

**UNIVERSIDAD MAYOR DE SAN ANDRÉS  
FACULTAD DE INGENIERÍA  
CARRERA DE INGENIERÍA ELECTRÓNICA**



**PROYECTO DE GRADO**

**SERVIDOR DNS ADMINISTRADO CON TECNOLOGÍA  
WEB BASADO EN SOFTWARE LIBRE – APLICACIÓN  
MINISTERIO DE ECONOMÍA Y FINANZAS PÚBLICAS**

**POR: HENRY GENARO CHAVEZ CONDE**

**TUTOR: MG. ING. FABIÁN TITO LUQUE**

**LA PAZ - BOLIVIA**

**2020**



**UNIVERSIDAD MAYOR DE SAN ANDRÉS  
FACULTAD DE INGENIERIA**



**LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICAMENTE ACADÉMICOS.**

**LICENCIA DE USO**

El usuario está autorizado a:

- a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
- b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
- c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

**TODOS LOS DERECHOS RESERVADOS. EL USO NO AUTORIZADO DE LOS CONTENIDOS PUBLICADOS EN ESTE SITIO DERIVARA EN EL INICIO DE ACCIONES LEGALES CONTEMPLADAS EN LA LEY DE DERECHOS DE AUTOR.**

## **Dedicatoria**

El presente trabajo está dedicado principalmente a Dios, por ser el inspirador y darme la fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

A mi madre, por su amor, trabajo y sacrificio en todos estos años.

A todas las personas que me han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos.

## **Agradecimientos**

Al finalizar este trabajo quiero utilizar este espacio para agradecer al Ing. Fabián Tito por su apoyo y paciencia en este proyecto de estudio.

También quiero agradecer a la Facultad de Ingeniería, directivos y docentes por impartir conocimiento, formarnos y encaminarnos a ser grandes profesionales.

## GLOSARIO

- **ActionScript:** Lenguaje de programación que viene con Macromedia Flash para crear scripts.
- **ActiveX:** Programa creado por Microsoft para controlar la interactividad en las páginas web.
- **Applet:** Programa en lenguaje Java que se utiliza en las páginas web para conseguir efectos especiales.
- **Caché:** Memoria volátil que borra la información cuando se apaga el ordenador.
- **Clave:** Código de signos utilizados para cifrar datos y garantizar la privacidad.
- **Cliente:** Elemento de un sistema de información que requiere un servicio.
- **Compilación:** Transformar un programa escrito en un lenguaje, en otro programa creado en lenguaje de máquina.
- **Consola de Comandos:** Es una herramienta que permite escribir comandos para llevar a cabo una determinada acción, hay consolas que vienen instaladas por defecto en los Sistemas Operativos como Mac OS, Windows y Linux por ende puedes ejecutar comandos para realizar alguna tarea dentro de estos Sistemas Operativos.
- **Criptografía:** Ciencia que estudia la manera de cifrar y descifrar mensajes.
- **Distribución:** Conjunto de software específico compilado y configurado.
- **Dominio:** Nombre equivalente a una dirección de internet.
- **Entidad:** Representación de un objeto o concepto del mundo real que se describe en una base de datos.
- **Firewall:** Software o hardware que permite asegurar que se respete la política de seguridad de una red de datos.
- **Hardware:** Conjunto de componentes que conforman la parte física de una computadora.
- **Hash:** Algoritmo matemático que transforma cualquier dato en una serie de caracteres de longitud fija.
- **Hipermedia:** (HIPERtexto multiMEDIA) Organización de información textual, visual, gráfica y sonora a través de vínculos que crean asociaciones entre información relacionada dentro del sistema.
- **Host:** Dispositivo de usuario dentro de un sistema informático.
- **Interfaz de Usuario:** Medio que permite a una persona comunicarse con una máquina.
- **Internet:** Red Global que utiliza los protocolo TCP/IP.
- **Licencia:** Documento que autoriza el derecho de uso de un bien a otra persona u organización.
- **Linux:** Es el núcleo del sistema cuya denominación es GNU/Linux.
- **Ordenador:** Sinónimo de computadora o computador.

- **Paquete:** Programas que se distribuyen conjuntamente donde cada uno requiere de los demás para su funcionamiento.
- **Perl:** Lenguaje de programación muy utilizado para la elaboración de aplicaciones CGI (Imagen Generada Por Computadora).
- **Plug-in:** Programa que extiende las capacidades del navegador web de un modo específico.
- **Programación:** Definir una serie de procesos para resolver un problema.
- **Protocolo:** Conjunto de normas y/o procedimientos para la transmisión de datos.
- **Python:** Lenguaje interpretado orientado a objetos que se caracteriza por su claridad y versatilidad.
- **Recursivo:** que se repite o aplica indefinidamente.
- **Red de Datos:** Infraestructura que posibilita la transmisión de información a través del intercambio de datos.
- **Script:** conjunto de instrucciones escrito para un intérprete de comandos con algún lenguaje de scripts.
- **Servidor:** Dispositivo de un sistema que resuelve las peticiones de otros elementos del sistema, denominados clientes.
- **Sistema:** Conjunto de elementos interrelacionados y regidos por normas propias, de modo tal que pueden ser vistos y analizados como una totalidad.
- **Software:** Conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar tareas en una computadora.
- **Tabla:** objeto o entidad que se identifica a través de sus atributos.
- **Tecnología:** Aplicación de un conjunto de conocimientos y habilidades con el objetivo resolver un problema.
- **Transacción:** Interacción con una estructura de datos.
- **Web:** Término utilizado para referirse a la World Wide Web, considerado un sistema de intercambio de información estandarizado.

## LISTADO DE ACRÓNIMOS

- **ADV** (*Abstract Data View*) Vista de Datos Abstracta.
- **AJAX** (*Asynchronous JavaScript And XML*) JavaScript y XML asíncronos.
- **AMD** Advanced Micro Device.
- **ARM** Advanced RISC Machine.
- **BD** base de datos
- **CPU** unidad de procesamiento central
- **CSS** Hojas de estilo en cascada
- **DHTML** (*Dynamic HTML*) HTML Dinamico.
- **DHTML** HTML Dinámico.
- **DNS** Sistema de Nombres de Dominio
- **DNSSEC** extensiones de seguridad del sistema de nombres de dominio
- **DS** (*Dad Son*) Registro de recurso que relaciona un servidor padre y su hijo.
- **E-R** Entidad –Relación
- **GNU** (*GNU's Not Unix*) GNU no es Unix.
- **GPL** (*General Public License*) Licencia Pública General.
- **HDM** metodología de desarrollo de Hipermédia
- **HTML** Lenguaje de marcado de Hipertexto
- **HTML5** HTML versión 5
- **HTTP** Protocolo de Transferencia de Hypertexto
- **HTTPS** Protocolo Seguro de Transferencia de Hypertexto
- **IBM** International Business Machines Corporation.
- **IP** (*Internet Protocol*) Protocolo de Internet
- **IWEB** Ingeniería Web.
- **IXFR** Protocolo de Transferencia de Zona Incremental
- **JS** JavaScript.
- **KSK** (*Key Signing Key*) clave de firma de clave
- **LAMP** Linux Apache Mysql Linux
- **LDD** Lenguaje de definición de datos
- **LMD** Lenguaje de manipulación de datos
- **MEFP** Ministerio de Economía y Finanzas Públicas.
- **MIPS** Microprocessor without Interlocked Pipeline Stage.
- **NIC** tarjeta de interfaz de Red
- **NS** (*Name server*) Registro de recurso para registrar el nombre del servidor.
- **OO** Orientado a objetos
- **OOHDM** (*Object Oriented Hypermedia Design Method*) Método de Diseño de Hipermédia Orientado a Objetos.
- **OSI** (*Open System Interconnection*) Modelo de interconexión de sistemas abiertos.
- **PHP** (*PHP: Hypertext Preprocessor*) Preprocesador de Hipertexto.

- **PHP** Páginas de Hypertexto Preprocesadas
- **PPC** Power PC.
- **RAM** memoria de acceso aleatorio.
- **RFC** (*Request For Comments*) solicitud de comentarios.
- **RNDC** (*Remote Name Daemon Control*) Control de dominio de nombres remoto.
- **SGBD** Sistema Gestor de Bases de Datos.
- **SOHDM** (*Scenario-based Object-oriented Hypermedia Design Methodology*) Metodología de diseño de Hipermedia Orientada a Objetos Basada en Escenarios.
- **SQL** Lenguaje de consulta estructurada.
- **TCP** (*Transmission Control Protocol*) Protocolo de Control de Transmisión.
- **TTL** (*time to live*) Tiempo de vida.
- **UWE** (*UML-based Web Engineering*) Ingeniería Web basada en UML.
- **VBScript** *Visual Basic Script Edition*.
- **W3C** *World Wide Web Consortium*.
- **WAE** (*Web Application Extension*) Extensión de la aplicación Web para UML.
- **WSDM** (*Web Site Design Method*) Método de Diseño de Sitios Web.
- **XHTML** HTML extensible.
- **XML** (*Extensible Markup Language*) Lenguaje de Marcado Extensible.
- **ZSK** (*Zone Signing Key*) clave de firma de zona.

## **ÍNDICE DE CONTENIDO**

|   |          |
|---|----------|
| <b>Capítulo I: Introducción y Generalidades .....</b>       | <b>1</b> |
| <b>    1.1. Antecedentes .....</b>                          | <b>1</b> |
| <b>    1.2. Descripción del Problema.....</b>               | <b>2</b> |
| <b>    1.3. Objetivos .....</b>                             | <b>3</b> |
| 1.3.1. Objetivo General .....                               | 3        |
| 1.3.2. Objetivos Específicos.....                           | 3        |
| <b>    1.4. Justificación .....</b>                         | <b>3</b> |
| 1.4.1. Justificación Social .....                           | 3        |
| 1.4.2. Justificación Económica.....                         | 4        |
| 1.4.3. Justificación Tecnológica.....                       | 4        |
| <b>    1.5. Alcances y Límites.....</b>                     | <b>4</b> |
| <b>    1.6. Estrategia de Desarrollo .....</b>              | <b>6</b> |
| <b>Capítulo II: FUNDAMENTOS TEÓRICOS .....</b>              | <b>7</b> |
| <b>    2.1. El Sistema de Nombres de Dominio (DNS).....</b> | <b>7</b> |
| 2.1.1. Fundamentos del DNS .....                            | 7        |
| 2.1.2. Nombres de Dominio .....                             | 7        |
| 2.1.3. Zonas .....  | 8        |
| 2.1.4. Tipos de Servidores.....                             | 8        |
| 2.1.4.1. Servidor Primario .....                            | 8        |
| 2.1.4.2. Servidor Esclavo .....                             | 9        |
| 2.1.4.3. Servidor <i>Stealth</i> .....                      | 9        |
| 2.1.4.4. Servidores de Nombres Recursivo .....              | 9        |

|  |           |
|--|-----------|
| 2.1.4.5. Servidor de Reenvío.....                                  | 10        |
| 2.1.5. Servidores de Nombre en Roles Múltiples.....                | 10        |
| 2.1.6. Servidor DNS BIND .....                                     | 10        |
| 2.1.7. Tipos de Registros DNS.....                                 | 12        |
| 2.1.8. Formato del Mensaje DNS.....                                | 14        |
| 2.1.8.1. Formato de la Sección del Encabezado de Mensajes DNS..... | 14        |
| 2.1.8.2. Formato de la Sección de Pregunta.....                    | 15        |
| 2.1.8.3. Formato de Registro de Recurso .....                      | 16        |
| 2.1.9. Puerto de DNS .....   | 17        |
| 2.1.10. Extensiones de Seguridad de DNS (DNSSEC).....              | 17        |
| 2.1.10.1. Tipos de Registros de Recurso DNSSEC .....               | 17        |
| 2.1.10.2. Validación DNSSEC .....                                  | 18        |
| 2.1.11. Transacciones Firmadas .....                               | 22        |
| 2.1.12. Transferencias de Zona Incremental - IXFR.....             | 22        |
| <b>2.2. Sistema Operativo Libre .....</b>                          | <b>22</b> |
| 2.2.1. Distribución Debian GNU/Linux .....                         | 23        |
| <b>2.3. Aplicación Web .....</b>                                   | <b>23</b> |
| 2.3.1. HTTP y HTTPS .....  | 24        |
| 2.3.2. HTML, CSS y JavaScript.....                                 | 25        |
| <b>2.4. Servidor web .....</b>                                     | <b>26</b> |
| 2.4.1. Servidor Apache.....  | 26        |
| <b>2.5. Sistema Gestor de Base de Datos .....</b>                  | <b>26</b> |
| 2.5.1. MariaDB.....  | 27        |

|  |           |
|--|-----------|
| 2.5.2. Modelos de Datos.....   | 28        |
| 2.5.2.1. Modelo de Datos Entidad-Relación .....                                    | 28        |
| 2.5.2.2. Modelo de Datos Relacional .....  | 29        |
| 2.5.3. Grado de Interrelaciones .....  | 30        |
| 2.5.3.1. Interrelaciones Binarias.....   | 30        |
| 2.5.3.2. Interrelaciones <i>n</i> -arias .....                                     | 31        |
| 2.5.4. Lenguajes de Bases de Datos .....   | 31        |
| 2.5.4.1. Lenguaje de Definición de Datos .....                                     | 31        |
| 2.5.4.2. Lenguaje de Manipulación de Datos.....                                    | 32        |
| 2.5.5. Diseño de Bases de Datos .....  | 32        |
| 2.5.5.1. Etapas del Diseño de Bases de Datos.....                                  | 32        |
| <b>2.6. Lenguajes de Programación.....</b>   | <b>33</b> |
| 2.6.1. PHP .....   | 33        |
| <b>2.7. Metodología de Desarrollo de Aplicaciones Web.....</b>                     | <b>34</b> |
| 2.7.1. Método de Diseño de Hipermedia Orientado a Objetos (OOHDM).....             | 35        |
| <b>Capítulo III: DESARROLLO DEL PROYECTO .....</b>                                 | <b>37</b> |
| <b>3.1. Análisis e Identificación de Requerimientos.....</b>                       | <b>37</b> |
| 3.1.1. Requerimientos de Software .....  | 37        |
| 3.1.2. Requerimientos de Hardware.....   | 38        |
| <b>3.2. Especificaciones del Sistema.....</b>                                      | <b>39</b> |
| <b>3.3. Diseño de Ingeniería.....</b>  | <b>43</b> |
| 3.3.1. Diseño del Sistema de Administración de Usuarios .....                      | 43        |
| 3.3.2. Diseño del Sistema de Administración y Configuración del Servicio DNS ..... | 54        |

|  |            |
|--|------------|
| 3.3.3. Diagramas de Secuencia del Sistema.....   | 80         |
| 3.3.3.1. Diagramas de Secuencia del Sistema de Administración de Usuarios .....                      | 80         |
| 3.3.3.2. Diagramas de Secuencia del Sistema de Administración y Configuración del servicio DNS ..... | 84         |
| <b>3.4. Licencia del Sistema.....</b>  | <b>92</b>  |
| 3.4.1. Licencia Pública General GNU v3.0.....  | 94         |
| <b>3.5. Implementación del Sistema.....</b>  | <b>95</b>  |
| <b>3.6. Pruebas de Funcionamiento y Resultados Obtenidos.....</b>                                    | <b>96</b>  |
| <b>Capítulo IV: EVALUACIÓN CUANTITATIVA DEL PROYECTO .....</b>                                       | <b>103</b> |
| <b>4.1. Tiempo de Desarrollo del Proyecto .....</b>  | <b>103</b> |
| <b>4.2. Cantidad de Líneas de Código Desarrolladas .....</b>   | <b>104</b> |
| <b>Capítulo V: CONCLUSIONES Y RECOMENDACIONES.....</b>   | <b>107</b> |
| <b>5.1. Conclusiones .....</b>   | <b>107</b> |
| <b>5.2. Recomendaciones .....</b>  | <b>108</b> |
| <b>BIBLIOGRAFÍA.....</b>   | <b>109</b> |
| <b>ANEXO A: PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA Y RESULTADOS OBTENIDOS.....</b>                    | <b>111</b> |
| <b>ANEXO B: DIAGRAMA DE BLOQUES DEL SISTEMA .....</b>  | <b>145</b> |

## **ÍNDICE DE TABLAS**

|  |            |
|--|------------|
| <b>TABLA 2-1. Ejemplo Tabla Cliente .....</b>  | <b>29</b>  |
| <b>TABLA 2-2. Ejemplo Tabla Cuenta.....</b>  | <b>30</b>  |
| <b>TABLA 2-3. Ejemplo Tabla Activar .....</b>  | <b>30</b>  |
| <b>TABLA 4-1. Cálculo de Horas Trabajadas que se Emplearon en el Desarrollo del Proyecto.....</b>                              | <b>103</b> |
| <b>TABLA 4-2. Cálculo de Líneas de Código Empleadas en el Sistema de Administración de Usuarios .....</b>                      | <b>104</b> |
| <b>TABLA 4-3. Cálculo de Líneas de Código Empleadas en el Sistema de Administración y Configuración del Servicio DNS .....</b> | <b>105</b> |
| <b>TABLA 4-4. Cálculo de Líneas de Código Totales del Sistema .....</b>  | <b>106</b> |

## **ÍNDICE DE CUADROS**

|   |           |
|---|-----------|
| <b>CUADRO 2-1. Fragmento de los Tipos de Registros de Recursos .....</b>                              | <b>13</b> |
| <b>CUADRO 2-2. Clases de Registro de Recurso.....</b>   | <b>13</b> |
| <b>CUADRO 2-3. Sistemas de Gestión de Bases de Datos de Libre Distribución<br/>Relacionales .....</b> | <b>27</b> |
| <b>CUADRO 2-4. Comparación de Requisitos de Metodologías en el Entorno Web.....</b>                   | <b>35</b> |
| <b>CUADRO 3-1. Características de la Licencia GNU GPLv3 .....</b>                                     | <b>94</b> |

## ÍNDICE DE FIGURAS

|   |           |
|---|-----------|
| <b>FIGURA 2-1. Jerarquía de Árbol de DNS.....</b>   | <b>8</b>  |
| <b>FIGURA 2-2. Consulta DNS mediante Servidor Recursivo o de Caché.....</b>   | <b>10</b> |
| <b>FIGURA 2-3. Tipos de Servidores DNS.....</b>   | <b>11</b> |
| <b>FIGURA 2-4. Formato de Registro de Recurso .....</b>   | <b>12</b> |
| <b>FIGURA 2-5. Formato de Mensajes DNS.....</b>   | <b>14</b> |
| <b>FIGURA 2-6. Formato de la Cabecera del Mensaje DNS .....</b>   | <b>14</b> |
| <b>FIGURA 2-7. Formato de la Sección de Pregunta del Mensaje DNS .....</b>  | <b>15</b> |
| <b>FIGURA 2-8. Formato de la Sección de Respuesta del Mensaje DNS .....</b>   | <b>16</b> |
| <b>FIGURA 2-9. Validación DNSSEC de 12 Pasos.....</b>   | <b>19</b> |
| <b>FIGURA 2-10. Generación de Firma Digital.....</b>  | <b>21</b> |
| <b>FIGURA 2-11. Verificación de Firma Digital.....</b>  | <b>21</b> |
| <b>FIGURA 2-12. Esquema Básico de una Aplicación Web .....</b>  | <b>24</b> |
| <b>FIGURA 2-13. Servidores Web más Utilizados .....</b>   | <b>26</b> |
| <b>FIGURA 2-14. Ejemplo de Diagrama E-R .....</b>   | <b>29</b> |
| <b>FIGURA 3-1. Diagrama de Funcionamiento del Sistema de Administración por Consola de Comandos del Servicio DNS.....</b> | <b>37</b> |
| <b>FIGURA 3-2. Diagrama de Funcionamiento del Sistema de Administración Web para el Servicio DNS .....</b>                | <b>40</b> |
| <b>FIGURA 3-3. Jerarquía de Páginas Web del Sistema .....</b>   | <b>41</b> |
| <b>FIGURA 3-4. Entidad –Atributo para la BD de Restricción por IP .....</b>   | <b>43</b> |
| <b>FIGURA 3-5. Diagrama de Clases Navegacionales para la Autenticación .....</b>  | <b>44</b> |
| <b>FIGURA 3-6. Diagrama de Contextos Navegacionales para Autenticación .....</b>  | <b>44</b> |

|   |           |
|---|-----------|
| <b>FIGURA 3-7. Interfaz de Adición de Direcciones IP Permitidas .....</b>                         | <b>44</b> |
| <b>FIGURA 3-8. Direcciones IP y de Red Permitidas para Acceder al Sistema .....</b>               | <b>45</b> |
| <b>FIGURA 3-9. Aviso de Permiso Denegado al Servidor .....</b>                                    | <b>45</b> |
| <b>FIGURA 3-10. Algoritmo de Autenticación del Sistema .....</b>                                  | <b>46</b> |
| <b>FIGURA 3-11. Modelo Conceptual Usuarios .....</b>  | <b>47</b> |
| <b>FIGURA 3-12. Diagrama de Clases Navegacionales para la Autenticación.....</b>                  | <b>48</b> |
| <b>FIGURA 3-13. Diagrama de Contextos Navegacionales para Autenticación .....</b>                 | <b>48</b> |
| <b>FIGURA 3-14. Interfaz de Autenticación de Usuarios.....</b>                                    | <b>48</b> |
| <b>FIGURA 3-15. Aviso de Ocupación por otro Usuario .....</b>                                     | <b>49</b> |
| <b>FIGURA 3-16. Interfaz de Registro de Usuario .....</b>   | <b>49</b> |
| <b>FIGURA 3-17. Interfaz de Eliminación de Usuario.....</b>                                       | <b>50</b> |
| <b>FIGURA 3-18. Ejemplo de Implementación de HTTPS por Consola.....</b>                           | <b>50</b> |
| <b>FIGURA 3-19. Resultado de la Implementación de HTTPS .....</b>                                 | <b>51</b> |
| <b>FIGURA 3-20. Algoritmo de Cierre de Sesión por Inactividad.....</b>                            | <b>52</b> |
| <b>FIGURA 3-21. Diagrama de Clases Navegacionales para el Tiempo de Sesión.....</b>               | <b>53</b> |
| <b>FIGURA 3-22. Diagrama de Contextos Navegacionales el Tiempo de Sesión .....</b>                | <b>53</b> |
| <b>FIGURA 3-23. Interfaz de Establecimiento del Tiempo de Sesión .....</b>                        | <b>53</b> |
| <b>FIGURA 3-24. Interfaz para Generar Copias de Respaldo de la Base de Datos de Usuario .....</b> | <b>54</b> |
| <b>FIGURA 3-25. Modelo Conceptual de la Zona Maestra Directa .....</b>                            | <b>55</b> |
| <b>FIGURA 3-26. Diagrama de Clases Navegacionales para la Zona Maestra Directa... </b>            | <b>56</b> |
| <b>FIGURA 3-27. Diagrama de Contextos Navegacionales para Zona Maestra Directa </b>               | <b>57</b> |
| <b>FIGURA 3-28. Interfaz de Creación de Zonas.....</b>  | <b>57</b> |

|  |           |
|--|-----------|
| <b>FIGURA 3-29. Interfaz de Creación de Zona Maestra Directa.....</b>  | <b>58</b> |
| <b>FIGURA 3-30. Interfaz de Edición y Eliminación de Zonas.....</b>  | <b>58</b> |
| <b>FIGURA 3-31. Interfaz de Edición de Zona Maestra Directa y Adición de Registros</b>   | <b>59</b> |
| <b>FIGURA 3-32. Interfaz de Permisos de la Zona Maestra Directa .....</b>  | <b>59</b> |
| <b>FIGURA 3-33. Modelo Conceptual del Servidor Recursivo .....</b>   | <b>60</b> |
| <b>FIGURA 3-34. Modelo Conceptual de la Zona de Reenvío .....</b>  | <b>61</b> |
| <b>FIGURA 3-35. Diagrama de Clases Navegacionales para el Servidor Recursivo.....</b>  | <b>62</b> |
| <b>FIGURA 3-36. Diagrama de Clases Navegacionales para la Zona de Reenvío.....</b>   | <b>62</b> |
| <b>FIGURA 3-37. Diagrama de Contextos Navegacionales para Servidor Recursivo y Zona de Reenvío .....</b>                       | <b>62</b> |
| <b>FIGURA 3-38. Interfaz de Habilitación de IPv6 y Acceso a la Configuración de Servidor Recursivo y Zona de Reenvío .....</b> | <b>63</b> |
| <b>FIGURA 3-39. Interfaz de Configuración de Servidor Recursivo .....</b>  | <b>63</b> |
| <b>FIGURA 3-40. Interfaz de Creación de Zona de Reenvío.....</b>   | <b>64</b> |
| <b>FIGURA 3-41. Modelo Conceptual para Realizar Respaldos del Sistema de Administración y Configuración de DNS .....</b>       | <b>64</b> |
| <b>FIGURA 3-42. Diagrama de Contextos Navegacionales para Servidor Recursivo y Zona de Reenvío .....</b>                       | <b>65</b> |
| <b>FIGURA 3-43. Interfaz de Respaldo de la Base de Datos del Sistema DNS.....</b>  | <b>65</b> |
| <b>FIGURA 3-44. Firma de Transacciones mediante TSIG .....</b>   | <b>66</b> |
| <b>FIGURA 3-45. Modelo Conceptual para la Creación de Claves TSIG.....</b>   | <b>66</b> |
| <b>FIGURA 3-46. Diagrama de Contextos Navegacionales para la Configuración y Uso de TSIG.....</b>                              | <b>67</b> |
| <b>FIGURA 3-47. Ejemplo de Clave TSIG Creada .....</b>   | <b>67</b> |

|   |           |
|---|-----------|
| <b>FIGURA 3-48. Interfaz de Creación de una Clave TSIG.....</b>   | <b>67</b> |
| <b>FIGURA 3-49. Clave Creada para Transacciones Firmadas entre Servidores .....</b>   | <b>68</b> |
| <b>FIGURA 3-50. Interfaz de Asociación de un Servidor con una Clave TSIG .....</b>  | <b>68</b> |
| <b>FIGURA 3-51. Asociación de la Dirección IP con una Clave TSIG creada .....</b>   | <b>68</b> |
| <b>FIGURA 3-52. Asociación de la IP del Servidor Externo con la clave TSIG. ....</b>  | <b>69</b> |
| <b>FIGURA 3-53. Modelo Conceptual para el Uso de DNSSEC .....</b>   | <b>71</b> |
| <b>FIGURA 3-54. Diagrama de Contextos Navegacionales para Uso de DNSSEC y Firma de Zonas.....</b>                             | <b>72</b> |
| <b>FIGURA 3-55. Interfaz para la Firma de Zonas con DNSSEC e Importación de Claves .....</b>                                  | <b>72</b> |
| <b>FIGURA 3-56. Interfaz de Creación de Claves ZSK y KSK.....</b>   | <b>73</b> |
| <b>FIGURA 3-57. Claves Creadas para el Dominio “ejemplo.com” con la Opción de ser Eliminadas y Exportadas .....</b>           | <b>73</b> |
| <b>FIGURA 3-58. Indicador de Firma de Zona que Expresa que la Zona “ejemplo.com” está Firmada.....</b>                        | <b>74</b> |
| <b>FIGURA 3-59. Interfaz de Firma de Zona .....</b>   | <b>74</b> |
| <b>FIGURA 3-60. Interfaz de Renovación de Clave KSK.....</b>  | <b>75</b> |
| <b>FIGURA 3-61. Muestra de los Archivos que Contienen los Registros DS para Enviar a la Zona Principal o Zona Padre .....</b> | <b>75</b> |
| <b>FIGURA 3-62. Configuración de Clave para RNDC.....</b>   | <b>77</b> |
| <b>FIGURA 3-63. Configuración de Restricciones para RNDC.....</b>   | <b>77</b> |
| <b>FIGURA 3-64. Modelo Conceptual del Uso de RNDC .....</b>   | <b>77</b> |
| <b>FIGURA 3-65. Modelo Conceptual de Herramientas de Diagnóstico del Servicio DNS.....</b>                                    | <b>77</b> |

|   |           |
|---|-----------|
| <b>FIGURA 3-66. Diagrama de Contextos Navegacionales para el Uso de RNDC .....</b>  | <b>78</b> |
| <b>FIGURA 3-67. Interfaz de Estado del Servicio DNS y Ventana de Resultado.....</b>   | <b>79</b> |
| <b>FIGURA 3-68. Interfaz de Estado del Sistema DNS.....</b>   | <b>79</b> |
| <b>FIGURA 3-69. Interfaz de Verificación de Archivos de Zona y Configuración .....</b>  | <b>79</b> |
| <b>FIGURA 3-70. Diagrama de Secuencias para la Configuración del Acceso al Sistema por IP .....</b>   | <b>80</b> |
| <b>FIGURA 3-71. Diagrama de Secuencias del Sistema de Autenticación por Contraseña .....</b>  | <b>81</b> |
| <b>FIGURA 3-72. Diagrama de Secuencias para el Registro y Eliminación del Sistema.</b>  | <b>81</b> |
| <b>FIGURA 3-73. Diagrama de Secuencias para Establecer el Cierre de Sesión por Inactividad .....</b>  | <b>82</b> |
| <b>FIGURA 3-74. Diagrama de Secuencias del Funcionamiento de Cierre de Sesión por Inactividad .....</b>                                     | <b>82</b> |
| <b>FIGURA 3-75. Diagrama de Secuencias para Respaldo del Sistema Administración de Usuarios.....</b>  | <b>83</b> |
| <b>FIGURA 3-76. Diagrama de Secuencias para Restauración de la BD del Sistema Administración de Usuarios .....</b>                          | <b>83</b> |
| <b>FIGURA 3-77. Diagrama de Secuencias para la Creación, Edición y Eliminación de Zonas .....</b>   | <b>84</b> |
| <b>FIGURA 3-78. Diagrama de Secuencias para la Edición de Zonas .....</b>   | <b>85</b> |
| <b>FIGURA 3-79. Diagrama de Secuencias para la Configuración de Servidores DNS Recursivos, Zonas de Reenvío y Habilitación de IPv6.....</b> | <b>86</b> |
| <b>FIGURA 3-80. Diagrama de Secuencias para el Respaldo del Sistema de Administración y Configuración de DNS .....</b>                      | <b>87</b> |

|  |            |
|--|------------|
| <b>FIGURA 3-81. Diagrama de Secuencias para la Restauración del Sistema de Administración y Configuración de DNS .....</b>                   | <b>87</b>  |
| <b>FIGURA 3-82. Diagrama de Secuencias para la Configuración Transacciones Firmadas entre Servidores mediante TSIG .....</b>                 | <b>88</b>  |
| <b>FIGURA 3-83. Diagrama de Secuencias para la Creación de Claves .....</b>  | <b>89</b>  |
| <b>FIGURA 3-84. Diagrama de Secuencias para la Firma de Zona .....</b>   | <b>89</b>  |
| <b>FIGURA 3-85. Diagrama de Secuencias del Estado del Servicio DNS .....</b>   | <b>90</b>  |
| <b>FIGURA 3-86. Diagrama de Secuencias del Estado del Sistema.....</b>   | <b>90</b>  |
| <b>FIGURA 3-87. Diagrama de Secuencias del Estado de Configuración de Zonas .....</b>  | <b>91</b>  |
| <b>FIGURA 3-88. Adición de la Dirección IP “192.168.222.246” Permitida para el Acceso al Sistema.....</b>                                    | <b>97</b>  |
| <b>FIGURA 3-89. Dirección IP “192.168.222.246” Configurada para el Acceso al Sistema .....</b>   | <b>97</b>  |
| <b>FIGURA 3-90. Acceso Restringido al Servidor para una Dirección no Configurada en la lista de direcciones IP o de Red permitidas .....</b> | <b>97</b>  |
| <b>FIGURA 3-91. Interfaz de Acceso para la Creación de una Zona Maestra Directa ...</b>  | <b>98</b>  |
| <b>FIGURA 3-92. Campos de llenado Formulario de una Zona Maestra Directa .....</b>   | <b>98</b>  |
| <b>FIGURA 3-93. Zona Maestra Directa Creada .....</b>  | <b>99</b>  |
| <b>FIGURA 3-94. Interfaz de Edición de una Zona Maestra Directa .....</b>  | <b>100</b> |
| <b>FIGURA 3-95. Interfaz de Permisos de una Zona Maestra Directa .....</b>   | <b>100</b> |
| <b>FIGURA 3-96. El Sistema Informa que los Datos de Zona se Cargaron Exitosamente.....</b>   | <b>101</b> |
| <b>FIGURA 3-97. Archivo Generado por el Sistema con el Resumen de la Zona Maestra Configurada.....</b>                                       | <b>101</b> |

**FIGURA 3-98. Archivo de Zona Maestra Directa Generada con el Sistema ..... 101**

**FIGURA 3-99. Consulta al Servidor por el Host “www.ejemplo.gob.bo” con la herramienta “dig” ..... 102**

## **Resumen**

El presente Proyecto de Grado plantea el desarrollo de un sistema de administración para un servidor DNS de uso intuitivo y con ventajas sobre sistemas existentes utilizando tecnología web y herramientas de software libre.

Inicialmente se identificaron los requerimientos necesarios para el desarrollo del sistema. Las herramientas de software libre empleadas para el desarrollo del sistema son Debian como Sistema Operativo; Apache como servidor web; MariaDB como Sistema Gestor de Base de Datos; PHP, HTML5, JavaScript y CSS como lenguajes para el desarrollo de aplicaciones web y BIND como el servicio de DNS a ser administrado. El sistema fue desarrollado aplicando el método de Diseño de Hipermedia Orientado a Objetos OOHDMD.

La administración del sistema, está basada en el uso de formularios de datos y botones que ejecutan tareas específicas. El sistema desarrollado permite trabajar con el protocolo IPv4 e IPv6; permite la configuración de servidores DNS recursivos y autoritativos; creación, edición y eliminación de zonas; herramientas de diagnóstico; administración de usuarios y restricción de accesos simultáneos; cuenta con autenticación de usuarios por contraseña; acceso restringido al sistema por listas de direcciones IPv4 e IPv6; el intercambio de datos entre cliente y servidor web será por medio del protocolo HTTP Seguro; cierre de sesión por inactividad con un tiempo configurable; activación de DNS Seguro DNSSEC y en consecuencia la creación y renovación de claves ZSK y KSK; implementa también, el uso de transacciones firmadas TSIG para las transferencias de zona entre servidores maestro-esclavo; el control remoto por consola del servicio DNS está configurado para ser administrado solamente de forma local y mediante la clave RNDC creada; permite realizar respaldos independientes de la configuración del sistema de administración de usuario y del sistema de administración del servicio DNS.

El sistema desarrollado es de uso intuitivo con muchas ventajas de seguridad y funcionalidad utilizando tecnología web y herramientas de software libre. En

consecuencia, el sistema desarrollado posee la licencia de software libre GNU GPL versión 3.

*Palabras claves: DNS, web, software libre, autenticación, sistema*

## **Summary**

This Degree Project proposes the development of an administration system for a DNS server for intuitive use and with advantages over existing systems using web technology and free software tools.

Initially the necessary requirements for the development of the system were identified. The free software tools used for system development are Debian as an Operating System; Apache as a web server; MariaDB as Database Management System; PHP, HTML5, JavaScript and CSS as languages for the development of web applications and BIND as the DNS service to be managed. The system was developed by applying the OOHDM Object Oriented Hypermedia Design method.

System Administration is based on the use of data forms and buttons that execute specific tasks. The developed system allows working with the IPv4 and IPv6 protocol; allows configuration of recursive and authoritative DNS servers; creation, editing and elimination of zones; diagnostic tools; user administration and restriction of simultaneous access; account with password authentication of users; restricted access to the system by lists of IPv4 and IPv6 addresses; the interchange of data between client and web server will be through the Secure HTTP protocol; logout due to inactivity with a configurable time; DNS activation DNSSEC Secure and consequently the creation and renewal of ZSK and KSK keys; also implements the use of signed TSIG transactions for zone transfers between master-slave servers; the console remote control of the DNS service is configured to be managed only locally and using the RNDC key created; allows backups independent of the configuration of the user administration system and the DNS service management system.

The system developed is intuitive to use with many security and functionality advantages using web technology and free software tools. Consequently, the system developed has the GNU GPL version 3 free software license.

*Keywords: DNS, web, free software, authentication, system*

# **Capítulo I: Introducción y Generalidades**

## **1.1. Antecedentes**

Todos los usuarios de internet cuentan con la opción de utilizar servidores DNS proporcionados por el proveedor de internet, o servidores públicos; sin embargo, si se cuenta con un nombre de dominio propio, una práctica recomendable es implementar un servidor DNS propio, esto ayuda en cierta medida a descongestionar el tráfico de red hacia internet, a mejorar la velocidad de conexión y la disponibilidad del servicio.

El uso de licencias representa un costo para cualquier empresa y actualmente existe una variedad de software propietario en el mercado para implementar el servicio DNS, y se debe pagar por las licencias de este servicio.

Por otro lado existen soluciones gratuitas para las distintas distribuciones de Linux, que ofrecen software libre para la administración del servicio DNS con características similares a las versiones comerciales y bastante potentes, pero con el inconveniente de no contar con una interfaz sencilla de operar, o con falencias en sus características respecto de otros más completos, lo que origina la necesidad de un entorno de administración más sencillo para las distintas características de un Servidor DNS en una red de datos.

En Redes de Datos medianas y grandes, se requiere una administración avanzada de los servicios que le demanda su red, de esta forma se logra dar una mejor experiencia a los usuarios, brindando seguridad e integridad a sus datos.

Conforme pasan los años, surgen nuevas herramientas y tecnologías para lograr una mayor adaptabilidad de los servicios a las necesidades de red empresariales, habiendo hoy en día varias opciones para la administración del servicio de DNS, desde implementaciones de software con características básicas, hasta software de administración avanzada.

## **1.2. Descripción del Problema**

Los obstáculos para lograr una administración eficaz de un Servidor DNS, mediante el uso de software libre disponible en el mercado, es que en su mayoría no cuentan con una interfaz sencilla de operar y presentan falencias de seguridad.

En el caso del uso de servidores, basados en distribuciones de Linux, la administración del servicio DNS, se ejecuta por consola de comandos, y este hecho representa un factor importante en inversión de tiempo y la adquisición de conocimientos avanzados sobre los comandos de configuración y administración del servicio DNS, los comandos de administración del sistema operativo sobre el que opera y conocimientos de Redes de Datos.

También se debe tomar en cuenta que en la gestión 2019 se tiene previsto implementar DNS Seguro (DNSSEC) en los dominios .bo; este hecho trae consigo, nuevas y más frecuentes tareas de administración del servicio DNS. [5]

Las distribuciones de Linux ofrecen la posibilidad de implementar muchas de las prestaciones mencionadas; sin embargo, la forma de administración por consola no es fácil de utilizar, esto implica obtener el conocimiento necesario para desarrollar una interfaz web que junto al Servicio DNS permita superar los obstáculos de la administración por consola.

Asimismo, existen leyes y decretos supremos en Bolivia que impulsan la migración de Software Propietario a Software Libre, entre los más importantes se puede mencionar al Parágrafo I del Artículo 77 de la Ley N° 164 de 8 de Agosto de 2011 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, que señala “...los Órganos Ejecutivo, Legislativo, Judicial y Electoral en todos sus niveles, promoverán y priorizarán la utilización del software libre y estándares abiertos...”. [1]

Asimismo, el Artículo 2 del DS N° 3251 de 12 de Julio de 2017, señala que “...el Plan de Implementación de Software Libre y Estándares Abiertos son aplicables por todos los niveles de Gobierno del Estado Plurinacional de Bolivia...”. [1]

## **1.3. Objetivos**

### **1.3.1. Objetivo General**

Desarrollar un sistema de administración para un servidor DNS, de uso intuitivo y con ventajas sobre sistemas existentes, utilizando tecnología web y herramientas de software libre para el Ministerio de Economía y Finanzas Públicas.

### **1.3.2. Objetivos Específicos**

- a) Identificar los requerimientos de software y hardware para el funcionamiento del sistema de administración web y las consideraciones a tomar en cuenta en la infraestructura de Red.
- b) Especificar los atributos que abarcará el sistema de administración de usuarios y el sistema de administración y configuración del servicio DNS a desarrollar.
- c) Diseñar el sistema de administración web para el servicio DNS, considerando funcionalidades adicionales a las que presentan los sistemas actuales.
- d) Implementar el sistema de administración web del servicio DNS en un servidor de pruebas, que inicialmente operará en una máquina virtual.
- e) Realizar pruebas de funcionamiento del sistema de administración web del servicio DNS y presentar los resultados obtenidos.

## **1.4. Justificación**

### **1.4.1. Justificación Social**

La presente propuesta permitirá hacer un uso eficaz del tiempo y reducir la cantidad de errores de sintaxis durante la configuración y administración del servicio DNS. Lo que permitirá al administrador abarcar nuevas tareas de administración en mejora de la seguridad de las tareas inherentes al servicio DNS, tales como la implementación de las

extensiones de seguridad DNSSEC y las transferencias de zona firmadas con claves TSIG.

#### **1.4.2. Justificación Económica**

El uso de herramientas de software, con licencia de software libre posibilita administrar sistemas potentes a un costo económico mínimo.

#### **1.4.3. Justificación Tecnológica**

El uso de programas con licencia de software libre, por medio del código abierto, posibilitan estudiar su funcionamiento y hacer mejoras de forma periódica, implementando nuevas características que los adaptan mejor a las necesidades y que mejoran la seguridad de los sistemas.

### **1.5. Alcances y Límites**

El **Sistema de Administración y Configuración del Servicio DNS**, contará con la posibilidad de habilitar la configuración para direcciones de red y de *host*, IPv6. Permitirá la configuración de servidores DNS recursivos y autoritativos, y para este último la creación, edición y eliminación de zonas maestras, esclavas e inversas. Para cada zona se permitirá la configuración de los permisos de consulta de clientes por dirección IP o redes específicas. Se crearán las herramientas de diagnóstico y de estado del servicio DNS, que permitan identificar errores de contenido en los archivos de configuración y conocer el estado de los recursos de *hardware* del sistema.

El **Sistema de Administración de Usuarios** permitirá el registro y eliminación de nuevos usuarios del sistema. Asimismo, evitará el ingreso de dos usuarios de forma simultánea con el fin de evitar sobrescribir configuraciones del servicio DNS.

El sistema estará protegido de accesos no autorizados, mediante el uso de autenticación por contraseña. También se implementará el acceso al sistema por dirección de red o de *host* para IPv4 e IPv6. El intercambio de datos entre cliente-servidor será a través del

protocolo HTTP Seguro. Se protegerán las sesiones de los usuarios mediante cierres de sesión, después de cierto tiempo de inactividad. Se implementará un botón para activar el uso de DNSSEC, para brindar integridad y autenticidad a los datos consultados. Se implementará un botón para habilitar las transacciones firmadas TSIG, entre pares de servidores, para las transferencias de zona. El control remoto del servicio DNS (RNDC) será configurado para ser administrado solamente de forma local y mediante la clave RNDC creada.

Las copias de respaldo del sistema desarrollado permitirán respaldar por separado la base de datos del sistema de administración de usuarios y por otro lado del sistema de administración del servicio DNS y de forma independiente permitirá respaldar las claves ZSK y KSK, junto a los Registros de Recurso DS correspondientes a la habilitación de DNSSEC.

El sistema no implementará actualizaciones dinámicas (RFC 2136) ya que no es utilizada en la Red de Datos del Ministerio de Economía y Finanzas Públicas, por ser considerada un factor vulnerable en la seguridad del servidor DNS.

Debido a que el sistema de administración del servicio DNS plantea la creación de una interfaz web, que reemplace la administración por consola, en servidores DNS que ya se encuentran en funcionamiento; el cálculo de los requerimientos de *hardware* del servidor que brinda el servicio DNS, queda fuera del alcance de este proyecto, debido a que depende del tipo de servidor recursivo o autoritativo, y las funcionalidades a implementar, así como de la redundancia en la topología de la red y el número estimado de clientes que realizan las consultas, sin embargo se proporcionarán ciertas recomendaciones, que coadyuvaran al correcto funcionamiento del servicio en las distintas implementaciones.

Como parte del sistema de administración web del servicio DNS desarrollado, se entregará un manual de administración, explicando el uso y funcionalidades del mismo.

Por motivos de confidencialidad, por parte del Ministerio de Economía y Finanzas, para la etapa de pruebas de funcionamiento, el sistema desarrollado será implementado en un servidor virtual, con las recomendaciones y requisitos de hardware mínimos.

## 1.6. Estrategia de Desarrollo

Entre los sistemas operativos libres que se encuentran disponibles para servidores, los fuertemente conocidos e implementados debido a su estabilidad son **Centos** y **Debian**; la herramienta de software para la administración del servidor DNS mediante tecnología web es **Apache**, junto a los lenguajes de desarrollo web **PHP**, **HTML5**, **JavaScript** y **CSS**; la herramienta de gestión de bases de datos que utiliza lenguaje SQL es **MariaDB** y el paquete de software de servicio DNS se denomina **BIND**. El conjunto de estas herramientas de software libre, harán posible el desarrollo del sistema planteado.

## Capítulo II: FUNDAMENTOS TEÓRICOS

### 2.1. El Sistema de Nombres de Dominio (DNS)

DNS cubre la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet.

#### 2.1.1. Fundamentos del DNS

El Sistema de nombres de dominio (DNS) es una base de datos jerárquica y distribuida que almacena información para mapear nombres de host de Internet a direcciones IP y viceversa, además de información de enrutamiento de correo y otros datos utilizados por aplicaciones de Internet. [4]

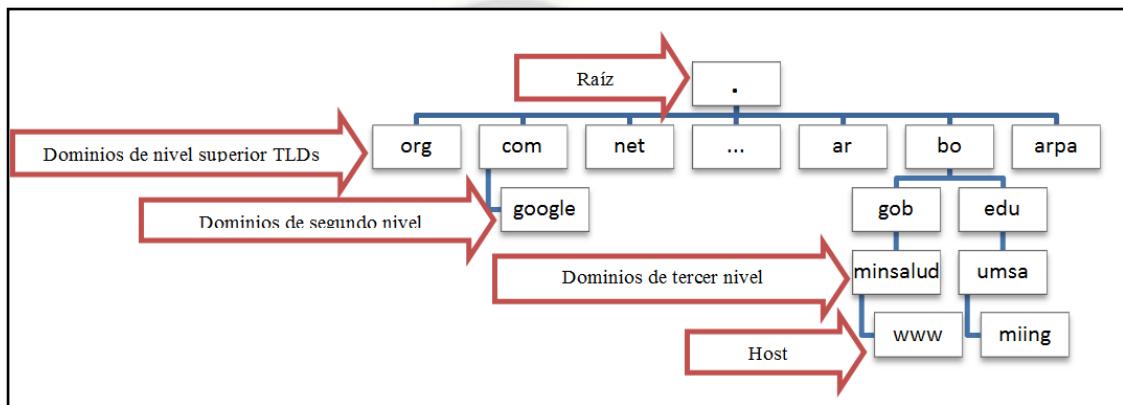
#### 2.1.2. Nombres de Dominio

Los datos almacenados en un servidor DNS, se identifican por los nombres de dominio que están organizados como un árbol. Cada nodo del árbol, recibe una etiqueta. El **nombre de dominio del nodo** es la concatenación de todas las etiquetas en la ruta, desde el nodo actual hasta el nodo raíz. Esto se representa en forma escrita como una cadena de etiquetas enumeradas de derecha a izquierda y separadas por puntos. Una etiqueta solo necesita ser única dentro de su dominio principal. [4]

Una etiqueta está formada por una cadena alfanumérica y el guion medio ‘-’ como único símbolo permitido, un mínimo de 1 carácter y un máximo de 63 caracteres de longitud comenzando por una letra. La concatenación de todas las etiquetas, tiene una longitud máxima total de 255 caracteres. [3]

Los datos asociados con cada nombre de dominio, se almacenan en forma de registros de recursos (RR).

La jerarquía DNS tiene una estructura de árbol invertido y tiene distintos niveles. Después de la **raíz** simbolizada por un punto “.”, están los dominios de nivel superior o TLDs (*Top-Level Domain*) y los dominios de segundo y tercer nivel (véase FIGURA 2-1). [2]



**FIGURA 2-1. Jerarquía de Árbol de DNS**

Fuente: Elaboración propia

### 2.1.3. Zonas

Una zona es un punto de delegación en el árbol DNS. Consta de las hojas de un nodo del árbol de dominios para las cuales un servidor de nombres tiene información completa y sobre la que tiene autoridad. Un punto de delegación está marcado por uno o más registros NS en la zona principal, que deben coincidir con registros NS equivalentes en la raíz de la zona delegada. [4]

### 2.1.4. Tipos de Servidores

#### 2.1.4.1. Servidor Primario

El servidor autoritativo donde se guarda la copia maestra de los datos de la zona se llama **servidor principal maestro**, o simplemente servidor primario. Este servidor carga los

contenidos de la zona desde un archivo local editado por el administrador, este archivo se denomina archivo de zona o archivo maestro. [4]

#### **2.1.4.2. Servidor Esclavo**

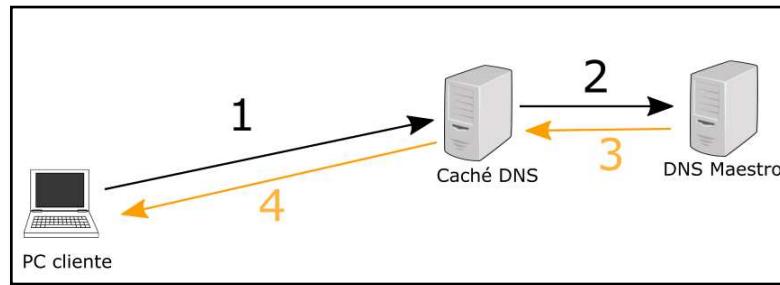
Los servidores esclavos, conocidos como **servidores secundarios**, cargan los contenidos de la zona desde otro servidor, utilizando un proceso de replicación conocido como transferencia de zona. Generalmente, los datos se transfieren directamente desde un servidor maestro primario, pero también es posible transferirlos desde otro servidor esclavo. [4]

#### **2.1.4.3. Servidor Stealth**

Es un servidor autoritativo para una zona, pero no figura en los registros NS de la zona, es decir, que están ocultos. Se pueden emplear para mantener una copia local de una zona para acelerar el acceso a los registros de la zona o para asegurarse de que la zona esté disponible, incluso si no se puede acceder a todos los servidores "oficiales" de la zona. [4]

#### **2.1.4.4. Servidores de Nombres Recursivo**

Las bibliotecas de resolución proporcionadas por la mayoría de los sistemas operativos en las computadoras de escritorio, no son capaces de realizar el proceso completo de resolución DNS por sí mismos, al hablar directamente con los servidores autoritativos (véase FIGURA 2-2). En cambio, confían en un servidor de nombre local para realizar la resolución en su nombre. Dado que los procesos de recursión y almacenamiento en caché están íntimamente conectados, los términos "servidor recursivo" y "servidor de caché" se utilizan a menudo como sinónimos. [4]



**FIGURA 2-2. Consulta DNS mediante Servidor Recursivo o de Caché**  
Fuente: Elaboración Propia

#### 2.1.4.5. Servidor de Reenvío

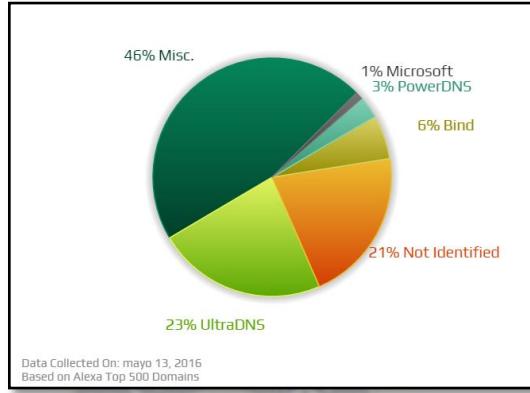
Un servidor de nombre recursivo no realiza necesariamente la búsqueda recursiva completa. En su lugar, puede reenviar algunas o todas las consultas que no puede satisfacer desde su caché a otro servidor de nombre, comúnmente denominado **servidor de reenvío**. [4]

#### 2.1.5. Servidores de Nombre en Roles Múltiples

El servidor de nombres puede actuar simultáneamente como maestro para algunas zonas, como esclavo para otras zonas y como servidor de caché (recursivo) para un conjunto de clientes locales. Sin embargo, dado que las funciones del servicio de nombres autoritativo y el servicio de nombres recursivo están lógicamente separados, a menudo es ventajoso ejecutarlos en máquinas de servidor separadas. [4]

#### 2.1.6. Servidor DNS BIND

A nivel Mundial existen diversas implementaciones de servidores DNS Autoritativos (véase FIGURA 2-3).



**FIGURA 2-3. Tipos de Servidores DNS**  
Fuente: Gráfico tomado de la página web [6]

De las implementaciones mostradas sobre los 500 dominios más visitados en internet, se pueden identificar que existen 3 tipos de servidores con licencia de software propietaria:

- Microsoft
- PowerDNS
- UltraDNS

Y solamente 1 que tiene licencia de software libre:

- BIND (*Berkeley Internet Name Domain*)

Licencia ISC (*Internet Systems Consortium*) para versiones anteriores a BIND 9.11.0 y licencia de *software libre* Mozilla MPL2.0 (*Mozilla Public License*) para versiones posteriores [7].

### 2.1.7. Tipos de Registros DNS

Todos los RR tienen el mismo formato de nivel superior (véase FIGURA 2-4).

| 0        | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|----------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|
| NAME     |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| TYPE     |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| CLASS    |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| TTL      |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| RDLENGTH |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| RDATA    |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |

**FIGURA 2-4. Formato de Registro de Recurso**

Fuente: Gráfico tomado de RFC [3]

Dónde:

- **NAME** es un nombre de dominio al que pertenece este registro de recursos.
- **TYPE** son dos octetos que contienen uno de los códigos de tipo RR. Este campo especifica el significado de los datos en el campo RDATA.
- **CLASS** son dos octetos que especifican la clase de los datos en el campo RDATA.
- **TTL** es un entero sin signo de 32 bits que especifica el intervalo de tiempo (en segundos) que el registro de recursos se puede almacenar en caché antes de que se deba descartar. Los valores de cero se interpretan en el sentido de que el RR solo se puede utilizar para la transacción en curso y no se debe almacenar en caché.
- **RDLENGTH** un entero de 16 bits sin signo que especifica la longitud en octetos del campo RDATA.
- **RDATA** una cadena de longitud variable de octetos que describe el recurso. El formato de esta información varía según el TIPO y la CLASE del registro de recursos. Por ejemplo, si el TYPE es A y la CLASE es IN, el campo RDATA es una dirección de Internet ARPA de 4 octetos.

Existe una gran cantidad de RR válidos, de los cuales no todos se aprovechan, debido a obsolescencia o próxima implementación (véase CUADRO 2-1).

|                |  |
|----------------|--|
| A              | Una dirección de host. En la clase IN, esta es una dirección IP de 32 bits. Descrito en RFC 1035.  |
| AAAA           | Dirección IPv6. Descrito en RFC 1886.  |
| CNAME          | Identifica el nombre canónico de un alias. Descrito en RFC 1035.   |
| DNSKEY         | Almacena una clave pública asociada con una zona DNS firmada. Descrito en RFC 4034.  |
| DS             | Almacena el hash de una clave pública asociada a una zona DNS firmada. Descrito en RFC 4034.   |
| HINFO          | Identifica la CPU y el sistema operativo utilizados por un host. Descrito en RFC 1035.   |
| MX             | Identifica un intercambio de correo para el dominio con un valor de preferencia de 16 bits (menor es mejor) seguido del nombre de host del intercambio de correo. Descrito en RFC 974, RFC 1035.   |
| NS             | El servidor de nombres autorizado para el dominio. Descrito en RFC 1035.   |
| NSEC           | Se usa en DNSSECbis para indicar de forma segura que los RR con un nombre de propietario en un determinado intervalo de nombre no existen en una zona e indican qué tipos de RR están presentes para un nombre existente. Descrito en RFC 4034.  |
| NSEC3          | Se usa en DNSSECbis para indicar de forma segura que los RR con un nombre de propietario en un determinado intervalo de nombre no existen en una zona e indican qué tipos de RR están presentes para un nombre existente. NSEC3 difiere de NSEC en que previene la enumeración de zonas, pero es más costoso desde el punto de vista computacional tanto para el servidor como para el cliente que NSEC. Descrito en RFC 5155. |
| NSEC3PA<br>RAM | Se usa en DNSSECbis para indicarle al servidor autoritario qué cadenas NSEC3 están disponibles para usar. Descrito en RFC 5155.  |
| PTR            | Un puntero a otra parte del espacio de nombre de dominio. Descrito en RFC 1035.  |
| RRSIG          | Contiene datos de firma DNSSECbis. Descrito en RFC 4034.   |
| SOA            | Identifica el inicio de una zona de autoridad. Descrito en RFC 1035.   |
| SPF            | Contiene la información del marco de políticas del remitente para un dominio de correo electrónico dado. Descrito en RFC 4408.   |
| SRV            | Información sobre servicios de red conocidos (reemplaza a WKS). Descrito en RFC 2782.  |
| TXT            | Registros de texto. Descrito en RFC 1035.  |

### CUADRO 2-1. Fragmento de los Tipos de Registros de Recursos

Fuente: Fragmento de Cuadro pág. 156 del texto [4]

Existen tres clases de RRs que actualmente son válidos en el DNS (véase CUADRO2-2).

|    |   |
|----|---|
| IN | Internet.   |
| CH | Chaosnet, un protocolo LAN creado en el MIT a mediados de la década de 1970. Rara vez se utiliza para su propósito histórico, pero se reutiliza para las zonas de información del servidor integradas de BIND, por ejemplo, version.bind. |
| HS | Hesiod, un servicio de información desarrollado por el Proyecto Athena del MIT. Se usa para compartir información sobre varias bases de datos de sistemas, como usuarios, grupos, impresoras, etc.  |

### CUADRO 2-2. Clases de Registro de Recurso

Fuente: Cuadro pág. 161 del texto [4]

### 2.1.8. Formato del Mensaje DNS

Todas las comunicaciones que implican una consulta y una respuesta DNS, se llevan en un formato único de mensaje. El formato de mensaje de nivel superior se divide en 5 secciones (véase FIGURA 2-5).

|            |   |
|------------|---|
| HEADER     | Cabecera con varios campos                        |
| QUESTION   | Pregunta para el servidor de nombres              |
| ANSWER     | Registro de Recurso respondiendo la pregunta      |
| AUTHORITY  | Registro de Recurso apuntando hacia una autoridad |
| ADDITIONAL | Registro de Recurso con información adicional     |

**FIGURA 2-5. Formato de Mensajes DNS**

Fuente: Figura tomada de RFC [2]

#### 2.1.8.1. Formato de la Sección del Encabezado de Mensajes DNS

La cabecera o HEADER de los mensajes DNS, contiene diferentes campos (véase FIGURA 2-6).

| 0  | 1      | 2       | 3  | 4  | 5  | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15    |
|----|--------|---------|----|----|----|---|---|---|---|----|----|----|----|----|-------|
| ID |        |         |    |    |    |   |   |   |   |    |    |    |    |    |       |
| QR | Opcode | AA      | TC | RD | RA |   | Z |   |   |    |    |    |    |    | RCODE |
|    |        | QDCOUNT |    |    |    |   |   |   |   |    |    |    |    |    |       |
|    |        | ANCOUNT |    |    |    |   |   |   |   |    |    |    |    |    |       |
|    |        | NSCOUNT |    |    |    |   |   |   |   |    |    |    |    |    |       |
|    |        | ARCOUNT |    |    |    |   |   |   |   |    |    |    |    |    |       |

**FIGURA 2-6. Formato de la Cabecera del Mensaje DNS**

Fuente: Figura tomada de RFC [3]

Dónde:

- **ID** es un identificador de 16 bits asignado por el programa que genera cualquier tipo de consulta.
- **QR** es un campo de un bit que especifica si este mensaje es una consulta (0) o una respuesta (1).
- **OPCODE** es un campo de cuatro bits que especifica el tipo de consulta en este mensaje. Este valor lo establece quien origina la consulta y se copia en la respuesta. Los valores son:
  - **0** una consulta estándar (QUERY)
  - **1** una consulta inversa (IQUERY)

- **2** una solicitud de estado del servidor (STATUS)
- **3-15** reservado para uso futuro
- **AA** es una Respuesta Autoritativa.
- **TC** (Truncamiento), este bit especifica que este mensaje se truncó debido a una longitud mayor que la permitida en el canal de transmisión.
- **RD** (Recursión deseada), este bit se puede establecer en una consulta y se copia en la respuesta.
- **RA** (Recursión disponible), este bit se establece o borra en una respuesta e indica si el soporte de consultas recursivas está disponible en el servidor de nombres.
- **Z** Reservado para uso futuro, hasta la llegada de DNSSEC. Debe ser cero en todas las consultas y respuestas. Sin embargo, si se establece el bit DO (DNSSEC OK), indica una solicitud que utiliza DNSSEC cuando se implementa.
- **RCODE** (Código de respuesta): este campo de 4 bits se establece como parte de las respuestas.
- **QDCOUNT** es un entero de 16 bits sin signo que especifica el número de entradas en la sección de preguntas.
- **ANCOUNT** es un entero de 16 bits sin signo que especifica el número de registros de recursos en la sección de respuestas.
- **NSCOUNT** es un entero de 16 bits sin signo que especifica el número de registros de recursos del servidor de nombres en la sección de registros de autoridad.
- **ARCOUNT** es un entero de 16 bits sin signo que especifica el número de registros de recursos en la sección de registros adicionales.

### 2.1.8.2. Formato de la Sección de Pregunta

La sección de preguntas se usa para llevar la "pregunta" en la mayoría de las consultas, es decir, los parámetros que definen lo que se está preguntando. La sección del encabezado contiene entradas **QDCOUNT** (generalmente 1), cada uno tiene el mismo formato (véase FIGURA 2-7). [3]

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|
|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
|   |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |

QNAME  
TYPE  
QCLASS

**FIGURA 2-7. Formato de la Sección de Pregunta del Mensaje DNS**

Fuente: Figura tomada de RFC [3]

Dónde:

- **QNAME** es un nombre de dominio representado como una secuencia de etiquetas.
- **QTYPE** es un código de dos octetos que especifica el tipo de la consulta.
- **QCLASS** es un código de dos octetos que especifica la clase de la consulta.

#### 2.1.8.3. Formato de Registro de Recurso

La sección de respuesta (ANSWER), de autoridad (AUTHORITY) y las secciones adicionales (ADDITIONAL) comparten el mismo formato. Contienen un número variable de Registros de Recursos, donde el número de registros se especifica en el campo de conteo correspondiente en el encabezado. Cada registro de recursos tiene el mismo formato (véase FIGURA 2-8). [3]

| 0        | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|----------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|
| NAME     |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| TYPE     |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| CLASS    |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| TTL      |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| RDLENGTH |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |
| RDATA    |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |

**FIGURA 2-8. Formato de la Sección de Respuesta del Mensaje DNS**

Fuente: Figura tomada de RFC [3]

Dónde:

- **NAME** es un nombre de dominio al que pertenece este registro de recursos.
- **TYPE** son dos octetos que contienen uno de los códigos de tipo RR. Este campo especifica el significado de los datos en el campo RDATA.
- **CLASS** son dos octetos que especifican la clase de los datos en el campo RDATA.
- **TTL** es un entero sin signo de 32 bits que especifica el intervalo de tiempo (en segundos) que el registro de recursos se puede almacenar en caché antes de que se deba descartar.
- **RDLENGTH** un entero de 16 bits sin signo que especifica la longitud en octetos del campo RDATA.
- **RDATA** una cadena de longitud variable de octetos que describe el recurso.

### **2.1.9. Puerto de DNS**

Los mensajes se envían utilizando el puerto 53 tanto UDP (Protocolo de Datagramas de Usuario) como TCP (Protocolo de Control de Transmisión). Los mensajes transportados por UDP están restringidos a 512 bytes. Los mensajes más largos se truncan y se establece el bit TC en el encabezado. UDP no es aceptable para transferencias de zona, pero es el método recomendado para consultas estándar en Internet. Las consultas enviadas utilizando UDP pueden perderse y, por lo tanto, se requiere una estrategia de retransmisión. Las consultas o sus respuestas pueden ser reordenadas por la red o procesadas en los servidores de nombres, por lo que los servidores recursivos no deben depender de que se devuelvan en orden. [3]

### **2.1.10. Extensiones de Seguridad de DNS (DNSSEC)**

El Sistema de nombres de dominio (DNS) fue diseñado en una época en que Internet era un lugar confiable. El protocolo en sí proporciona poca protección contra respuestas maliciosas o falsificadas. Las Extensiones de Seguridad del Sistema de Nombres de Dominio DNS (DNSSEC) responde a esta necesidad, agregando firmas digitales a los datos de DNS, para que se pueda verificar la integridad de cada respuesta de DNS y autenticidad. En el mundo ideal cuando DNSSEC esté completamente implementado, cada respuesta DNS puede ser validada y confiable. [8]

#### **2.1.10.1. Tipos de Registros de Recurso DNSSEC**

DNSSEC introduce seis nuevos tipos de registro de recursos [8]:

- a) RRSIG (firma digital)
- b) DNSKEY (clave pública)
- c) DS (padre-hijo)
- d) NSEC (prueba de inexistencia)
- e) NSEC3 (prueba de inexistencia)
- f) NSEC3PARAM (prueba de inexistencia)

**a) RRSIG:** con DNSSEC habilitado, casi todas las respuestas de DNS incluirán al menos una RRSIG o una firma de registro de recurso.

**b) DNSKEY:** DNSSEC se basa en la criptografía de clave pública para la autenticidad e integridad de los datos. En general, existen dos categorías de claves utilizadas en DNSSEC, la clave de firma de zona (ZSK) que se usa para proteger todos los datos de la zona, y la clave de firma de clave (KSK) se utiliza para proteger otras claves.

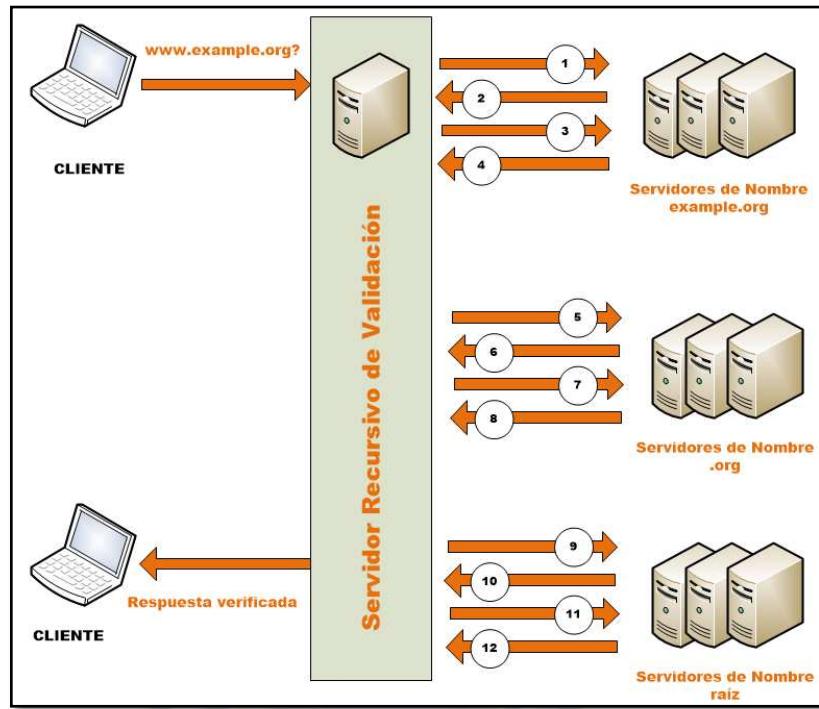
**c) DS:** El registro de DS es información verificable generada a partir de una de las claves públicas DNSKEY del hijo, que una zona principal publica sobre una zona que se denomina hijo.

Todos los registros de recursos de **d) NSEC**, **e) NSEC3** y **f) NSEC3PARAM** tratan con el problema de probar que algo no existe.

#### **2.1.10.2. Validación DNSSEC**

Con la validación de DNSSEC habilitada, un servidor de nombres recursivo de validación solicitará registros de recursos adicionales en su consulta, y espera que los servidores de nombres autorizados remotos respondan con registros de firma adicionales a la respuesta. Cuando DNSSEC esté completamente implementado en el mundo, todos los servidores recursivos de validación solo necesitarán confiar en una clave: la clave raíz. [8]

El proceso de validación de DNSSEC se realiza en 12 pasos (véase FIGURA 2-9).



**FIGURA 2-9. Validación DNSSEC de 12 Pasos**

Fuente: Basada en la figura tomada del texto [8]

1. El servidor recursivo de validación consulta al servidor de nombres **example.org** sobre el registro A de www.example.org.
2. La zona example.org responde con la respuesta a la consulta del registro A, más la RRSIG para el registro A.
3. El servidor recursivo de validación requiere claves criptográficas. Así que solicita el DNSKEY para example.org.
4. El servidor de nombres example.org responde con los registros DNSKEY y RRSIG. El DNSKEY se usa para verificar las respuestas recibidas en #2.
5. El servidor recursivo de validación consulta al padre **.org** por el registro de DS para example.org.
6. El servidor de nombres **.org** responde con los registros DS y RRSIG. El registro DS se usa para verificar las respuestas recibidas en #4.

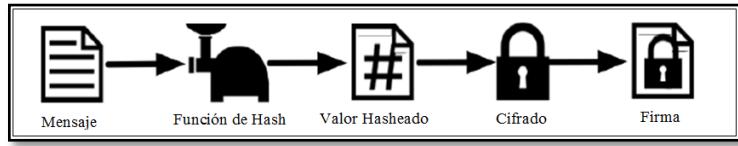
- 
7. El servidor recursivo de validación solicita a los servidores de nombres autorizados de **.org** sus claves criptográficas DNSKEY, con el fin de verificar las respuestas recibidas en #6.
  8. El servidor de nombres **.org** responde con DNSKEY y RRSIG. El DNSKEY se usa para verificar las respuestas recibidas en #6.
  9. El servidor recursivo de validación solicita a la raíz (padre de **.org**) información verificable que guarda sobre su hijo, entonces consulta al padre (raíz) por el registro de DS para **.org**.
  10. El servidor de nombres de raíz envía la información verificable de **.org** y responde con registros DS y RRSIG. El registro DS se usa para verificar las respuestas recibidas en #8.
  11. El servidor recursivo de validación solicita al servidor de nombres raíz sus claves criptográficas DNSKEY para verificar las respuestas recibidas en #10.
  12. El servidor de nombres de la raíz envía claves DNSKEY y RRSIG, en este punto, el DNSKEY se usa para verificar las respuestas recibidas en #10.

Entonces, una vez que se reciben las respuestas en #12, el servidor recursivo de validación toma la respuesta recibida y la compara con la clave que ya tiene en un archivo de forma local, y estas dos deben coincidir. Esto se conoce como "cadena de confianza" en DNSSEC.

### Verificación de Respuesta DNSSEC

La criptografía de clave pública se usa para proporcionar **autenticidad** e **integridad** de los datos, pero cualquier intruso puede ver las solicitudes y respuestas de DNS en texto claro, incluso cuando DNSSEC está habilitado.

En el servidor autoritativo con DNSSEC habilitado, cada Registro de Recurso DNS se ejecuta a través de una función de hash, luego este valor se cifra mediante una clave privada ZSK. Este valor hash cifrado es la firma digital RRSIG (véase FIGURA 2-10).

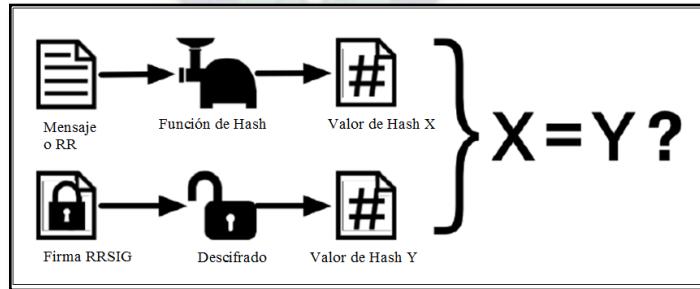


**FIGURA 2-10. Generación de Firma Digital**

Fuente: Figura tomada del texto [8]

Cuando el servidor recursivo de validación consulta por el registro de recursos, recibe tanto el mensaje de texto sin formato como la(s) firma(s) digital(es) RRSIG.

El servidor recursivo de validación conoce la función hash utilizada, por lo que puede tomar el mensaje de texto sin formato y ejecutarlo a través de la misma función hash para generar un valor hash “X”. El servidor recursivo de validación también puede obtener la clave pública, descifrar la firma digital y recuperar el valor de hash original, valor de hash “Y”. Si los valores hash “X” e “Y” son idénticos, la respuesta se verifica (véase FIGURA 2-11), lo que significa que esta respuesta provino del servidor autorizado, y el contenido se mantuvo intacto durante el tránsito. [8]



**FIGURA 2-11. Verificación de Firma Digital**

Fuente: Basada en la figura tomada del texto [8]

### **2.1.11. Transacciones Firmadas**

TSIG (*Transaction Signatures*) es un mecanismo para autenticar mensajes DNS, fue originalmente especificado en RFC 2845. Permite que los mensajes DNS se firmen criptográficamente utilizando una clave secreta compartida. Se puede utilizar en cualquier transacción DNS, como una forma de restringir el acceso a ciertas funciones del servidor a clientes autorizados cuando el control de acceso basado en IP es insuficiente y se necesita asegurar la autenticidad del mensaje cuando es crítico para la integridad del servidor, como las transferencias de zona entre un servidor maestro y uno esclavo. [4]

### **2.1.12. Transferencias de Zona Incremental - IXFR**

El protocolo de transferencia de zona incremental (IXFR) es una forma para que los servidores esclavos transfieran solo datos modificados, en lugar de tener que transferir toda la zona. El protocolo IXFR se especifica en RFC 1995. [4]

## **2.2. Sistema Operativo Libre**

Los **Sistemas Operativos**, aportan mecanismos y reglas básicas de funcionamiento, de forma que los programas puedan acceder a los recursos del ordenador de una forma adecuada.

El **núcleo** o *kernel* es el programa que asigna los recursos de la máquina y se comunica con el *hardware*. Para Linux, una **distribución** es la agrupación del núcleo Linux y una serie de aplicaciones de uso general lo que se conoce como **Sistema Operativo**. [9]

El **Software Libre** es el que se difunde bajo una licencia libre, es decir, que permita al usuario el ejercicio de las siguientes libertades [10]:

- Ejecutar el software, para cualquier propósito, sin restricción alguna.
- Estudiar cómo funciona el software y modificarlo para que cumpla un determinado propósito, a través del acceso al código fuente del mismo y todos

los componentes que hacen posible su funcionamiento. El acceso al código fuente es una condición necesaria e imprescindible.

- Redistribuir copias del software.
- Distribuir copias de las versiones modificadas a terceros. El acceso al código fuente es una condición necesaria e imprescindible.

El presente proyecto, hace uso de una distribución de Linux denominada **Debian GNU/Linux**, que al cumplir con las cuatro libertades de software libre se puede decir que se trata de un **Sistema Operativo Libre**.

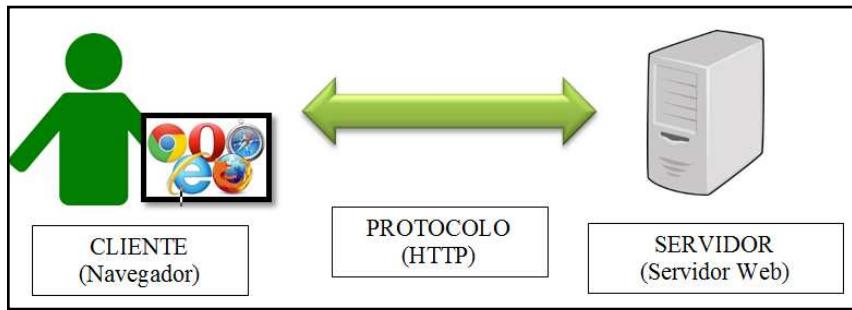
### **2.2.1. Distribución Debian GNU/Linux**

Esta distribución admite varios tipos de procesadores para 32 y 64 bits, entre ellos AMD, ARM, MIPS, PPC e IBM S390. Es una de las distribuciones más antiguas y actualmente es el proveedor de distribución basado en un grupo mundial de voluntarios más grande y se compone completamente de software libre.

Debian se inició en agosto de 1993 por Ian Murdock, fue patrocinado por el Proyecto GNU de “*The Free Software Foundation*”, la organización iniciada por Richard Stallman y asociada con la Licencia Pública General (GPL), por un año, desde Noviembre de 1994 hasta Noviembre de 1995. [11]

## **2.3. Aplicación Web**

Una aplicación web, es una aplicación cliente/servidor, donde el cliente, el servidor y protocolo están estandarizados (véase FIGURA 2-12). Para la transmisión de datos entre el servidor y cliente se utiliza el protocolo HTTP (*Hypertext Transfer Protocol*) o HTTPS (HTTP seguro), pertenecientes a la capa de aplicación del modelo OSI. [24]



**FIGURA 2-12. Esquema Básico de una Aplicación Web**

Fuente: Elaboración propia

Las tecnologías que se suelen emplear para programar el cliente web son [24]:

- HTML
- CSS
- DHTML
- Lenguajes de *script*: JavaScript, VBScript, JScript, ActionScript, etc.
- ActiveX
- Applets programados en lenguaje Java.
- Tecnologías que necesitan un *plug-in* en el navegador: Adobe Acrobat Reader, Autodesk MapGuide, Live Picture PhotoVista, Macromedia Flash, etc.

### 2.3.1. HTTP y HTTPS

HTTP es un protocolo de solicitud/respuesta. Cuando un cliente, por lo general un navegador Web, envía una solicitud a un servidor Web, HTTP especifica los tipos de mensaje que se utilizan para esa comunicación. Los tres tipos de mensajes comunes son *GET*, *POST* y *PUT*. [20]

HTTP no es un protocolo seguro. Los mensajes de solicitud envían información al servidor en un texto sin formato que puede ser interceptado y leído. El protocolo HTTPS utiliza el mismo proceso de solicitud del cliente-respuesta del servidor que HTTP, pero el *stream* de datos se encripta con la capa de *sockets* seguros (SSL) antes de transportarse a través de la red. El HTTPS crea una carga y un tiempo de procesamiento adicionales en el servidor debido a la encriptación y el descifrado de tráfico. [20]

El puerto estándar para el protocolo HTTP es el TCP/80 y para el protocolo HTTPS el puerto TCP/443.

### **2.3.2. HTML, CSS y JavaScript**

HTML es el Lenguaje de Marcas de Hipertexto utilizado para el desarrollo de páginas web. Es un estándar a cargo de la *World Wide Web Consortium* (W3C) y que se ha impuesto en la visualización de páginas web y que todos los navegadores han adoptado. HTML sirve para indicar como va ordenado el contenido de una página web, esto lo hace por medio de las marcas de hipertexto las cuales se denominan etiquetas. [13]

**HTML5** es la quinta y principal versión actual del estándar HTML, e incluye XHTML.

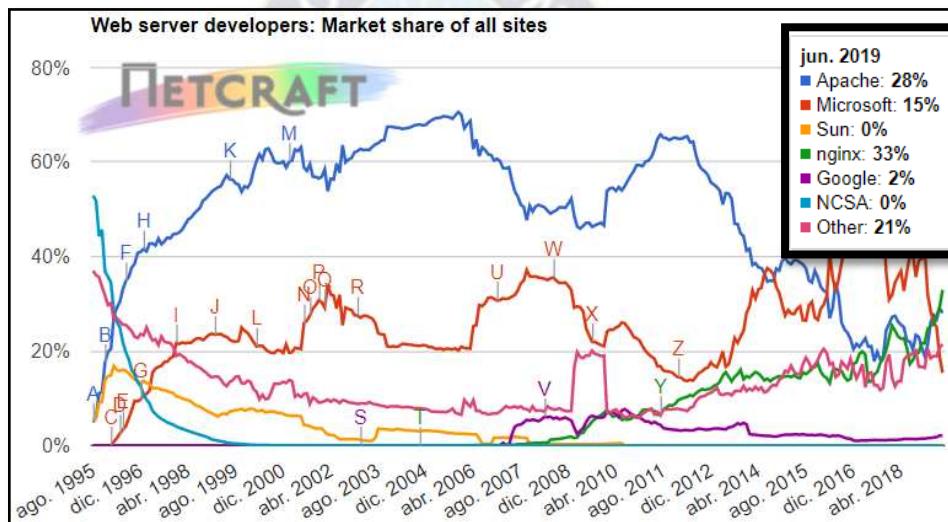
CSS es el lenguaje para describir la presentación de las páginas web, incluye los colores, el diseño y las fuentes. Permite adaptar la presentación a diferentes tipos de dispositivos, como pantallas grandes, pantallas pequeñas o impresoras. CSS es independiente de HTML y se puede utilizar con cualquier lenguaje de marcado basado en XML. [13]

ECMAScript más conocido como **JavaScript** es el lenguaje de *scripting* más común. Un *script* es un código de programa que no necesita pre-procesamiento (por ejemplo, compilación) antes de ejecutarse. En el contexto de un navegador web, las secuencias de comandos generalmente se refieren al código del programa escrito en JavaScript que ejecuta el navegador cuando se descarga una página, o en respuesta a un evento desencadenado por el usuario. Las secuencias de comandos pueden hacer que las páginas web sean más dinámicas. Por ejemplo, sin volver a cargar una nueva versión de una página, puede permitir modificaciones en el contenido de esa página a esto se denomina DHTML (HTML dinámico), o permitir que el contenido se agregue o se envíe desde esa página, a esto se denomina AJAX (JavaScript Asíncrono y XML). [12]

## 2.4. Servidor web

### 2.4.1. Servidor Apache

El servidor HTTP **Apache** es el más antiguo y actualmente continúa siendo ampliamente utilizado. Si bien su cuota de mercado ha ido descendiendo en los últimos años, aún es usado por el 28 % de las páginas web, de forma similar que **Nginx** con el 33% (véase FIGURA 2-13). [14]



**FIGURA 2-13. Servidores Web más Utilizados**

Fuente: Figura tomada de la página web [14]

## 2.5. Sistema Gestor de Base de Datos

Un **sistema gestor de bases de datos** (SGBD) consiste en una colección de datos interrelacionados y un conjunto de programas para acceder a dichos datos. La colección de datos denominada base de datos, contiene información relevante para una empresa. El objetivo principal de un SGBD es proporcionar una forma de almacenar y recuperar la información de una base de datos de manera que sea tanto práctica como eficiente. [15]

Actualmente los SGBD relacionales están en plena transformación para adaptarse a tres tecnologías fuertemente relacionadas: la multimedia (imagen y sonido), la orientación a objetos (OO), y la web e Internet.

Existe en el mercado una variedad de programas para la administración de BD, de libre distribución y propietarias, de los cuales una pequeña fracción son de libre distribución – Relacionales (véase CUADRO 2-3).

| CLASIFICACIÓN                        | SISTEMA GESTOR DE BASE DE DATOS  |
|--------------------------------------|--|
| De Libre Distribución- Relacionales: | <ul style="list-style-type: none"><li>- MySQL</li><li>- MariaDB</li><li>- PostgreSQL</li></ul> |

**CUADRO 2-3. Sistemas de Gestión de Bases de Datos de Libre Distribución Relacionales**

Fuente: Fragmento de cuadro tomado de la página web [18]

MySQL ha sido indiscutiblemente durante años el sistema gestor de base de datos más popular. Mucho ha tenido que ver con ello la proliferación de sistemas LAMP (Linux, Apache, MySQL, PHP/ Python/ Perl) utilizados para la implementación de sitios web.

Un grupo, de empleados originales de **MySQL AB**, liderado e iniciado por el cofundador de MySQL Michael Widenius, tuvo la determinación de dejar **Sun/Oracle**, y crear una rama de MySQL llamada **MariaDB**.

### **2.5.1. MariaDB**

El objetivo general de MariaDB es el de ser una alternativa a MySQL, con más funcionalidades y mejor rendimiento. MariaDB está basado en la versión homóloga de MySQL, si ésta existe. [19]

## **2.5.2. Modelos de Datos**

Bajo la estructura de la base de datos se encuentra el modelo de datos, una colección de herramientas conceptuales para describir datos, las relaciones, la semántica y las restricciones de consistencia.

Los modelos de datos se clasifican en tres grandes grupos diferentes [16]:

- Modelos lógicos basados en objetos
- Modelos lógicos basados en registros
- Modelos físicos

Existen dos modelos de datos ampliamente utilizados:

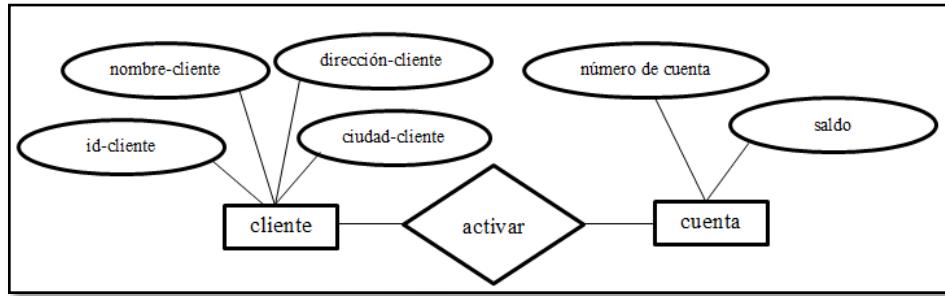
- El modelo entidad-relación
- El modelo relacional.

### **2.5.2.1. Modelo de Datos Entidad-Relación**

El modelo de datos entidad-relación (E-R) está basado en una percepción del mundo real que consta de una colección de objetos básicos llamados entidades, y de relaciones entre estos objetos. Las entidades se describen en una base de datos mediante un conjunto de atributos. [15]

La estructura lógica general de una base de datos se puede expresar gráficamente mediante un diagrama E-R (véase FIGURA 2-14), que consta de los siguientes componentes [15]:

- Rectángulos: representan entidades.
- Elipses: representan atributos.
- Rombos: representan relaciones entre entidades
- Líneas: unen los atributos con las entidades, y entidades con relaciones.



**FIGURA 2-14. Ejemplo de Diagrama E-R**  
Fuente: Elaboración propia

### 2.5.2.2. Modelo de Datos Relacional

En el modelo relacional se utiliza un grupo de tablas para representar los datos y las relaciones entre ellos. Cada tabla está compuesta por varias columnas, y cada columna tiene un nombre único. A continuación, se presenta un ejemplo de base de datos relacional consistente en tres tablas: la primera muestra los clientes de un banco, la segunda muestra las cuentas, y la tercera muestra las cuentas que pertenecen a cada cliente. [15]

#### Ejemplo de Base de Datos Relacional

| id-cliente | nombre-cliente | dirección-cliente  | ciudad-cliente |
|------------|----------------|--------------------|----------------|
| 571        | Pérez          | Av. Miraflores #45 | La Paz         |
| 579        | Gómez          | Av. Carrasco #100  | Cochabamba     |
| 455        | Fernández      | Av. Arce # 250     | Oruro          |

**TABLA 2-1. Ejemplo Tabla Cliente**

Fuente: Elaboración propia

| número-cuenta | saldo |
|---------------|-------|
| c-100         | 5000  |
| c-205         | 1500  |
| c-320         | 2300  |

**TABLA 2-2. Ejemplo Tabla Cuenta**

Fuente: Elaboración propia

| id-cliente | número-cuenta |
|------------|---------------|
| 571        | c-100         |
| 579        | c-205         |
| 455        | c-320         |

**TABLA 2-3. Ejemplo Tabla Activar**

Fuente: Elaboración propia

El modelo de datos relacional es un modelo de datos ampliamente utilizado, y se encuentra a un nivel de abstracción inferior al modelo de datos E-R, por lo que los diseños de bases de datos se realizan primero en el modelo E-R para luego traducirse al modelo relacional. [15]

### 2.5.3. Grado de Interrelaciones

Una interrelación puede asociar dos o más entidades. El número de entidades que asocia una interrelación es el grado de la interrelación. Las interrelaciones de grado dos se denominan también **interrelaciones binarias**. Todas las interrelaciones de grado mayor que dos se denominan, en conjunto, interrelaciones n-arias. Así pues, una interrelación n-aria puede tener grado tres y ser una interrelación ternaria, o puede tener grado cuatro y ser una interrelación cuaternaria, etc. [17]

#### 2.5.3.1. Interrelaciones Binarias

La conectividad de una interrelación expresa el tipo de correspondencia que se establece entre las ocurrencias de entidades asociadas con la interrelación. En el caso de las

interrelaciones binarias, expresa el número de ocurrencias de una de las entidades con las que una ocurrencia de la otra entidad puede estar asociada según la interrelación. [17]

Una interrelación binaria entre dos entidades puede tener tres tipos de conectividad [17]:

- Conectividad uno a uno (1:1). La conectividad 1:1 se denota poniendo un 1 en un lado de la interrelación y un 1 en el otro.
- Conectividad uno a muchos (1:N). La conectividad 1:N se denota poniendo un 1 en un lado de la interrelación y una N en el otro.
- Conectividad muchos a muchos: (M:N). La conectividad M:N se denota poniendo una M en uno de los lados de la interrelación, y una N en el otro.

#### **2.5.3.2. Interrelaciones *n*-arias**

Las interrelaciones *n*-arias, igual que las binarias, pueden tener diferentes tipos de conectividad. Las **interrelaciones ternarias** pueden tener cuatro tipos de conectividad: M:N:P, M:M:1, N:1:1 y 1:1:1. [17]

#### **2.5.4. Lenguajes de Bases de Datos**

Un sistema de bases de datos proporciona un lenguaje de definición de datos para especificar el esquema de la base de datos y un lenguaje de manipulación de datos para expresar las consultas a la base de datos y las modificaciones.

En la práctica, los lenguajes de definición y manipulación de datos no son dos lenguajes separados; en su lugar simplemente forman parte de un único lenguaje de base de datos, tal como el ampliamente usado SQL (Lenguaje de consulta estructurada).

##### **2.5.4.1. Lenguaje de Definición de Datos**

Un esquema de base de datos se especifica mediante un conjunto de definiciones expresadas mediante un lenguaje especial llamado lenguaje de definición de datos (LDD). [15]

#### **2.5.4.2. Lenguaje de Manipulación de Datos**

La manipulación de datos es [15]:

- La recuperación de información almacenada en la base de datos.
- La inserción de información nueva en la base de datos.
- El borrado de información de la base de datos.
- La modificación de información almacenada en la base de datos.

#### **2.5.5. Diseño de Bases de Datos**

El diseño de una base de datos consiste en definir la estructura de los datos que debe tener la base de datos de un sistema de información determinado. En el caso relacional, esta estructura será un conjunto de esquemas de relación con sus atributos, dominios de atributos, claves primarias, claves foráneas, etc. [17]

##### **2.5.5.1. Etapas del Diseño de Bases de Datos**

Conviene descomponer el proceso del diseño en varias etapas y en cada una de ellas se obtiene un resultado intermedio que sirve de punto de partida de la etapa siguiente. En la última etapa se obtiene el resultado deseado.

El diseño de bases de datos se descompone en tres etapas [17]:

- 1) **Etapa del diseño conceptual:** en esta etapa se obtiene una estructura de la información de la futura base de datos, independiente de la tecnología a emplear.

El resultado de la etapa del diseño conceptual se expresa mediante algún modelo de datos de alto nivel. Uno de los más empleados es el modelo E-R.

- 2) **Etapa del diseño lógico:** en esta etapa se parte del resultado del diseño conceptual, que se transforma para adaptarse a la tecnología que se debe emplear.

El diseño lógico de una base de datos relacional, se hace tomando como punto de partida un diseño conceptual expresado con el modelo E-R.

- 3) **Etapa del diseño físico:** en esta etapa se transforma la estructura obtenida en la etapa del diseño lógico, con el objetivo de conseguir una mayor eficiencia; además, se completa con aspectos de implementación física que dependerán del SGBD.

## 2.6. Lenguajes de Programación

Los lenguajes de programación pueden ser clasificados de acuerdo a varios criterios. Una de las primeras clasificaciones que se suele efectuar es la distinción entre lenguajes de bajo y de alto nivel.

Cuando se está desarrollando un programa utilizando un lenguaje de programación se genera un código fuente que es comprensible para todo aquel usuario con los conocimientos suficientes sobre el correspondiente lenguaje, pero que no es comprensible directamente para la máquina. El proceso de traducción de código fuente a lenguaje de máquina, se puede realizar de dos maneras [22]:

- a. **Lenguajes compilados:** donde el código fuente pasa por un proceso denominado "compilación" en el que se genera un código denominado "objeto", y junto con otros posibles módulos de código objeto necesarios, genera el fichero ejecutable con el programa.
- b. **Lenguajes interpretados:** donde la traducción de las instrucciones se va realizando de forma secuencial por una aplicación, denominada "intérprete", al mismo tiempo que se ejecuta el programa.

El lenguaje PHP pertenece a la categoría de los lenguajes interpretados al igual que el lenguaje de *script* denominado JavaScript.

### 2.6.1. PHP

PHP es un lenguaje interpretado del lado del servidor que surge dentro de la corriente denominada código abierto. Se caracteriza por su potencia, versatilidad, robustez y

modularidad. Al igual que ocurre con tecnologías similares, los programas son integrados directamente dentro del código HTML. [22]

PHP es rápido y está optimizado para ser utilizado con **Apache**. La comunidad de PHP es una de las más grandes de todos los lenguajes de programación, lo que significa, que existen libros, cursos de capacitación, foros y miles de publicaciones en sitios web de soporte. [20]

PHP es utilizado por el 79% de todos los sitios web como lenguaje de programación del lado del servidor. [21]

De los servidores que utilizan PHP [21]:

- 63.7% utiliza la versión 5
- 35.8% utiliza la versión 7
- 0.5% utiliza la versión 4
- menos del 0.1% utiliza la versión 3

## 2.7. Metodología de Desarrollo de Aplicaciones Web

La implementación de metodologías en la creación de aplicaciones web mejora el proceso de creación y por tanto el desarrollo de software, disminuyendo los niveles de riesgos y mejorando la calidad de la aplicación.

Las metodologías de aplicaciones web están compuestas de etapas, que dependerán de la metodología a utilizar. La mayoría de los métodos coinciden en las siguientes [23]:

- **Diseño Conceptual:** en esta sección se abarca temas relacionados a la especificación del dominio del problema, a través de su definición y las relaciones que contrae.
- **Diseño Navegacional:** está enfocado en lo que respecta al acceso y forma en la que los datos son visibles.
- **Diseño de la presentación o diseño de interfaz:** se centra en la forma en que la información es mostrada a los usuarios, cabe mencionar que en esta sección

intervienen mayormente el cliente definiendo los requerimientos y los usuarios definiendo como quieren interactuar con el sistema.

- **Implementación:** es la construcción del software a partir de los objetos generados en las etapas previas.

Cada metodología cumple una serie de requisitos que abarcan diferentes aspectos (véase CUADRO 2-4).

| Requerimientos      | Metodologías |       |       |     |     |      |
|---------------------|--------------|-------|-------|-----|-----|------|
|                     | WSDM         | SOHDM | OOHDM | UWE | WAE | IWEB |
| DATOS               | x            | x     | x     | x   | x   | x    |
| INTERFAZ DE USUARIO |              | x     | x     | x   | x   | x    |
| NAVEGACIONALES      |              |       | x     | x   | x   | x    |
| PERSONALIZACION     | x            |       | x     |     |     |      |
| TRANSACCIONALES     |              | x     |       | x   |     |      |
| NO FUNCIONALES      | x            | x     | x     | x   | x   | x    |

**CUADRO 2-4. Comparación de Requisitos de Metodologías en el Entorno Web**

Fuente: Cuadro tomado del texto [23]

De acuerdo al CUADRO 2-4 se infiere que los métodos OOHDM y UWE son los más adaptables a la mayoría de proyectos de desarrollo de aplicaciones web. De los cuales “OOHDM está considerada como la más óptima para programadores y desarrolladores”. [23]

### 2.7.1. Método de Diseño de Hipermedia Orientado a Objetos (OOHDM)

OOHDM fue creado como una extensión del Modelo de Diseño de Hipermedia (HDM), y a diferencia de éste introduce el modelado orientado a objetos en el desarrollo de hipermedia.

En OOHDM se modela la navegación a través del diagrama de clases navegacionales y del diagrama de contextos.

Las etapas del método OOHDM son desarrolladas en un proceso de diseño incremental, iterativo y basado en prototipos.

Posee actividades separadas que permiten obtener diseños modulares y reusables.

Las etapas principales del método OOHDM son [23]:

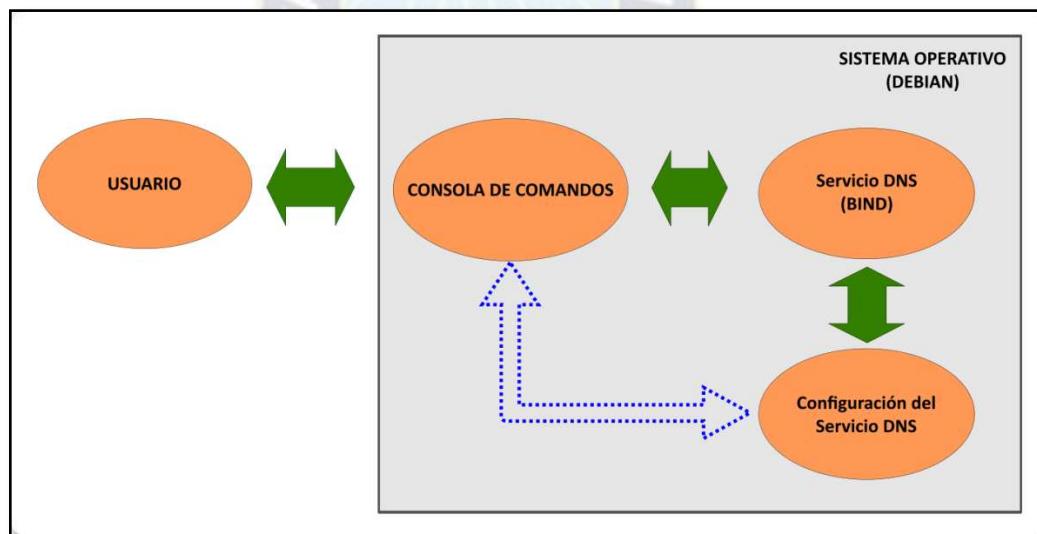
- **Obtención de Requerimientos:** se realiza de manera cuidadosa, tomando en cuenta los actores y tareas que se deben modelar en los casos de uso.
- **Diseño Conceptual:** es la construcción de un modelo del dominio de la aplicación, a través de técnicas de modelado orientado a objetos, que parte de un modelo E/R.
- **Diseño Navegacional:** en OOHDM, la navegación es considerada un paso crítico en el diseño de aplicaciones de hipertexto, es construido como una vista del modelo conceptual. El modelo navegacional está conformado por el diagrama de clases navegacionales y el diagrama de contextos navegacionales.
- **Diseño de Interfaz Abstracta:** en esta etapa se define la forma en la que serán percibidos los objetos a través de la interfaz de usuario y también la apariencia que tendrán. En OOHDM se utilizan vistas abstractas de datos (ADV). Mediante un ADV se representa la estructura estática de la interfaz, la composición de objetos y los eventos a los que responden.
- **Implementación:** es la última etapa, donde a partir de los modelos diseñados, se deben escoger las correspondencias con los objetos concretos de la plataforma de implementación. Por lo tanto, es una etapa totalmente dependiente de la plataforma de implementación escogida.

# Capítulo III: DESARROLLO DEL PROYECTO

## 3.1. Análisis e Identificación de Requerimientos

### 3.1.1. Requerimientos de Software

La administración del servicio DNS fundamentalmente necesita de la instalación del paquete que proporciona el servicio DNS denominado **BIND** y la **consola de comandos** del sistema operativo para su administración, sin embargo, para una interacción amigable, evitar cometer errores de sintaxis y facilitar su administración se requieren herramientas de software adicionales.



**FIGURA 3-1. Diagrama de Funcionamiento del Sistema de Administración por Consola de Comandos del Servicio DNS**

Fuente: Elaboración Propia

Para el desarrollo del proyecto es necesario contar con un sistema operativo y herramientas de software libre, la combinación a utilizar se denomina LAMP:

- L: Referida a una distribución de Linux. En este caso **Debian**.
- A: Servidor web **Apache**.
- M: Sistema gestor de bases de datos Mysql o MariaDB. En este caso **MariaDB**.
- P: Lenguaje de programación Perl, PHP o Python. En este caso **PHP**.

Estos componentes son utilizados principalmente para definir la infraestructura de un servidor web. Para el proyecto los componentes LAMP serán instalados de forma individual considerando que las versiones actualizadas y estables de cada componente ayudan a mejorar la seguridad del sistema. Adicionalmente al lenguaje del lado del servidor, como es PHP, se debe mencionar que los lenguajes de programación del lado del usuario que mejoran la interacción con el servidor, son: HTML, JavaScript y CSS.

Adicionalmente se debe instalar el software del servicio DNS a administrar, que para el presente caso es **BIND**, también se hará uso del paquete **openssl** para implementar el protocolo HTTP Seguro, para el intercambio de datos entre cliente y servidor web.

### 3.1.2. Requerimientos de Hardware

Debido a que el cálculo de requerimientos de hardware depende de factores como la redundancia requerida según la topología de la Red, también el número de clientes que solicitan servicios de DNS y considerando que por ejemplo para verificar que se haya escogido un tamaño adecuado de Memoria RAM según el manual de referencia de BIND [4] “...la mejor manera de determinar esto para una instalación dada es observar el servidor de nombres en funcionamiento ...”. Por lo tanto, se realizará algunas sugerencias para el correcto funcionamiento del servicio DNS en atención del *hardware* requerido, cuando se planea implementar DNSSEC en un servidor autoritativo y servidor recursivo.

#### Requisitos de un Servidor Recursivo [8]:

- **CPU:** la tarea de validación de un Registro de Recurso conlleva un mayor uso de CPU, a menos que el servidor tenga incorporado hardware para cálculos criptográficos.
- **Memoria RAM:** DNSSEC hace uso de respuestas más grandes debido a las firmas acompañantes por lo que se ocupará mayor espacio en memoria.

- **Interfaz de Red:** Es poco probable que se necesite actualizar la tarjeta de interfaz de red (NIC) a menos que se cuente con un hardware realmente obsoleto.

#### **Requisitos de un Servidor Autoritativo [8]:**

- **CPU:** con DNSSEC habilitado y considerando firmar una zona de forma periódica, conforme dicha periodicidad incrementa el uso de CPU.
- **Memoria en Disco:** una zona firmada es generalmente 3 veces más grande que una zona sin firmar.
- **Memoria RAM:** los archivos de zona firmados ocuparán más espacio en la memoria.
- **Interfaz de Red:** Es poco probable que se necesite actualizar la tarjeta de interfaz de red (NIC) a menos que se cuente con un hardware realmente obsoleto.

#### **3.1.3. Consideraciones en la Infraestructura de Red**

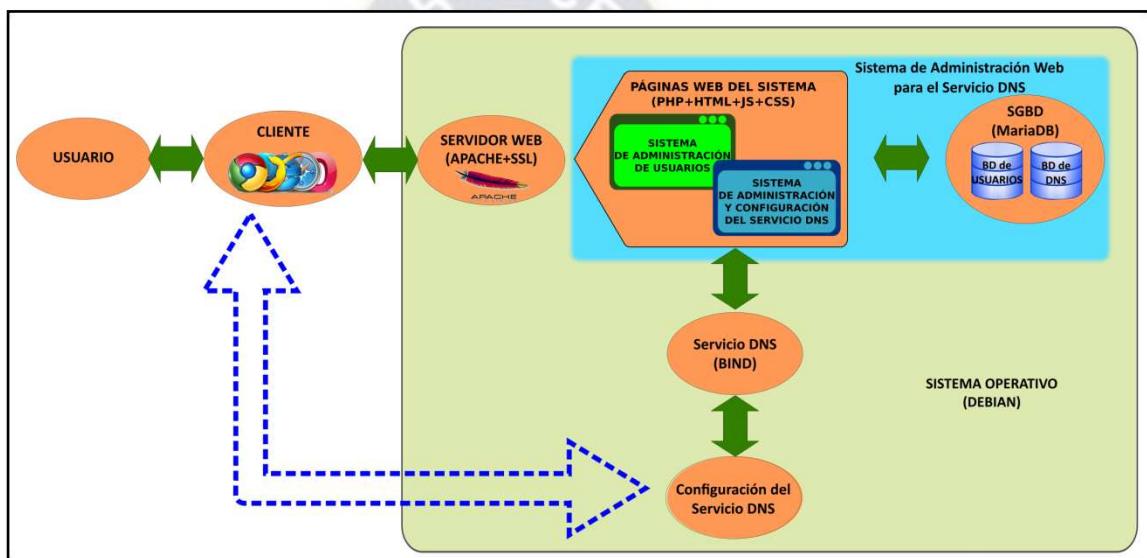
Debido a que los paquetes de DNSSEC son más grandes que un paquete DNS normal, es probable que en algunos casos se utilice TCP en lugar de UDP, durante las consultas. [8]

- **DNS sobre TCP:** se debe verificar la conectividad a través del puerto TCP 53, lo que podría implicar un cambio en la lista de control de acceso ACL o *firewall*
- **DNS sobre UDP:** un *firewall* puede suponer un tamaño para los paquetes UDP de DNS y rechazar paquetes DNSSEC debido a su mayor tamaño. Por lo tanto, se debe hacer una verificación durante una consulta con el objetivo de garantizar la respuesta.

### **3.2. Especificaciones del Sistema**

El desarrollo del sistema de administración del servicio DNS, requiere de la interacción sincronizada de los paquetes de software mediante los lenguajes de programación, y su funcionamiento requiere de la interoperabilidad, entre el Servidor web **Apache** (en la que interviene el uso de PHP, HTML, JavaScript y CSS, para su funcionamiento), el SGBD denominado **MariaDB**, el sistema operativo **Debian** y el paquete de software que administra el servicio DNS denominado **BIND**.

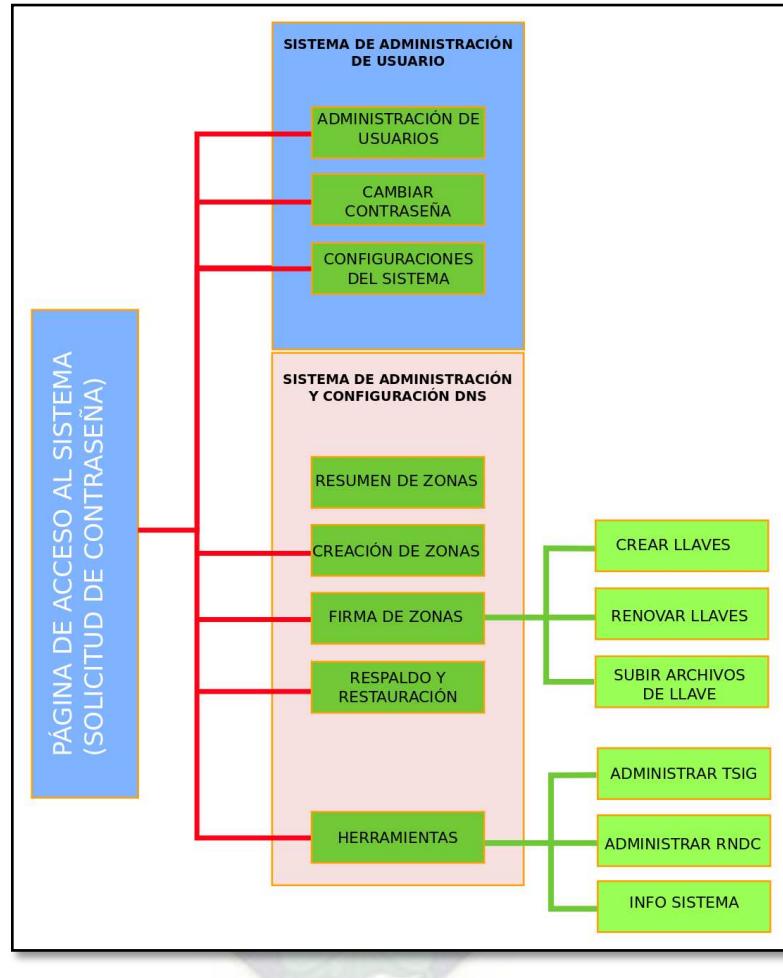
La interfaz de usuario está conformada por el **Sistema de Administración** y **Configuración del servicio DNS** y el **Sistema de Administración de Usuario**, donde cada uno cuenta con su propia Base de Datos (Véase FIGURA 3-2).



**FIGURA 3-2. Diagrama de Funcionamiento del Sistema de Administración Web para el Servicio DNS**

Fuente: Elaboración Propia

Asimismo la interrelación entre las páginas web visibles al usuario del sistema de administración se muestran a continuación:



**FIGURA 3-3. Jerarquía de Páginas Web del Sistema**

Fuente: Elaboración Propia

Los requerimientos del sistema se identifican en función de los atributos relacionados al Sistema de Administración de Usuarios y al Sistema de Administración y Configuración del Servicio DNS, los cuales se detallan a continuación:

**A. Atributos del Sistema de Administración de Usuarios:**

- i. Acceso al sistema por dirección IP o de red.
- ii. Acceso al sistema mediante autenticación por contraseña y prevención de ingresos de forma simultánea.
- iii. Registro y eliminación de usuarios del sistema.
- iv. Intercambio de datos seguro entre cliente y servidor web, mediante HTTPS.
- v. Cierre de sesión después de cierto tiempo de inactividad.
- vi. Copia de respaldo del sistema administración de usuarios.

**B. Atributos del Sistema de Administración y Configuración del Servicio DNS:**

- I. Creación, edición y eliminación de zonas maestras y esclavas; así como sus zonas directas e inversas, para servidores DNS autoritativos y configuración de clientes permitidos para consultas DNS.
- II. Configuración de servidores DNS recursivos, zonas de reenvío y soporte para el uso de direcciones IPv6.
- III. Copia de respaldo del sistema de administración y configuración de DNS.
- IV. Uso de transacciones firmadas entre servidores mediante TSIG.
- V. Uso de DNSSEC y respaldo de claves ZSK y KSK.
- VI. Uso de RNDC para tareas de monitoreo del estado del sistema y diagnóstico del servicio DNS.

### 3.3. Diseño de Ingeniería

#### 3.3.1. Diseño del Sistema de Administración de Usuarios

##### i. Acceso al Sistema por Dirección IP o de Red

A continuación, se desarrollan las etapas del método OOHD:

###### 1) Obtención de Requerimientos

Básicamente para restringir el acceso a la página web del sistema por dirección IP es necesario una pequeña base de datos que almacene las direcciones IP o de red. Así mismo se consulta a la BD de Usuarios, sobre los datos almacenados, para escribir en los archivos de configuración de Apache.

###### 2) Diseño Conceptual

Para la implementación del Acceso Restringido por IP, el sistema se apoya en una base de datos que almacena direcciones de red o de host IPv4 e IPv6. La base de datos está conformada por una entidad y un atributo, y no se relaciona con otras entidades.



**FIGURA 3-4. Entidad –Atributo para la BD de Restricción por IP**

Fuente: Elaboración propia

###### 3) Diseño Navegacional (diagrama de clases navegacionales y diagrama de contextos navegacionales)

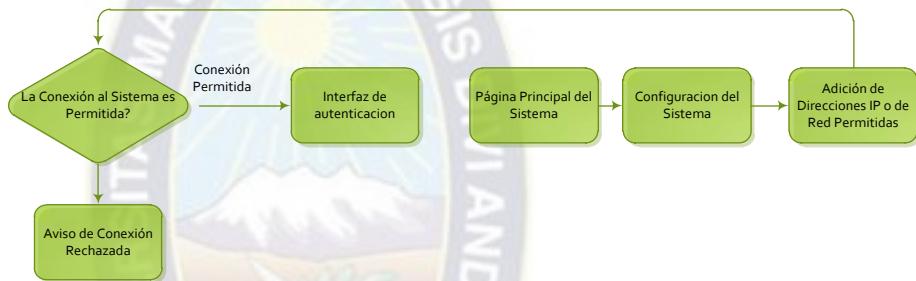
Modelo Relacional de la base de datos es la siguiente:

$$R1 \rightarrow IP\_Permitida(Id\_IP, Direccion\_IP\_Red)$$

En base al modelo relacional se puede expresar el diagrama de clases navegacionales y el diagrama de contextos navegacionales y estructuras de acceso como parte del diseño Navegacional.

| IP Permitida       |
|--------------------|
| id int(2)          |
| IP_Red varchar(42) |

**FIGURA 3-5. Diagrama de Clases Navegacionales para la Autenticación**  
Fuente: Elaboración propia



**FIGURA 3-6. Diagrama de Contextos Navegacionales para Autenticación**  
Fuente: Elaboración propia

#### 4) Diseño de Interfaz Abstracta e Implementación

La interfaz que simplifica los pasos anteriores, se muestra a continuación:

Lista de IPs Permitidas de Acceso al Servidor Web

Advertencia!: Agregar o Quitar Redes o IPs reinicia el servicio Apache2 por lo que sufre una desconexión y debe volver a cargar la página anterior.  
Soporta Redes y Direcciones IPv4 e IPv6

Ej.: 192.168.0.1

**FIGURA 3-7. Interfaz de Adición de Direcciones IP Permitidas**  
Fuente: Elaboración propia

Un ejemplo de las direcciones IP o de Red se muestra en el siguiente gráfico:

**Lista de IPs Permitidas de Acceso al Servidor Web**

**Advertencia!** Agregar o Quitar Redes o IPs reinicia el servicio Apache2 por lo que sufre una desconexión y debe volver a cargar la página anterior.  
Soporta Redes y Direcciones IPv4 e IPv6

|   |   |
|---|---|
| <input style="width: 100%;" type="text" value="Ej.: 192.168.0.1"/>  | <input style="background-color: #008000; color: white; border: none; padding: 2px 10px;" type="button" value="Añadir"/> |
| <b>192.168.100.0/24</b>   |   |
| <input style="background-color: #c00000; color: white; border: none; padding: 2px 10px;" type="button" value="Borrar"/> |   |
| <b>2001:db8:acad:1::/64</b>   |   |
| <input style="background-color: #c00000; color: white; border: none; padding: 2px 10px;" type="button" value="Borrar"/> |   |
| <b>192.168.200.10</b>   |   |
| <input style="background-color: #c00000; color: white; border: none; padding: 2px 10px;" type="button" value="Borrar"/> |   |

**FIGURA 3-8. Direcciones IP y de Red Permitidas para Acceder al Sistema**

Fuente: Elaboración propia



**FIGURA 3-9. Aviso de Permiso Denegado al Servidor**

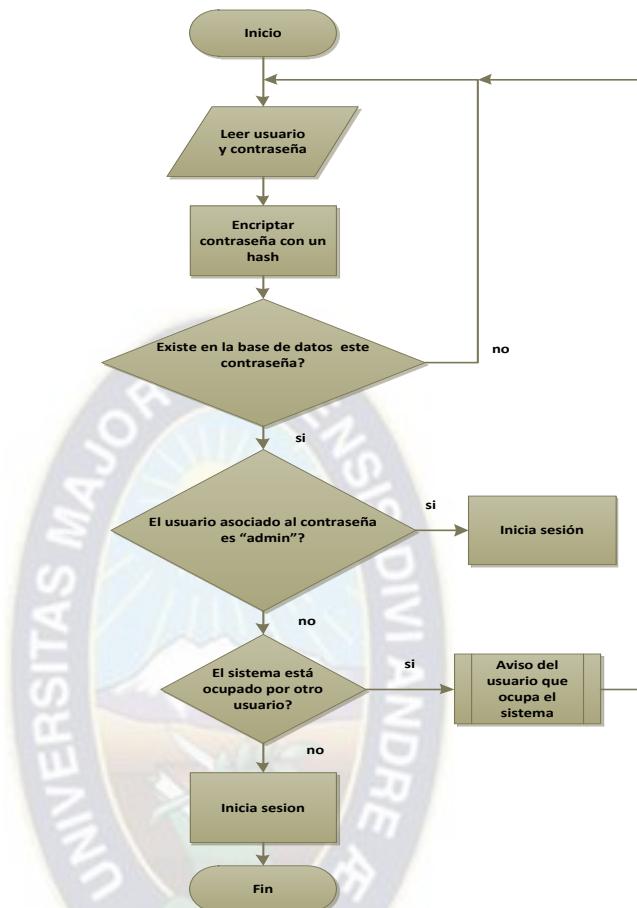
Fuente: Elaboración propia

**ii. Acceso al Sistema mediante Autenticación por Contraseña y Prevención de Ingresos de Forma Simultánea.**

A continuación, se desarrollan las etapas del método OOHDMD:

**1) Obtención de Requerimientos**

Se necesita un algoritmo que verifique la existencia de un usuario y su correspondiente contraseña.



**FIGURA 3-10. Algoritmo de Autenticación del Sistema**  
Fuente: Elaboración Propia

## 2) Diseño Conceptual

Durante la autenticación se emplea una BD para verificar el nombre de **usuario** y su respectiva **contraseña** y una BD adicional para informar sobre el **estado de uso** del sistema. Las bases de datos contienen una sola entidad en cada caso. A continuación, se muestra el modelo conceptual para las bases de datos mencionadas.



**FIGURA 3-11. Modelo Conceptual Usuarios**

Fuente: Elaboración propia

## 3) Diseño Navegacional (diagrama de clases navegacionales y diagrama de contextos navegacionales)

### Modelo Relacional

$$R_1 \rightarrow \text{Usuario}(\text{Nombre}, \text{usuario}, \text{contraseña})$$

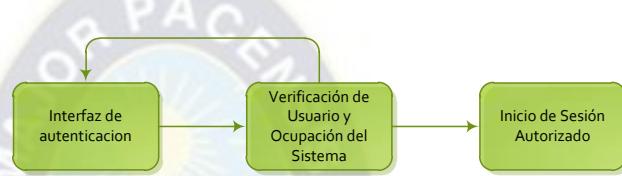
$$R_2 \rightarrow \text{VerificaUsuario}(\text{ocupado}, \text{usuario})$$

En base al modelo relacional se puede expresar el diagrama de clases navegacionales y el diagrama de contextos navegacionales y estructuras de acceso como parte del diseño Navegacional.

| verifusu                 | user                |
|--------------------------|---------------------|
| id INT(2)                | id INT(10)          |
| ocupado ENUM('no', 'si') | nombre VARCHAR(50)  |
| usuario VARCHAR(40)      | usuario VARCHAR(80) |
| Indexes                  | Indexes             |

**FIGURA 3-12. Diagrama de Clases Navegacionales para la Autenticación**

Fuente: Elaboración propia



**FIGURA 3-13. Diagrama de Contextos Navegacionales para Autenticación**

Fuente: Elaboración propia

#### 4) Diseño de Interfaz Abstracta e Implementación

Una vez diseñado el sistema de autenticación, corresponde la implementación en el lenguaje de programación PHP y su correspondiente sintaxis para interactuar con las bases de datos. El resultado de la página web de autenticación se muestra a continuación:

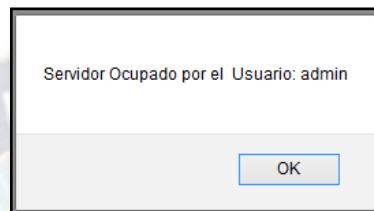
La captura de pantalla muestra una ventana de diálogo titulada "Administración del Servicio DNS". Dentro de esta ventana, se encuentra un formulario de "Login" con los siguientes campos y botones:

- Título: "Login"
- Campo de texto: "Nombre de usuario" (con placeholder "Nombre de usuario")
- Campo de texto: "Contraseña" (con placeholder "Contraseña")
- Botón: "Ver" (en azul)
- Botones de acción: "Acceder" (en verde) y "Cancelar" (en rojo)

**FIGURA 3-14. Interfaz de Autenticación de Usuarios**

Fuente: Elaboración propia

Cuando se detecta que otro usuario se encuentra utilizando el sistema, se informa oportunamente, el nombre de dicho usuario y se reenvía a la página de autenticación. A continuación, se muestra el mensaje informativo de estado de ocupación:



**FIGURA 3-15. Aviso de Ocupación por otro Usuario**  
Fuente: Elaboración propia

### iii. Registro y Eliminación de Usuarios del Sistema

Esta característica se apoya en la BD de Usuarios y las etapas previas ya diseñadas para su funcionamiento, y solamente resta su implementación.

En este caso el usuario por defecto es “**admin**” y posteriormente se pueden registrar y eliminar los demás usuarios que tendrán acceso al sistema, sin embargo, el usuario “**admin**” no es posible eliminarlo precautelando el mantener, al menos un acceso seguro al sistema de administración.



| Registrar Usuario                |            |
|----------------------------------|------------|
| Nombre                           | juan perez |
| Usuario                          | jperez     |
| Contraseña                       | *****      |
| Confirmar Contraseña             | *****      |
| <b>Registrar</b> <b>Cancelar</b> |            |

**FIGURA 3-16. Interfaz de Registro de Usuario**  
Fuente: Elaboración propia



**FIGURA 3-17. Interfaz de Eliminación de Usuario**

Fuente: Elaboración propia

**iv. Intercambio de datos seguro entre cliente y servidor web, mediante HTTPS**

Para habilitar HTTPS en el servicio web de **Apache**, es necesario instalar el paquete “**openssl**” sobre el sistema operativo Debian, para crear una clave (archivo con extensión “key”) y un certificado (con extensión “crt”), luego con estos dos componentes se habilita SSL en el servicio web de **Apache**, dicha configuración permitirá cifrar la comunicación entre el cliente y el servidor web.

La creación de claves para el servicio HTTPS en el Sistema Operativo **Debian**, tendría el siguiente formato:

```
openssl genrsa -out ssl.key 2048
openssl req -new -key ssl.key -out ssl.csr -subj
"/C=BO/ST=LAPAZ/L=LA PAZ/O=NOMBRE_EMPRESA/OU=TIC/CN=NOMBRE_HOST"
openssl x509 -req -days 3650 -in ssl.csr -signkey ssl.key -out
ssl.crt
cp ssl.crt /etc/ssl/certs/ssl.crt
cp ssl.key /etc/ssl/certs/ssl.key
a2enmod ssl
a2ensite default-ssl
```

**FIGURA 3-18. Ejemplo de Implementación de HTTPS por Consola**

Fuente: Elaboración propia



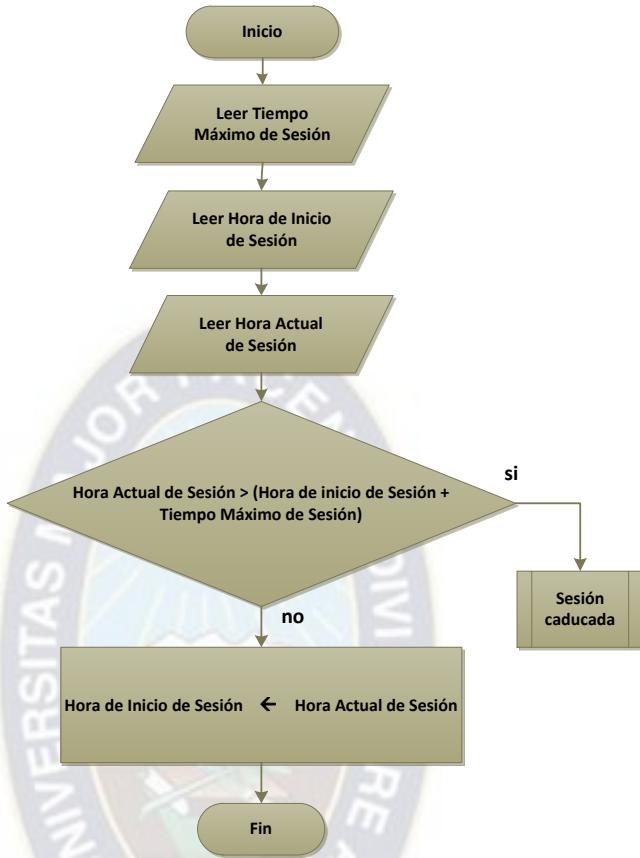
**FIGURA 3-19. Resultado de la Implementación de HTTPS**  
Fuente: Elaboración propia

v. **Cierre de Sesión después de Certo Tiempo de Inactividad.**

PHP dispone de herramientas de sesión y por medio de ellas permite configurar el cierre de sesión del sistema, donde una vez transcurrido el tiempo de inactividad configurado por el administrador, se cierra la sesión, evitando de esta manera el acceso de personas ajena al sistema y contribuyendo a su seguridad.

**1) Obtención de Requerimientos**

Se necesita un algoritmo que verifique si se excedió el tiempo de sesión establecido.



**FIGURA 3-20. Algoritmo de Cierre de Sesión por Inactividad**

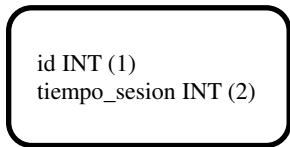
Fuente: Elaboración Propia

## 2) Diseño Conceptual

La característica de tiempo de sesión, está representado por una tabla de datos con un solo campo, perteneciente a la BD de Usuario, por lo cual, el diseño conceptual se limita a identificar una sola entidad llamada “**Tiempo de Sesión**”.

## 3) Diseño Navegacional

El diseño navegacional se basa en la entidad “**Tiempo de Sesión**” del diseño conceptual y se genera el **diagrama de clases navegacionales** y **diagrama de contextos navegacionales**:



**FIGURA 3-21. Diagrama de Clases Navegacionales para el Tiempo de Sesión**

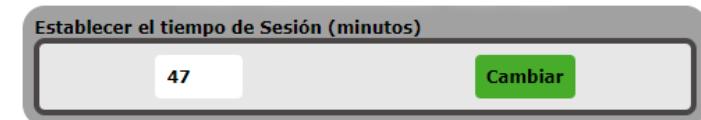
Fuente: Elaboración propia



**FIGURA 3-22. Diagrama de Contextos Navegacionales el Tiempo de Sesión**

Fuente: Elaboración propia

#### 4) Diseño de Interfaz Abstracta e Implementación



**FIGURA 3-23. Interfaz de Establecimiento del Tiempo de Sesión**

Fuente: Elaboración propia

#### vi. Copia de Respaldo del Sistema Administración de Usuarios

El diseño de la interfaz para realizar los respaldos y restauraciones de la del sistema de administración de Usuarios, se basa en una solicitud al gestor de base de datos, para la generación de un archivo con extensión “.sql” que incluye todas las tablas diseñadas que pertenecen a la BD de Usuarios. Los comandos utilizados mediante consola de comandos en **Debian**, para la generación de un respaldo, se reduce a presionar el botón “crear respaldo” y de forma análoga el botón “Restaurar” para

recuperar la configuración de la BD de Usuarios, como se muestra a continuación:



**FIGURA 3-24. Interfaz para Generar Copias de Respaldo de la Base de Datos de Usuario**

Fuente: Elaboración propia

Adicionalmente si se requiere respaldar los datos en un almacenamiento externo o si se desea replicar dicha configuración en otro servidor, se utilizan los botones “Down sql” para descargar y “Subir Archivo sql” para cargar la configuración deseada en el mismo u otro servidor.

### 3.3.2. Diseño del Sistema de Administración y Configuración del Servicio DNS

#### I. Creación, Edición y Eliminación de Zonas Maestras y Esclavas; así como sus Zonas Directas e Inversas, para Servidores DNS Autoritativos y Configuración de Clientes Permitidos para Consultas DNS

El diseño de una zona maestra directa, es bastante similar al de una zona maestra inversa y más completa en atributos que una zona esclava, por lo cual, su desarrollo bastaría para explicar también el diseño de una zona maestra inversa y las zonas esclavas.

A continuación, se desarrollan las etapas del método OOHDM para una Zona Maestra Directa:

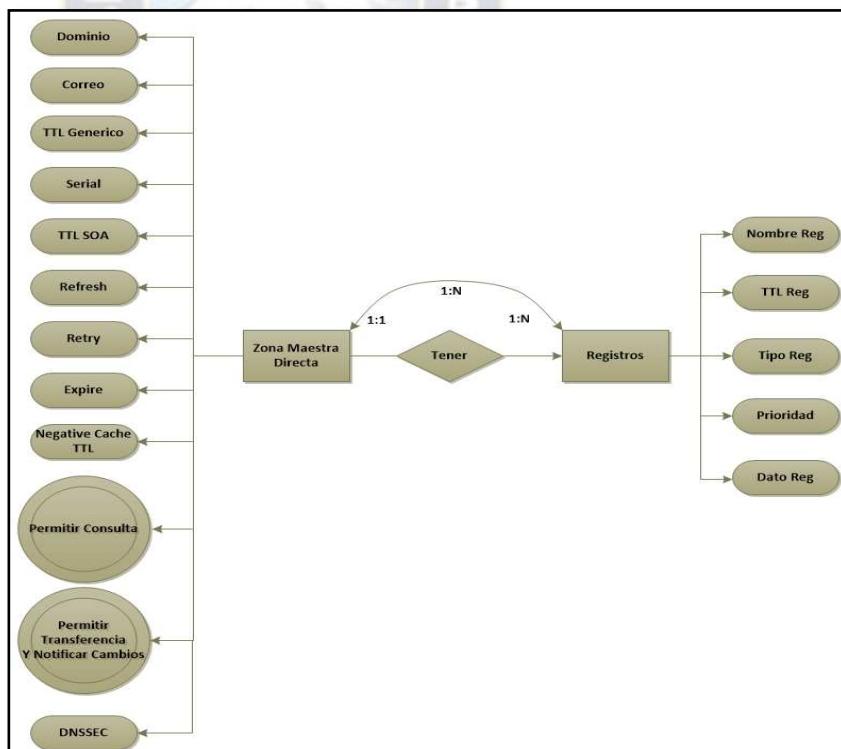
## 1) Requerimientos

Una **zona maestra directa** es una entidad compuesta de varios atributos que se almacenan en el archivo de zona, tales como: Nombre de dominio, Correo electrónico, *serial*, TTL genérico, TTL SOA, *Refresh*, *Retry*, *Expire*, *Negative caché TTL*.

Cada zona almacena **registros** sobre los que tiene autoridad, y cada uno de ellos está compuesto por atributos característicos, tales como: Nombre de Registro, TTL, Tipo, Prioridad y Dato.

## 2) Diseño Conceptual

Una vez identificadas las entidades y sus atributos se pueden construir las relaciones e implementarlas en el sistema. A continuación, se muestra la construcción de la base de datos de la zona maestra directa del sistema:



**FIGURA 3-25. Modelo Conceptual de la Zona Maestra Directa**

Fuente: Elaboración propia

### 3) Diseño Navegacional

Modelo Relacional:

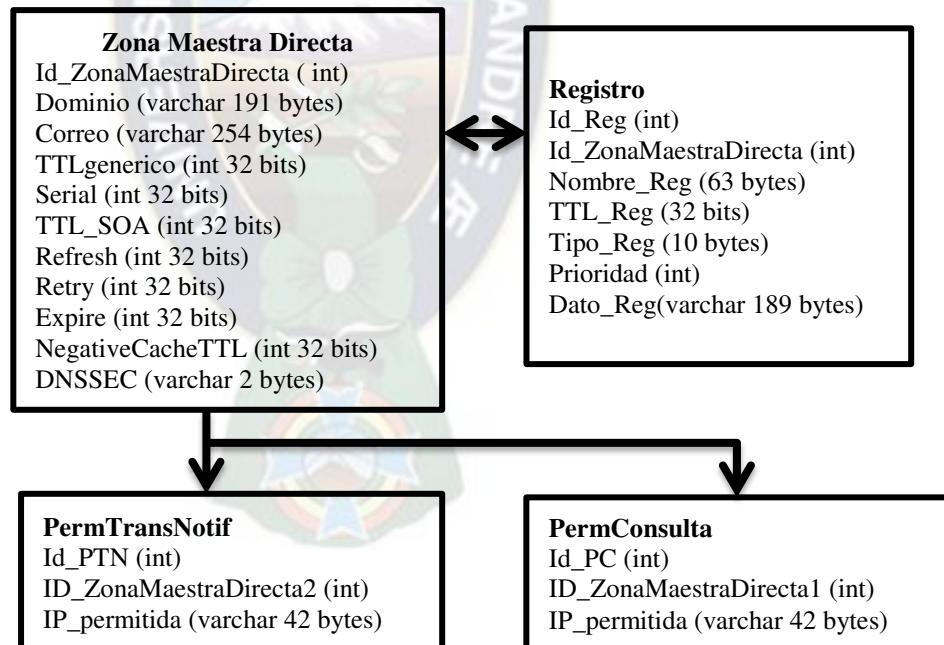
*R1 → ZonaMaestraDirecta (Id\_ZonaMaestraDirecta, Dominio, Correo, TTLgenerico, Serial, TTL\_SOA, Refresh, Retry, Expire, NegativeCacheTTL, DNSSEC)*

*R2 → Registro(Id\_Reg, NombreReg, TTL\_Reg, Tipo\_Reg, Prioridad, Dato\_Reg)*

*R3 → PermConsulta(Id, Id\_ZonaMaestraDirecta1, ip\_permitida)*

*R4 → PermTransfNotif(Id, Id\_ZonaMaestraDirecta2, ip\_permitida)*

En base al modelo relacional se puede expresar el diagrama de clases navegacionales y el diagrama de contextos navegacionales.



**FIGURA 3-26. Diagrama de Clases Navegacionales para la Zona Maestra Directa**

Fuente: Elaboración propia



**FIGURA 3-27. Diagrama de Contextos Navegacionales para Zona Maestra Directa**

Fuente: Elaboración propia

#### 4) Diseño de Interfaz Abstracta e Implementación



**FIGURA 3-28. Interfaz de Creación de Zonas**

Fuente: Elaboración propia

**Zona Maestra Directa**

|                          |                        |
|--------------------------|------------------------|
| Dominio:                 | Ej.: dominio.com.      |
| Correo admin:            | Ej.: mail.dominio.com. |
| TTL genérico[seg]:       | 604800                 |
| TTL SOA[seg]:            | 604800                 |
| Refresh[seg]:            | 604800                 |
| Retry[seg]:              | 86400                  |
| Expire[seg]:             | 2419200                |
| Negative Cache TTL[seg]: | 604800                 |

**FIGURA 3-29. Interfaz de Creación de Zona Maestra Directa**  
 Fuente: Elaboración propia

**Resumen de zonas**

| Zona Maestra - Directa                   |        |        |           |
|--|--------|--------|-----------|
| dominio1.com.                            | Editar | Borrar | Descargar |
| Zona Maestra - Inversa                   |        |        |           |
| dominio1.com. (100.168.192.in-addr.arpa) | Editar | Borrar | Descargar |
| Zona Esclava - Directa                   |        |        |           |
| Zona Esclava - Inversa                   |        |        |           |
| Zonas de Reenvío                         |        |        |           |
| otrodominio.com. (192.168.200.100)       | Editar | Borrar |           |

**FIGURA 3-30. Interfaz de Edición y Eliminación de Zonas**  
 Fuente: Elaboración propia

**Zona Maestra Directa**

|                          |   |
|--------------------------|---|
| Dominio:                 | dominio1.com.                                   |
| Correo admin:            | <input type="text" value="mail.domonio1.com."/> |
| TTL genérico(seg):       | <input type="text" value="604800"/>             |
| TTL SOA(seg):            | <input type="text" value="604800"/>             |
| Serial(seg):             | <input type="text" value="1"/>                  |
| Refresh(seg):            | <input type="text" value="604800"/>             |
| Retry(seg):              | <input type="text" value="86400"/>              |
| Expire(seg):             | <input type="text" value="2419200"/>            |
| Negative Cache TTL(seg): | <input type="text" value="604800"/>             |

| Nombre                                    | TTL                                    | Tipo de Registro  | Prioridad (MX)                                  | Dato de Registro |
|---|--|---|---|------------------|
| <input type="text" value="Ej.: www, ns"/> | <input type="text" value="Ej.:86400"/> | <input style="width: 20px; height: 20px; border: none; border-bottom: 1px solid black;" type="text" value="A"/> | <input type="text" value="Ej.: 192.168.100.1"/> | <b>Insertar</b>  |

|                 |                |              |
|-----------------|----------------|--------------|
| <b>permisos</b> | <b>Guardar</b> | <b>Salir</b> |
|-----------------|----------------|--------------|

**FIGURA 3-31. Interfaz de Edición de Zona Maestra Directa y Adición de Registros**

Fuente: Elaboración propia

**Permisos Zona Maestra Directa**

|  |                 |
|--|-----------------|
| Redes permitidas para Consultas                          | <b>Insertar</b> |
| <input type="text" value="Ej.:any.none, 192.168.0.0/2"/> |                 |
| IPs Esclavos   | <b>Insertar</b> |
| <input type="text" value="Ej.:any.none, 192.168.0.10"/>  |                 |

|                             |
|-----------------------------|
| <b>Volver a Editar Zona</b> |
|-----------------------------|

**FIGURA 3-32. Interfaz de Permisos de la Zona Maestra Directa**

Fuente: Elaboración propia

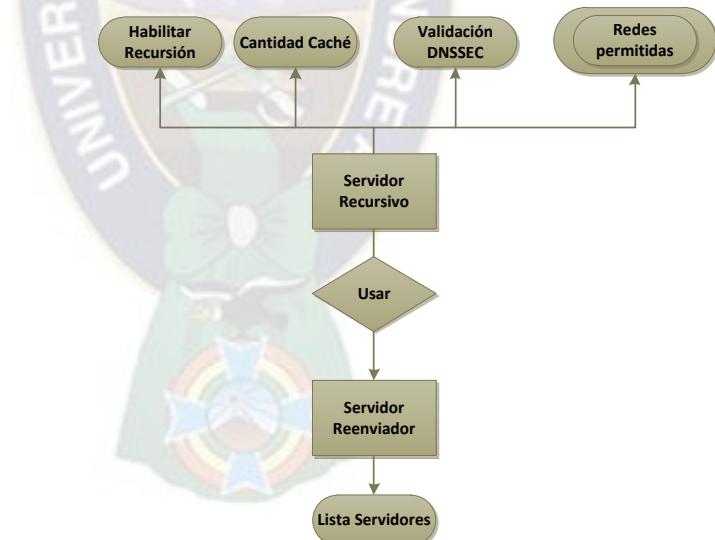
## **II. Configuración de Servidores DNS Recursivos, Zonas de Reenvío y Soporte para el Uso de Direcciones IPv6.**

## **1) Obtención de Requerimientos**

El servidor recursivo debe contar con las siguientes opciones:

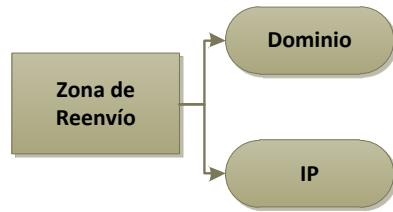
- Opción de Activación y Desactivación.
  - Configuración del tamaño de la memoria caché.
  - Habilitar la validación de DNSSEC para las consultas.
  - Opción para uso de un servidor reenviador.
  - Redes permitidas para consultas.

## 2) Diseño Conceptual



## **FIGURA 3-33. Modelo Conceptual del Servidor Recursivo**

Fuente: Elaboración propia



**FIGURA 3-34. Modelo Conceptual de la Zona de Reenvío**

Fuente: Elaboración propia

### 3) Diseño Navegacional

Modelo Relacional para Servidor Recursivo:

$$R_1 \rightarrow Recursivo(idrec, habilitar, cache, validacion)$$

$$R_2 \rightarrow Permisos\_Recursion(id\_perm, idrec2, permitidos)$$

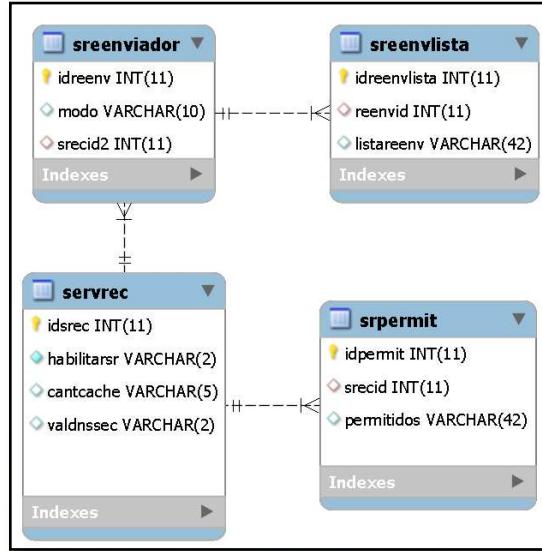
$$R_3 \rightarrow Serv\_Reenviador(id\_reenv, idrec3, modo)$$

$$R_4 \rightarrow serv\_reenv\_lista(id\_lista, id\_reenv1, listareenv)$$

Modelo Relacional para Zona de Reenvío:

$$R_1 \rightarrow Zona\_Reenvio(dominio, IP\_Reenvio)$$

En base al modelo relacional se puede expresar el diagrama de clases navegacionales y el diagrama de contextos navegacionales y estructuras de acceso como parte del diseño Navegacional.



**FIGURA 3-35. Diagrama de Clases Navegacionales para el Servidor Recursivo**

Fuente: Elaboración propia



**FIGURA 3-36. Diagrama de Clases Navegacionales para la Zona de Reenvío**

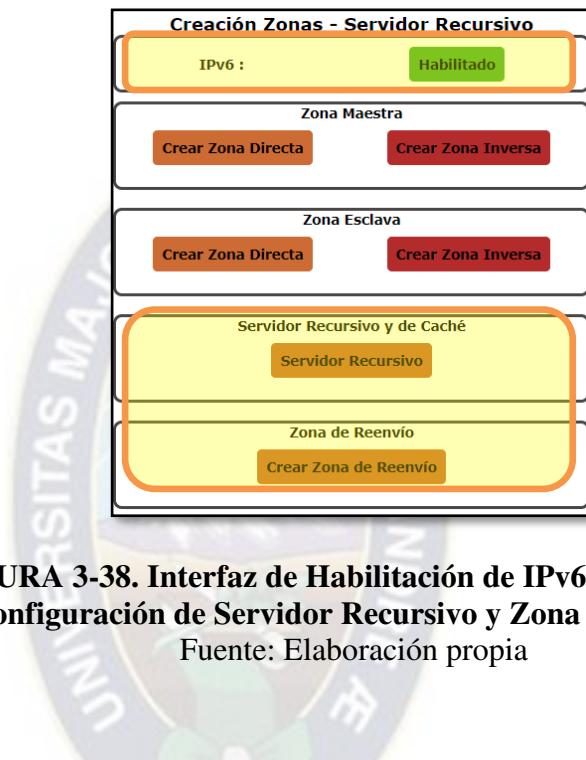
Fuente: Elaboración propia



**FIGURA 3-37. Diagrama de Contextos Navegacionales para Servidor Recursivo y Zona de Reenvío**

Fuente: Elaboración propia

#### 4) Diseño de Interfaz Abstracta e Implementación



**FIGURA 3-38. Interfaz de Habilitación de IPv6 y Acceso a la Configuración de Servidor Recursivo y Zona de Reenvío**

Fuente: Elaboración propia

**Servidor Recursivo y de Caché**

habilitar como servidor recursivo?  
si (Resuelve dominios externos)

Tamaño de caché [MB] (por defecto es ilimitado):  
Ej.:2

habilitar validacion dnssec?  
si (Valida respuestas con dn)

Reenviar consultas a servidor reenviador?  
no (Este servidor resuelve la)

Redes Permitidas para la Recusión  
Ej.:any, none, 192.168.100. Insertar

Lista de IPs de Servidores reenviadores  
Ej.:192.168.0.100. Insertar

Salir Descargar Guardar

**FIGURA 3-39. Interfaz de Configuración de Servidor Recursivo**

Fuente: Elaboración propia

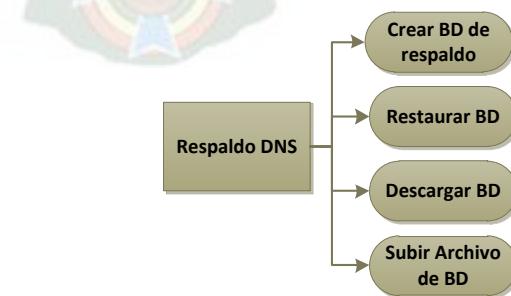
**FIGURA 3-40. Interfaz de Creación de Zona de Reenvío**  
Fuente: Elaboración propia

### III. Copia de Respaldo del Sistema de Administración y Configuración de DNS.

#### 1) Obtención de Requerimientos

- El sistema de administración y configuración debe tener la capacidad de generar una copia de la BD que contenga los valores de configuración que están directamente relacionados con el dominio, y asignarle un nombre distintivo a dicha copia.
- Debe ser capaz de realizar la Restauración de la configuración con la BD generada anteriormente.
- También debe poder exportarse hacia un almacenamiento externo y así mismo recuperarlo desde dicho lugar.

#### 2) Diseño Conceptual



**FIGURA 3-41. Modelo Conceptual para Realizar Respaldos del Sistema de Administración y Configuración de DNS**  
Fuente: Elaboración propia

### 3) Diseño Navegacional

El Diagrama de Clases Navegacionales, no necesita representación debido a que se trabaja con archivos y no con clases de datos.



**FIGURA 3-42. Diagrama de Contextos Navegacionales para Servidor Recursivo y Zona de Reenvío**

Fuente: Elaboración propia

### 4) Diseño de Interfaz Abstracta e Implementación



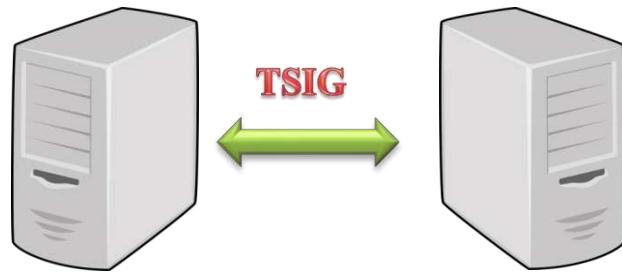
**FIGURA 3-43. Interfaz de Respaldo de la Base de Datos del Sistema DNS**

Fuente: Elaboración propia

## IV. Uso de Transacciones Firmadas entre Servidores mediante TSIG

### 1) Obtención de Requerimientos

Después que el servicio DNS se encuentra activo, las comunicaciones entre el servidor primario y secundario, pueden ser protegidas firmando los paquetes entre ambos, mediante el uso de una clave TSIG compartida.

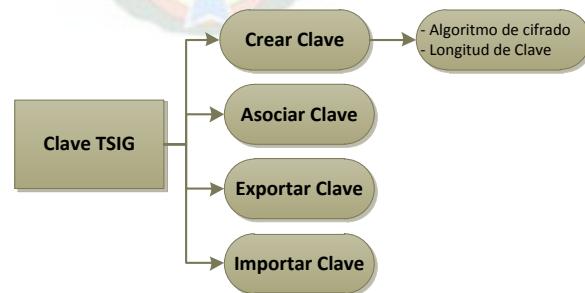


**FIGURA 3-44. Firma de Transacciones mediante TSIG**  
Fuente: Elaboración propia

Para la implementación se debe realizar la configuración para cada par de servidores. A continuación, se muestran los requerimientos para su implementación:

- Debe tener la capacidad de generar una clave TSIG con un algoritmo de cifrado.
- Debe ser capaz de **asociar** la clave TSIG generada, con la dirección IP que corresponde al servidor con quien se realizarán las transacciones.
- Debe poder exportarse hacia un almacenamiento externo, con el fin copiar la clave TSIG en el otro servidor y así mismo importar una clave TSIG y cargarla al sistema, en caso de que la clave TSIG compartida haya sido creada por otro servidor.

## 2) Diseño Conceptual



**FIGURA 3-45. Modelo Conceptual para la Creación de Claves TSIG**  
Fuente: Elaboración propia

### 3) Diseño Navegacional

El Diagrama de Clases Navegacionales, no necesita representación debido a que se trabaja con archivos de claves y algoritmos, y no con clases de datos.



**FIGURA 3-46. Diagrama de Contextos Navegacionales para la Configuración y Uso de TSIG**

Fuente: Elaboración propia

### 4) Diseño de Interfaz Abstracta e Implementación

Una clave TSIG se crea con valores predeterminados, donde el algoritmo es hmac-sha256 y una longitud de clave de 256 bits, generando el siguiente resultado:

```
key "tsig_key1" {
    algorithm hmac-sha256;
    secret "0jhgfASptfPGWe2NdJkOrgWl+sflGFaQGFj3fMjPwsM=";
};
```

**FIGURA 3-47. Ejemplo de Clave TSIG Creada**

Fuente: Elaboración propia

Dónde:

- *tsig\_key1* es el nombre de la clave TSIG.
- *hmac-sha256* es el algoritmo utilizado para crear la clave, y
- *"0jhgfASp...PwsM="* es el contenido de la clave creada.

La interfaz del sistema para la Creación de una clave se muestra a continuación:



**FIGURA 3-48. Interfaz de Creación de una Clave TSIG**

Fuente: Elaboración propia

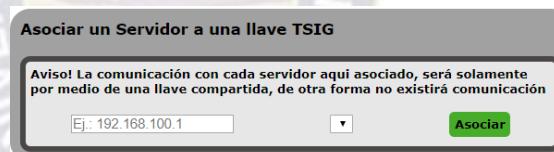
Para crear una clave, se debe anotar un nombre de clave y presionar el botón “CREAR TSIG” y la clave se crea automáticamente, como se muestra a continuación:



**FIGURA 3-49. Clave Creada para Transacciones Firmadas entre Servidores**

Fuente: Elaboración propia

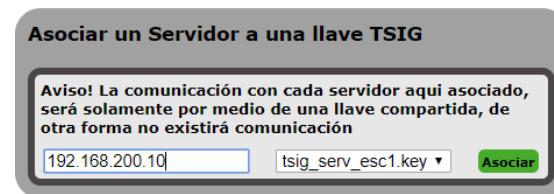
La interfaz del sistema para la Asociación de un Servidor a una Clave se muestra a continuación:



**FIGURA 3-50. Interfaz de Asociación de un Servidor con una Clave TSIG**

Fuente: Elaboración propia

Para asociar una dirección IPv4 o IPv6 se anota dicha dirección y junto a ella se debe seleccionar de una lista desplegable la clave creada, luego se presiona el botón “ASOCiar”, como se muestra a continuación:



**FIGURA 3-51. Asociación de la Dirección IP con una Clave TSIG creada**

Fuente: Elaboración propia

De esta operación resulta un vínculo entre la IP del Servidor Secundario con una Clave TSIG, como se muestra en la siguiente imagen:



**FIGURA 3-52. Asociación de la IP del Servidor Externo con la clave TSIG.**

Fuente: Elaboración propia

## V. Uso de DNSSEC y Respaldo de Claves ZSK y KSK.

### 1) Obtención de Requerimientos

Los atributos necesarios para la implementación de DNSSEC son:

- Crear y Eliminar Claves ZSK y KSK.
- Renovar Claves ZSK y KSK.
- Firmar una Zona con las claves creadas.
- Quitar Firma de Zona.
- Exportar e Importar una Clave ZSK o KSK.
- Opción de Uso de NSEC o NSEC3.

### 2) Diseño Conceptual

#### Creación de Claves

La firma de zona implica la creación de un par de claves ZSK y un par de claves KSK. Es decir, que tanto para ZSK y KSK, existe una clave privada y una clave pública respectivamente.

Para la creación de claves ZSK y KSK se toma en cuenta dos atributos esenciales:

- **Tipo de Algoritmo:** RSASHA256, RSASHA512, ECDSAP256SHA256 y ECDSAP384SHA 384.

- **Longitud de Clave:** de 1024 a 4096 bits.

Los comandos de creación de una clave ZSK, considerando un algoritmo y una longitud, es la siguiente:

```
dnssec-keygen -a algoritmo_zsk -b longitud_zsk nombre_clave_zsk
```

El comando para la creación de una clave KSK, se muestra a continuación:

```
dnssec-keygen -a algoritmo_ksk -b longitud_ksk -f KSK  
nombre_clave_ksk
```

Para la creación de los registros DS intervienen dos algoritmos: SHA-1 y SHA-256, según los requerimientos de la zona padre será cargado uno de ellos. Los comandos para crear los registros DS de acuerdo al algoritmo son:

```
dnssec-dsfromkey -a SHA-1 Kejemplo.com+008+62979.key
```

```
dnssec-dsfromkey -a SHA-256 Kejemplo.com+008+62979.key
```

### **Renovación de claves**

La renovación de claves es algo más compleja que la creación, debido a que se trabaja con los metadatos de sincronización de las claves.

Se debe tomar en cuenta la frecuencia de renovación y la longitud mínima de claves recomendables.

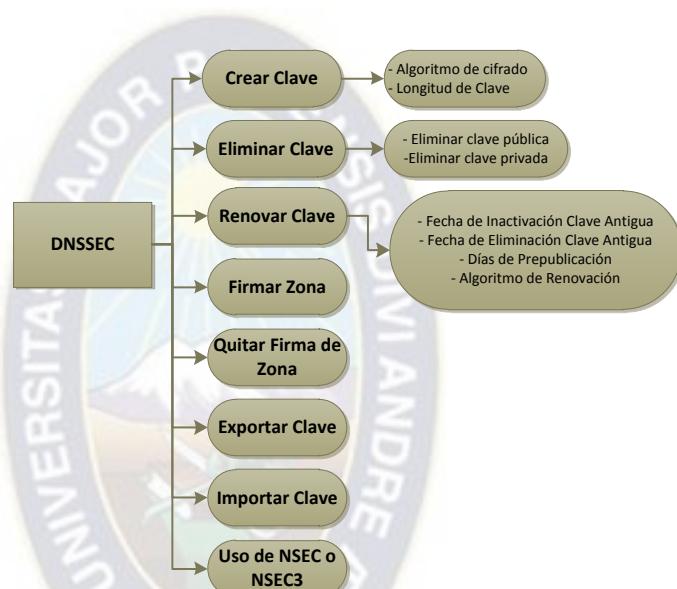
Los comandos necesarios para Heredar los parámetros de la clave actual a una nueva clave, son los siguientes:

```
dnssec-settime -I Fecha_Inactivación -D Fecha_Eliminación  
Nombre_Dominio dnssec-keygen -i Días_Prepública -S  
Nombre_Clave_Para_Renovar
```

Para crear una clave con un algoritmo y longitud nuevos, el comando es el siguiente:

`dnssec-keygen -a Algoritmo_Clave -b Longitud_Clave -i  
 Días_Prepublishación -A Fecha_Activación Nombre_Dominio`

A continuación, se muestra el modelo conceptual resultante:



**FIGURA 3-53. Modelo Conceptual para el Uso de DNSSEC**  
 Fuente: Elaboración propia

### 3) Diseño Navegacional

El Diagrama de Clases Navegacionales, no necesita representación debido a que no se trabaja con clases de datos.



**FIGURA 3-54. Diagrama de Contextos Navegacionales para Uso de DNSSEC y Firma de Zonas**  
Fuente: Elaboración propia

### 4) Diseño de Interfaz Abstracta e Implementación

La interfaz de creación y renovación de claves se muestra a continuación:



**FIGURA 3-55. Interfaz para la Firma de Zonas con DNSSEC e Importación de Claves**  
Fuente: Elaboración propia

En la figura anterior también se puede importar una clave mediante la opción **Subir Key**.

El procedimiento de creación de claves ZSK y KSK mediante la interfaz web se muestra a continuación:

**Crear Llave ZSK**

Algoritmo:

Longitud de Llave:

**Crear ZSK**

**Crear Llave KSK**

Algoritmo:

Longitud de Llave:

**Crear KSK**

## **FIGURA 3-56. Interfaz de Creación de Claves ZSK y KSK**

Fuente: Elaboración propia

Una vez que se elige el Algoritmo y la Longitud, se presiona el botón “Crear ZSK”.

Para la creación de la clave KSK se efectúa el mismo procedimiento. El resultado son un par de claves ZSK y un par de claves KSK:

| Llaves Creadas para "ejemplo.com." |  |
|------------------------------------|--|
| ZSK: Kejemplo.com.+008+62979.key   | <button>Borrar</button> <button>Descargar</button> |
| KSK: Kejemplo.com.+008+08491.key   | <button>Borrar</button> <button>Descargar</button> |

**FIGURA 3-57. Claves Creadas para el Dominio “ejemplo.com” con la Opción de ser Eliminadas y Exportadas**

Fuente: Elaboración propia

En figura anterior se puede apreciar las opciones de **Eliminación** de Clave y la opción de **Descargar** la clave para su respaldo, y exportarla a un almacenamiento externo como medida de seguridad.

Durante este proceso también se descargan los **Registros DS** que se deben proveer a la **Zona Padre “.gob.bo”**.

La firma de una zona se puede verificar visualmente mediante un indicador de color verde, como se muestra a continuación:



**FIGURA 3-58. Indicador de Firma de Zona que Expresa que la Zona “ejemplo.com” está Firmada**  
Fuente: Elaboración propia

A continuación, se ejemplifica la renovación de una clave KSK considerando que a diferencia de una clave ZSK, se generan los registros DS para cargar en la zona Padre.

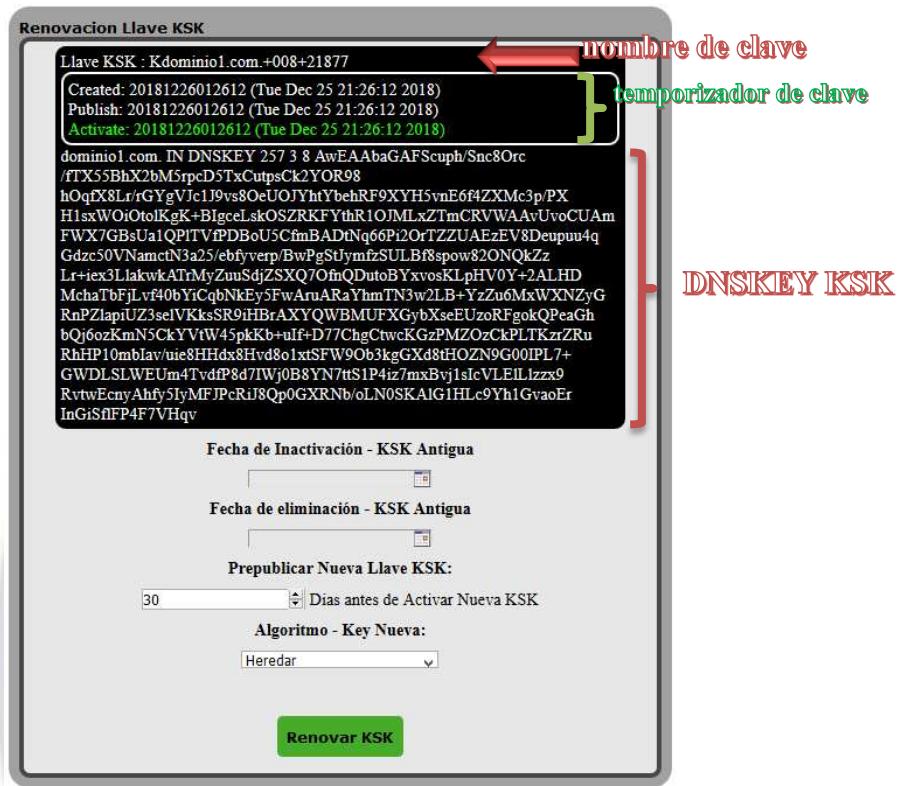
Para la renovación de claves se presiona el botón Renovar Claves de la interfaz de firma de Zona:

## Firma de Zonas con DNSSEC

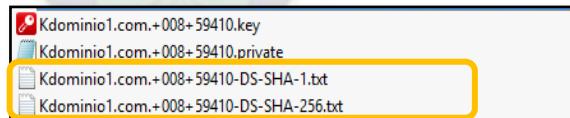


**FIGURA 3-59. Interfaz de Firma de Zona**  
Fuente: Elaboración propia

Para la renovación de claves, son necesarios los datos de “Fecha de Inactivación” y “Fecha de Eliminación” de la clave KSK actual y se recomienda 30 días de Prepublicación. Además, se puede heredar los atributos de la clave antigua o asignar un nuevo algoritmo y longitud de clave.



**FIGURA 3-60. Interfaz de Renovación de Clave KSK**  
Fuente: Elaboración propia



**FIGURA 3-61. Muestra de los Archivos que Contienen los Registros DS para Enviar a la Zona Principal o Zona Padre**  
Fuente: Elaboración propia

## VI. Uso de RNDC para Tareas de Monitoreo del Estado del Sistema y Diagnóstico del Servicio DNS.

El servicio DNS puede ser administrado de modo local y de modo remoto, con la ayuda de RNDC (*Remote Name Daemon Control*), a través de una clave que

debe ser copiada en el archivo de configuración del equipo local y equipos remotos. En este caso por motivos de seguridad, RNDC se encuentra configurado de forma local y deshabilitado para la administración remota de DNS, debido a que el servicio web proporciona el servicio de administración remota con las medidas de seguridad necesarias.

### 1) Obtención de Requerimientos

Las tareas básicas que realiza el sistema a través de RNDC, para la administración del servicio DNS, son:

- Iniciar el servicio DNS.
- Detener el servicio DNS.
- Reiniciar el servicio DNS.
- Cargar cambios en la configuración DNS sin reiniciar el sistema, para conservar el contenido de consultas de la memoria caché.

Otras herramientas de diagnóstico para resolución de problemas incluyen:

- Registros del sistema relacionados con el servicio DNS.
- Estado del sistema: Hora del Sistema, Tiempo de Servicio, Estado de los Recursos de Hardware, Información de la Red y Estado de la Red.
- Búsqueda de errores de contenido, en los archivos de configuración de zonas maestras y archivos de configuración del servicio DNS.

RNDC está implícito en las tareas de guardado de datos, cambios en la configuración de zona, adición de registros, permisos de zona, y también forma parte de las herramientas del sistema que permiten realizar parte de las tareas de forma manual, con el fin de verificar el funcionamiento y resolución de errores de contenido, en la configuración.

Para su implementación y configuración en el servicio DNS se debe generar una clave y configurar en un archivo, como se muestra a continuación:

```

key "rndc-key" {
    algorithm hmac-md5;
    secret "ZMm8z4e8GTO+1AvsFwWg8A==";
};

```

**FIGURA 3-62. Configuración de Clave para RNDC**

Fuente: Elaboración propia

Luego la clave creada se añade en la configuración que controla el acceso a la administración del servicio DNS:

```

controls {
    inet 127.0.0.1 port 953
    allow { 127.0.0.1; } keys { "rndc-key"; };
    inet ::1 port 953
    allow { ::1; } keys { "rndc-key"; };
};

```

**FIGURA 3-63. Configuración de Restricciones para RNDC**

Fuente: Elaboración propia

## 2) Diseño Conceptual



**FIGURA 3-64. Modelo Conceptual del Uso de RNDC**

Fuente: Elaboración propia



**FIGURA 3-65. Modelo Conceptual de Herramientas de Diagnóstico del Servicio DNS**

Fuente: Elaboración propia

### 3) Diseño Navegacional

El Diagrama de Clases Navegacionales, no necesita representación debido a que no se trabaja con clases de datos.



**FIGURA 3-66. Diagrama de Contextos Navegacionales para el Uso de RNDC**

Fuente: Elaboración propia

#### 4) Diseño de Interfaz Abstracta e Implementación

La interfaz para la administración del servicio DNS, se muestra a continuación:



**FIGURA 3-67. Interfaz de Estado del Servicio DNS y Ventana de Resultado**

Fuente: Elaboración propia



**FIGURA 3-68. Interfaz de Estado del Sistema DNS**

Fuente: Elaboración propia



**FIGURA 3-69. Interfaz de Verificación de Archivos de Zona y Configuración**

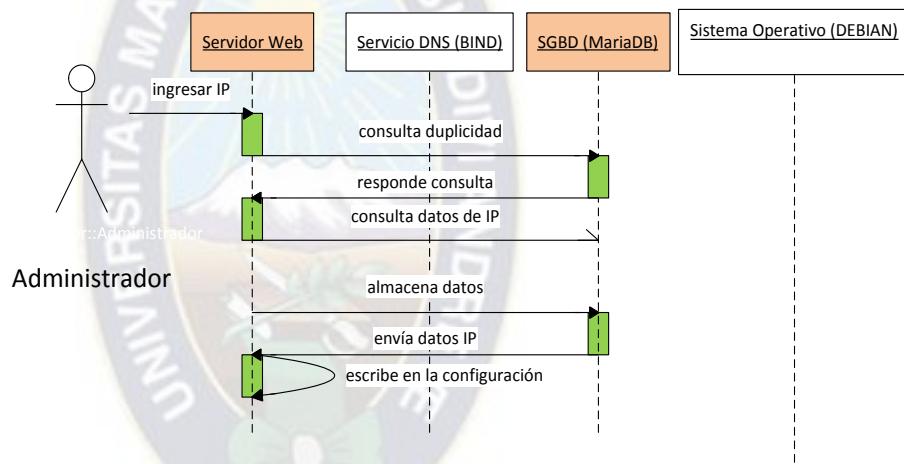
Fuente: Elaboración propia

### 3.3.3. Diagramas de Secuencia del Sistema

Los diagramas de secuencia ayudan a visualizar el funcionamiento de las características del sistema durante su ejecución, y de manera implícita, muestran los actores y procedimientos que se tomaron en cuenta durante el desarrollo del sistema.

#### 3.3.3.1. Diagramas de Secuencia del Sistema de Administración de Usuarios

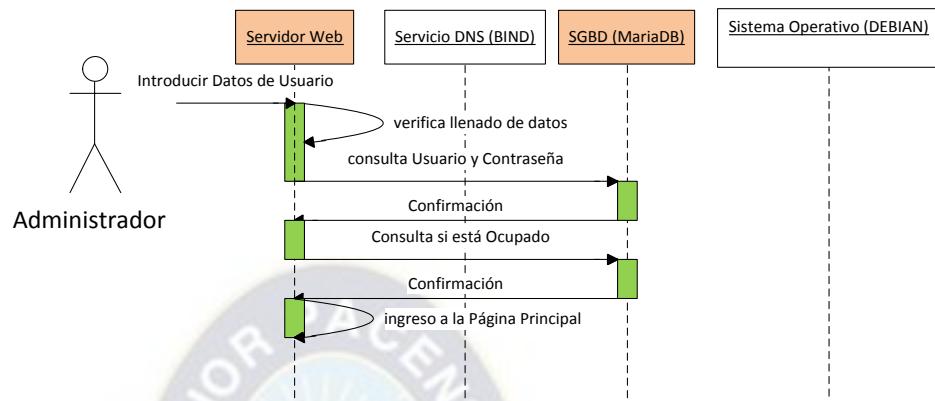
- i. Acceso al sistema por dirección IP o de red.



**FIGURA 3-70. Diagrama de Secuencias para la Configuración del Acceso al Sistema por IP**

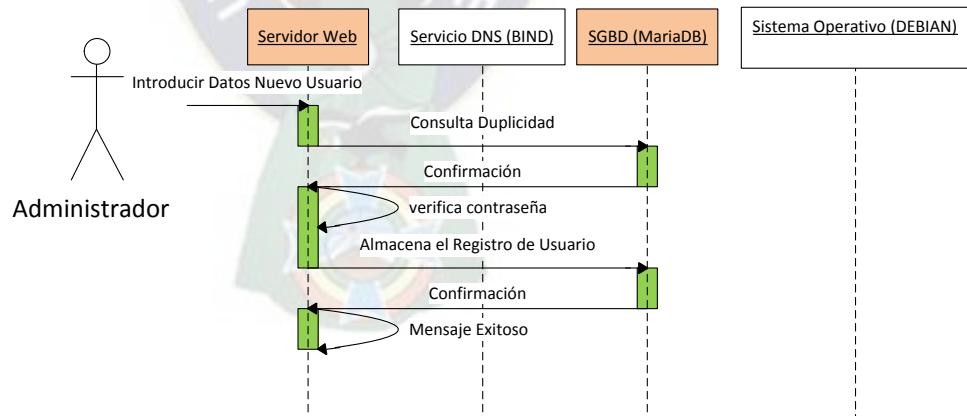
Fuente: Elaboración propia

- ii. Acceso al sistema mediante autenticación por contraseña y prevención de ingresos de forma simultánea.



**FIGURA 3-71. Diagrama de Secuencias del Sistema de Autenticación por Contraseña**  
Fuente: Elaboración propia

iii. Registro y eliminación de usuarios del sistema.

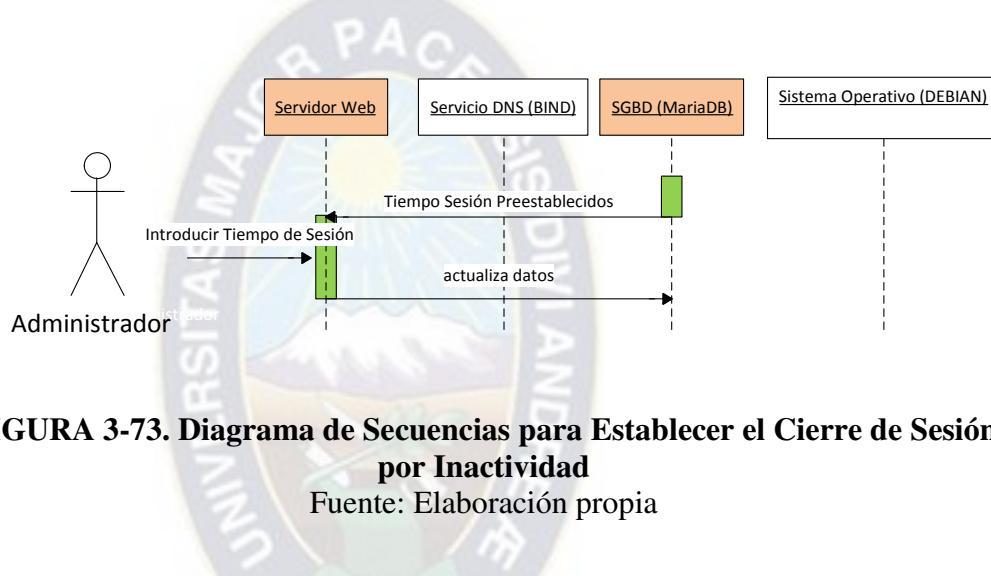


**FIGURA 3-72. Diagrama de Secuencias para el Registro y Eliminación del Sistema**  
Fuente: Elaboración propia

- iv. Intercambio de datos seguro entre cliente y servidor web, mediante HTTPS.

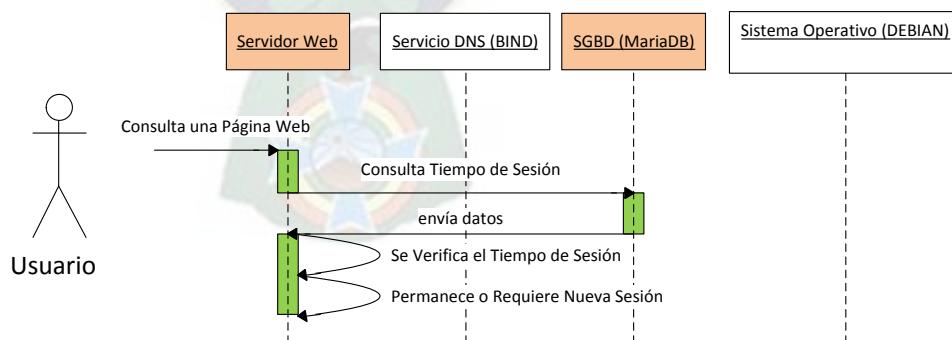
El cifrado de datos entre cliente y servidor se realiza únicamente entre el dispositivo de cliente y el servidor web, durante cualquier uso del sistema.

- v. Cierre de sesión después de cierto tiempo de inactividad.



**FIGURA 3-73. Diagrama de Secuencias para Establecer el Cierre de Sesión por Inactividad**

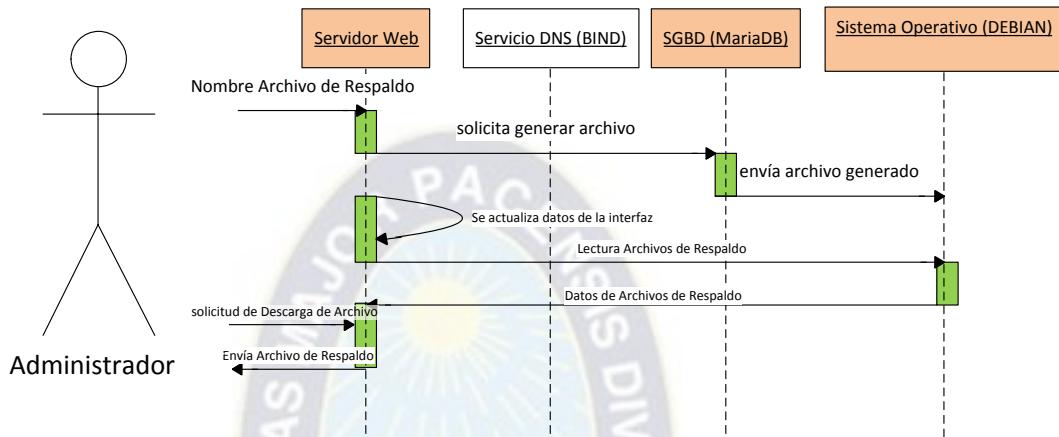
Fuente: Elaboración propia



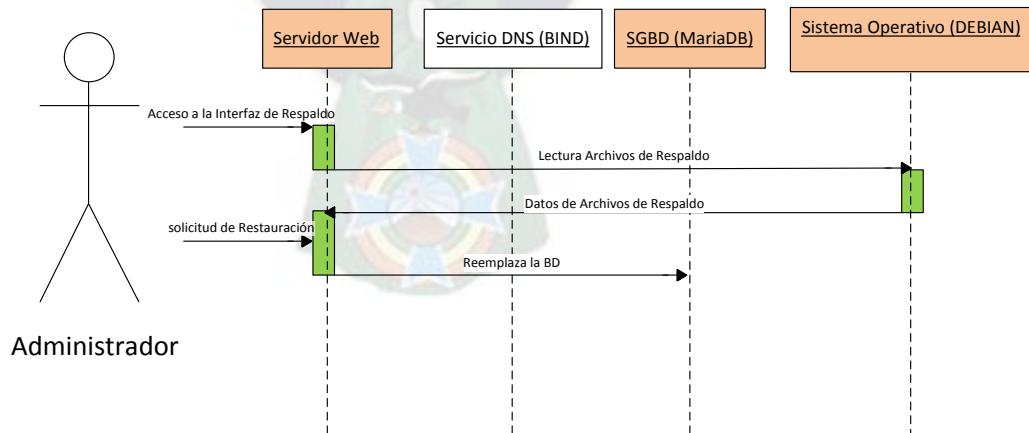
**FIGURA 3-74. Diagrama de Secuencias del Funcionamiento de Cierre de Sesión por Inactividad**

Fuente: Elaboración propia

vi. Copia de respaldo del sistema administración de usuarios.



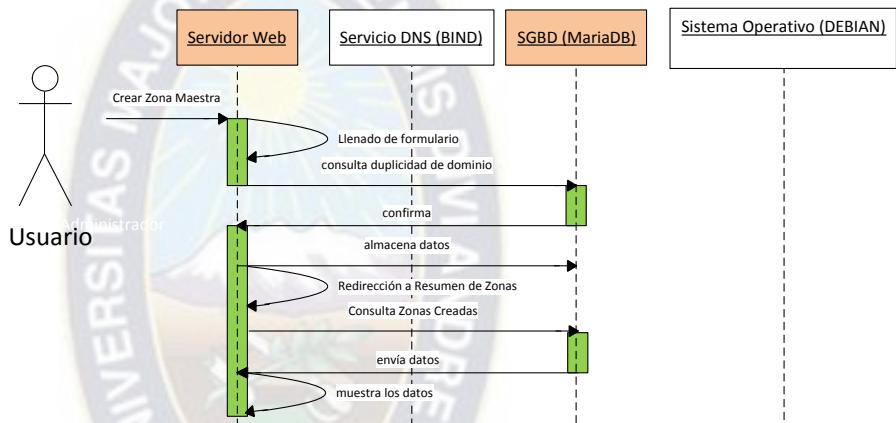
**FIGURA 3-75. Diagrama de Secuencias para Respaldo del Sistema Administración de Usuarios**  
 Fuente: Elaboración propia



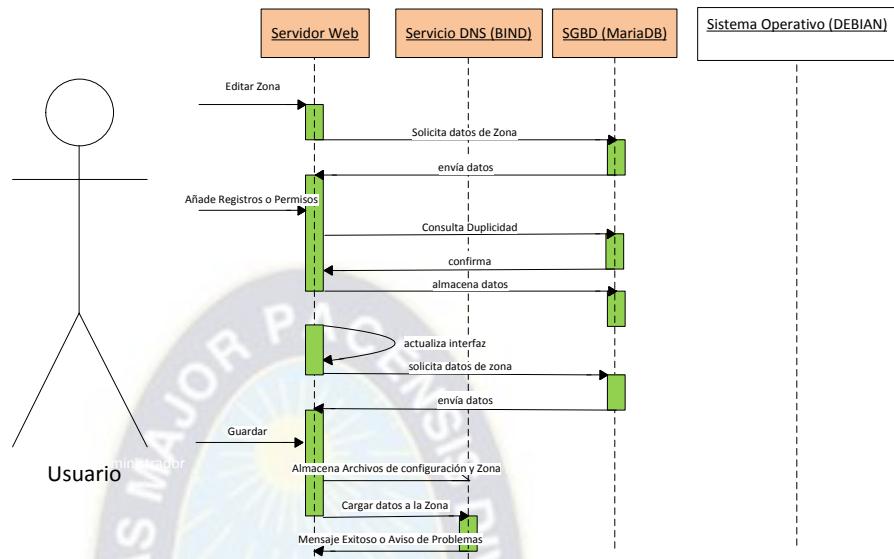
**FIGURA 3-76. Diagrama de Secuencias para Restauración de la BD del Sistema Administración de Usuarios**  
 Fuente: Elaboración propia

### 3.3.3.2. Diagramas de Secuencia del Sistema de Administración y Configuración del servicio DNS

- I. Creación, edición y eliminación de zonas maestras y esclavas; así como sus zonas directas e inversas, para servidores DNS autoritativos y configuración de clientes permitidos para consultas DNS.

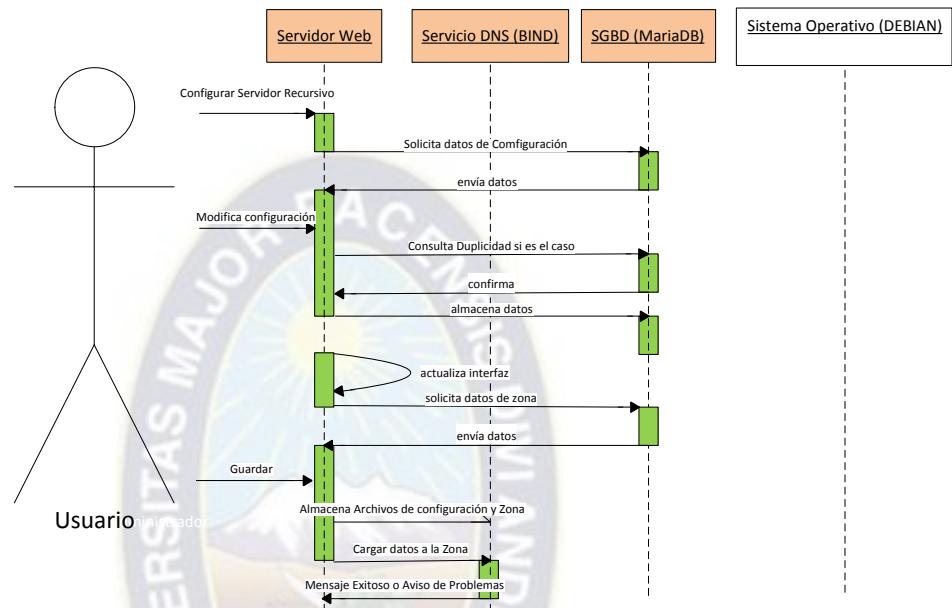


**FIGURA 3-77. Diagrama de Secuencias para la Creación, Edición y Eliminación de Zonas**  
Fuente: Elaboración propia



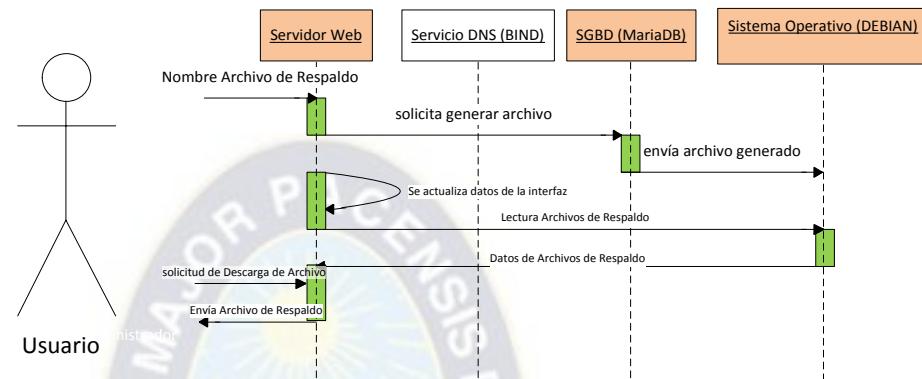
**FIGURA 3-78. Diagrama de Secuencias para la Edición de Zonas**  
 Fuente: Elaboración propia

II. Configuración de servidores DNS recursivos, zonas de reenvío y soporte para el uso de direcciones IPv6.



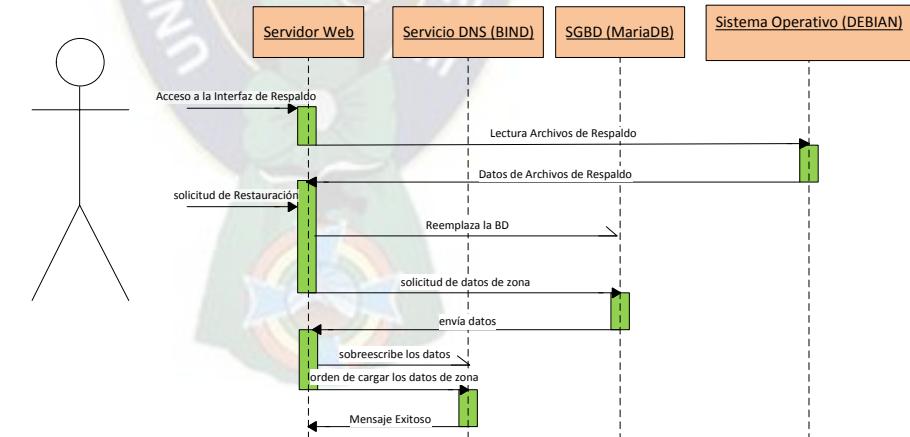
**FIGURA 3-79. Diagrama de Secuencias para la Configuración de Servidores DNS Recursivos, Zonas de Reenvío y Habilitación de IPv6**  
Fuente: Elaboración propia

### III. Copia de respaldo del sistema de administración y configuración de DNS.



**FIGURA 3-80. Diagrama de Secuencias para el Respaldo del Sistema de Administración y Configuración de DNS**

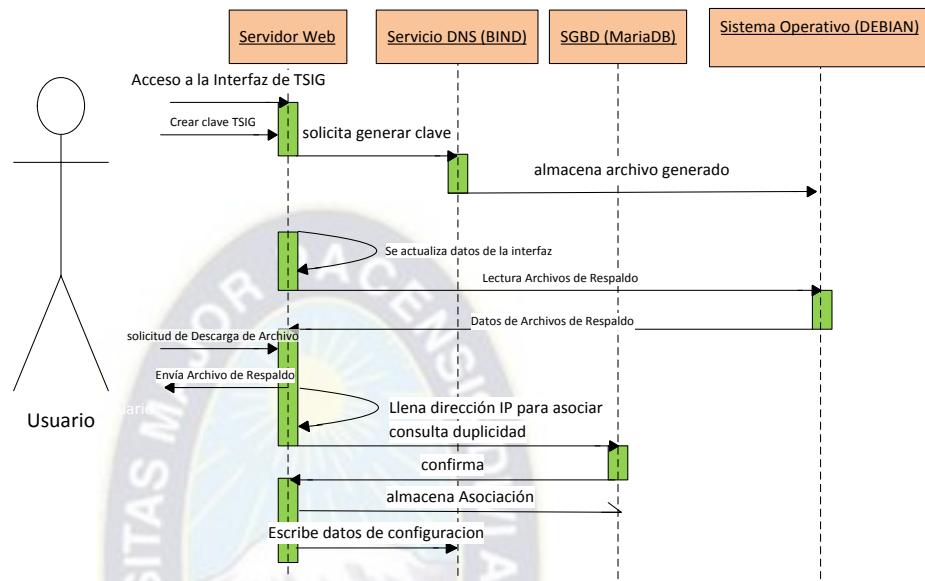
Fuente: Elaboración propia



**FIGURA 3-81. Diagrama de Secuencias para la Restauración del Sistema de Administración y Configuración de DNS**

Fuente: Elaboración propia

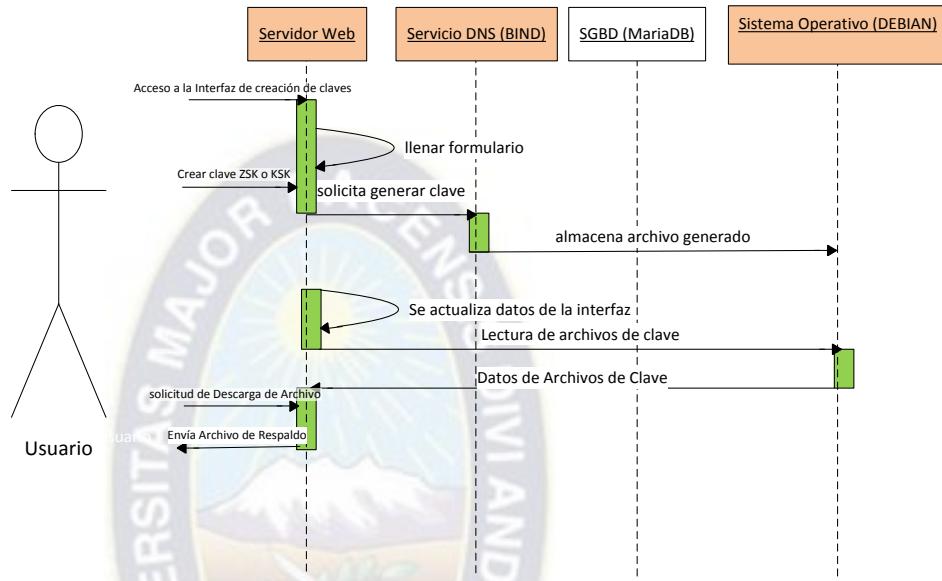
#### IV. Uso de transacciones firmadas entre servidores mediante TSIG.



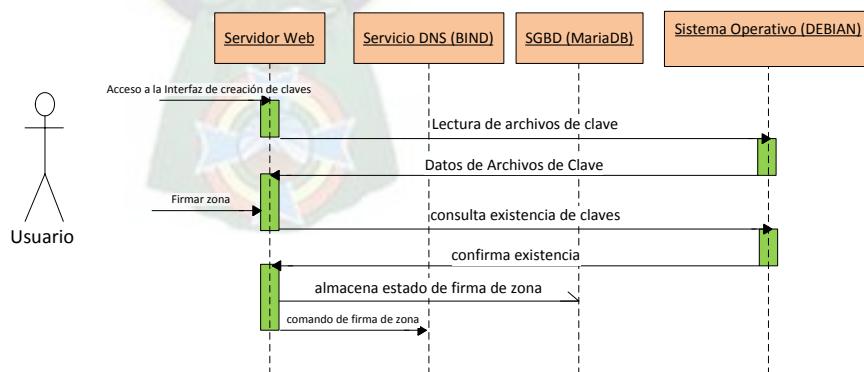
**FIGURA 3-82. Diagrama de Secuencias para la Configuración Transacciones Firmadas entre Servidores mediante TSIG**

Fuente: Elaboración propia

## V. Uso de DNSSEC y respaldo de claves ZSK y KSK.

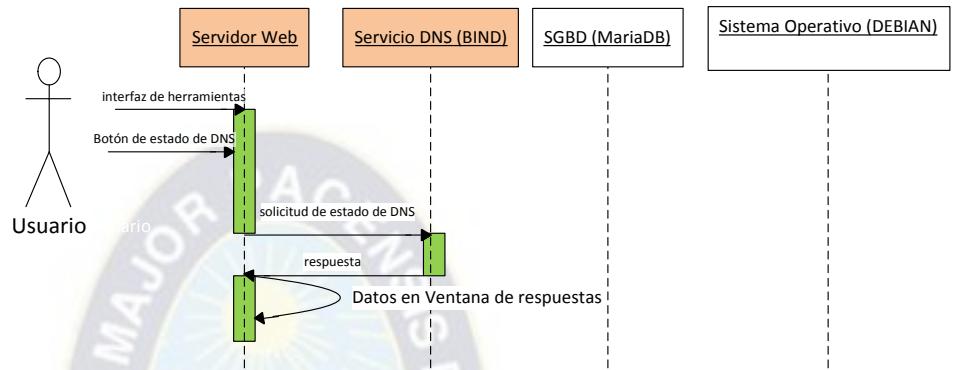


**FIGURA 3-83. Diagrama de Secuencias para la Creación de Claves**  
Fuente: Elaboración propia



**FIGURA 3-84. Diagrama de Secuencias para la Firma de Zona**  
Fuente: Elaboración propia

VI. Uso de RNDC para tareas de monitoreo del estado del sistema y diagnóstico del servicio DNS.



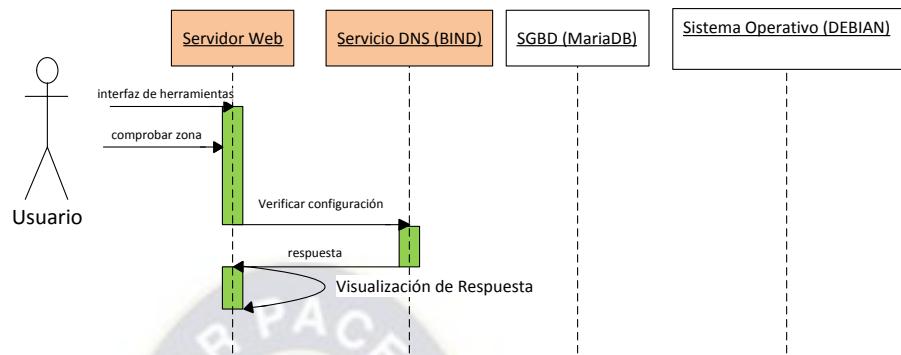
**FIGURA 3-85. Diagrama de Secuencias del Estado del Servicio DNS**

Fuente: Elaboración propia



**FIGURA 3-86. Diagrama de Secuencias del Estado del Sistema**

Fuente: Elaboración propia



**FIGURA 3-87. Diagrama de Secuencias del Estado de Configuración de Zonas**

Fuente: Elaboración propia

### **3.4. Licencia del Sistema**

El software libre se refiere al programa informático en el que el usuario tiene las libertades de usar, copiar, modificar y distribuir dicho software.

Las licencias correspondientes a cada una de las herramientas de software libre utilizadas en el proyecto se muestran a continuación:

#### **Debian:**

Las licencias de Debian siguen las directrices de software libre de Debian (DFSG), disponible en línea en [https://www.debian.org/social\\_contract#guidelines](https://www.debian.org/social_contract#guidelines) donde el primer punto del contrato social con la comunidad de software libre indica que el sistema, así como todos sus componentes se mantendrán completamente libres y el segundo punto señala que los nuevos componentes del sistema Debian, serán licenciados de acuerdo a su definición de software libre. Las licencias que se encuentran en la sección *main* de Debian, incluyen: GNU GPL, GNU LGPL, BSD, Apache, Expat/MIT, PHP, OpenSSL entre otros.

#### **Apache:**

El software de servidor HTTP Apache se encuentra bajo la licencia Apache 2.0, que permite reproducir y distribuir copias de la obra u obra derivada de la misma en cualquier medio, con o sin modificaciones, y en forma de fuente u objeto, bajo ciertas condiciones. Mayor información sobre la licencia se puede encontrar en <http://www.apache.org/licenses/LICENSE-2.0.txt>.

#### **MariaDB:**

MariaDB está basado en MySQL y está disponible bajo los términos de la licencia GPL v2. Mayor información sobre la licencia se puede encontrar en <https://mariadb.com/kb/en/library/mariadb-license/>.

## **PHP:**

Las versiones de PHP 4, PHP 5 y PHP 7 se distribuyen bajo la Licencia PHP v3.01, copyright (c) del Grupo PHP. Esta es una licencia de Código Abierto y que no tiene las restricciones "copyleft" asociadas con GPL. Por lo que se permite modificar y redistribuir con restricciones menores. Más información sobre la licencia del código de este lenguaje de programación se encuentra disponible en línea en [https://www.php.net/license/3\\_01.txt](https://www.php.net/license/3_01.txt).

## **BIND (*Berkeley Internet Name Domain*):**

Utiliza la licencia ISC (*Internet Systems Consortium*) para versiones anteriores a BIND 9.11.0 y licencia de software libre Mozilla MPL2.0 (*Mozilla Public License*) para versiones posteriores.

Para una selección apropiada de una licencia para el software resultante en el presente proyecto se toma en cuenta la información contenida en línea, en la URL <https://choosealicense.com/>, donde la selección de la licencia para este proyecto se efectúa en función de tres situaciones:

- Trabajar en un proyecto en comunidad, en la que se contribuye o de la que se depende.
- Trabajar en un proyecto simple y permisivo, en la que se puede utilizar el proyecto, modificarlo e incluso hacer y distribuir versiones de código cerrado.
- Proyecto en el que importa compartir mejoras, permite realizar casi cualquier cosa con el código, excepto distribuir versiones de código cerrado.

Considerando que lo que importa es compartir mejoras del software, la licencia de software libre que mejor se adapta a nuestras necesidades y apoya a difundir el software libre y gratuito, es la licencia **GNU GPLv3**.

### **3.4.1. Licencia Pública General GNU v3.0**

Los permisos de ésta sólida licencia están condicionados a poner a disposición el código fuente completo de obras con licencia y modificaciones, que incluyen obras más grandes que utilizan una obra con licencia, bajo la misma licencia. Los avisos de copyright y licencia deben conservarse.

Los contribuyentes otorgan una concesión expresa de derechos de patente. Sus características se muestran a continuación:

| Permisos  | Condiciones   | Limitaciones   |
|---|---|--|
| <ul style="list-style-type: none"><li>• Uso Comercial</li><li>• Distribución</li><li>• Modificación</li><li>• Uso de patentes</li><li>• Uso privado</li></ul> | <ul style="list-style-type: none"><li>• Revelar fuente</li><li>• Licencia y aviso de copyright</li><li>• Misma licencia</li><li>• Cambios de estado</li></ul> | <ul style="list-style-type: none"><li>• Responsabilidad</li><li>• Garantía</li></ul> |

**CUADRO 3-1. Características de la Licencia GNU GPLv3**

Fuente: Extraída de la página web [24]

### 3.5. Implementación del Sistema

Para la implementación del sistema se debe hacer consideraciones sobre los requisitos de hardware mínimos para llevar a cabo las pruebas necesarias sin inconvenientes.

El sistema desarrollado se implementó en una máquina virtual, realizando variaciones a los valores de sus recursos de *hardware*, donde se realizó el monitoreo hasta encontrar un desempeño óptimo con las cantidades mínimas de recursos, verificando las funcionalidades y características implementadas.

A continuación, se muestran algunas recomendaciones que son el resultado de un análisis básico de recursos mínimos de *hardware*, para las distintas funciones del sistema.

#### **Requisitos Mínimos de un Servidor Recursivo de Pruebas:**

- **Memoria RAM:** Se necesita al menos 150 MB, por parte del Sistema Operativo cuando el sistema se encuentra instalado y en funcionamiento. El resto sería aprovechado por los Registros de Recurso consultados. Por lo tanto, se recomienda tener entre 250 MB a 500MB de Memoria RAM de acuerdo al número de clientes del servicio DNS.
- **Memoria en Disco:** El sistema operativo **Debian** instalado ocupa alrededor de 1GB de espacio en disco y el sistema de administración de DNS desarrollado ocupa 60 MB. Considerando que el sistema desarrollado permite almacenar registros de los eventos, relacionados a las solicitudes del servicio DNS, se necesitan 12MB adicionales, por lo que con un Disco Duro de 4GB, bastaría para cubrir los requerimientos de almacenamiento.
- **CPU:** Después de múltiples pruebas en máquinas virtuales se llegó a la conclusión de que es necesario al menos un núcleo de 2GHz para las validaciones de DNSSEC.

### **Requisitos Mínimos de un Servidor Autoritativo:**

- **Memoria RAM:** El servidor autoritativo no almacena una gran cantidad de Registros de Recurso en su memoria como un servidor recursivo, y solo necesita almacenar la zona firmada cuando DNSSEC se encuentra activado. Por lo tanto, se necesita al menos 250 MB de memoria RAM tomando en cuenta que el sistema operativo ya ocupa 150 MB aproximadamente, para su funcionamiento.
- **Memoria en Disco:** Utilizando el mismo análisis de requerimientos que para un servidor recursivo y considerando el almacenamiento de zona se necesitan al menos 4GB.
- **CPU:** De forma análoga al servidor recursivo, para firmar una zona se necesita un núcleo de al menos a 2GHz.

## **3.6. Pruebas de Funcionamiento y Resultados Obtenidos**

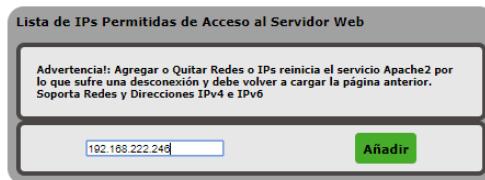
En correspondencia a los atributos presentados en el Diseño de Sistema de Administración Web del Servicio DNS, las pruebas de funcionamiento y los resultados obtenidos, corresponden al Sistema de Administración de Usuarios y al Sistema de Administración y Configuración del Servicio DNS, como se muestra a continuación:

### **3.6.1. Pruebas de Funcionamiento para el Sistema de Administración de Usuarios**

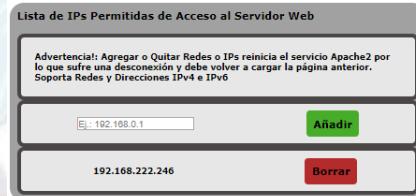
#### **a. Acceso al Sistema por dirección IP o de Red**

Inicialmente el sistema no lleva configurado ninguna regla restrictiva para el acceso por dirección IP o de Red, debido a que puede ser implementado en distintos rangos de Red, y posteriormente realizar las restricciones respectivas, de acuerdo a las necesidades de la infraestructura de la Red de Datos.

- Configuración para una Dirección de Red de Prueba



**FIGURA 3-88. Adición de la Dirección IP “192.168.222.246” Permitida para el Acceso al Sistema**  
Fuente: Elaboración propia



**FIGURA 3-89. Dirección IP “192.168.222.246” Configurada para el Acceso al Sistema**  
Fuente: Elaboración propia

Después de esta configuración, si otro dispositivo trata de ingresar al sistema y tiene una dirección que no está configurada, se prohíbe su ingreso.



**FIGURA 3-90. Acceso Restringido al Servidor para una Dirección no Configurada en la lista de direcciones IP o de Red permitidas**  
Fuente: Elaboración propia

Las pruebas de funcionamiento del Sistema de Administración de Usuarios, pueden ser revisados en su totalidad en el ANEXO A, de la sección de ANEXOS.

### **3.6.2. Pruebas de Funcionamiento para el Sistema de Administración y Configuración del Servicio DNS**

Se debe considerar que el sistema de administración de DNS tiene la dirección IP **192.168.100.7** de una red local de pruebas.

#### **A. Creación, Edición y Eliminación de Zonas Maestras y Esclavas; así como sus Zonas Directas e Inversas, para Servidores DNS Autoritativos y Configuración de Clientes Permitidos para Consultas DNS**

- **Creación de una Zona Maestra Directa**

The screenshot shows a simple web form with a white background and black text. At the top center, it says "Zona Maestra". Below that are two buttons: a blue one labeled "Crear Zona Directa" and a red one labeled "Crear Zona Inversa".

**FIGURA 3-91. Interfaz de Acceso para la Creación de una Zona Maestra Directa**

Fuente: Elaboración propia

This screenshot shows a more detailed configuration form for a master zone. It has a title "Zona Maestra Directa" at the top. Below it are eight input fields with dropdown menus for selecting values. The fields are: "Dominio" (ejemplo.gob.bo), "Correo admin" (mail.ejemplo.gob.bo), "TTL genérico(seg)" (604800), "TTL SOA(seg)" (604800), "Refresh(seg)" (604800), "Retry(seg)" (86400), "Expire(seg)" (2419200), and "Negative Cache TTL(seg)" (604800). At the bottom are two buttons: a green "Crear" button and a red "Salir" button.

**FIGURA 3-92. Campos de llenado Formulario de una Zona Maestra Directa**

Fuente: Elaboración propia

**Resumen de zonas**

| Zona Maestra - Directa  |
|---|
| ejemplo.gob.bo.   |
| <a href="#">Editar</a> <a href="#">Borrar</a> <a href="#">Descargar</a> |
| Zona Maestra - Inversa  |
| Zona Esclava - Directa  |
| Zona Esclava - Inversa  |
| Zonas de Reenvío  |

[Descargar Resumen de Zonas](#)

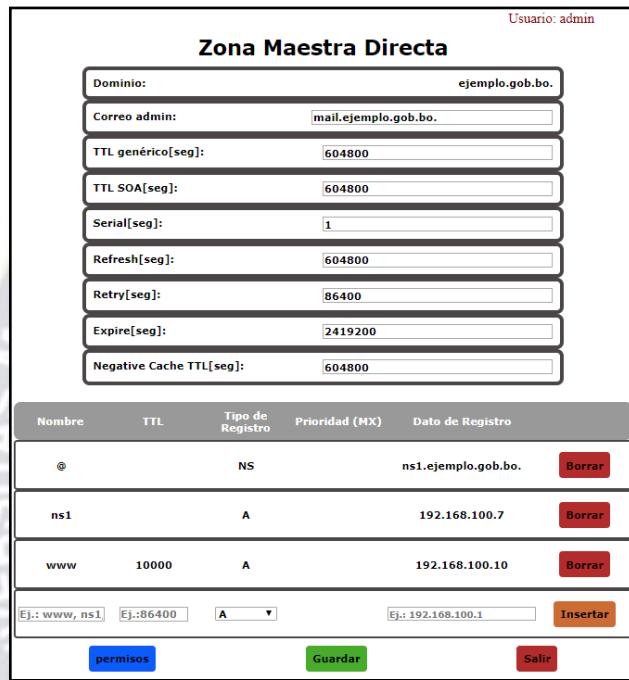
**FIGURA 3-93. Zona Maestra Directa Creada**

Fuente: Elaboración propia



- **Edición de una Zona Maestra Directa y Permisos de Consultas DNS**

En esta etapa se puede añadir los Registros de Recurso de la Zona.



| Nombre        | TTL       | Tipo de Registro | Prioridad (MX) | Dato de Registro   |
|---------------|-----------|------------------|----------------|--|
| @             |           | NS               |                | ns1.ejemplo.gob.bo. <span style="background-color: red; color: white; border-radius: 5px; padding: 2px;">Borrar</span>     |
| ns1           |           | A                |                | 192.168.100.7 <span style="background-color: red; color: white; border-radius: 5px; padding: 2px;">Borrar</span>           |
| www           | 10000     | A                |                | 192.168.100.10 <span style="background-color: red; color: white; border-radius: 5px; padding: 2px;">Borrar</span>          |
| Ej.: www, ns1 | Ej.:86400 | A                |                | Ej.: 192.168.100.1 <span style="background-color: orange; color: white; border-radius: 5px; padding: 2px;">Insertar</span> |

Buttons at the bottom: permisos (Permissions), Guardar (Save), and Salir (Exit).

**FIGURA 3-94. Interfaz de Edición de una Zona Maestra Directa**

Fuente: Elaboración propia



| Redes permitidas para Consultas |  |
|---------------------------------|--|
| 192.168.222.0/24                | <span style="background-color: red; color: white; border-radius: 5px; padding: 2px;">Borrar</span>     |
| Ej.:any.none, 192.168.0.0       | <span style="background-color: green; color: white; border-radius: 5px; padding: 2px;">Insertar</span> |

| IPs Esclavos              |  |
|---------------------------|--|
| none                      | <span style="background-color: red; color: white; border-radius: 5px; padding: 2px;">Borrar</span>     |
| Ej.:any.none, 192.168.0.1 | <span style="background-color: green; color: white; border-radius: 5px; padding: 2px;">Insertar</span> |

**FIGURA 3-95. Interfaz de Permisos de una Zona Maestra Directa**

Fuente: Elaboración propia

Una vez guardados los cambios el sistema envía un mensaje indicando si se pudieron guardar los datos correctamente:



**FIGURA 3-96. El Sistema Informa que los Datos de Zona se Cargaron Exitosamente**

Fuente: Elaboración propia

```
backup_zonas.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
zone "ejemplo.gob.bo" {
    type master;
    file "/var/lib/bind/db.ejemplo.gob.bo";
    dnssec-secure-to-insecure yes;
    allow-query {
        192.168.222.0/24;
    };
    allow-transfer {
        none;
    };
    also-notify {
    };
};
```

**FIGURA 3-97. Archivo Generado por el Sistema con el Resumen de la Zona Maestra Configurada**

Fuente: Elaboración propia

```
backupZMD.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
$TTL 604800
@ 604800 SOA ejemplo.gob.bo. mail.ejemplo.gob.bo. (
    4 ; serial
    604800 ; refresh (168 hours)
    86400 ; retry (24 hours)
    2419200 ; expire (4 weeks)
    604800 ; minimum (168 hours)
)
@ NS ns1.ejemplo.gob.bo.
ns1 A 192.168.100.7
www 10000 A 192.168.100.10
@ 10000 MX 10 mail.ejemplo.gob.bo.
```

**FIGURA 3-98. Archivo de Zona Maestra Directa Generada con el Sistema**

Fuente: Elaboración propia

```

:\Users\henry>dig @192.168.100.7 www.ejemplo.gob.bo
;; <>> DiG 9.12.3 <>> @192.168.100.7 www.ejemplo.gob.bo
; (1 server found)
; global options: +cmd
; Got answer:
; ->HEADER<- opcode: QUERY, status: NOERROR, id: 33676
; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
; WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
www.ejemplo.gob.bo.          IN      A

; ANSWER SECTION:
www.ejemplo.gob.bo.    10000   IN      A      192.168.100.10
; AUTHORITY SECTION:
ejemplo.gob.bo.        604800  IN      NS      ns1.ejemplo.gob.bo.
; ADDITIONAL SECTION:
ns1.ejemplo.gob.bo.    604800  IN      A      192.168.100.7

; Query time: 4 msec
; SERVER: 192.168.100.7#53(192.168.100.7)
; WHEN: Sat Feb 01 16:01:30 Hora est&ndar oeste, Sudam&rica 2020
; MSG SIZE rcvd: 97

```

**FIGURA 3-99. Consulta al Servidor por el Host “www.ejemplo.gob.bo” con la herramienta “dig”**

Fuente: Elaboración propia

Las pruebas de funcionamiento del Sistema de Administración y Configuración del Servicio DNS se pueden observar en el ANEXO A, de la sección de ANEXOS.

# Capítulo IV: EVALUACIÓN CUANTITATIVA DEL PROYECTO

## 4.1. Tiempo de Desarrollo del Proyecto

Para el cálculo de tiempo empleado en la elaboración del software se tomará en cuenta la cantidad de horas en promedio trabajadas por día, por semana y por mes.

| Parámetro de Tiempo | Tiempo de Trabajo | Tiempo Total Estimado   |
|---------------------|-------------------|---|
| 1 día               | 10 [horas]        | $T = 12[\text{meses}] * \frac{4[\text{semanas}]}{1[\text{mes}]} * \frac{6[\text{días}]}{1[\text{semana}]} * \frac{10[\text{horas}]}{1[\text{día}]}$<br>$T = 2880[\text{horas}]$ |
| 1 semana            | 6 [días]          |   |
| 1 mes               | 4 [semanas]       |   |

**TABLA 4-1. Cálculo de Horas Trabajadas que se Emplearon en el Desarrollo del Proyecto**

Fuente: Elaboración Propia

El tiempo total de horas empleadas en el desarrollo del proyecto está conformado tanto por el tiempo de aprendizaje de los distintos lenguajes de programación (PHP, MySQL, Linux, Apache, HTML, CSS, JavaScript, BIND), así como el tiempo de desarrollo, implementación, pruebas del proyecto, y elaboración de un manual de administración del sistema, entregado al Ministerio de Economía y Finanzas Públicas.

## 4.2. Cantidad de Líneas de Código Desarrolladas

La cantidad de líneas de código desarrolladas, están conformadas por la cantidad de líneas de código del Sistema de Administración de Usuarios y por la cantidad de líneas de código del Sistema de Administración y Configuración del servicio DNS. También se debe tomar en cuenta la cantidad de líneas de código de los estilos aplicados que contribuyeron a una visualización más intuitiva y una adaptabilidad de visualización para dispositivos móviles.

| Sub Módulo                 | Cantidad de Líneas de Código | Líneas de Código Totales |
|----------------------------|------------------------------|--------------------------|
| Actualizar <i>Password</i> | 69                           |                          |
| Cambio de <i>Password</i>  | 46                           |                          |
| Conexión BD Usuarios       | 12                           |                          |
| Configuración de Admin     | 279                          |                          |
| Eliminar Usuario           | 20                           |                          |
| Formulario de Usuario      | 94                           |                          |
| <i>Index</i>               | 52                           |                          |
| <i>Login</i>               | 89                           |                          |
| <i>Logout</i>              | 12                           |                          |
| Registro de Usuario        | 66                           |                          |
| Respaldo para Usuario      | 4                            |                          |
| Subir Usuario              | 76                           |                          |
| Tiempo de Sesión           | 18                           |                          |

T = 837 Líneas de Código

**TABLA 4-2. Cálculo de Líneas de Código Empleadas en el Sistema de Administración de Usuarios**

Fuente: Elaboración Propia

| Sub Módulo                    | Cantidad de Líneas de Código | Líneas de Código Totales |
|-------------------------------|------------------------------|--------------------------|
| Conexión BD DNS               | 21                           |                          |
| Configurar TSIG               | 245                          |                          |
| Configuración General         | 104                          |                          |
| Crear Esclavo                 | 93                           |                          |
| Crear Esclavo Inverso         | 134                          |                          |
| Crear Llaves                  | 515                          |                          |
| Crear Llave Esclava           | 498                          |                          |
| Crear Maestro                 | 136                          |                          |
| Crear Maestro Inverso         | 170                          |                          |
| Crear Reenvío                 | 119                          |                          |
| Declarar Zona                 | 259                          |                          |
| Dirección Ipv4 Inversa        | 155                          |                          |
| Dirección Ipv6 Inversa        | 201                          |                          |
| DNSSEC                        | 115                          |                          |
| Editar Maestro                | 378                          |                          |
| Editar Maestro Inverso        | 293                          |                          |
| Editar Recursivo              | 380                          |                          |
| Editar Reenvío                | 116                          |                          |
| Gráficos Monitoreo            | 97                           |                          |
| Herramientas                  | 453                          |                          |
| Info Recursos                 | 252                          |                          |
| Eliminación                   | 681                          |                          |
| Permisos Zona Directa         | 139                          |                          |
| Permisos Zona Esclava Directa | 211                          |                          |
| Permisos Zona Esclava Inversa | 208                          |                          |
| Permisos Zona Inversa         | 135                          |                          |
| Renovar Llaves                | 539                          |                          |
| Respaldo BD DNS               | 240                          |                          |
| Respaldo para DNS             | 4                            |                          |
| Resumen de Zonas              | 169                          |                          |
| Subir BD DNS                  | 76                           |                          |
| Subir Key                     | 124                          |                          |
| Subir TSIG                    | 139                          |                          |

$T = 7399$  Líneas de Código

**TABLA 4-3. Cálculo de Líneas de Código Empleadas en el Sistema de Administración y Configuración del Servicio DNS**

Fuente: Elaboración Propia

| Módulo   | Cantidad de Líneas de Código | Líneas de Código Totales     |
|--|------------------------------|------------------------------|
| Sistema de Administración de Usuarios                      | 837                          | $T = 10601$ Líneas de Código |
| Sistema de Administración y Configuración del Servicio DNS | 7399                         |                              |
| Barra de Navegación  | 169                          |                              |
| Hojas de Estilos   | 2196                         |                              |

**TABLA 4-4. Cálculo de Líneas de Código Totales del Sistema**

Fuente: Elaboración Propia

El diagrama de bloques que muestra la interconexión entre los sub módulos del Sistema de Administración de Usuarios y el Sistema de Administración y Configuración del Servicio DNS puede ser revisado en el ANEXO B, de la sección de ANEXOS.



# Capítulo V: CONCLUSIONES Y RECOMENDACIONES

## 5.1. Conclusiones

1. Se utilizó **Apache** como servidor web; **MariaDB** como **SGBD**; y **PHP, HTML, JavaScript** y **CSS** como lenguajes de desarrollo web, los cuales se instalan sobre el sistema operativo **Debian**, para administrar el servicio DNS instalado con **Bind**, así mismo se utiliza **OpenSSL**, para proveer un canal seguro de comunicación. Y se establecieron las recomendaciones de *hardware* necesarias para implementar las distintas funciones del sistema.
2. El sistema desarrollado está compuesto por el **Sistema de Administración de Usuarios** que consta de: control de acceso por IP; autenticación por contraseña, prevención de ingresos de forma simultánea; registro y eliminación de usuarios; intercambio de datos seguro entre cliente y servidor, mediante HTTPS; cierre de sesión por tiempo de inactividad; y copia de respaldo de la BD de Usuarios. También está compuesto por el **Sistema de Administración y Configuración del Servicio DNS** que consta de: creación, edición y eliminación de zonas maestras y esclavas, directas e inversas para servidores autoritativos y configuración de clientes permitidos; configuración de servidores recursivos, zonas de reenvío y soporte para uso de direcciones IPv6; copia de respaldo de la BD del sistema de administración y configuración; uso de transacciones firmadas entre servidores mediante TSIG; uso de DNSSEC y respaldo de claves ZSK y KSK; y uso de RNDC para monitoreo del estado del sistema y diagnóstico del servicio DNS.
3. El sistema fue desarrollado siguiendo las etapas de la metodología de desarrollo web OOHDM.

4. Se realizó la implementación en un servidor virtual de pruebas, y se identificaron como requerimientos mínimos del sistema: 350 MB de Memoria RAM, 4GB de espacio en Disco y 1 núcleo de 2 GHz.
5. Las pruebas de funcionamiento fueron exitosas; y se añadieron los requerimientos a la interfaz de usuario, y al proceso de renovación de claves, que se solicitó por parte del MEFP.
6. Se logró desarrollar un sistema de administración para un servidor DNS de uso intuitivo y con grandes ventajas de seguridad y funcionalidad utilizando tecnología web y herramientas de software libre.

## **5.2. Recomendaciones**

Para disponer de integridad y autenticidad de los datos consultados ya sea como servidor recursivo o autoritativo, se recomienda hacer uso de DNSSEC.

Con el propósito de mejorar el servicio del sistema desarrollado se puede añadir la funcionalidad de generar reportes a partir de los registros que el sistema almacena por las consultas de resolución de domino que realizan los clientes al sistema.

## BIBLIOGRAFÍA

- [1].BOLIVIA. 2017. “Decreto Supremo N° 3251” Artículo 2. 12 de Julio de 2017. 8p [en línea]: <<https://www.agetic.gob.bo/pdf/documentos/DS-3251.pdf>> [consulta: 20 Noviembre 2018].
- [2].IETF. 1987. “RFC 1034: Domain Names – Concepts And Facilities” [en línea] <<https://tools.ietf.org/html/rfc1034>> [consulta: 12 Diciembre 2018].
- [3].IETF. 1987. “RFC 1035: Domain Names – Implementation and Specification” [en línea] <<https://tools.ietf.org/html/rfc1035>> [consulta: 12 Diciembre 2018].
- [4].INTERNET SYSTEM CONSORTIUM. 2018. “BIND 9 Administrator Reference Manual” [en línea] California, USA. Internet System Consortium Inc. <<https://downloads.isc.org/isc/bind9/9.11.5-P1/>> [consulta: 15 Diciembre 2018].
- [5].ADSIB. 2019. “En marcha despliegue de DNSSEC en el ccTLD .bo” [en línea] <<https://www.bolnet.bo/En-marcha-despliegue-de-DNSSEC-en>> [consulta: 10 Abril 2019]
- [6].ULTRATOOLS. 2016. “Statistics top 500 Domains DNS Server Types” [en línea] <<https://www.ultratools.com/statistics>> [consulta: 10 Diciembre 2018].
- [7].INTERNET SYSTEM CONSORTIUM. 2018. “Licencia ISC - Mozilla Public License” [en línea] <<https://www.isc.org/downloads/software-support-policy/isc-license/>> [consulta: 10 Diciembre 2018].
- [8].INTERNET SYSTEM CONSORTIUM. 2017. “Bind Dnssec Guide. [en línea] <<https://ftp.isc.org/isc/dnssec-guide/dnssec-guide.pdf>> [consulta: 12 Diciembre 2018].
- [9].LWN Feature Article. 1999-2019. “The LWN.net Linux Distribution List” [en línea] <<https://lwn.net/Distributions/>> [consulta: 1 Noviembre 2018].
- [10]. ADSIB. 2018. “Políticas de Implementación y Gestión del Repositorio Estatal de Software Libre” [en línea] ADSIB-SL-POLT-001, La Paz, Bolivia <<https://softwarelibre.gob.bo/auth/login>> [consulta: 12 Diciembre 2018].
- [11]. Debian. 2019. “A Brief History of Debian” [en línea] <<https://www.debian.org/doc/manuals/project-history/index.en.html#contents>> [consulta: 1 Enero 2019].
- [12]. W3C Working Group. 2016. “JAVASCRIPT WEB APIS” [en línea] <<https://www.w3.org/standards/webdesign/script.html>> [consulta: 1 Noviembre 2018].
- [13]. W3C Working Group. 2018. “HTML Y CSS” [en línea] <<https://www.w3.org/standards/webdesign/htmlcss>> [consulta: 1 Noviembre 2018].
- [14]. NETCRAFT. 2019. “June 2019 Web Server Survey” [en línea] <<https://news.netcraft.com/archives/2019/06/17/june-2019-web-server-survey.html>> [consulta: 25 Junio 2019].
- [15]. SILBERSCHATZ, A., KORTH, H.F., SUDARSHAN, S. 2002. “Fundamentos de Bases de Datos”. 4<sup>a</sup>. Edición. Madrid, España. McGraw-Hill/Interamericana de España. 770p. [consulta: 5 Enero 2019].
- [16]. MILLÁN, M.E. 2012. “Fundamentos de Bases de Datos”, Edición Digital 2017. Cali, Colombia. Programa Editorial/Universidad del Valle. 154p.

- [17]. CAMPS, R. *et al.* 2005. “Bases de Datos”. Barcelona, España. Editorial Eureka Media. 460p. [consulta: 10 Enero 2019].
- [18]. DB-ENGINES. 2019. “DB-Engines Ranking” [en línea] <<https://db-engines.com/en/ranking>> [consulta: 11 Enero 2019].
- [19]. MARIADB. 2019. “MariaDB versus MySQL – Compatibility” [en línea] <<https://mariadb.com/kb/en/library/mariadb-vs-mysql-compatibility/>> [consulta: 15 Enero 2019].
- [20]. ROCHKIND, M. 2013. “Expert PHP and MySQL”. Boulder, Colorado. Editorial Apress, 329. [consulta: 15 Enero 2019].
- [21]. W3TECHS. 2019. “Usage Statistics and market share of PHP for websites” [en línea] <<https://w3techs.com/technologies/details/pl-php/all/all>> [consulta: 5 enero 2019].
- [22]. COBO, A. *et al.* 2005. “PHP y MySQL Tecnologías para el Desarrollo de Aplicaciones Web”. España. Editorial Diaz de Santos. 504p. [consulta: 5 Febrero 2019].
- [23]. MOLINA, J. et al. 2018. “Comparación de Metodologías en Aplicaciones Web” [en línea] Revista 3CTecnología. 14 de marzo de 2018. Volumen 7, Número 1, Edición 25 <<http://dx.doi.org/10.17993/3ctecno.2018.v7n1e25.1-19>> [consulta: 5 Febrero 2019].
- [24]. CHOOSE A LICENSE. 2019. “GNU General Public License v3.0” [en línea] <<https://choosealicense.com/licenses/gpl-3.0/>> [consulta: 10 Febrero 2019].

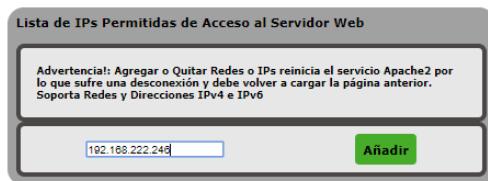
**ANEXO A: PRUEBAS DE FUNCIONAMIENTO DEL  
SISTEMA Y RESULTADOS OBTENIDOS**

# Pruebas de Funcionamiento para el Sistema de Administración de Usuarios

## a. Acceso al Sistema por dirección IP o de Red

Por defecto el sistema no lleva configurado ninguna regla restrictiva para el acceso por dirección IP o de Red, debido a que puede ser implementado en distintos rangos de Red, y posteriormente realizar las restricciones respectivas.

- **Configuración para una Dirección de Red de Prueba**



**FIGURA 1. Adición de la Dirección IP “192.168.222.246” Permitida para el Acceso al Sistema**  
Fuente: Elaboración propia



**FIGURA 2. Dirección IP “192.168.222.246” Configurada para el Acceso al Sistema**  
Fuente: Elaboración propia

Después de esta configuración, si otro dispositivo trata de ingresar al sistema y tiene una dirección que no está configurada se prohíbe su ingreso.



**FIGURA 3. Acceso Restringido al Servidor para una Dirección no Configurada en la lista de direcciones IP o de Red permitidas**

Fuente: Elaboración propia

- b. Acceso al sistema mediante autenticación por contraseña y prevención de ingresos de forma simultánea.

Caso 1: Ingreso de usuario “admin” e ingreso posterior del usuario “jperez”

- Prueba de Ingreso con el Usuario “admin”

**FIGURA 4. Prueba de Ingreso con el Usuario “admin”**

Fuente: Elaboración propia



**FIGURA 5. Ingreso al Sistema Exitoso del Usuario “admin”**

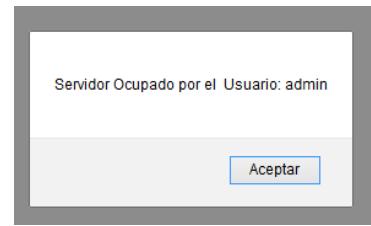
Fuente: Elaboración propia

**Prueba de un Segundo Ingreso con el Usuario “jperez”**



**FIGURA 6. Prueba de Ingreso con el Usuario “jperez”**

Fuente: Elaboración propia



**FIGURA 7. Ingreso Denegado al Sistema debido al Uso del Sistema**

**por el Usuario “admin”**

Fuente: Elaboración propia

### c. Registro y Eliminación de Usuarios del Sistema

El registro y eliminación de Usuarios del sistema es accesible únicamente por el usuario “admin”.

- **Prueba de Registro para el usuario “sbolivar”**

Registrar Usuario

Nombre: Simón Bolívar

Usuario: sbolivar

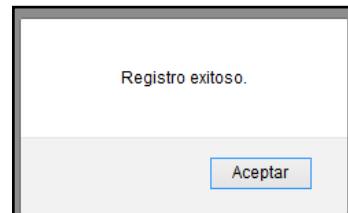
Contraseña: [REDACTED]

Confirmar Contraseña: [REDACTED]

Botones: Registrar (verde), Cancelar (rojo)

**FIGURA 8. Registro del Usuario “sbolivar”**

Fuente: Elaboración propia



**FIGURA 9. Registro Exitoso del Usuario “sbolivar”**

Fuente: Elaboración propia

- **Eliminación de Usuario “jperez”**

La eliminación de un usuario se realiza presionando el botón “borrar”

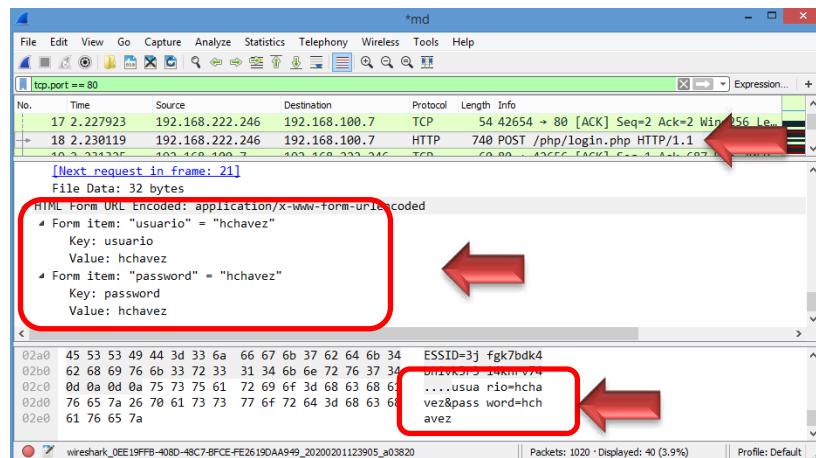
| Usuarios Registrados |        |
|----------------------|--------|
| admin                |        |
| hchavez              | Borrar |
| sbolivar             | Borrar |

**FIGURA 10. Resultado de Presionar el Botón “Borrar” en el Usuario “jperez”**

Fuente: Elaboración propia

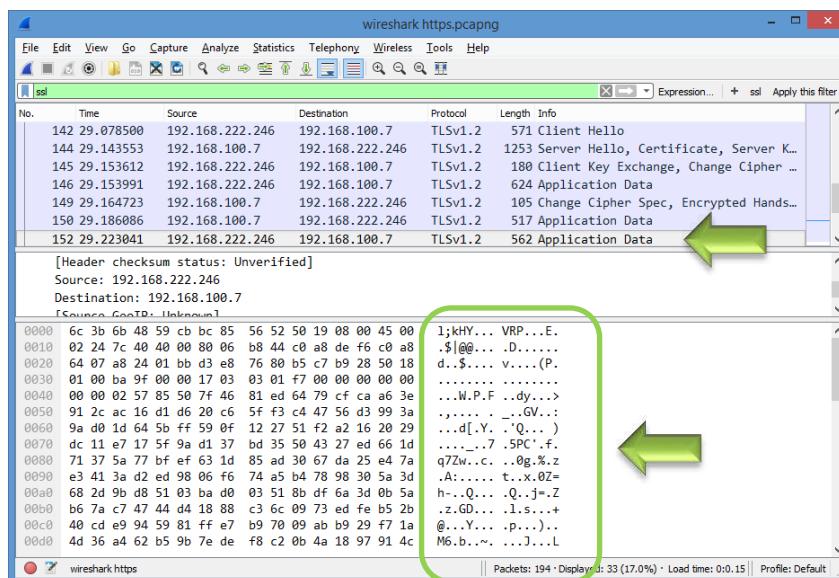
**d. Intercambio de datos seguro entre cliente y servidor web, mediante HTTPS**

- Prueba de Ingreso con el Protocolo HTTP.



**FIGURA 11. Ingreso al Sistema con el Protocolo HTTP con Datos de Usuario Vulnerables**  
Fuente: Elaboración propia

- Prueba de Ingreso con el Protocolo HTTPS.



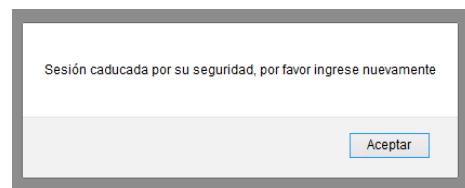
**FIGURA 12. Ingreso al Sistema con el Protocolo HTTPS con Datos de Usuario Cifrados**  
Fuente: Elaboración propia

**e. Cierre de Sesión después de Cierto Tiempo de Inactividad**

Con el tiempo de sesión configurado, una vez excedido el tiempo establecido, se cierra la sesión del usuario, debido a la inactividad de la página actual en la que se encuentre.



**FIGURA 13. Configuración del Tiempo de Sesión en 5 minutos**  
Fuente: Elaboración propia



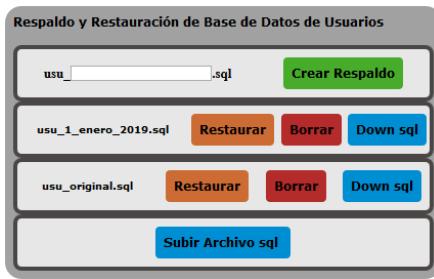
**FIGURA 14. Respuesta del Sistema una vez Excedido el Tiempo de Sesión Establecido**  
Fuente: Elaboración propia

**f. Copia de Respaldo del Sistema Administración de Usuarios**

• **Respaldo de la BD de Usuarios**



**FIGURA 15. Creación de una BD de Usuarios con un Nombre Distintivo**  
Fuente: Elaboración propia



**FIGURA 16. BD de Usuarios Creada**  
Fuente: Elaboración propia

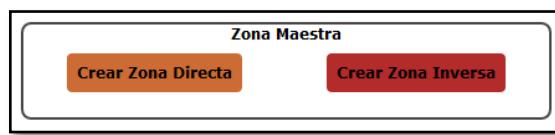
```
(1,'admin','admin',21024/WxREGV.,'2018-05-21 15:13:34'),  
(4,'henry Chavez','hchavez',a5EtV0SVsh/KU,'2019-01-01 11:22:09'),  
(5,'Simón Bolívar ','sbolivar',5r60rystRIwpg,'2019-01-01 11:34:38');
```

**FIGURA 17. Descarga de la BD de Usuarios “usu\_1\_enero\_2019.sql” con los Datos de Contraseña Cifrados**  
Fuente: Elaboración propia

## **Pruebas de Funcionamiento para el Sistema de Administración y Configuración del Servicio DNS**

- A. Creación, Edición y Eliminación de Zonas Maestras y Esclavas; así como sus Zonas Directas e Inversas, para Servidores DNS Autoritativos y Configuración de Clientes Permitidos para Consultas DNS**

- Creación de una Zona Maestra Directa



**FIGURA 18. Interfaz de Acceso para la Creación de una Zona Maestra Directa**

Fuente: Elaboración propia

A screenshot of a "Zona Maestra Directa" configuration form. It contains the following fields:

|                          |                     |
|--------------------------|---------------------|
| Dominio:                 | ejemplo.gob.bo      |
| Correo admin:            | mail.ejemplo.gob.bo |
| TTL genérico(seg):       | 604800              |
| TTL SOA(seg):            | 604800              |
| Refresh(seg):            | 604800              |
| Retry(seg):              | 86400               |
| Expire(seg):             | 2419200             |
| Negative Cache TTL(seg): | 604800              |

At the bottom are two buttons: "Crear" (Create) in green and "Salir" (Exit) in red.

**FIGURA 19. Campos de llenado Formulario de una Zona Maestra Directa**

Fuente: Elaboración propia



**FIGURA 20. Zona Maestra Directa Creada**  
Fuente: Elaboración propia

- **Edición de una Zona Maestra Directa y Permisos de Consultas DNS**

En esta etapa se puede añadir los Registros de Recurso de la Zona.

| Nombre        | TTL       | Tipo de Registro | Prioridad (MX) | Dato de Registro   |
|---------------|-----------|------------------|----------------|--|
| @             | NS        |                  |                | ns1.example.gob.bo. <span style="color:red">Borrar</span>    |
| ns1           | A         |                  |                | 192.168.100.7 <span style="color:red">Borrar</span>          |
| www           | 10000     | A                |                | 192.168.100.10 <span style="color:red">Borrar</span>         |
| Ej.: www, ns1 | Ej.:86400 | A                |                | Ej.: 192.168.100.1 <span style="color:green">Insertar</span> |

**FIGURA 3-21. Interfaz de Edición de una Zona Maestra Directa**  
Fuente: Elaboración propia



**FIGURA 3-22. Interfaz de Permisos de una Zona Maestra Directa**  
Fuente: Elaboración propia

Una vez guardados los cambios el sistema envía un mensaje indicando si se pudieron guardar los datos correctamente:



**FIGURA 3-23. El Sistema Informa que los Datos de Zona se Cargaron Exitosamente**  
Fuente: Elaboración propia

The screenshot shows a Windows Notepad window titled 'backup\_zonas.txt'. The content of the file is a BIND zone configuration for 'ejemplo.gob.bo'. The code is as follows:

```

zone "ejemplo.gob.bo" {
    type master;
    file "/var/lib/bind/db.ejemplo.gob.bo";
    dnssec-secure-to-insecure yes;
    allow-query {
        192.168.222.0/24;
    };
    allow-transfer {
        none;
    };
    also-notify {};
};

```

**FIGURA 3-24. Archivo Generado por el Sistema con el Resumen de la Zona Maestra Configurada**  
Fuente: Elaboración propia

```

$TTL 604800
@ 604800 SOA ejemplo.gob.bo. mail.ejemplo.gob.bo. (
    4 ; serial
    604800 ; refresh (168 hours)
    86400 ; retry (24 hours)
    2419200 ; expire (4 weeks)
    604800 ; minimum (168 hours)
)
@ NS ns1.ejemplo.gob.bo.
ns1 A 192.168.100.7
www 10000 A 192.168.100.10
@ 10000 MX 10 mail.ejemplo.gob.bo.

```

**FIGURA 3-25. Archivo de Zona Maestra Directa Generada con el Sistema**

Fuente: Elaboración propia

```

; <>> DiG 9.12.3 <>> @192.168.100.7 www.ejemplo.gob.bo
; (1 server found)
; global options: +cmd
; Got answer:
; ->HEADER- opcode: QUERY, status: NOERROR, id: 33676
; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
; WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
www.ejemplo.gob.bo. IN A
; ANSWER SECTION:
www.ejemplo.gob.bo. 10000 IN A 192.168.100.10
; AUTHORITY SECTION:
ejemplo.gob.bo. 604800 IN NS ns1.ejemplo.gob.bo.
; ADDITIONAL SECTION:
ns1.ejemplo.gob.bo. 604800 IN A 192.168.100.7

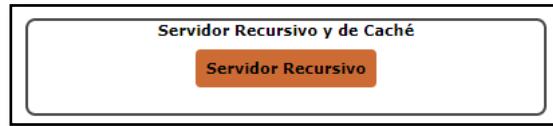
; Query time: 4 msec
; SERVER: 192.168.100.7#53(192.168.100.7)
; WHEN: Sat Feb 01 16:01:30 Hora est&ndar oeste, Sudam&rica 2020
; MSG SIZE rcvd: 97

```

**FIGURA 3-26. Consulta al Servidor por el Host “www.ejemplo.gob.bo” con la herramienta “dig”**

Fuente: Elaboración propia

## B. Configuración de Servidores DNS Recursivos, Zonas de Reenvío y Soporte para el Uso de Direcciones IPv6



**FIGURA 27. Interfaz de Acceso para la Configuración del Servidor Recursivo**

Fuente: Elaboración propia

A detailed screenshot of the configuration interface. It includes sections for enabling recursion (set to 'si'), cache size (100 MB), validating DNSSEC responses (set to 'si'), and retranslating queries (set to 'no'). It also shows a list of allowed recursion networks (192.168.222.0/24) and a list of relay servers (192.168.0.100). At the bottom are buttons for Salir, Descargar, and Guardar.

**FIGURA 28. Configuración del Servidor Recursivo**

Fuente: Elaboración propia



**FIGURA 29. El Sistema Informa que los Datos de Configuración se Cargaron Exitosamente**

Fuente: Elaboración propia

```
C:\Users\henry>dig @192.168.100.7 www.isc.org
;; <>> DiG 9.12.3 <>> @192.168.100.7 www.isc.org
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 48598
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.isc.org.           IN  A
;; ANSWER SECTION:
www.isc.org.      50    IN  CNAME  dualstack.osff2.map.fastly.net.
dualstack.osff2.map.fastly.net. 20 IN  A   151.101.222.217
```

**FIGURA 30. Consulta al Servidor Recursivo sobre el Host Externo “www.isc.org”**

Fuente: Elaboración propia

```
C:\Users\henry>dig @192.168.100.7 www.isc.org +dnssec +multi
;; <>> DiG 9.12.3 <>> @192.168.100.7 www.isc.org +dnssec +multi
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 21926
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.isc.org.           IN  A
;; ANSWER SECTION:
www.isc.org.      60    IN  CNAME  dualstack.osff2.map.fastly.net.
www.isc.org.      60    IN  RRSIG  CHAME 5 3 60 (
20200302140019 20200201134210 28347 isc.org.
Kh8TqgsPAB6hsf0hjF4vG3RT07g0495nbTBV7MS2kPM
1C1a2trDjQFH7Saewu0IUp4X/HlxxygC1xLpixe1lh
0mngfijcUHtq8XYUjK5td+7ropkfBVUlufq05gVVh
rDnXJM07660xfGzfxPfbCARE0fa2cUKtAnkrW0o= )
www.isc.org.      60    IN  RRSIG  CHAME 13 3 60 (
20200302140019 20200201134210 27566 isc.org.
mUuAXTM5D0WILx1X/IX1UhQleKgSmjL2u8FU5q00U33
j4Lm8bDVn0C+80pRTR/qokQ0Nk7i9tUKu4DCGJa2Ew== )
dualstack.osff2.map.fastly.net. 30 IN  A  151.101.222.217
```

**FIGURA 31. Consulta al Servidor Recursivo de Validación sobre un Host Externo que Tiene Implementado DNSSEC**

Fuente: Elaboración propia

- **Prueba de la Zona de Reenvío**

Implementando el sistema en otro servidor con dirección IP **192.168.100.100**, donde se activó la recursión y se configuró la zona de reenvío del dominio “**ejemplo.gob.bo**”, para que reenvíe las consultas al servidor **192.168.100.7**, donde se ubica el servidor autoritativo de ese dominio.



**FIGURA 32. Configuración de una Zona de Reenvío**  
Fuente: Elaboración propia



**FIGURA 33. Resultado de la Creación de la Zona de Reenvío**  
Fuente: Elaboración propia

**FIGURA 34. Archivo Generado por el Sistema con el Resumen de la Zona de Reenvío Creada**  
Fuente: Elaboración propia

```
C:\Users\henry>dig @192.168.100.100 www.ejemplo.gob.bo
;; <>> DiG 9.12.3 <>> @192.168.100.100 www.ejemplo.gob.bo
;; 1 server found
;; global options: +cmd
;; Got answer:
->>HEADER<- opcode: QUERY, status: NOERROR, id: 45962
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
www.ejemplo.gob.bo.           IN      A
;; ANSWER SECTION:
www.ejemplo.gob.bo.    10000   IN      A      192.168.100.10
```

**FIGURA 35. Consulta al Servidor Configurado sobre el Host “www.ejemplo.gob.bo” ubicado en otro Servidor**

Fuente: Elaboración propia

### C. Copia de Respaldo del Sistema de Administración y Configuración de DNS



**FIGURA 36. Creación de una Copia de la BD del Sistema de Administración y Configuración de DNS**

Fuente: Elaboración propia



**FIGURA 37. BD Creada Disponible para su Descarga y Restauración**

Fuente: Elaboración propia

#### D. Uso de Transacciones Firmadas entre Servidores mediante TSIG

Para demostrar su uso debemos configurar un par de servidores, para lo cual teniendo el servidor maestro ya configurado (con la IP 192.168.100.7), es necesario configurar un servidor esclavo en otro servidor (con IP 192.168.100.100) y verificar que las transacciones utilizan TSIG.

- **Configurando servidor esclavo del dominio “ejemplo.gob.bo”, con dirección IP 192.168.100.100.**



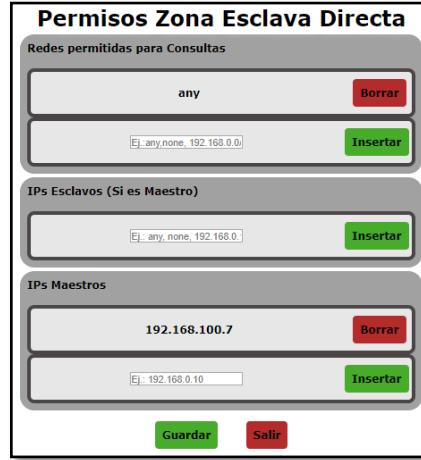
**FIGURA 38. Creación de una Zona Esclava Directa**

Fuente: Elaboración propia



**FIGURA 39. Resultado de la Creación de una Zona Esclava Directa**

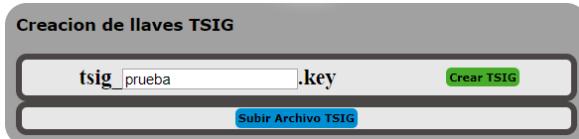
Fuente: Elaboración propia



**FIGURA 40. Configuración de Permisos de una Zona Esclava Directa**

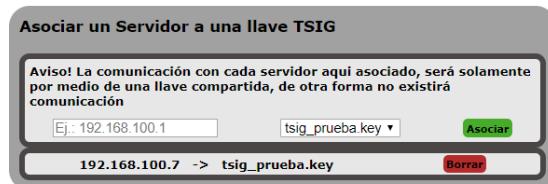
Fuente: Elaboración propia

- **Se crea una clave TSIG en uno de los servidores indistintamente, en este caso será creada en el servidor esclavo con IP 192.168.100.**



**FIGURA 41. Creación de una Clave TSIG en el Servidor Esclavo**

Fuente: Elaboración propia



**FIGURA 42. Asociación de una Clave TSIG con la dirección IP del Servidor Maestro**

Fuente: Elaboración propia

Se descarga la clave TSIG del servidor esclavo con IP 192.168.100.100 y se carga en el servidor maestro con IP 192.168.100.7



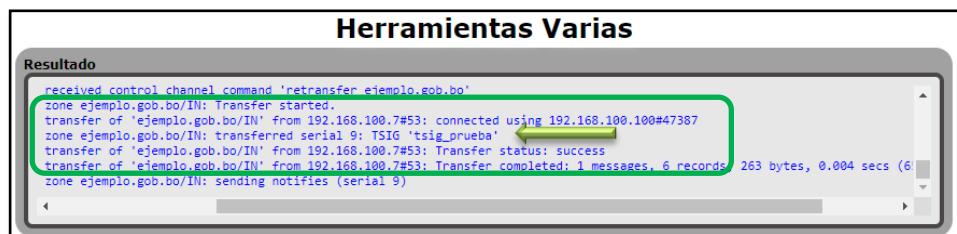
**FIGURA 43. Carga de un Archivo de Clave TSIG al Servidor Maestro**

Fuente: Elaboración propia



**FIGURA 44. Asociación de la Clave TSIG Cargada en el Servidor Maestro**

Fuente: Elaboración propia



**FIGURA 45. Resultado de la Transferencia de Zona entre Servidor Maestro y Esclavo utilizando TSIG**

Fuente: Elaboración propia

```
C:\Users\henry>dig @192.168.100.7 www.ejemplo.gob.bo
;; <>> DiG 9.12.3 <>> @192.168.100.7 www.ejemplo.gob.bo
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 51867
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.ejemplo.gob.bo.           IN      A
;;
;; ANSWER SECTION:
www.ejemplo.gob.bo.    10000   IN      A      192.168.100.10
```

**FIGURA 46. Consulta del Host “www.ejemplo.gob.bo” al Servidor Maestro**

Fuente: Elaboración propia

```
C:\Users\henry>dig @192.168.100.100 www.ejemplo.gob.bo
;; <>> DiG 9.12.3 <>> @192.168.100.100 www.ejemplo.gob.bo
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 56715
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.ejemplo.gob.bo.           IN      A
;;
;; ANSWER SECTION:
www.ejemplo.gob.bo.    10000   IN      A      192.168.100.10
```

**FIGURA 47. Consulta del Host “www.ejemplo.gob.bo” al Servidor Esclavo**

Fuente: Elaboración propia

## E. Uso de DNSSEC y respaldo de claves ZSK y KSK

- Creación de Claves

The image shows two separate windows from a web application. The top window is titled 'Crear Llave KSK' and contains fields for 'Algoritmo' (set to RSASHA256(+008)) and 'Longitud de Llave' (set to 4096), with a green 'Crear KSK' button. The bottom window is titled 'Crear Llave ZSK' and contains similar fields, with a green 'Crear ZSK' button.

**FIGURA 48. Creación de Claves ZSK Y KSK**  
Fuente: Elaboración propia

This screenshot displays a list of created keys for the zone 'ejemplo.gob.bo.' under the heading 'Llaves Creadas para "ejemplo.gob.bo."' There are two entries: 'KSK: Kejemplo.gob.bo.+008+25375.key' and 'ZSK: Kejemplo.gob.bo.+008+47193.key'. Each entry has a red 'Borrar' button and a blue 'Descargar' button. At the bottom of the list are four buttons: 'Key Priv' (green), 'Firmar la Zona' (blue), 'NSEC' (red), and 'NSEC3' (red).

**FIGURA 49. Par de Claves ZSK y KSK creadas**  
Fuente: Elaboración propia

This screenshot provides a detailed view of the created keys. It lists four items under 'Llaves Creadas para "ejemplo.gob.bo."': 'Priv: Kejemplo.gob.bo.+008+47193.private' (red 'Borrar' button), 'KSK: Kejemplo.gob.bo.+008+25375.key' (red 'Borrar' button, blue 'Descargar' button), 'Priv: Kejemplo.gob.bo.+008+25375.private' (red 'Borrar' button), and 'ZSK: Kejemplo.gob.bo.+008+47193.key' (red 'Borrar' button, blue 'Descargar' button).

**FIGURA 50. Vista Desglosada del par de Claves ZSK y KSK**  
Fuente: Elaboración propia

- Firmar una Zona Maestra Directa



**FIGURA 51. Zona Maestra Directa Firmada**

Fuente: Elaboración propia

```
<>> Di6 9.12.3 <>> @192.168.100.7 www.ejemplo.gob.bo +dnssec +multi
(1 server found)
global options: +cmd
got answer:
->>HEADER<- opcode: QUERY, status: NOERROR, id: 15717
flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
EDNS: version: 0, flags: do; udp: 4096
;QUESTION SECTION:
www.ejemplo.gob.bo. IN A
; ANSWER SECTION:
www.ejemplo.gob.bo. 10000 IN RRSIG A 8 4 10000 (
www.ejemplo.gob.bo. 10000 IN RRSIG A 8 4 10000 (
20200302231746 20200201221901 47193 ejemplo.gob.bo.
8d4d1a137Nb6vsSalH2C80Gu0zNhd0U1+U3D
uFpEri110c1gWv1JaxmV1f2kq
Dw+IhLsAeLwv1ab/CST45LNGnsk2P+0
Kf
skTluu3aa2zM7dH6L3tjnHbjn+gPPoSne@11o1e
MatedSKcq9ohkbraT60RpfbBKF2uug+kciITvtHQHw+II
jCh03ejNSasn5k7KyrQbL2PfxzsjkRCJCW5Jb6jU0YY
00Nb iEM@Evat7XfLsKR74H33ssspS0jpVwIE24jkry
CZN9FH95w1D3JQlcymmin9b0G18rw2Jtpg== )
```

**FIGURA 52. Consulta al Servidor Autoritativo y Respuesta sobre el Host “www.ejemplo.gob.bo” con las Firmas Digitales**

Fuente: Elaboración propia



**FIGURA 53. Eliminación de la Firma de la Zona “ejemplo.gob.bo”**

Fuente: Elaboración propia

```

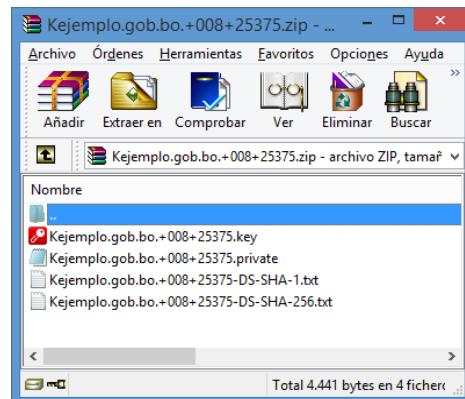
C:\Users\henry>dig @192.168.100.7 www.ejemplo.gob.bo +dnssec +multi
; <>> DiG 9.12.3 <>> @192.168.100.7 www.ejemplo.gob.bo +dnssec +multi
; (1 server found)
; global options: +cmd
; Got answer:
;-->HEADER<- opcode: QUERY, status: NOERROR, id: 59899
; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
; WARNING: recursion requested but not available
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; QUESTION SECTION:
;www.ejemplo.gob.bo. IN A
; ANSWER SECTION:
www.ejemplo.gob.bo. 10000 IN A 192.168.100.10

```

**FIGURA 54. Consulta al Servidor Autoritativo y Respuesta sobre el Host “www.ejemplo.gob.bo” sin las Firmas Digitales tras desactivar la Firma de Zona**

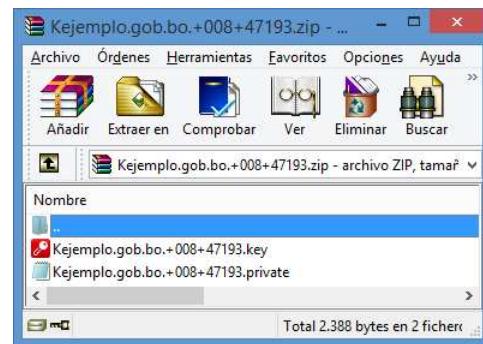
Fuente: Elaboración propia

- Exportar e Importar Claves ZSK y KSK



**FIGURA 55. Archivo de Clave KSK con las Claves Pública y Privada y los Registro DS**

Fuente: Elaboración propia



**FIGURA 56. Archivo de Clave ZSK con las Claves Pública y Privada**

Fuente: Elaboración propia



**FIGURA 57. Botón que Permite la Carga de Claves ZSK y KSK al Sistema**

Fuente: Elaboración propia

- **Uso de NSEC y NSEC3**

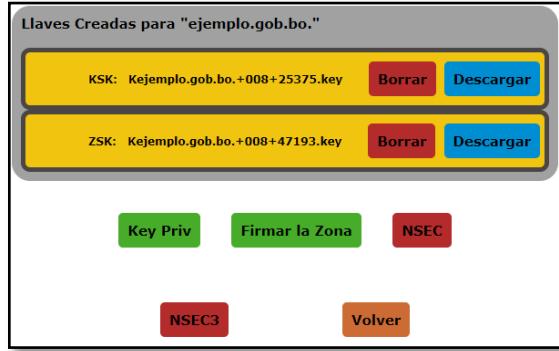
Cuando se firma una zona por defecto se utiliza NSEC para demostrar la no existencia de un registro, en el dominio del que se tiene autoridad. Sin embargo una mejora en la seguridad es el uso de NSEC3.

A continuación se muestra su configuración:

```
><>> Dig 9.12.3 <>> @192.168.100.7 ejemplo.gob.bo A +dnssec +multiline
; (1 server found)
; global options: +cmd
; Got answer:
;-->>HEADER<- opcode: QUERY, status: NOERROR, id: 60794
; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
; WARNING: recursion requested but not available
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; QUESTION SECTION:
;ejemplo.gob.bo. IN A
; AUTHORITY SECTION:
ejemplo.gob.bo. 604800 IN SOA ejemplo.gob.bo. mail.ejemplo.gob.bo. (
    16 ; serial
    604800 ; refresh (1 week)
    86400 ; retry (1 day)
    2419200 ; expire (4 weeks)
    604800 ; minimum (1 week)
)
ejemplo.gob.bo. 604800 IN RRSIG SOA 8 3 604800 (
    20200303000854 2020021230854 47193 ejemplo.gob.bo.
    1/IUNxKLZtlf1Y6KuhmJg6m1Y8rJ2p+h1fi1rc3e6t
    Mf5TgxWfTn7d6cacwJKXselxJf8/MN3jVN0THJWvuxEto
    WIBOYthPjRjNsKKL9ZSP2eu9MEhxH8s2WFze5Mkwoy3P8
    +o7N2Qul2YFT60ynrRDZ+hqbSwGQzUxM6Uq87FoeJ/g
    /vpjLJPxbP+U6/DcUjorK4oxKzhe5hU8SjApEuKppnp
    X3sPg2TJS56uR6kvJgE4pSh2vx0m0/A36jRF4mdhJ
    UhKRFzUELiLyj2FCv7y0UjYTUU/iyH81y1Kpualyn5
    aR0VNmawiznIMZTG0f1om7gJndRNivf0== )
ejemplo.gob.bo. 604800 IN NSEC ns1.ejemplo.gob.bo. NS SOA MX RRSIG NSEC DNSKEY TYPE61
ejemplo.gob.bo. 604800 IN RRSIG NSEC 8 3 604800 (
    20200302234533 2020021230854 47193 ejemplo.gob.bo.
    bpr0/v/b/EgZPlbmQCeuh1nUtazho/B1fdxPm8ok1A
    U4bZupry1l0t0fsI4fjIasvhUUrqhAb01jRy2Rrooh
    Mp43wy+1Xun07LgkjIn7srl40TKjMSEb0jsa23qhi3
    Uytd1ofFMkCSf06naEEExD2F10VKIgwqqICRD68yzIdw
    Mis5Hn5NyUoPCRbsbH65t0jRkp0OfzK0HAAU-Dsy5Hto
    mHn0bzIzASech+bhSNDUCr5hR0UwKhBBWV1e90iCw
    gykHcM2didi02Fx1t2MPUs61268e60gKf6g9zL2i0ibq
    UvnxjmA4zeCUMtTjeRC08ehqD1Udpqo+zQ== )
```

**FIGURA 58. Consulta del Registro “A” de la Zona “ejemplo.gob.bo” que Muestra el Uso de NSEC**

Fuente: Elaboración propia



**FIGURA 59. Interfaz para el Cambio de NSEC a NSEC3 para la Prueba de no Existencia**  
Fuente: Elaboración propia

```
; AUTHORITY SECTION:
ejemplo.gob.bo.      604800 IN SOA ejemplo.gob.bo. mail.ejemplo.gob.bo. (
    19                      ; serial
    604800                  ; refresh (1 week)
    86400                   ; retry (1 day)
    2419200                 ; expire (4 weeks)
    604800                  ; minimum (1 week)
)
ejemplo.gob.bo.      604800 IN RRSIG SOA 3 604800 (
    20200301001 2020021231001 47193 ejemplo.gob.bo.
    f/EOj17tTPGPB/sAM9IQPtGMuTqOioW/4jICvFu31z
    GF8TI17SPfc+fSE51ooyk8RZ31tyLPm70/X1DFzJxg
    /SMMtgecErSZQ16f15553dWJrvsn9RK616b60+JUjm
    AMMP2Kw+/cUThgsffTLN26S0IEQBSQ00071Cg9adUts
    K/L644u6a6/U00KBUEI5XT2sdU62w0vfa4Mpuy0U3rB
    2Pm6WE6ogqaaSrez75ocptL1k/u8mA4Kc6OLHLkJSuX
    ZEk26TSBhSwanXU14Yxir09PMun10cVScgDEAGk/
    V:1UP01Hw+jt+5:0cwu72fE6L29...H0D-20-->
P299A3E7H045JC63TDTEKD085H1BNRM exemplo.gob.bo. 604800 IN NSEC3 1 0 10 002F&CF800162978_0
NN60027J101071R085SD6LKD9J938URS
NS SOA MX RRSIG NSEC3PARAM
TYPE65534 )
LP299A3E7H045JC63TDTEKD085H1BNRM exemplo.gob.bo. 604800 IN RRSIG NSEC3 8 4 604800 (
    20200302231348 2020021231000 47193 ejemplo.gob.bo.
    BV0nwP07wKR01xPk3zScTwu2IB21mfVmBfaZgr/Pry
    JNjNrqxSDJnP/ntIA8GCT0X16r/D05Mi+16z8HE3axrn
    B1xF2w069w09Q0gF8CfukhWU66C1us97Q0Zlirnd
    p4x1eJn/5qt3s+f4nAxAU0qQ0uj6s7stcl+aEl5lsno
    dMWh5+UpkpbGjnHHy4Xy+o0DVb36fjTuf02YiyeFl/Sf
    QRccijQElor86puShJcy/Wu8DWgnqXt1sQsBe7LMzP
    en1x+f8AvnD245tK00n6excdRc6nryBC+6uEvT11YMct
    KfD1DwpTf5nZdZXQYciB6d9iTHzDPEwEsq== )
```

**FIGURA 60. Consulta del Registro “A” de la Zona “ejemplo.gob.bo” que Muestra el Uso de NSEC3**  
Fuente: Elaboración propia

- **Renovación de Claves ZSK y KSK**

La renovación de Claves ZSK y KSK mediante el uso de comando no es sencilla, debido a la cantidad de campos para una correcta renovación.

Para renovar una clave ZSK, se toma en cuenta que la renovación de una clave KSK, es bastante similar, con la diferencia en que en que esta última implica el envío de un archivo que contiene los Registros DS, a la zona padre, que en este caso sería “.gob.bo”.

Antes de renovar la Clave ZSK se muestra las claves actuales del dominio:

**Llaves Creadas para "ejemplo.gob.bo."**

|                                     |        |           |
|-------------------------------------|--------|-----------|
| KSK: Kejemplo.gob.bo.+008+25375.key | Borrar | Descargar |
| ZSK: Kejemplo.gob.bo.+008+47193.key | Borrar | Descargar |

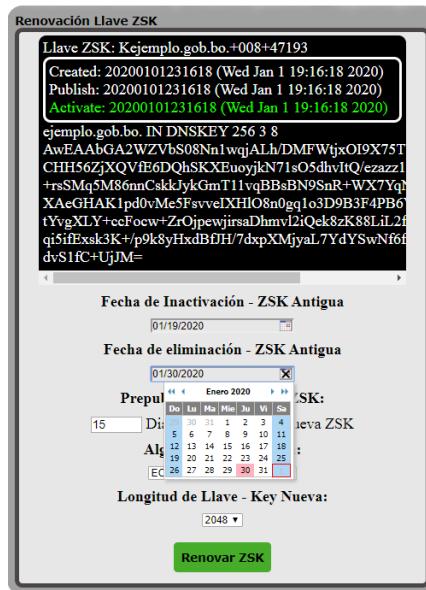
  

```
;; ANSWER SECTION:
ejemplo.gob.bo.          604800 IN DNSKEY 256 3 8 
    AwEAAbGz2VzbS0n1wqjALh/DMFWtjx0I9X75TMeew
    Pp0yq04tozTOCHNS6ZjXQ0FE600hSKxEuoyjkN7s05d
    hvIt0/ezazz1xXdu+15fr+rSMq5M086nnCskkJyKG
    mT11vgBbSH9SnrW-X7TqMFVXF8m1zopGXxeHAK1
    pd0vMe5fsvuIXH108a0gg1a309B3F4PB6WiroUZMa8P
    SmkrtVvgXLV-ccFocus-7r0jpeuirsaDhnw1210ek8ZK
    881il2fsDyu43x8Pq15ifexsk3K+ /p9k8yhxd8bfJH/7d
    xp2Miwal74dVsuhf740BC-SUDEdvS1fc+0jJM
) ; ZSK; alg = RSASHA256 ; key id = 47193
ejemplo.gob.bo.          604800 IN DNSKEY 257 3 8 
    AwEAAkBLyt6suC1igH7qjUbMF70Ph0In5bFlpYRztL
    /Y-a0X0JJ3BorNbHg9BWqT92kh0Ry30Fp7ufPbHKSS
    9a0Bn0501c6KuvAt1TPa5/850+x0e2y5LcGbr/vYTbU
    AzhkrppgBfk9i453/XcDhDE4c1b6G3hBMUReDCn105fb
    LcTBocp4BubtH4Bv0C3qELAuIB8ICVFtu9k161ZMrb
    RtxsNaR1KmbosXtirswZP6Ppfy6du18kP28Ezbh3zyv
    x67SRPPuasSNHku4m82Q61qo2852X1c0p1w1M6-TxMk
    vy23t+ +Z2JbaTPn6Ty60fuP0h3/bzSSp7b0IBeBs
    T0sC211MnaJ0/08GbhbJ0JCBCDr46a5THUHeCrCu2+
    t6ueJdY1d8u7AK6n8f01K8a7nx1fTyHUKkhZ/RDFKa1M
    Ftev5UbzJb4j6eE//Sf1bquHzH0ceyo4/K81a2TKLNlp
    C6Te7z5880PPS4R11wprCxqol_zkZcf7PxEEM5zgSUS/tv
    JB1pu06mf b/UpgHqbpk3r1h0oxu8MoUrbyS8SSjy+e9
    rmwSRW01SyOChii+955164zvupjphshTSrPCQf0/11
    1J8zXm4fc33E0BNaNef0qq92p1f6d5c01wujwP5dp9n
    0rMeoIBz/jiruL0xf7v7e01B
) ; KSK; alg = RSASHA256 ; key id = 25375
ejemplo.gob.bo.          604800 IN RRSIG DNSKEY 3 604800 
    20200204024714 20200105014714 25375 exemplo.gob.bo.
    E18n06ls000p8x6zKluax1gsrcIu0fmcSdsbg7761
    t08G1imYqlaro1hVtU/W0tpqPxrn0pXZ/nP+h0T0p5C/
    L9161hgG6vfc6797QzCB0unP5v05rrHa825kVezk0Sa
    QyRUzudeirK7/kbHJTM3u0hxbLFcq6UVy3Pd4ePkrx
    g0vREBhU5g3e61Z8naJt0h+XoKdg0en5LPKUj0beG
    0xfuFBbPHicmGnp+VagtGBzDmBZTefsLH0U1z0p1
    0+9hj0/oMKiVFF90in/135aMcIaFz0gEf+co+4+1+0
    sc4oKgH2qj-0y0Ku67321Q/mhJF5dK8LHbzwa1zABR/
    aka167j44CDLuhahkx+23aQloj4mkHwdKpofbR66C1m
    Dn1tBr7jklZX/M8252J0G8K0fG0zofpYios23apKvs
    mCcXqeit1df0yj10My0Yr2h/c+9152QMCkfj2h0u94
    yBbIw8RckJjHHxQNg+SE0nkspsb/r0x60HbzZ0wcz
    AvRE01lm91lood10dHk51yDhL9Qv7LkPC2B1oHrVnx
    zETq1auNzSDz1pE61howMcBfgf2n0LWnRwnK0Dge
    QRKbodd0dqSEF26sQa1m17r7Vu1bLspua8XB000CTa
    1vEnyurPHJksaBcrd0du68= )
ejemplo.gob.bo.          604800 IN RRSIG DNSKEY 3 604800 
    20200204024714 20200105014714 47193 exemplo.gob.bo.
    0k5ppE7fca20uy8r+8shK2/eax2Smk/RUsC/Jh0f'sGUx
    cmGMcbWA3mHLy0B8107KfBznxr5ac05EJu8GudRETx/
    PgVnB51b0/bc6nyt/KL+Que2oxyHxd6pouyZfj4kC1G
    3Pw751JP8LMkc6K91okTdworL6Vf4sDmPnmmH10B0m+z
    mCNwASRb-xh1aWb4t8AB/f8hC28u7pHbQlxubBr9yjs
    BsbbX6pyS6IMgunglikijM/mCriz2mRzwZ0mRkt+j0D
    v0Rs2nf8jUigt5K+df00P21nmj03bR6qH078$q80rRP
    uYfuc/GmzMxjjjSLxkwfBk1YC1n/z+Z0w== )

```

**FIGURA 61. Consulta del Dominio por las Claves Públicas de ZSK y KSK y sus Firmas de la Zona “ejemplo.gob.bo”**

Fuente: Elaboración propia



**FIGURA 62. Interfaz de Renovación de Clave que Muestra los Metadatos de Tiempo de la Clave ZSK Actual**

Fuente: Elaboración propia

Ingresando a la opción de Renovar Claves, se pueden encontrar la clave ZSK con los parámetros actualizados

Llave ZSK: Kejemplo.gob.bo.+008+47193

Created: 20200101231618 (Wed Jan 1 19:16:18 2020)  
 Publish: 20200101231618 (Wed Jan 1 19:16:18 2020)  
 Activate: 20200101231618 (Wed Jan 1 19:16:18 2020)  
 Inactive: 20200120030146 (Sun Jan 19 23:01:46 2020)  
 Delete: 20200131030146 (Thu Jan 30 23:01:46 2020)  
 (manualmente)

```

ejemplo.gob.bo. IN DNSKEY 256 3 8
AwEAAbGA2WZVbS08Nn1wqjAL.b/DMFWtjxO19X75TWeevPp
CHH56ZjXQVf6DQhSKxEuoyjkN71s05dhvItQ/ezazzJxXcdv+
+rsSMq5M86nmCskkJykGmT11vqBBsBN9SnR+WX7YqNWFtX
XAeGHAK1pd0vMe5FsvveIXHlO8n0gg1o3D9B3F4PB6ViroVZ
tYvgXLY+ccFocw+ZrOjpewjrsaDhmvl2iQek8zK88L.iL2fS0yw43
qj5ifExsk3K+/p9k8yHxdBfJH/7dxpXMjyaL7YdYSwNff74QBC
dvS1fc+UjJM=
  
```

Llave ZSK: Kejemplo.gob.bo.+013+09368

Created: 20200105030136 (Sat Jan 4 23:01:36 2020)  
 Publish: 20200105030146 (Sat Jan 4 23:01:46 2020)  
 Activate: 20200120030146 (Sun Jan 19 23:01:46 2020)

```

ejemplo.gob.bo. IN DNSKEY 256 3 13
4euf79D15nJROly0jXZYMR9XnEYdLn4KkyetVlyThR6CxDKut
QsoBLF8YGL0v0UnEq7526YqWoS12Yw==
  
```

**FIGURA 63. Clave ZSK Actual con Fechas de Inactivación y Eliminación y Clave ZSK Nueva Próxima a Activarse**  
 Fuente: Elaboración propia



**FIGURA 64. Nueva Clave ZSK y Clave ZSK Antigua sin Botón de Eliminación hasta que la Fecha de Inactivación se Cumpla**  
 Fuente: Elaboración propia

```

; <>> Dig 9.12.3 <>> @192.168.100.7 ejemplo.gob.bo DNSKEY +dnssec +multiline
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 59643
; flags: qr aa rd; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
; WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; QUESTION SECTION:
ejemplo.gob.bo.          IN  DNSKEY

; ANSWER SECTION:
ejemplo.gob.bo.      604800 IN  DNSKEY 257 3 8 C
                        AwEAAZkDlyt6suCiiH7qjUbMf70PhUtn5bfLpYBzTLL
                        /Y+RDX0J3hOrNbNgqBwqZty2kH0ry30Fp71uPbaKSS
                        9aU8n0S01c6KuvAflTPa/858*x0eZy5ElcGbr/wYTDU
                        fzMrppg0fk9i453/XcDNE4c1wG3h8MUHDCn0i5Fb
                        LcTB0cp4BUbhT4AbvC3ELA1B8ICVFTrwQk1G1pZMrb
                        RtxNaB1kmBvsXtirisuZPGPAfyd6ut8kp28Ezbh3zyPv
                        x675SRPPUsNNHKuAM8ZUq61qo2852Xle0pjwIu6-TxMk
                        uy23E+*Z0ZJBaTPm6kTyg6ufuUh3/b0Z$Sp7b0IBe0s
                        10sC21lMnaJ0/U68hh0J0CB0r9g46aSTHU0HeVcRcWu2-
                        t6uejdY1ldu78K6a8fV1KA87nx1fLyHUKkhZ/RDfKa1M
                        Ftvе15UbzJb4j6eE//Sf1hqvhZNoeyo4Bk1g2TK1NLp
                        C6Te7zS880PPSAB1lwprCxqolzkc7p7xEM5zgS8Ss/tv
                        JBfpq06nFbUpPNaqbk3rlhQoxXuRMoUrS8Ssjiy+C9
                        msSRuN01Sy0Ch9+i5S516FzvulphxhTSrPCQf0/11
                        iJ8zKnkf33EQBQNaEf0qq92ipF6u5c0YuuwjwP5wp9n
                        qRMeoIBFz/JjruLqxfE7Y7e0610
                        ) ; ZSK; alg = RSASHA256 ; key id = 25375

ejemplo.gob.bo.      604800 IN  DNSKEY 256 3 8 C
                        AwEAnbGA2VzVs08Nn1wqjAlh/DMFWtjx0I9X75TWeev
                        Pp0ya04tozTOCHH56ZjXQ0FE60QhsKXEuoyjkN71s05d
                        hv1lq/eazz1xXcdv+f+15Fr+r+sSMsM86nnsskjykg
                        mT11qBBsBN9SnR+jWY7VqMUFxFYFBnn1zopGXeGHAK1
                        pd0WeF5sveeIXH108nfgq1o3D983F4PB6iroUZMa8P
                        SmRktYvgXLY+cceFcw+rz0jpeuwjrsadhmv12i0ek8zK
                        88Lil2FS0yu43x8Pqi5iftxsks3K+p9k8yHxDfJH/7d
                        xpXMjya17YdYsNsH740BCrSUQEdvS1fC+Uj,M=
                        ) ; ZSK; alg = RSASHA256 ; key id = 47193

ejemplo.gob.bo.      604800 IN  DNSKEY 256 3 13 C
                        4euF9B15nJRB0ly0jXZMB89XnEydnln4WkyetUlyThB6C
                        xOKutuirajhm0s0RIyF961l0u0InFa7526Yn0nS129w==

ejemplo.gob.bo.      604800 IN  RRSIG DNSKEY 8 3 604800 (
                        20200204030312 2020105020312 25375 ejemplo.gob.bo.
                        WEivtCjthgkRaeMhe8bh5xH509mJp1GwZxt+nmvJPe1
                        poF6R+E-KPtCqqu06o6eh0RJS5uUnN80XpTMeAOmhwgM
                        oS1hBLIxwU05dGpuB9i1PlkwmrC1r9SUSKBxvmoBjC7
                        3S1IEk2P2e1u/dhix1u0tKaucZJnxlvcohsB3LgrPpC
                        j4hSjqhUbisPuZtej5gXXxeHszefIUbZuhEBLcfaf6t7
                        FNB10u8s281i9gbImyJfw1Bt26LUn0WEw0669dMgea6Q
                        LR1E9Yn0fFitug8x8bktq60z1g6/n54J0BF56p1Mqe
                        0DRF7k21jP7PqcBYB01jxdwM0+003P4vc/80d6JQX0f
                        ky5QfSC61E/YV1J7i1l0+*RyDg,Jhu60SPakfSPrVmh
                        Vc2zUc+50YH/TuBn0IMeho0ouxYe*9kptUf3.j1l5Wr
                        ehfMBw4YgrTD6iyF2767850yKuw-00ltw7tSbjv1HWrx
                        K7u8MDQquS05YfNa+Pj715z795QHx1a7ch3mRMzQ5hpX
                        ahTPSSNrg00XgaF4yRgHemcEESuWSF61gU3b1d27bu0
                        57N7yUqfvZ0231DKhUScwuk6/+kb7PD6xZiBjpaQmr6H
                        UNN10d0w88rReY6178c1a2erYZK1ZhXQx3MLjUXDxts
                        Yik28z15EYzE9/IndLkgebw= )

ejemplo.gob.bo.      604800 IN  RRSIG DNSKEY 8 3 604800 (
                        20200204030312 2020105020312 47193 ejemplo.gob.bo.
                        ZHT6rMpWUd07T/LfJ4M02J7GQ7/Ho1+mQa4qD1gIzv
                        Q47Fy9G0g6d+uBMe6n7zeE1uIuXHQ1777hb4uRgEjMUS
                        +CCqg0d1MFfCp6hY0u1X1XH+bz9Xsc2U3pujmD1MqS
                        K612ZnAaVuLQBH1+81BFEmxrA30yb0ER196/e6Q0MfeYK
                        J/cXFzuGc+WDTHYrxnbHT+0XYZgn0ILyRnPRCmpKRCW
                        ZxP/1g8oXaB4+SpApAildknE0Jf2s66xMfpCa2FzRz50
                        Bj1Qc+ichPqkCosqSEs04h081hkETShrWIwAnD9qJld
                        nrPp+kC9UhAhhYfDso796pvbj3M6yEdcB@= )

```

**FIGURA 65. Fig. Nueva Clave ZSK Pre-Publicada Sin Firma Digital Hasta su Fecha de Activación**  
Fuente: Elaboración propia

## F. Uso de RNDC para tareas de monitoreo del estado del sistema y diagnóstico del servicio DNS

- Estado del Servicio de DNS



**FIGURA 66. Interfaz de Consulta de Estado del Servicio DNS y Ventana de Resultados**  
Fuente: Elaboración propia

A screenshot of a terminal window titled 'Resultado' showing the status of the bind9 service. The output is as follows:

```
* bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-02-01 22:32:35 -04; 3 weeks 6 days ago
     Docs: man:named(8)
   Process: 4478 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
   Main PID: 4546 (named)
  CGroup: /system.slice/bind9.service
          -4546 /usr/sbin/named -t -u bind
```

**FIGURA 67. Resultado de la Consulta “Estado de DNS”**  
Fuente: Elaboración propia

A screenshot of a terminal window titled 'Resultado' showing the status of the bind9 service after it has been stopped. The output is as follows:

```
* bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Sat 2020-01-04 22:39:19 -04; 3s ago
     Docs: man:named(8)
   Process: 4815 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
   Process: 4546 ExecStart=/usr/sbin/named -t $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 4546 (code=exited, status=0/SUCCESS)
```

**FIGURA 68. Resultado de Detener el Servicio DNS**  
Fuente: Elaboración propia

```

Resultado
Jan 04 22:39:59 raspberrypi named[4878]: automatic empty zone: A.E.F.IP6.ARPA
Jan 04 22:39:59 raspberrypi named[4878]: automatic empty zone: B.E.F.IP6.ARPA
Jan 04 22:39:59 raspberrypi named[4878]: automatic empty zone: 8.B.D.0.1.0.0.2.IP6.ARPA
Jan 04 22:39:59 raspberrypi named[4878]: automatic empty zone: EMPTY.A5112.ARPA
Jan 04 22:39:59 raspberrypi named[4878]: command channel listening on 127.0.0.1#953
Jan 04 22:39:59 raspberrypi named[4878]: managed-keys-zone: loaded serial 0
Jan 04 22:40:00 raspberrypi named[4878]: zone ejemplo.gob.bo/IN: exemplo.gob.bo/MX 1r
Jan 04 22:40:00 raspberrypi named[4878]: zone ejemplo.gob.bo/IN: loaded serial 9
Jan 04 22:40:00 raspberrypi named[4878]: all zones loaded
Jan 04 22:40:00 raspberrypi named[4878]: running
Jan 04 22:40:00 raspberrypi named[4878]: zone ejemplo.gob.bo/IN: sending notifies (se

```

**FIGURA 69. Resultado de la Consulta de Logs del Sistema relacionados al servicio DNS**

Fuente: Elaboración propia

- Estado del Sistema



**FIGURA 70. Interfaz de Consulta del Estado General del Sistema**

Fuente: Elaboración propia

```

Resultado
La fecha y hora del Sistema es:
Sat Jan 4 22:36:15 -04 2020

```

**FIGURA 71. Resultado de la Consulta “Hora Sistema”**

Fuente: Elaboración propia

```

Resultado
up 6 hours, 1 minute

```

**FIGURA 72. Resultado de la Consulta “server uptime”**

Fuente: Elaboración propia

**Resultado**

```

1: lo: mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00
        valid_lft forever preferred_lft forever
2: eth0: mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether b8:27:eb:03:aa:e2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.7/24 brd 192.168.100.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::ba27:ebff:fe03:aae2/64 scope link
        valid_lft forever preferred_lft forever
3: wlan0: mtu 1500 qdisc noqueue state DOWN group default qlen 1000

```

**FIGURA 73. Resultado de la Consulta “info Red”**  
Fuente: Elaboración propia

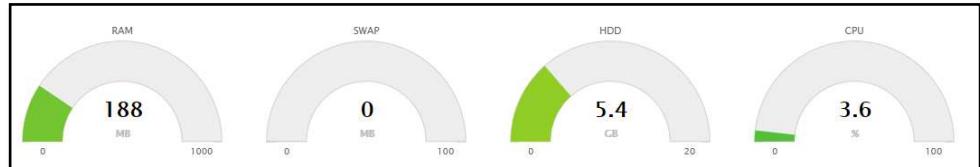
**Resultado**

```

* networking service - Raise network interfaces
  Loaded: loaded (/lib/systemd/system/networking.service; enabled; vendor preset: enabled)
  Active: active (exited) since Sat 2020-02-01 16:36:20 -04; 3 weeks 6 day
    Docs: man:interfaces(5)
  Process: 296 ExecStart=/sbin/ifup -a --read-environment (code=exited, status=0/SUCCESS)
  Process: 278 ExecStartPre=/bin/sh -c [ "$CONFIGURE_INTERFACES" != "no" ] && [ -n "$(if
 Main PID: 296 (code=exited, status=0/SUCCESS)
 CGroup: /system.slice/networking.service

```

**FIGURA 74. Resultado de la Consulta “Estado de Red”**  
Fuente: Elaboración propia



**FIGURA 75. Resultado de la Consulta “Info Recursos”**  
Fuente: Elaboración propia

- Estado de Zonas Maestras y Archivos de Configuración



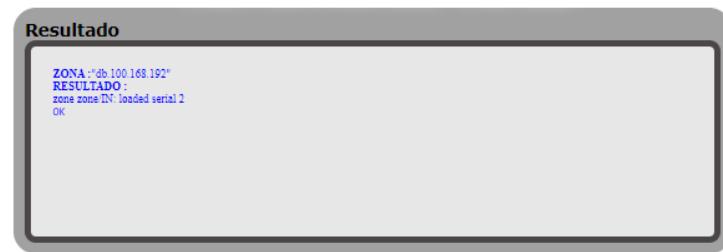
**FIGURA 76. Interfaz de Consulta de Estado de Zonas y Archivos de Configuración**

Fuente: Elaboración propia



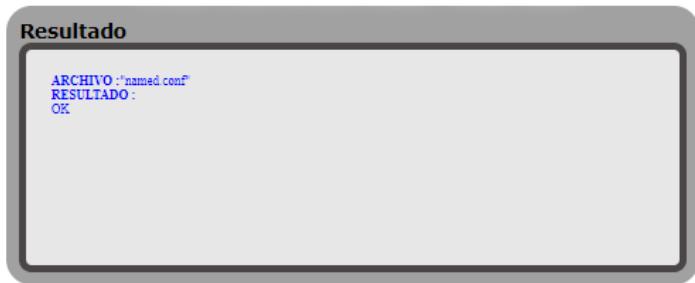
**FIGURA 77. Resultado de la Consulta “Check Zona Dir.” con Resultado Exitoso**

Fuente: Elaboración propia



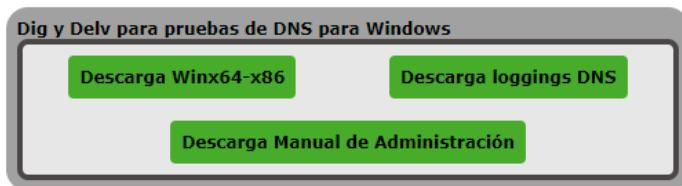
**FIGURA 78. Resultado de la Consulta “Check Zona Inv.” con Resultado Exitoso**

Fuente: Elaboración propia



**FIGURA 79. Resultado de la Consulta “Check Conf” con Resultado Exitoso**

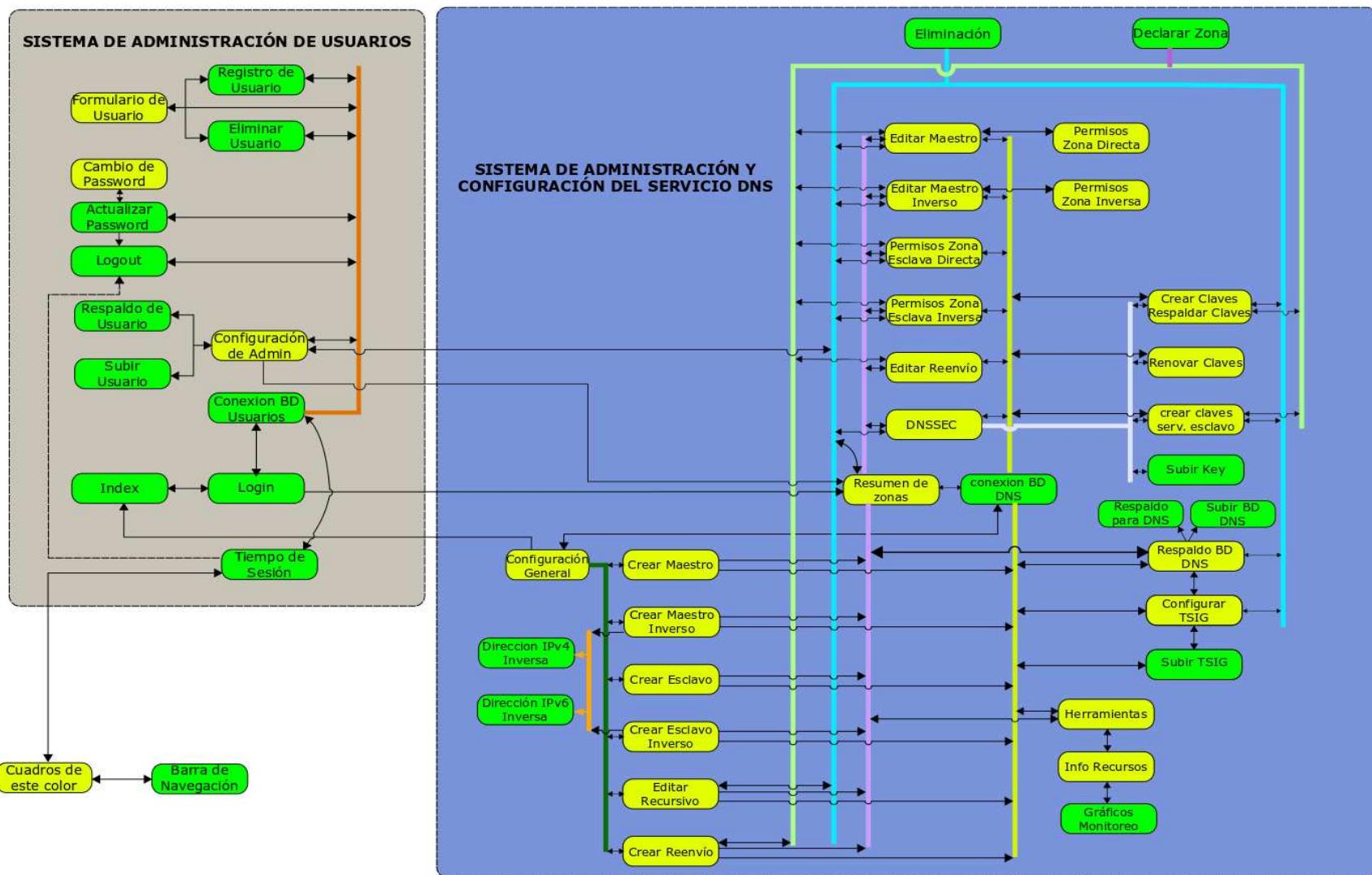
Fuente: Elaboración propia



**FIGURA 80. Interfaz de Descarga del Manual de Administración del Sistema, Herramienta DIG y DELV, y Descarga de Registros del Servicio DNS**

Fuente: Elaboración propia

**ANEXO B: DIAGRAMA DE BLOQUES DEL  
SISTEMA**



**FIGURA 1. Diagrama de Bloques del Sistema de Administración Web**  
 Fuente: Elaboración propia