# Cadenas de confianza por medio de extensiones de seguridad del sistema de nombres de dominio aplicadas a comunidades virtuales de aprendizaje

Gabriela P. Espinoza Ami, Luis A. Chamba Eras
Carrera de Ingeniería en Sistemas
Universidad Nacional de Loja
Loja, Ecuador
{gpespinozaa, lachamba}@unl.edu.ec

Ana Arruarte, Jon Ander Elorriaga
Departamento de Lenguajes y Sistemas Informáticos
Universidad del País Vasco UPV/EHU
Donostia, España
{a.arruarte, jon.elorriaga}@ehu.es

***Resumen*—El presente artículo se basa en un estudio sobre las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) aplicado en comunidades virtuales de aprendizaje de las instituciones de educación superior, cuyo objetivo es validar la autenticidad y la integridad de los datos del Sistema de Nombres de Dominio (DNS) mediante cadenas de confianza. Durante este estudio se efectuó un análisis del estado del arte del DNS de las instituciones de educación superior a nivel internacional, nacional y local; luego se desarrolló una virtualización de los servidores DNS de 3 universidades, en los que se realizó las configuraciones necesarias para el funcionamiento de DNSSEC, mediante el proceso de firma de las zonas DNS por medio de claves públicas y privadas que establecen una cadena de confianza. Además, se configuró un servidor de nombres recursivo que almacena 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 se establecieron islas de confianza mediante los dominios firmados que a su vez crearon un archipiélago de confianza entre los mismos. Finalmente, se utilizó el complemento DNSSEC Validator en los navegadores web para validar que los dominios de las instituciones de educación superior estén asegurados con DNSSEC.**

***Palabras Clave*—DNSSEC; cadena de confianza; anclas de confianza; islas de confianza; archipiélagos de confianza; modelo de confianza.**

## I. 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].

Debido a que la mayor amenaza del DNS está asociada con la consulta/respuesta 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 originaron 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 del DNS son la autenticación del origen de los datos y la verificación de integridad de los datos.

DNSSEC fue diseñado para tratar el envenenamiento de caché y un conjunto de otras vulnerabilidades del 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 del DNS en cualquier parte del sistema DNS se puede detectar [2].

Esto se implementa mediante el uso de certicados 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 del DNS [3].

A traves de la introducción de DNSSEC en el entorno, no solo 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 [2].

### *A. DNSSEC en comunidades virtuales de aprendizaje.*

Las comunidades virtuales de aprendizaje proporcionan el ambiente idóneo para que el estudiante se inicie en la comunicación virtual con otros congéneres con los cuales comparte información [4], 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 cierto tipo 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 [5].

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 objetos de aprendizaje creados en este tipo de ambientes virtuales [6].

### *B. Consecuencias en la educación superior.*

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 altos. 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 [7].

Razones por las cuales se ha realizado un estudio para la implementación de DNSSEC, utilizando un ambiente virtualizado de los servidores DNS de tres universidades para realizar el aseguramiento de las zonas DNS, así como también un servidor de nombres recursivo que valida las respuestas efectuadas por los usuarios; además se emplea como herramienta de validación el plugin DNSSEC Validator que comprueba la existencia de DNSSEC en las zonas aseguradas.

El artículo ha sido estructurado de la siguiente manera: en la sección II se presenta el estado del arte de esta investigación, en la sección III se detalla la metodología utilizada para la implementación de DNSSEC, en la sección IV se presentan los resultados obtenidos, en la sección V se exponen las consecuencias del despliegue de DNSSEC y los beneficios del mismo, en la sección VI se abordan casos de éxito de la implementación de DNSSEC en instituciones de educación superior y en la sección VII se expone las deducciones de las experiencias obtenidas, así como los trabajos futuros a realizar.

## II. MARCO REFERENCIAL

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 [8].

### *A. 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 "." [9].

*B. 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 [5].

*C. 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 [10].

## III. MÉTODOS

Durante el desarrollo de esta investigación, se utilizó una metodología de resolución de problemas que se organiza en siete etapas descritas a continuación:

**Etapa 1: Identificar el problema:** en esta etapa se visualizó 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:** durante esta etapa se indagó el estado del arte del Sistema de Nombres de Dominio de las instituciones de educación superior, partiendo de la recolección de información tanto a nivel internacional (ver sección Resultados subsección A apartado 1), nacional (ver sección Resultados subsección A apartado 2) y local (ver sección Resultados subsección A apartado 3), 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 firme y extendido sobre la naturaleza del problema.

**Etapa 3: Idear las estrategias alternativas de intervención:** en esta etapa se propuso las soluciones en cuanto a la forma de proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de educación superior (ver sección Resultados subsección B y C), con lo cual se obtuvo las opciones factibles de aplicación.

**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 instituciones de educación superior (ver sección Resultados subsección A), proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje (ver sección Resultados subsección B), y validar el suncionamiento de DNSSEC (ver sección Resultados subsección C), 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.

**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 y la protección de los datos DNS de las comunidades virtuales de aprendizaje de las instituciones de educación superior.

**Etapa 6: Desarrollar la intervención:** durante esta fase se realizó la revisión del estado del arte del sistema DNS en las instituciones de educación superior (ver sección Resultados subsección A) y las configuraciones (ver sección Resultados subsección B) y validaciones (ver sección Resultados subsección C) necesarias para la protección de los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de educación superior.

**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 las instituciones de educación superior, que se presentan en el apartado de discusión.

## IV. RESULTADOS

*A. Análisis del estado del arte del Sistema de Nombres de Dominio de las instituciones de educación superior.*

*1) Recopilar información a nivel internacional:* de acuerdo a la iniciativa DNSSEC Deployment [1], entre las principales

instituciones de educación superior que han implementado DNSSEC, se encuentran:

- Universidad Berkeley de California (berkeley.edu)
- Universidad China de Hong Kong (cuhk.edu)
- Laboratorio de Física Aplicada de la Universidad Johns Hopkins (jhuapl.edu)
- Universidad de Missouri de Ciencia y Tecnología (mst.edu)
- Universidad de Oxford (oxford-university.edu)
- Universidad de Pensilvania (penn.edu, upenn.edu)
- Centro de Supercomputación de Pittsburgh (psc.edu)
- Corporación Universitaria para el Desarrollo de Internet Avanzado (ucaid.edu)
- Universidad Pompeu Fabra (upf.edu)
- Universidad de Valencia (valencia.edu)

En Portugal, conforme a la asociación DNSSEC .PT [11] 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.

Resaltando como casos de éxito a la Universidad de Pensilvania [12] y la Universidad Pompeu Fabra [13].

*2) Recopilar 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.

a) *Recopilar información en 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 [14]; 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.

*3) Recopilar información a nivel local:*

a) *Recopilar información en la Universidad Nacional de Loja:* en la Universidad Nacional de Loja no se ha realizado la implementación de la tecnología DNSSEC, mecanismo que resulta conveniente desarrollar, 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.

b) *Recopilar información en la Universidad Técnica Particular de Loja:* en la Universidad Técnica Particular de Loja no se ha efectuado el despliegue de la tecnología DNSSEC, procedimiento que surge beneficioso implementar, 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.

*B. Protección de los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de las instituciones de educación superior.*

*1) Instalación y configuración de los servidores DNS maestros:* la instalación de los servidores DNS se realizó en máquinas virtuales mediante la utilización del servidor DNS de código abierto BIND9 [15] y sus paquetes dependientes, lo cual se efectuó a través de la consola del sistema operativo Debian 7.

La instalación de los servidores DNS se efectuó de forma virtualizada 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 ya que estos proveedores aún no han desplegado DNSSEC en sus zonas, por lo que no podrían almacenar los registros DNSKEY de las universidades y de esta manera los usuarios que realicen una consulta DNS sobre estos dominios no tendrán la seguridad de que la información se encuentra autenticada.

Así mismo, se virtualizó los servidores DNS de la Escuela Superior Politécnica del Litoral, en el que no se configuró el aseguramiento de las zonas con DNSSEC y 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 las consultas a un servidor inseguro (espol.edu.ec, cva.espol.edu.ec).

Las configuraciones que se establecieron para los servidores de las universidades se observan en la Fig. 1, el detalle de las mismas se presentan a continuación:

- **Universidad Nacional de Loja**
  - Sitio web
    - Dirección IP del servidor: **192.168.1.30**
    - Nombre del servidor: **unl**
    - Dominio a crear: **unl.edu.ec**
  - Comunidad virtual de aprendizaje
    - Dirección IP del servidor: **192.168.1.35**
    - Nombre del servidor: **cvaunl**
    - Dominio a crear: **cva.unl.edu.ec**

- **Universidad Técnica Particular de Loja**
  - Sitio web
    - Dirección IP del servidor: **192.168.1.40**
    - Nombre del servidor: **utpl**
    - Dominio a crear: **utpl.edu.ec**
  - Comunidad virtual de aprendizaje
    - Dirección IP del servidor: **192.168.1.45**
    - Nombre del servidor: **cvautpl**
    - Dominio a crear: **cva.utpl.edu.ec**

- **Escuela Superior Politécnica del Litoral**
  - Sitio web
    - Dirección IP del servidor: **192.168.1.50**
    - Nombre del servidor: **espol**
    - Dominio a crear: **espol.edu.ec**
  - Comunidad virtual de aprendizaje
    - Dirección IP del servidor: **192.168.1.55**
    - Nombre del servidor: **cvaespol**
    - Dominio a crear: **cva.espol.edu.ec**

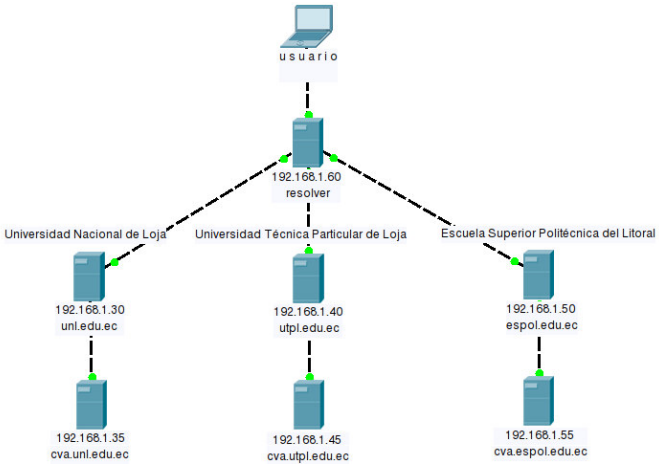


*Figura 1. Esquema DNS del experimento.*

Dentro de las configuraciones realizadas en los servidores se ejecutaron los siguientes pasos:

1) Instalar el servidor DNS Bind9:

*# apt-get install bind9*

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

*# nano /etc/resolv.conf*

3) Editar el archivo */etc/bind/named.conf.local* donde se asigna las zonas y el fichero en el que se encuentran:

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

4) Crear el archivo */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:

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

5) Crear el archivo */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:

*# nano /etc/bind/db.192.168.1*

6) Reiniciar el servicio:

*# /etc/init.d/bind9 restart*

*2) Aseguramiento de la zona DNS:* las zonas unl.edu.ec, cva.unl.edu.ec, utpl.edu.ec, cva.utpl.edu.ec han sido firmadas y su clave se ha configurado en un servidor de nombres recursivo validador, formándose una "isla" 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 Fig. 2.

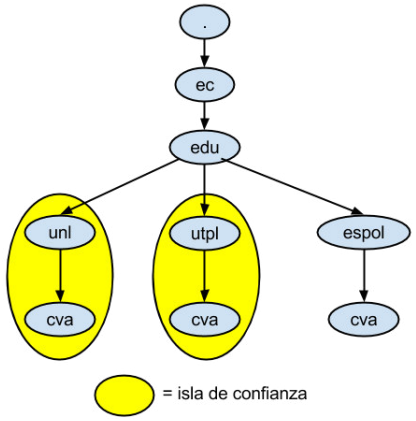


*Figura 2. Islas de confianza entre dominios.*

Para crear una "isla" de confianza se firmó las zonas y se distribuyó los "puntos de entrada seguros" al servidor de nombres recursivo [2]. 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 Fig. 3.

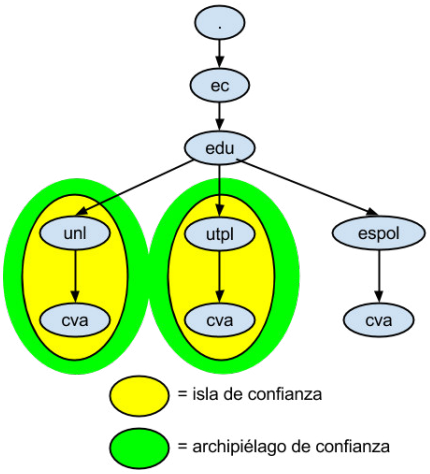


*Figura 3. Archipiélago de confianza.*

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.

Es así que el aseguramiento de las zonas DNS de las instituciones de educación superior se ilustra en la Fig. 4.

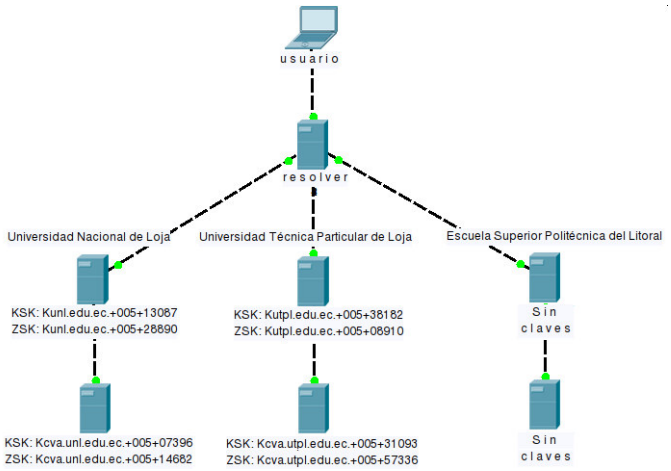


*Figura 4.Esquema del aseguramiento de las zonas DNS.*

Lo anteriormente mencionado se lo realizó llevando a cabo el siguiente procedimiento:

1) *Configurar servidor autoritativo:* el servidor autoritativo se configuró para soportar DNSSEC. Los pasos esenciales fueron:
   a) Habilitar DNSSEC en el archivo /etc/bind/-named.conf.options:
   *options* {
   *dnssec-enable yes;*
   *dnssec-validation auto;*
   *dnssec-lookaside auto;*
   };
   b) Reiniciar el servicio:
   *# /etc/init.d/bind9 restart*
2) *Crear pares de claves:* se creó una KSK (Key Signing Key) inicial y ZSK (Zone Signing Key) para cada zona para estar asegurado. Estas claves no tienen tiempo de expiración, y pueden ser usadas por el tiempo que se desee. Las partes privadas deben mantenerse en privado y seguras [16]. Los pasos para crear las claves fueron:
   a) Crear la KSK:
   *# dnssec-keygen -r /dev/random -f KSK -a RSASHA1 -b 1280 -n ZONE unl.edu.ec*
   b) Crear la ZSK:
   *# dnssec-keygen -r /dev/random -a RSASHA1 -b 1024 -n ZONE unl.edu.ec*
3) *Insertar las claves de la zona:* al crear pares de claves, estas se las incluyó en el archivo de zona. Para incluir las claves en la zona se hizo lo siguiente:
   a) 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*
4) *Firmar la zona:* una vez que las claves han sido incluidas en el archivo de zona, se prosigue a firmar la zona, para lo cual se utilizó la herramienta dnssec-signzone. Para firmar la zona se realizó lo siguiente:
   a) 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*
   b) 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";*
   *};*
   c) Reiniciar el servicio:
   *# /etc/init.d/bind9 restart*

*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 seguros y validados o inseguros. Como resultado, la información segura que no supere la validación, no va a encontrar su camino a los usuarios; ya que al 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 [2].

En el servidor de nombres recursivo se almacenó las claves KSK (claves públicas) de las zonas firmadas con DNSSEC como se observa en la Fig. 5, para de esta manera crear anclas de confianza.

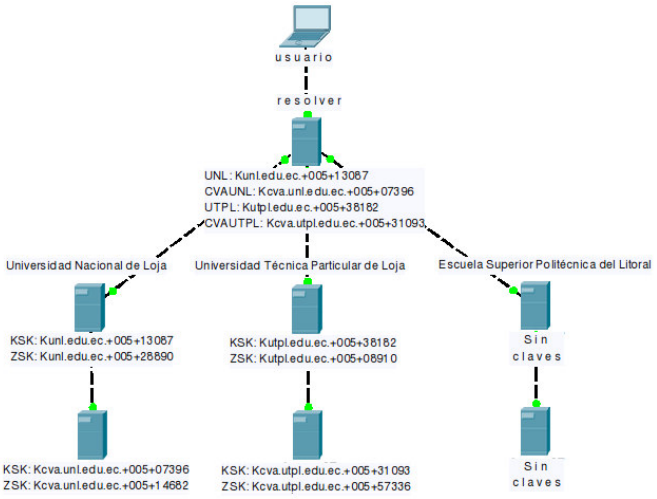


*Figura 5. Esquema del servidor de nombres recursivo con claves KSK.*

Lo anteriormente mencionado se lo realizó llevando a cabo el siguiente procedimiento:

1) *Configuración del promotor de almacenamiento en caché:* el promotor de almacenamiento en caché se configuró para soportar DNSSEC. Para instalar y configurar el servidor se siguieron los siguientes pasos:
   a) Instalar BIND 9 con OpenSSL:
      *# apt-get install bind9*
   b) Habilitar DNSSEC en el archivo /etc/bind/named.conf.options:
      *options {*
      *dnssec-enable yes;*
      *dnssec-validation auto;*
      *dnssec-lookaside auto;*
      *};*
   c) Reiniciar el servicio:
      *# /etc/init.d/bind9 restart*
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 [2]. Pero debido a que las zonas padres (ec., edu.ec.) aún no están firmadas se configuró múltiples anclas de confianza.
   a) Crear el archivo /etc/bind/named.conf.keys:
      *# nano /etc/bind/named.conf.keys*
   b) Incluir el archivo /etc/bind/named.conf.keys en el archivo /etc/bind/named.conf:
      *include "/etc/bind/named.conf.keys";*
   c) Modificar el archivo /etc/bind/named.conf.options:
      *# nano /etc/bind/named.conf.options*
   d) Reiniciar el servicio:
      *# /etc/init.d/bind9 restart*
3) *Configurar el registro:* es importante comprobar que la validación está funcionando correctamente, esto se hizo mediante el uso de las facilidades del registro de BIND en la máquina que está configurada como servidor de nombres recursivo validador. Para configurar el registro se realizó:
   a) Crear el archivo /var/log/dnssec.log:
      *# nano /var/log/dnssec.log*
   b) Crear el archivo /etc/bind/named.conf.logging:
      *# nano /etc/bind/named.conf.logging*
   c) Incluir el archivo /etc/bind/named.conf.logging en el archivo /etc/bind/named.conf:
      *include "/etc/bind/named.conf.logging";*
   d) Reiniciar el servicio:
      *# /etc/init.d/bind9 restart*

## C. Validación de DNSSEC.

*1) 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 [17]. Para la verificación de DNSSEC se instaló este plugin en el navegador web Mozilla Firefox.

a) *Servidores Universidad Nacional de Loja:* se comprobó que los dominios unl.edu.ec y cva.unl.edu.ec están asegurados mediante DNSSEC, como se muestra en las Fig. 6 y 7 respectivamente.


*Figura 6. Validación del dominio unl.edu.ec.*

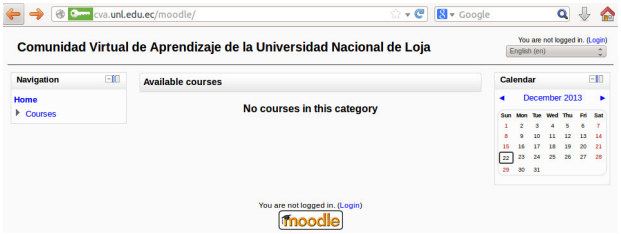


*Figura 7. Validación del dominio cva.unl.edu.ec.*

b) *Servidores Universidad Técnica Particular de Loja:* se verificó que los dominios utpl.edu.ec y cva.utpl.edu.ec están asegurados mediante DNSSEC, como se muestra en las Fig. 8 y 9 respectivamente.


*Figura 8. Validación del dominio utpl.edu.ec.*

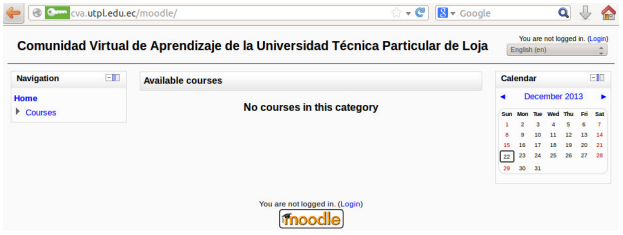


*Figura 9. Validación del dominio cva.utpl.edu.ec.*

c) *Servidores Escuela Superior Politécnica del Litoral:* se validó que los dominios espol.edu.ec y cva.espol.edu.ec no están asegurados mediante DNSSEC, como se muestra en las Fig. 10 y 11 respectivamente.


*Figura 10. Validación del dominio espol.edu.ec.*


*Figura 11. 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.

## V. DISCUSIÓN

De acuerdo a los experimentos realizados, es fundamental la implementación de DNSSEC en los dominios de las instituciones de educación superior porque de esta manera se fortalece la infraestructura de ambientes de aprendizaje, autenticando el origen de los datos y verificando su integridad, así mismo, se da protección contra los datos provenientes de DNS falsos usando criptografía de clave pública/privada para firmar digitalmente información del dominio; mediante lo cual la suplantación de identidad resulta más difícil y el envenenamiento de caché deja de ser una amenaza.

Mediante el proceso de firma digital, DNSSEC ofrece respuestas autenticadas a las consultas DNS recibidas, es decir que 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 y de esta forma verificar que los datos DNS no han sido alterados durante su transferencia.

La implementación de DNSSEC utilizando la virtualización de servidores DNS de instituciones de educación superior como: Universidad Nacional de Loja y Universidad Técnica Particular de Loja, ha permitido verificar el aseguramiento de los datos DNS que se transfieren en comunidades virtuales de aprendizaje de las mismas a nivel de laboratorio experimental; para ello se llevó a cabo el aseguramiento de las zonas DNS a través de la generación de pares de claves KSK y ZSK y la configuración de un servidor de nombres recursivo 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.

Al implementar DNSSEC se establecen islas de confianza conformadas por los dominios de la universidades y a su vez se crea un archipiélago de confianza entre ellas.

Como medio de validación, se utilizó el plugin DNSSEC Validator que se instaló en el navegador Mozilla Firefox que ha permitido verificar que los dominios de las instituciones de educación superior a nivel experimental están asegurados con DNSSEC.

## VI. TRABAJOS RELACIONADOS

### A. *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.

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.

”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” [12].

### *B. 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, 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.

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.

Una vez se implantó la nueva arquitectura, se implementó DNSSEC para los dominios upf.edu y upf.cat. 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.

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.

Con el plugin DNSSEC Validator instalado en Mozilla 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 [13].

## VII. CONCLUSIONES Y TRABAJOS FUTUROS

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.

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.

Como trabajos futuros se preveé implementar DNSSEC en las zonas DNS de los proveedores de servicios de internet y de las instituciones de educación superior, 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 planea realizar la implementación de DNSSEC 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.

## REFERENCIAS


[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 02-Sep-2013.

[2] Olaf Kolkman. *DNSSEC HOWTO, a tutorial in disguise*. [En línea] link: http://www.nlnetlabs.nl/publications/dnssec_howto/dnssec_howto.pdf. Consulta realizada 02-Sep-2013.

[3] 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 03-Sep-2013.

[4] 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.

[5] 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.

[6] .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.

[7] Educause. *Things you should know about DNSSEC*. [En línea] link: http://net.educause.edu/ir/library/pdf/est1001.pdf. Consulta realizada 03-Sep-2013.

[8] 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 05-Sep-2013.

[9] R. Gieben. Chain of Trust. NLnet Labs. [En línea] link: http://www.nlnetlabs.nl/downloads/publications/CSI-report.pdf. Consulta realizada 05-Sep-2013.

[10] 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 06-Sep-2013.

[11] 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-Oct-2013.

[12] 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-Oct-2013.

[13] 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-Oct-2013.

[14] APNIC. *Resolvers by as*. Laboratorios APNIC. [En línea] link: http://labs.apnic.net/dnssec/resolvers_by_as.txt. Consulta realizada 28-Oct-2013.

[15] 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 13-Nov-2013.

[16] Internet Systems Consortium. *DNSSEC Look-aside Validation Registry*. [En línea] link: https://dlv.isc.org/about/using. Consulta realizada 14-Nov-2013.

[17] Martin Straka, Karel Slaný, Ondřej Surý, Ondřej Filip.*DNSSEC Validator*. CZ.NIC. [En línea] link: https://www.dnssec-validator.cz/. Consulta realizada 22-Dic-2013.