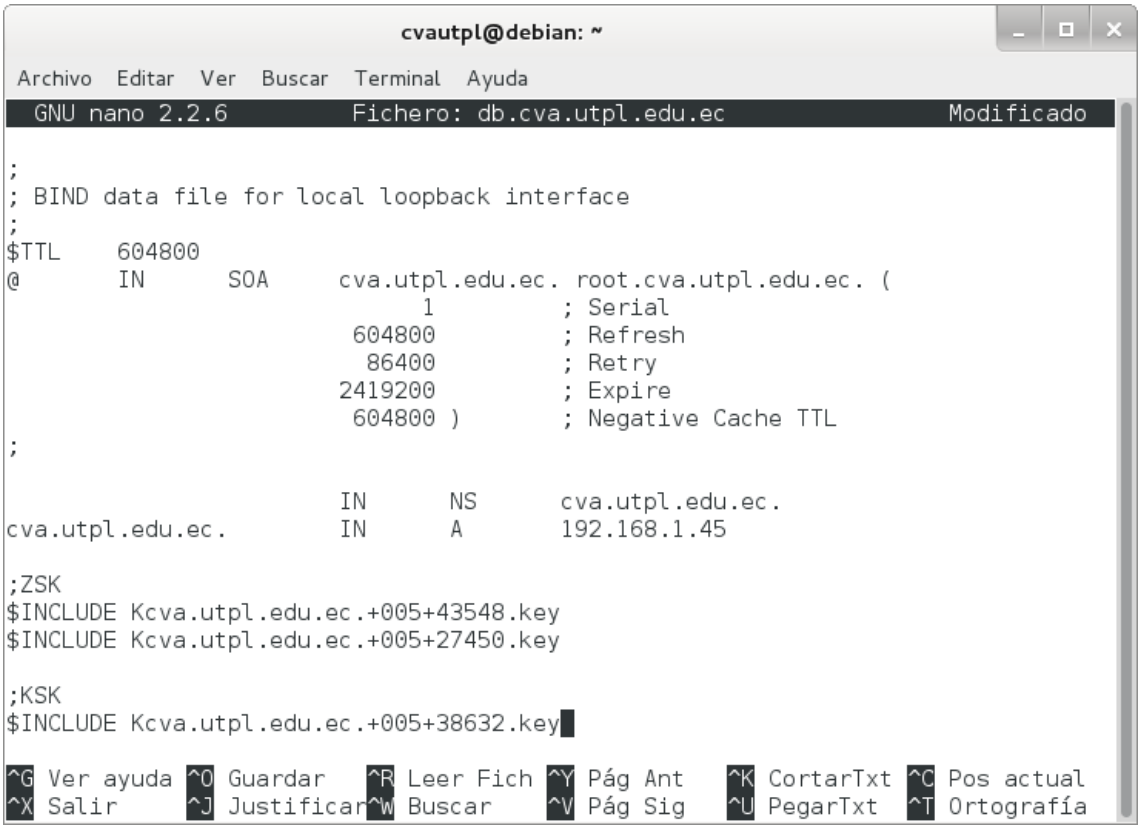

Figura 190. Inserción de las claves en la zona.

3. Firmar la zona:

 # dnssec-signzone -o cva.utpl.edu.ec -k Kcva.utpl.edu.ec.+005+38632.key db.cva.utpl.edu.ec Kcva.utpl.edu.ec.+005+43548.key

2. Renovar ZSK (fase 1).

En el momento de la renovación se tuvo que:

1. Hacer activa la clave pasiva actual (27450) y pasiva la clave activa actual (43548).
2. Re-firmar la zona utilizando la nueva clave activa:

 # dnssec-signzone -o cva.utpl.edu.ec -k Kcva.utpl.edu.ec.+005+38632.key db.cva.utpl.edu.ec Kcva.utpl.edu.ec.+005+27450.key

3. Limpiar ZSK (fase 2).

Se tuvo que reemplazar la clave ZSK pasiva (43548) por una nueva clave pasiva, para lo cual se hizo:

1. Generar la nueva clave ZSK pasiva:

   # dnssec-keygen -a RSASHA1 -b 1024 -n ZONE cva.utpl.edu.ec

2. Incluir la nueva clave pasiva (56943) en el archivo /etc/bind/db.cva.utpl.edu.ec y remover la anterior clave pasiva de la zona:

   ;ZSK
   $INCLUDE Kcva.utpl.edu.ec.+005+27450.key
   $INCLUDE Kcva.utpl.edu.ec.+005+56943.key

   ;KSK
   $INCLUDE Kcva.utpl.edu.ec.+005+38632.key

Observe la figura 191, donde se utiliza la directiva $INCLUDE para incluir las claves.

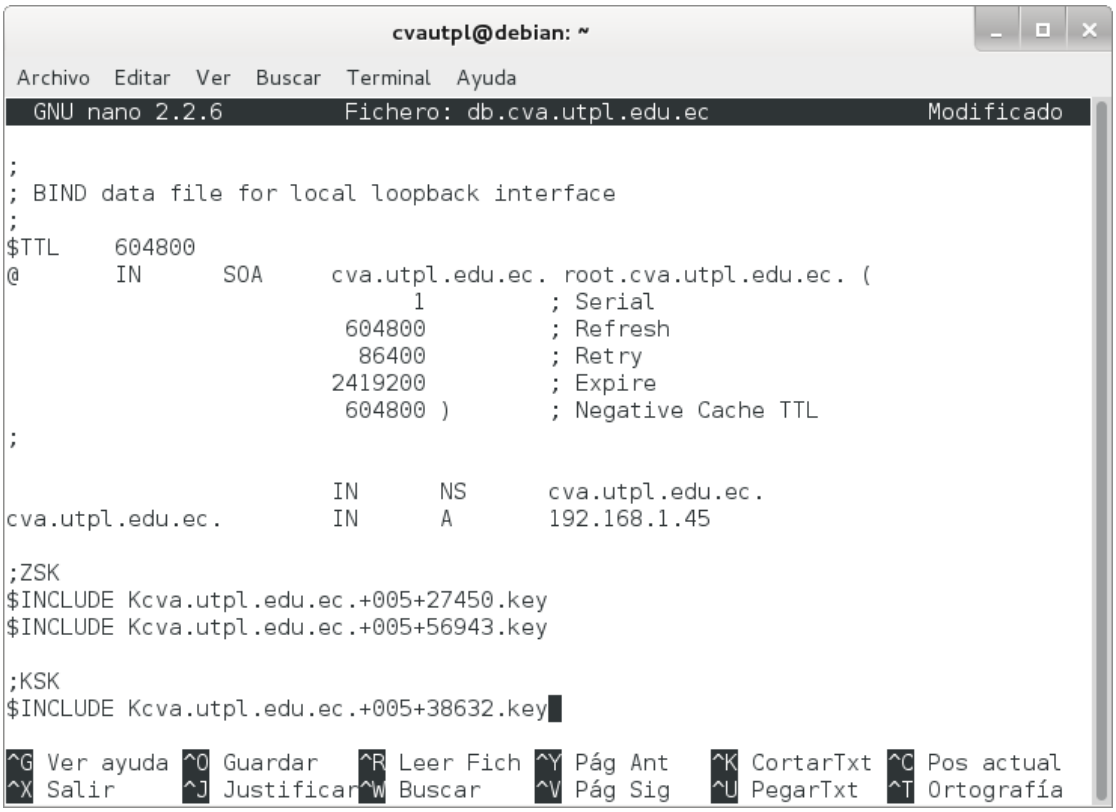

Figura 191. Inserción de las claves en la zona.

3. Re-firmar la zona utilizando la misma clave activa de la fase 1:

   # *dnssec-signzone -o cva.utpl.edu.ec -k Kcva.utpl.edu.ec.+005+38632.key db.cva.utpl.edu.ec Kcva.utpl.edu.ec.+005+27450.key*

4. Borrar la anterior clave pasiva (43548):

   # *rm Kcva.utpl.edu.ec.+005+43548.key*

Anexo 19: Renovación de la clave KSK del sitio web de la Universidad Nacional de Loja.

1. Preparar KSK (fase de producción).

Para lo cual se siguieron los siguientes pasos:

1. Incluir las mismas claves de la sección 3 del Anexo 15 en la zona añadiendo la directiva $INCLUDE al archivo /etc/bind/db.unl.edu.ec:

   ;ZSK
   $INCLUDE Kunl.edu.ec.+005+49083.key
   $INCLUDE Kunl.edu.ec.+005+02580.key

   ;KSK
   $INCLUDE Kunl.edu.ec.+005+33448.key

Observe la figura 192, donde se utiliza la directiva $INCLUDE para incluir las claves.

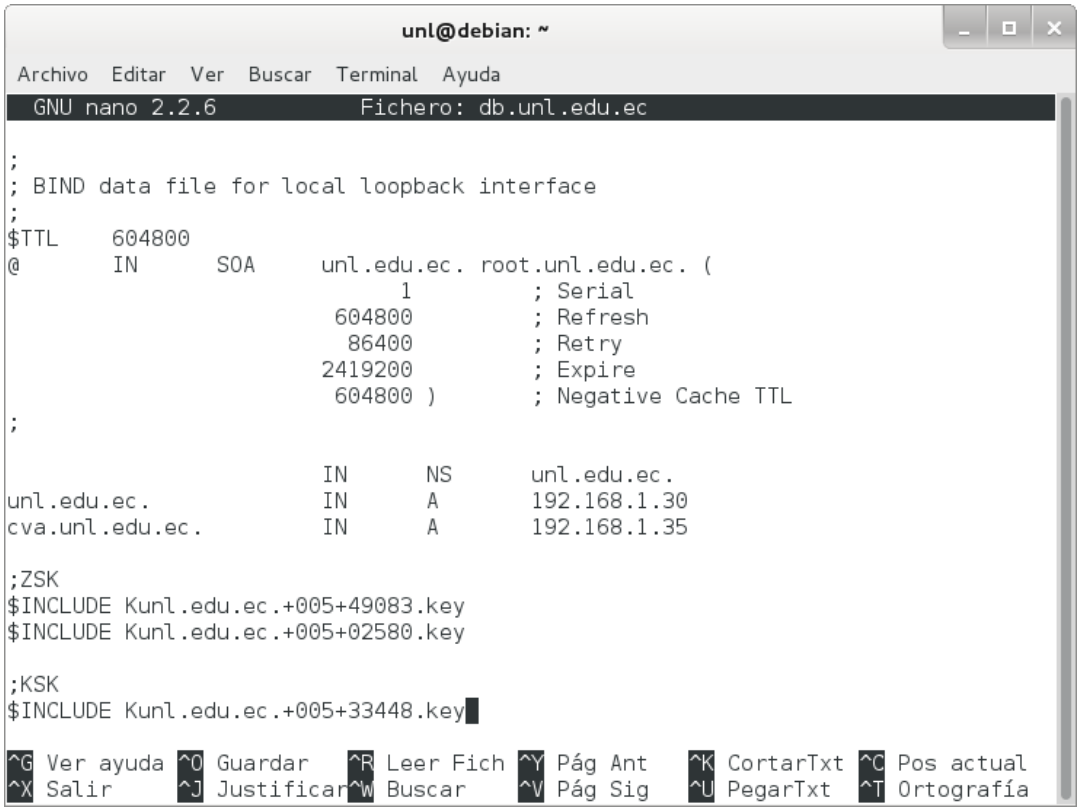

Figura 192. Inserción de las claves en la zona.

2. Firmar la zona al igual que en la sección 3 del Anexo 15:

   # dnssec-signzone -o unl.edu.ec -k Kunl.edu.ec.+005+33448.key db.unl.edu.ec Kunl.edu.ec.+005+49083.key

2. Renovar KSK (fase 1).

Se realizó haciendo lo siguiente:

1. Generar una nueva clave KSK:

   # dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE unl.edu.ec

2. Incluir la nueva clave KSK (13039) en el archivo /etc/bind/db.unl.edu.ec:

   ;ZSK
   $INCLUDE Kunl.edu.ec.+005+49083.key
   $INCLUDE Kunl.edu.ec.+005+02580.key

   ;KSK
   $INCLUDE Kunl.edu.ec.+005+33448.key
   $INCLUDE Kunl.edu.ec.+005+13039.key

Observe la figura 193, donde se utiliza la directiva $INCLUDE para incluir las claves.

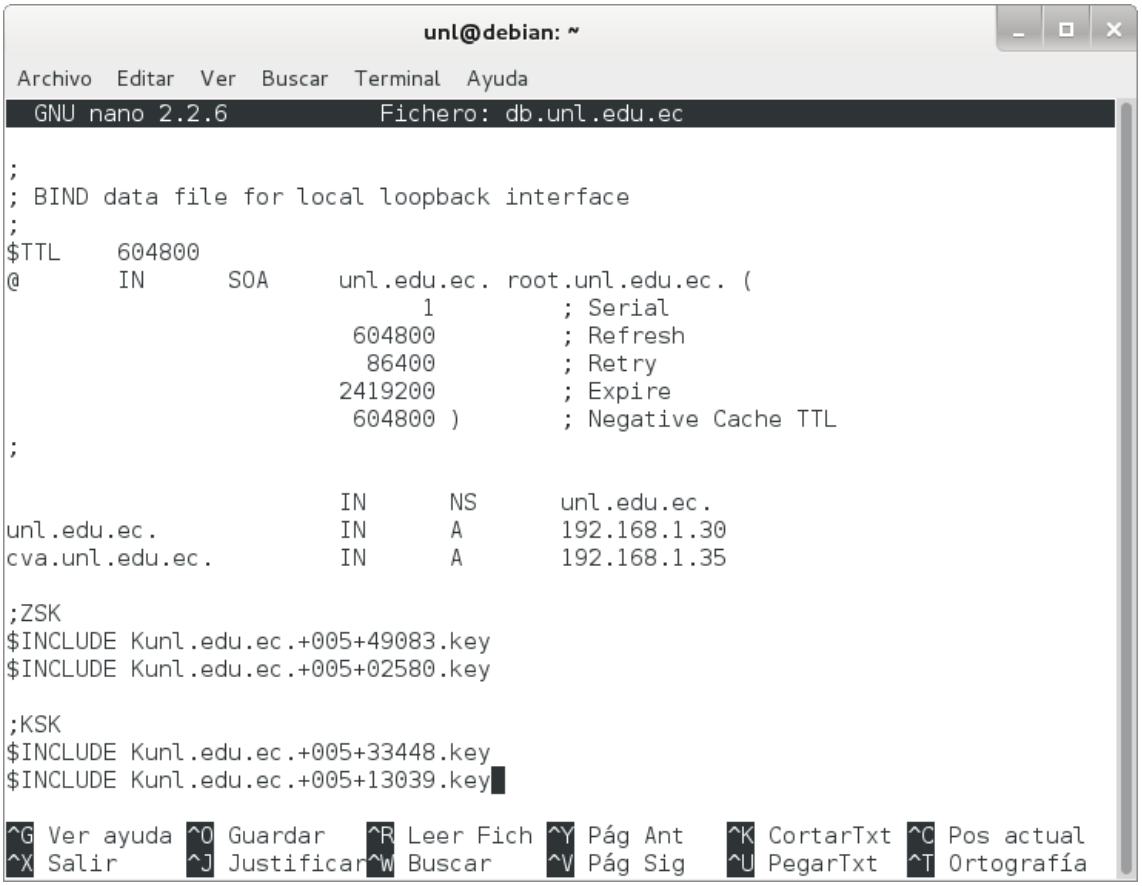

Figura 193. Inserción de las claves en la zona.

3. Firmar la zona utilizando ambas claves KSK y la clave ZSK activa:

   # dnssec-signzone -o unl.edu.ec -k Kunl.edu.ec.+005+33448.key -k Kunl.edu.ec.+005+13039.key db.unl.edu.ec Kunl.edu.ec.+005+49083.key

3. Limpiar KSK (fase 2).

Para ello se hizo:

1. Remover la clave anterior (33448) del conjunto de inclusiones:

   ;ZSK
   $INCLUDE Kunl.edu.ec.+005+49083.key
   $INCLUDE Kunl.edu.ec.+005+02580.key

   ;KSK
   $INCLUDE Kunl.edu.ec.+005+13039.key

Observe la figura 194, donde se ha eliminado la clave KSK anterior.

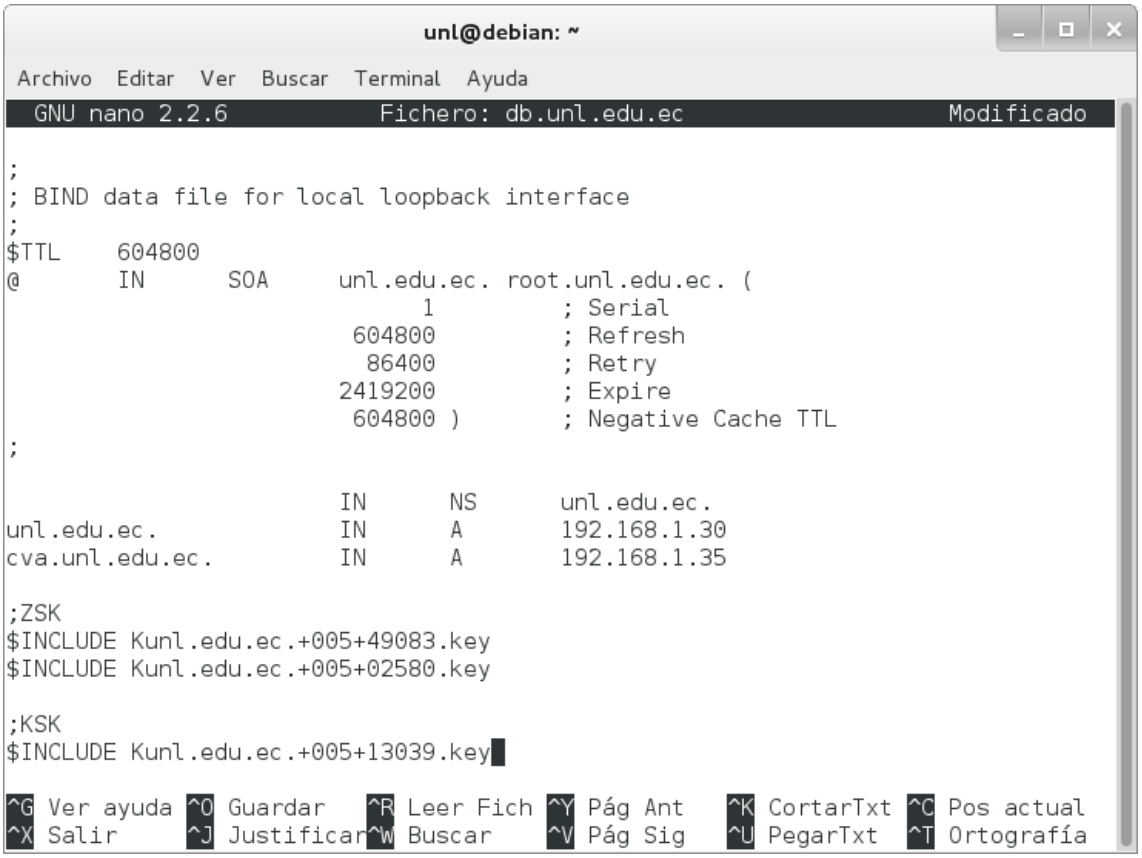

Figura 194. Eliminación de una clave KSK.

2. Firmar la zona utilizando la nueva clave KSK y la clave ZSK activa:

   # dnssec-signzone -o unl.edu.ec -k Kunl.edu.ec.+005+13039.key db.unl.edu.ec Kunl.edu.ec.+005+49083.key

3. Borrar la anterior clave anterior (33448):

   # rm Kunl.edu.ec.+005+33448.key

Anexo 20: Renovación de la clave KSK de la comunidad virtual de aprendizaje de la Universidad Nacional de Loja.

1. Preparar KSK (fase de producción).

Para lo cual se siguieron los siguientes pasos:

1. Incluir las mismas claves de la sección 3 del Anexo 16 en la zona añadiendo la directiva $INCLUDE al archivo /etc/bind/db.cva.unl.edu.ec:

   ;ZSK
   $INCLUDE Kcva.unl.edu.ec.+005+38691.key
   $INCLUDE Kcva.unl.edu.ec.+005+54081.key

   ;KSK
   $INCLUDE Kunl.edu.ec.+005+04003.key

Observe la figura 195, donde se utiliza la directiva $INCLUDE para incluir las claves.

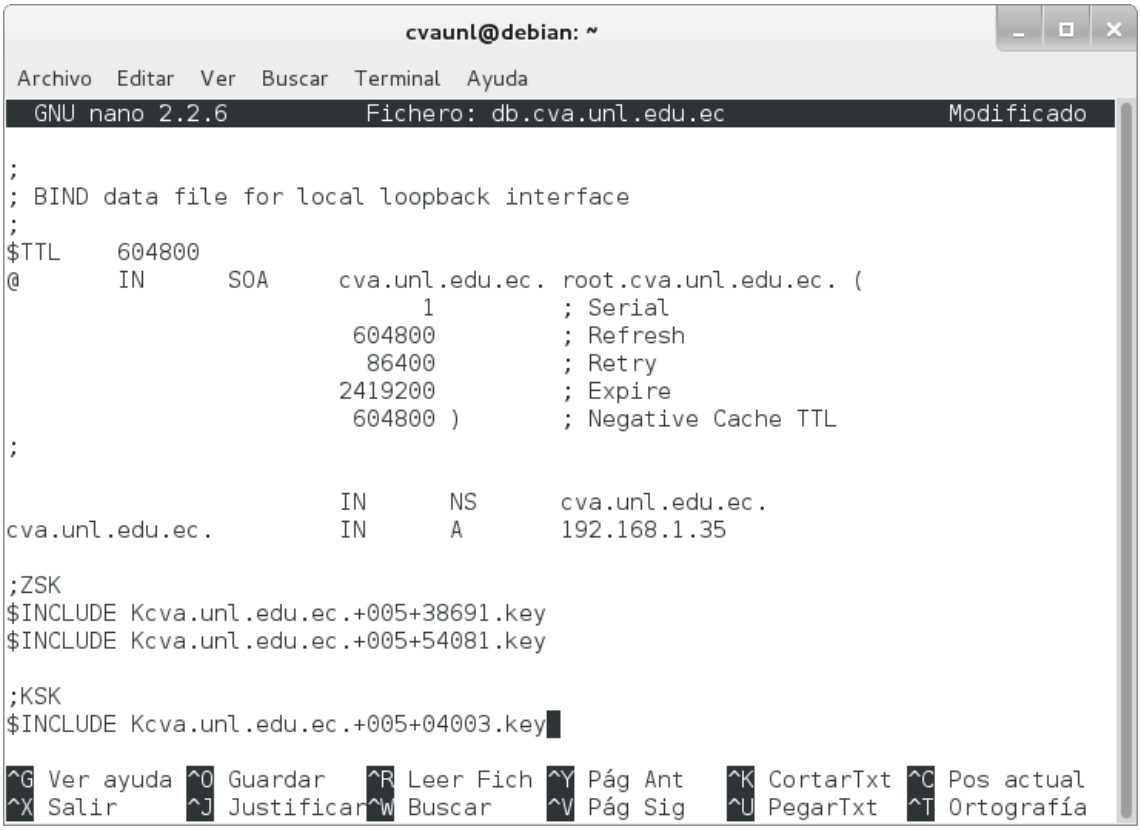

Figura 195. Inserción de las claves en la zona.

2. Firmar la zona al igual que en la sección 3 del Anexo 16:

   # dnssec-signzone -o cva.unl.edu.ec -k Kcva.unl.edu.ec.+005+04003.key db.cva.unl.edu.ec Kcva.unl.edu.ec.+005+38691.key

2. Renovar KSK (fase 1).

Se realizó haciendo lo siguiente:

1. Generar una nueva clave KSK:

   # dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE cva.unl.edu.ec

2. Incluir la nueva clave KSK (09928) en el archivo /etc/bind/db.cva.unl.edu.ec:

   ;ZSK
   $INCLUDE Kcva.unl.edu.ec.+005+38691.key
   $INCLUDE Kcva.unl.edu.ec.+005+54081.key

   ;KSK
   $INCLUDE Kcva.unl.edu.ec.+005+04003.key
   $INCLUDE Kcva.unl.edu.ec.+005+09928.key

Observe la figura 196, donde se utiliza la directiva $INCLUDE para incluir las claves.

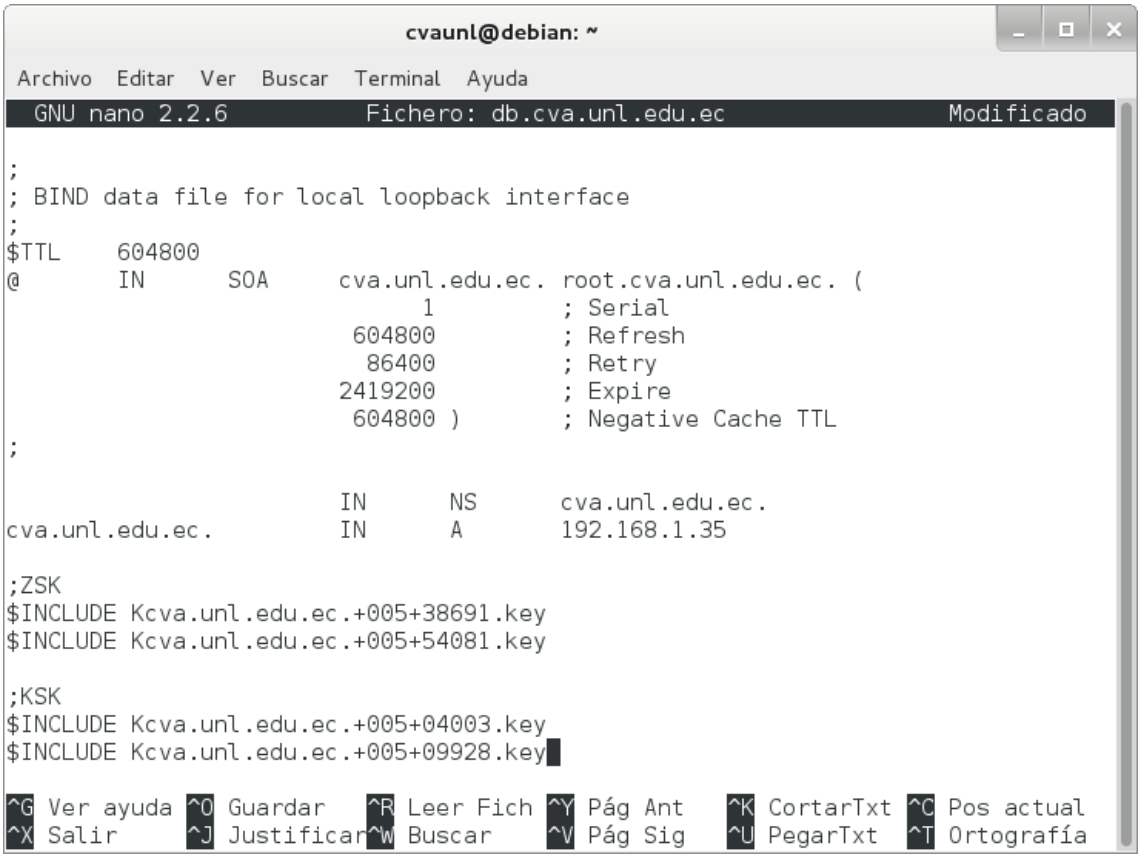

Figura 196. Inserción de las claves en la zona.

3. Firmar la zona utilizando ambas claves KSK y la clave ZSK activa:

   # dnssec-signzone -o cva.unl.edu.ec -k Kcva.unl.edu.ec.+005+04003.key -k Kcva.unl.edu.ec.+005+09928.key db.cva.unl.edu.ec Kcva.unl.edu.ec.+005+38691.key

3. Limpiar KSK (fase 2).

Para ello se hizo:

1. Remover la clave anterior (04003) del conjunto de inclusiones:

   ;ZSK
   $INCLUDE Kcva.unl.edu.ec.+005+39691.key
   $INCLUDE Kcva.unl.edu.ec.+005+54081.key

   ;KSK
   $INCLUDE Kcva.unl.edu.ec.+005+09928.key

Observe la figura 197, donde se ha eliminado la clave KSK anterior.

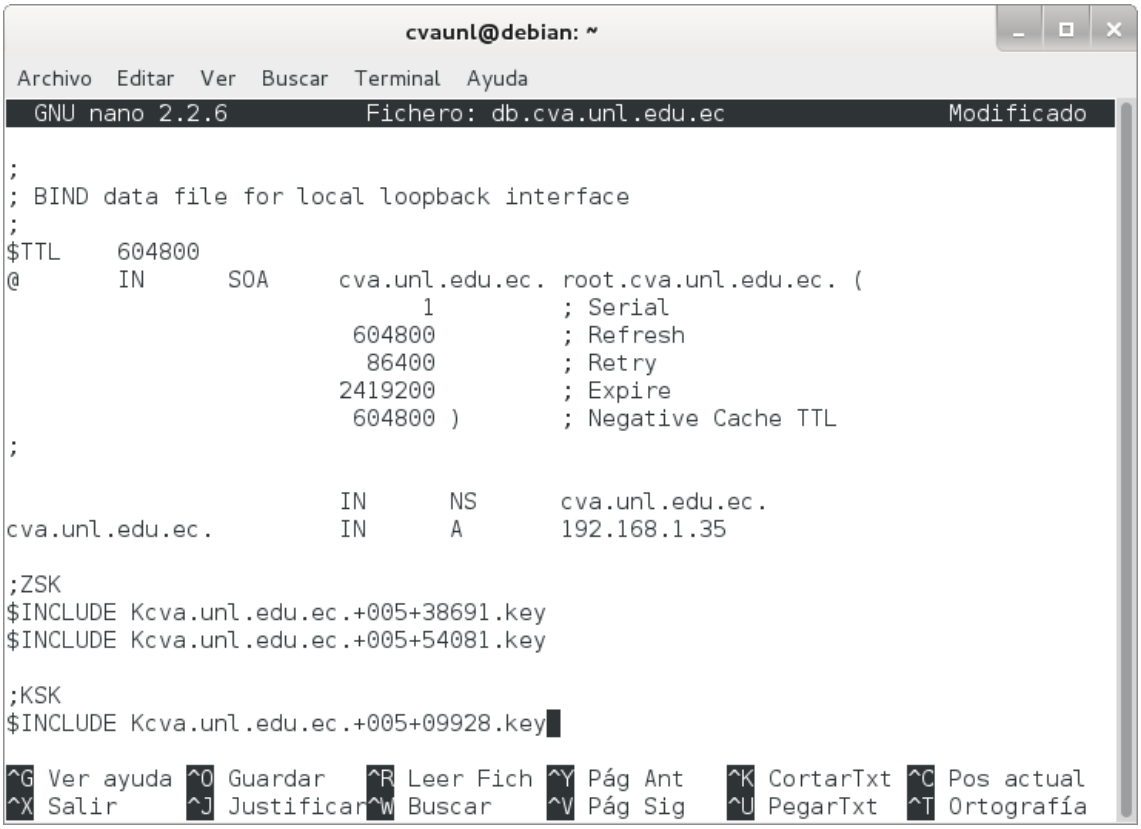

Figura 197. Eliminación de una clave KSK.

2. Firmar la zona utilizando la nueva clave KSK y la clave ZSK activa:

   # dnssec-signzone -o cva.unl.edu.ec -k Kcva.unl.edu.ec.+005+09928.key db.cva.unl.edu.ec Kcva.unl.edu.ec.+005+38691.key

3. Borrar la anterior clave anterior (04003):

   # rm Kcva.unl.edu.ec.+005+04003.key

Anexo 21: Renovación de la clave KSK del sitio web de la Universidad Técnica Particular de Loja.

1. Preparar KSK (fase de producción).

Para lo cual se siguieron los siguientes pasos:

1. Incluir las mismas claves de la sección 3 del Anexo 17 en la zona añadiendo la directiva $INCLUDE al archivo /etc/bind/db.utpl.edu.ec:

   ;ZSK
   $INCLUDE Kutpl.edu.ec.+005+21003.key
   $INCLUDE Kutpl.edu.ec.+005+35841.key

   ;KSK
   $INCLUDE Kutpl.edu.ec.+005+62482.key

Observe la figura 198, donde se utiliza la directiva $INCLUDE para incluir las claves.

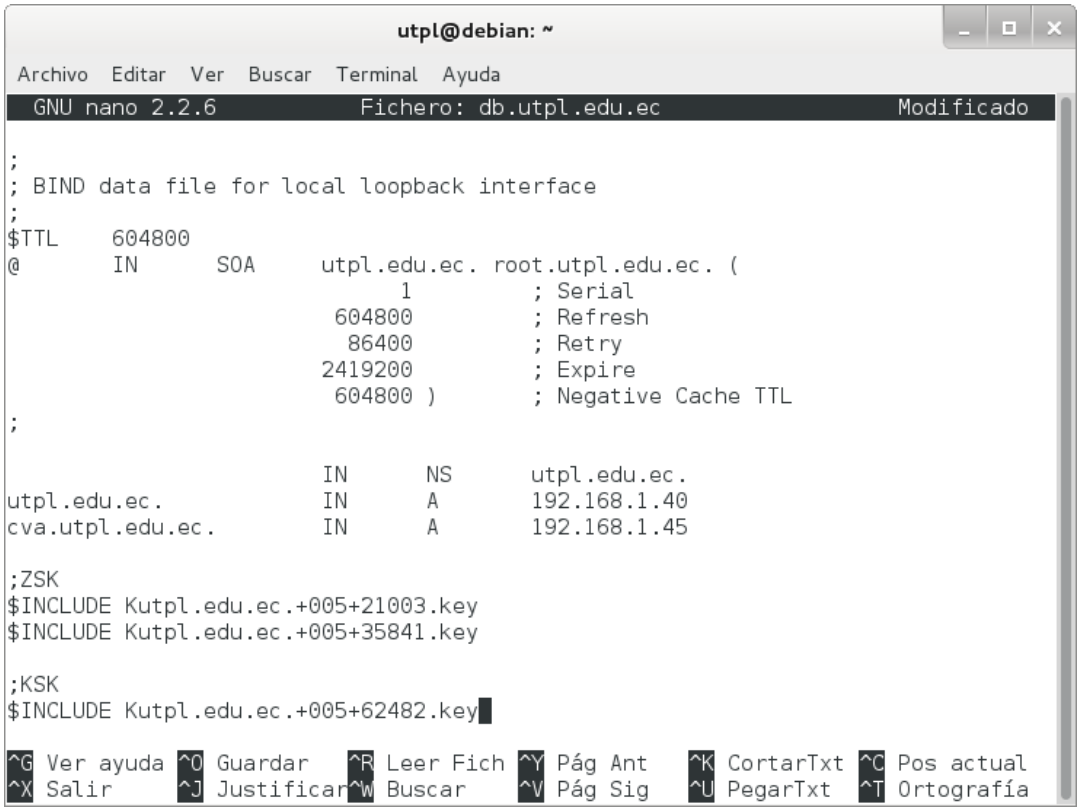

Figura 198. Inserción de las claves en la zona.

2. Firmar la zona al igual que en la sección 3 del Anexo 17:

   # dnssec-signzone -o utpl.edu.ec -k Kutpl.edu.ec.+005+62482.key db.utpl.edu.ec Kutpl.edu.ec.+005+21003.key

2. Renovar KSK (fase 1).

Se realizó haciendo lo siguiente:

1. Generar una nueva clave KSK:

   # dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE utpl.edu.ec

2. Incluir la nueva clave KSK (18949) en el archivo /etc/bind/db.utpl.edu.ec:

   ;ZSK
   $INCLUDE Kutpl.edu.ec.+005+21003.key
   $INCLUDE Kutpl.edu.ec.+005+35841.key

   ;KSK
   $INCLUDE Kutpl.edu.ec.+005+62482.key
   $INCLUDE Kutpl.edu.ec.+005+18949.key

Observe la figura 199, donde se utiliza la directiva $INCLUDE para incluir las claves.

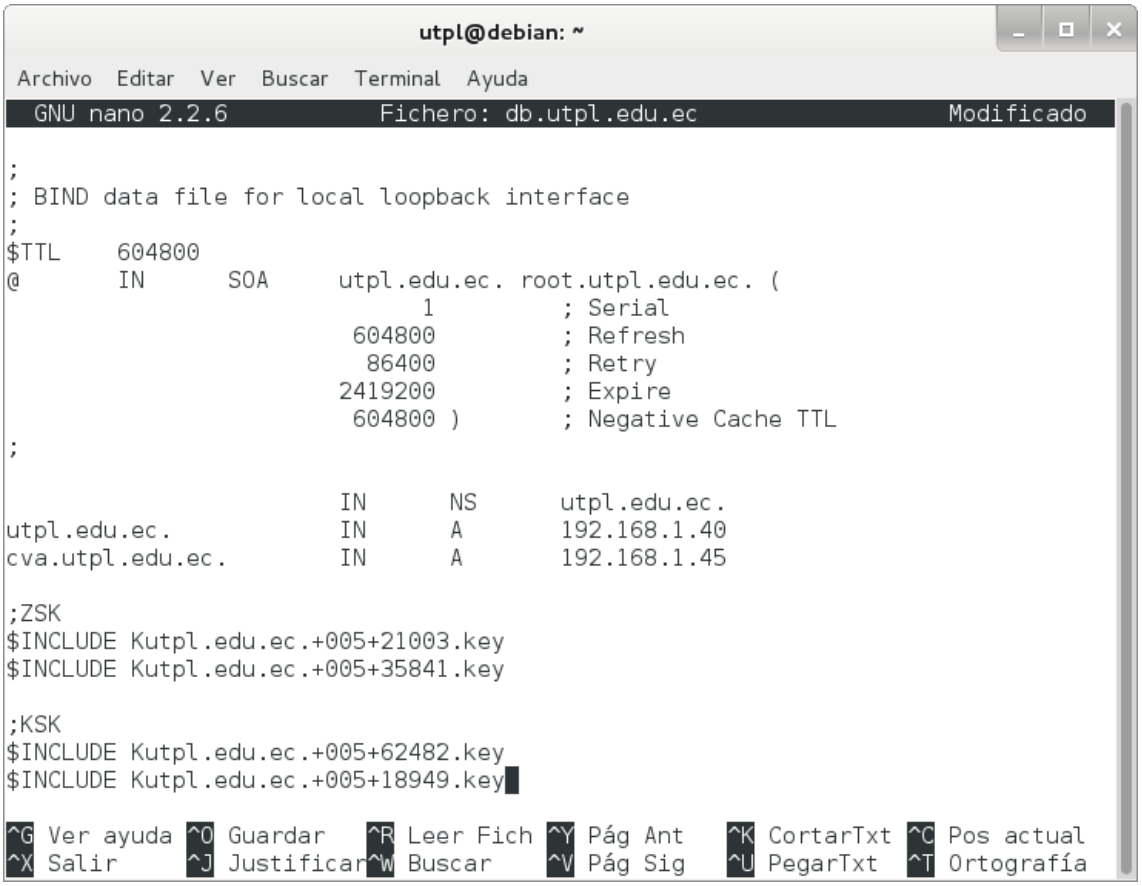

Figura 199. Inserción de las claves en la zona.

3. Firmar la zona utilizando ambas claves KSK y la clave ZSK activa:

   # dnssec-signzone -o utpl.edu.ec -k Kutpl.edu.ec.+005+62482.key -k Kutpl.edu.ec.+005+18949.key db.utpl.edu.ec Kutpl.edu.ec.+005+21003.key

3. Limpiar KSK (fase 2).

Para ello se hizo:

1. Remover la clave anterior (62482) del conjunto de inclusiones:

   ;ZSK
   $INCLUDE Kutpl.edu.ec.+005+21003.key
   $INCLUDE Kutpl.edu.ec.+005+35841.key

   ;KSK
   $INCLUDE Kutpl.edu.ec.+005+18949.key

Observe la figura 200, donde se ha eliminado la clave KSK anterior.

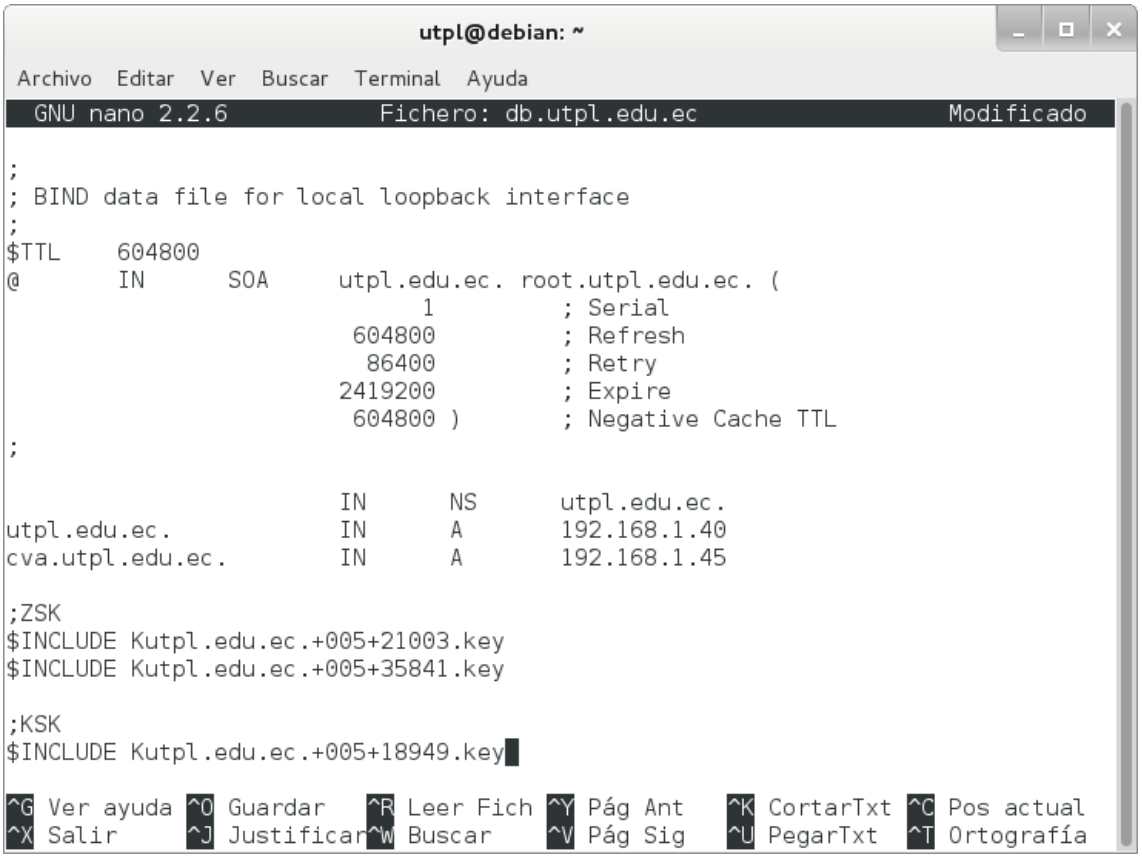

Figura 200. Eliminación de una clave KSK.

2. Firmar la zona utilizando la nueva clave KSK y la clave ZSK activa:

   # dnssec-signzone -o utpl.edu.ec -k Kutpl.edu.ec.+005+18949.key db.utpl.edu.ec Kutpl.edu.ec.+005+21003.key

3. Borrar la anterior clave anterior (62482):

   # rm Kutpl.edu.ec.+005+62482.key

Anexo 22: Renovación de la clave KSK de la comunidad virtual de aprendizaje de la Universidad Técnica Particular de Loja.

1. Preparar KSK (fase de producción).

Para lo cual se siguieron los siguientes pasos:

1. Incluir las mismas claves de la sección 3 del Anexo 18 en la zona añadiendo la directiva $INCLUDE al archivo /etc/bind/db.cva.utpl.edu.ec:

   ;ZSK
   $INCLUDE Kcva.utpl.edu.ec.+005+27450.key
   $INCLUDE Kcva.utpl.edu.ec.+005+56943.key

   ;KSK
   $INCLUDE Kcva.utpl.edu.ec.+005+38632.key

Observe la figura 201, donde se utiliza la directiva $INCLUDE para incluir las claves.

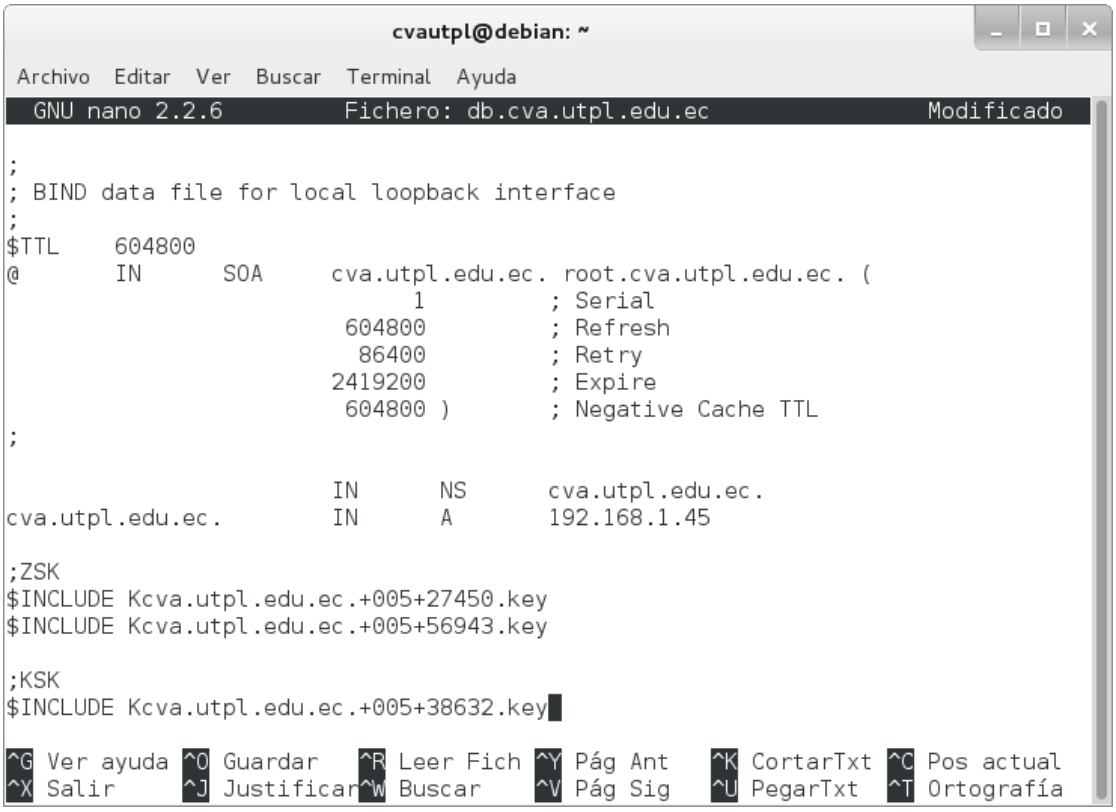

Figura 201. Inserción de las claves en la zona.

2. Firmar la zona al igual que en la sección 3 del Anexo 18:

   # dnssec-signzone -o cva.utpl.edu.ec -k Kcva.utpl.edu.ec.+005+38632.key db.cva.utpl.edu.ec Kcva.utpl.edu.ec.+005+27450.key

2. Renovar KSK (fase 1).

Se realizó haciendo lo siguiente:

1. Generar una nueva clave KSK:

   # dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE cva.utpl.edu.ec

2. Incluir la nueva clave KSK (56536) en el archivo /etc/bind/db.cva.utpl.edu.ec:

   ;ZSK
   $INCLUDE Kcva.utpl.edu.ec.+005+27450.key
   $INCLUDE Kcva.utpl.edu.ec.+005+56943.key

   ;KSK
   $INCLUDE Kcva.utpl.edu.ec.+005+38632.key
   $INCLUDE Kcva.utpl.edu.ec.+005+56536.key

Observe la figura 202, donde se utiliza la directiva $INCLUDE para incluir las claves.

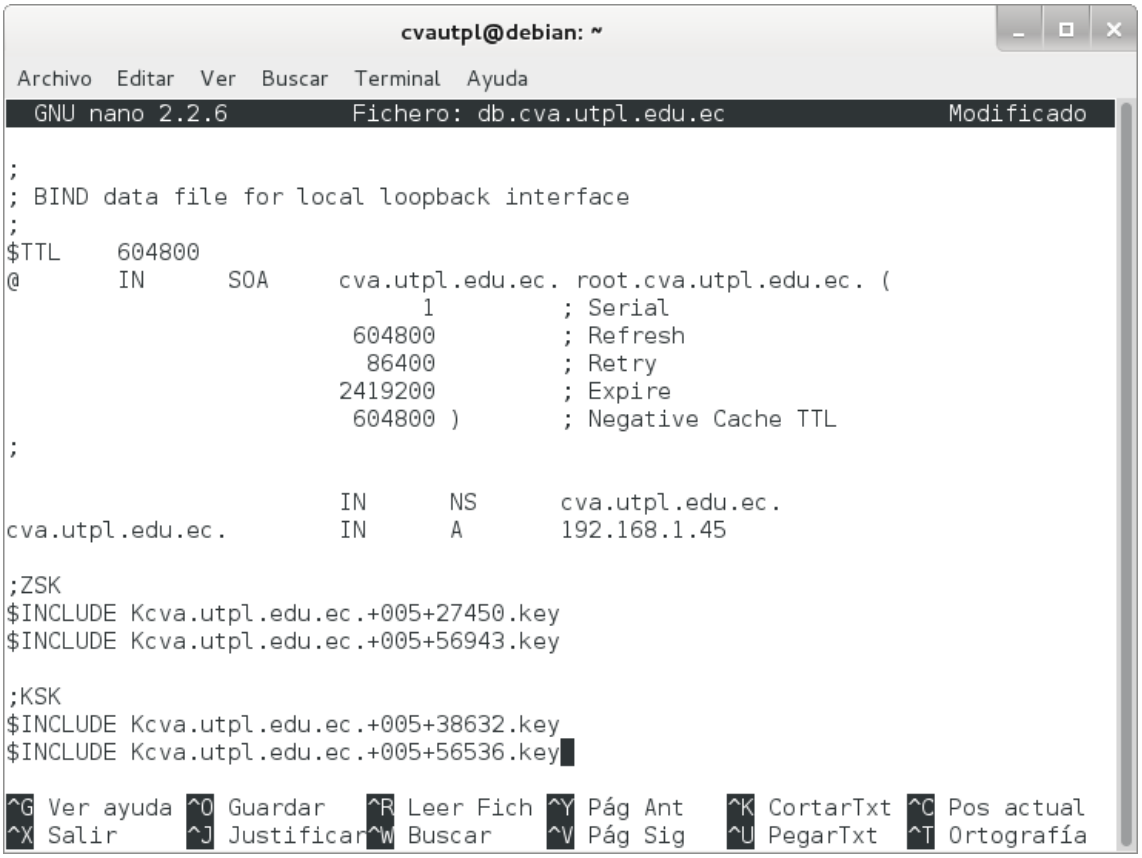

Figura 202. Inserción de las claves en la zona.

3. Firmar la zona utilizando ambas claves KSK y la clave ZSK activa:

 # dnssec-signzone -o cva.utpl.edu.ec -k Kcva.utpl.edu.ec.+005+38632.key -k Kcva.utpl.edu.ec.+005+56536.key db.cva.utpl.edu.ec Kcva.utpl.edu.ec.+005+27450.key

3. Limpiar KSK (fase 2).

Para ello se hizo:

1. Remover la clave anterior (38632) del conjunto de inclusiones:

;ZSK
$INCLUDE Kcva.utpl.edu.ec.+005+27450.key
$INCLUDE Kcva.utpl.edu.ec.+005+56943.key

;KSK
$INCLUDE Kcva.utpl.edu.ec.+005+56536.key

Observe la figura 203, donde se ha eliminado la clave KSK anterior.

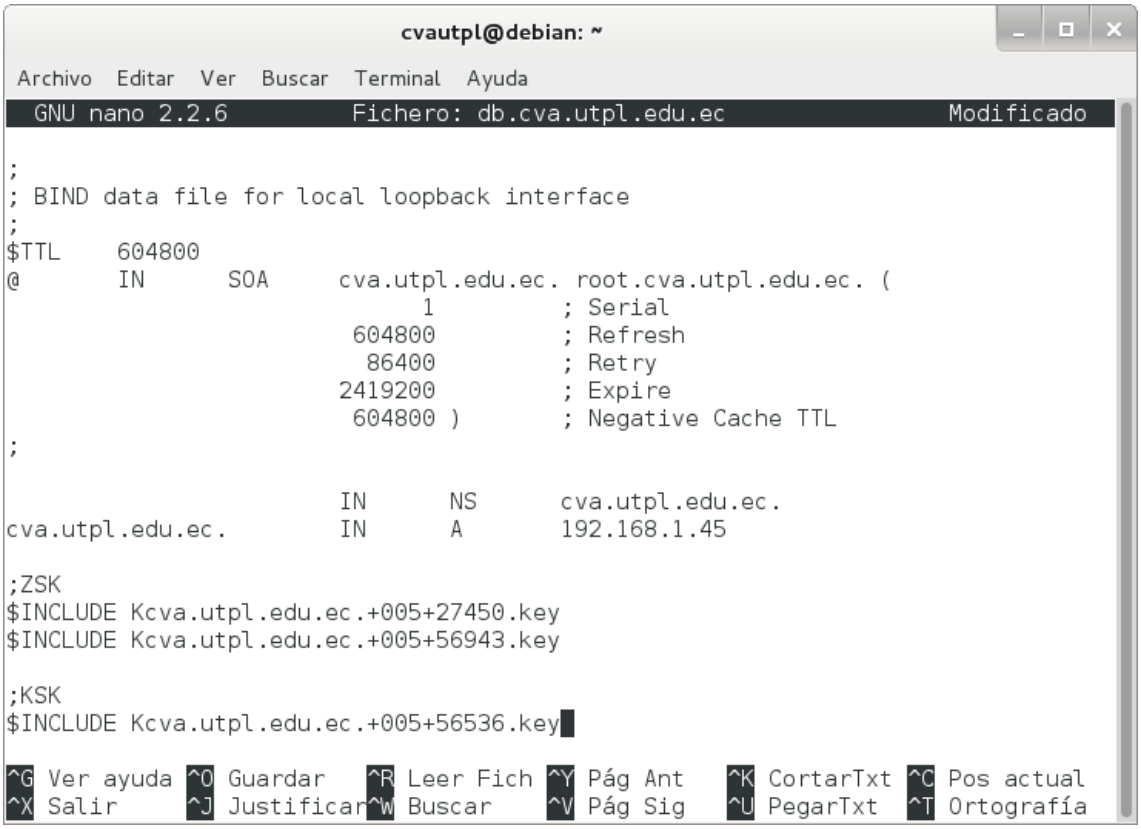

Figura 203. Eliminación de una clave KSK.

2. Firmar la zona utilizando la nueva clave KSK y la clave ZSK activa:

   # dnssec-signzone -o cva.utpl.edu.ec -k Kcva.utpl.edu.ec.+005+56536.key db.cva.utpl.edu.ec Kcva.utpl.edu.ec.+005+27450.key

3. Borrar la anterior clave anterior (38632):

   # rm Kcva.utpl.edu.ec.+005+38632.key

Anexo 23: Transferencia de zona del sitio web de la Universidad Nacional de Loja.

1. Generación de una clave TSIG.

Se creó un secreto compartido con dnssec-keygen que es la herramienta utilizada para generar un número aleatorio codificado en base64 que se utilizó como el secreto.

Para generar una clave TSIG se utilizó los argumentos que ofrece dnssec-keygen que son:

 # dnssec-keygen -a hmac-md5 -b 256 -n HOST unl.edu.ec.

Con lo que se creó una clave TSIG con el tipo de algoritmo HMAC-MD5, tamaño de la clave 256 y unl.edu.ec. como el nombre de la zona, tal como se muestra en la figura 204.

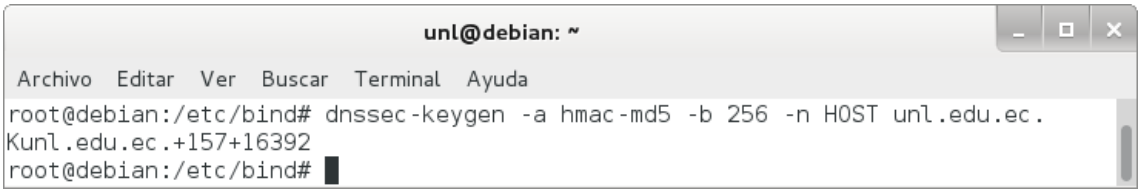

Figura 204. Clave TSIG.

El comando generó dos archivos como se muestra en las figuras 205 y 206.

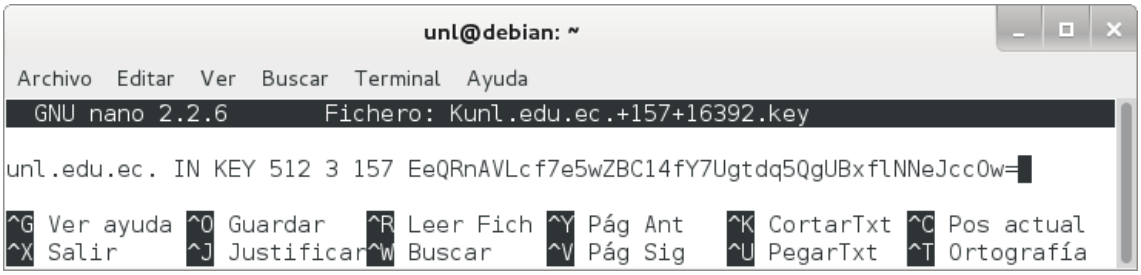

Figura 205. Archivo Kunl.edu.ec.+157+16392.key.

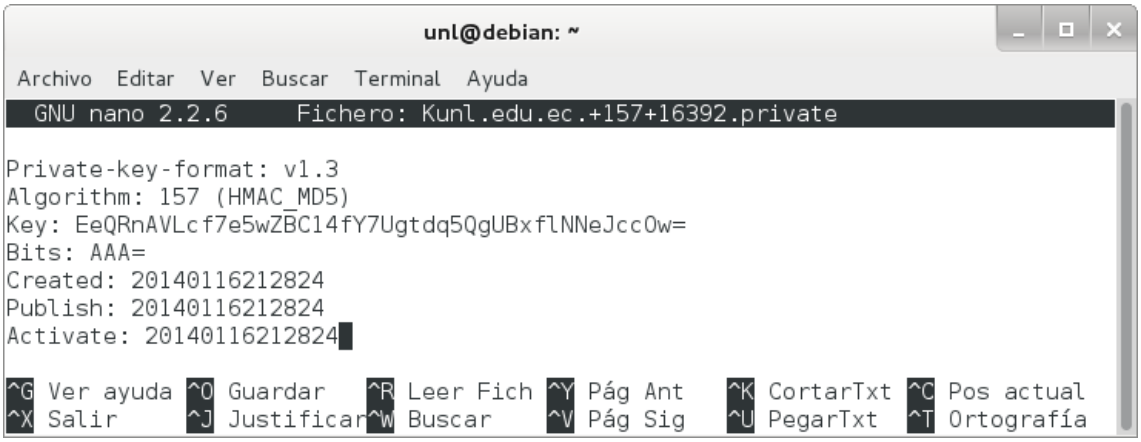

Figura 206. Archivo Kunl.edu.ec.+157+16392.private.

El nombre de los archivos contiene información relevante:

Kdomain_name+algorithm_id+key_id.extension

El domain_name es el nombre especificado como el nombre de la clave. El algorithm_id identifica el algoritmo utilizado: 5 para HMAC-MD5 (1 y 3 son para RSA y DSA, respectivamente). El key_id es un identificador para el material clave, no es de relevancia para las claves simétricas.La extension es cualquier key o private, la primera es la clave pública y la segunda es la clave privada [17].

2. Configurar las claves TSIG.

Para asegurar una transferencia de zona, el servidor primario y los administradores de los servidores secundarios tienen que configurar una clave TSIG en named.conf. La clave TSIG se compone de un secreto y un algoritmo de hash y son identificados por los nombres del dominio [17].

Los pasos para configurar las claves TSIG son:

1. Crear el archivo /etc/bind/tsig.keys:

 # nano /etc/bind/tsig.keys

Donde se especifica el algoritmo y el secreto de la zona como se ilustra en la figura 207.

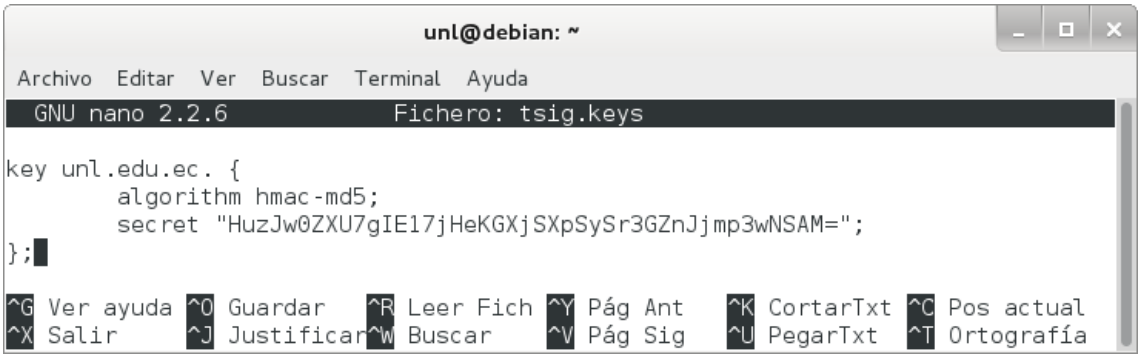

Figura 207. Archivo tsig.keys.

2. Incluir el archivo /etc/bind/tsig.keys en el archivo /etc/bind/named.conf:

include "/etc/bind/tsig.keys";

Observe la figura 208, donde se incluye el archivo /etc/bind/tsig.keys.

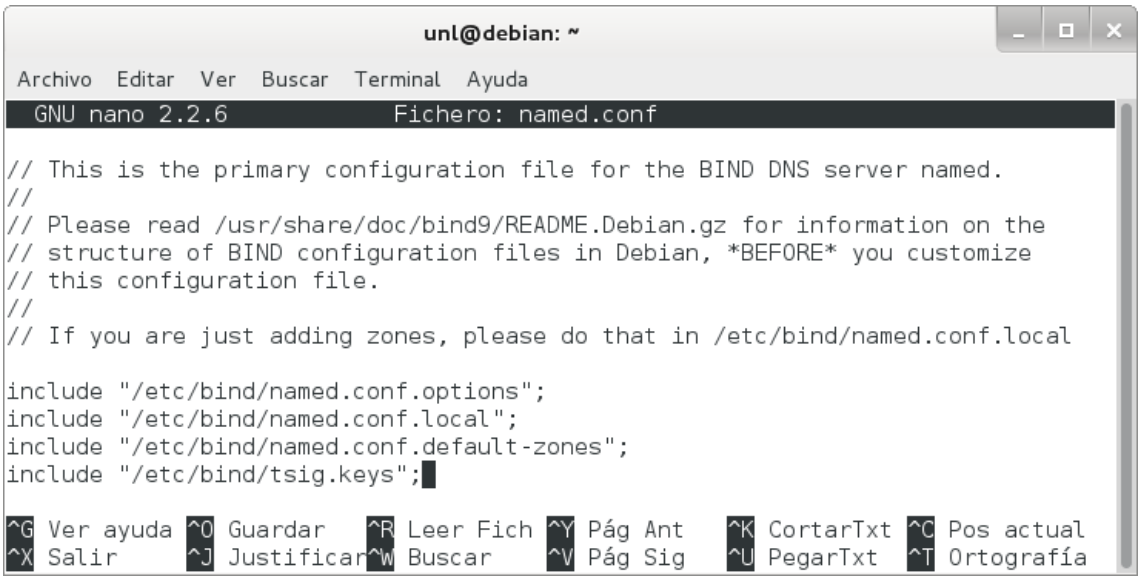

Figura 208. Inserción del archivo tsig.keys.

3. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 209.

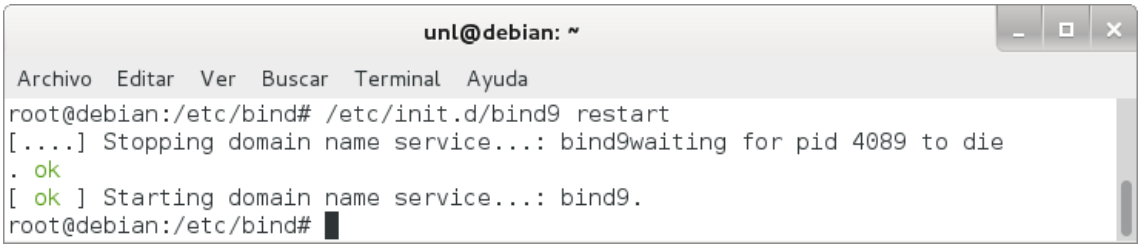

Figura 209. Reinicio del servicio.

3. Configurar el servidor primario de TSIG.

En el servidor de nombres primario, se puede restringir las transferencias de zona sólo a las firmadas con una clave específica.

El procedimiento para configurar el servidor primario fue:

1. Permitir la transferencia agregando el parámetro allow-transfer en el archivo /etc/bind/named.conf.local:

```
zone “unl.edu.ec” {
        type master;
         file “/etc/bind/db.unl.edu.ec.signed”;
         allow-transfer {  key unl.edu.ec. ; };
};
```

Donde se restringe las transferencias de zona a los firmados con la clave unl.edu.ec. como se muestra en la figura 210.

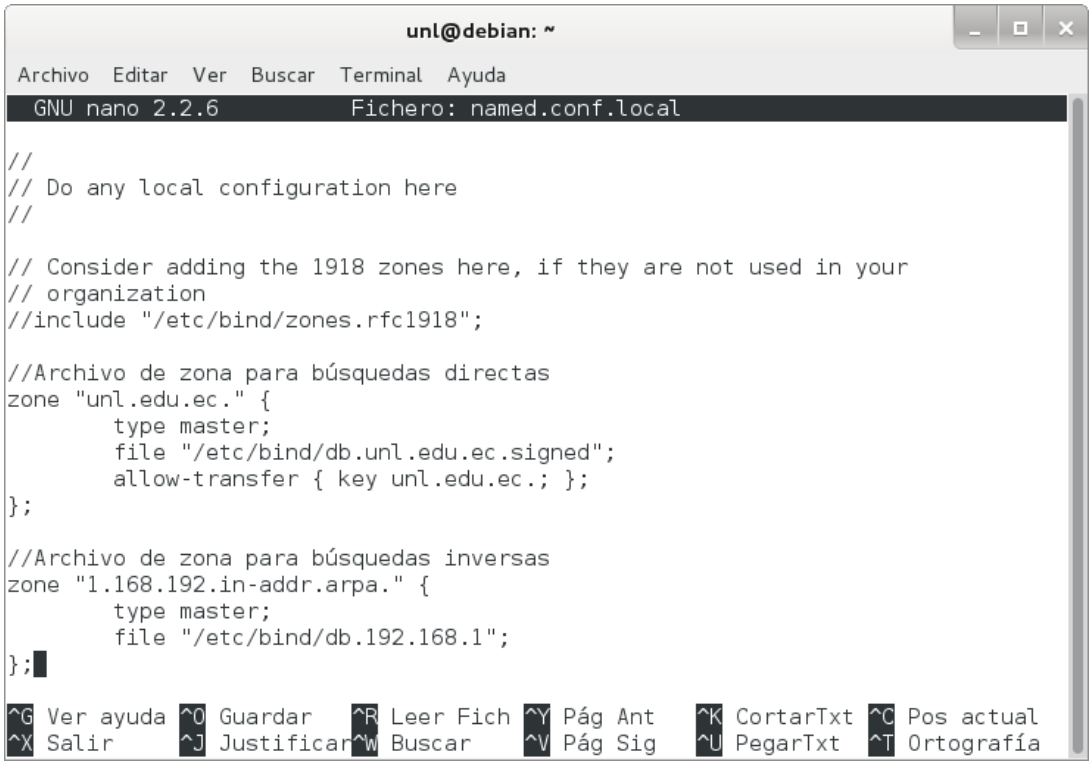

Figura 210. Restricción de la transferencia.

2. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 211.

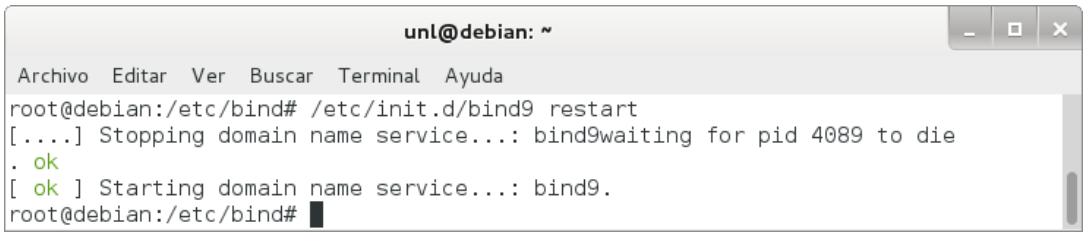

Figura 211. Reinicio del servicio.

4. Realizar pruebas.

Para esto se realizó lo siguiente:

1. Emplear el comando dig en el servidor:

 # dig @localhost -k Kunl.edu.ec.+157+16392.key unl.edu.ec AXFR

Con lo que el resultado de la clave TSIG para la zona unl.edu.ec configurada correctamente quedaría como se muestra en la figura 212.

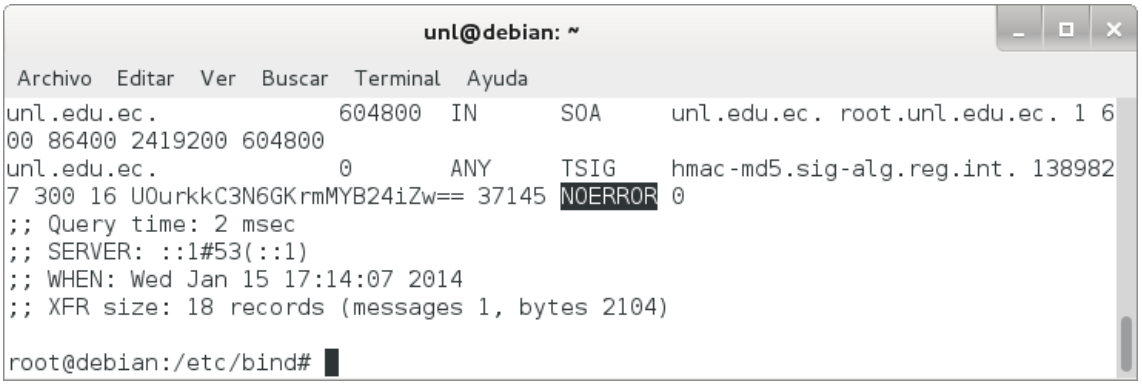

Figura 212. Ejecución correcta de dig.

2. Revisar el log del sistema:

 # tail -f /var/log/syslog

Donde el resultado del log muestra la transferencia exitosa como se indica en la figura 213.

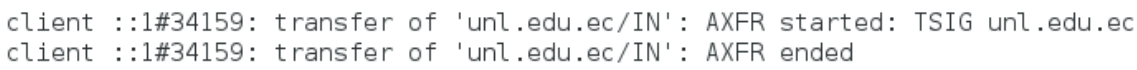

Figura 213. Registro del sistema.

3. Emplear el comando dig desde el usuario:

 # dig unl.edu.ec @192.168.1.30 AXFR

Lo que da como resultado una transferencia fallida como se manifiesta en la figura 214.

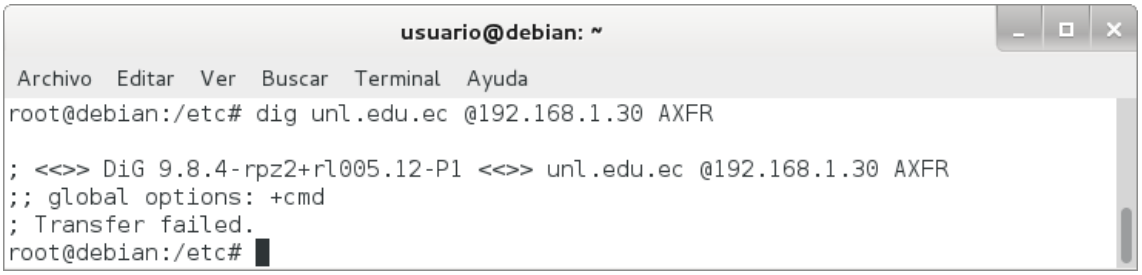

Figura 214. Transferencia fallida.

Anexo 24: Transferencia de zona de la comunidad virtual de aprendizaje de la Universidad Nacional de Loja.

1. Generación de una clave TSIG.

Se creó un secreto compartido con dnssec-keygen que es la herramienta utilizada para generar un número aleatorio codificado en base64 que se utilizó como el secreto.

Para generar una clave TSIG se utilizó los argumentos que ofrece dnssec-keygen que son:

 # dnssec-keygen -a HMAC-MD5 -b 256 -n HOST cva.unl.edu.ec.

Con lo que se creó una clave TSIG con el tipo de algoritmo HMAC-MD5, tamaño de la clave 256 y cva.unl.edu.ec. como el nombre de la zona, tal como se observa en la figura 215.

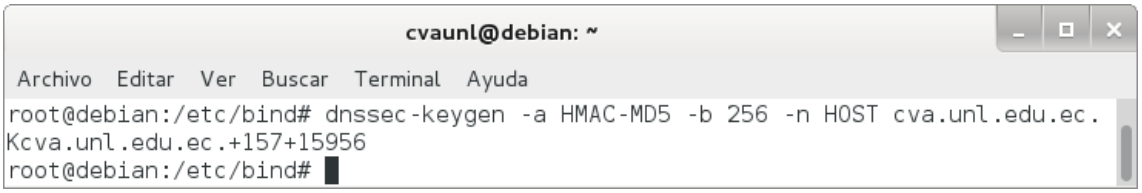

Figura 215. Clave TSIG.

El comando generó dos archivos como se muestra en las figuras 216 y 217.

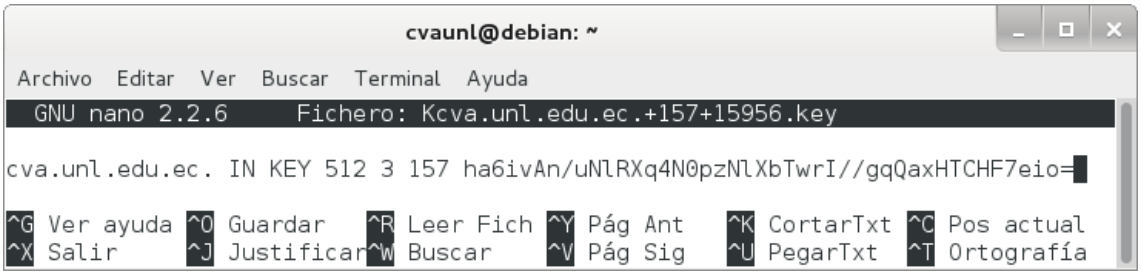

Figura 216. Archivo Kcva.unl.edu.ec.+157+15956.key.

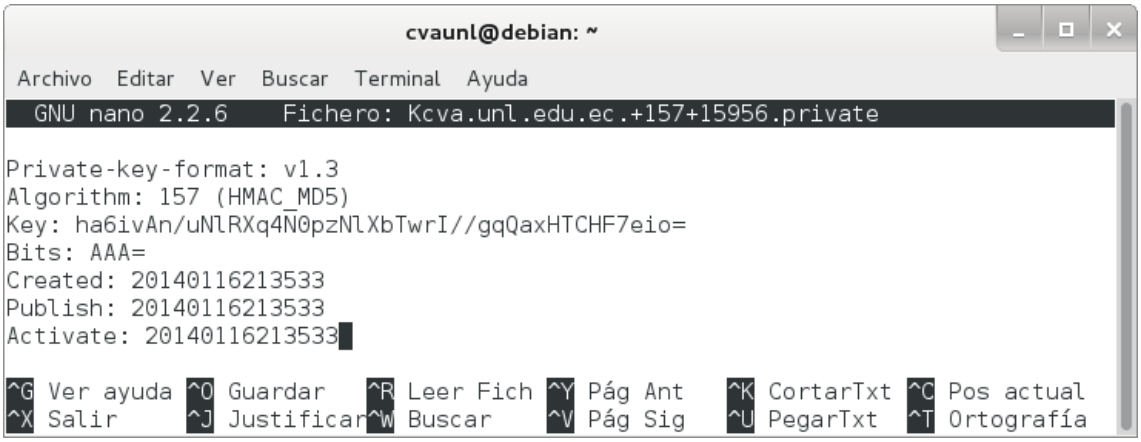

Figura 217. Archivo Kcva.unl.edu.ec.+157+15956.private.

El nombre de los archivos contiene información relevante:

Kdomain_name+algorithm_id+key_id.extension

El domain_name es el nombre especificado como el nombre de la clave. El algorithm_id identifica el algoritmo utilizado: 5 para HMAC-MD5 (1 y 3 son para RSA y DSA, respectivamente). El key_id es un identificador para el material clave, no es de relevancia para las claves simétricas.La extension es cualquier key o private, la primera es la clave pública y la segunda es la clave privada [17].

2. Configurar las claves TSIG.

Para asegurar una transferencia de zona, el servidor primario y los administradores de los servidores secundarios tienen que configurar una clave TSIG en named.conf. La clave TSIG se compone de un secreto y un algoritmo de hash y son identificados por los nombres del dominio [17].

Los pasos para configurar las claves TSIG son:

1. Crear el archivo /etc/bind/tsig.keys:

   # nano /etc/bind/tsig.keys

Donde se especifica el algoritmo y el secreto de la zona como se ilustra en la figura 218.

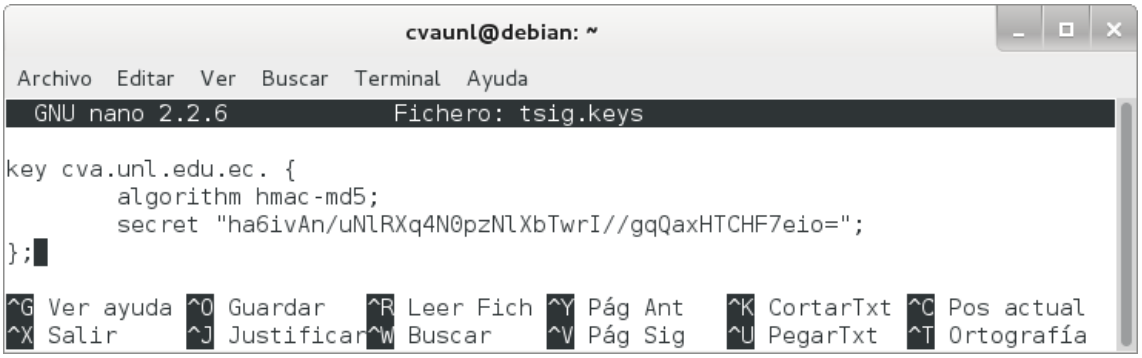

Figura 218. Archivo tsig.keys.

2. Incluir el archivo /etc/bind/tsig.keys en el archivo /etc/bind/named.conf:

include "/etc/bind/tsig.keys";

Observe la figura 219, donde se incluye el archivo /etc/bind/tsig.keys.

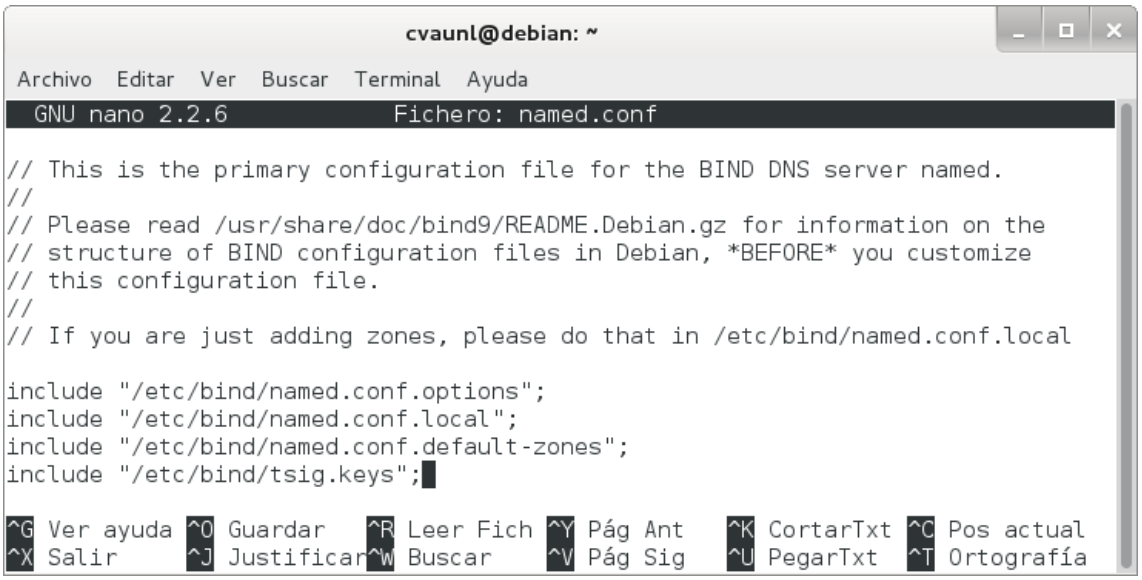

Figura 219. Inserción del archivo tsig.keys.

3. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 220.

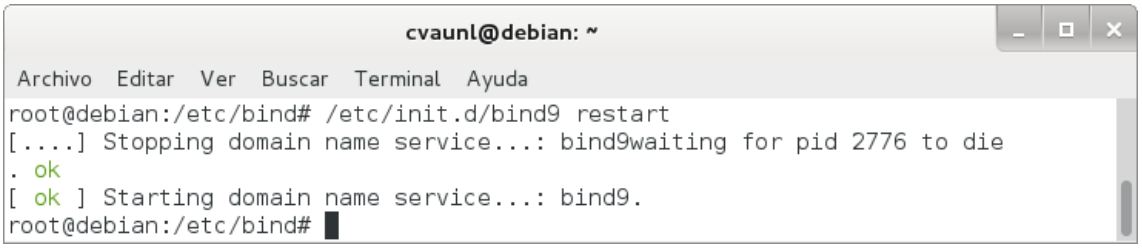

Figura 220. Reinicio del servicio.

3. Configurar el servidor primario de TSIG.

En el servidor de nombres primario, se puede restringir las transferencias de zona sólo a las firmadas con una clave específica.

El procedimiento para configurar el servidor primario fue:

1. Permitir la transferencia agregando el parámetro allow-transfer en el archivo /etc/bind/named.conf.local:

```
zone “cva.unl.edu.ec” {
        type master;
         file “/etc/bind/db.cva.unl.edu.ec.signed”;
         allow-transfer {  key cva.unl.edu.ec. ; };
};
```

Donde se restringe las transferencias de zona a los firmados con la clave cva.unl.edu.ec. como se muestra en la figura 221.

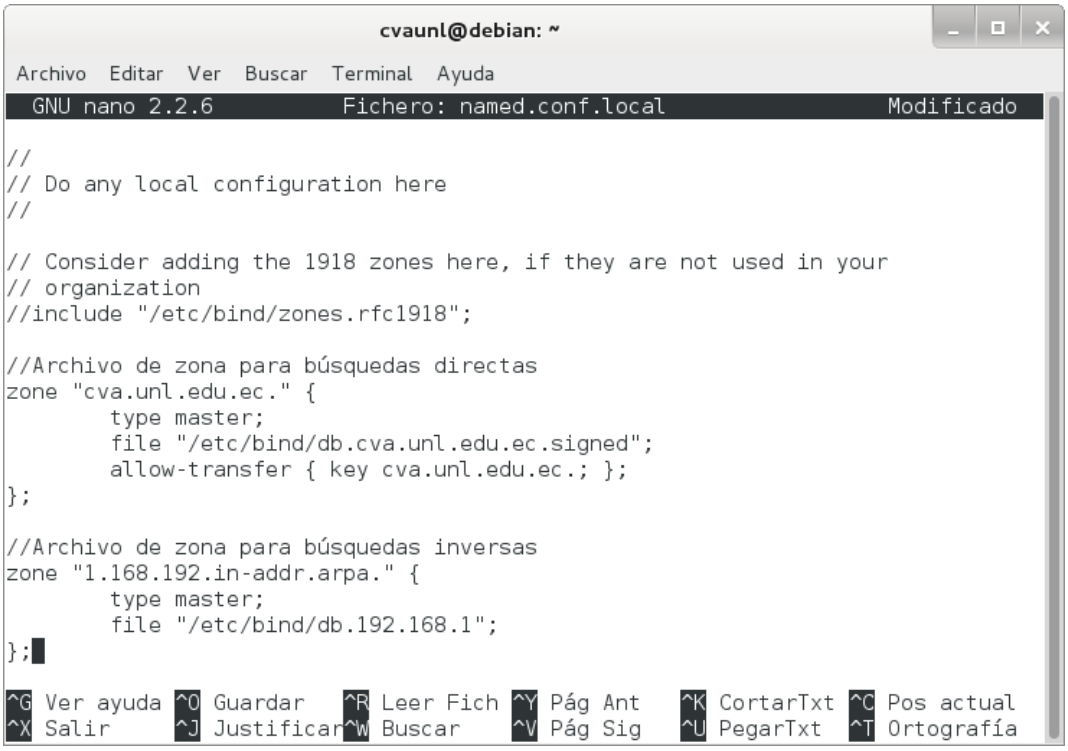

Figura 221. Restricción de la transferencia.

2. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 222.

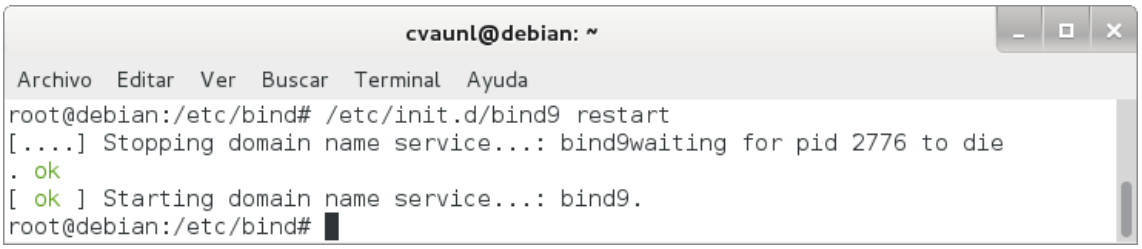

Figura 222. Reinicio del servicio.

4. Realizar pruebas.

Para esto se realizó lo siguiente:

1. Emplear el comando dig:

 # dig @localhost -k Kcva.unl.edu.ec.+157+01751.key cva.unl.edu.ec AXFR

Con lo que el resultado de la clave TSIG para la zona cva.unl.edu.ec configurada correctamente quedaría como se muestra en la figura 223.

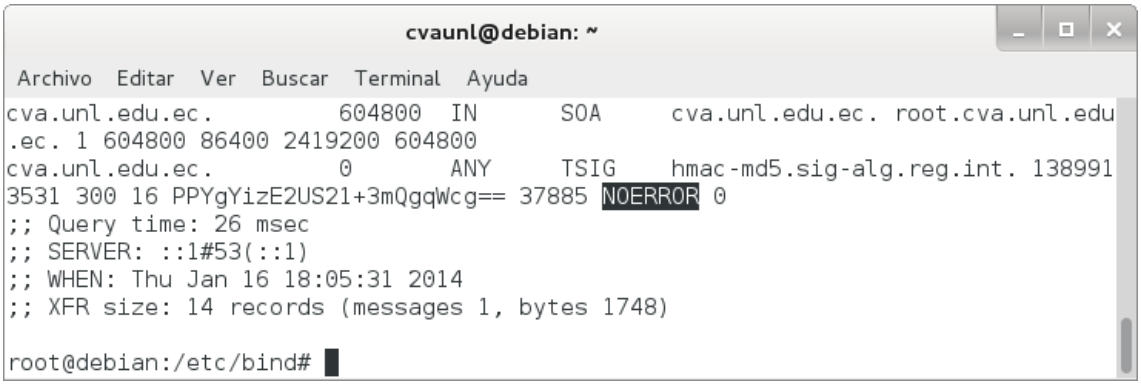

Figura 223. Ejecución correcta de dig.

2. Revisar el log del sistema:

 # tail -f /var/log/syslog

Donde el resultado del log muestra la transferencia exitosa como se indica en la figura 224.

```
client ::1#55475: transfer of 'cva.unl.edu.ec/IN': AXFR started: TSIG cva.unl.edu.ec
client ::1#55475: transfer of 'cva.unl.edu.ec/IN': AXFR ended
```

Figura 224. Registro del sistema.

3. Emplear el comando dig desde el usuario:

 # dig cva.unl.edu.ec @192.168.1.35 AXFR

Lo que da como resultado una transferencia fallida como se manifiesta en la figura 225.

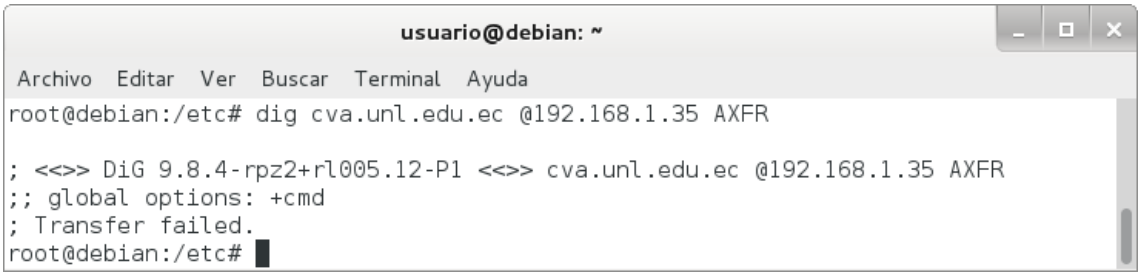

Figura 225. Transferencia fallida.

Anexo 25: Transferencia de zona del sitio web de la Universidad Técnica Particular de Loja.

1. Generación de una clave TSIG.

Se creó un secreto compartido con dnssec-keygen que es la herramienta utilizada para generar un número aleatorio codificado en base64 que se utilizó como el secreto.

Para generar una clave TSIG se utilizó los argumentos que ofrece dnssec-keygen que son:

 # dnssec-keygen -a HMAC-MD5 -b 256 -n HOST utpl.edu.ec.

Con lo que se creó una clave TSIG con el tipo de algoritmo HMAC-MD5, tamaño de la clave 256 y utpl.edu.ec. como el nombre de la zona, tal como se observa en la figura 226.

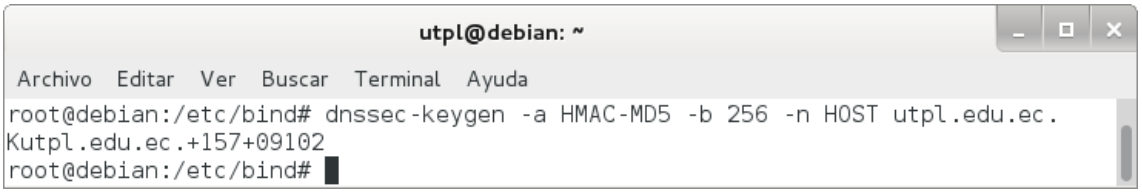

Figura 226. Clave TSIG.

El comando generó dos archivos como se muestra en las figuras 227 y 228.

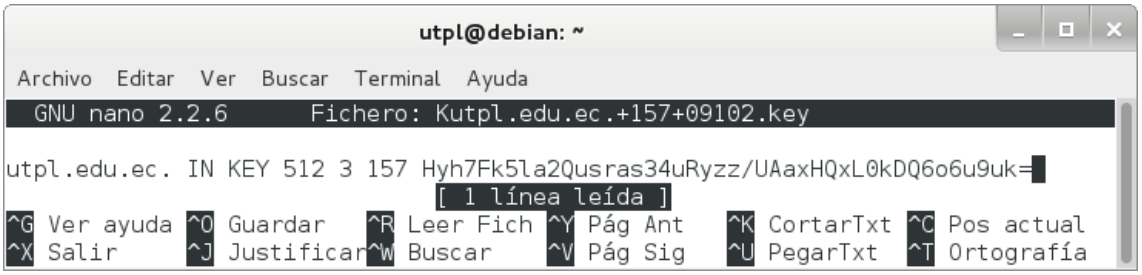

Figura 227. Archivo Kutpl.edu.ec.+157+09102.key.

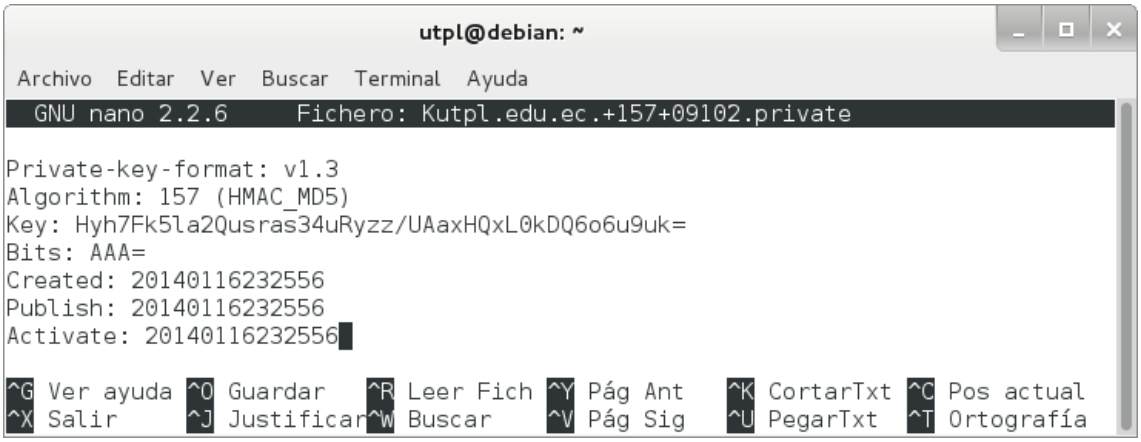

Figura 228. Archivo Kutpl.edu.ec.+157+09102.private.

El nombre de los archivos contiene información relevante:

Kdomain_name+algorithm_id+key_id.extension

El domain_name es el nombre especificado como el nombre de la clave. El algorithm_id identifica el algoritmo utilizado: 5 para HMAC-MD5 (1 y 3 son para RSA y DSA, respectivamente). El key_id es un identificador para el material clave, no es de relevancia para las claves simétricas.La extension es cualquier key o private, la primera es la clave pública y la segunda es la clave privada [17].

2. Configurar las claves TSIG.

Para asegurar una transferencia de zona, el servidor primario y los administradores de los servidores secundarios tienen que configurar una clave TSIG en named.conf. La clave TSIG se compone de un secreto y un algoritmo de hash y son identificados por los nombres del dominio [17].

Los pasos para configurar las claves TSIG son:

1. Crear el archivo /etc/bind/tsig.keys:

 # nano /etc/bind/tsig.keys

Donde se especifica el algoritmo y el secreto de la zona como se ilustra en la figura 229.

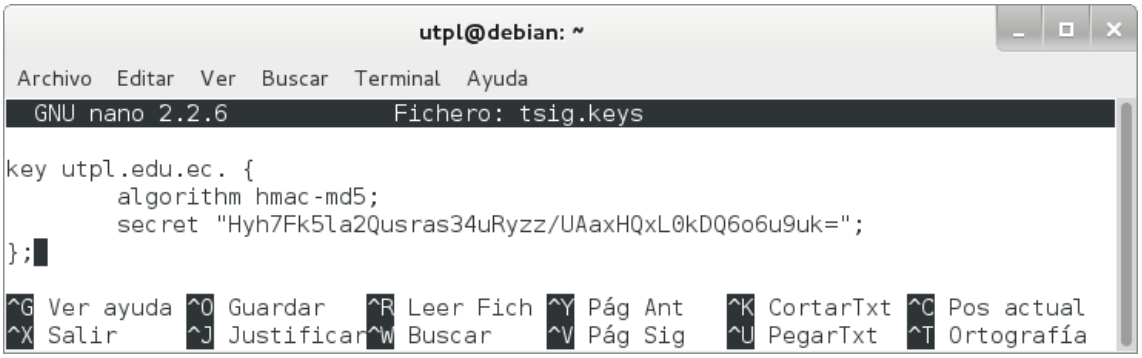

Figura 229. Archivo tsig.keys.

2. Incluir el archivo /etc/bind/tsig.keys en el archivo /etc/bind/named.conf:

include "/etc/bind/tsig.keys";

Observe la figura 230, donde se incluye el archivo /etc/bind/tsig.keys.

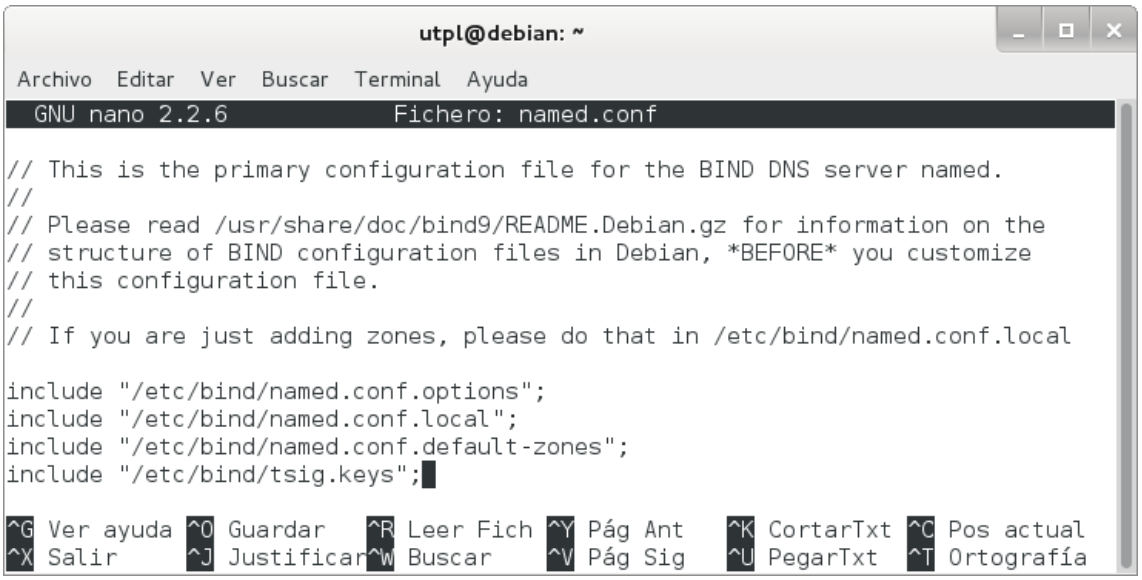

Figura 230. Inserción del archivo tsig.keys.

3. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 231.

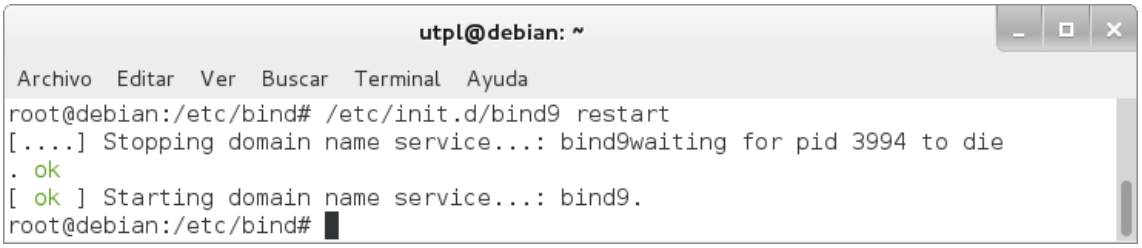

Figura 231. Reinicio del servicio.

3. Configurar el servidor primario de TSIG.

En el servidor de nombres primario, se puede restringir las transferencias de zona sólo a las firmadas con una clave específica.

El procedimiento para configurar el servidor primario fue:

1. Permitir la transferencia agregando el parámetro allow-transfer en el archivo /etc/bind/named.conf.local:

```
zone “utpl.edu.ec” {
        type master;
         file “/etc/bind/db.utpl.edu.ec.signed”;
         allow-transfer {  key utpl.edu.ec. ; };
};
```

Donde se restringe las transferencias de zona a los firmados con la clave utpl.edu.ec. como se muestra en la figura 232.

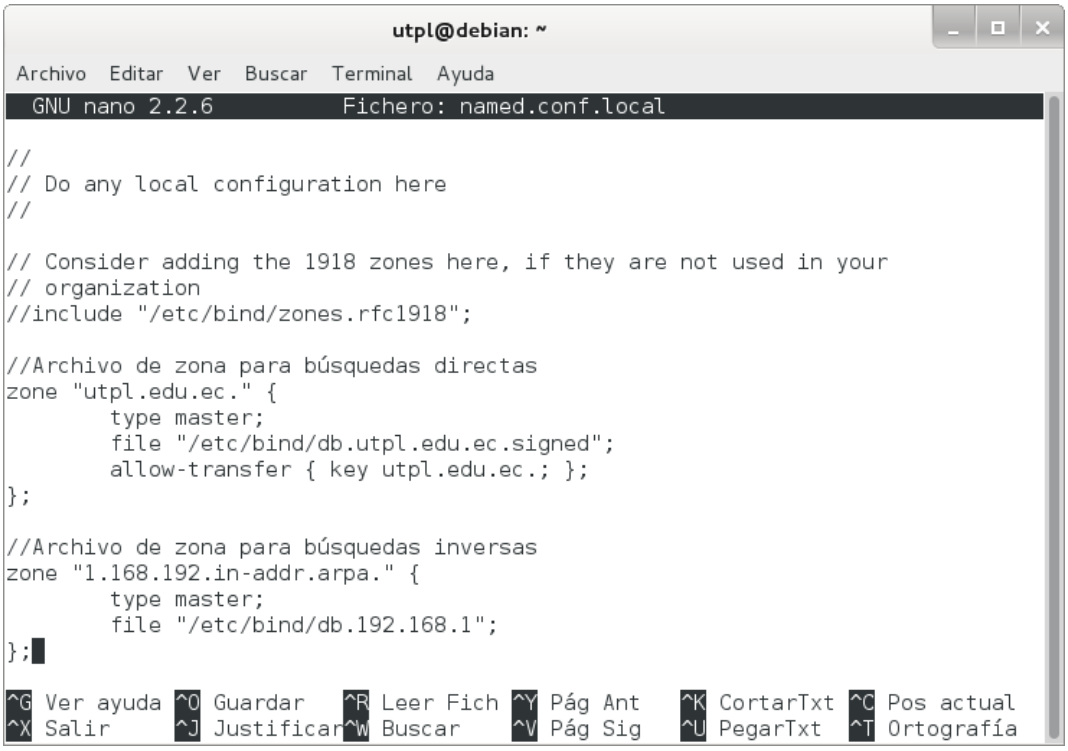

Figura 232. Restricción de la transferencia.

2. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 233.

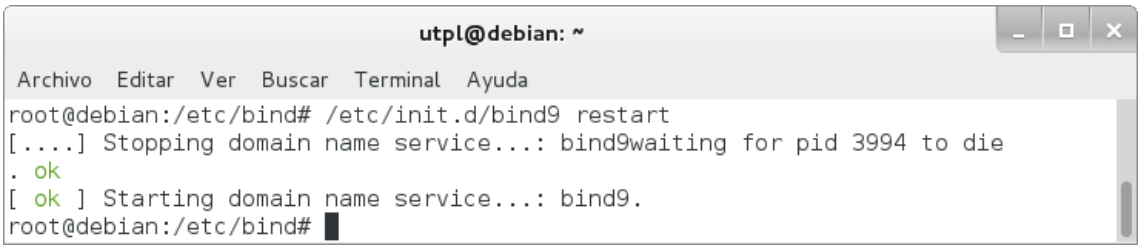

Figura 233. Reinicio del servicio.

4. Realizar pruebas.

Para esto se realizó lo siguiente:

1. Emplear el comando dig:

 # dig @localhost -k Kutpl.edu.ec.+157+09102.key utpl.edu.ec AXFR

Con lo que el resultado de la clave TSIG para la zona utpl.edu.ec configurada correctamente quedaría como se muestra en la figura 234.

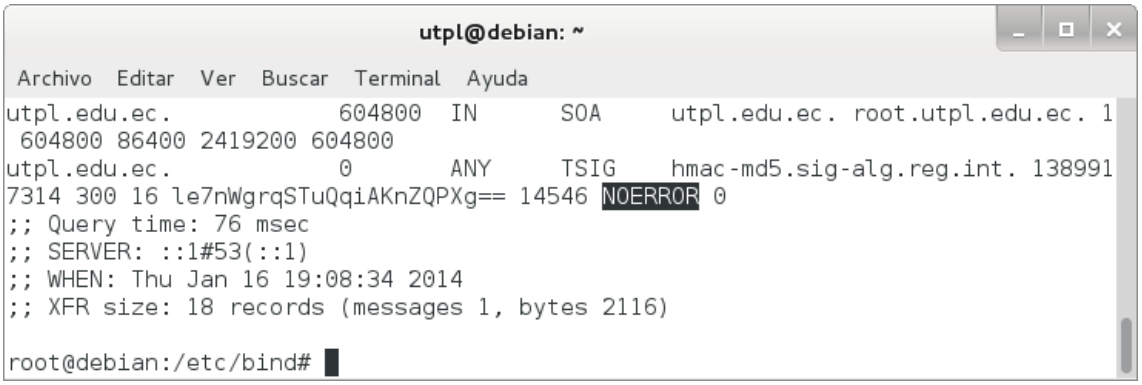

Figura 234. Ejecución correcta de dig.

2. Revisar el log del sistema:

 # tail -f /var/log/syslog

Donde el resultado del log muestra la transferencia exitosa como se indica en la figura 235.

```
client ::1#53376: transfer of 'utpl.edu.ec/IN': AXFR started: TSIG utpl.edu.ec
client ::1#53376: transfer of 'utpl.edu.ec/IN': AXFR ended
```

Figura 235. Registro del sistema.

3. Emplear el comando dig desde el usuario:

 # dig utpl.edu.ec @192.168.1.40 AXFR

Lo que da como resultado una transferencia fallida como se manifiesta en la figura 236.

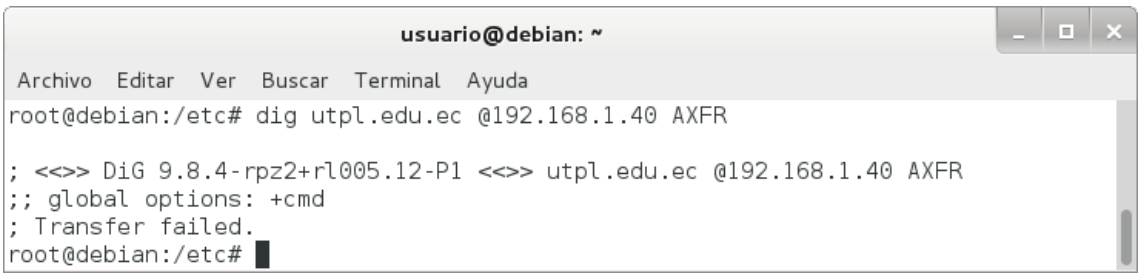

Figura 236. Transferencia fallida.

Anexo 26: Transferencia de zona de la comunidad virtual de aprendizaje de la Universidad Técnica Particular de Loja.

1. Generación de una clave TSIG.

Se creó un secreto compartido con dnssec-keygen que es la herramienta utilizada para generar un número aleatorio codificado en base64 que se utilizó como el secreto.

Para generar una clave TSIG se utilizó los argumentos que ofrece dnssec-keygen que son:

 # dnssec-keygen -a HMAC-MD5 -b 256 -n HOST cva.utpl.edu.ec.

Con lo que se creó una clave TSIG con el tipo de algoritmo HMAC-MD5, tamaño de la clave 256 y cva.utpl.edu.ec como el nombre de la zona, tal como se observa en la figura 237.

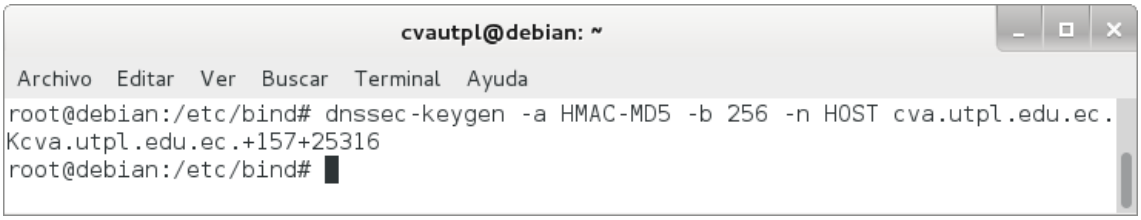

Figura 237. Clave TSIG.

El comando generó dos archivos como se muestra en las figuras 238 y 229.

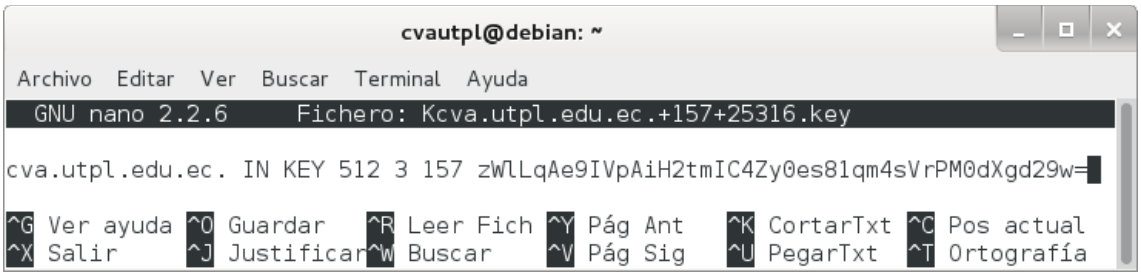

Figura 238. Archivo Kcva.utpl.edu.ec.+157+25316.key.

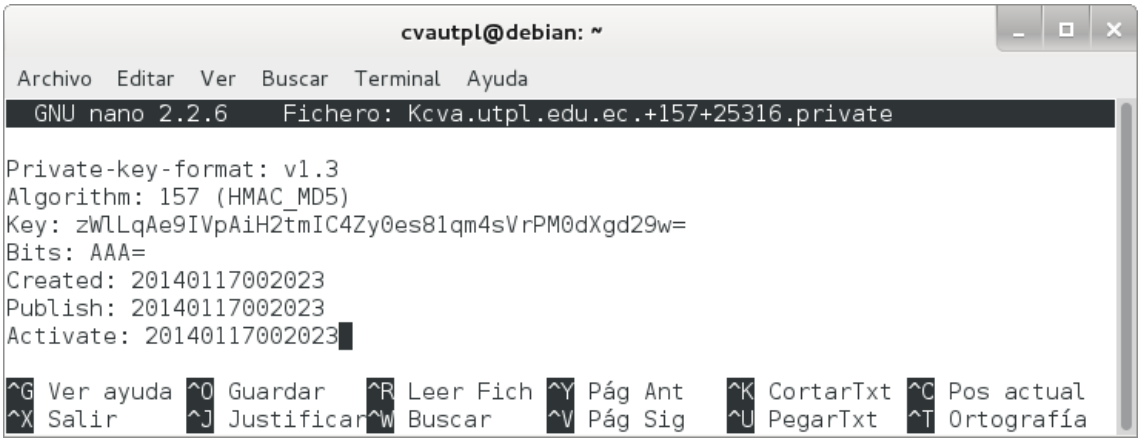

Figura 239. Archivo Kcva.utpl.edu.ec.+157+25316.private.

El nombre de los archivos contiene información relevante:

Kdomain_name+algorithm_id+key_id.extension

El domain_name es el nombre especificado como el nombre de la clave. El algorithm_id identifica el algoritmo utilizado: 5 para HMAC-MD5 (1 y 3 son para RSA y DSA, respectivamente). El key_id es un identificador para el material clave, no es de relevancia para las claves simétricas.La extension es cualquier key o private, la primera es la clave pública y la segunda es la clave privada [17].

2. Configurar las claves TSIG.

Para asegurar una transferencia de zona, el servidor primario y los administradores de los servidores secundarios tienen que configurar una clave TSIG en named.conf. La clave TSIG se compone de un secreto y un algoritmo de hash y son identificados por los nombres del dominio [17].

Los pasos para configurar las claves TSIG son:

1. Crear el archivo /etc/bind/tsig.keys:

   # nano /etc/bind/tsig.keys

Donde se especifica el algoritmo y el secreto de la zona como se ilustra en la figura 240.

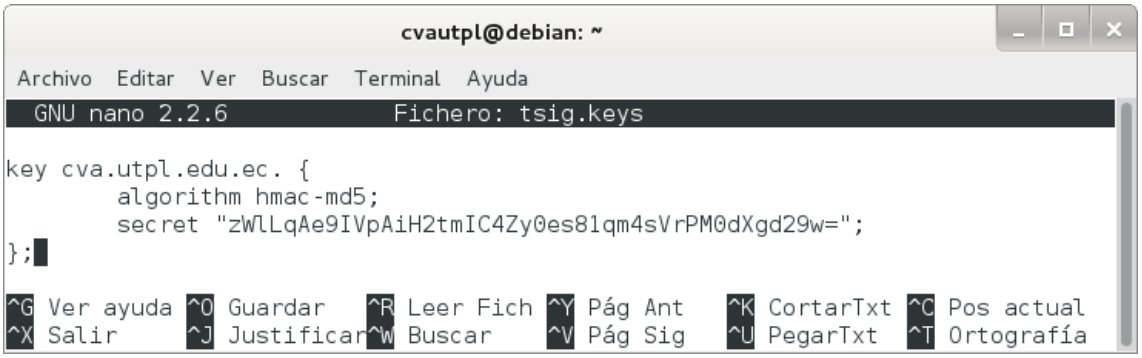

Figura 240. Archivo tsig.keys.

2. Incluir el archivo /etc/bind/tsig.keys en el archivo /etc/bind/named.conf:

include "/etc/bind/tsig.keys";

Observe la figura 241, donde se incluye el archivo /etc/bind/tsig.keys.

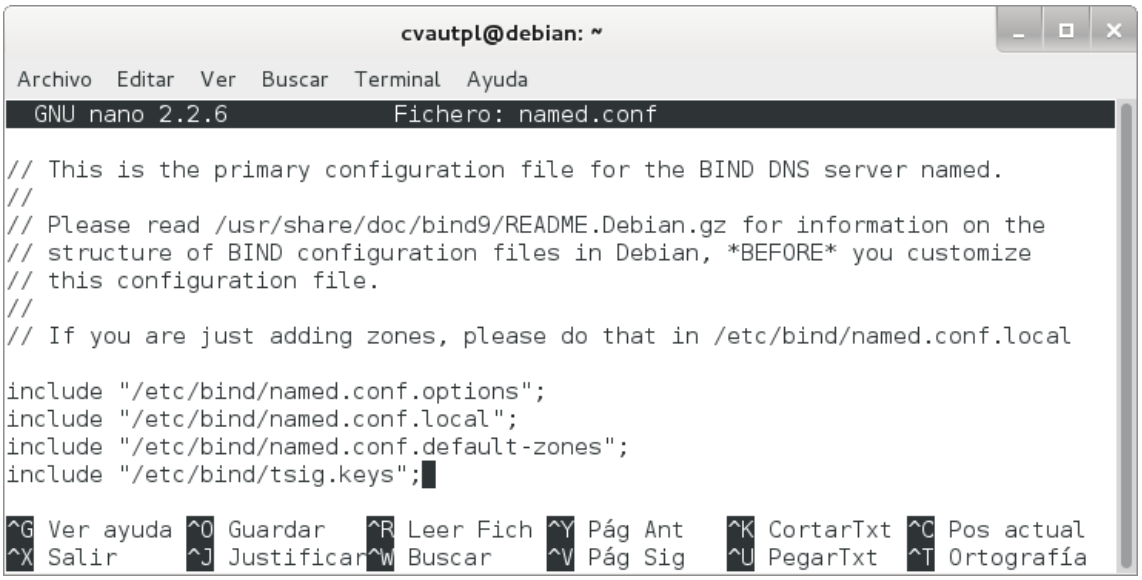

Figura 241. Inserción del archivo tsig.keys.

3. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 242.

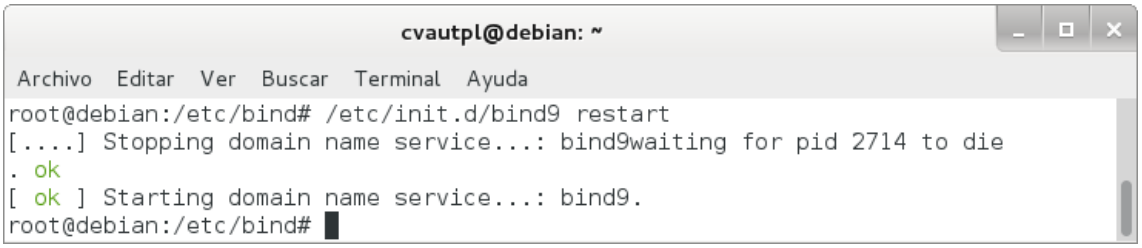

Figura 242. Reinicio del servicio.

3. Configurar el servidor primario de TSIG.

En el servidor de nombres primario, se puede restringir las transferencias de zona sólo a las firmadas con una clave específica.

El procedimiento para configurar el servidor primario fue:

1. Permitir la transferencia agregando el parámetro allow-transfer en el archivo /etc/bind/named.conf.local:

```
zone “cva.utpl.edu.ec” {
        type master;
         file “/etc/bind/db.cva.utpl.edu.ec.signed”;
         allow-transfer {  key cva.utpl.edu.ec. ; };
};
```

Donde se restringe las transferencias de zona a los firmados con la clave cva.utpl.edu.ec. como se muestra en la figura 243.

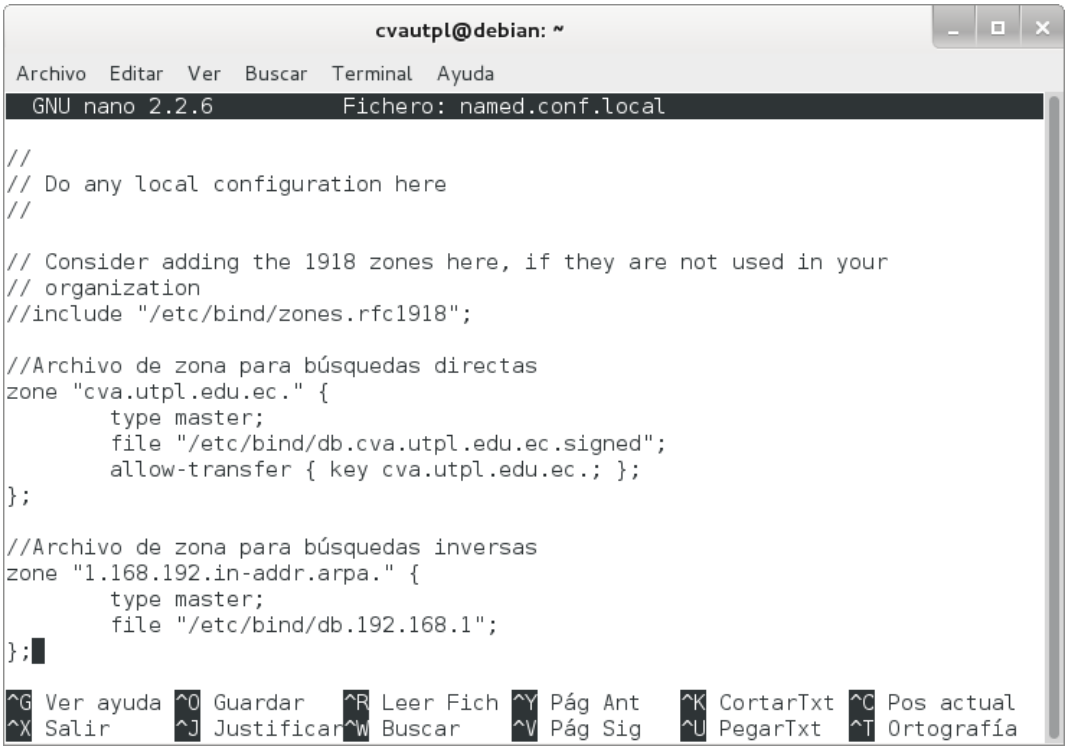

Figura 243. Restricción de la transferencia.

2. Reiniciar el servicio:

 # /etc/init.d/bind9 restart

Si todo se ha realizado bien, veremos que está OK, como se puede ver en la figura 244.

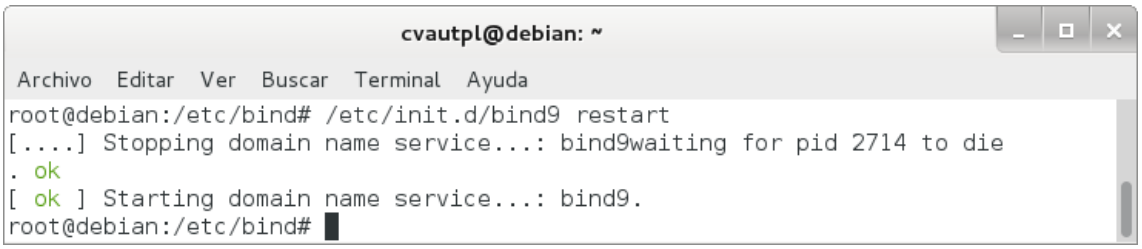

Figura 244. Reinicio del servicio.

4. Realizar pruebas.

Para esto se realizó lo siguiente:

1. Emplear el comando dig:

 # dig @localhost -k Kcva.utpl.edu.ec.+157+25316.key cva.utpl.edu.ec AXFR

Con lo que el resultado de la clave TSIG para la zona cva.utpl.edu.ec configurada correctamente quedaría como se muestra en la figura 245.

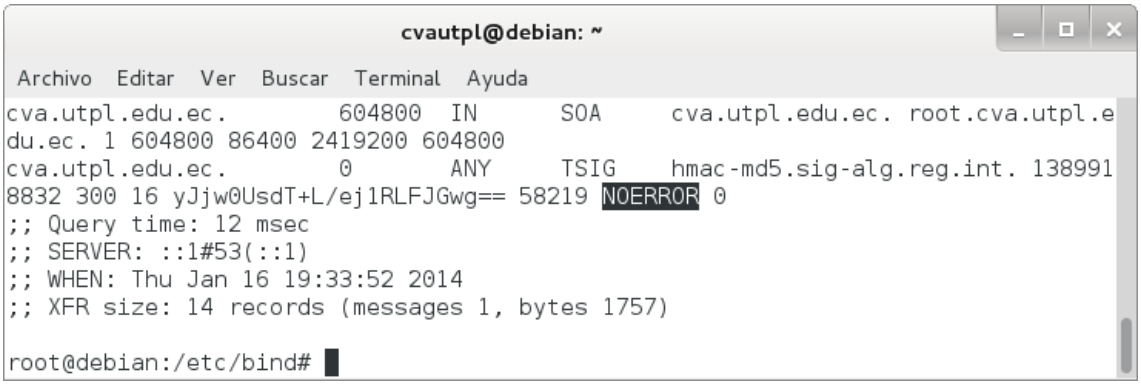

Figura 245. Ejecución correcta de dig.

2. Revisar el log del sistema:

 # tail -f /var/log/syslog

Donde el resultado del log muestra la transferencia exitosa como se indica en la figura 246.

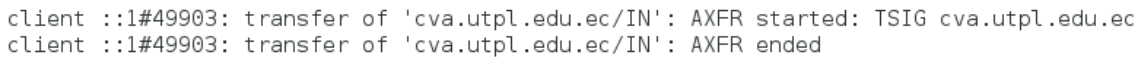

Figura 246. Registro del sistema.

3. Emplear el comando dig desde el usuario:

 # dig cva.utpl.edu.ec @192.168.1.45 AXFR

Lo que da como resultado una transferencia fallida como se manifiesta en la figura 247.

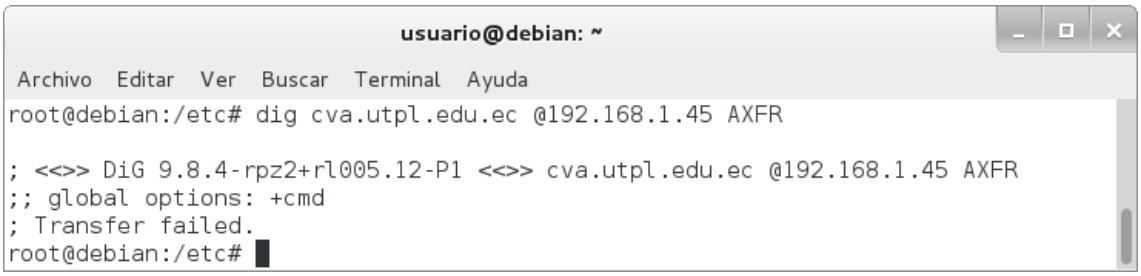

Figura 247. Transferencia fallida.

Anexo 27: Declaración de confidencialidad.

Gabriela Paulina Espinoza Ami (en adelante: la declarante), con C.I. 1105139453 DECLARA lo siguiente:

PRIMERO: Antecedentes

1. La declarante va a participar y ha participado en el trabajo de titulación "Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicadas en comunidades virtuales de aprendizaje de las instituciones de Educación Superior", dirigido por Ing. Luis Antonio Chamba Eras, en calidad de director de trabajo.

2. Por el presente documento se regula el tratamiento que la declarante ha de dar la información a la que pueda tener acceso en el desarrollo de las tareas de investigación que se realicen en dicho trabajo, el cual se regulará por las disposiciones contenidas en las cláusulas siguientes.

SEGUNDO: Información Confidencial

La información referida a materiales, métodos y resultados científicos, técnicos y comerciales utilizados u obtenidos durante la realización del trabajo de investigación o una vez realizado el mismo, se considerará siempre Información Confidencial.

TERCERO: Excepciones

No será considerada como Información Confidencial:

a) La información que la declarante pueda probar que tenía en su legítima posesión con anterioridad al conocimiento de la Información Confidencial.
b) La información que la declarante pueda probar que era de dominio público en la fecha de la divulgación o pase a serlo, con posterioridad, por haberse publicado o por otro medio, sin intervención ni negligencia de la declarante.
c) La información que la declarante pueda probar que corresponde en esencia a información facilitada por terceros, sin restricción alguna sobre su divulgación, en virtud de un derecho de la declarante a recibirla.

CUARTO: Secreto de la Información Confidencial

La declarante se compromete a mantener totalmente en secreto la Información Confidencial recibida en relación con el trabajo referido anteriormente y no divulgarla a terceros durante la vigencia de esta Declaración de Confidencialidad.

Asimismo, la declarante se compromete a emplear la Información Confidencial, exclusivamente, en el desempeño de las tareas que tenga encomendadas en dicho trabajo.

QUINTO: Duración

La obligación de la declarante respecto al mantenimiento del compromiso de secreto de la Información Confidencial, será indefinido para fines de investigación a partir de la fecha de la recepción de la Información Confidencial.

Loja, Abril 2014

Gabriela Paulina Espinoza Ami

Anexo 28: IX Congreso de Ciencia y Tecnología ESPE 2014.

La Universidad de las Fuerzas Armadas – ESPE consciente de su responsabilidad social y buscando impulsar iniciativas tendientes a promover el desarrollo integral de la Ciencia y Tecnología en el Ecuador, invita a todos los investigadores y estudiantes a participar en el IX Congreso de Ciencia y Tecnología ESPE 2014, que se llevará a cabo en el Campus Politécnico, los días 28, 29 y 30 de mayo de 2014. El evento incluye varias actividades, entre las que se destacan sesiones técnicas, paneles de discusión, minicursos y conferencias plenarias.

De igual forma, el Comité Editorial del Congreso ESPE 2014 tiene el honor de invitar a la comunidad científica nacional e internacional a presentar trabajos sobre investigación, desarrollo e innovación en las siguientes 6 áreas (no exclusivas ni totalmente restrictas):

Ciencias de la Computación

- Tecnologías de información y comunicación
- Seguridad informática
- Software aplicado

Eléctrica y Electrónica

- Telecomunicaciones
- Automatización y control
- Redes y comunicación de datos

Mecánica y Energía

- Materiales y producción
- Energías alternativas
- Mecatrónica

Ciencias de la Tierra y Construcción

- Estructuras
- Ciencias geoespaciales
- Ciencias ambientales

Ciencias de la Vida

- Biotecnologĺa
- Ciencias agropecuarias

Ciencias Económicas, Administrativas y Comercio

- Economía
- Administración
- Producción
- Mercadotecnia
- Auditoria
- Finanzas
- Comercio

Más información

Para obtener más información sobre el Congreso o el envío de artículos, por favor visite el sitio web: http://ciencia.espe.edu.ec.

Anexo 29: Convocatoria TICAL 2014.

Con el objetivo de aportar a los temas que comprometen el rol y la labor de los Directores de Tecnologías de Información y Comunicación (TIC) de las universidades de la región, desde inicios de 2011, la Red de Directores de Tecnologías de Información y Comunicación de las universidades latinoamericanas, ha ido construyendo un espacio de actuación que busca fortalecer el mejoramiento continuo de sus instituciones.

La Conferencia TICAL es el espacio donde confluye esta comunidad, que se nutre principalmente de las experiencias, iniciativas y conocimientos que exponen las mismas universidades, aportando soluciones significativas e inéditas en las instituciones de educación superior desde el área de las TIC, en todos los ámbitos del quehacer universitario.

Ejes Temáticos:

1. **Soluciones TIC para la Enseñanza y la Investigación** | Visualización científica, Herramientas para la simulación, Herramientas para la colaboración, Laboratorios de computación virtuales, Gestión y distribución de software especializado, soluciones TIC para la implementación de MOOC (Massive Open Online Courses); Desarrollos de soluciones en HPC (High Performance Computing), Tecnología de la sala de clases, Gestión del conocimiento (repositorios, revistas digitales, etc.), Soluciones integrales de videoconferencia, Redes sociales institucionales.
2. **Soluciones TIC para la Gestión** | Soluciones de trabajo colaborativo, Soluciones para gestión de proyectos, Soluciones que permitan la integración de procesos, Soluciones de Inteligencia de negocios* (Business Intelligence), Apoyo a los procesos de acreditación, Gestión documental y digitalización, Soluciones para la gestión basadas en nube, Soluciones de gestión para ser accedidas desde dispositivos móviles, Soluciones basadas en servicios de terceros.
3. **Gobernanza y Administración de las TIC** | Estructura organizacional del área TIC y RRHH, Políticas y buenas prácticas en la adquisición y retención de talentos, Presupuesto y Gestión de costos y servicios, Definición de la Estrategia TIC, Gestión de proyectos, Gestión de la innovación, Adaptabilidad al entorno, Gestión del conocimiento TIC, Gestión de procesos, Métricas, Gestión de los centros de datos, Sustentabilidad ecológica de IT en la gestión (Green IT).

4. **Infraestructura** | Ingeniería y gestión de Redes para soportar BYOD**, Redes inalámbricas (soluciones WiFi interno y externo), Infraestructura de PKI, Soluciones de Identidad (single sing-on y movilidad), Soluciones de Almacenamiento, Centros de datos, Nubes** públicas y/o privadas integradas a la infraestructura, Soluciones de VOIP, implementación de IPv6, Computación de Alto Rendimiento (HPC), Sustentabilidad ecológica de IT (Green IT).
5. **Seguridad de la información** | Soluciones para restringir accesos, implementación de normas Internacionales, Seguridad en la gestión y manejo de datos, Aspectos legales en la prestación de los servicios de la Universidad, Protección de la privacidad, calidad de servicios y gestión de seguridad de los proveedores; Seguridad en servicios de nubes, Aspectos relevantes a considerar en la incorporación de redes sociales, Planificación y gestión de la seguridad, Resguardo de la propiedad intelectual de la información digitalizada.

Más información

Para saber más sobre la Convocatoria TICAL 2014 por favor visite: http://tical2014.redclara.net/es/index.html.

Anexo 30: Anteproyecto.

ANTEPROYECTO-CIS

UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicadas en comunidades virtuales de aprendizaje de las instituciones de Educación Superior"

ANTEPROYECTO

Autora: Espinoza-Ami, Gabriela-Paulina

Director: Chamba-Eras, Luis-Antonio

LOJA-ECUADOR
2013

A. Tema

Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicadas en comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

B. Problemática

1. Situación Problemática

Internet es la red más grande del mundo, desde la perspectiva de un usuario, cada nodo o recurso en la red se identifica por un nombre único: el nombre de dominio. Para alcanzar un ordenador o cualquier otro recurso de una red, es necesaria alguna forma de indicar el destino, esto se consigue asignando direcciones de red. Desde la perspectiva de los dispositivos de red que solo encaminan paquetes a través de Internet, son solo transacciones de paquetes. Pero desde la perspectiva del usuario para acceder a los recursos de Internet, se utilizan los nombres de dominio, los usuarios necesitan un sistema que traduzca los nombres de dominio a direcciones IP y viceversa. Esta traducción es la tarea principal del Sistema de Nombres de Dominio (DNS) [1].

El DNS fue diseñado durante los primeros años de Internet y durante esta época todos los usuarios pertenecían al sector académico, organizaciones militares y entusiastas de la informática, en los cuales, en general, se podía confiar. Todo aquello implicó que la seguridad no fuese uno de los principales objetivos de diseño del sistema de nombres de dominio. Como consecuencia, existen vulnerabilidades en el sistema. La más importante vulnerabilidad se debe a que los servidores de nombres realizan consultas entre sí, sin un método seguro de verificación de los resultados obtenidos. Esto permite un tipo de ataque llamado “envenenamiento de caché” [2].

Las amenazas a una transacción DNS dependen del tipo de transacción, como son las consultas de resolución de nombres y respuestas, la zona de transferencia, la actualización dinámica y las transacciones de notificación DNS. Las consultas de resolución de nombres y respuestas entre los clientes DNS y los servidores DNS podría implicar cualquier nodo de Internet, por lo que las amenazas en su contra son mucho mayores en número y gravedad, dentro de las amenazas que se presentan en este tipo de transacción se encuentran la respuesta forzada o falsa, la eliminación de algunos RRs (Registros de Recursos) de la respuesta y las reglas de expansión incorrectas aplicadas al comodín RRs en un archivo de zona.

Debido a que la función subyacente es la mayor amenaza asociada con la consulta/respuesta de DNS en la integridad de los datos que el DNS devuelve en la respuesta, el objetivo de seguridad es para verificar la integridad de cada respuesta

recibida. Una parte integral de la verificación de la integridad es asegurar que los datos válidos se originó a partir de la fuente correcta. Establecer la confianza en la fuente se denomina autenticación del origen de datos, por lo tanto, los objetivos de seguridad que se requieren para asegurar la transacción de consulta/respuesta de DNS son la autenticación del origen de los datos y la verificación de integridad de los datos.

Estos servicios pueden ser prestados por el establecimiento de la confianza en la fuente y la verificación de la firma de los datos enviados por esa fuente, y es aquí donde la Corporación de Internet para la Asignación de Nombres y Números (ICANN) crea la norma DNSSEC (Extensiones de Seguridad del DNS) como el mecanismo de especificación de firma digital en el contexto de la infraestructura DNS [3].

DNSSEC fue diseñado para tratar el envenenamiento de caché y un conjunto de otras vulnerabilidades de DNS como los ataques del hombre y los datos de modificación en servidores autorizados. Su principal objetivo es proporcionar la capacidad de validar la autenticidad y la integridad de los mensajes DNS de tal manera que la manipulación de la información de DNS en cualquier parte del sistema DNS se puede detectar [4].

Esto se implementa mediante el uso de certificados digitales en la gestión de los dominios y subdominios. Cada registro DNS es firmado usando algoritmos criptográficos, con lo que las resoluciones a consultas pueden comprobar estas firmas y así verificar la autenticación de la información facilitada. El algoritmo criptográfico debe ser suficientemente fuerte para prevenir un ataque que intente falsear un registro de DNS [5].

A través de la introducción de DNSSEC en el entorno, no sólo se protege a los usuarios de los datos, sino que también ayuda en la construcción de un sistema mundial seguro que se puede utilizar para las relaciones de confianza bootstrap en otros protocolos [4].

Además, esta tecnología permite establecer una cadena de confianza en las comunidades virtuales de aprendizaje, para lo cual se considera fundamental que cada institución de Educación Superior implemente una de ellas, en donde se garantice la procedencia de contenidos creados en este tipo de ambientes de aprendizaje.

Es así que mediante este mecanismo de seguridad propuesto, se pretende realizar un estudio para la implementación de DNSSEC, como soporte al Sistema de Nombres de

Dominio (DNS) empleado en las instituciones de Educación Superior; con lo cual este proyecto permita resolver los siguientes problemas detectados, los mismos que se encuentran sustentados en [6 - 10]:

- El DNS no tiene formas seguras de garantizar la autenticidad de la información.
- El DNS no puede garantizar la integridad de la información.
- El DNS es una base de datos altamente distribuida, ya que no hay un ente centralizado a verificar y hay varios posibles puntos de falla.
- Existen muchos escenarios que se derivan del dominio de las instituciones de Educación Superior, los cuales pueden ser suplantados.
- Redirección del dominio completo de una institución de Educación Superior hacia otros dominios ajenos.
- Sacar de servicio a todo el dominio de una institución de Educación Superior.
- Falsificación completa de la página en línea de las instituciones de Educación Superior.

2. Problema de Investigación

¿La validación de la autenticidad y la integridad de los datos transferidos en las comunidades virtuales de aprendizaje de las instituciones de Educación Superior, se realizan de manera insegura a través del protocolo DNS?.

C. Justificación

Los profesionales de la carrera de Ingeniera en Sistemas están llamados a brindar soluciones a organizaciones de todo tipo que se presenten durante la vida profesional, desde pequeños negocios hasta grandes organizaciones multinacionales. Por lo tanto es importante trabajar en conjunto para que estas logren un desarrollo óptimo dentro de la sociedad competitiva en la que se encuentra actualmente.

El proyecto a desarrollarse abarca el empleo de conocimiento basado en Redes de Computadoras, con lo cual se pretende investigar sobre la seguridad aportada al Sistema de Nombres de Dominio de las instituciones de Educación Superior, así como a sus dependencias; que será de importancia debido a que permitirá resolver el problema existente en la validación de la autenticidad para las consultas DNS e integridad de los datos transferidos.

Con el nuevo modelo pedagógico implementado en la Educación Superior, es importante la investigación y el aporte que como futuros profesionales se puede dar a la sociedad, por lo que a través del presente proyecto, se pretende indagar sobre la tecnología DNSSEC como medio para establecer confianza y seguridad al DNS y a las comunidades virtuales de aprendizaje, las cuales desempeñan una labor importante al ser el medio que permite la interacción en red entre estudiantes y docentes, además de la movilidad con lo que se eliminan las limitaciones espacio-temporales; por lo que mediante la implementación de este mecanismo se permite que el usuario final se conecte al sitio web real que corresponde al nombre de dominio de las instituciones de Educación Superior. Además, se reforzará los conocimientos adquiridos durante la formación académica, los mismos que serán complementados con la investigación y práctica en el desarrollo de esta implementación.

Para la realización del presente proyecto es necesaria la utilización de equipos informáticos y herramientas tecnológicas para el estudio e implementación de DNSSEC, las cuales se harán uso a lo largo del proyecto y de acuerdo a las necesidades que se presenten.

La ejecución del proyecto no provoca ninguna alteración negativa para el medio ambiente, ya que dirige su atención hacia el estudio de la tecnología DNSSEC con el objeto de promover la implementación de seguridad para el DNS.

En cuanto al recurso económico, será adjudicado por la autora del proyecto debido a que esta investigación se considera de carácter formativo y que permitirá la obtención del título profesional.

En consecuencia, la realización del presente proyecto se justifica plenamente desde el punto de vista científico, académico, técnico-tecnológico, ambiental y económico.

D. Objetivos

1. Objetivo General

Realizar un estudio de las Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicado en comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

2. Objetivos Específicos

- Analizar el estado del arte del Sistema de Nombres de Dominio de las instituciones de Educación Superior, para determinar los requerimientos de implementación de DNSSEC.

- Proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

- Asegurar la comunicación entre servidores de las instituciones de Educación Superior.

E. Alcance

En el presente proyecto se determinó un tiempo de desarrollo de diez meses, durante el cual se pretende dar cumplimiento a los objetivos planteados anteriormente, mediante los cuales se aumentará las capacidades del DNS de las instituciones de Educación Superior, proporcionando formas de permitir a los consumidores de información DNS la verificación de que la información que les está llegando es la que la fuente original de esa información publicó. Para lo cual se plantean tres fases en base a los objetivos, cada una con sus respectivas actividades y tareas:

Fase 1: Analizar el estado del arte del Sistema de Nombres de Dominio de las instituciones de Educación Superior, para determinar los requerimientos de implementación de DNSSEC.

1. Búsqueda bibliográfica sobre casos de éxito de DNSSEC en instituciones de Educación Superior.
    1.1. Recogida de información a nivel internacional.
    1.2. Recogida de información a nivel nacional.
        1.2.1. Recogida de información sobre TELCONET S.A.
    1.3. Recogida de información a nivel local.
        1.3.1. Recogida de información en la Universidad Nacional de Loja.
            1.3.1.1. Entrevistar al encargado del centro de cómputo.
            1.3.1.2. Analizar la administración del servicio DNS.
            1.3.1.3. Elaborar una lista con las principales vulnerabilidades del servicio DNS.
        1.3.2. Recogida de información en la Universidad Técnica Particular de Loja.
            1.3.2.1. Entrevistar al encargado del centro de cómputo.
            1.3.2.2. Analizar la administración del servicio DNS.
            1.3.2.3. Elaborar una lista con las principales vulnerabilidades del servicio DNS.

Fase 2: Proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

1. Configuración de un servidor de nombres recursivo para validar las respuestas.
    1.1. Configuración del promotor de almacenamiento en caché.
        1.1.1. Configurar un ancla de confianza.

1.1.2. Realizar pruebas.

1.2. Realización de la validación lookaside.

1.2.1. Configuración de la validación lookaside.

1.2.1.1. Configurar una ancla de confianza para el Registro DLV.

1.2.1.2. Configurar la forma de las anclas del espacio de nombre DNS en el espacio de nombres DLV.

1.2.1.3. Realizar pruebas.

2. Aseguramiento de una zona DNS.

2.1. Configurar servidores con autoridad.

2.2. Crear pares de claves.

2.3. Firmar la zona.

2.4. Configurar caching forwarder.

3. Delegación de la firma de autoridad.

3.1. Inscribir en un registro DLV.

Fase 3: Asegurar la comunicación entre servidores de las instituciones de Educación Superior.

1. Aseguramiento de las transferencias de zona.

1.1. Generación de una clave TSIG.

1.1.1. Generar un secreto TSIG con dnssec-keygen.

1.2. Configurar las claves TSIG.

1.3. Configurar los servidores primarios de TSIG.

1.4. Configurar los servidores secundarios de TSIG.

1.5. Asegurar el mensaje de notificación.

1.6. Configurar la solución de problemas TSIG.

1.7. Realizar pruebas.

F. Metodología

Para desarrollar el presente trabajo de titulación, se ha realizado una serie de pasos sucesivos y ordenados llegando a la aplicación de métodos respectivos siendo esta la base principal para establecer el tema a investigar, establecer objetivos, estructurar el marco teórico, plantear soluciones al problema trazado, además de poner en práctica los conocimientos obtenidos durante la formación académica, para lo cual se hizo uso de los siguientes métodos y técnicas de investigación científica:

Con el **método deductivo** se determinó el tema a investigar en base a todo lo referente teórico, puesto que dicho método parte de un marco general de referencia que en este caso son los conocimientos generales e información recopilada, para determinar un caso en particular como lo es el estudio de las Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicado en comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

Con el **método inductivo**, que es el razonamiento que partiendo de casos particulares, se eleva a conocimientos generales; se lo utilizó para estructurar el marco teórico, buscando información relacionada con el tema en material bibliográfico.

Con el **método científico** se obtuvo, analizó y sintetizó los conceptos teóricos de la temática y a su vez la creación del estado del arte que da fundamento teórico al proceso investigativo.

Además de los métodos antes mencionados se pondrá en práctica una **metodología de resolución de problemas** que permitirá develar qué hacer con el problema planteado, de forma tal de asegurar calidad y realización, la misma que se centra en tres objetivos: la comprensión del problema, la creación de una estrategia de resolución o intervención y el logro del mejoramiento o la solución al problema.

Para ello, la metodología se organiza en siete etapas descritas a continuación; pero, si bien estas se presentan en forma sucesiva, en los hechos se desarrollan en formas no lineales, es decir, avanzando y algunas veces retrocediendo sobre la etapa anterior para ganar claridad y decisión [38].

Etapa 1: Identificar el problema.

La identificación de la situación problemática es la primera etapa que se ocupa de estudiar las manifestaciones visibles del problema, conocerlo a través de indicadores y

registros, delimitar el área y población de influencia, y compararlo con la situación existente en otros escenarios [38].

Esta etapa se la realizó con anterioridad, dando como resultado el problema de investigación, el mismo que se refiere a la comprobación de la seguridad en el protocolo DNS en cuanto a la validación de la autenticidad y la integridad de los datos transferidos en las comunidades virtuales de aprendizaje de las instituciones de Educación Superior.

Etapa 2: Explicar el problema.

Explicar el problema supone identificar todos los factores potenciales que pueden causar el problema, formular un modelo explicativo para la intervención y seleccionar las causas más relevantes [38].

Durante esta etapa se indagará sobre el estado del arte del Sistema de Nombres de Dominio de las instituciones de Educación Superior, partiendo de la recogida de información tanto a nivel internacional, nacional y local, de forma específica en la Universidad Nacional de Loja y Universidad Técnica Particular de Loja; con el propósito de determinar las principales vulnerabilidades del DNS, lo que permitirá avanzar en un consenso más firme y extendido sobre la naturaleza del problema.

Etapa 3: Idear las estrategias alternativas de intervención.

En esta fase se pretende lograr una diversidad de ideas de acciones, de procedimientos, roles, proyectos, equipamientos, apoyaturas, que puedan contribuir al mejoramiento de la situación actual y que a la vez permitan avanzar hacia la situación propuesta como ideal [38].

Es por ello que durante esta etapa se propondrá las soluciones en cuanto a la manera de proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje y la forma adecuada de asegurar la comunicación entre servidores de las instituciones de Educación Superior, con lo cual se obtendrá las opciones factibles de aplicación.

Etapa 4: Decidir la estrategia.

La cuarta etapa en esta metodología de resolución de problemas tiene por objetivo decidir cuál es la estrategia más efectiva para lograr el mejoramiento de la situación

actual, la cual relaciona el problema a resolver, es decir, que parte del reconocimiento de las mayores debilidades del sistema o de la situación y que, apoyándose en las fortalezas, reconoce ese “punto crucial” que posibilitaría una profunda transformación y acrecentaría la capacidad institucional de lograr sus propósitos [38].

Partiendo de las estrategias abordadas en la etapa anterior, esta fase permitirá afirmar que una solución es mejor que las restantes de acuerdo al escenario de aplicación, con lo que se logrará aportar seguridad en la autenticación y procedencia de datos en las comunidades virtuales de aprendizaje transferidos por el protocolo DNS.

Etapa 5: Diseñar la intervención.

El diseño de la intervención es la programación cuidadosa y minuciosa de todas las acciones, roles, recursos, decisiones auxiliares, plazos, instrumentos, métodos y asesoramientos necesarios para llevar adelante el proceso de mejoramiento [38].

En esta etapa se establecerá las acciones, plazos y recursos, para lo cual se tomarán decisiones en relación con las actividades, relativas a los tiempos y en relación con los recursos; las mismas que se llevarán a cabo en base al cronograma establecido, en donde se han especificado una serie de actividades y tareas que harán posibles las acciones respectivas, las cuales son de previsión y de anticipación que asegurarán realmente los mejoramientos y cambios previstos.

Etapa 6: Desarrollar la intervención.

El desarrollo de la intervención es entendido como la implementación, para lo cual es necesario poner en marcha el programa y monitorear y regular el desarrollo de la intervención [38].

Es así que durante esta fase se procederá a realizar las configuraciones y validaciones necesarias para la protección de los datos DNS que se transfieren en las comunidades virtuales de aprendizaje y el aseguramiento de la comunicación entre servidores de las instituciones de Educación Superior, tomando en consideración posibles decisiones que se presenten a lo largo del desarrollo, las cuales fomentarán un mejor resultado.

Etapa 7: Evaluar los logros.

La última etapa en la metodología de resolución de problemas está marcada por la evaluación del logro, del cambio de comportamiento organizacional y del mejoramiento

de la calidad registrados, para lo cual se debe diseñar los objetivos de la evaluación y decidir la estrategia de investigación-evaluación y desarrollar el trabajo de recopilación y análisis [38].

Finalmente en esta etapa se analizará los resultados obtenidos durante el proceso de implementación, con lo que se determinará la eficiencia de los beneficios aportados por la tecnología DNSSEC en las comunidades virtuales de aprendizaje de las instituciones de Educación Superior, además se verificará el cumplimiento de los objetivos planteados en el presente proyecto y se elaborarán las conclusiones producto de la investigación realizada.

G. Cronograma

	Nombre	Inicio	Fin
1	**Fase 1: Análisis del estado del arte del DNS.**	**28/10/2013**	**15/11/2013**
2	**Búsqueda bibliográfica sobre casos de éxito de DNSSEC en i**	**28/10/2013**	**14/11/2013**
3	Recogida de información a nivel internacional.	28/10/2013	29/10/2013
4	**Recogida de información a nivel nacional.**	**30/10/2013**	**31/10/2013**
5	Recogida de información sobre TELCONET S.A.	30/10/2013	31/10/2013
6	**Recogida de información a nivel local.**	**01/11/2013**	**14/11/2013**
7	**Recogida de información en la Universidad Nacional d**	**01/11/2013**	**07/11/2013**
8	Entrevistar al encargado del centro de cómputo.	01/11/2013	01/11/2013
9	Analizar la administración del servicio DNS.	04/11/2013	05/11/2013
10	Elaborar una lista con las principales vulnerabilidad	06/11/2013	07/11/2013
11	**Recogida de información en la Universidad Técnica Pa**	**08/11/2013**	**14/11/2013**
12	Entrevistar al encargado del centro de cómputo.	08/11/2013	08/11/2013
13	Analizar la administración del servicio DNS.	11/11/2013	12/11/2013
14	Elaborar una lista con las principales vulnerabilidad	13/11/2013	14/11/2013
15	Presentación del avance del PFC.	15/11/2013	15/11/2013
16	Análisis del estado del arte del DNS terminado.	15/11/2013	15/11/2013
17	**Fase 2: Protección de los datos DNS.**	**18/11/2013**	**20/03/2014**
18	**Configuración de un servidor de nombres recursivo para vali**	**18/11/2013**	**31/12/2013**
19	**Configuración del promotor de almacenamiento en caché**	**18/11/2013**	**29/11/2013**
20	Configurar una ancla de confianza.	18/11/2013	27/11/2013
21	Realizar pruebas.	28/11/2013	29/11/2013
22	**Realización de la validación lookaside.**	**02/12/2013**	**31/12/2013**
23	**Configuración de la validación lookaside.**	**02/12/2013**	**31/12/2013**
24	Configurar una ancla de confianza para el Registro [	02/12/2013	12/12/2013
25	Configurar la forma de las anclas del espacio de no	13/12/2013	25/12/2013
26	Realizar pruebas.	26/12/2013	31/12/2013
27	Presentación del avance del PFC.	01/01/2014	01/01/2014

Figura 1. Cronograma de actividades.

28	**⊟Aseguramiento de una zona DNS.**	**02/01/2014**	**26/02/2014**
29	Configurar servidores con autoridad.	02/01/2014	20/01/2014
30	Crear pares de claves.	21/01/2014	31/01/2014
31	Firmar la zona.	03/02/2014	13/02/2014
32	Configurar caching forwarder.	14/02/2014	26/02/2014
33	**⊟Delegación de la firma de autoridad.**	**27/02/2014**	**19/03/2014**
34	Inscribir en un registro DLV.	27/02/2014	19/03/2014
35	Presentación del avance del PFC.	20/03/2014	20/03/2014
36	Protección de los datos DNS terminada.	20/03/2014	20/03/2014
37	**⊟Fase 3: Aseguramiento de la comunicación entre servidores.**	**21/03/2014**	**21/08/2014**
38	**⊟Aseguramiento de las transferencias de zona.**	**21/03/2014**	**20/08/2014**
39	**⊟Generación de una clave TSIG.**	**21/03/2014**	**15/04/2014**
40	Generar un secreto TSIG con dnssec-keygen.	21/03/2014	15/04/2014
41	Configurar las claves TSIG.	16/04/2014	13/05/2014
42	Configurar los servidores primarios de TSIG.	14/05/2014	04/06/2014
43	Configurar los servidores secundarios de TSIG.	05/06/2014	26/06/2014
44	Asegurar el mensaje de notificación.	27/06/2014	22/07/2014
45	Configurar la solución de problemas TSIG.	23/07/2014	15/08/2014
46	Realizar pruebas.	18/08/2014	20/08/2014
47	Presentación del avance del PFC.	21/08/2014	21/08/2014
48	Aseguramiento de la comunicación entre servidores terminado	21/08/2014	21/08/2014
49	Realización del informe final del PFC.	22/08/2014	28/08/2014
50	Sustentación del PFC.	29/08/2014	29/08/2014
51	Culminación del PFC.	29/08/2014	29/08/2014

Figura 2. Cronograma de actividades (continuación).

H. Presupuesto y Financiamiento

El desarrollo del presente proyecto implica una inversión económica, puesto que exige aseguramientos y recursos que se dedicarán, en la medida que se requieran, para alcanzar los objetivos plasmados, los cuales se materializarán a través de acciones basadas en un plan lógico, el cual corresponde con los costos estimados del presupuesto, cuyo diseño contempla diez meses que durará la investigación.

1. Talento humano.

La estimación presupuestaria para el coste del talento humano, dentro del periodo estipulado en el cronograma, se detalla en la tabla 1.

Equipo de trabajo	Horas	Precio/hora	Valor total
Gabriela Espinoza	1600	5,00	8.000,00
Director	24	15,00	360,00
SUBTOTAL			**8.360,00**

Tabla 1. Coste de talento humano.

En la que se ha establecido un monto de $8.360,00 dólares para el coste de talento humano, el cual se encuentra dividido en $8.000,00 dólares producto de 1.600 horas de trabajo a $5,00 dólares cada hora para la autora del proyecto, y $360,00 dólares producto de 24 horas de trabajo a $15,00 dólares cada hora para el director del proyecto.

2. Bienes.

La estimación presupuestaria para el coste de bienes, dentro del periodo estipulado en el cronograma, se detalla en la tabla 2.

Descripción	Cantidad	Depreciación		Valor Unitario	Valor Total
		V. Real	T. util/mes		
Hardware					
Portátil Dell Core i5	1	999,00	5	25,60	128,00
Servidor Clon 1	1	800,00	5	20,50	102,50
Servidor Clon 2	1	800,00	5	20,50	102,50
Impresora	1	60,00	5	2,50	12,50
Subtotal					**345,50**
Software					
Sistema Operativo Ubuntu	2				0,00
Sistema Operativo Windows 7	1				149,00
Texmaker	1				0,00
Gantter Project	1				0,00
Subtotal					**149,00**
Material de oficina					
Resma de papel	1			4,50	4,50
Copias	60			0,02	1,20
Perfil	3			0,70	2,10
Subtotal					**7,80**
SUBTOTAL					**502,30**

Tabla 2. Coste de bienes.

En la cual se ha establecido un monto de $502,30 dólares para el coste de bienes, el cual se encuentra dividido en $345,50 dólares para hardware, $149,00 dólares para software y $7,80 dólares para material de oficina.

3. Servicios.

La estimación presupuestaria para el coste de servicios, dentro del periodo estipulado en el cronograma, se detalla en la tabla 3.

Descripción	Horas	Valor Unitario	Valor Total
Internet	400	0,70	280,00
Llamadas telefónicas	20	0,20 x min	30,00
Bus	200	0,25	50,00
Taxi	20	1,00	30,00
SUBTOTAL			**390,00**

Tabla 3. Coste de servicios.

Donde se ha establecido un monto de $482,40 dólares para el coste de servicios, el cual se encuentra dividido en $280,00 dólares para internet, $2,40 dólares para llamadas telefónicas, $80,00 dólares para bus y $120,00 dólares para taxi.

4. Presupuesto general.

Por lo tanto los costes totales definitivos para el desarrollo del proyecto son los que se detallan en la tabla 4.

Descripción	Total
Talento humano	8.360,00
Bienes	502,30
Servicios	390,00
Subtotal	9.344,70
Imprevistos (10%)	934,47
Total	**10.279,17**

Tabla 4. Coste general.

Dando como resultado un monto total de $10.279,17 dólares, dividido en $8.360,00 dólares del coste de talento humano, $502.30 dólares del coste de bienes, $482,40 dólares del coste de servicios y $934,47 dólares para gastos imprevistos.

I. Bibliografía

[1] P. Mockapetris. ***Domain names – concepts and facilities.*** Request for Comments 1034, Internet Engineering Task Force, Noviembre 1987. Obsoletos RFC 0973; Actualizado por RFC 1101. [En línea] link: http://tools.ietf.org/html/rfc1034. Consulta realizada 23-Jun-2013.

[2] DNSSEC. ***¿Por qué DNS es inseguro?.*** [En línea] link: http://www.dns-sec.es/index.php/inseguridad-en-dns/. Consulta realizada 23-Jun-2013.

[3] Ramaswamy Chandramouli, Scott Rose. ***Secure Domain Name System (DNS) Deployment Guide.*** Recommendations of the National Institute of Standards and Technology. [En línea] link: http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf. Consulta realizada 07-Jul-2013.

[4] Olaf Kolkman. ***DNSSEC HOWTO, a tutorial in disguise.*** [En línea] link: http://www.nlnetlabs.nl/publications/dnssec_howto/dnssec_howto.pdf. Consulta realizada 06-Ago-2013.

[5] R. Arends. ***DNS Security Introduction and Requirements.*** Request for Comments 4033, Internet Engineering Task Force, Marzo 2005. Obsoletos RFC 2535, 3008, 3090, 3445, 3655, 3658, 3755, 3757, 3845; Actualizado por RFC 1034, 1035, 2136, 2181, 2308, 3225, 3007, 3597, 3226. [En línea] link: http://tools.ietf.org/html/rfc4033. Consulta realizada 06-Ago-2013.

[6] Steve Friedl. ***An Illustrated Guide to the Kaminsky DNS Vulnerability***. [En línea] link: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html. Consulta realizada 06-Ago-2013.

[7] Tomás Barros. ***Extensiones de Seguridad para DNS.*** OpenNIC 2008, NicLabs. [En línea] link: http://www.nic.cl/OpenNIC/ponencias/tbarros-dnssec.pdf. Consulta realizada 06-Ago-2013.

[8] Miguel Ángel Hernández Vallejos. ***Riesgos en el sistema de DNS.*** Revista SIC (Seguridad en Informática y Comunicaciones), Febrero 2006, Nº 68. [En línea] link: http://www.geocities.ws/lowis00/hwct/foros/local/pag15.pdf. Consulta realizada 23-Ago-2013.

[9] D. Atkins. ***Threat Analysis of the Domain Name System (DNS)***. Request for Comments 3833, Internet Engineering Task Force, Agosto 2004. [En línea] link: http://tools.ietf.org/html/rfc3833. Consulta realizada 26-Ago-2013.

[10] Jhon Francined Herrera C. ***Las vulnerabilidades de seguridad de DNS.*** Revista Inventum, No. 6, Facultad de Ingeniería Uniminuto, Junio de 2009, ISSN 1909 -

2520. [En línea] link: http://biblioteca.uniminuto.edu/ojs/index.php/Inventum/article/download/42/41. Consulta realizada 27-Ago-2013.

[11] Microsoft. ***Introducción a DNS.*** [En línea] link: http://technet.microsoft.com/es-es/library/cc730775.aspx. Consulta realizada 15-Ago-2013.

[12] Tanenbaum, A.S. ***Redes de computadoras.*** Editorial Alhambra S. A. (SP). 2003. [En línea] link: http://books.google.com.ec/books?id=WWD-4oF9hjEC. Consulta realizada 15-Ago-2013.

[13] Miguel Morillo Iruela. ***Infraestructura DNS.*** Universidad de Castilla-La Mancha. [En línea] link: http://www.dns-sec.es/index.php/sistema-de-nombres-de-dominio-dns/infraestructura-dns/. Consulta realizada 19-Ago-2013.

[14] Jesús Moreno León, Alberto Molina Coballes. ***DNS: Domain Name System.*** Consejería de Educación. [En línea] link: http://www.josedomingo.org/web/mod/resource/view.php. Consulta realizada 21-Ago-2013.

[15] Alfredo Barrainkua Zallo. ***DNS Domain Name Service.*** Instituto de Iurreta. [En línea] link: http://www1.iurreta-institutua.net/sarezerlinux/ServiciosRedLinux-DNS-v1.0-ES.pdf. Consulta realizada 21-Ago-2013.

[16] John Deivis Tabares Tobón, Luis Fernando Ramirez. ***DNS Domain Name System Sistema de Nombres de Dominio.*** Servicio Nacional de Aprendizaje. [En línea] link: http://redesjdeivis.files.wordpress.com/2011/10/servidor-dns-windows-server2.pdf. Consulta realizada 21-Ago-2013.

[17] George Coulouris, Jean Dollimore and Tim Kindberg. ***Distributed Systems: Concepts and Design.*** Segunda Edición. Editorial Addison Wesley, 1994. [En línea] link: http://www.cs.rutgers.edu/~pxk/417/notes/content/ms_dns.pdf. Consulta realizada 21-Ago-2013.

[18] Fernando Ferrer. ***Curso de Linux Básico.*** [En línea] link: http://fferrer.dsic.upv.es/files/2006/04/LinuxAvanzado.pdf. Consulta realizada 21-Ago-2013.

[19] Nicolás Madrid Gallego. ***DNS.*** Instituto de Educación Secundaria "Gregorio Prieto". [En línea] link: http://nikosri.files.wordpress.com/2011/12/nicolas-madrid-gallego-dns1.pdf. Consulta realizada 21-Ago-2013.

[20] Eduard Lara. ***Domain Name Server (DNS).*** Universidad Politécnica de Cataluña. [En línea] link: http://personals.ac.upc.edu/elara/documentacion/INTERNET%20-%20UD6%20-%20DNS.pdf. Consulta realizada 21-Ago-2013.

[21] Geoff Huston. ***DNSSEC - The Theory.*** Internet Society. The ISP Column. [En línea] link: http://www.cse.iitd.ernet.in/~siy117527/sil765/readings/dnssec.pdf. Consulta realizada 28-Ago-2013.

[22] R. Gieben. ***DNSSEC in NL.*** NLnet Labs. [En línea] link: http://www.nlnetlabs.nl/downloads/publications/dnssec/dnssecnl/secreg-report.pdf. Consulta realizada 28-Ago-2013.

[23] A10 Networks, Inc. ***Domain Name System Security Extensions (DNSSEC): Preparing the Network.*** [En línea] link: http://www.a10networks.com.cn/resources/files/WP_DNSSEC_98768755098.pdf. Consulta realizada 28-Ago-2013.

[24] R. Gieben. ***Chain of Trust.*** NLnet Labs. [En línea] link: http://www.nlnetlabs.nl/downloads/publications/CSI-report.pdf. Consulta realizada 30-Ago-2013.

[25] Miguel Morillo Iruela. ***DNSSEC (DNS Security Extensions).*** Universidad de Castilla-La Mancha. [En línea] link: http://www.dns-sec.es/wp-content/uploads/2010/12/DNSSEC_mmi.pdf. Consulta realizada 30-Ago-2013.

[26] Eric Amberg. ***Cadena de Confianza.*** Revista Linux Magazine, Nº 41. [En línea] link: http://www.linux-magazine.es/issue/41/058-064DNSSECLM41.pdf. Consulta realizada 30-Ago-2013.

[27] Paul Brand, Rick van Rein, Roland van Rijswijk, David Yoshikawa. ***Hardening the Internet. The impact and importance of DNSSEC.*** SURFnet. [En línea] link: http://www.surfnet.nl/Documents/rapport_200909_hardening_the_internet_DNSSSEC.pdf. Consulta realizada 01-Sep-2013.

[28] S. Weiler. ***DNSSEC Lookaside Validation (DLV).*** Request for Comments 5074, Internet Engineering Task Force, Noviembre 2007. [En línea] link: http://tools.ietf.org/html/rfc5074. Consulta realizada 01-Sep-2013.

[29] R. Arends. ***Resource Records for the DNS Security Extensions.*** Request for Comments 4034, Internet Engineering Task Force, Marzo 2005. Obsoletos RFC 2535, 3008, 3090, 3445, 3655, 3658, 3755, 3757, 3845; Actualizado por 1034, 1035, 2136, 2181, 2308, 3225, 3007, 3597, 3226. [En línea] link: http://tools.ietf.org/html/rfc4034. Consulta realizada 01-Sep-2013.

[30] R. Arends. ***Protocol Modifications for the DNS Security Extensions.*** Request for Comments 4035, Internet Engineering Task Force, Marzo 2005. Obsoletos RFC 2535, 3008, 3090, 3445, 3655, 3658, 3755, 3757, 3845; Actualizado por RFC

1034, 1035, 2136, 2181, 2308, 3225, 3007, 3597, 3226. [En línea] link: http://tools.ietf.org/html/rfc4035. Consulta realizada 01-Sep-2013.

[31] R. Elz. ***Clarifications to the DNS Specification.*** Request for Comments 2181, Internet Engineering Task Force, Julio 1997. Actualizado por RFC 1034, 1035, 1123. [En línea] link: http://tools.ietf.org/html/rfc2181. Consulta realizada 01-Sep-2013.

[32] J. Schlyter, Ed. ***DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format.*** Request for Comments 3845, Internet Engineering Task Force, Agosto 2004. Actualizado por RFC 3755, 2535. [En línea] link: http://tools.ietf.org/html/rfc3845. Consulta realizada 01-Sep-2013.

[33] M. Andrews. ***Negative Caching of DNS Queries (DNS NCACHE).*** Request for Comments 2308, Internet Engineering Task Force, Marzo 1998. Actualizado por RFC 1034, 1035. [En línea] link: http://tools.ietf.org/html/rfc2308. Consulta realizada 01-Sep-2013.

[34] DNSSEC Deployment. ***DNSSEC in Higher Education — 1% isn't enough***. [En línea] link: https://www.dnssec-deployment.org/index.php/2012/03/dnssec-in-higher-education-1-isnt-enough/. Consulta realizada 02-Sep-2013.

[35] Edilia Bautista Acosta, Rodolfo Sánchez reyes. ***Las comunidades virtuales de aprendizaje en la educación presencial como medio para fomentar el uso de las TIC en los estudiantes de nivel medio superior (Propuesta)***. [En línea] link: http://www.comie.org.mx/congreso/memoriaelectronica/v10/pdf/area_tematica_07/ponencias/1101-F.pdf. Consulta realizada 09-Oct-2013.

[36] .CO Internet S.A.S. ***Una introducción a DNSSEC***. [En línea] link: http://www.cointernet.com.co/sites/default/files/documents/DNSSEC_Informacion_Mar2012_ES.pdf. Consulta realizada 09-Oct-2013.

[37] Educause. ***Things you should know about DNSSEC.*** [En línea] link: http://net.educause.edu/ir/library/pdf/est1001.pdf. Consulta realizada 03-Sep-2013.

[38] Instituto Internacional de Planeamiento de la Educación (IIPE Buenos Aires). ***Resolución de problemas***. Ministerio de Educación de la Nación. Argentina. [En línea] link: http://187.174.84.106/siise/procap/ktml2/files/uploads/modulo07.pdf. Consulta realizada 10-Oct-2013.

Anexo 31: Licencia Creative Commons.