# UNIVERSIDAD NACIONAL DE LOJA

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

### CARRERA DE INGENIERÍA EN SISTEMAS

***"Implementación de protocolos seguros y herramienta de monitoreo para la red de datos del Gobierno Autónomo Descentralizado Municipal de Loja"***

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


**Autores:**

Henry Cristian Cuesta Vega

Franklin Rolando Mingo Morocho

**Director:**

Ing. Gabriela Viñán Rueda, Mg. Sc.


**Loja – Ecuador**

**2014**

# Certificación del Director

Ingeniera

Gabriela Viñán Rueda, Mg. Sc.

**DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA UNIVERSIDAD NACIONAL DE LOJA**

## CERTIFICA:

Que el presente proyecto fin de carrera elaborado previo a la obtención del Título de Ingeniería en Sistemas, titulado: **"Implementación de protocolos seguros y herramienta de monitoreo, para la red de datos del Gobierno Autónomo Descentralizado Municipal de Loja."**, realizada por los Egresados **Henry Cristian Cuesta Vega** y **Franklin Rolando Mingo Morocho**, cumple con los requisitos establecidos por las normas generales para la graduación en la Universidad Nacional de Loja, tanto en aspecto de forma como de contenido.

Por lo tanto, autorizo proseguir los trámites legales para su presentación y defensa.

Loja, 09 de octubre del 2014

Ing. Gabriela Viñán Rueda, Mg. Sc.

**DIRECTORA DE TESIS**

# AUTORÍA

Nosotros Henry Cristian Cuesta Vega y Franklin Rolando Mingo Morocho declaramos ser autores del presente trabajo de tesis y eximimos expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente aceptamos y autorizamos a la Universidad Nacional de Loja, la publicación de nuestra tesis en el Repositorio Institucional - Biblioteca Virtual.

| | | |
|---|---|---|
| **Autor:** | Henry Cristian Cuesta Vega | Franklin Rolando Mingo Morocho |
| **Firma:** | …… | …… |
| **Cédula:** | 1104225865 | 1104879380 |
| **Fecha:** | 4 de noviembre de 2014 | |

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

Nosotros **Henry Cristian Cuesta Vega** y **Franklin Rolando Mingo Morocho**, declaramos ser autores de la tesis titulada: **Implementación de protocolos seguros y herramienta de monitoreo, para la red de datos del Gobierno Autónomo Descentralizado Municipal de Loja**, como requisito para optar al grado de: **Ingeniero en Sistemas**; autorizamos al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

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

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

Para la constancia de esta autorización, en la cuidad de Loja, cuatro días del mes de noviembre del dos mil catorce.

**Firma:** …….
**Autor:** Henry Cristian Cuesta Vega
**Cédula:** 1104225865
**Dirección:** Loja (Ciudadela del Maestro)
**Correo Electrónico:** cristiancv100@gmail.com
**Teléfono:** 2573991 **Celular:** 0993276248

**Firma:** ……
**Autor:** Franklin Rolando Mingo Morocho
**Cédula:** 1104879380
**Dirección:** Loja (Barrio Belén Av. Isidro Ayora y Virgilio Rodas)
**Correo Electrónico:** wolf.Aries89@gmail.com
**Teléfono:** 2552443 **Celular:** 0989515980

**DATOS COMPLEMENTARIOS**

**Director de Tesis:** Ing. Gabriela Viñan Rueda, Mg. Sc.

**Tribunal de Grado:** Ing. Henry Patricio Paz Arias, Mg. Sc.
Ing. Lorena Elizabeth Conde Zhingre, Mg. Sc.
Ing. Waldemar Victorino Espinoza Tituana, Mg. Sc.

# Agradecimiento

A mis padres les agradezco el haberme inculcado valores humanos, el brindarme la educación necesaria para llegar a dónde me encuentro hoy, gracias por ser el soporte principal en mi vida.

A la Universidad Nacional de Loja y docentes de la carrera de Ingeniería en Sistemas, por ayudar a desarrollarme profesionalmente y aprobar el desarrollo de esta tesis.

Atte.: Henry Cuesta

Ante todo a Dios por brindarme salud durante el desarrollo de la tesis la sabiduría necesaria para cumplir con cada uno de los objetivos del proyecto.

Al administrador de la red de datos del GAD por coordinar y supervisar los avances en cada una de las fases y brindar las facilidades para la implementación del proyecto.

Atte.: Franklin Mingo

# Dedicatoria

A mis padres por el apoyo y motivación constante, a mi familia, les dedico este documento como el fruto del esfuerzo y empeño puesto en la realización de este proyecto de fin de carrera.

Atte.: Henry Cuesta

Este trabajo se lo dedico a mis padres por el apoyo brindado desde que inicie la carrera hasta la obtención del título.

Atte.: Franklin Mingo

# Cesión de Derechos

Los autores del presente trabajo investigativo, autorizamos a la Universidad Nacional de Loja hacer uso del mismo en lo que estime sea conveniente con fines académicos para la divulgación de información.

# a. Título

“Implementación de protocolos seguros y herramienta de monitoreo, para la red de datos del Gobierno Autónomo Descentralizado Municipal de Loja”.

# b. Resumen

Usar protocolos seguros y certificados digitales, en los servicios de red de instituciones públicas o privadas, permiten el acceso seguro a la información confidencial; al tratarse de una comunicación segura, se garantiza que la identidad del servidor al que se conecta es el apropiado y esta conexión está debidamente cifrada desde el momento en el que se inició, es por este motivo que el presente trabajo brinda una solución con la implementación de protocolos seguros.

En el desarrollo del tema propuesto, se emplean técnicas de investigación como la entrevista y encuesta con el fin de determinar en qué condiciones se encuentra la red de datos del GAD Municipal de Loja, identificar posibles amenazas y vulnerabilidades más críticas y relacionarlas con el tema.

Se realizó una réplica del servicio de correo con las aplicaciones que se utilizan en la red de datos, se usa la distribución de Linux Debian Wheezy como sistema base, sobre el que se instalarán y configuraran cada una de las aplicaciones para usar certificados digitales, todo esto en un entorno controlado a fin de preparar las mejoras de seguridad correspondientes antes de su implementación.

Además de las configuraciones mencionadas anteriormente, también se utilizó VPN IPSec, que brinda una comunicación segura en la capa red del modelo OSI, creando un canal seguro, sobre uno inseguro, garantizando que la información no sufra ningún cambio entre los extremos de la comunicación.

Para tener un control de los servicios de la red de datos se eligió Nagios como herramienta de monitoreo y control de estados de los servicios de cada uno de los equipos que se desee monitorear.

Con el uso de certificados digitales se tiene una comunicación segura, mientras que Nagios permite el seguimiento del estado de los servicios.

# Summary

Using secure protocols and digital certificates, network services from public or private institutions, allow safe access to confidential information, as it is a secure communication ensures that the identity of the server to which connect its appropriate and this connection is properly encrypted from the moment the connection is started, it is for this reason that this document provides a solution with the implementation of secure protocols.

In developing the proposed topic, techniques were used as the interview and poll in order to determine under what conditions the data network of the Municipal GAD Loja is, identify potential threats and most critical vulnerabilities related to the topic.

It was decided to provide security to public services of the institution, a replica of the mail service was performed with the applications that are used in the data network, using the Linux distribution Debian Wheezy as a base system, on which will be installed and will configure each of the applications using digital certificates, all in a controlled environment to prepare relevant safety improvements before implementation.

In addition to the above configurations, VPN IPSec is also used, which provides secure communication on the network layer of the OSI model, creating a secure channel over an insecure, ensuring that information is any way between the ends of the communication.

To keep track of the web services data, it was decided to use Nagios as a tool for monitoring and controlling service statuses of each of the computers you want to monitor.

With the use of digital certificates you have a secure communication, while Nagios allows monitoring service status.

# Índice de Contenidos

## Índice General

## Índice de Figuras

## Índice de Tablas

# c. Introducción

En esta era de las nuevas tecnologías de la comunicación, es indispensable que cualquier empresa o Institución deba emplear redes de datos y su activo principal es la información que desean compartir entre miembros de dicha organización, por ejemplo aplicaciones web, bases de datos, correo electrónico, mensajería instantánea y otros servicios. Cada día es más sencillo establecer algún tipo de comunicación, esto gracias al avance tecnológico de nuevos dispositivos y lo asequible que es contratar un servicio de internet actualmente; esto obliga a las entidades sean del sector público o privado a implementar redes informáticas, y mediante estás alcanzar mayor competitividad ante el mercado.

Es por esto que en cualquier red de datos es de vital importancia brindar seguridad a los servidores sean estos accedidos por personal de la empresa o de acceso público mediante internet. Es necesario brindar periódicamente mejoras de seguridad a las comunicaciones que los sistemas ofrecen, al no realizar esta tarea exponemos a que la información de vital importancia sea interceptada por personas con fines maliciosos, se corre el riesgo de que los usuarios sean víctimas de estafas y fraudes electrónicos. Es por esta razón que planteamos realizar nuestro tema de tesis “Implementación de protocolos seguros y herramienta de monitoreo para la red de datos del Gobierno Autónomo Descentralizado Municipal de la ciudad de Loja”, de acuerdo a este tema se pretende dar solución al siguiente problema de investigación:

***La seguridad lógica existente dentro de la Institución no permite establecer comunicaciones seguras, es decir comprobar la integridad de la información desde los servidores a los clientes autorizados y verificar la autenticidad de los equipos, el sistema de monitoreo es básico, no brinda información en tiempo real tanto de los servicios como de los equipos correspondientes***.

El principal objetivo de este proyecto es “Implementar el Sistema de Monitoreo y el establecimiento de protocolos para mejorar la seguridad de las comunicaciones en la de red de datos del GAD Municipal de Loja”.

La ejecución de esta investigación se la delimitó a mejorar la seguridad de los servidores públicos para establecer comunicaciones seguras y mantener el debido control del estado de los servicios ayudando así, de manera oportuna a solventar problemas en dichos servicios.

Durante el transcurso de esta investigación se llevó acabo las siguientes fases previamente planteadas:

*Desarrollo de la situación actual:* Ayudó a comprender cuál es la realidad actual de los servicios de la red de datos.

*Planteamiento de la solución:* En base a resultados anteriormente obtenidos se eligió los correctivos pertinentes a intervenir como solución al problema general de investigación.

*Configuraciones:* Se trabajó con las aplicaciones que actualmente cuenta la Institución en un ambiente de equipos virtualizados para replicar el comportamiento de los servicios y llevar acabo las respectivas pruebas de funcionamiento con las nuevas configuraciones respectivas.

*Evaluación y pruebas de la solución:* Este tipo de pruebas tienen como propósito evaluar el correcto desempeño de los servidores con las respectivas configuraciones aplicadas. Luego de esto también se realiza un contraste entre el nuevo estado de los servicios y el estado que estuvieron antes de realizar las respectivas configuraciones de seguridad en las comunicaciones.

# d. Revisión Literaria

## 1. Adquisición de información (Information Gathering)

Más conocido como prueba de penetración, consiste en realizar el ataque a un sistema informático y de encontrar fallas o vulnerabilidades en la seguridad obtener información relevante del sistema víctima.

Para entender mejor por qué este tipo de pruebas es tan importante, imaginemos lo siguiente, por ejemplo alguien que quiere robar un banco. Los ladrones no precisamente, se levantan de un día para otro y determinan un objetivo (banco). Ellos, primero necesitan reunir una información preliminar. Visitarán las principales sucursales para observar los horarios de entrada y salida de los guardias de seguridad, localizarán las cámaras de seguridad, sistemas de alarma y quizás su fabricante. Adicionalmente usarán las páginas blancas para localizar direcciones y levantarán un mapa de la entidad para planear una ruta de entrada.

Exactamente como en los robos de bancos, el primer paso para atacar máquinas es investigar el objetivo, utilizando la información que esté disponible. En la mayoría de los casos, el éxito del ataque depende de la cantidad de información reunida acerca del objetivo. Si la información ha sido reunida correctamente y con todo detalle, el acceso a los sistemas está garantizado.

### 1.1. Google como herramienta de búsqueda de información

Es una técnica que utiliza parámetros especiales de google, con la finalidad de conseguir búsquedas avanzadas y precisas para obtener datos críticos que pudiesen comprometer a personas particulares y empresas de carácter público o privado.

Esta técnica se continúa empleando actualmente que con tan solo hacer unas simples consultas a través del buscador podemos encontrar información sensible sobre un objetivo como archivos de configuración, puntos de acceso, claves y contraseñas de sistemas, datos personales, e-mails entre otras cosas y para lo que es más utilizado búsqueda de puntos vulnerables.

Para la obtención de esta información, se realizó una búsqueda sencilla usando google y enviándole como parámetro parte del nombre de la Institución, como

podemos observar en la figura 1, el primer resultado nos brinda el dato del sitio web del GAD Municipal de Loja (www.loja.gob.ec).

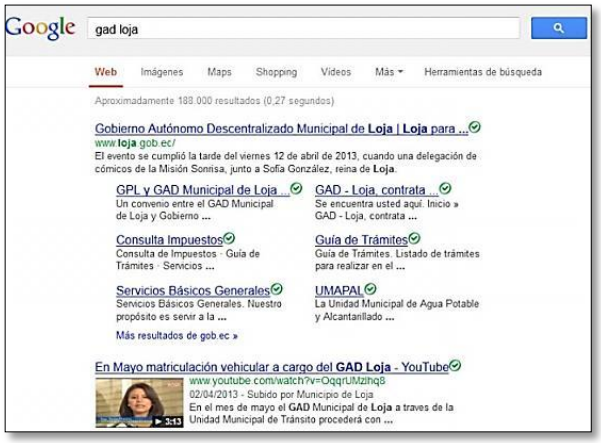



Figura 1: Dirección web del GAD Municipal de Loja.

## 1.2. Uso de herramientas de búsqueda mediante ip/dominio.

Las aplicaciones aquí descritas fueron usadas para realizar consultas whois, whois es la mayor base de datos que existe a nivel mundial acerca de los nombres de dominio registrados y accesibles desde internet, entre estas podemos clasificarlas en herramientas desde consola y en herramientas de tipo web.

### 1.2.1. Herramientas usadas desde terminal linux

#### 1.2.1.1. Comando Ping

Es el primer comando que todo atacante debe conocer, un simple ping da información útil. Al ejecutar esta instrucción con un nombre del dominio, el programa analiza la dirección IP del host y la imprime en la pantalla, el resultado se puede apreciar en la figura 2, dando como resultado la dirección IP del servidor al cual se le está realizando la consulta.

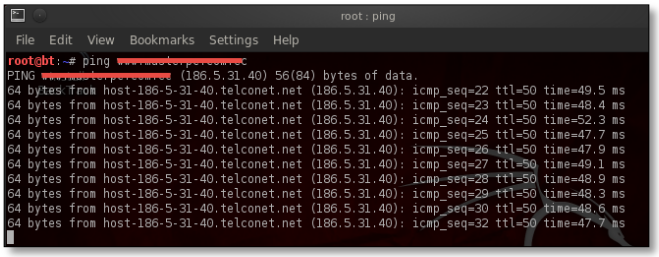



Figura 2: Uso simple del comando ping, para identificar la ip de un sitio.

#### 1.2.1.2. Whois

Es una herramienta utilizada para comprobar la disponibilidad de un dominio y para obtener información sobre la persona o entidad que lo posee.

Además de hacer búsquedas, la variedad de bases de datos whois en internet es demasiado útil como fuente de información. Estas bases de datos contienen una gran variedad de elementos con respecto a la asignación de direcciones en internet, nombres de dominio y contactos individuales.

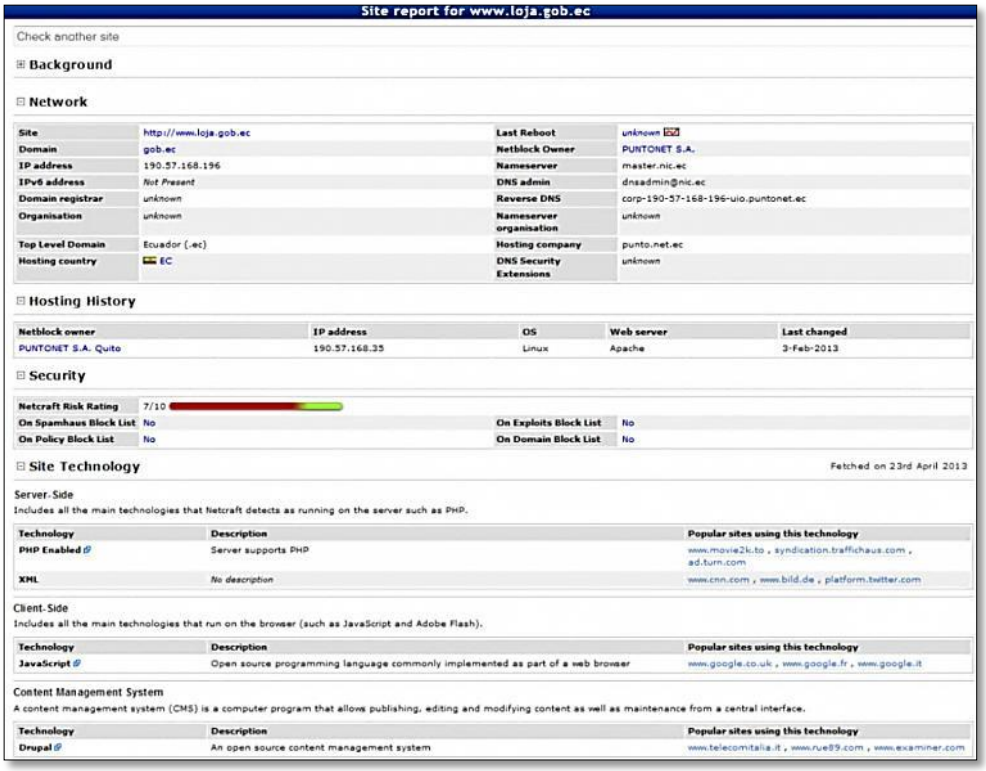
Por otra parte además de nombres de dominio y direcciones de red, algunas bases de datos whois están llenas de información correspondiente a los empleados que son responsables de los servidores y la conectividad de dichas organizaciones inclusive otros muestran la ubicación geo referenciada del dominio. Esta información puede ser utilizada por el atacante con el fin de crear un perfil de las personas que crearon el dominio o por el contrario para reunir información de dichas personas, lo suficiente; como para realizar un ataque de Ingeniería Social.

Muchas versiones de UNIX poseen el comando ***"whois"*** incluido; sin embargo las grandes posibilidades de Internet y la evolución de los navegadores, permiten utilizar herramientas vía web más precisas.

### 1.2.2. Herramientas usadas desde navegador web

#### 1.2.2.1. Sitio searchdns.netcraft.com

Esta herramienta web recopila información sobre el sistema operativo, servidor web usado, el tiempo que lleva el servidor funcionando (uptime), propietario del espacio de direcciones IP, o el historial de cambios relacionados con el servidor web y el Sistema Operativo, como lo muestra la figura 3.



Site report for www.loja.gob.ec

Check another site

Background

Network

| | | | |
|---|---|---|---|
| Site | http://www.loja.gob.ec | Last Reboot | unknown |
| Domain | gob.ec | Netblock Owner | PUNTONET S.A. |
| IP address | 190.57.168.196 | Nameserver | master.nic.ec |
| IPv6 address | Not Present | DNS admin | dnsadmin@nic.ec |
| Domain registrar | unknown | Reverse DNS | corp-190-57-168-196-uio.puntonet.ec |
| Organisation | unknown | Nameserver organisation | unknown |
| Top Level Domain | Ecuador (.ec) | Hosting company | punto.net.ec |
| Hosting country | EC | DNS Security Extensions | unknown |

Hosting History

| Netblock owner | IP address | OS | Web server | Last changed |
|---|---|---|---|---|
| PUNTONET S.A. Quito | 190.57.168.35 | Linux | Apache | 3-Feb-2013 |

Security

| | | | |
|---|---|---|---|
| Netcraft Risk Rating | 7/10 | | |
| On Spamhaus Block List | No | On Exploits Block List | No |
| On Policy Block List | No | On Domain Block List | No |

Site Technology

Fetched on 23rd April 2013

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| PHP Enabled | Server supports PHP | www.movie2k.to , syndication.traffichaus.com , ad.turn.com |
| XML | No description | www.cnn.com , www.bild.de , platform.twitter.com |

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

| Technology | Description | Popular sites using this technology |
|---|---|---|
| JavaScript | Open source programming language commonly implemented as part of a web browser | www.google.co.uk , www.google.fr , www.google.it |

Content Management System

A content management system (CMS) is a computer program that allows publishing, editing and modifying content as well as maintenance from a central interface.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Drupal | An open source content management system | www.telecomitalia.it , www.rue89.com , www.examiner.com |

Figura 3: Resultados de consulta del objetivo utilizando netcraft

De la figura anterior, tal como se muestra en la Tabla I se puede obtener algunos de los datos más relevantes, de la consulta realizada mediante la herramienta web netcraft.

TABLA I: DATOS OBTENIDOS CON NETCRAFT SOBRE EL PORTAL DE LA INSTITUCIÓN

| **RED** | |
|---|---|
| Dominio | gob.ec |
| Dirección IPv4 | 190.57.168.196 |
| Servidor de Nombres | master.nic.ec |
| Administrador de DNS | dnsadmin@nic.ec |
| DNS Inverso | corp-190-57-168-196-uio.puntonet.ec |
| Compañía que hospeda | punto.net.ec |
| **Historial de Hospedaje** | |
| Propietaria de bloque de red | PUNTONET S. A. Quito |
| Dirección IP | 190.57.168.35 |
| Sistema Operativo | Linux |
| Servidor Web | Apache |
| Último cambio realizado | 3 de Febrero de 2013 |
| Seguridad | 7/10 |
| **Tecnología del sitio** | |
| **Lado del Servidor** | |
| PHP habilitado | El servidor soporta PHP |

| | |
|---|---|
| XML | No hay descripción |
| **Lado del Cliente** | |
| Javascript | Lenguaje de programación de código abierto normalmente implementado como parte de un navegador web |
| **Gestor de Contenidos** | |
| Drupal | Un sistema de gestión de contenido de código abierto. |

### 1.2.2.2. Sitio www.tcpiputils.com

Esta herramienta permite realizar consultas de sitios web, direcciones IP similar a www.domaintools.com y otros servicios web de esta índole, basta con ingresar la dirección ip del dominio, cuyo resultado se muestra en la figura 4.

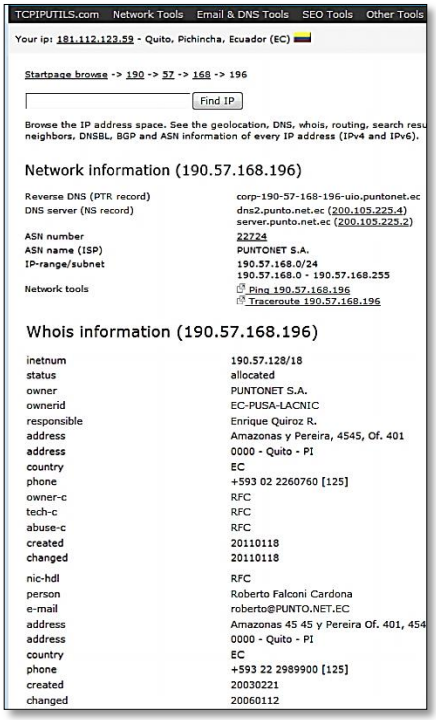



Figura 4: Consulta a la dirección IPv4 del portal web del GAD Municipal Loja.

En la tabla 2 se destaca la información más relevante de la consulta realizada con la herramienta del sitio web indicado, la primera impresión que da, es que tanto el alojamiento web como el servicio de internet del GAD Municipal de Loja es administrado por la compañía ecuatoriana Puntonet, y a diferencia de la consulta realizada con Domaintools, en la primera sección de la Tabla II se muestra información del bloque de direcciones ip públicas asignadas a la Institución. En la segunda sección

en cambio se ve los datos más relevantes pero esta vez pertenecientes a la compañía Puntonet.

TABLA II: INFORMACIÓN DE DIRECCIÓN IP DEL DOMINIO, CON TCPIPUTILS

| **Información de red** | |
|---|---|
| DNS Inverso (Registro PTR) | corp-190-57-168-196-uio.puntonet.ec |
| Servidor DNS (Registro NS) | dns2.punto.net.ec (200.105.225.4)<br>server.punto.net.ec (200.105.225.2) |
| Número ASN (Sistema de número autónomo) | 22724 |
| Nombre ASN (Sistema de número autónomo) (ISP) | PUNTONET S. A. |
| Rango IP/ subred | 190.57.X.Y/24<br>190.57.X.Y – 190.57.X.Y |
| **Información Whois** | |
| Inetnum | 190.57.128/18 |
| Estado | Asignadas |
| Propietario | PUNTONET S.A. |
| Id del propietario | EC-PUSA-LACNIC |
| Responsable | Enrique Quiroz R. |
| Dirección | Amazonas y Pereira, 4545, Of. 401<br>0000 – Quito - PI. |
| País | EC |
| Teléfono | +593 02 2260760 [125] |
| Persona encargada | Roberto Falconi Cardona |
| Dirección de correo | roberto@PUNTO.NET.EC |
| Dirección | Amazonas y Pereira, 4545, Of. 401, 454<br>0000 – Quito - PI. |
| Teléfono | +593 22 2989900 [125] |

### 1.3. Herramienta de escaneo de puertos Nmap.

El término escáner de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red.

Este tipo de escaneo se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos, dependiendo del tipo de escaneo que se realice, se puede llegar a detectar el sistema operativo que está ejecutando la máquina.

Es usado por administradores de sistemas para analizar posibles problemas de seguridad, pero también es utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red.

### 1.3.1. Definición

Nmap es un programa de código abierto que permite realizar el rastreo de puertos. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática. [1]

Nmap utiliza paquetes IP en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando; así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos. [2]

Nmap, conocido también como mapeador de redes, permite la exploración de redes y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien para analizar equipos individuales.

### 1.3.2. Características

Nmap posee gran variedad de comandos, que lo hace una herramienta bastante útil entre las características más relevantes están:

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

TABLA III: INFORMACIÓN GENERAL DE NMAP

| | |
|---|---|
| **Desarrollador(es)** | Gordon Lyon |
| **Última versión estable** | 6.25 |
| **Sistema operativo** | Multiplataforma |
| **Tipo** | Seguridad Informática |
| **Licencia** | GNU |
| **Sitio web** | http://nmap.org/ |

## 1.4. Herramientas de escaneo de vulnerabilidades

Un escáner de vulnerabilidades es un tipo de programa o herramienta que permite realizar una auditoría a un sistema; existe gran variedad de herramientas que permiten cumplir el objetivo principal (el descubrir vulnerabilidades) pero cada una se distingue por la forma en que consiguen sus objetivos.

Estas herramientas son utilizadas por los atacantes para intentar obtener información o el acceso a una red. El objetivo es determinar qué equipos presentan algún tipo de vulnerabilidad, para luego aprovecharse de ello y obtener información relevante. Esta información puede ser analizada en busca de vulnerabilidades conocidas o recientemente descubiertas para las cuales todavía no se ha elaborado la corrección pertinente; las mismas que pueden ser explotadas para obtener acceso al sistema.

A continuación se detalla algunas de las herramientas que permiten el escaneo de vulnerabilidades:

### 1.4.1. Nessus

El proyecto Nessus dio sus primeros pasos hace 15 años, en 1998, cuando Renaud Deraison quiso que la comunidad de Internet tenga un escáner remoto de seguridad que sea libre, desarrollado por Tenable Network Security, es una herramienta libre para uso personal en un entorno no empresarial, tiene como objetivo detectar posibles vulnerabilidades en los sistemas. [3]

Nessus 3 está disponible para muchos sistemas Unix y Windows, ofrece parche de auditoría para UNIX y hosts de Windows, sin necesidad de un agente y es de 2 a 5 veces más rápido que Nessus 2.

La versión 4 de Nessus fue lanzada el 9 de abril de 2009, mientras que Nessus 5.0 fue lanzada el 15 de febrero de 2012, la versión actual y liberada desde el 23 de abril de 2013 es la 5.2 disponible en el sitio web.

TABLA IV: NFORMACIÓN GENERAL DE NESSUS

| | |
|---|---|
| **Desarrollador(es)** | Tenable Network Security |
| **Última versión estable** | 5.0 |
| **Sistema operativo** | Multiplataforma |
| **Tipo** | Escáner de vulnerabilidad |
| **Licencia** | Propietaria, GPL |
| **Sitio web** | http://www.tenable.com/ |

### 1.4.1.1. Funcionamiento

Nessus permite exploraciones para los siguientes tipos de vulnerabilidades:

- Las vulnerabilidades que permiten a los hackers controlar o acceder a datos confidenciales en un sistema.
- La configuración errónea, por ejemplo falta de parches.
- Contraseñas débiles o por defecto.
- Denegación de servicio en contra de la pila TCP / IP.
- Preparación para auditorías TCP/IP.

Un escaneo normal de Nessus empieza con un escaneo de puertos con uno de sus cuatro portscanners internos, con el objetico de determinar que puertos están abiertos y luego tratar con varios exploit para los puertos abiertos.

Los resultados de las exploraciones se pueden exportar en varios formatos, como texto plano, HTML, XML, pdf.

### 1.4.2. OpenVas

OpenVAS es una variante del escáner de seguridad Nessus cuando este cambió su tipo de licenciamiento, por el año de 2005. La primera versión fue lanzada en julio del 2008 OpenVas 1.0, mientras que la versión 5.0.0 (estable) fue liberada el 10 mayo de 2012. [4]

TABLA V: INFORMACIÓN GENERAL DE OPENVAS

| | |
|---|---|
| **Desarrollador(es)** | Greenbone Networks GMBH |
| **Última versión estable** | 5.0.0 |
| **Sistema operativo** | Multiplataforma |
| **Tipo** | Escáner de vulnerabilidades |
| **Licencia** | GNU |
| **Sitio web** | http://www.openvas.org/ |

#### 1.4.2.1. Arquitectura de OpenVas.

OpenVAS al igual que Nessus sigue un modelo cliente-servidor. El componente servidor es responsable de la planificación y ejecución de los análisis de red, mientras que el componente cliente se utiliza para configurarlo y acceder a los resultados. El servidor normalmente se instala en un servidor Unix o Linux, y el cliente se ejecuta usualmente desde la estación de trabajo del administrador.

### 1.4.3. Nexpose

Es una herramienta que permite ejecutar diferentes tipos de escaneos en búsqueda de vulnerabilidades en un host o red, permite la definición de determinadas opciones que nos permiten acceder a un escaneo mucho más preciso con el uso de filtros por puertos, máquinas, segmentos de red, protocolos, etc. [5]

Nexpose es una herramienta diseñada por la empresa Rapid7 para el análisis de vulnerabilidades de redes, identifica y analiza los datos de cada exploración las vulnerabilidades encontradas en sistemas operativos, bases de datos, aplicaciones y archivos, también detecta todo tipo de programa malicioso. [6]

Cuenta con una gran base de datos que nos almacena la información de cada escaneo además crea informes para poder remediar las vulnerabilidades encontradas y nos dan los exploits a usar en cada vulnerabilidad crítica.

### 1.4.4. Nikto.

Nikto es una herramienta de escaneo de servidores web que se encarga de efectuar diferentes tipos de actividades tales como, detección de malas configuraciones y vulnerabilidades en el servidor objetivo, detección de ficheros en instalaciones por defecto, listado de la estructura del servidor, versiones y fechas de actualizaciones de servidores, test de vulnerabilidades XSS, ataques de fuerza bruta por diccionario, reportes en formatos txt, csv, html, etc. [7]

Este tipo de escáner desarrollado en lenguaje Perl, bajo licencia Open Source GPL realiza todo tipo de pruebas de ataques y vulnerabilidades por medio de un extensible sistema de plugins, es un excelente punto de partida para comprobar la seguridad del servidor web a nuestro cargo, funciona tanto en Linux como en Windows y tiene una gran base de datos de ataques (CGI y otros) en 230 tipos de servidores distintos. [8]

Las categorías en las cuales se destaca son:

- Problemas de configuración.
- Archivos por defecto y ejemplos.
- Archivos y scripts inseguros.
- Versiones desactualizadas de productos.

### 1.4.5. W3af.

Web Application Attack and Audit Framework, por sus siglas en inglés es un framework, opensource bajo licencia GPLv2.0, de auditoría que permite detectar vulnerabilidades y explotarlas. [9]

Tiene como objetivo crear un marco para ayudar a proteger sus aplicaciones web mediante la búsqueda y explotación de todas las vulnerabilidades de las aplicaciones web desarrolladas en Python. Además la herramienta puede ser utilizada por expertos en seguridad web que no sean necesariamente programadores, también lo pueden utilizar investigadores.

Entre los objetivos a largo plazo que persigue w3af están:

- Crear la mayor comunidad de hackers de aplicaciones web.
- Convertirse en el mejor escáner de aplicaciones Web.
- Convertirse en el mejor framework para la explotación aplicaciones web.
- Convertirse en el nmap para la Web.

Dentro de w3af se trabaja con 4 pestañas, en Configuración del análisis se indica el objetivo y se seleccionan los plugins o escáneres que se desean utilizar; en Log se puede ver el estado del proceso; en Resultados se puede evidenciar las vulnerabilidades detectadas con todo los detalles (SQL Injection, Cross Site Scripting, Full Path Disclosure, File Inclusion, etc.); y por último en la pestaña Exploit se pueden explotar estos fallos. [9]

#### 1.4.5.1. Arquitectura de W3af

W3af tiene dos partes principales, el núcleo y los plugins. El núcleo coordina el proceso y proporciona características que son consumidos por los plugins, que encuentran las vulnerabilidades y permiten explotarlos. Los plugins están conectados y comparten información entre ellos utilizando una base de conocimientos, esto es propio de cada herramienta.

Los plugins se clasifican en los siguientes tipos:

- Discovery.
- Audit.
- Attack.
- Output.
- Evasion.
- Bruteforce

TABLA VI: INFORMACIÓN GENERAL DE W3AF

| | |
|---|---|
| **Desarrollador(es)** | Andrés Riancho |
| **Última versión estable** | 1.1 |
| **Sistema operativo** | Multiplataforma |
| **Tipo** | Escáner de vulnerabilidades |
| **Licencia** | GPLv2.0 |
| **Sitio web** | http://w3af.org/ |

# 2. Servidor de correo

En servidor de correo es de gran importancia dentro de las instituciones tanto públicas como privadas, permite el intercambio de mensajes de texto, documentos digitales (imágenes, videos, audio, etc.). El intercambio de puede dar entre usuarios, servidores, cliente – servidor.

## 2.1. Sistema de nombres de dominio (DNS)

Veámoslo de la siguiente forma, si se tiene conectado un computador a una red (sea casera o internet), tiene una dirección ip, en el caso de una red casera con pocos equipos resulta fácil conocer la ip de cada computador, ahora si estamos conectados a internet en donde hay miles de millones de computadores y cada uno de ellos tiene una ip distinta sería imposible el recordar las direcciones ip, para eso están los DNS que permite traducir los dominios (sitio al que se desea acceder) en una dirección ip o viceversa, para que el usuario no tenga que escribir la ip sino un nombre que pueda recordar como por ejemplo www.google.com.

### 2.1.1. Propósito de un DNS

Localizar un ordenador o cualquier otro recurso de una red, es necesaria alguna forma de indicar el destino, esto se consigue asignando direcciones de red. La dirección de red debe de ser única para poder encaminar correctamente los paquetes de un host o router a otro. Esta dirección está formada por un identificador numérico el cual los routers o cualquier dispositivo de red puedan entender y procesar. Desde la perspectiva de los dispositivos de red (por ejemplo, router) que solo encaminan paquetes a través de Internet, son solo transacciones de paquetes. Pero desde la perspectiva del usuario para acceder a los recursos de internet se utilizan los nombres de dominio, los usuarios necesitan un sistema que traduzca los nombres de dominio a direcciones IP y viceversa. Esta traducción es la tarea principal del Domain Name System (DNS). [10]

### 2.1.2. Jerarquía de un DNS

En respuesta a la rápida expansión de Internet, incrementando cada día el número de direcciones IP del espectro normalizado, se introdujo el servicio de nombres de dominio DNS en 1983 para poder gestionar de manera eficiente el direccionamiento. [10]

El sistema de nombres de dominio es un sistema jerarquizado, es decir, existe un dominio raíz (representado por un solo punto “.”) un conjunto de dominios de primer nivel, como .com o .es, y cualquier número de niveles debajo de estos dominios [10]. La figura 5 muestra un ejemplo de la jerarquía de nombres de dominio.

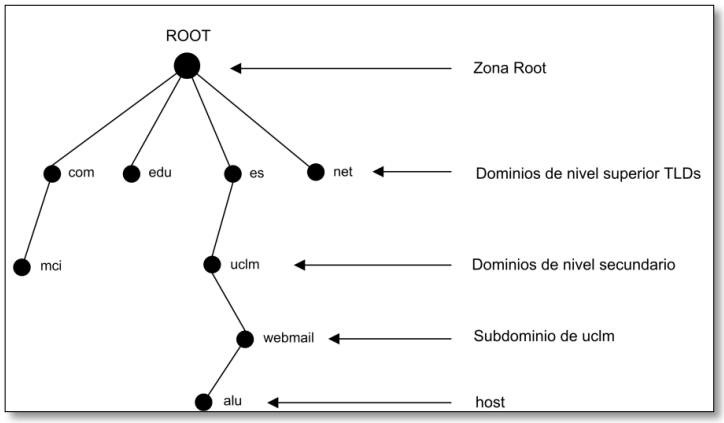



Figura 5: Jerarquía de dominios.

La zona de la parte superior de la jerarquía (el dominio “.”) se llama la zona root o zona raíz. Las entradas de esta zona son los dominios de nivel superior (Top Level Domains, TLDs). Existen dominios de primer nivel como .com para empresas, .edu para instituciones educativas y dominios genéricos de nivel superior formado por el código de país.

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. [10]

### 2.1.3. Registro de recursos

Cada dominio puede tener un grupo de registros de recursos asociados a él, entonces la función real de un DNS es relacionar los nombres de dominio con los registros de recursos asociados a éste [11]. Un registro de recursos tiene las siguientes partes:

**Nombre_dominio:** Indica el dominio al que pertenece el recurso

**Tiempo_de_vida:** Indica la estabilidad del registro, la información altamente estable recibe un valor de 86400s, y la información muy volátil recibe un valor de 60s.

**Tipo**: Indica el tipo de registro asociado, puede ser:

TABLA VII: TIPO DE REGISTRO DE DNS

| Tipo | Significado | Valor |
|---|---|---|
| SOA | Inicio de Autoridad (Start of Authority) | Define el inicio de una zona |
| A | Dirección IP de un HOST | Entero de 32 bits |
| MX | Intercambio de correo | Dominio dispuesto a recibir correo-e |
| NS | Servidor de nombres | Nombre de un servidor para este dominio, define el fin de la zona SOA |
| CNAME | Nombre Canónico | Nombre de dominio |
| PTR | Apuntador | Alias de una dirección IP |
| HINFO | Descripción del Host | CPU y SO en Ascii |
| TXT | Texto | Texto ascii no interpretado |

## 2.2. Agente de transporte de correo Postfix.

Postfix es un agente de transporte de correo de software libre que permite realizar el enrutamiento y envío de correo, fue creado como una alternativa a Sendmail, para que sea más rápido, amigable al usuario y seguro. [12]

Dentro de los servicios de correo estos MTA (agente de entrega de correo) tiene las siguientes formas de comunicarse:

- Recibe los mensajes desde otro MTA. Actúa como “servidor” de otros servidores.
- Envía los mensajes hacia otro MTA. Actúa como un “cliente” de otros servidores.
- Actúa como intermediario entre un “Mail Submision Agent” y otro MTA.

### 2.2.1. Características.

Postfix tiene varias características entre las que se destacan:

- Soporta TLS (Transport Layer Security).
- Es compatible con base de datos como: MySQL, PostgreSQL y LDAP
- Soporte para mbox, maildir y dominios virtuales.
- Maneja SMTP-AUTH, mecanismo de autenticación SASL.
- Maneja un gran volumen de correos.

### 2.2.2. Protocolo simple para la transferencia de correo (SMTP)

SMTP es un protocolo TCP/IP utilizado en el envío y recepción de correo electrónico. Sin embargo, está limitado en su capacidad de hacer cola de mensajes en el extremo receptor, se utiliza por lo general con uno de los otros dos protocolos POP3 o IMAP, que permiten al usuario guardar los mensajes en un buzón del servidor y descargarlos periódicamente desde el servidor, es decir, los usuarios suelen utilizar un programa que utiliza SMTP para el envío de e-mail y POP3 o IMAP para recibir correo electrónico. [13]

Los administradores del servidor de correo pueden elegir si sus clientes utilizan el puerto 25 (SMTP) o el puerto 587 (Presentación) para retransmitir el correo saliente.

## 2.3. Agente de entrega de correo Dovecot.

Dovecot es un servidor de IMAP y POP3 de código abierto para sistemas basados en Linux/Unix, es una excelente opción para instalaciones grandes como pequeñas con una instalación sumamente sencilla. [14]

### 2.3.1. Características

Entre las principales características están:

- No se requiere de una administración extraordinaria.
- Utiliza muy poca memoria.
- Es uno de los servidores de más alto rendimiento IMAP, apoyado en los estándares mbox y Maildir.
- Permite la migración desde servidores IMAP y POP3.

- Dovecot es altamente extensible, gracias a los plugins se puede agregar nuevos parámetros, agregar datos en los archivos de índice.
- Es compatible con SSL y TLS.

### 2.3.2. Protocolo de acceso a mensajes de internet IMAP

Es un sistema que permite que nuestro programa de correo electrónico se conecte a nuestra cuenta de correo electrónico y visualice los mensajes allí almacenados. Los correos permanecen en el servidor por lo que pueden ser visualizados desde otros dispositivos y programas. [15]

Los puertos en los que funciona IMAP pueden ser el 143 (TCP), 220 (IMAP3), 993 (IMAPS). Las principales características del protocolo son:

- Permite visualizar los mensajes de manera remota, sin la necesidad de descargarlos localmente.
- Permite realizar un gran número de transacciones.
- Desde el servidor se puede gestionar archivos y carpetas locales.
- Acceso simultáneo a múltiples clientes.

Aunque parezca llamativo este protocolo tiene algunas desventajas, si las comparamos con POP.

- Las carpetas que se crean con IMAP, solo las puede leer utilizando POP.
- Se tiene que estar conectado a internet para poder leer los correos.
- Si la conexión se interrumpe no se podrá acceder al correo recibido.

### 2.3.3. Protocolo de Oficina de correo POP3

Al igual que IMAP el protocolo de oficina de correo, cuya función radica en obtener los mensajes de correo en clientes locales.

Por lo general cuando se emplea el término POP, se refiere a POP3, pues las versiones anteriores conocidas como POP1 y POP2 quedaron obsoletas gracias a las modificaciones de POP3.

Funciona en la capa de aplicación del Modelo OSI en los puertos 110/TCP, 995/TCP, este último sirve para cifrar los mensajes.

Frente a IMAP presenta algunas características como:

- Está diseñado para recibir correo.
- Se puede acceder al correo mediante una única cuenta de correo.
- Los clientes pueden descargar el correo para luego leerlos incluso si no están conectados al internet.
- La nueva versión de cuenta con una serie de mecanismos de autenticación lo que proporciona una serie de niveles de protección contra los accesos ilegales al buzón de correo.

## 2.4. Protocolo ligero de acceso a directorios LDAP.

Es un protocolo que funciona en el nivel de aplicación para acceder a información almacenada en un directorio de información en un entorno de red. Siendo un directorio un conjunto de objetos con atributos organizados en una manera lógica y jerárquica

A LDAP se la confunde con una base de datos porque se puede realizar consultas sobre el directorio, pero a diferencia de una base datos que están diseñadas para realizar miles de consultas en fracciones de segundos y procesar cientos de cambios, LDAP está optimizado para un rendimiento de lectura. [16]

- LDAP es fácil de instalar, de configurar.
- Los servidores LDAP pueden replicar todos o algunos de sus datos, a través de métodos de envío y recepción.
- El protocolo LDAP es utilizable en distintas plataformas y basado en estándares, de ese modo las aplicaciones no necesitan preocuparse por el tipo de servidor en que se hospeda el directorio.
- LDAP es particularmente utilizable para almacenar información que desees leer desde muchas localizaciones, pero que no sea actualizada frecuentemente.

### 2.4.1. Estructura de un árbol de directorio LDAP

Un árbol de directorio LDAP refleja varios límites políticos, geográficos u organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar sistema de nombres de dominio (DNS) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada

en el árbol (o múltiples entradas). Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para identificarse, aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red. [17]

Los siguientes RFCs permitieron definir LDAP en una mejor estructura: RFC 2251, RFC 2256 es el documento base de LDAP, RFC 2829 donde se describe el método de autenticación para LDAP, RFC 2830 extensión para TLS, y por último RFC 3377 especificación técnica.

Las ventajas de utilizar el protocolo LDAP se podrían resumir en las siguientes:

- La lectura de los registros es muy rápida.
- Al momento de replicar el servidor se vuelve una tarea sencilla y no demanda muchos gastos económicos.
- Algunas aplicaciones se pueden integrar fácilmente mediante sus interfaces.
- Utiliza un sistema de almacenamiento jerárquico para la información.
- Permite múltiples directorios independientes.

#### 2.4.1.1. Nivel superior de un directorio LDAP

El nivel superior de un directorio LDAP es la base, conocido como el “DN base”. Un DN base, generalmente, toma una de las tres formas que se listaran a continuación. Tomemos como ejemplo una empresa de ventas de dominios por internet en EC (Ecuador) llamada Hosting, Inc., la cual está en Internet como hosting.com

**DN base en formato X.500 - o=” Hosting, Inc”, c=EC**

En este ejemplo, o=Hosting, Inc. se refiere a la organización, que en este contexto debería ser tratada como un sinónimo del nombre de la empresa. c=EC asumiremos que su centro de operaciones está en Ecuador. Este método era el más utilizado por mucho tiempo pero desde que X.500 evolucionó se dieron dos nuevo formatos.

**DN base derivado de la presencia en Internet de la empresa - o=hosting.com**

Este formato es bastante sencillo, utiliza el nombre de dominio de la empresa como base, hasta hace poco, fue el formato más común de los formatos usados actualmente.

**DN base derivado de los componentes de dominio DNS de la empresa - dc=hosting, dc=com**

Como el formato previo, este utiliza el nombre de dominio DNS como su base. Pero donde el otro formato deja el nombre de dominio intacto, este formato está separado en componentes de dominio: hosting.com quedando de la siguiente forma dc=hosting, dc=com.

### 2.4.1.2. Terminología LDAP

**Entrada:** Una entrada es una unidad en un directorio LDAP. Cada entrada se identifica por su único nombre distinguido (DN).

**Atributos:** Los atributos son piezas de información directamente asociada con la entrada. Por ejemplo, una organización puede ser representada como una entrada LDAP. Los atributos asociados con la organización pueden ser su número de fax, su dirección, etc. En un directorio LDAP las entradas pueden ser también personas, con atributos comunes como el número de teléfono y la dirección de e-mail.

**LDIF:** El formato de intercambio de datos de LDAP (LDIF) es una representación de texto ASCII de entradas LDAP. Los archivos usados para importar datos a los servidores LDAP deben estar en formato LDIF. Una entrada LDIF se ve similar al ejemplo siguiente:

```
[<id>]
dn: <distinguished name>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
```

Una entrada puede contener tantos pares *<attrtype>*: *<attrvalue>* como sean necesarios. Una línea en blanco indica el final de una entrada.

Cualquier valor comprendido dentro de "< … >" es una variable y puede ser configurado cuando se cree una nueva entrada LDAP. Sin embargo, esta regla no se aplica a *<id>*. El *<id>* es un número determinado por la aplicación que se usa para modificar la entrada. [18]

# 3. Herramientas de monitoreo de red

Una herramienta de monitoreo de redes es fundamental para asegurar el funcionamiento de los sistemas informáticos y para evitar fallos en la red. La monitorización de redes también ayuda a optimizar la red, permite detallar con facilidad la información sobre el uso, supervisión de servicios y otros recursos de la red.

A continuación se detallan algunas de las herramientas de monitoreo que se pueden ejecutar bajo plataforma Linux y con licencia GPL (GNU Public License):

## 3.1. Nagios

En un principio se diseñó para ejecutarse en entornos Linux. Proporciona supervisión de los servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH) y recursos de host (carga del procesador, uso de disco, los registros del sistema). Gracias a su diseño ofrece a los administradores desarrollar sus chequeos de servicio sin esfuerzo propio basado en las necesidades y mediante el uso de cualquiera de las herramientas de apoyo que guste [19]. Cuando los servicios o los problemas de acogida se plantean, la notificación será enviada a la persona que está a cargo de la red a través del correo electrónico, SMS, etc.

## 3.2. Zabbix

Es una herramienta capaz de monitorear y dar seguimiento de la situación de los diferentes tipos de servicios de red, servidores y otro hardware de red. Vistas definidas por el usuario, cartografía (visualización de mapas), son algunas de sus funcionalidades. Son tres módulos con lo que cuenta: el servidor, los agentes, y el usuario. Las bases de datos que utiliza para almacenar los reportes son: MySQL, PostgreSQL, Oracle o SQLite. En el equipo remoto es necesario instalar un agente para supervisar recursos como carga del CPU, espacio de disco, entre otros. [20]

## 3.3. Cacti

Es una herramienta web en donde su interfaz gráfica está escrita en PHP, almacena datos de RRDtool en una base de datos Mysql, permite a los usuarios monitorear y ver gráficamente servicios como: carga de la CPU, la utilización de ancho de banda de red, el tráfico de red, entre otras. Cacti permite sondear los servicios en el período

preestablecido y se puede obtener un gráfico de los mismos. Cacti se puede ampliar para controlar cualquier fuente a través de scripts de shell y ejecutables. Es compatible con arquitectura de plugins. [21]

### 3.4. Zenoss

Conocido también como Zenoss Core, está escrito en Python y está basado en aplicaciones del servidor Zope, es muy versátil puesto que combina la programación original y proyectos de código abierto para integrar el almacenamiento de datos y los procesos de recopilación de los mismos a través de la interfaz de usuario Web. Permite a los usuarios supervisar la disponibilidad, inventario y configuración, desempeño y los acontecimientos. También brinda la posibilidad de supervisar dispositivos de red mediante SNMP, SSH, WMI, servicios de red (HTTP, POP3, NNTP, SNMP, FTP) y los recursos del host (procesador, uso de disco) en la mayoría de sistemas operativos de red. Una arquitectura plug-in proporcionada por ZenPacks (encapsulado en Python) permite a miembros de la comunidad aumentar la funcionalidad de esta herramienta de acuerdo a las necesidades de la empresa.

### 3.5. PandoraFMS

Pandora FMS es un software de monitorización para todo tipo de empresas, pero especialmente diseñado para grandes entornos, que le ayuda a detectar problemas antes de que ocurran mediante la gestión de servidores, comunicaciones y aplicaciones. Además, Pandora FMS cuenta con un sistema de informes configurable que evaluará el nivel de cumplimiento de sus sistemas y reportará la información a sus clientes. Creada en 2004, Pandora FMS es utilizada hoy en día por miles de empresas de todo el mundo. [22]

# 4. Certificado Digital

## 4.1. Introducción

Los sistemas que ofrecen servicios mediante Internet requieren de confianza, privacidad y seguridad entre ellos y sus clientes. El problema de la identificación de personas o sistemas que usan medios de comunicación no fiables se puede resolver usando certificados digitales. [23]

Los certificados digitales son el equivalente digital del DNI, en lo que a la autentificación de individuos se refiere, ya que permiten que un individuo demuestre que es quien dice ser, es decir, que está en posesión de la clave secreta asociada a su certificado. [24]

Para los usuarios proporcionan un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo encriptado y/o firmado digitalmente, el control de acceso a recursos, etc.

## 4.2. Certificado Digital

Un certificado de clave pública es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada. [24]

Los certificados de clave pública se denominan comúnmente Certificado Digital, ID Digital o simplemente certificado. La entidad identificada se denomina sujeto del certificado o subscriptor (si es una entidad legal como, por ejemplo, una persona).

Los certificados digitales sólo son útiles si existe alguna Autoridad Certificadora (Certification Authority o CA) que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo conozca.

## 4.3. Certificados X.509

El formato de certificados X.509 es un estándar del ITU-T (International Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (International Standards Organization/International Electrotechnical Commission) que

se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios. Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996. [24]

Los elementos que conforman un certificado X.509 v3 son los siguientes:

- **Versión:** El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables 1, 2 y 3.
- **Número de serie del certificado:** Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- **Identificador del algoritmo de firmado:** Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- **Nombre del emisor:** Este campo identifica la CA que ha firmado y emitido el certificado.
- **Periodo de validez:** Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
- **Nombre del sujeto:** Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- **Información de clave pública del sujeto:** Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- **Identificador único del emisor:** Este es un campo opcional que permite reutilizar nombres de emisor.

- **Identificador único del sujeto:** Este es un campo opcional que permite reutilizar nombres de sujeto.

- **Extensiones:** Otros campos específicos de cada protocolo que están sujetos a sus propias regulaciones.

## 4.4. Autoridades Certificadoras

Una autoridad certificadora es una organización fiable que acepta solicitudes de certificados de entidades, las valida, genera certificados y mantiene la información de su estado.

Una CA debe proporcionar una Declaración de Prácticas de Certificación (Certification Practice Statement o CPS) que indique claramente sus políticas y prácticas relativas a la seguridad y mantenimiento de los certificados, las responsabilidades de la CA respecto a los sistemas que emplean sus certificados y las obligaciones de los subscriptores respecto de la misma. [24]

Además una CA tiene que cumplir con labores como:

- **Admisión de solicitudes:** En el momento que un usuario hace la petición de un certificado.

- **Autentificación del sujeto:** Antes de firmar la información proporcionada por el sujeto la CA debe verificar su identidad. Dependiendo del nivel de seguridad deseado y el tipo de certificado se deberán tomar las medidas oportunas para la validación.

- **Generación de certificados:** Después de recibir una solicitud y validar los datos la CA genera el certificado correspondiente y lo firma con su clave privada. Posteriormente lo manda al subscriptor y, opcionalmente, lo envía a un almacén de certificados para su distribución.

- **Distribución de certificados:** La entidad certificadora puede proporcionar un servicio de distribución de certificados para que las aplicaciones tengan acceso y puedan obtener los certificados de sus subscriptores. Los métodos de distribución pueden ser: correo electrónico, servicios de directorio como el X.500 o el LDAP, etc.

- **Anulación de certificados:** La CA debe validar el origen y autenticidad de una solicitud de anulación. La CA debe mantener información sobre una anulación durante todo el tiempo de validez del certificado original. [24]

- **Almacenes de datos:** La designación oficial de una base de datos como almacén tiene por objeto señalar que el trabajo con los certificados es fiable y de confianza.

## 4.5. Tipos de certificados de clave pública

Dentro del ámbito de los certificados digitales existen cuatro tipos de certificados:

1. **Certificados de autoridad:** Las entidades emisoras de certificados raíz tienen la capacidad de asignar certificados a certificados de autoridad. Corresponden a entidades que certifican. Los certificados raíz son los únicos auto-firmados y son los que inician una cadena de certificación de acuerdo a la jerarquía definida en el estándar X.509.

2. **Certificado de servidor:** Certifica que un servidor es de la empresa que dice ser y que el identificador del servidor es correcto. Los certificados de servidor identifican a servidores que participan en comunicaciones seguras con otros equipos mediante la utilización de protocolos de comunicaciones. Estos certificados permiten al servidor probar su identidad ante los clientes.

3. **Certificados personales:** Los certificados personales aseguran que una dirección de correo y clave pública corresponden a una persona. Estos certificados identifican a personas y se pueden utilizar para autenticar usuarios con un servidor.

4. **Certificados de productores de software:** Se utilizan para “firmar” el software y asegurar que no ha sido modificado. Esto no implica que se pueda ejecutar con seguridad, pero informa al usuario que el fabricante de software participa en la infraestructura de compañías y entidades emisoras de certificados de confianza. Estos certificados se utilizan para firmar el software que se distribuye por Internet. [23]

## 4.6. Aplicaciones de los Certificados digitales

La utilización de los certificados digitales permite tanto a empresas como usuarios vender, comprar, intercambiar información, firmar documentos a través de internet, por estas razones se los suele utilizar en:

- Correo electrónico.
- Acceso a base de datos confidenciales.
- Redes privadas virtuales.
- Relación proveedores/clientes.
- Transacciones económicas y comerciales.
- Banca personal, empresarial y corporativa.

# 5. Redes privadas virtuales (VPN)

## 5.1. Introducción

Una red privada virtual es una tecnología que permite interconectar a equipos pertenecientes a diferentes redes físicas de distintas localizaciones, estableciendo comunicaciones seguras a través de una red generalmente pública por ejemplo internet para garantizar la confidencialidad, disponibilidad e integridad del flujo de información de los equipos participantes, los que virtualmente son elementos de una nueva red de datos. Esto abarata los costos al utilizar internet como infraestructura de comunicación, porque comúnmente lo que se necesita era contratar servicios de enlace de terceros, alquiler de dispositivos para este tipo de conexiones.

Básicamente, existen dos tipos de VPN:

- **VPN de acceso remoto:** Es aquella que se utiliza para permitir el acceso de un ordenador cliente remoto a una red local, pudiendo adquirir el ordenador remoto la mayoría de privilegios que poseería si se encontrara físicamente dentro de la red local, para lo que se suele asignar al cliente IP mediante la VPN una dirección IP perteneciente a la red local.

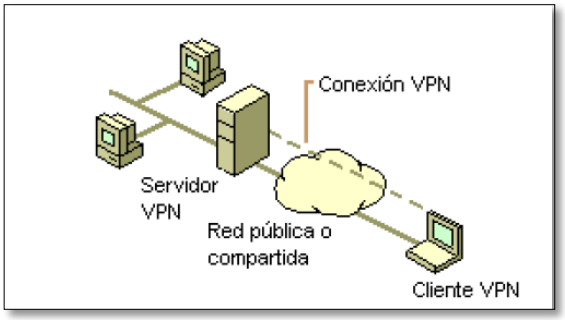



Figura 6: VPN de acceso remoto

- **VPN punto a punto:** Es aquella en que dos ordenadores establecen entre ellos una conexión VPN, permitiendo el acceso entre los ordenadores que se encuentran en sus LAN.

  Generalmente se utilizan para unir distintas sedes de empresas, permitiendo el intercambio de información entre las distintas LAN con la privacidad necesaria, y eliminando el uso de redes punto a punto, generalmente muy costosas económicamente.

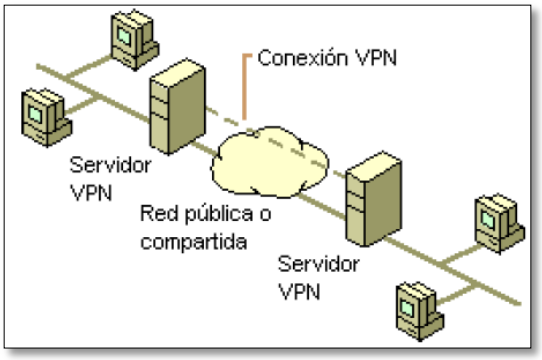



Figura 7: VPN punto a punto

Las soluciones VPN existentes utilizan mecanismos de encapsulamiento llamados entunelamiento para los que existen respectivos protocolos que permiten realizar este tipo de procesamiento a la información, entre ellos se tiene: PPTP, L2F, L2TP, OpenVPN, IPSec. La solución más adaptable acorde a los requerimientos de los clientes VPN existentes en la red de datos del GAD Municipal, se trata de la combinación del uso de dos protocolos L2TP e IPSec, un estándar con soporte nativo en terminales Windows, desde la versión Windows 2000 hasta la actualidad.

## 5.2. L2TP

### 5.2.1. Antecedentes de la tecnología L2TP (LAYER 2 TUNNELING PROTOCOL)

L2TP fue creado como el sucesor de PPTP y L2F. Las dos compañías de cada uno de estos protocolos, Microsoft por PPTP y Cisco por L2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 (nivel enlace de datos) y así lograr su estandarización por parte de la IETF. Como PPTP, L2F fue diseñado como un protocolo de entunelamiento usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el entunelamiento de este último no depende de IP y GRE (Generic Router Encapsulation), permitiéndole trabajar con otros medios físicos por ejemplo Frame Relay. Paralelamente al diseño de PPTP, L2F utilizó PPP para autenticación de usuarios accediendo vía telefónica conmutada, pero también incluyó soporte para TACACS+ y Radius. Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión.

Puesto que L2TP usa PPTP en enlaces conmutados, incluye mecanismos de autenticación nativos de PPP como PAP y CHAP. Microsoft incluye L2TP a partir del

sistema operativo Windows 2000, ya que las mejoras de L2TP con respecto a PPTP saltan a la vista.

El L2TP sobre las redes IP utiliza UDP y una serie de mensajes del L2TP para el mantenimiento del túnel. Se pueden encriptar y/o comprimir las cargas útiles de las tramas PPP encapsuladas. En la figura 8 muestra la forma en que se ensambla un paquete L2TP antes de su transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño final de trama muestra la encapsulación para un cliente de marcación (controlador de dispositivos PPP). La encapsulación supone el L2TP sobre IP.

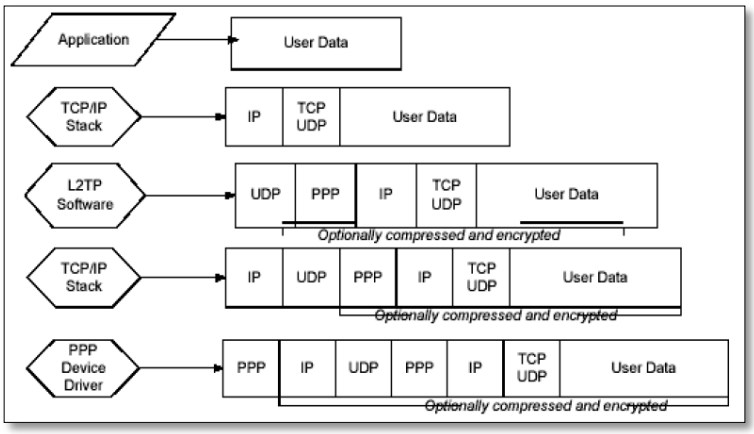



Figura 8: Encapsulación L2TP

### 5.2.2. Componentes básicos de un túnel L2TP

#### 5.2.2.1. Concentrador de acceso l2tp (LAC)

Un LAC es un nodo que se encuentra en un punto extremo de un túnel L2TP. El LAC se encuentra entre un LNS y un sistema remoto y reenvía los paquetes hacia y desde cada uno. Los paquetes enviados desde el LAC hasta el LNS van tunelizados. En algunas ocasiones el sistema remoto actúa como un LAC, esto se presenta cuando se cuenta con un software cliente LAC.

#### 5.2.2.2. Servidor de red L2TP (LNS)

Un LNS es un nodo que se encuentra en un punto extremo de un túnel L2TP y que interactúa con el LAC, o punto final opuesto. El LNS es el punto lógico de terminación de una sesión PPP que está siendo tunelizada desde un sistema remoto por el LAC.

#### 5.2.2.3. Túnel

Un Túnel existe entre una pareja LAC-LNS. El túnel consiste de una conexión de control y de ninguna o más sesiones L2TP. El túnel transporta datagramas PPP encapsulados y mensajes de control entre el LAC y el LNS. [25]

## 5.3. IPSEC

Es un estándar compuesto por protocolos, algoritmos de cifrado, métodos hash y encapsulamiento creado para brindar seguridad al protocolo IP, surge de la necesidad de agregar mecanismos que provean de autenticación, confidencialidad y disponibilidad a los datos que se envían a través de redes IPv4. De hecho en redes IPv6 ya se provee mecanismos de seguridad para este nuevo estándar. [26]

### 5.3.1. Características de seguridad

***Administración automática de claves:*** Las claves largas y el cambio dinámico de claves durante las comunicaciones ya establecidas protegen contra los ataques.

***Autenticación mutua:*** La comprobación mutua (autenticación) se utiliza para establecer la confianza entre los sistemas que se comunican. Sólo los sistemas de confianza se pueden comunicar entre sí. Los usuarios no tienen que estar en el mismo dominio para comunicar con la protección de IPSec.

Los protocolos de IPsec actúan en la capa de red (capa 3 del modelo OSI). Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7 hacia arriba). Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP Y UDP los protocolos de capa de transporte más usados.

### 5.3.2. Arquitectura de seguridad

IPSec está implementado por un conjunto de protocolos criptográficos para:

- Asegurar el flujo de paquetes.
- Garantizar la autenticación mutua.
- Establecer parámetros criptográficos

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPSec.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPSec utiliza el índice de parámetro de seguridad (SPI - Security Parameter Index), un índice a la base de datos de asociaciones de seguridad (SADB – Security Association Database), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPSec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

### 5.3.3. Modos de funcionamiento

Dependiendo del nivel sobre el que se actúe, se establecen dos modos básicos de operación de IPSec: modo transporte y modo túnel, como se muestra en la figura 9.

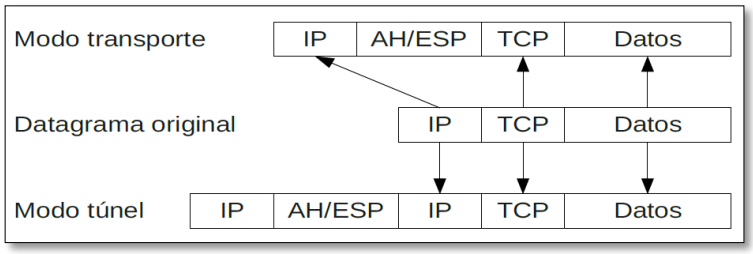



Figura 9: Modos de funcionamiento de IPSec

#### 5.3.3.1 Modo transporte

En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de

puerto TCP y UDP). El modo transporte se utiliza para comunicaciones ordenador a ordenador.

#### 5.3.3.2 Modo túnel

En el modo túnel, todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

### 5.3.4. Los protocolos IPSec

La familia de protocolos IPSec está formada por dos protocolos: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50. [27]

#### 5.3.4.1. AH - Cabecera de autenticación

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete. La cabecera AH se muestra en la siguiente figura 10.

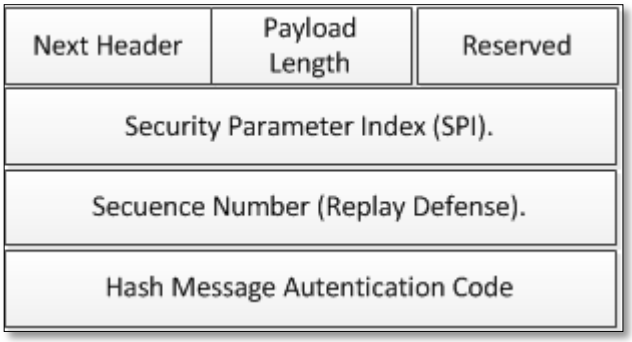



Figura 10: Cabecera AH. Protege la integridad del paquete

Este HMAC protege la integridad de los paquetes ya que solo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMACs. AH proporciona autenticación de origen de datos, integridad de datos y protección anti eco para todo el paquete (tanto el encabezado IP, como la carga de datos que transporta

el paquete), excepto los campos del encabezado IP que pueden cambiar en tránsito. AH no proporciona confidencialidad de datos, es decir, no cifra los datos. Los datos pueden leerse pero están protegidos contra modificaciones e imitaciones.

Como el protocolo AH protege la cabecera IP incluyendo las partes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT reemplaza la dirección IP de la cabecera por una IP diferente, tras el intercambio, la HMAC ya no es válida. La extensión a IPsec NAT-transversal implementa métodos que evitan esta restricción. En la práctica, casi nadie utiliza AH. En la figura 11 se muestra la ubicación de la cabecera de autenticación.

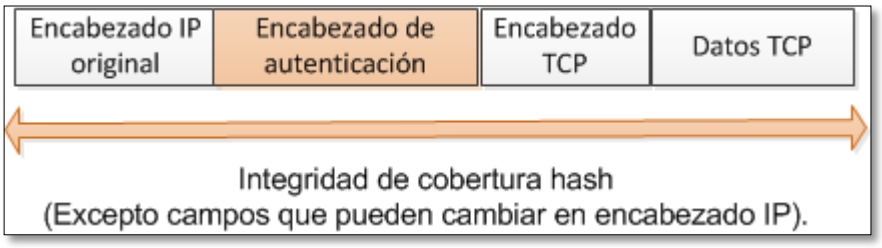



Figura 11: Protección de la información con protocolo AH

### 5.3.4.2. ESP - Carga de Seguridad Encapsulada

El protocolo ESP puede asegurar la integridad de los datos del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC.

Esta HMAC solo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo. El uso de NAT, por lo tanto, no rompe el protocolo ESP. En la figura 12 se muestra la ubicación del protocolo ESP.

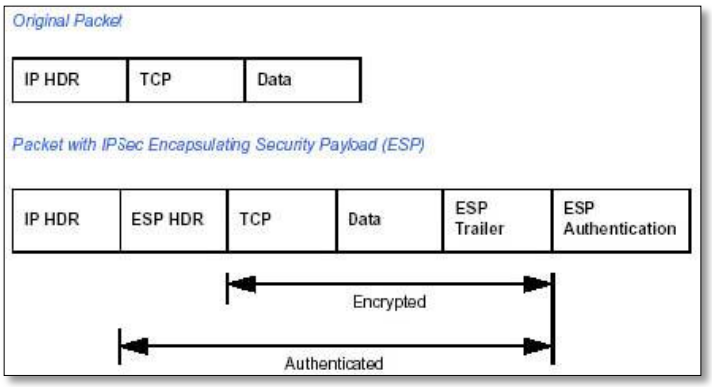



Figura 12: Cabecera ESP

#### 5.3.4.3. IKE

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Emplea el puerto 500 UDP para su comunicación.

El protocolo IKE funciona en dos fases. La autenticación de los participantes, en la primera fase suele basarse en claves compartidas con anterioridad (PSK - Pre-shared keys), claves RSA y certificados X.509. En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad.

### 5.3.5. Implementaciones IPSec para Linux.

Los siguientes paquetes descritos a continuación son los que permiten implementar IPSec en servidores:

**FreeS/wan:** Esta fue la primera implementación de IPSec para Linux. Sin embargo, FreeS/wan ya no es un proyecto en desarrollo, continuó en otros dos proyectos: Openswan y strongSwan. [28]

**Openswan:** Es una implementación opensource de IPSec para linux. Es un código hijo del proyecto FreeS/Wan, realizado por el equipo de trabajo que formó la compañía Xelerance. [28]

**StrongSwan:** Es también otra continuación del proyecto FreeS/WAN. Su principal autor es Andreas Steffen, el creador del parche sobre certificados X.509 para FreeS/Wan. [28]

**ipsec-tools:** Está basado en el proyecto KAME (implementación original de IPSec para BSD) y son unas herramientas utilizadas por defecto en muchas distribuciones. Su demonio de IKE se llama racoon. [28]

# e. Materiales y Métodos

El desarrollo del presente trabajo investigativo fue producto de una serie de pasos que permitieron realizar: la delimitación del tema a desarrollar, el planteamiento de los objetivos, recolección de información, dar solución a los problemas que se presentaron y además hacer uso de los métodos que se detallan a continuación:

## 1. Métodos de investigación.

### 1.1. Método deductivo.

Este tipo de método se utilizó para determinar el tema de investigación, es decir que partiendo de conocimientos generales se determinó las posibles soluciones (casos particulares), en cada una de las fases del desarrollo del tema, como fue el problema en el uso de los certificados digitales, comunicación de las dependencias con el departamento central y el monitoreo del estado de los servicios de la red de datos.

Además a este método se lo empleo en el desarrollo de la fase 1, para determinar la situación inicial de la red de datos de la Institución, partiendo con la recolección de información hasta llegar a determinar, mediante el empleo de herramientas como: Nessus, whois y Nmap, cuáles son las vulnerabilidades más críticas a las que se encuentra expuesta y elaborar el respectivo informe sobre las amenazas encontradas.

### 1.2. Método inductivo.

La utilización de este método se empleó en la elaboración de la estructura del marco teórico, buscando información relacionada con el desarrollo del tema.

Este método se lo empleo en la fase 2, ayudo a determinar que la solución para las principales vulnerabilidades encontradas comprende el uso de protocolo TLS en los servicios públicos (correo – portal web), lo que garantiza una comunicación segura con el usuario y así reducir el nivel de riesgo de las vulnerabilidades.

### 1.2. Método científico.

Este método se lo empleo en la fase 3, para analizar las distintas pruebas que se hicieron en base a las configuraciones, para comprobar la validez de los resultados y

realizar un contraste de un antes y un después de aplicar los protocolos seguros sobre los servicios públicos.

Gracia a este método se pudo elegir de mejor manera las herramientas para las actividades como: obtención de información de la Institución, búsqueda de vulnerabilidades, determinación de la herramienta de monitoreo.

## 2. Materiales

Dentro de los materiales necesarios se empleó: computador portátil HP, para establecer las configuraciones de los servicios en equipos virtualizados.

Se virtualizó individualmente equipos con GNU/Linux Debian Wheezy sistema operativo vigente a la fecha del proyecto, para los siguientes servidores:

- Servidor de Correo Seguro.
- Servidor VPN L2TP/IPSec.
- Servidor de Monitoreo (Nagios).

## 3. Técnicas.

### 3.1. Entrevista.

Esta técnica se la aplicó a la Ing. Mónica Jaramillo jefe de departamento de informática de la Institución, con el fin de determinar los distintos inconvenientes que presentaba la red de datos del GAD, delimitar la situación problemática y el problema de investigación, que permitió la elaboración del anteproyecto de tesis.

# f. Resultados.

Corresponden al desarrollo práctico del tema de investigación, para ello se ha dividido en cuatro fases, que se encuentran en el cronograma de actividades.

En la fase 1, se realiza un análisis del estado de la situación de la red de datos del GAD, partiendo de la entrevista al administrador de la red, lo que permitió diseñar la topología del equipamiento físico, así mismo se emplearon herramientas para la obtención de información como: whois y domaintools, identificación y detección de las amenazas más críticas en los servicios de la Institución con la ayuda de la herramienta Nessus, reconocimiento de equipos activos mediante Nmap. Para culminar esta fase se elaboró el informe respectivo sobre la situación actual de la red de datos de la Institución.

Dentro de la fase 2 se realizó la configuración del servidor de correo en un entorno controlado usando los paquetes: postfix, dovecot, ldap, phamm utilizados en el correo institucional y sobre estas configuraciones activar el soporte TLS para los servicios involucrados. Además se configuro Nagios como herramienta para el monitoreo de los servicios que maneja la Institución y por último se realizó la configuración tanto de cliente como servidor para establecer una comunicación mediante VPN usando el estándar L2TP/IPSEC, simulando la conexión que se realiza desde las dependencias hacia el servidor de aplicaciones.

En la fase 3 se realizó pruebas de las configuraciones de la fase anterior tanto del servidor de correo como de la VPN L2TP/IPSEC y la herramienta de monitoreo Nagios, determinar el rendimiento de cada una de las soluciones, observar el beneficio que estas brindan para garantizar una comunicación segura y monitorear aquellos servicios que se consideren esenciales para la red de datos.

En la fase 4 se proporcionó la documentación adecuada al administrador de la red, para que este pueda aplicar las configuraciones en el servidor de pruebas de la Institución.

**Fase 1: Diagnóstico de la situación de la red de datos del GAD.**

Dentro de esa fase se tomó como punto de partida la información proporcionada por el administrador de la red de datos de la Institución, quien informó los problemas de la red de datos, luego se continuó con las demás actividades que a continuación se detallan:

## 1. Equipamiento disponible en la red de la Institución.

En base a la información proporcionada por el administrador de la red se pudo elaborar una topología, que se muestra en la figura 13, que indica la ubicación de los principales elementos de la red de datos como son: dispositivos finales (terminales) de acuerdo a las áreas físicas de la Institución; dispositivos intermediarios (switchs/conmutadores); equipos servidores. Además conocer cómo se realizan las conexiones tanto internamente como hacia internet.

En la Tabla VIII se muestra en resumen el total de servidores que dispone la Institución con sus características físicas:

TABLA VIII: SERVIDORES DE LA RED DE DATOS DEL GAD

| SERVIDORES DE LA RED DE DATOS DEL GAD | | | | | |
|---|---|---|---|---|---|
| Etiqueta | **Marca** | **Modelo** | **Núm. / Procesador / Ghz** | **HDD Núm/Cap.** | **RAM** |
| **Web 1.1** | IBM | System X3650 | 4 / Intel Xeon / 2.66 | 1 / 500 GB | 18 GB |
| **Proxy** | IBM | X Series 226 | 2 / Intel Xeon / 3.00 | 2 / 75 GB | 1 GB |
| **Aplicaciones** | IBM | X Series 226 | 4 / Intel Xeon / 2.66 | 2 / 75 GB | 1 GB |
| **Quipux** | IBM | X Series 226 | 4 / Intel Xeon / 3.20 | 2 / 75 GB | 8 GB |
| **Base de Datos** | IBM | X Series 226 | 4 / Intel Xeon / 2.66 | 2 / 75 GB | 2 GB |
| **Catastros** | HP | Proliant DL 160G6 | 1 / Intel Xeon / 2.00 (4 núcleos) | 2 / 250 GB | 4 GB |
| **SIGAME** | IBM | X Series 226 | 4 / Intel Xeon / 3.20 | 1 / 300 GB | 1 GB |
| **GIMM** | HP | BL 460C G7 X 5670 | 4 / Intel Xeon / 2.93 | 1 / 500 GB | 12 GB |
| **Base de** | HP | BL 460C G7 | 4 / Intel Xeon / 2.93 | 1 / 500 GB | 16 |

| | | | | | |
|---|---|---|---|---|---|
| **Datos** | | X 5670 | | | GB |
| **P Pless** | HP | BL 460C G7 X 5670 | 4 / Intel Xeon / 2.93 | 1 / 500 GB | 12 GB |
| **Sistema de pruebas** | HP | BL 460C G7 X 5670 | 4 / Intel Xeon / 2.93 | 1 / 500 GB | 12 GB |

La topología indicada en la figura 13 muestra el direccionamiento y distribución principal de los equipos que pertenecen a la Institución permitiendo así tener una visión global de cómo está constituida la red de datos. En ella se puede observar que no se cuenta al menos con un dispositivo cortafuego, que esté conectado directamente al enrutador proveído por el ISP de la institución, con este dispositivo se filtraría de manera precisa las conexiones desde y hacia los equipos de la intranet, además permitiría establecer una zona DMZ que permita el acceso a los servidores públicos desde internet, garantizar acceso a los servidores privados solo desde la red local y extranet. Sin embargo los servidores de la institución poseen cada uno sus políticas de seguridad individuales, los servidores no cuentan con software para detección y prevención de intrusiones por lo tanto estos se encuentran expuestos a ataques informáticos desde internet y desde la intranet.

Se observa que los equipos correspondientes a dependencias locales conectan a un servidor de aplicaciones, esta intercomunicación la realizan mediante el alquiler de servicio de enlace de datos a la empresa Telconet, por lo tanto la seguridad de las comunicaciones dependientes de este enlace son responsabilidad de dicha empresa.

También se aprecia que los equipos correspondientes a dependencias rurales conectan al mismo servidor de aplicaciones indicado anteriormente, pero este tipo de conexión es solventado por un servicio VPN de acceso remoto a lo cual el administrador de la red indicó que es una solución que se encuentra bajo pruebas.

La última sección restante del gráfico es la correspondiente a equipos con direccionamiento privado, tanto para servidores como computadores de uso personal y recursos compartidos a nivel local.

Cabe añadir que en esta topología tampoco se indica una sección de cobertura de red inalámbrica, esto puesto que no es una necesidad el proveer este tipo de acceso a toda el área que compone la infraestructura física institucional. De existir puntos de

accesos configurados para permitir conexiones inalámbricas se desconoce su ubicación y por esto no han sido incluidos en la topología.

De todas estas secciones indicadas en está topología solo se consiguió acceso a trabajar sobre la red pública concerniente a los servidores. Entonces se procedió a realizar un análisis de las vulnerabilidades sobre la red pública de servidores como se indica en este documento.

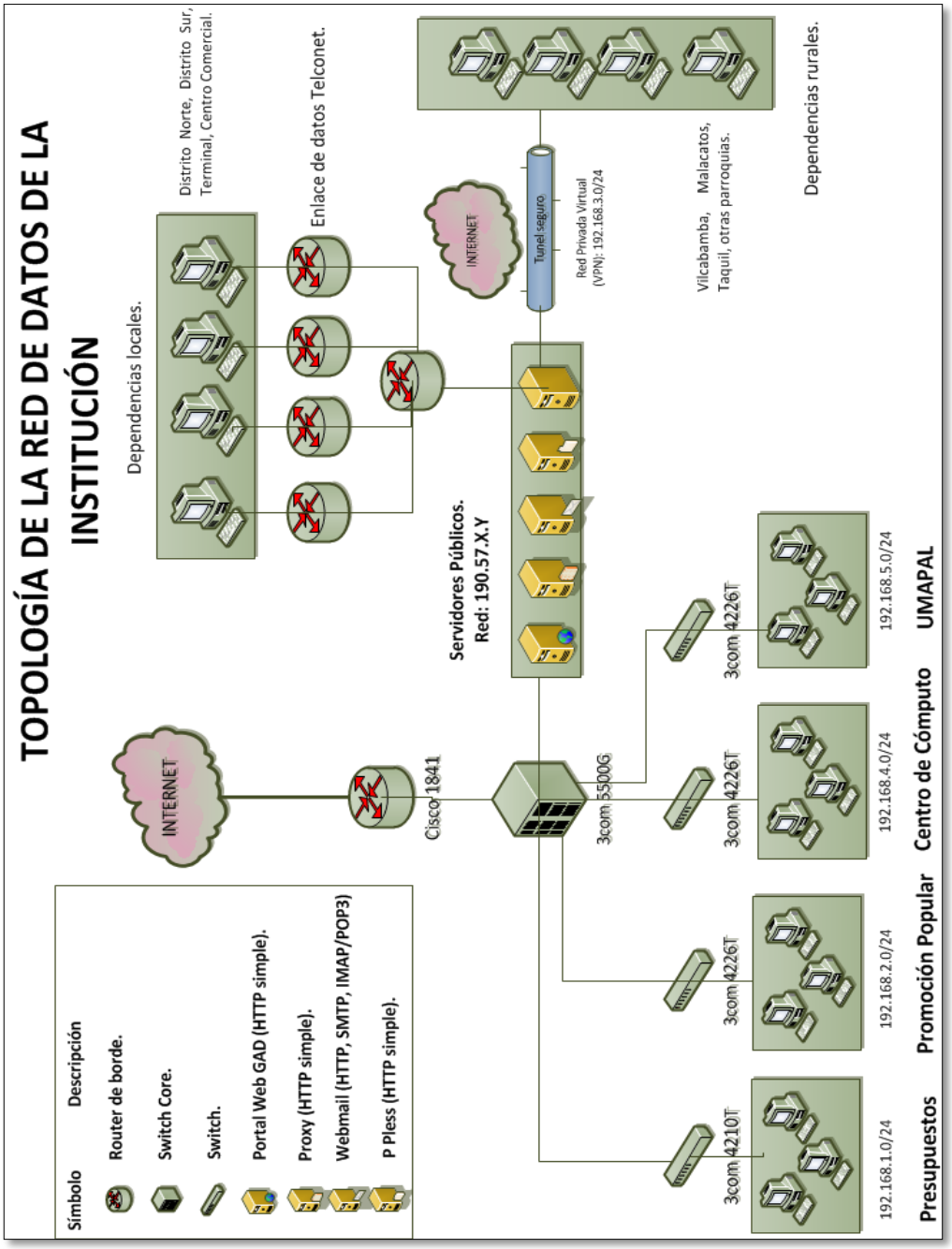



Figura 13: Topología de la red de datos del GAD Municipal de Loja

En cuanto respecta a los equipos intermediarios, en la figura 14 se muestra cada uno de ellos, los mismos están ubicados en cada una de las dependencias de la Institución y garantizan una comunicación exitosa con los servicios que dispone la Institución.

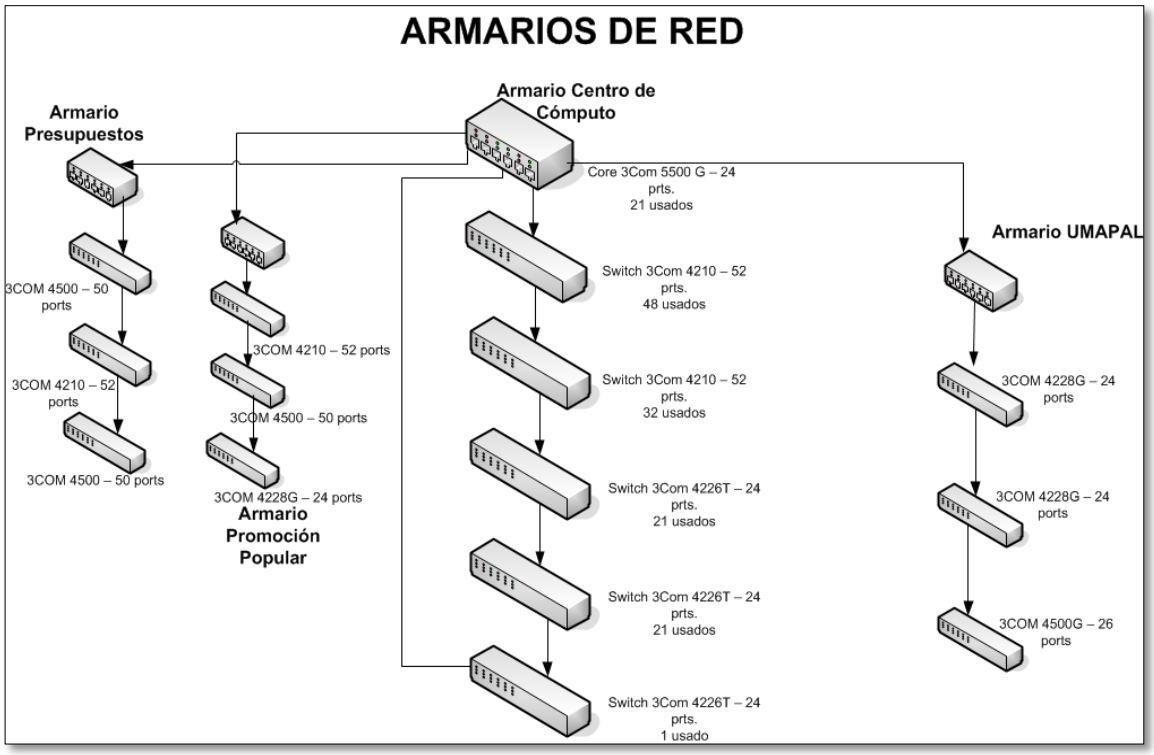



Figura 14: Equipos intermediarios de la red de datos de la Institución.

## 1.1. Listado de servidores disponibles en la red de datos.

Para respaldar la topología anteriormente mostrada, en esta sección se indica el total de servidores disponibles físicamente en la red de datos de la Institución; para determinar en los siguientes puntos sobre cuál(es) se aplicará la mejora de seguridad.

La red de datos dispone de un total de 11 servidores, para conocer el detalle de cada uno de ellos, las aplicaciones que tiene instaladas y la función que cumple dentro de la red de datos; se elaboró una ficha para cada uno (ver Anexo 2 para más detalle). A continuación se listan algunos de los servidores disponibles:

- Servidor Web.
- Servidor Proxy.
- Servidor de Correo.

- Servidor de Base de datos.
- Servidor de Aplicaciones.
- Quipux.
- Servidor de Pruebas.

## 2. Recolección de información.

Esta sección tiene como fin recolectar información relevante de la Institución como dirección IP, registro del dominio; a través de herramientas como: ***whois*** (funciona solo en linux), ***domainstool*** y ***searchdns.netcraft*** (estas dos últimas son herramientas web); utilizando como parámetro de búsqueda el dominio institucional (loja.gob.ec).

El uso de las herramientas antes mencionadas permitieron obtener información como: el dominio (loja.gob.ec), la empresa encargada del registro, conocer la dirección ip del portal del GAD y con ello se determinó el bloque de direcciones ip's que maneja la Institución. A continuación se detalla el resultado obtenido de cada una de ellas:

### 3.1 Uso del sitio: www.domaintools.com

Este sitio web es uno de los más utilizados al momento de realizar consultas, brinda información detallada de la Institución, del empleo del dominio se obtuvo la Tabla IX:

TABLA IX: EMPLEO DE DOMAINSTOOLS SOBRE EL PORTAL DEL GAD

| **Información del dominio** | |
|---|---|
| Servidores de nombre | server.punto.net.ec<br>dns2.punto.net.ec |
| **Información del registro** | |
| Nombre de organización encargada del registro | NIC.EC Registrar |
| **Información del registrante** | |
| Nombre del registrante | Ing. Jorge Bailón Abad |
| Organización | Municipio de Loja |
| Dirección de correo | alcalde@municipiodeloja.gov.ec |
| Número de teléfono | 5937-2570407 |
| **Contacto administrativo** | |
| Nombre | Fausto Maldonado |
| Organización | Municipio de Loja |
| Dirección de correo | fmaldonado@municipiodeloja.gov.ec |
| Número de teléfono | 5937-2570407 |
| **Contacto Técnico** | |

| | |
|---|---|
| Nombre | Ing. Darwin Betancourt Castillo |
| Organización | Municipio de Loja |
| Dirección de correo | soporte.iml@gmail.com |
| Número de teléfono | 5937-2570407 |
| **Contacto de facturación** | |
| Nombre | Lic. Fausto Rojas |
| Organización | Municipio de Loja |
| Dirección de correo | frojas@ municipiodeloja.gov.ec |
| Número de teléfono | 5937-2570407 |

### 3.2 Uso del sitio: http://searchdns.netcraft.com/

Esta herramienta web permite recopilar información sobre el sistema operativo, servidor web usado, el tiempo que lleva el servidor funcionando (uptime), propietario del espacio de direcciones IP, o el historial de cambios relacionados con el servidor Web y el Sistema Operativo, en la Tabla X se muestra información relevante luego de aplicar sobre el dominio de la Institución.

TABLA X: DATOS OBTENIDOS CON EL USO DE NETCRAFT

| **RED** | |
|---|---|
| Dominio | gob.ec |
| Dirección IPv4 | 190.57.168.196 |
| Servidor de Nombres | master.nic.ec |
| Administrador de DNS | dnsadmin@nic.ec |
| DNS Inverso | corp-190-57-168-196-uio.puntonet.ec |
| Compañía que hospeda | punto.net.ec |
| **Historial de Hospedaje** | |
| Propietaria de bloque de red | PUNTONET S. A. Quito |
| Dirección IP | 190.57.168.35 |
| Sistema Operativo | Linux |
| Servidor Web | Apache |
| Último cambio realizado | 3 de Febrero de 2013 |
| Seguridad | 7/10 |
| **Tecnología del sitio** | |
| **Lado del Servidor** | |
| PHP habilitado | El servidor soporta PHP |
| XML | No hay descripción |
| **Lado del Cliente** | |
| Javascript | Lenguaje de programación de código abierto normalmente implementado como parte de un navegador web |
| **Gestor de Contenidos** | |
| Drupal | Un sistema de gestión de contenido de código abierto. |

## 3.3 Uso del comando Whois

En la figura 15 se muestra parte del resultado de emplear este comando, la misma que especifica la entidad del sitio que se busca, en este caso es ***http://nic.ec*** y es precisamente esta entidad quien registra los sitios web a nivel nacional.

```
root@kali:~# whois www.loja.gob.ec


Los datos detallados a continuación por NIC.EC es informacion publica cuyo propo
sito es
unicamente informativo que sirve para la obtencion de la informacion acerca de o
relacionado con los registros de un Nombre de Dominio. Los datos se muestran de
acuerdo
a los datos de NIC.EC en la ultima actualizacion de su base de datos. Al realiza
r una
busqueda de WHOIS de un dominio, usted declara y acepta que los datos seran util
izados
solo para fines legales y que no utilizara los datos para envios masivos no soli
citados
de correo electronico o para publicidad o fines comerciales no solicitados.



Domain Information
Query: www.loja.gob.ec
Status: This WHOIS server does not have any records for that zone.
```

Figura 15: Uso del comando whois ingresando url del sitio

Pero en cambio, ingresando la dirección ip correspondiente al sitio objetivo muestra el resultado tal como se observa en la figura 16.

```
root@kali:~# whois 190.57.168.196

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2013-06-12 00:56:36 (BRT -03:00)

inetnum:     [redacted]
status:      reallocated
owner:       MUNICIPIO DE LOJA - MATRIZ
ownerid:     EC-MLMA1-LACNIC
responsible: MONICA JARAMILLO
address:     BOLIVAR Y JOS$ ANTONIO EGUIGUREN, ESQUINA, ,
address:     593 - Loja -
country:     EC
phone:       +593 07 2570407 []
owner-c:     RFC
tech-c:      RFC
abuse-c:     RFC
created:     20130426
changed:     20130426
inetnum-up:  190.57.128/18

nic-hdl:     RFC
person:      Roberto Falconi Cardona
e-mail:      roberto@PUNTO.NET.EC
address:     Amazonas 45 45 y Pereira Of. 401, 4545,
address:     0000 - Quito - PI
country:     EC
phone:       +593 22 2989900 [125]
created:     20030221
changed:     20060112

% whois.lacnic.net accepts only direct match queries.
```

Figura 16: Uso de comando whois ingresando la dirección IP del portal

De la figura anterior se recopila información que se detalla en la Tabla XI, además la red de direcciones públicas asignadas para el GAD Municipal de Loja posee un prefijo 27, esto indica que la red puede hacer uso de 30 Ip's públicas a su disposición.

TABLA XI: DATOS OBTENIDOS MEDIANTE WHOIS

| **Datos obtenidos mediante la aplicación whois** | |
|---|---|
| Inetnum (Bloque de red asignado) | 190.57.X.Y/27 |
| Propietario | MUNICIPIO DE LOJA - MATRIZ |
| Id de Propietario | EC-MLMA1-LACNIC |
| Responsable | Mónica Jaramillo |
| Teléfono de la Institución(GAD) | +593 07 2570407 |
| Contacto Administrativo (owner-c) | RFC |
| Contacto Técnico (tech-c) | RFC |
| Contacto de Seguridad (abuse-c) | RFC |
| Fecha de creación | 20130426 |
| Fecha de último cambio | 20130426 |
| **Información administrativa** | |
| Nic-hdl | RFC |
| Persona encargada | Roberto Falconi Cardona |
| Correo electrónico | Roberto@PUNTO.NET.EC |
| País | EC |
| Teléfono | +593 22 2989900 [125] |
| Fecha de creación | 20030221 |
| Fecha de último cambio | 20060112 |

## 3. Reconocimiento de equipos activos en la red de datos de la Institución.

Con el uso de Nmap, utilizando el bloque de direcciones del GAD como parámetro, se obtuvo las direcciones IP activas que maneja la Institución, el resultado se aprecia en la Tabla XII.

# **nmap -sn 190.57.X.Y/27**; comando utilizado

TABLA XII: DIRECCIONES IP ACTIVAS DEL GAD

| **DIRECCIÓN IP** |
|---|
| 190.57.X.Y |
| 190.57.X.Y |
| 190.57.X.Y |
| 190.57.X.Y |
| 190.57.X.Y |
| 190.57.X.Y |
| 190.57.X.Y |
| 190.57.X.Y |
| 190.57.X.Y |
| 190.57.X.Y |

Una vez conocidas las direcciones activas, nuevamente se empleó Nmap (sobre cada una de las direcciones de la Tabla XII), pero en esta ocasión, se determinó los puertos abiertos, el resultado se muestra en la Tabla XIII.

TABLA XIII: PUERTOS ABIERTOS SOBRE CADA UNA DE LAS DIRECCIONES IP

| **IP: 190.57.X.Y** | | | |
|---|---|---|---|
| **PUERTO** | **ESTADO** | **SERVICIO** | **VERSIÓN** |
| 23/tcp | abierto | telnet | Cisco router telnetd |
| 25/tcp | filtrado | smtp | |
| 53/udp | filtrado | domain | |
| 161/udp | abierto | snmp | Cisco SNMP service |
| **IP: 190.57.X.Y** | | | |
| 22/tcp | abierto | ssh | OpenSSH 5.5p1 Debian 6 (protocol 2.0) |
| 25/tcp | filtrado | smtp | |
| 53/tcp | abierto | domain | ISC BIND 9.7.3 |
| 53/udp | abierto | | |
| 161/udp | abierto | snmp | SNMPv1 server (public) |
| **IP: 190.57.X.Y** | | | |
| 25/tcp | filtrado | smtp | |
| 80/tcp | abierto | http | |
| 110/tcp | abierto | pop3 | Dovecot pop3d |
| **IP: 190.57.X.Y** | | | |
| 22/tcp | abierto | ssh | |
| 25/tcp | filtrado | smtp | |
| 80/tcp | abierto | http | |
| 110/tcp | abierto | pop3 | Dovecot pop3d |
| 143/tcp | abierto | imap | Dovecot imapd |
| 389/tcp | abierto | ldap | OpenLDAP 2.2.X - 2.3.X |
| | | | |
| **IP: 190.57.X.Y** | | | |
| **PUERTO** | **ESTADO** | **SERVICIO** | **VERSIÓN** |
| 21/tcp | abierto | ftp | Alfresco Document Management |
| 22/tcp | abierto | ssh | OpenSSH 5.5p1 Debian 6+squeeze1 (protocol 2.0) |
| 25/tcp | filtrado | smtp | |
| 80/tcp | abierto | http | Apache httpd 2.2.16 ((Debian)) |
| 111/tcp | abierto | rpcbind | 2 (RPC #100000) |
| 139/tcp | abierto | netbios-ssn | |
| 389/tcp | abierto | ldap | OpenLDAP 2.2.X - 2.3.X |
| 445/tcp | abierto | microsoft-ds | |
| 1090/tcp | abierto | ff-fms | |
| 1098/tcp | abierto | rmiregistry | Java RMI |
| 1099/tcp | abierto | ovm-manager | Oracle VM Manager |
| 4444/tcp | abierto | krb524 | |
| 4445/tcp | abierto | ovm-manager | Oracle VM Manager |

| | | | |
|---|---|---|---|
| 4446/tcp | abierto | ovm-manager | Oracle VM Manager |
| 5432/tcp | abierto | postgresql | PostgreSQL DB (Spanish) |
| 8008/tcp | abierto | ajp13 | Apache Jserv (Protocol v1.3) |
| 8009/tcp | abierto | ajp13 | Apache Jserv (Protocol v1.3) |
| 8080/tcp | abierto | http | Apache Tomcat/Coyote JSP engine |
| 8083/tcp | abierto | http | JBoss service httpd |
| 8088/tcp | abierto | http | Apache Tomcat/Coyote JSP engine |
| 8443/tcp | abierto | ssl/http | Apache Tomcat/Coyote JSP engine |
| 50500/tcp | abierto | unknown | |
| 111/udp | abierto | rpcbind | |
| 5353/udp | abierto | mdns | DNS-based service discovery |
| **IP: 190.57.X.Y** | | | |
| **PUERTO** | **ESTADO** | **SERVICIO** | **VERSIÓN** |
| 22/tcp | abierto | ssh | OpenSSH 5.5p1 Debian 6+squeeze1 (protocol 2.0) |
| 25/tcp | filtrado | smtp | |
| 80/tcp | abierto | http | Apache httpd 2.2.16 ((Debian)) |
| 111/tcp | abierto | rpcbind | |
| 443/tcp | abierto | http | Apache httpd 2.2.16 ((Debian)) |
| 1198/tcp | abierto | cajo-discovery | |
| 1199/tcp | abierto | ovm-manager | Oracle VM Manager |
| 1201/tcp | abierto | nucleus-sand | |
| 5555/tcp | abierto | freeciv | |
| 8000/tcp | abierto | http | Apache httpd 2.2.16 ((Debian)) |
| 8080/tcp | abierto | http | Apache httpd 2.2.16 ((Debian)) |
| 8180/tcp | abierto | http | Apache Tomcat/Coyote JSP |
| 111/udp | abierto | rpcbind | |
| 5353/udp | abierto | mdns | DNS-based service discovery |
| **IP: 190.57.X.Y** | | | |
| **PUERTO** | **ESTADO** | **SERVICIO** | **VERSIÓN** |
| 21/tcp | abierto | ftp | Alfresco Document Management System ftpd |
| 22/tcp | abierto | ssh | OpenSSH 5.5p1 Debian 6+squeeze1 (protocol 2.0) |
| 25/tcp | filtrado | smtp | |
| 111/tcp | abierto | rpcbind | 2 (RPC #100000) |
| 139/tcp | abierto | netbios-ssn | |
| 445/tcp | abierto | microsoft-ds | |
| 1198/tcp | abierto | cajo-discovery | |
| 1199/tcp | abierto | ovm-manager | Oracle VM Manager |
| 5432/tcp | abierto | postgresql | PostgreSQL DB (Spanish) |

| | | | |
|---|---|---|---|
| 8008/tcp | abierto | ajp13 | Apache Jserv (Protocol v1.3) |
| 8080/tcp | abierto | http | Apache Tomcat/Coyote JSP |
| 8088/tcp | abierto | http | Apache Tomcat/Coyote JSP engine 1.1 |
| 8180/tcp | abierto | http | Apache Tomcat/Coyote JSP engine 1.1 |
| 8443/tcp | abierto | ssl/http | Apache Tomcat/Coyote JSP engine 1.1 |
| 50500/tcp | abierto | unknown | |
| 111/udp | abierto | rpcbind | |
| 137/udp | abierto | netbios-ns | |
| 5353/udp | abierto | mdns | DNS-based service discovery |
| **IP: 190.57.X.Y** | | | |
| **PUERTO** | **ESTADO** | **SERVICIO** | **VERSIÓN** |
| 25/tcp | filtrado | smtp | |
| 111/tcp | abierto | rpcbind | 2 (RPC #100000) |
| 5432/tcp | abierto | postgresql | PostgreSQL DB 9.1.0 - 9.1.1 |
| 111/udp | abierto | rpcbind | |
| **IP: 190.57.X.Y** | | | |
| **PUERTO** | **ESTADO** | **SERVICIO** | **VERSIÓN** |
| 25/tcp | filtrado | smtp | |
| 111/tcp | abierto | rpcbind | |
| 111/udp | abierto | rpcbind | |
| **IP: 190.57.X.Y** | | | |
| **PUERTO** | **ESTADO** | **SERVICIO** | **VERSIÓN** |
| 22/tcp | abierto | ssh | OpenSSH 5.5p1 Debian 6+squeeze1 (protocol 2.0) |
| 25/tcp | filtrado | smtp | |
| 80/tcp | abierto | http | Apache httpd 2.2.16 ((Debian)) |
| 111/tcp | abierto | rpcbind | 2 (RPC #100000) |
| 1090/tcp | abierto | ff-fms | |
| 1091/tcp | abierto | ff-sm | |
| 1098/tcp | abierto | rmiregistry | Java RMI |
| 1099/tcp | abierto | ovm-manager | Oracle VM Manager |
| 4446/tcp | abierto | ovm-manager | Oracle VM Manager |
| 5500/tcp | abierto | hotline | |
| 8009/tcp | abierto | ajp13 | Apache Jserv (Protocol v1.3) |
| 8080/tcp | abierto | http-proxy | |
| 8083/tcp | abierto | http | JBoss service httpd |
| 111/udp | abierto | rpcbind | |

## 4. Elección de herramienta para la detección de amenazas.

Primero se seleccionó la herramienta a utilizar para determinar el tipo de amenazas a las que está expuesto la red de datos de la Institución; la Tabla XIV muestra las principales características de cada una de las herramientas destinadas a la detección de amenazas.

TABLA XIV: COMPARACIÓN DE LAS HERRAMIENTAS DE ESCANEO DE VULNERABILIDADES

| | Nessus | OpenVas | NexPose | Nikto | W3af |
|---|---|---|---|---|---|
| **Distribuciones** | 2 Professional/ HomeFeed | 1 | 2 Enterprise/ Comunity | 1 | 2 |
| **Versión** | v5 | 5.0 | | 2.1.5 | 1.1 |
| **Liberada** | | Mayo 2012 | | 17/12/2012 | - |
| **Plugins** | 54575 | 30000 | - | - | 130 |
| **Plataforma** | Multi-plataforma | | Multi-plataforma | | Multi-plataforma |
| **Licencia** | GPL | GPL | | GPL | GLPv2 |
| **Desarrollado** | | | | Perl | Python |
| **IP a escanear** | 16 | no tiene limitante | 32 | - | - |
| **Interfaz** | Consola/ Navegador | Gráfica | Gráfica | Consola | Consola/ Gráfica |
| **Arquitectura** | Cliente/ Servidor | Cliente/ Servidor | - | - | Cliente/ Servidor |

Para determinar cuál de estas herramientas permiten cumplir el objetivo de detectar las vulnerabilidades, se probó cada una de ellas en base a los siguientes criterios:

- Consumo de recursos hardware.
- Complejidad en la configuración de la herramienta.
- Detalle de los escaneos realizados.

Al analizar cada herramienta en base a los criterios antes mencionados; Nexpose en el primer requisito quedo fuera, por cuanto la cantidad de memoria que debe de utilizarse es de 4 GB, una desventaja evidente el consumo elevado de RAM si comparamos con herramientas como: nikto y w3af que se pueden ejecutar desde consola.

Nikto y W3af son herramientas que en cuanto a recursos de hardware funcionan sobre el sistema base, a través de la línea de comando, mientras que su configuración es bastante sencilla. La desventaja que tienen y que también es notoria es el detalle de los escaneos que realiza.

Por último solo queda por revisar Nessus y OpenVas las cuales son herramientas que brindan un detalle completo del escaneo, cada una de ellas da una puntuación de acuerdo a la vulnerabilidad que encontró. Su instalación y configuración en sencilla, además posee licencia GPL. EL detalle de los escaneos de OpenVas, está más orientado a aquellas personas con un conocimiento más técnico en las amenazas, puesto que utiliza CVS para identificar y categorizar las mismas; por esta razón a OpenVas no se la considero.

La herramienta con la cual se realizará el escaneo de las vulnerabilidades será Nessus, por que no consume muchos recursos de hardware, además brinda un detalle completo de los escaneos que realiza y cada tipo de vulnerabilidad que encuentre la evalúa según los tipos de nivel ya sea: crítico, alto, medio, bajo e inf (este último nivel hace referencia solo al tipo informativo, es decir proporciona únicamente información).

## 5. Elección de alternativa a VPN OpenVPN.

La Institución hace uso de OpenVPN en la actualidad para interconectar las dependencias rurales con la oficina central, en la Tabla XV se muestra las principales características de los protocolos más conocido y utilizados en una VPN, además se realiza una comparativa para determinar cuál de ellas brinda mayor seguridad y rendimiento:

TABLA XV: PROTOCOLOS USADOS EN VPN

| | **PPTP** | **L2TP/IPSEC** | **OPENVPN** | **SSTP** |
|---|---|---|---|---|
| **Método de autenticación** | MS-CHAP v2 | Claves pre-compartidas, certificado X509 | Basado en llaves secretas pre-compartidas o Certificados X509 | EAP MS-CHAP v2, EAP-TLS |
| **Plataformas** | A partir de Windows 2000, Linux, iOS, Android | A partir de Windows XP, Linux, iOS, Android | Requiere que en sistema operativo se instale el cliente | A partir de Windows Vista, |

| | | | OpenVPN | |
|---|---|---|---|---|
| **Instalación** | Fácil | Fácil | Fácil | Fácil |
| **Claves de cifrado** | Microsoft Point-to-Point Encryption (MPPE) de 128 bits | AES 128 bits.<br><br>AES 256 bits | AES 128 bits<br><br>AES 256 bits | Canal SSL al protocolo HTTPS |
| **Puertos que maneja** | Puerto TCP 1723, además del protocolo con el id 47 (GRE) | Puertos 1701, udp 500 y los protocolos de id 50 (ESP) y 51 (AH) | Puerto upd 1194, aunque se puede configurar para que funcione en el puerto TCP 443 | Se configura para que trabaje sobre el puerto TCP 443. |

Para determinar que protocolo de VPN es un buen candidato como alternativa a OpenVPN, se realizó un análisis de cada una de ellas:

- PPTP (Point to Point Tunneling Protocol) se utiliza en clientes de Microsoft, a partir de Microsoft Windows 2000. Al contrario que L2TP/IPsec, PPTP ofrece un mayor desempeño al momento del envió de datos y proporcionan confidencialidad de datos, pero no garantiza integridad ni autenticación si se compara con L2TP/IPSEC, por estas razones se determinó de PPTP no cumple con los requisitos mínimos de seguridad.

- En lo que respecta a SSTP (Secure Socket Tunneling Protocol) puede usarse en equipos cliente que ejecuten Windows a partir de la versión Vista Service Pack 1 (SP1) o posteriores. Las conexiones VPN basadas en SSTP proporcionan confidencialidad, integridad y autenticación de datos si se utiliza con el protocolo SSL. Al tratarse de un protocolo creado por Microsoft su código fuente aún no ha sido liberado por lo tanto no está disponible para otros tipos de plataformas, esto impide que se pueda utilizar en entornos que utilizan sistemas operativos heterogéneos como es el caso de la Institución.

- L2TP/IPSec se puede usar en equipos cliente a partir de Windows XP o posteriores. Admite certificados de usuario o una clave pre-compartida como método de autenticación. La autenticación de certificados de equipo, que es el método de autenticación recomendado, requiere una PKI para emitir

certificados de equipo al servidor VPN y a todos los equipos cliente VPN. Las conexiones VPN basadas en L2TP/IPSec proporcionan confidencialidad, integridad y autenticación de datos.

Luego de conocidas las soluciones VPN's anteriormente indicadas se pudo concluir que la mejor alternativa a OpenVPN, gracias a su desempeño, fiabilidad en las comunicaciones, fácil instalación en el cliente y por cumplir con los requerimientos de seguridad necesarios, L2TP/IPSEC es considerado dentro del desarrollo de esta investigación.

## 6. Elección de la herramienta de monitoreo para la red de datos.

A continuación se pone a consideración las herramientas de monitoreo, se las evalúa en base a ciertos criterios tales como: medio de control, capacidad de instalar plugins adicionales, funcionalidad de enviar alertas, así como las bases de datos que utiliza. La Tabla XVI muestra las características de las herramientas.

Para determinar qué herramienta cumple mejor el papel de monitoreo, se consideraron las siguientes herramientas: Nagios, Cacti, Zabbix, Zenoss y Pandora FMS, las cuales son evaluadas en base a los siguientes criterios:

- Generación de informes.
- Elaboración de estadísticas.
- Soporte técnico, a través de foros.
- Base de datos que administra.

TABLA XVI: TABLA COMPARATIVA DE LAS HERRAMIENTAS DE MONITOREO

| | NAGIOS | ZABBIX | CACTI | ZENOSS | PANDORAFMS |
|---|---|---|---|---|---|
| **Gráficas** | Si | Si | Si | Si | Si |
| **Informes SLA Acuerdo de Nivel de Servicio** | Si | Si | Si | No | Tiempo real y programados |
| **Grupos Lógicos** | Si | Si | Si | Si | Si |
| **Estadísticas** | Si | Si | Si | Si | Si |
| **Agentes** | Si | Si | Si | SNMP, WMI, JMX | Con y sin Agente |
| **SNMP** | A través de plugins | Si | Si | Si | Si |
| **SYSLOG** | Si | Si | Si | Si | Si |
| **Scripts externos** | Si | Si | Si | Si | Si |
| **Plugins** | Si | Si | Si | Si | Si |
| **Alertas** | Si | Si | Si | Si | Si |
| **Aplicación Web** | | Control total | Si | Control total | Control total |
| **Base de datos** | MySQL | MySQL, PostgreSQL, Oracle o SQLite | RRDtools | MySQL | MySQL |
| **Licencia** | GPL | GPL | GPL | Privativa | GPL/Entreprise |
| **Mapas** | - | Si | Si | Si | Mapas de red automáticos |

PandoraFMS cumple con los requisitos antes mencionados, pero al tener dos versiones la Enterprise y la Open Source, la primera brinda muchas más funcionalidades incluyendo soporte técnico en tiempo real con personas especializadas en su funcionamiento, mientras que para la segunda se reducen significativamente funciones tales como: almacenar datos a largo plazo, inventario remoto, personalización de informes, entre otras.

Zenoss se descarta por poseer licencia privativa, y además porque el desarrollo del tema está centrado en la utilización de software libre.

En cuanto a Zabbix, es una herramienta que posee grandes funcionalidades y prestaciones, pero al momento de realizar el monitoreo de un equipo remoto no se pudo establecer la comunicación con el servidor.

Se determinó que Cacti, es una herramienta que brinda las funciones necesarias para poder monitorear las red del GAD, pero como esta herramienta está destinada a

obtener estadísticas del tráfico de la red, se optó por Nagios, si bien no posee la capacidad de generar mapas, tal como lo hace Cacti, sus funciones siguen siendo ideales para poder utilizarla en el monitoreo del estado de los servicios. Además por poseer una comunidad extensa que aporta con scripts para monitorear un servicio en específico, solo hay que buscarlo detenidamente dentro de su sitio web.

## 7. Listado de amenazas detectadas en los servidores de la Institución.

A continuación se muestra las amenazas detectadas por Nessus sobre el bloque de direcciones de equipos activos al momento del escaneo:

**Amenaza detectada en la IP 192.57.X.Y**

TABLA XVII: NIVEL DE LA AMENAZA DETECTADA EN LA IP 192.57.X.Y

| Gravedad | ID del Plugin | Nombre |
|---|---|---|
| Bajo (2.6) | 42263 | Unencrypted Telnet Server |

TABLA XVIII: DESCRIPCIÓN DE LA AMENAZA DE LA IP 192.57.X.Y

| Plugin | Descripción |
|---|---|
| 42263 | El host remoto está ejecutando un servidor Telnet sin cifrar a través de una canal. No se recomienda el uso de un canal no cifrado puesto que un atacante puede espiar a una sesión de Telnet y obtener credenciales u otra información sensible. |

**Amenaza detectada en la IP 192.57.X.Y**

TABLA XIX: NIVEL DE LA AMENAZA DETECTADA EN LA IP 192.57.X.Y

| Gravedad | ID del Plugin | Nombre |
|---|---|---|
| Alto (7.5) | 41028 | SNMP Agent Default Community Name (public) |

TABLA XX: DESCRIPCIÓN DE LA AMENAZA DE LA IP 192.57.X.Y

| Plugin | Descripción |
|---|---|
| 41028 | Es posible obtener el nombre predeterminado del servidor remoto SNMP. Un atacante puede utilizar esta información para obtener más conocimientos sobre el host remoto, o para cambiar la configuración del sistema remoto. |

**Amenaza detectada en la IP 192.57.X.Y**

TABLA XXI: NIVEL DE LA AMENAZA DETECTADA EN LA IP 192.57.X.Y

| Gravedad | ID del Plugin | Nombre |
|---|---|---|
| Medio (5.0) | 46803 | PHP expose_php Information Disclosure |
| Medio (4.3) | 11213 | HTTP TRACE / TRACK Methods Allowed |
| Medio (4.3) | 58040 | phpLDAPadmin lib/QueryRender.php base Parameter XSS |

| | | |
|---|---|---|
| Bajo (2.6) | 26194 | Web Server Uses Plain Text Authentication Forms |
| Bajo (2.6) | 34850 | Web Server Uses Basic Authentication Without HTTPS |

TABLA XXII: DESCRIPCIÓN DE LA AMENAZA DE LA IP 192.57.X.Y

| Plugin | Descripción |
|---|---|
| 46803 | La instalación de PHP en el servidor remoto está configurada de una manera que permite la divulgación de información potencialmente sensible a un atacante a través de una URL especial. |
| 11213 | El servidor web remoto admite el trazado y/o métodos de pista. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones de servidor Web. |
| 58040 | La versión de phpLDAPadmin en el host remoto no limpia adecuadamente el parámetro de "lib/QueryRender.php", lo que ocasiona que un atacante pueda inyectar código script en el navegador de un usuario. |
| 26194 | El servidor web remoto contiene varios campos de formulario HTML que contiene una entrada del tipo "password" que transmite la información a un servidor web remoto en texto plano, tanto así que un atacante puede espiar el tráfico entre el navegador y el servidor y obtener nombres de usuario y contraseñas de los usuarios. |
| 34850 | El servidor web remoto contiene páginas web que están protegidas por una autenticación básica sobre texto plano, un atacante podría obtener los nombres de usuarios y contraseñas. |

### Amenaza detectada en la IP 192.57.X.Y

TABLA XXIII: NIVEL DE LA AMENAZA DETECTADA EN LA IP 192.57.X.Y

| Gravedad | ID del Plugin | Nombre |
|---|---|---|
| Alto (7.5) | 10166 | Windows NT FTP 'guest' Account Present |
| Medio (6.4) | 51192 | SSL Certificate Cannot Be Trusted |
| Medio (6.4) | 57582 | SSL Self-Signed Certificate |
| Medio (5.0) | 57608 | SMB Signing Disabled |
| Bajo (2.6) | 26194 | Web Server Uses Plain Text Authentication Forms |
| Bajo (2.6) | 34324 | FTP Supports Clear Text Authentication |
| Bajo (2.6) | 65821 | SSL RC4 Cipher Suites Supported |

TABLA XXIV: DESCRIPCIÓN DE LA AMENAZA DE LA IP 192.57.X.Y

| Plugin | Descripción |
|---|---|
| 10166 | Hay una cuenta de FTP "invitado".<br>Esta cuenta se ejecuta en un entorno chroot, por lo que es muy probable que un atacante puede utilizarla para entrar en el sistema. |
| 51192 | El certificado del servidor X.509 no tiene la firma de una autoridad de certificación pública conocida. Esta situación puede presentarse en tres formas diferentes, cada una de las cuales da lugar a una ruptura en la cadena por debajo del cual los certificados no se pueden confiar. |
| 57582 | La cadena de certificados X.509 para este servicio no está firmada por una |

| | |
|---|---|
| | autoridad de certificación reconocida. Si el host remoto es un sistema público de producción, este anula el uso de SSL, cualquiera podría establecer un man-in-the-middle contra el host remoto. |
| 57608 | La firma está deshabilitado en el servidor SMB remoto. Esto puede permitir ataques man-in-the-middle contra el servidor SMB. |
| 26194 | El servidor web remoto contiene varios campos de formulario HTML que contiene una entrada del tipo “password” que transmite la información a un servidor web remoto en texto plano. |
| 34324 | El servidor FTP remoto permite que el nombre y la contraseña del usuario se transmitan en texto plano, esto puede ser interceptado por un sniffer de red o un ataque man-in-the-middle. |
| 65821 | El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. |

### Amenaza detectada en la IP 192.57.X.Y

TABLA XXV: NIVEL DE LA AMENAZA DETECTADA EN LA IP 192.57.X.Y

| Gravedad | ID del Plugin | Nombre |
|---|---|---|
| Alto (7.5) | 10166 | Windows NT FTP ‘guest’ Account Present |
| Medio (6.4) | 51192 | SSL Certificate Cannot Be Trusted |
| Medio (6.4) | 57582 | SSL Self-Signed Certificate |
| Medio (5.0) | 12218 | mDNS Detection |
| Medio (5.0) | 45411 | SSL Certificate with Wrong Hostname |
| Medio (5.0) | 57608 | SMB Signing Disabled |
| Bajo (2.6) | 26194 | Web Server Uses Plain Text Authentication Forms |
| Bajo (2.6) | 34324 | FTP Supports Clear Text Authentication |
| Bajo (2.6) | 65821 | SSL RC4 Cipher Suites Supported |

TABLA XXVI: DESCRIPCIÓN DE LA AMENAZA DE LA IP 192.57.X.Y

| Plugin | Descripción |
|---|---|
| 10166 | Hay una cuenta de FTP “invitado”.<br>Esta cuenta se ejecuta en un entorno chroot, por lo que es muy probable que un atacante puede utilizarla para entrar en el sistema. |
| 51192 | El certificado del servidor X.509 no tiene la firma de una autoridad de certificación pública conocida. Esta situación puede presentarse en tres formas diferentes, cada una de las cuales da lugar a una ruptura en la cadena por debajo del cual los certificados no se pueden confiar. |
| 57582 | La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un sistema público de producción, este anula el uso de SSL, cualquiera podría establecer un man-in-the-middle contra el host remoto. |
| 12218 | El servicio remoto entiende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite que cualquiera pueda descubrir la información de la máquina remota como el tipo de sistema operativo y versión exacta, el nombre del host, y la lista de servicios que se están ejecutando. |
| 45411 | El commonName (CN) del certificado SSL presente en este servicio es para un equipo diferente. |
| 57608 | La firma está deshabilitado en el servidor SMB remoto. Esto puede permitir |

| | |
|---|---|
| | ataques man-in-the-middle contra el servidor SMB. |
| 26194 | El servidor web remoto contiene varios campos de formulario HTML que contiene una entrada del tipo “password” que transmiten la información a un servidor web remoto en texto plano. |
| 34324 | El servidor FTP remoto permite que el nombre y la contraseña del usuario se transmitan en texto plano, esto puede ser interceptado por un sniffer de red o un ataque man-in-the-middle. |
| 65821 | El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. |

**Amenaza detectada en la IP 192.57.X.Y**

TABLA XXVII: NIVEL DE LA AMENAZA DETECTADA EN LA IP 192.57.X.Y

| Gravedad | ID del Plugin | Nombre |
|---|---|---|
| Medio (5.0) | 12218 | mDNS Detection |

TABLA XXVIII: DESCRIPCIÓN DE LA AMENAZA DE LA IP 192.57.X.Y

| Plugin | Descripción |
|---|---|
| 12218 | El servicio remoto entiende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite que cualquiera pueda descubrir la información de la máquina remota como el tipo de sistema operativo y versión exacta, su nombre de host, y la lista de servicios que se está ejecutando. |

## 8. Principales vulnerabilidades encontradas en la red de datos de la Institución.

Luego de conocer e identificar las amenazas a las que se encuentran expuestos los servicios de la Institución, así como el correo institucional y el portal, se elabora la Tabla XXIX que comprende las principales vulnerabilidades que pueden afectar a la red de datos:

TABLA XXIX: VULNERABILIDADES MÁS CRÍTICAS DE LA RED DE DATOS

| Dirección IP / Amenazas | Efecto |
|---|---|
| **190.57.X.Y**<br>HTTP TRACE / TRACK Methods Allowed<br>Web Server Uses Plain Text Authentication Forms<br>Web Server Uses Basic Authentication without HTTPS | Robo de la información de inicio de sesión por un atacante |
| **190.57.X.Y**<br>SSL Certificate Cannot Be Trusted<br>SSL Self-Signed Certificate<br>FTP Supports Clear Text Authentication | Los certificados SSL no cuentan con la firma de una autoridad de |

| | |
|---|---|
| SSL RC4 Cipher Suites Supported | certificación reconocida. |
| **190.57.X.Y**<br>SSL Certificate Cannot Be Trusted<br>SSL Self-Signed Certificate<br>SSL Certificate with Wrong Hostname<br>Web Server Uses Plain Text Authentication Forms<br>FTP Supports Clear Text Authentication | Los certificados SSL no cuentan con la firma de una autoridad de certificación |

## 9. Informe de la situación actual de la red de datos de la Institución.

La red de datos de la institución, en lo que respecta a la parte física se pudo constatar, que no cuenta con un equipo hardware dedicado al filtrado de tráfico (cortafuegos), por este motivo cada uno de los servidores tiene configurado sus propias reglas de seguridad incluyendo su cortafuego interno.

En cuanto a la parte lógica los servidores usan como sistema operativo predilecto las siguientes distribuciones: GNU/Linux Debian Lenny, GNU/Linux Debian Squeeze, Suse; por cuestiones de licencias, además de aprovechar los beneficios del software libre como por ejemplo modificar su código y adaptarlo a las necesidades de la Institución.

En lo que respecta a las amenazas, y en base a los resultados obtenidos se concluyó que los servicios que más se ven afectados son el servicio de correo como el del portal por estar al alcance del usuario común a través de internet.

## Fase 2: Desarrollo de la solución.

### 1. Análisis de los correctivos pertinentes para evitar las vulnerabilidades encontradas.

Luego de conocer el impacto que tienen las amenazas sobre la red de datos de la Institución, la mejor alternativa para reducir el impacto es la utilización de **Certificados Digitales** y empleo de protocolos seguros **SSL/TLS**.

Se seleccionó SSL/TLS ya que es un protocolo que brinda seguridad a las comunicaciones desde la capa 4 (transporte) del modelo OSI. Esta decisión fue tomada en base a la información proporcionada por la herramienta Nessus, que además de encontrar las vulnerabilidades en los equipos, también recomienda los correctivos que se deben aplicar para mitigar las amenazas que se encontraron. En el caso de los servidores públicos escaneados, la herramienta recomienda que cualquier aplicación web que haga uso de información confidencial transmita ese contenido a través de HTTPS. En el caso de que Nessus hubiese descubierto otros tipos de vulnerabilidades diferentes, también advertiría sobre qué soluciones se debe realizar para mitigar las mismas.

Otro factor que hace uso en la utilización de certificados digitales como parte de la solución, es la idea que tiene la Institución a futuro de brindar el servicio de transacciones electrónicas (pago de impuestos), facturación electrónica (declaración de impuestos); por decreto del Gobierno esta tecnología debe estar vigente desde el año 2015.

Los certificados digitales serán utilizados tanto en el portal como en el correo institucional; ya que actualmente este último es el primer servicio público que se puede acceder vía web, por eso se exige que las comunicaciones que se establecen sobre este servicio estén debidamente cifradas y que se asegure la integridad de la información de los usuarios cuando se comunican.

En base a la información obtenida sobre la interconexión de las dependencias que se encuentran fuera de la cuidad con la institución, están utilizando OpenVPN para llevar a cabo esta tarea, pero todavía se encuentra en análisis para evaluar su rendimiento y beneficios a futuro.

Como alternativa a OpenVPN se propuso utilizar una solución VPN, que permita comunicar terminales Windows hacia un servidor dentro de la Institución. Para esta tarea se eligió el tipo de VPN de acceso remoto basada en L2TP/IPSec, que se adapta a este requerimiento de intercomunicación.

## 2. Delimitación del espacio de trabajo.

Dentro de esta fase, se montó un laboratorio o escenario de pruebas; lo que permite tener un control de las aplicaciones que se utilizarán, conocer el comportamiento y tener un control de los errores, antes de realizar la implementación en el entorno de producción.

Este escenario cuenta con sistemas virtualizados empleando el sistema operativo GNU/LINUX Debian Wheezy, en donde se realizan las configuraciones para brindar seguridad al servicio de correo, empleando certificados digitales y garantizar un acceso seguro mediante el uso del protocolo HTTPS, con el fin de reducir el impacto de las amenazas.

De la misma manera se ha configurado el servicio de VPN utilizando el estándar L2TP/IPSec, con los certificados creados previamente para cumplir con la propuesta a OpenVPN.

También se abarca las configuraciones y pruebas del servidor nagios para monitorear los servicios del servidor de correo.

## 3. Servicios a implementar.

A continuación se describe las configuraciones para el servicio de correo, alternativa L2TP/IPSEC y herramienta de monitoreo Nagios:

### 3.1 Servidor de correo.

La configuración del servidor de correo, fue llevada a cabo aplicando la paquetería de software sugerida por el administrador de la red, cuyo propósito fue replicar el servicio de correo institucional. A continuación se listan los puntos correspondientes para la configuración del correo seguro:

- Creación de certificados digitales y certificado de la autoridad de certificación local con openssl v1.0.1e, a usar en los servicios del correo seguro, VPN L2TP/IPSec; actuando localmente como una autoridad de certificación (CA).

- Configuración de un sistema de nombres de dominio (tesisgad.com) con bind9 v9.8.4, permitirá identificar de mejor manera la dirección url que hace uso del correo, en lugar de la dirección IP.

- Instalación y configuración de agente de envío de correo postfix v2.9.6, permite el despacho de correo electrónico entre los usuarios de este sistema, usando el protocolo SMTP (Simple Mail Transfer Protocol).

- Instalación de Sldapd v2.4.31 para almacenar cuentas de correo virtuales, corresponde a la base de directorio que almacenará las cuentas virtuales de correo electrónico a usar en el escenario de pruebas, a cada usuario del servicio le corresponderá su cuenta virtual respectiva, haciendo uso del dominio tesisgad.com configurado en el punto anterior.

- Gestión de cuentas de correo virtuales con phamm v.0.5.18, facilita la creación de las cuentas virtuales de correo para cada usuario que desea acceder al sistema.

- Activación del soporte TLS sobre el servicio de postfix v2.9.6, para que el servicio postfix haga uso de los certificados digitales.

- Instalación y configuración de agente de entrega de correo dovecot v2.1.7, facilita al usuario acceder al correo desde el servidor y visualizarlo en su computador, mediante los protocolos IMAP o POP3.

- Configuración de apache v2.2.22 para conexiones SSL.

- Instalación y configuración de cliente de correo web Roundcube v0.7.2, permite la visualización e interacción con los correos a los usuarios que acceden al servicio mediante su cuenta virtual.

Una vez realizada las configuraciones de los puntos anteriores, se realizan las respectivas pruebas; las mismas que se detallan en la fase 3.

## 3.2 Servidor VPN L2TP/IPSEC.

La configuración del servicio IPSec, para intercomunicar las dependencias con la agencia matriz, se resume en dos fases:

- **Preparación del servidor:** Instalación y configuración del servicio IPSec en el equipo servidor, utilizando los paquetes: OpenSwan v2.6.37 y Xl2tpd v1.3.1.
- **Preparación del cliente:** El equipo cliente que hará uso de este servicio debe configurar los siguientes tres aspectos: creación del perfil de conexión, importación de los certificados tanto del usuario como del CA, configuración de políticas de conexión en el firewall para el servicio de IPSec.

## 3.3 Servidor de monitoreo Nagios.

Para facilitar la administración de los servicios que posee la institución se configura Nagios como herramienta de monitoreo opensource en dos fases:

- **Preparación del servidor:** En el equipo servidor se instaló: Nagios Core v4.0.5, front-end Check_mk v1.2.4p4 para visualizar los servicios desde el navegador web y los plugins de Nagios v2.0.
- **Preparación del equipo a monitorear:** El equipo que se monitorea es el servidor de correo (implementado en los pasos anteriores), para ello se debe instalar los siguientes agentes para el monitoreo de los recursos privados: check-mk-agent v1.2.4p4 y check-mk-agent-logwatch v1.2.4p4 (deben corresponder a la misma versión de Check_mk).

## Fase 3: Pruebas de las configuraciones realizadas.

Luego de las configuraciones realizadas tanto en el servidor de correo, l2tp/ipsec y la herramienta de monitoreo Nagios, se deben realizar las pruebas necesarias para verificar su desempeño.

### 1. Pruebas de configuración del servidor de correo

En este apartado se detalla las pruebas realizadas en el servidor de correo, comprenden un total de cuatro, en cada una de ellas se describen las respectivas conclusiones luego de terminada la prueba.

**Prueba 1:** Análisis de servidor de correo Postfix, Dovecot y LDAP, comunicaciones en texto plano (Sin TLS).

**Objetivo:**

- Analizar el flujo de datos en las comunicaciones realizadas entre cliente y servidor de correo cuando este no establece comunicaciones seguras.

**Actividades:**

1. Usar la herramienta wireshark en cliente o servidor para capturar el tráfico que genera la comunicación de prueba.
2. Establecer la comunicación por parte del usuario usando un cliente de correo como thunderbird, icedove, o similar.
3. Analizar el tráfico, identificar y señalar la información sensible que se obtuvo en los siguientes momentos: inicio de sesión, envío de correo, recepción de correo.
4. Visualizar la información sensible encontrada en el tráfico capturado con herramienta wireshark.

**Escenario:**

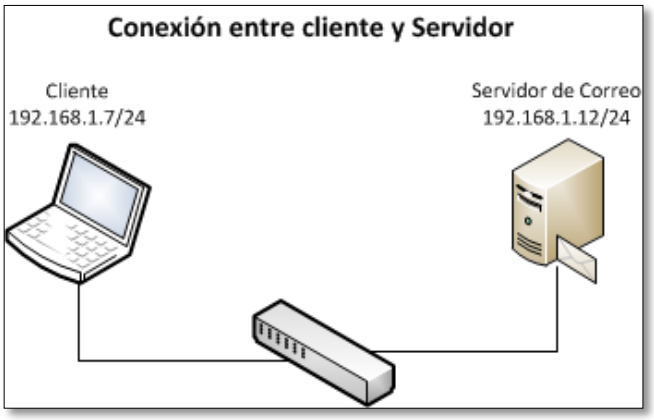



Figura 17: Escenario para análisis de comunicación entre cliente y servidor

**Aplicaciones utilizadas:**

Analizador de tráfico: **Wireshark**

Cliente de correo para escritorio: **Thunderbird**

**Pasos a seguir:**

1. Ejecutar el programa wireshark en el cliente Windows, e iniciar una captura de tráfico como se muestra en la figura 18:


Figura 18: Wireshark como iniciar nueva captura de tráfico

2. Ejecutar el cliente de correo Thunderbird, para asociar una cuenta de correo existente.


Figura 19: ThunderBird ventana de integración con el sistema

3. En la siguiente ventana de Thunderbird cliquear en “Saltarse esto y usar mi cuenta de correo existente”.

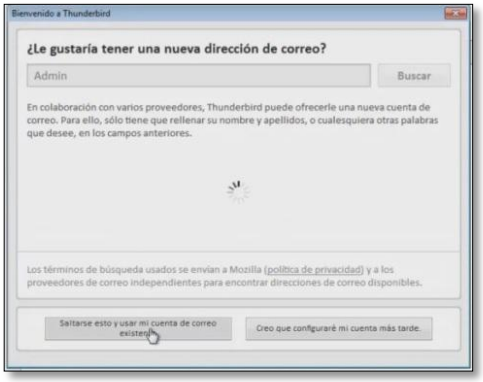



Figura 20: ThunderBird ventana de bienvenida

4. En la ventana a continuación ingresar los datos concernientes a la cuenta de correo que se usará, en este caso la del primer usuario: “María Sánchez” y cliquear en continuar, figura 21.


Figura 21: ThunderBird ventana de configuración de cuenta de correo

5. En la siguiente ventana se observa la información del servidor de correo, el dato más importante es el que indica que el servidor tanto para correo entrante como saliente no soporta cifrado, pulsar en “Hecho” para continuar, figura 22.

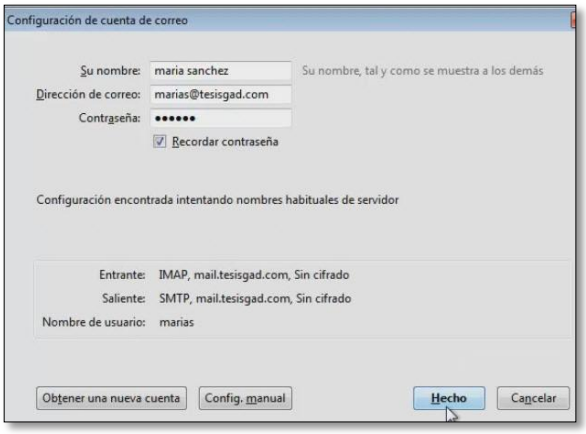



Figura 22: ThunderBird información del tipo de conexión con el servidor

6. A continuación se muestra una ventana de advertencia debido a que el servidor no soporta actualmente conexiones cifradas, señalar “Entiendo los riesgos” y cliquear en “Hecho” para finalizar, figura 23.


Figura 23: ThunderBird ventana de advertencia al momento de iniciar sesión sin usar cifrado.

7. Luego de unos segundos la aplicación muestra el nombre de la cuenta ingresado en su panel de cuentas, figura 24.


Figura 24: ThunderBird cuenta agregada correctamente al panel de cuentas

8. En este momento detener la captura de tráfico que se inició en Wireshark, guardar con un nombre de archivo y analizar el flujo de datos durante el inicio de sesión de dicha cuenta, en la siguiente figura se aprecia en la información obtenida los datos de inicio de sesión de la cuenta ejemplo.

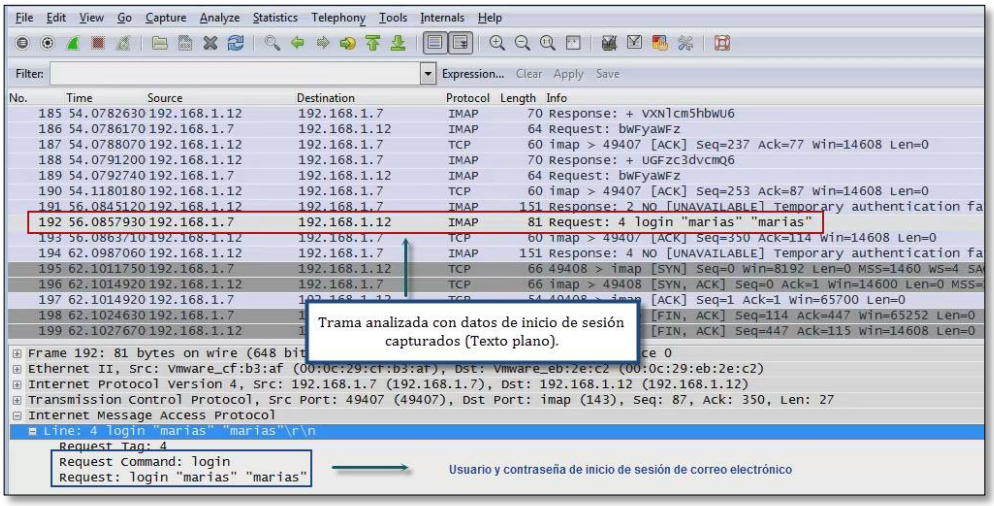



Figura 25: Wireshark datos obtenidos al usar cliente ThunderBird cuando el servidor no ofrece conexiones seguras

9. Para obtener más detalles del fijo de datos de dicha trama seleccionar en el menú contextual la opción “Follow TCP Stream” de la aplicación, tal y como se muestra en la figura 26.

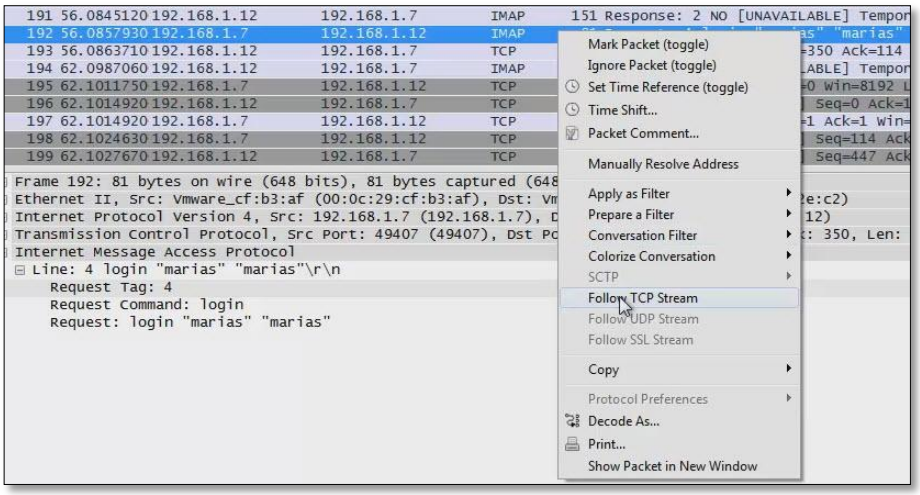


Figura 26: Wireshark opción “Follow TCP Stream” menú contextual

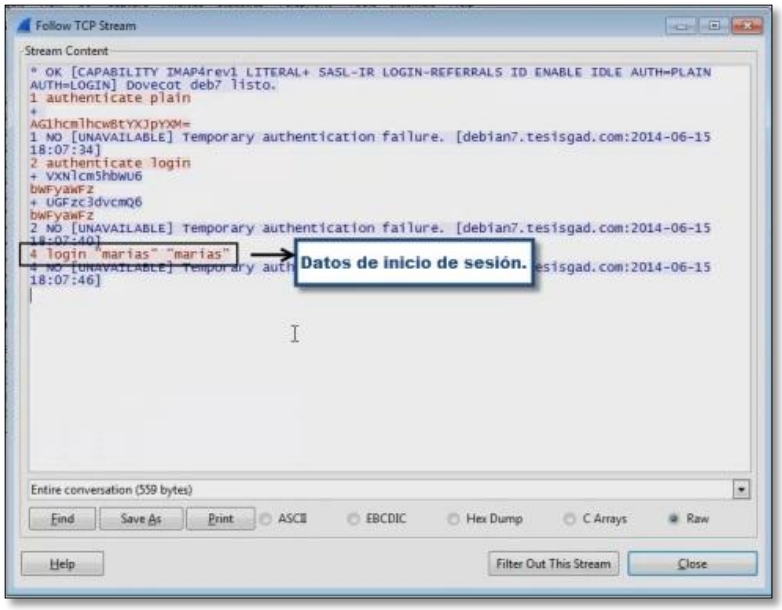



Figura 27: Wireshark vista detallada de flujo en ventana “Follow TCP Stream”

10. En este paso analizar otra trama del tráfico en la que se puede identificar la información y contenido de un mensaje cuando “Llega un mensaje”.

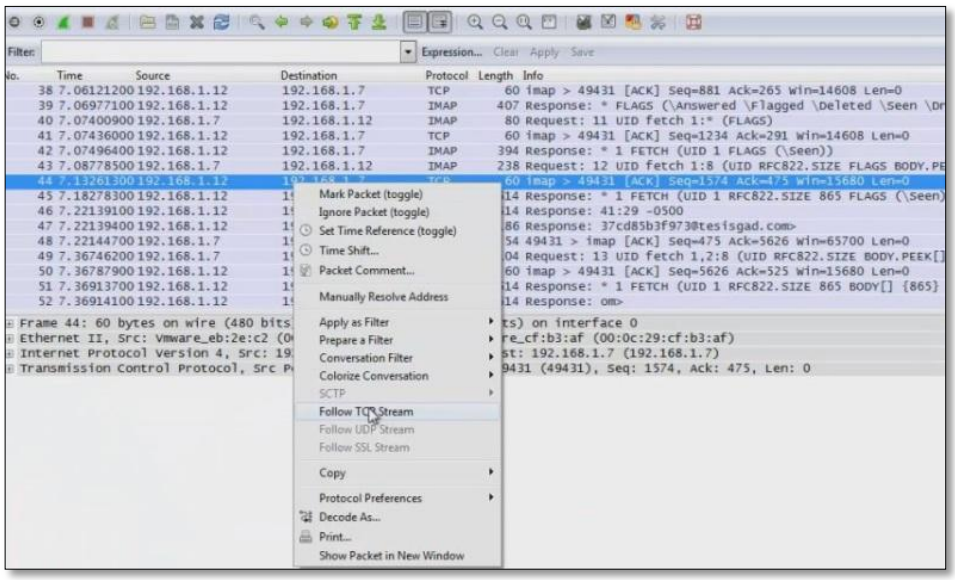



Figura 28: Wireshark datos obtenido de cliente ThunderBird, trama con información de mensaje recibido

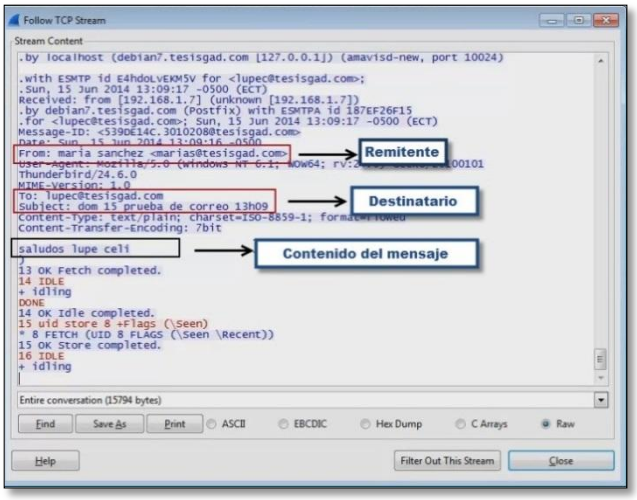



Figura 29: Wireshark vista detallada de flujo en ventana “Follow TCP Stream”, información y contenido de mensaje recibido

11. En este paso analizar otra trama del tráfico en la que se puede identificar la información y contenido de un mensaje cuando “Enviamos un mensaje”.

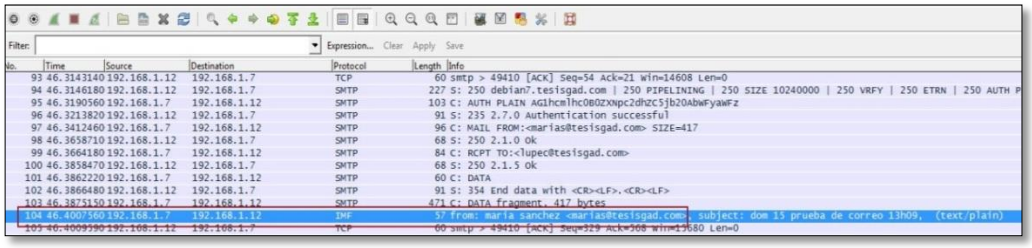


Figura 30: Wireshark trama analizada durante el proceso de envío de un mensaje

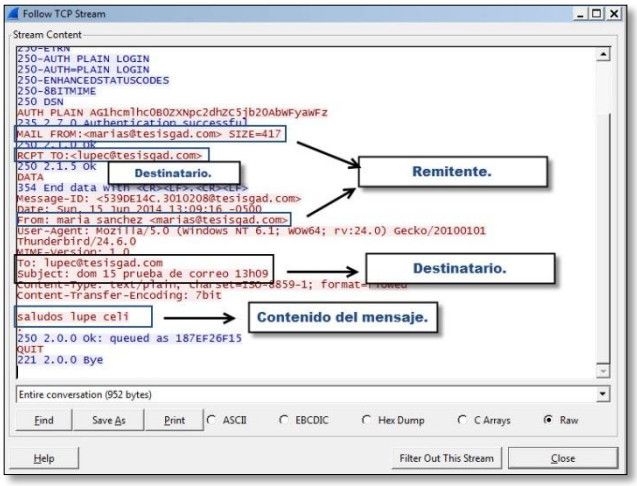



Figura 31: Wireshark vista detallada de flujo de ventana “Follow TCP Stream”, información y contenido de mensaje enviado

**Conclusiones:**

- La información importante relacionada a cada cuenta de correo puede ser interceptada, esto debido a que no existe un mecanismo de seguridad que brinde comunicaciones cifradas entre el servidor y el cliente.
- Si algún intruso mal intencionado tiene acceso al equipo del cliente e instala software del tipo keylogger, puede hacerse con la información de su cuenta en cualquier momento por falta de seguridad en las comunicaciones.
- Con ayuda del analizador de tráfico se pudo observar como viaja la información en texto plano y lo peligroso que esto puede resultar si al servicio que se accede no ofrece cifrado en sus conexiones.

**Recomendaciones:**

- No se debe acceder a servicios de correo que no brinden cifrado en sus conexiones, ya que se expone información personal a través de la red que se está conectado.
- Se recomienda siempre conectarse a servidores que ofrezcan seguridad SSL/TLS a lo referente al servicio de correo.
- Si debe conectarse a servicios de correo que no brinden mecanismos de seguridad, no lo haga desde un lugar público como: bibliotecas, parques, cafés, universidades; pues al conectarse a redes públicas expone a que intrusos en la red capturen su información valiosa para acceder a su correo y otros servicios personales.

**Prueba 2:** Análisis de servidor de correo Postfix, Dovecot y LDAP, comunicaciones cifradas mediante protocolo seguro TLS.

**Objetivo:**

- Analizar el flujo de datos de las conexiones cifradas entre cliente y servidor de correo.
- Indicar los beneficios que implica establecer comunicaciones seguras en este tipo de servicio.

**Actividades:**

1. Usar la herramienta wireshark en cliente o servidor para capturar el tráfico que genera la comunicación de prueba.

2. Establecer la comunicación por parte del usuario usando un cliente de correo como **thunderbird**, **icedove,** o similar.

3. Analizar el tráfico, identificar y señalar la información sensible que se obtuvo en los siguientes momentos: inicio de sesión, envío de correo, recepción de correo.

4. Visualizar la información sensible encontrada en el tráfico capturado con herramienta wireshark.

**Escenario:**

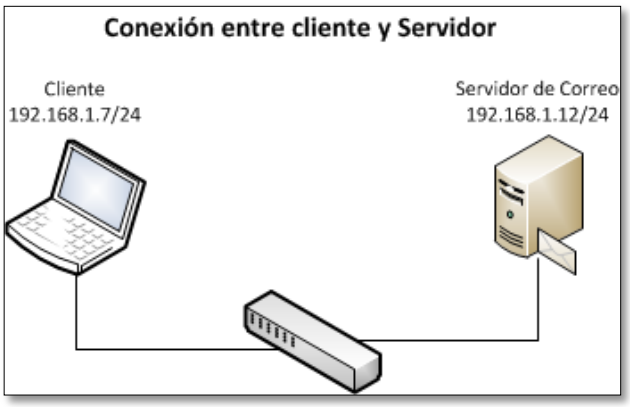



Figura 32: Escenario para análisis de comunicación entre cliente y servidor

**Aplicaciones utilizadas:**

Analizador de tráfico: **Wireshark**

Cliente de correo para escritorio: **Thunderbird**

**Pasos a seguir:**

1. Repetir los pasos 1 al 4 de la prueba 1, el procedimiento y las imágenes son las mismas hasta el punto 5 en el que la ventana indica que el tipo de conexión soporta cifrado mediante el uso de *"STARTTLS"*, figura 33.

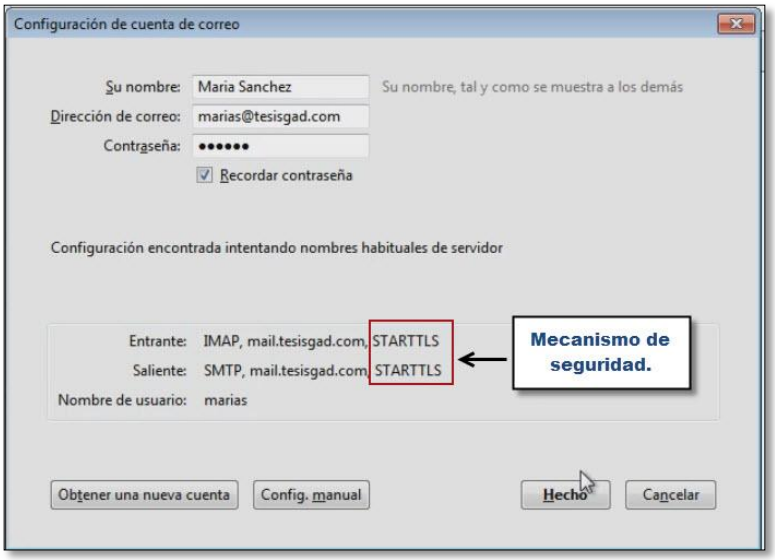



Figura 33: ThunderBird ventana de configuración de cuenta de correo indicando mecanismo STARTTLS

2. Luego cliquear en el botón “Hecho”, al cabo de unos segundos se presentara una ventana con información del certificado digital que se debe aceptar para establecer la comunicación segura.

   Detener el tráfico capturado por wireshark, y buscar de igual manera la cadena de texto referente al inicio de sesión de correo de usuario, en este caso solo se puede obtener la dirección de email, el resto de la comunicación viaja de manera cifrada, como se observa en la figura 34, de modo que no es legible como en el caso de la práctica 1 que todo viajaba en texto plano.

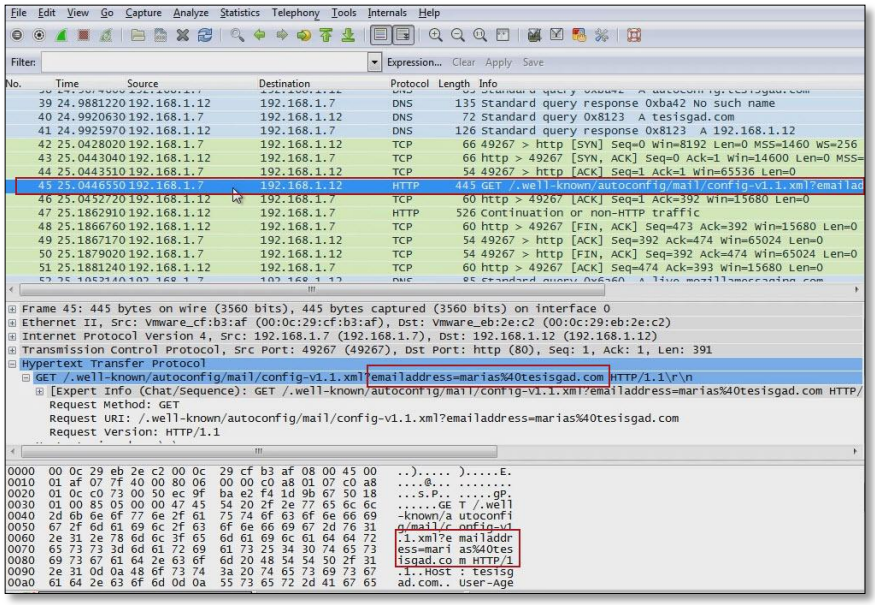



Figura 34: Wireshark tráfico capturado usando como cliente ThunderBird, seguridad TLS activa

3. Si se analiza otra trama del tráfico capturado, en este caso del proceso de envío de correo lo que se obtuvo el tráfico cifrado tal y como se aprecia en la figura 35; la información legible es concerniente al certificado digital que usa el servidor para emitir a sus clientes.

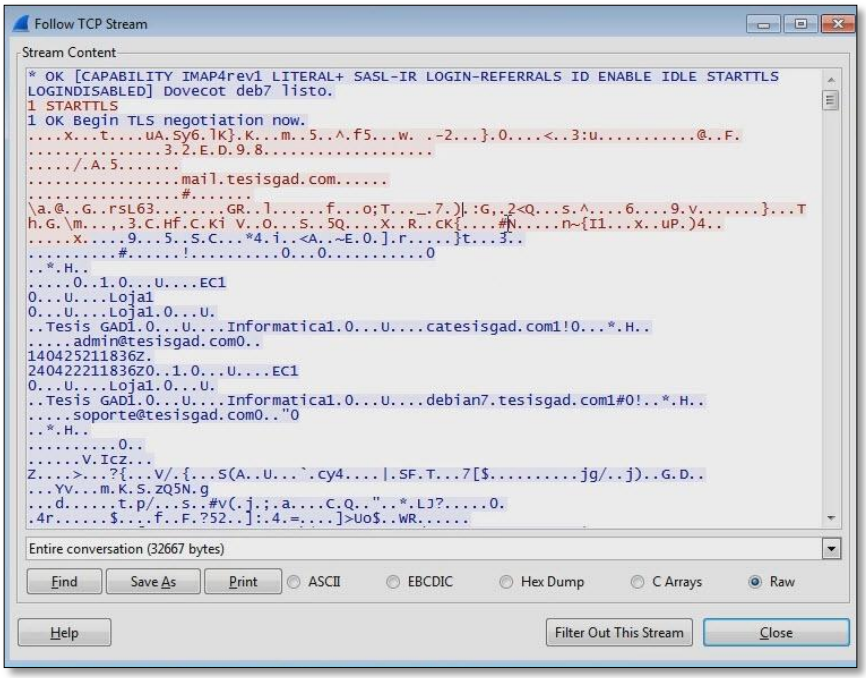



Figura 35: Wireshark tráfico capturado pruebas ThunderBird, seguridad TLS activada

**Conclusiones:**

- En esta práctica la única información sensible que se obtuvo mediante la captura de tráfico fue la dirección de email, esto cuando el usuario usa un cliente de correo como Thunderbird.
- La comunicación segura cifra la información importante para no hacerla legible a intrusos dentro de nuestra red.
- Es ventajoso y más seguro usar este tipo de conexiones para los usuarios.

**Recomendaciones:**

- Se recomienda configurar los servidores de acceso local y acceso al público para que brinden este tipo de comunicaciones y así no se vea comprometida la información de los usuarios que acceden a estos servicios.
- No debe usarse ningún tipo de servicio de correo sin estas configuraciones de seguridad, ya que se verificó, como información vital puede ser observada por intrusos en la red o en el mismo equipo.

**Prueba 3:** Análisis de servidor de correo Postfix, Dovecot y LDAP plataforma webmail, con roundcube, comunicaciones en texto plano (Sin TLS).

**Objetivo:**

- Analizar el flujo de datos en las comunicaciones realizadas entre cliente y servidor de correo cuando este no establece comunicaciones seguras.

**Actividades:**

1. Usar la herramienta wireshark en cliente o servidor para capturar el tráfico que genera la comunicación de prueba.
2. Establecer la comunicación por parte del usuario usando un navegador web y acceder al sitio roundcube.
3. Analizar el tráfico, identificar y señalar la información sensible que se obtuvo en los siguientes momentos: inicio de sesión, envío de correo, recepción de correo.

4. Visualizar la información sensible encontrada en el tráfico capturado con herramienta wireshark.

**Escenario:**

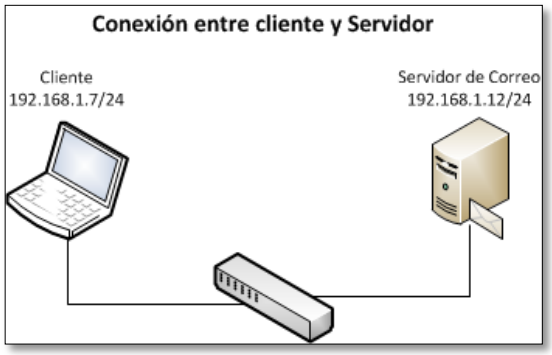



Figura 36: Escenario para análisis de comunicación entre cliente y servidor

**Aplicaciones utilizadas:**

Analizador de tráfico: **Wireshark**

Cliente de correo para escritorio: **Google Chrome**

**Pasos a seguir:**

1. Iniciar una captura de tráfico de la misma forma que las prácticas anteriores.

2. En el navegador web “Google Chrome”, ingresar a la dirección web del servicio de correo tal y como se observa en la figura 37 y proporcionar los datos de la cuenta para iniciar sesión.

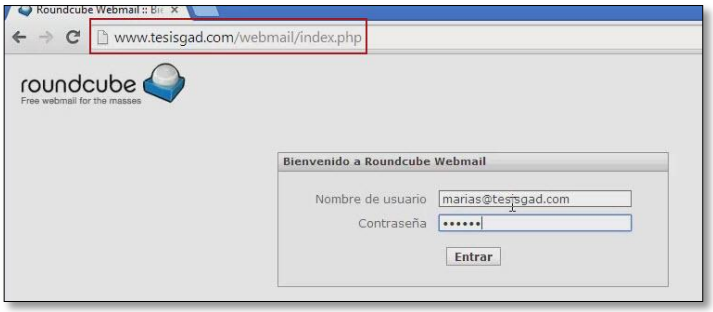



Figura 37: Google Chrome inicio de sesión en sitio sin protección SSL/TLS

3. Detener la captura de tráfico para su análisis, y buscar la cadena correspondiente al usuario ingresado en el navegador tal como se aprecia en la figura 38.

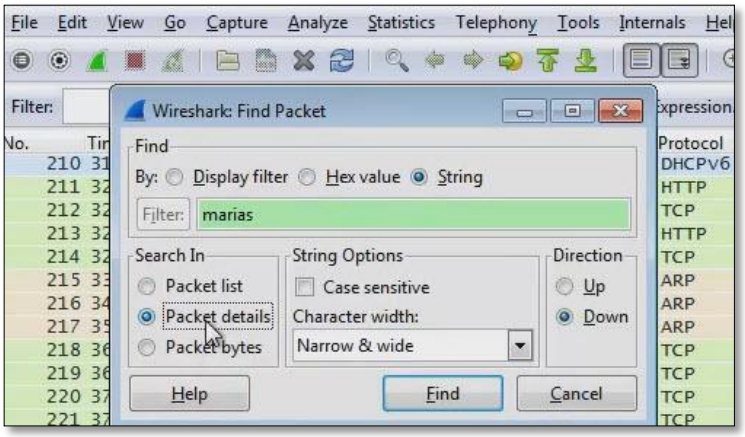



Figura 38: Wireshark tráfico de Google Chrome, búsqueda de cadena con nombre de usuario

4. La trama que se encontró con la cadena, se muestra en la figura 39, claramente se identifica los datos de email y contraseña.

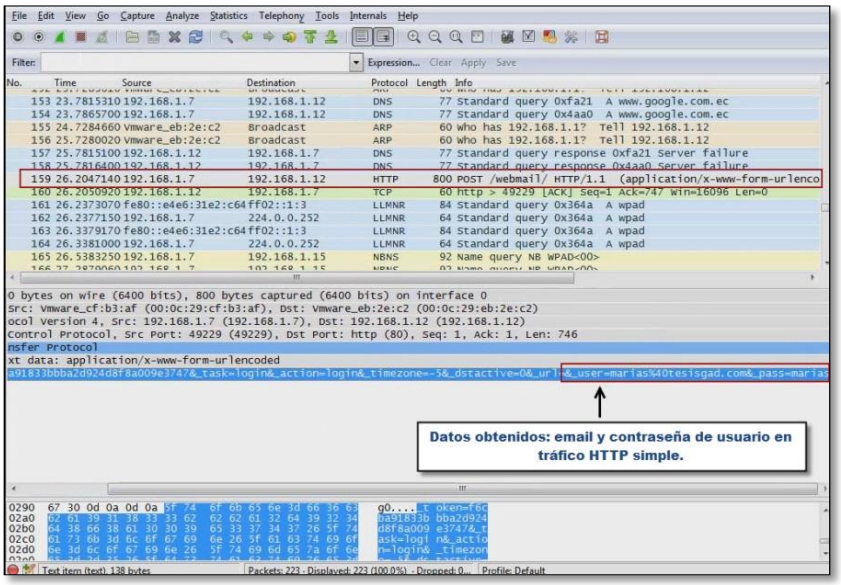



Figura 39: Wireshark tráfico de Google Chrome, trama encontrada con datos de inicio de sesión servidor sin SSL/TLS

5. Para observar de una forma más detallada abrir la ventana de seguimiento de flujo tcp, el resultado se observa en la figura 40.

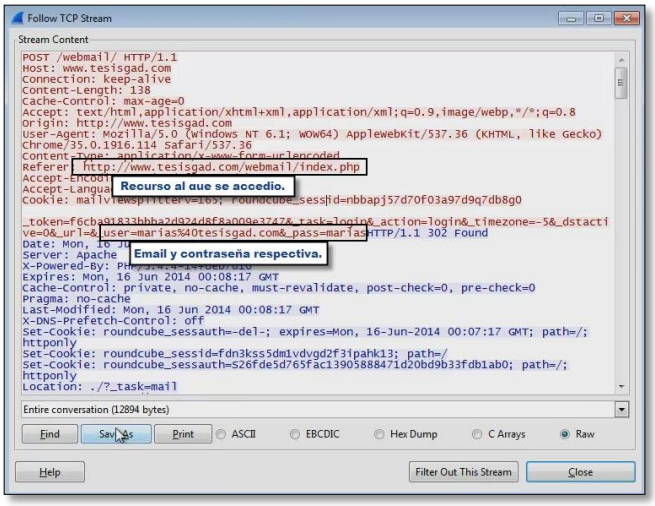



Figura 40: Wireshark tráfico de Google Chrome, inicio de sesión seguimiento de flujo tcp.

6. Enviar un mensaje desde la aplicación, figura 41.

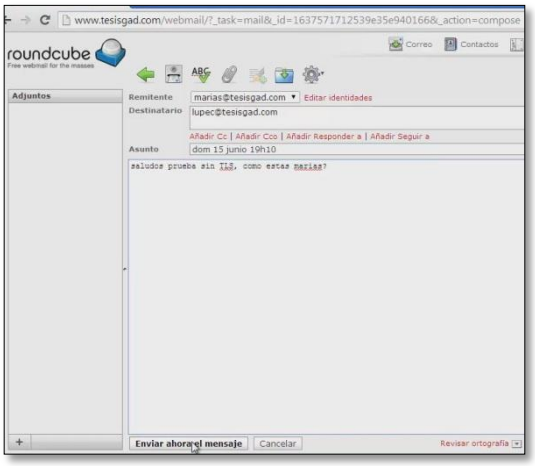



Figura 41: Google Chrome envío de mensaje en sitio sin protección SSL/TLS

7. Buscar la cadena de texto “marias”, el resultado se puede observar en la figura 42.

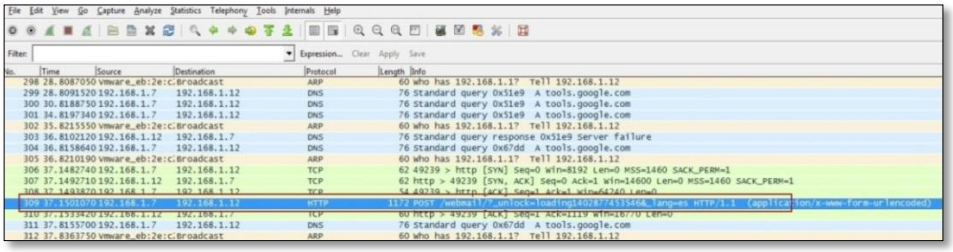


Figura 42: Wireshark captura de tráfico Google Chrome trama de envío de mensaje en conexión sin seguridad SSL/TLS

8. Abrir la ventana de seguimiento de flujo TCP, para ver el texto que se envió como mensaje, como se muestra en la figura 43.

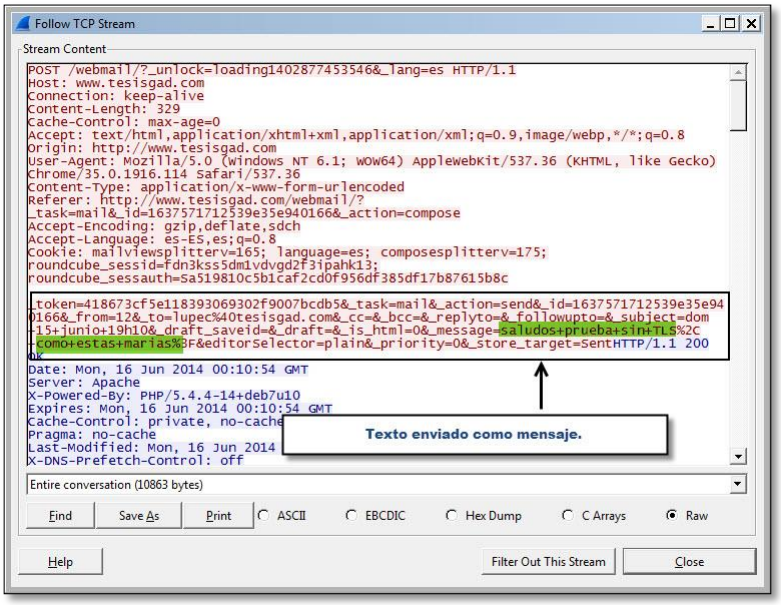



Figura 43: Wireshark captura de tráfico Google Chrome, seguimiento de flujo tcp de mensaje enviado en conexión sin seguridad SSL/TLS

**Conclusiones:**

- Usando el analizador de tráfico Wireshark se obtuvo información esencial de la cuenta de correo que se utilizó de ejemplo.
- Al momento que se ingresa a sitios web de correo electrónico sin seguridad SSL/TLS, la información de la cuenta de sesión puede ser capturada por intrusos en la red, e incluso pueden leer los mensajes.

**Recomendaciones:**

- Se debe evitar en lo posible el acceso a sitios web HTTP al menos se debe ingresar información personal en estos sitios ya que se demostró que la información personal como datos de una cuenta de correo viajan en texto plano y pueden ser interceptados.
- Se puede usar HTTP simple (sin cifrado) en sitios web que muestran todo tipo de contenido y esto no implique el ingreso de información sensible como el que es solicitado en transacciones electrónicas, compras en línea, o incluso en

aplicaciones web que sirven para administración de un servicio, ya que eso puede comprometer información de usuario o la administración de servidores como en el último ejemplo.

- Si accede a una red de acceso público como en parques, escuelas, universidades y otros lugares de bastante concurrencia y necesita ingresar a un sitio web realícelo usando el protocolo HTTPS como por ejemplo acceder a https://misitio.com ya que esto indica que sus comunicaciones establecen mecanismos de seguridad.

**Prueba 4:** Análisis de servidor de correo Postfix, Dovecot y LDAP plataforma webmail, con roundcube, tipo comunicaciones cifradas mediante protocolo seguro HTTPS

**Objetivo:**

- Analizar el flujo de datos de las conexiones cifradas entre cliente y servidor de correo.
- Indicar los beneficios que implica establecer comunicaciones seguras en este tipo de servicio.

**Actividades:**

1. Usar la herramienta wireshark en cliente o servidor para capturar el tráfico que genera la comunicación de prueba.
2. Establecer la comunicación por parte del usuario usando un navegador web y acceder al sitio roundcube**.**
3. Analizar el tráfico, identificar y señalar la información sensible que se obtuvo en los siguientes momentos: inicio de sesión, envío de correo, recepción de correo.
4. Visualizar la información sensible encontrada en el tráfico capturado con herramienta wireshark.

**Escenario:**

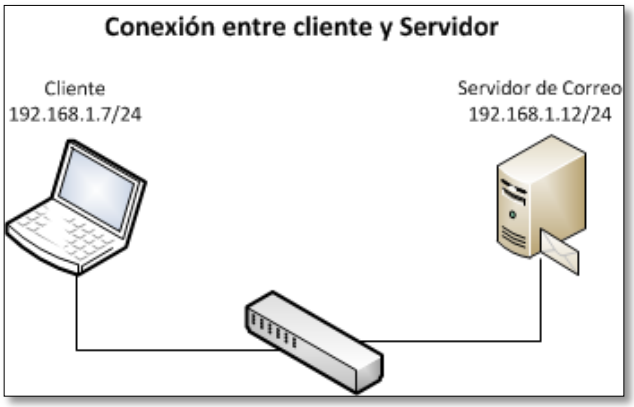



Figura 44: Escenario para análisis de comunicación entre cliente y servidor

**Aplicaciones utilizadas:**

Analizador de tráfico: **Wireshark**

Cliente de correo para escritorio: **Google Chrome**

**Pasos a seguir:**

1. Iniciar una captura de tráfico como se observó en las prácticas anteriores.

2. En el navegador web, ingresar a la dirección web del servicio de correo tal y como se observa en la figura 45, fíjese que aparece un candado verde indicando que se usa el protocolo HTTPS en el sitio, proporcione los datos de la cuenta para iniciar sesión.

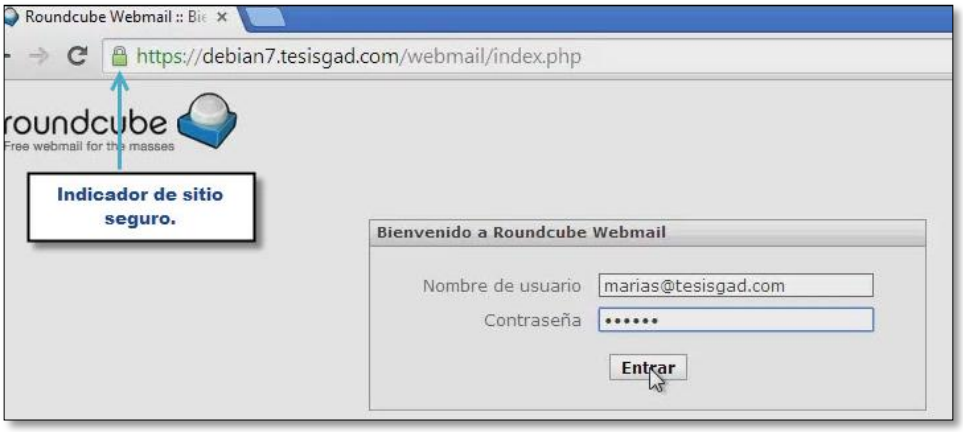



Figura 45: Google Chrome ventana de inicio de sesión a correo sitio seguro SSL/TLS

3. Seguir los mismos pasos que en la práctica 3.

   Al tratar de buscar la cadena de texto con nombre de usuario, no se encuentra ninguna coincidencia, esto se debe a la nueva configuración de servidor que usa HTTPS, la misma que somete a mecanismos de codificación a la información que se envía en sus comunicaciones, y al analizar dichas tramas en su forma más detallada es decir mediante un seguimiento de flujo tcp, se obtendrán los resultados como se muestra en la figura 46.

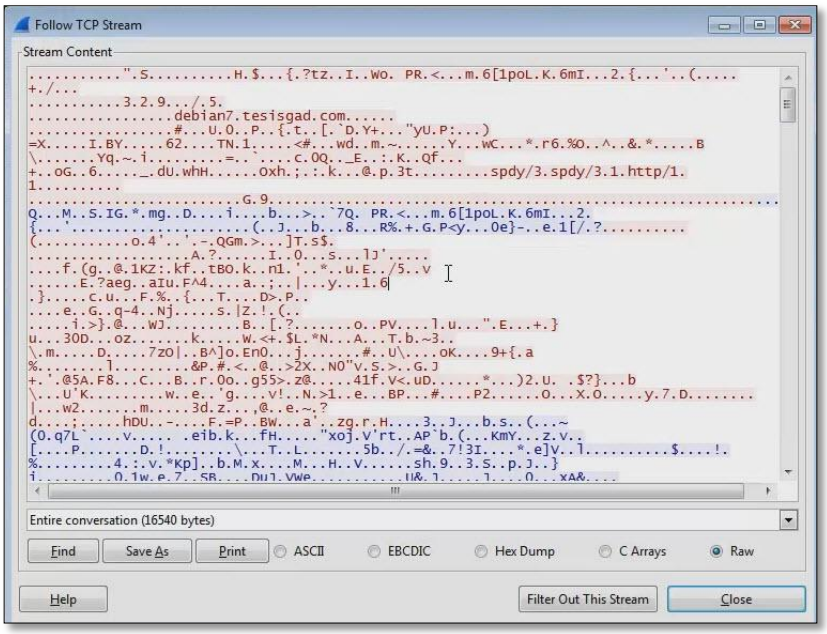



Figura 46: Wireshark tráfico capturado de Google Chrome, seguimiento de flujo tcp cuando se establece comunicaciones seguras SSL/TLS

No se adjunta más imágenes del tráfico generado, porque el análisis del resto de tramas mostrará resultados similares, es decir la información sensible está cifrada.

**Conclusiones:**

- El tráfico capturado con la herramienta wireshark, no permitió identificar información sensible a diferencia de la práctica 3, en la que la comunicación se la realizo cuando el servidor ofreció HTTP simple.

- El uso de protocolos seguros como HTTPS brindan un canal seguro de comunicación entre el cliente y el sitio web al que accede el usuario, por eso es más confiable usarlo para fines como transacciones electrónicas o enviar información de carácter confidencial.

- Los usuarios que acceden al servicio de correo pueden sentirse más tranquilos al usar el mismo, porque su información no será interceptada por intrusos que comparten la misma red o internet.

- La comunicación segura SSL/TLS provee cifrado a los datos que viajan por ésta, y debido a esto la información que se encontró no se ve en un formato fácilmente legible, por tanto es indispensable que al menos sitios que gestionan información crítica usen esta configuración en sus servidores.

**Recomendaciones:**

- Se recomienda configurar a los servidores web para que brinden comunicaciones HTTPS estrictamente si sus aplicaciones van a solicitar a sus usuarios datos personales críticos como información referente a tarjetas de crédito, compras en línea.

- Si utiliza una aplicación web de carácter administrativo, establezca las comunicaciones mediante HTTPS y si debe aplicar nuevas configuraciones tómese su tiempo y aplíquelas, pues al usar HTTP tradicional sus datos de inicio de sesión serán fácilmente interceptados por intrusos.

Cómo indicación general recuerde verificar que siempre que navegue por sitios web estos inicien por HTTPS, más aún si se trata de redes sociales, correo electrónico u otros sitios que soliciten información personal.

## 2. Prueba de conexión entre cliente – servidor utilizando IPSec

En esta sección se describe la prueba realizada al servicio de l2tp/ipsec, en cuanto al tráfico generado en una comunicación cliente – servidor.

**Prueba:** Análisis de Servidor VPN L2TP/IPSEC, Simulación de topología de red pública.

**Objetivo:**

- Analizar el flujo de datos en las comunicaciones realizadas entre cliente y servidor VPN cuando se establece una comunicación.

**Actividades:**

1. Establecer una conexión desde cliente Windows usando autenticación mediante certificado digital.

2. Analizar el tráfico, identificar el tráfico de la conexión VPN que fluye a través de las interfaces externas.

3. Utilizar el servicio de correo electrónico web, pues este servicio también está disponible en el servidor.

**Escenario:**

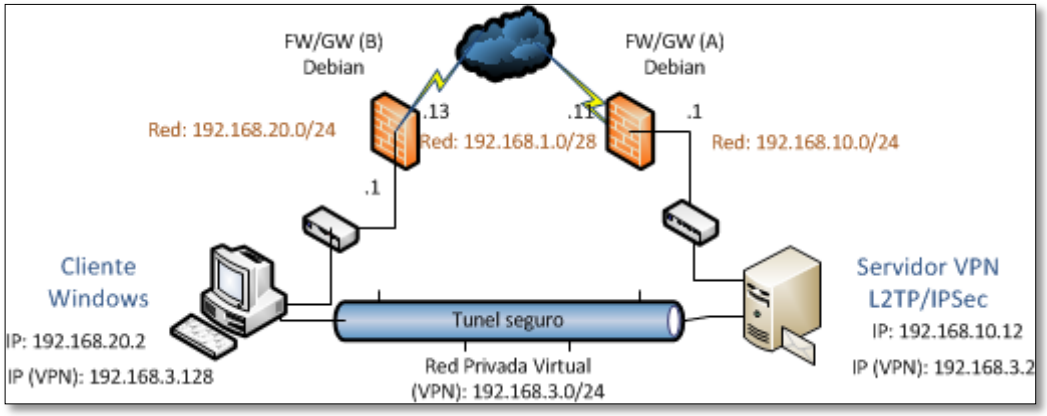



Figura 47: Escenario para análisis de comunicación entre cliente y servidor

TABLA XXX: DIRECCIONAMIENTO DE LA RED WAN PLANTEADA DE FORMA VIRTUAL

| **Servidor** | **IP Externa/Interfaz** | **IP Interna/Interfaz** |
|---|---|---|
| Gateway A | 192.168.1.11 (eth0) | 192.168.10.1 (eth1) |
| Gateway B | 192.168.1.13 (eth0) | 192.168.20.1 (eth1) |
| | | |
| **EQUIPOS PARTICIPANTES DE LA VPN** | | |
| **Equipo** | **IP Física** | **IP Virtual** |
| VPN IPSec | 192.168.10.12 | 192.168.3.2 |
| Windows 7 | 192.168.20.2 | 192.168.3.128 |

**Aplicaciones utilizadas:**

Analizador de tráfico: **Wireshark**

Navegador Web: **Google Chrome**

**Pasos a seguir:**

1. Seleccionar el perfil de conexión creado anteriormente, y cliquear en “Conectar”, debe apreciar una imagen como la figura 48.

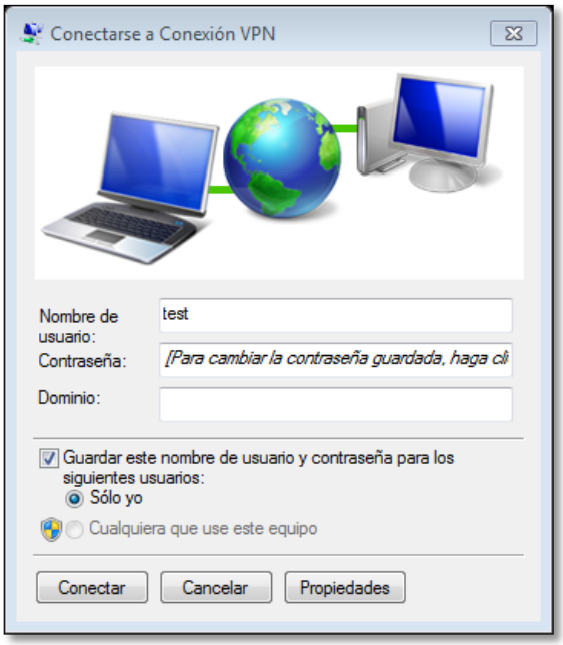



Figura 48: Ventana de perfil de conexión VPN creado

2. Cliquear en el botón “Conectar”, el proceso de conexión inicia tal como se muestra en la figura 49.

   **Nota:** El nombre de usuario y contraseña corresponden a ***“test”***.


Figura 49: Conectándose a Conexión VPN, IP Gateway A

3. Luego se realiza la comprobación del usuario y su contraseña, tal como se muestra en la figura 50.


Figura 50: Conectándose a Conexión VPN, comprobación de usuario y contraseña

4. Una vez conectado se puede ver el estado de la conexión, dando clic derecho en el perfil de conexión y eligiendo la opción “Estado”, como se muestra en la figura 51.


Figura 51: Seleccionando opción Estado para tener detalles de la conexión VPN

5. En la ventana de “Estado de conexión”, cliquear en el Menú “Detalles” esto muestra la información más destacada de la conexión.


Figura 52: Ventana Estado de Conexión VPN, vista del menú “Detalles”

6. Para obtener detalles mucho más minuciosos acerca del adaptador de red virtual, ejecutar en una terminal de Windows el comando ***"ipconfig /all"***, lo que dará como resultado información, que se muestra en la figura 53.

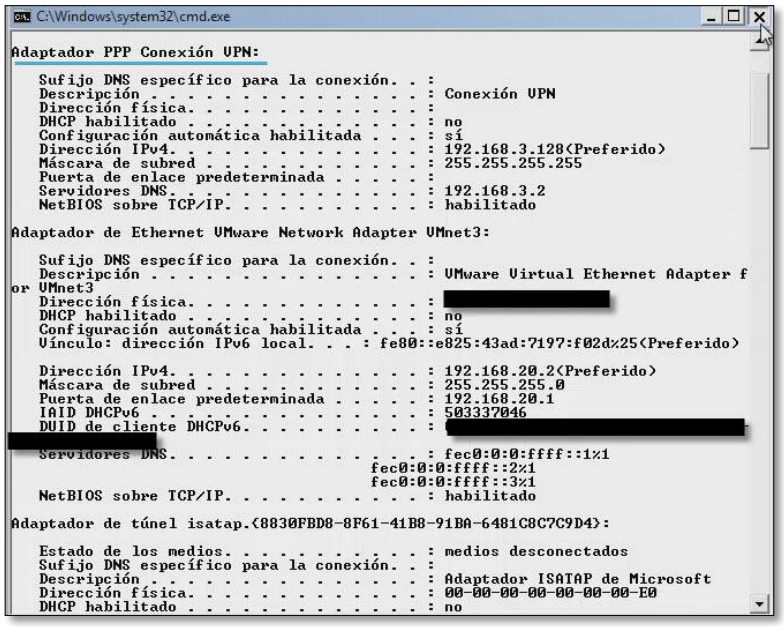



Figura 53: Detalles de direccionamiento obtenidos mediante el comando "ipconfig /all"

Como se observa en la imagen anterior se obtuvo información detallada del direccionamiento actual del equipo ejecutando Windows 7.

7. Ahora ingresar al sitio web del correo electrónico del servidor VPN, para ello usar Google Chrome y digitar la dirección del sitio ***"tesisgad.com"***, que presentara un mensaje como el que se muestra en la figura 54.


Figura 54: Google Chrome mensaje de petición mal realizada

Lo que se observa en la imagen es un mensaje de **"Petición mala"** e indica que se está tratando de acceder a un sitio web usando HTTP cuando este solo trabaja con peticiones HTTPS, esto es una medida que se adoptó para proteger el acceso a aplicaciones web y evitar la captura de información que viajaría en forma plana (legible) si se usa HTTP; para acceder al sitio basta con cliquear en el enlace que se sugiere con la etiqueta **Hint**.

8. Una vez que se accede al sitio web correcto se debe prestar especial atención al ícono de candado verde, recuadro de color verde en la figura 55, que indica conexión segura, esto se debe a que, al momento de importar el certificado personal, también importar el certificado de la Autoridad Certificadora y está fue quien emitió todos los certificados que intervienen en esta práctica.

   Para continuar con la actividad de la práctica ingresar una de las cuentas de correo existentes.


Figura 55: Sitio web de la aplicación de correo disponible en el servidor VPN

En la siguiente imagen se evidencia que el acceso a la aplicación web alojada en el servidor VPN ha sido un éxito, figura 56 y se puede trabajar en ella como si se tratase de una conexión tradicional de equipos pertenecientes al mismo segmento de red, pero con el beneficio de encapsulamiento y protección de la información brindado por el Servicio L2TP/IPSec.

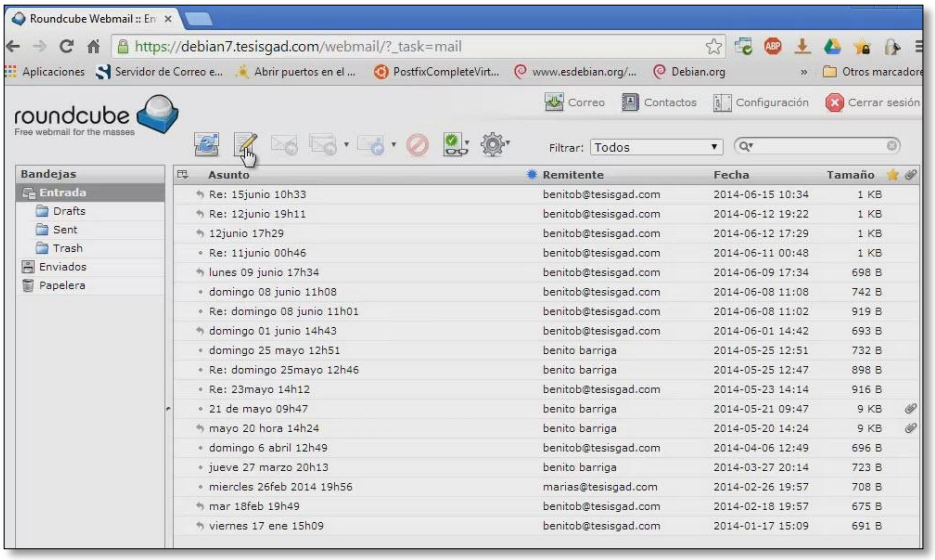



Figura 56: Cuenta de correo electrónico accedida a través de la VPN

9. Para observar cómo está viajando los datos a través de la comunicación se realizó una breve captura de tráfico y se observa como IPSec encapsula la información mediante el protocolo ESP. Esta captura de tráfico se la realizó desde Windows obteniendo los paquetes de la interfaz física del equipo, como se aprecia en la figura 57, no sé distingue que tipo de peticiones de servicio se está solicitando porque todo está encapsulado y solo los extremos de la comunicación pueden negociar está información una vez que se establece el túnel de la VPN.

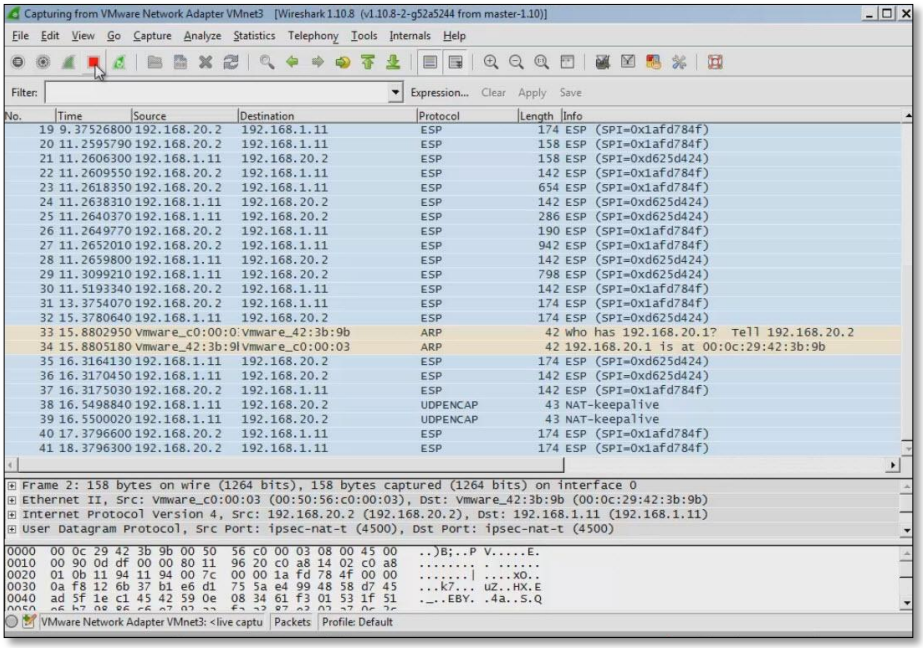



Figura 57: Captura de tráfico con la interfaz física desde el cliente VPN Windows 7

10. Además el la figura 58, se puede observar el flujo de datos de la conexión.

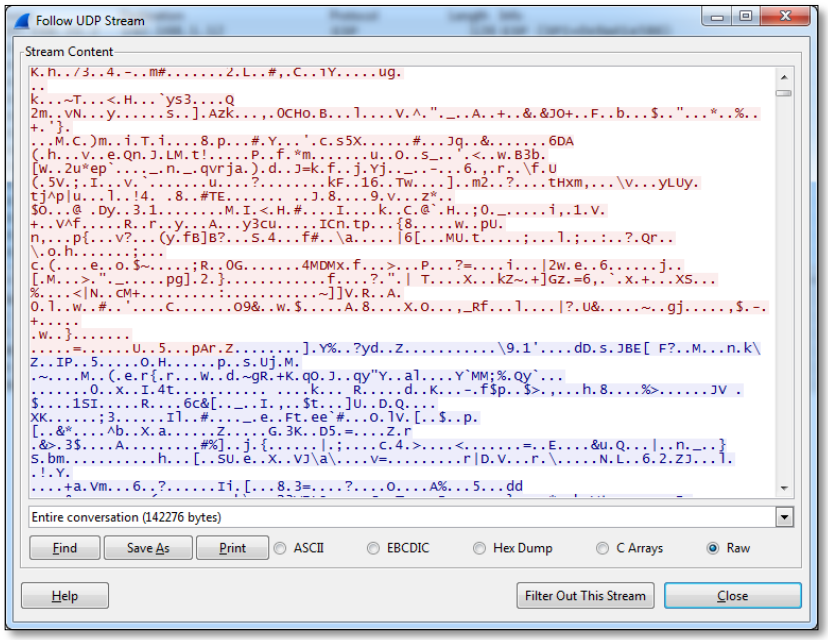



Figura 58: Flujo udp de conexión l2tp/ipsec

**Conclusiones:**

- La herramienta wireshark muestra el tipo de encapsulado generado por la implementación de la vpn l2tp/ipsec, donde se observa el tráfico identificado como ESP, que es el protocolo que maneja ipsec.

- A diferencia de OpenVPN se observó que la implementación de la VPN l2tp/ipsec necesita de un mayor conocimiento, ya que requiere de una configuración más compleja entre los equipos participantes.

- A diferencia de OpenVPN la solución aquí propuesta realiza dos tipos de autenticación, siendo la primera la validación de los equipos, mientras que la segunda corresponde a la validación de los usuarios.

- La solución propuesta se adapta a las necesidades de la Institución, puesto que se está utilizando una vpn host a host con terminales Windows.

## 3. Prueba de monitoreo de los servicios del equipo remoto.

En este apartado, se realiza una prueba a la herramienta de monitoreo Nagios, para comprobar si registra el estado de los servicios monitoreados y envía las notificaciones si alguno de los servicios fallase o cambiase de estado.

**Prueba:** Monitorear el estado de los servicios públicos del servidor de correo.

**Objetivo:**

- Comprobar que nagios registra las actividades de los servicios en tiempo real, y si alguno de estos fallan son notificados al usuario correspondiente.

**Actividades:**

1. Provocar el cambio de estado en alguno de los servicios que nagios monitorea.
2. Determinar si nagios registra el cambio de estado de cualquiera de los servicios públicos.
3. Verificar que las notificaciones llegan al destinatario, luego de que un servicio cambie de estado al que no sea “OK”.

**Escenario:**

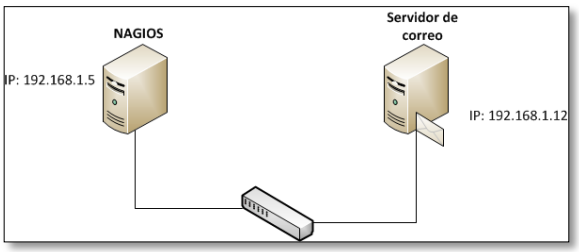



Figura 59: Escenario de prueba del monitoreo de los servicios

**Pasosa seguir:**

Para este ejemplo se utiliza como equipo de pruebas el servidor de correo (configurado anteriormente), pues posee servicios como ldap, dovecot, postfix, ssh, etc.

1. Al comienzo de la práctica los estados se encuentran en “OK”, como se observa en la figura 60.

| | | | | | | |
|---|---|---|---|---|---|---|
| servidor_correo | APACHE 443 | OK | 08-12-2014 12:07:33 | 0d 1h 22m 51s | 1/3 | OK 0.053641 seconds response time. Idle 0, busy 0, open slots 1 |
| | APACHE 80 | OK | 08-12-2014 12:07:10 | 0d 1h 22m 49s | 1/3 | TCP OK - 0.003 second response time on 192.168.1.12 port 80 |
| | PING | OK | 08-12-2014 12:02:55 | 0d 6h 55m 28s | 1/3 | PING OK - Packet loss = 0%, RTA = 0.70 ms |
| | imap | OK | 08-12-2014 12:07:50 | 0d 3h 21m 32s | 1/3 | IMAP OK - 0.020 second response time on 192.168.1.12 port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot deb7 listo.] |
| | ldap 389 | OK | 08-12-2014 12:07:50 | 0d 4h 4m 3s | 1/3 | TCP OK - 0.007 second response time on 192.168.1.12 port 389 |
| | pop3 | OK | 08-12-2014 12:07:37 | 0d 3h 21m 24s | 1/3 | POP OK - 0.024 second response time on 192.168.1.12 port 110 [+OK Dovecot deb7 listo.] |
| | servicio ssh | OK | 08-12-2014 12:07:47 | 0d 0h 0m 14s | 1/3 | SSH OK - OpenSSH_6.0p1 Debian-4 (protocol 2.0) |
| | smtp simple | OK | 08-12-2014 12:07:26 | 0d 4h 3m 32s | 1/3 | SMTP OK - 0.006 sec. response time |
| | url smtp | OK | 08-12-2014 12:07:10 | 0d 4h 3m 49s | 1/3 | SMTP OK - 0.010 sec. response time |

Figura 60: Estado de los servicios del servidor_correo

2. En el equipo remoto (servidor_correo), detener el servicio de ssh, y comprobar que nagios lo registra.

   **# /etc/init.d/ssh stop**, para detener el servicio.

3. Revisar el log del mail ***"mail.log"*** en el servidor, para comprovar que la notificacion se envía al destinatario indicado, el la figura 1, se muestra el log del envió del correo

```
Aug 12 12:02:47 debian postfix/pickup[33073]: 696A426BF: uid=1001 from=<nagios>
Aug 12 12:02:47 debian postfix/cleanup[33486]: 696A426BF: message-id=<20140812170247.696A426BF@debian.localdomain>
Aug 12 12:02:47 debian postfix/qmgr[33074]: 696A426BF: from=<nagios@debian.localdomain>, size=593, nrcpt=1 (queue active)
Aug 12 12:02:47 debian postfix/smtp[33488]: warning: database /etc/postfix/sasl/passwd.db is older than source file /etc/postfix/sasl/passwd
Aug 12 12:02:47 debian postfix/smtp[33488]: 696A426BF: to=<panchog@tesisgad.com>, relay=mail.tesisgad.com[192.168.1.12]:25, delay=0.16, delays=0.11/0.
03/0.01/0.02, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 7D5E326F0F)
Aug 12 12:02:47 debian postfix/qmgr[33074]: 696A426BF: removed
```

Figura 61: Envío del correo desde el log

4. Ingresar a la cuenta de correo y como se muestra en la figura 62, el correo que nagios envía al destinatario.

| | | | |
|---|---|---|---|
| " PROBLEM Service Alert: debian7.tesisgad.com/servicio ssh is CRITICAL " | nagios@debian.localdomain | Hoy 12:02 | 896 B |
| "prueba | root@debian.localdomain | Hoy 11:47 | 719 B |
| "prueba | root@debian.localdomain | Hoy 11:34 | 751 B |
| "prueba | root@debian.localdomain | Hoy 11:26 | 730 B |

Figura 62: Correo enviado al destinatario

5. Al abrir el mensaje, se puede observar cual el la causa de la advertencia, como se muestra en la figura 63.

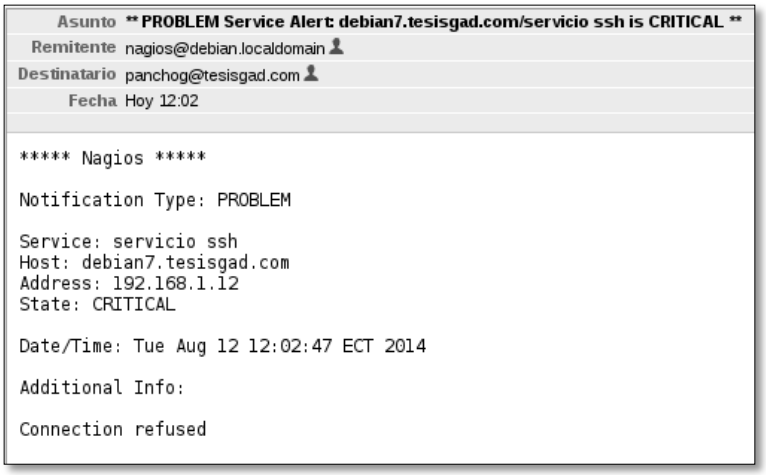



Figura 63: Información del mensaje enviado desde nagios

6. Iniciar el servicio ssh.

   **# /etc/init.d/ssh start**

7. Revisar el log del mail, para verificar que la notificación se envió al usuario, como se muestra en la figura 64.


Figura 64: Log del mail, del envío de la notificación

8. Al revisar la cuenta de correo, se observa un nuevo correo que nagios envió, como se observa en la figura 65, luego de que el estado del servicio cambió.


Figura 65: Envío de correo al destinatario

Como se indicó en los pasos anteriores, cada vez que el estado de un servicio cambie, nagios lo registra e inmediatamente envía la notificación al destinatario correspondiente.

## Fase 4: Implantación de la solución.

El proceso de llevar a cabo las configuraciones descritas en la fase 3 e incorporarlas al sistema de producción, es una labor a cargo del administrador de la red.

### 1. Servidor de Correo.

Las configuraciones para el servicio de correo seguro es algo que actualmente no se encuentra en producción debido a que el servicio web debe permanecer activo las 24 horas del día, lo que impide un reinicio para que el servicio aplique las nuevas configuraciones, por lo tanto estas se aplicaron a un servidor de pruebas dentro de la institución, esto para analizar los cambios y desempeño antes de pasar a ser implantados en los servicios correspondientes.

Los cambios que se realizaron para activar el soporte TLS sobre el servicio de correo son los siguientes haciendo hincapié en los archivos que se deben modificar para conseguir el propósito:

### 1.1 Creación de certificados digitales y certificado de la autoridad de certificación local con openssl v1.0.1e.

Se deben crear la llave privada y pública para el CA local, en la figura 66 se muestra el proceso de creación:

```
root@debian7:~/CA# openssl req -new -x509 -days 3650 -config /root/CA/tesisgad.cnf -keyout /root/CA/private/cate
sisgad.com.key -out /root/CA/catesisgad.com.pem
Generating a 4096 bit RSA private key
.............................................................++
...............++
writing new private key to '/root/CA/private/catesisgad.com.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [EC]:
State or Province Name (full name) [Loja]:
Locality Name (eg, city) [Loja]:
Organization Name (eg, company) [Tesis GAD]:
Organizational Unit Name (eg, section) [Informatica]:
Common Name (e.g. server FQDN or YOUR name) []:catesisgad.com
Email Address []:admin@tesisgad.com
root@debian7:~/CA#
```

Figura 66: Creación del certificado de autoridad de certificación (CA)

Una vez creado el CA, se tiene que crear el certificado que identificará el servidor de correo, para ello se crear una llave privada para el servidor con el comando que se

muestra en la figura 67, el nombre utilizado para identificar el certificado será *“tesisgad.com”*.

```
root@debian7:~/CA# openssl genrsa -des3 -out tesisgad.com.key 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................
.....................................................................
```

Figura 67: Creación de clave privada de certificado para servidor de correo

Crear una petición de firma de certificado, la figura 68 indica el comando para crear un archivo CSR, el cual contendrá previamente la información de la organización que está destinada al certificado del servidor, el archivo debe ser enviado al servidor CA para que este lo revise y si cree conveniente lo firme.

```
root@debian7:~/CA# openssl req -new -key tesisgad.com.key -out tesisgad.com.csr -config tesisgad.cnf
Enter pass phrase for tesisgad.com.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [EC]:
State or Province Name (full name) [Loja]:
Locality Name (eg, city) [Loja]:
Organization Name (eg, company) [Tesis GAD]:
Organizational Unit Name (eg, section) [Informatica]:
Common Name (e.g. server FQDN or YOUR name) []:debian7.tesisgad.com
Email Address []:soporte@tesisgad.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:tesisgadpass
An optional company_name []:tesisgad
```

Figura 68: Creación de archivo de petición de certificado para enviar a CA

EL administrador de CA revisara la petición de certificado ingresando el comando que se muestra en la figura 69.

```
root@debian7:~/CA# openssl req -in /root/CA/tesisgad.com.csr -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=EC, ST=Loja, L=Loja, O=Tesis GAD, OU=Informatica, CN=d
e@tesisgad.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

Figura 69: Fragmento de texto de la petición de certificado de servidor examinado por la CA

El administrador de la CA ingresa el comando que se observa en la figura 70, para generar el certificado digital solicitado por el servidor en base al archivo de petición

recibido. Antes de firmar se recomienda verificar que la información del certificado sea la auténtica, de ser así presionar la tecla *"y"*, para firmar el certificado.

```
root@debian7:~/CA# openssl ca -config /root/CA/tesisgad.cnf -in /root/CA/tesisgad.com.csr -verbose
Using configuration from /root/CA/tesisgad.cnf
Enter pass phrase for /root/CA/private/catesisgad.com.key:
0 entries loaded from the database
generating index
message digest is sha1
policy is policy_match
next serial number is 01
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=EC, ST=Loja, L=Loja, O=Tesis GAD, OU=Informatica, CN=debian7.tesisgad.com/emailAddress=soport
e@tesisgad.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:ef:56:d4:49:63:7a:c3:0f:cd:0d:5a:f1:0b:c9:
                    da:3e:80:8d:d2:3f:7b:81:1e:fa:56:2f:1c:7b:db:
                    c8:1b:53:28:41:a7:fa:55:93:ec:86:60:cc:63:79:
                    34:9b:93:cd:1a:7c:05:53:46:84:54:10:ee:8f:37:
                    5b:24:9f:86:d4:f2:1a:a7:f5:d1:87:94:6a:67:2f:
                    b1:db:6a:29:c9:11:47:94:44:93:ea:0a:9c:b6:0b:
                    59:76:ed:de:80:6d:a1:4b:ad:53:92:7a:51:35:4e:
                    b3:67:0a:8d:b7:b8:64:8b:85:17:b5:f3:0e:74:7f:
Check that the request matches the signature
Signature ok
The subject name appears to be ok, checking data base for clashes
Everything appears to be ok, creating and signing the certificate
Successfully added extensions from config
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Apr 25 21:18:36 2014 GMT
            Not After : Apr 22 21:18:36 2024 GMT
        Subject:
            countryName               = EC
            stateOrProvinceName       = Loja
            organizationName          = Tesis GAD
            organizationalUnitName    = Informatica
            commonName                = debian7.tesisgad.com
            emailAddress              = soporte@tesisgad.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                5D:01:64:09:C5:1E:35:5C:B1:AE:D8:A4:0B:5E:1D:E7:15:4E:C2:20
            X509v3 Authority Key Identifier:
                keyid:A8:49:19:2D:D5:F7:09:42:E5:73:EA:F3:AD:04:3B:7D:88:47:B1:4E

Certificate is to be certified until Apr 22 21:18:36 2024 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]
```

Figura 70: Firma de la petición y generación de certificado digital

Se debe seguir un procedimiento similar a la creación del certificado para el servidor de correo, pero en este caso para la creación del certificado de usuario, ingresando la sentencia:

***# openssl req -new -nodes -out benito-req.pem -keyout benito-key.pem -days 365 -config tesisgad.cnf***, con esta línea se crea la llave privada y la petición de firma de certificado para el usuario.

***# openssl ca –out benito-cert.pem –days 365 –config tesisgad.cnf –infile benito-req.pem***, mientras que esta línea permite al CA generar y firmar el certificado para el usuario "benito".

## 1.2 Configuración de un sistema de nombres de dominio (tesisgad.com) con bind9 v9.8.4.

Se deben configurar las zonas de autoridad o dominio a usar en la red, para eso editar el archivo ***named.conf.local***.

La resolución directa estará determinado por el nombre de la zona, para este caso será el nombre ***tesisgad.com***, para la segunda zona (resolución inversa) misma que traduce direcciones IP en nombres de red, aquí colocar la IP correspondiente en forma inversa, omitiendo el último dígito.

En la figura 71, dentro de este fichero se añade dos zonas la primera para la resolución directa, mientras que la segunda será para la resolución inversa.

db.tesisgad.com (como superusuario)

Archivo Editar Buscar Opciones Ayuda

```
1  ; BIND zone file for db.tesisgad
2  ;
3  ;$ORIGIN tesisgad.com.
4  $TTL 86400      ;1 día
5  @               IN      SOA     debian7.tesisgad.com.    soporte.tesisgad.com. (
6                          2013072701      ; serial
7                          7200            ; refresh
8                          3600            ; retry
9                          604800          ; expire
10                         86400 )         ; minimum
11 ;
12                 IN      NS      debian7
13                 MX      10      mail            ; Primary mail exchanger
14 debian7         A       192.168.1.12
15
16 mail                    A       192.168.1.12
17 tesisgad.com.           A       192.168.1.12
```

Figura 71: Servicios en la zona de resolución directa

El archivo de resolución inversa tendrá el nombre **db.1.168.192**, las primeras líneas serán igual que el archivo anterior modificando tanto el **SOA** como el **NS**.

El aspecto clave de este archivo será en no utilizar registros A, como fue el caso anterior, en cambio se utilizará **direcciones PTR** que permita resolver las direcciones IP en nombres de dominio, tal como lo muestra la figura 72, nótese que el primer registro coincide con el propio servidor DNS.

```
db.1.168.192 (como superusuario)
Archivo  Editar  Buscar  Opciones  Ayuda
1  ;
2  ; BIND zone file for 192.168.1.xxx
3  ;
4
5  $TTL    3D
6  @       IN      SOA     debian7.tesisgad.com.    soporte.tesisgad.com. (
7                          2013072701      ; serial
8                          8H              ; refresh
9                          2H              ; retry
10                         4W              ; expire
11                         1D )            ; minimum
12 ;
13                 NS      debian7.tesisgad.com.    ; Nameserver address
14 12              PTR     debian7.tesisgad.com.
```

Figura 72: Resolución inversa

Ahora se tienen que configurar servidor DNS para que redirija las peticiones que no pueda resolver, a otro DNS. El archivo a modificar es ***named.conf.options*** y en la sección ***forwarders***, colocar los DNS, en este caso las direcciones ip de los DNS de Google, como se muestra en la figura 73.

```
1  options {
2          directory "/var/cache/bind";
3          version "Welcome";
4
5          // If there is a firewall between you and nameservers you want
6          // to talk to, you may need to fix the firewall to allow multiple
7          // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
8
9          // If your ISP provided one or more IP addresses for stable
10         // nameservers, you probably want to use them as forwarders.
11         // Uncomment the following block, and insert the addresses replacing
12         // the all-0's placeholder.
13
14         forwarders {
15                 8.8.8.8;
16                 8.8.4.4;
17         };
18         listen-on port 53 { 127.0.0.1; 192.168.1.12;};
19         allow-query { 127.0.0.1; 192.168.1.0/24;};
20         allow-recursion { 127.0.0.1; 192.168.1.0/24;};
```

Figura 73: Servidor DNS de Google

## 1.3 Configuración de Sldapd v2.4.31 para activar soporte TLS.

Como ya se tiene creado los certificados, se procede a crear un fichero de texto con extensión ldif en el que se indica los certificados digitales que usara el servicio, el archivo será ***olcSSL.ldif*** y su contenido se muestra en figura 74.

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certificados/ca.crt
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/certificados/tesisgad.com.key
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certificados/tesisgad.com.crt
```

Figura 74: Contenido de archivo olcSSL.ldif

Para importar estas líneas de configuración ejecutar el siguiente comando:

**# ldapmodify -Y EXTERNAL -H ldapi:/// -f ./olcSSL.ldif**

El resultado se muestra en la figura 75.

```
root@debian7:/home/cristian# ldapmodify -Y EXTERNAL -H ldapi:/// -f ./olcSSL.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"

root@debian7:/home/cristian#
```

Figura 75: Líneas importadas al archivo olcSSL.ldif

## 1.4 Gestión de cuentas de correo virtuales con phamm v.0.5.18.

Instalar el paquete phamm e ingresar al sitio web de la aplicación para descargar los *schemas* que se muestran dentro del recuadro rojo de la figura 76, que serán utilizados en la aplicación.

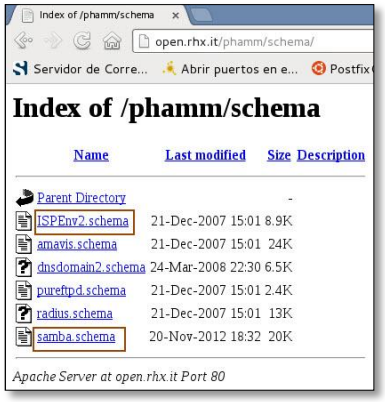



Figura 76: Phamm schemas en sitio web de la aplicación

Descargar los archivos, copiarlos a la ruta de archivos schema del paquete slapd como se muestra en la figura 77.

```
~/temp/phamm_schemas# cp ISPEnv2.schema /etc/ldap/schema/ISPEnv2.schema
~/temp/phamm_schemas# cp samba.schema /etc/ldap/schema/samba.schema
```

Figura 77: Copia de archivos schema a la carpeta schema del servicio LDAP

Para usar estos esquemas en la nueva configuración del servidor ldap, convertir estos archivos al formato ldif, el que permite hacer cambios en la configuración en caliente, es decir sin tener que reiniciar el servicio para que las modificaciones se apliquen.

Crear un archivo denominado ***"test.conf"*** con el contenido que se muestra en la figura 78.

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/phamm.schema
include         /etc/ldap/schema/samba.schema
include         /etc/ldap/schema/ISPEnv2.schema
include         /etc/ldap/schema/amavis.schema
```

Figura 78: Contenido del archivo test.conf

Crear un directorio para alojar los archivos en el nuevo formato (ldif) y luego ingresar los comandos que se muestran en la figura 79, para la conversión de formato, en la primera línea se crea un directorio temporal, mientras que la segunda línea se aplica la conversión.

```
root@deb7p4vm:~/temp/phamm_schemas# mkdir /tmp/slapd.d/
root@deb7p4vm:~/temp/phamm_schemas# slaptest -f test.conf -F /tmp/slapd.d/
config file testing succeeded
```

Figura 79: Uso de comando slaptest para la conversión de archivos schema a ldif

Copiar los archivos ldif almacenados en la carpeta temporal hacia el directorio correspondiente ldap, como se muestra en la figura 80.

```
root@deb7p4vm:~/temp/phamm_schemas# cp /tmp/slapd.d/cn\=config/cn\=schema/cn\=\{4\}phamm.ldif /etc/ldap/slapd.d/
cn\=config/cn\=schema/cn\=\{4\}phamm.ldif
root@deb7p4vm:~/temp/phamm_schemas# cp /tmp/slapd.d/cn\=config/cn\=schema/cn\=\{5\}samba.ldif /etc/ldap/slapd.d/
cn\=config/cn\=schema/cn\=\{5\}samba.ldif
root@deb7p4vm:~/temp/phamm_schemas# cp /tmp/slapd.d/cn\=config/cn\=schema/cn\=\{6\}ispenv2.ldif /etc/ldap/slapd.
d/cn\=config/cn\=schema/cn\=\{6\}ispenv2.ldif
root@deb7p4vm:~/temp/phamm_schemas# cp /tmp/slapd.d/cn\=config/cn\=schema/cn\=\{7\}amavis.ldif /etc/ldap/slapd.d
/cn\=config/cn\=schema/cn\=\{7\}amavis.ldif
```

Figura 80: Copiado de archivos ldif al directorio correspondiente LDAP

Verificar que los archivos ldif copiados tengan como propietario al usuario openldap (usuario asociado al servicio ldap) de no ser así, cambiar el propietario de estos archivos, para evitar errores al tratar de añadir información al directorio ldap. Para ello usar el comando "*chown*" tal como se muestra en la figura 81 y comprobar listando el directorio en cuestión.

```
root@deb7p4vm:/etc/phamm# ls -lash /etc/ldap/slapd.d/cn\=config/cn\=schema
total 88K
4,0K drwxr-x--- 2 openldap openldap 4,0K feb  6 13:13 .
4,0K drwxr-x--- 3 openldap openldap 4,0K feb  5 21:15 ..
 16K -rw------- 1 openldap openldap  16K feb  5 21:15 cn={0}core.ldif
 12K -rw------- 1 openldap openldap  12K feb  5 21:15 cn={1}cosine.ldif
8,0K -rw------- 1 openldap openldap 6,4K feb  5 21:15 cn={2}nis.ldif
4,0K -rw------- 1 openldap openldap 2,9K feb  5 21:15 cn={3}inetorgperson.ldif
8,0K -rw------- 1 root     root     7,9K feb  6 13:11 cn={4}phamm.ldif
 12K -rw------- 1 root     root      12K feb  6 13:11 cn={5}samba.ldif
8,0K -rw------- 1 root     root     7,9K feb  6 13:12 cn={6}ispenv2.ldif
 12K -rw------- 1 root     root     8,2K feb  6 13:13 cn={7}amavis.ldif
root@deb7p4vm:/etc/phamm# chown -R openldap:openldap /etc/ldap/slapd.d/cn\=config/cn\=schema
root@deb7p4vm:/etc/phamm# ls -lash /etc/ldap/slapd.d/cn\=config/cn\=schema
total 88K
4,0K drwxr-x--- 2 openldap openldap 4,0K feb  6 13:13 .
4,0K drwxr-x--- 3 openldap openldap 4,0K feb  5 21:15 ..
 16K -rw------- 1 openldap openldap  16K feb  5 21:15 cn={0}core.ldif
 12K -rw------- 1 openldap openldap  12K feb  5 21:15 cn={1}cosine.ldif
8,0K -rw------- 1 openldap openldap 6,4K feb  5 21:15 cn={2}nis.ldif
4,0K -rw------- 1 openldap openldap 2,9K feb  5 21:15 cn={3}inetorgperson.ldif
8,0K -rw------- 1 openldap openldap 7,9K feb  6 13:11 cn={4}phamm.ldif
 12K -rw------- 1 openldap openldap  12K feb  6 13:11 cn={5}samba.ldif
8,0K -rw------- 1 openldap openldap 7,9K feb  6 13:12 cn={6}ispenv2.ldif
 12K -rw------- 1 openldap openldap 8,2K feb  6 13:13 cn={7}amavis.ldif
root@deb7p4vm:/etc/phamm#
```

Figura 81: Asignación de propietario para archivos ldif copiados recientemente

Reiniciar el servicio slapd para que los cambios surtan efecto y el servicio pueda usar los archivos copiados recientemente.

En este momento ya se puede configurar el archivo principal de la interfaz web de la aplicación phamm, para ello abrir el archivo ***"/etc/phamm/config.php"***.

Verificar que la información de nombre distinguido sea la correcta de nuestro equipo, figura 82.

```
46 // The container
47 define ('SUFFIX','dc=tesisgad,dc=com');
48
49 // The admin bind dn (could be rootdn)
50 define ('BINDDN','cn=admin,dc=tesisgad,dc=com');
51
52 // The Phamm container
53 define ('LDAP_BASE','o=hosting,dc=tesisgad,dc=com');
```

Figura 82: Información de nombre distinguido en config.php

Ubicar la sección de encriptación y cambiar a MD5, como se muestra en la figura 83.

```
175 // Standard LDAP encryption type [CRYPT,MD5,CLEAR]
176 //define ('ENC_TYPE','CRYPT');
177 define ('ENC_TYPE','MD5');
```

Figura 83: Fijando tipo de encriptación LDAP  estándar en config.php

Guardar los cambios realizados en el archivo, luego desde el navegador ingresar a la interfaz web de la aplicación, como se observa en la figura 84, a continuación, acceder como usuario *admin*, el que permite la creación de los dominios, cuentas de correo y tareas administrativas de la aplicación.


Figura 84: Pantalla de acceso web a la aplicación phamm

Una vez iniciado sesión, crear un dominio en la sección correspondiente que se muestra en el recuadro rojo de la figura 85, este se agregara al directorio LDAP del servidor. Ingresar el nombre y cliquear en ***"Add new domain"***.

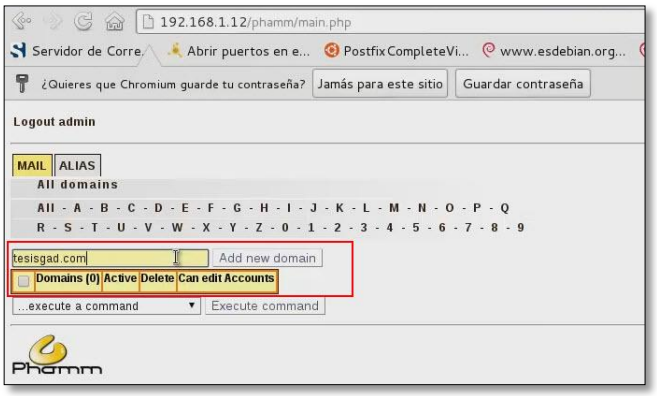



Figura 85: Agregando nuevo dominio al directorio LDAP en Phamm

En la siguiente ventana ingresar una contraseña, como se muestra en la figura 86, para asociarla al dominio creado recientemente, y cliquear en el botón ***"Add new domain"***.


Figura 86: Ingreso de contraseña para dominio creado en Phamm

Para crear cuentas de correo pertenecientes al dominio creado, cliquear en el nombre de dominio correspondiente, como se muestra en la figura 87.

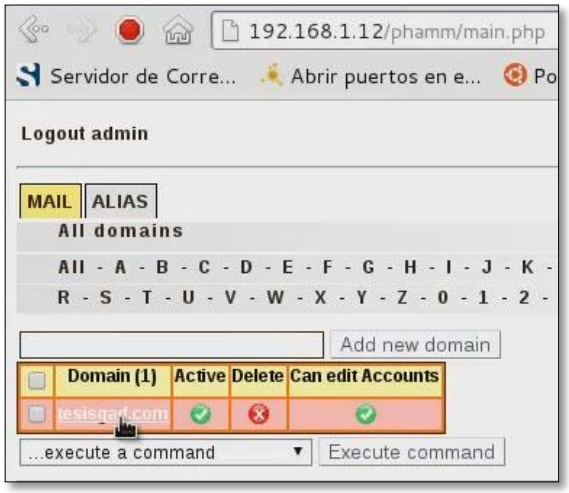



Figura 87: Listado de dominios creados en Phamm

Ingresar el nombre de la cuenta, como se muestra en la figura 88, se crea la cuenta ***"user2"***, no es necesario completar @dominio.com, y cliquear en ***"Add new account"***.


Figura 88: Agregando nueva cuenta de correo en Phamm

En la siguiente ventana, ingresar los datos de la cuenta en los campos correspondientes, figura 89, en los datos de la sección **MAIL**, escoger el valor "YES", para finalizar cliquear en ***"Add new account"***.


Figura 89: Configuración de una nueva cuenta de correo en Phamm

La nueva cuenta creada debe constar en el listado de cuentas del dominio. De esta manera se pueden crear las cuentas necesarias para el dominio tesisgad.com.

## 1.5 Activación del soporte TLS sobre el servicio de postfix v2.9.6.

En esta sección se indica las líneas que se deben de agregar en el archivo principal de postfix ***"/etc/postfix/main.cf"***, la parte esencial para configura el soporte TLS se indica en la sección *"Sección de parámetros TLS"*, en estas líneas se activa el soporte TLS y se cargan los archivos correspondientes del certificado digital para el servicio de correo, como se muestra en el figura 90.

La sección correspondiente a *"Configuración de Postfix para trabajar con usuarios virtuales LDAP"*, se encuentra el archivo principal *"ldap-aliases.cf"* que permite conectar a postfix con LDAP leyendo los parámetros básicos para establecer la comunicación, como se muestra en la figura 90.

El contenido del archivo *"/etc/postfix/ldap-aliases.cf",* será el siguiente:

```
server_host = localhost
search_base = dc=tesisgad,dc=com
start_tls = yes
version = 3
```

La sección correspondiente a *"Seccion para usuarios virtuales LDAP"*, en donde se detallan parámetros para indicar al servicio postfix que va a gestionar cuentas virtuales de correo, almacenadas en el directorio LDAP.

Para validar estas cuentas postfix debe hacer uso del archivo “”/etc/postfix/ldap-users.cf”, cuyo contenido es el siguiente:

```
server_host = localhost
search_base = dc=tesisgad,dc=com
version = 3
query_filter = (&(objectClass=VirtualMailAccount)(accountActive=TRUE)(mail=%u@%d))
result_attribute= mailbox
result_format = %sMaildir/
```

```
####Configuración de Postfix para trabajar con cuentas virtuales LDAP
myhostname = debian7.tesisgad.com
alias_maps = hash:/etc/aliases, ldap:/etc/postfix/ldap-aliases.cf
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = localhost
mynetworks = 127.0.0.0/8, 192.168.1.0/24
home_mailbox = Maildir/

####Sección de parámetros TLS####
#En esta sección se especifica los parámetros para establecer comunicaciones TLS (conexiones #cifradas)
smtpd_tls_cert_file=/etc/ssl/certificados/tesisgad.com.crt
smtpd_tls_key_file=/etc/ssl/certificados/tesisgad.com.key
smtpd_use_tls=yes
#smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache
#smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_scache

##Sección para usuario virtuales ldap
virtual_mailbox_base = /home/vmail/domains
virtual_mailbox_maps = ldap:/etc/postfix/ldap-users.cf
virtual_mailbox_domains = tesisgad.com
virtual_minimum_uid = 100
virtual_uid_maps = static:5000
virtual_gid_maps = static:5000
virtual_transport = virtual

##Sección para interactuar con SASL
#smtpd_sasl_local_domain = tesisgad.com
#smtpd_sasl_auth_enable = yes
#smtpd_sasl_security_options = noanonymous,noactive
#smtpd_sasl_type = dovecot
#smtpd_sasl_path = private/auth
#broken_sasl_auth_clients = yes

#Visualización de registros logs de Postfix
debug_peer_list=tesisgad.com
debug_peer_level=2
```

Figura 90: Extracto de archivo “/etc/postfix/main.cf” todas las líneas que fueron modificadas

**NOTA:** Crear un usuario en el sistema para que tanto Postfix como Dovecot utilicen este usuario para gestionar comunicación entre ambos servicios. Crear el usuario vmail con valor 5000 para usuario id y grupo id, con los siguientes comandos. Este usuario será el encargado de leer el correo desde el servidor:

```
# groupadd -g 5000 vmail
# useradd -g vmail -u 5000 vmail -d /home/vmail
# mkdir -p /home/vmail
# chown -R vmail.vmail /home/vmail
```

## 1.6 Instalación y configuración del agente de entrega de correo dovecot v2.1.7.

El paquete dovecot es el que facilita al usuario acceder al correo desde el servidor y visualizarlo en su computador, mediante los protocolos IMAP o POP3.

**Editar el archivo: "/etc/dovecot/dovecot.conf"**

Habilitar los protocolos instalados en el caso de que la línea esté comentada: !include_try /usr/share/dovecot/protocols.d/*.protocol

Indicar los protocolos que utilizara Dovecot: protocols = imap pop3

Agregar el siguiente bloque de sentencia para indicar que la base de datos para contraseñas se administra mediante el controlador ldap y los argumentos o parámetros los leerá del archivo: */etc/dovecot/dovecot-ldap.conf.ext*

```
passdb {
driver = ldap
args = /etc/dovecot/dovecot-ldap.conf.ext
  }

userdb {
driver = prefetch
  }

userdb {
driver = ldap
args = /etc/dovecot/dovecot-ldap.conf.ext
  }
```

En donde ***prefetch, userdb*** puede ser usado para combinar búsquedas *passdb* y *userdb* dentro de una sola búsqueda. Es usualmente utilizado por SQL, LDAP y base de datos del tipo checkpassword.

**Editar el archivo: "/etc/dovecot/conf.d/10-auth.conf"**

No desactivar la autenticación por texto plano: disable_plaintext_auth = no

Configurar como mecanismos de autenticación lo siguiente: auth_mechanisms = plain login

Configurar el mecanismo de autenticación mediante ldap, des comentar la línea: *"!include auth-ldap.conf.ext"*, y dejar comentado el resto de líneas de la sección que se muestra en la figura 91.

```
#!include auth-deny.conf.ext
#!include auth-master.conf.ext
#!include auth-system.conf.ext
#!include auth-sql.conf.ext
!include auth-ldap.conf.ext
#!include auth-passwdfile.conf.ext
#!include auth-checkpassword.conf.ext
#!include auth-vpopmail.conf.ext
#!include auth-static.conf.ext
```

Figura 91: Sección de autenticación de dovecot

**Editar el archivo: "/etc/dovecot/conf.d/10-mail.conf"**

En este archivo configurar la variable correspondiente a la localización de correo de la siguiente manera: mail_location = maildir:/home/vmail/domains/%d/%n/Maildir/

Dentro de la variable anterior se tiene dos parámetros especiales que son:

**%d**, hace referencia a la parte del dominio usado en la dirección de correo.

**%n**, hace referencia solo a la parte correspondiente a usuario en la dirección de correo.

Reemplazando con un ejemplo práctico se tendría que el buzón para el usuario user1@tesisgad.com, se ubicaría en: /home/vmail/domains/tesisgad.com/user1/Maildir/

Indicar el valor numérico de grupo y de usuario encargado de gestionar los buzones.

```
mail_uid = 5000
mail_gid = 5000
```

**Editar el archivo: "/etc/dovecot/conf.d/10-master.conf"**

En este archivo especificar los protocolos y los puertos de escucha que estos utilizaran, en nuestra configuración habilitar imap para funcionar mediante TLS, la sección a modificar quedaría como se muestra a continuación:

```
service imap-login {
inet_listener imap {
port = 143
```

```
    }
inet_listener imaps {
#port = 993
#ssl = yes
    }
```

También se crea la configuración necesaria de socket para permitir la autenticación SASL configurada en postfix usando dovecot.

```
unix_listener /var/spool/postfix/private/auth {
group = postfix
mode = 0660
user = postfix
 }
```

**Editar el archivo: "/etc/dovecot/conf.d/10-ssl.conf"**

En este archivo configurar los parámetros relacionados con el soporte para SSL/TLS.

Adicionalmente si se posee el certificado digital de nuestra autoridad certificadora (emisora de nuestro certificado) se debe añadir la ruta donde está almacenado.

```
ssl = required
ssl_cert = </etc/ssl/certificados/tesisgad.com.crt
ssl_key = </etc/ssl/certificados/tesisgad.com.key
ssl_ca = /etc/ssl/certificados/ca.crt
```

**Editar el archivo: "/etc/dovecot/conf.d/10-logging.conf"**

Este archivo está destinado a configurar los *logs* que serán generados según las necesidades que se especifiquen en el mismo.

Indicar el archivo de registro de errores para dovecot: log_path = /var/log/dovecot.log

Indicar el archivo de registro de carácter solo informativo: info_log_path = /var/log/dovecot.info

Indicar el archivo que contendrá registro de depuración: debug_log_path = /var/log/dovecot/dovecotdebug.log

Configurar que el proceso de autenticación sea detallado: auth_verbose = yes

Para tener más detalles sobre el proceso de autenticación también activar la depuración: auth_debug = yes

Habilitar la depuración para los procesos de correo: mail_debug = yes

Mostrar errores de nivel en protocolo SSL: verbose_ssl = yes

**Editar el archivo: "/etc/dovecot/conf.d/auth-ldap.conf.ext"**

En este archivo se específica el conector que se usara para base de datos de usuarios y el archivo del cual se leerá la respectivas configuraciones de conexiones.

```
passdb {
driver = ldap
args = /etc/dovecot/dovecot-ldap.conf.ext
}
```

**Editar el archivo: "/etc/dovecot/dovecot-ldap.conf.ext"**

Indicar el equipo servidor de ldap al que se va a conectar.

```
hosts = localhost
uris = ldap://localhost
```

Indicar el nombre distinguido (DN) del usuario que se conectara al servidor ldap.

```
dn = cn=admin,dc=tesisgad,dc=com
```

Indicar la contraseña del usuario indicado anteriormente:

```
dnpass = admin
```

Indicar la ruta del certificado de la autoridad certificadora (en caso de poseerlo).

```
tls_ca_cert_file = /etc/ssl/certificados/ca.crt
tls_ca_cert_dir = /etc/ssl/certificados/
```

Activar la autenticación enlazada para verificar la validación de contraseñas, esto lo realiza con los datos del usuario que se indicó en pasos anteriores.

```
auth_bind = yes
```

Se indica también el tipo de objeto que se buscara del directorio LDAP en formato (DN).

```
auth_bind_userdn =mail=%u,vd=%d,o=hosting,dc=tesisgad,dc=com
```

Configurar la versión 3 del protocolo LDAP.

```
ldap_version = 3
```

Especificar el directorio base de configuración LDAP, a partir de este nodo raíz realizará la búsqueda hacia los nodos extremos.

```
base = dc=tesisgad, dc=com
```

Fijar que el alcance de la búsqueda sea hacia los subárboles.

```
scope = subtree
```

Especificar el filtro de búsqueda para usuarios de la siguiente manera:

```
user_filter = (&(objectClass=VirtualMailAccount)(accountActive=TRUE)(mail=%u))
```

Especificar el filtro de búsqueda para contraseñas de la siguiente manera:

```
pass_filter = (&(objectClass=VirtualMailAccount)(accountActive=TRUE)(mail=%u))
```

Indicar el esquema de contraseñas a usar por defecto, guardar los cambios realizados

```
default_pass_scheme = MD5
```

## 1.7 Configuración de apache v2.2.22 para conexiones SSL.

Básicamente esta configuración se refiere al uso de los certificados digitales previamente creados para el uso del servidor de correo. Para hacer uso esta configuración seguir los siguientes pasos:

a. Ubicarse en el directorio de apache donde se almacenan los archivos de sitios web que se desea habilitar ***/etc/apache2/sites-enabled*** y deshabilitar el sitio SSL por defecto con el comando:
   # **a2dissite default-ssl**, tal como se observa en la figura 92.

```
root@debian7:/etc/apache2/sites-enabled# a2dissite default-ssl
Site default-ssl disabled.
To activate the new configuration, you need to run:
  service apache2 reload
```

Figura 92: Deshabilitar sitio SSL por defecto

b. Ahora ubicarse en el directorio ***/etc/apache2/sites_available*** y realizar una copia del archivo ***default-ssl***, con un nombre relacionado al sitio que se quiere habilitar, para nuestro caso debian7.tesisgad.com, el resultado se muestra en la figura 93.

```
root@debian7:/etc/apache2/sites-available# cp default-ssl www.tesisgad.com
root@debian7:/etc/apache2/sites-available# ls
default  default-ssl  default-ssl.orig  www.tesisgad.com
root@debian7:/etc/apache2/sites-available# mv www.tesisgad.com debian7.tesisgad.com
```

Figura 93: Generando archivo de configuración para nuevo sitio SSL

c. Editar el archivo anteriormente creado y modificar las siguientes líneas:

**ServerName = debian7.tesisgad.com**, ingresar la url con la que se accederá al sitio.

**ServerAlias = www.tesisgad.com**, ingresar un alias de url, con la que también se puede acceder al sitio.

**SSLEngine on**, si se deja como está, activa el motor SSL.

**SSLCertificateFile = /etc/ssl/certificados/tesisgad.com.crt**

**SSLCertificateKeyFile = /etc/ssl/certificados/tesisgad.com.key**, las líneas anteriores especifican la ruta del certificado digital y su clave pública.

**SSLCACertificatePath = /etc/ssl/certificados/**

**SSLCACertificateFile = /etc/ssl/certificados/ca.crt**, las variables anteriores indica tanto la ruta y el archivo del certificado digital correspondiente a la autoridad de certificación CA privada.

**SSLCARevocationPath = /etc/ssl/certificados/**

**SSLCARevocationFile = /etc/ssl/certificados/crl.pem**, estas dos variables indican tanto la ruta y el archivo correspondiente a la lista de revocación de certificados.

**SSLRequireSSL**, Esta variable se usa dentro de una sección directory, indica que para acceder al recurso o directorio indicado se debe ingresar por https, por ejemplo en ***"/var/www/"***, con se muestra en la figura 94:

```
<Directory /var/www/>
    Options Indexes +FollowSymLinks Includes ExecCGI
    AllowOverride None
    Order allow,deny
    allow from all
    SSLRequireSSL
</Directory>
```

Figura 94: Uso de la sentencia SSLRequireSSL

`SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire`, en donde:

**FakeBasicAuth:** Permite utilizar los métodos estándar Auth/DBMAuth para controlar el acceso.

**ExportCertData:** Exporta las variables de entorno SSL_CLIENT_CERT y SSL_SERVER_CERT, que contienen en formato PEM los certificados del servidor y del cliente si se usa autenticación del cliente.

**StrictRequire:** Cuando se usa también con SSLRequireSSL forzar el uso de conexiones seguras.

Guardar los cambios realizados en el archivo debian7.tesisgad.com

d. Habilitar el nuevo sitio modificado anteriormente con el comando:

# **a2ensite debian7.tesisgad.com**, la figura 95 muestra el resultado de tal comando:

```
root@debian7:/etc/apache2/sites-available# a2ensite debian7.tesisgad.com
Enabling site debian7.tesisgad.com.
To activate the new configuration, you need to run:
  service apache2 reload
```

Figura 95: Activación del nuevo sitio SSL

e. Editar el archivo ***ports.conf***, se encuentra en la ruta ***/etc/apache2/***, en donde se agrega la configuración referente a los puertos de escucha del servicio, modificando las siguientes líneas:

**NameVirtualHost *:443**, esta línea por defecto esta comentada, dejarla así para que utilice cualquier dirección ip que posea el servidor, solo por

cuestiones de tratarse de un entorno controlado (es recomendable indicar la ip específica).

**Listen 443**, se coloca el puerto de escucha en la figura 96 se muestra lo indicado anteriormente.

```
<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to change
    # the VirtualHost statement in /etc/apache2/sites-available/default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently not
    # supported by MSIE on Windows XP.
    Listen 443
</IfModule>
```

Figura 96: Configurando puerto de escucha para el sitio seguro

f. Por último solo se tiene que habilitar el módulo ssl de apache, usando el siguiente comando; para aplicar los cambios reiniciar el servicio de apache

# **a2enmod ssl**, la figura 97 muestra el resultado del comando.

```
root@debian7:/etc/apache2# a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and create self-signed certificates
.
To activate the new configuration, you need to run:
  service apache2 restart
root@debian7:/etc/apache2#
```

Figura 97: Habilitando módulo SSL para el servicio de apache

## 1.8 Instalación y configuración de cliente de correo web Roundcube v0.7.2.

Editar el archivo ***"/etc/roundcube/main.inc.php"***, modificando las siguientes secciones:

**Sección IMAP.**

En la figura 98, se muestran las líneas para realizar conexiones de tipo TLS (Conexión segura) al equipo local (localhost) pues tanto los servicios como el cliente de correo se encuentran en el mismo equipo, el puerto por defecto es 97, pues en dovecot se usa también el puerto conocido para el servicio IMAP.

```
$rcmail_config['default_host'] = 'tls://localhost';
// TCP port used for IMAP connections
$rcmail_config['default_port'] = 143;
```

Figura 98: Sección IMAP del archivo main.inc.php

### Sección SMTP

En la figura 99, se indica que las conexiones al servidor SMTP deben realizarse usando TLS hacia el equipo local (localhost) y el puerto a usar es el 25, puerto por defecto también configurado en el paquete Postfix para el servicio SMTP.

```
$rcmail_config['smtp_server'] = 'tls://localhost';

// SMTP port (default is 25; 465 for SSL)
$rcmail_config['smtp_port'] = 25;
```

Figura 99: Sección SMTP del archivo main.inc.php

### Sección LDAP

En esta sección se encuentran parámetros referentes de conexión al servidor LDAP, cambiar a ***'true'*** el valor de la variable ***'use_tls'***, tal y como se observa en la figura 100.

```
'port'          => 389,
//'use_tls'           => false,
'use_tls'           => true,
'ldap_version'  => 3,       // using LDAPv3
```

Figura 100: Sección LDAP del archivo main.inc.php

Guardar los cambios realizados en el archivo y reiniciar el servicio apache.

**# service apache2 restart**

Antes de probar el correo web es necesario crear un enlace fácilmente accesible y fácil de recordar para el usuario, el archivo se llamará ***"rondcube.conf"*** dentro de la ruta ***"/etc/apache2/conf.d/"***, (para este ejemplo) y cuyo contenido será el que se muestra en la figura 101:

```
Alias /web /usr/share/roundcube
<Location /web>
    Order Allow,Deny
    Allow from 127.0.0.1 192.168.1.0/24
</Location>
```

Figura 101: Archivo roundcube.com, ejemplo de alias web

En donde, la primera línea indica que al momento de que el usuario ingrese a *misitio.com/web* sea enlazado al contenido de la carpeta **/usr/share/roundcube**, en esta carpeta es dónde se encuentran los archivos de interacción del cliente web de correo con el servidor.

En las siguientes líneas lo que se indica son políticas de acceso a directorio en base a direccionamiento IP, concretamente se indica que direcciones IP o de red pueden acceder a este directorio, en el caso que un equipo con una ip no permitida desee acceder al recurso recibirá el siguiente mensaje como el de la figura 102.


Figura 102: Intento de acceso a recurso web por equipo con direccionamiento ip no permitido

**Nota:** Asegúrese de reiniciar los servicios de postfix, dovecot, apache y ldap.

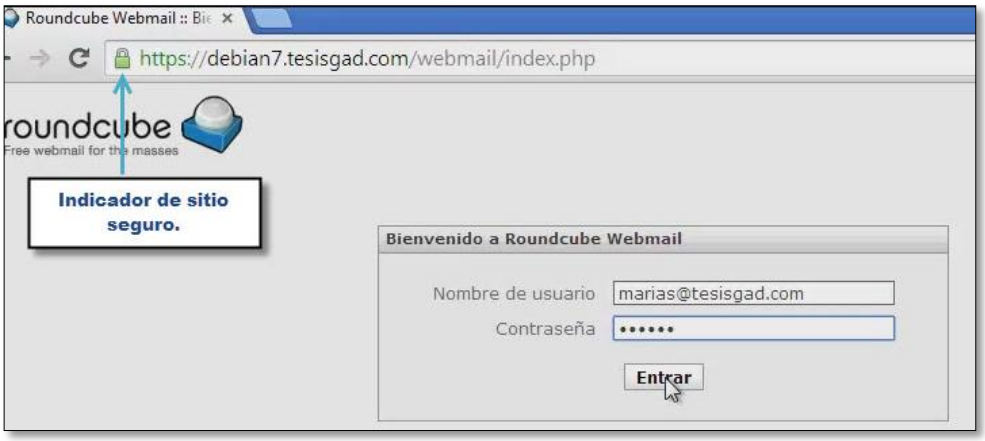



Figura 103: Prueba del servicio web de correo electrónico con Roundcube

## 2. Servidor VPN L2TP/IPSec.

La propuesta VPN L2TP/IPSec y dado los resultados de las pruebas realizadas en el entorno controlado es una decisión a ser tomada a futuro por miembros de la Institución, en este tema se cumplió con la demostración del desempeño de esta solución VPN.

Hay que tener en cuenta ciertos aspectos cuando se realice la configuración en el servidor VPN.

### 2.1 Configuración del servidor.

Editar el archivo principal del servicio ipsec, ***ipsec.conf***, se encuentra en la ruta ***"/etc/ipsec.conf"***:

**config setup**, es la sección que indica los parámetros generales de la configuración, dentro de ella se encuentra:

**nat_traversal=yes**, colocar el valor de "*yes*", cuando cualquiera de los 2 extremos del túnel ipsec está usando NAT, es decir se realiza una traducción de direcciones como por ejemplo una red detrás de un modem adsl.

**virtual_private**, aquí se declaran las subredes que se permite trabajar a través del túnel y cuales se desean excluir del mismo, generalmente se excluye aquellas direcciones de red que se superponen a las redes locales, el formato de la sub red a colocar es:

**virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12**

**protostack=netkey**, esta sentencia le indica a openswan a usar la implementación de IPSec por defecto desde el núcleo(kernel).

#### 2.1.1 Tipo de autenticación mediante clave pre compartida (PSK)

Una vez configurados los parámetros generales, indicar que tipo de autenticación se utiliza, se indicara primero el uso de clave pre-compartida o PSK.

Dentro del mismo archivo ***ipsec.conf***, colocar una sección para la autenticación mediante PSK, con los siguientes valores:

```
conn L2TP-PSK-NAT
```

```
      rightsubnet=vhost:%priv
      also=L2TP-PSK-noNAT

conn L2TP-PSK-noNAT
      authby=secret
      pfs=no
      auto=add
      keyingtries=3
      rekey=no
      ikelifetime=8h
      keylife=1h
      type=transport
      left=192.168.1.12
      leftprotoport=17/1701
      right=%any
      rightprotoport=17/%any
```

Las nuevas líneas agregadas corresponden al perfil de conexión, cada nuevo perfil de conexión inicia con la sentencia ***"conn"***, a continuación se explica los parámetros de conexión que se editaron.

**authby=secret**, indica el tipo de autenticación que se va a utilizar para la conexión, en este caso PSK.

**pfs=no**, esta opción garantiza que, la clave utilizada en una conexión no se vuelva a generar, para nuestro caso utilizar el valor por defecto "no".

**auto=add**, indica a openswan que la conexión este activa al iniciar el servicio.

**keyingtries=3**, el valor "3", indica el número de reconexiones en caso de fallo.

**rekey=no**, indica si una conexión debe ser renegociada o no.

**ikelifetime=8h**, el valor de "8h", indica el tiempo que debe pasar en la conexión de canal de "Asociación de Seguridad" ISAKMP antes de una renegociación de llaves.

**keylife=1h**, indica el tiempo que una conexión debe durar, desde el momento de una negociación exitosa hasta su momento de expiración.

**type = transport**, indica el tipo de funcionamiento a la protección IPSec, elegir transporte, debido a que el establecimiento de túnel se lo hace mediante l2tp del paquete xl2tpd.

**left=192.168.1.12**, aquí se especifica la dirección IP del servidor que estará a la escucha para este servicio.

**leftprotoport=17/1701**, indica el puerto de escucha para el servicio.

**right=%any**, el valor de "%any", se establece para indicar que acepte conexiones de cualquier dirección, esto para acceder al servicio de VPN, también se podría especificar una dirección de red o ip en particular.

**rightprotoport=17/%any**, este valor le indica al servidor que puerto va usar el cliente, se lo puede reemplazar con el valor 1701 ej.: **rightprotoport=17/1701**

### 2.1.2 Archivo ipsec.secrets

En este archivo se guarda la información sobre las contraseñas que se utilizan para autenticar los equipos en el caso de usar autenticación mediante PSK. O en el caso de usar certificados digitales como autenticación, se agrega la contraseña de la llave privada del certificado digital que usara este servidor VPN, su ubicación es ***"/etc/ipsec.secrets"***

```
: PSK "ConexionIPSec"
: RSA tesisgad.com.key.secure "tesisgadkey"
```

Como se observa en el ejemplo anterior, la primera línea indica la contraseña de autenticación que se utilizará como llave pre-compartida (PSK) de la conexión, también se puede utilizar la siguiente estructura:

IP_Servidor dirección_ip/red_cliente: PSK "contraseña"

Mientras que la segunda línea indica el nombre del certificado, que se especifica cuando se trabaja con autenticación mediante certificados digitales. Su estructura es:

IP_Servidor dirección_ip/red_cliente: RSA llave_privada.key "clave_de_llave_privada"

### 2.1.3 Archivo xl2tpd.conf

Es un archivo que se creó luego de la instalación del paquete xl2tpd, en la ruta ***"/etc/xl2tpd/xl2tpd.conf"***, en él se especifica el rango de direcciones ip's que el servidor ofrecerá como parte del túnel, es decir las direcciones que se les asigna al establecerse la autenticación de usuarios al servidor VPN. También se indica que tipo de autenticación soportado por el servidor para validar los usuarios, en muestro caso hemos colocado los siguientes valores:

```
[lns default]
```

```
ip range = 192.168.3.128-192.168.3.200
local ip = 192.168.3.2
length bit = yes
refuse pap = yes
refuse chap = yes
require authentication = yes
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
```

Esta sección llamada “lns default” o Sección Servidor de red L2tp por defecto (en español), es dónde se indica, el rango de direcciones que se asigna a los clientes VPN ya conectados correctamente **(ip range)**, la dirección IP del servidor local (dirección virtual también establecida al momento de establecerse el túnel), activar la longitud de bit para los paquetes **(length bit)**, que tipos de autenticación se van a rechazar **(pap y chap)**, indicar que se requiere autenticación del cliente **(require authentication)**, activar la depuración para las operaciones relacionadas al protocolo ppp **(ppp debug)** e indicar el archivo del cual se leerán las opciones para las comunicaciones ppp **(pppoptfile)**.

### 2.1.4 Archivo options.xl2tpd

Se encuentra en la ruta ***“/etc/ppp/options.xl2tpd”***, permite establecer opciones sobre la comunicación ppp brindada por el paquete xl2tpd, los valores que agregados son:

```
require-mschap-v2
ms-dns 192.168.3.2
asyncmap 0
auth
crtscts
lock
hide-password
modem
debug
name l2tpd
mtu 1200
mru 1200
proxyarp
lcp-echo-interval 30
lcp-echo-failure 4
nodefaultroute
```

Aquí se indica el mecanismo de autenticación requerido “mschap-v2”, la dirección ip del servidor dns para la red virtual, a los clientes se les asigna está dirección/es como dns local.

Con el valor *name* fijar el nombre del servidor de conexión, este se usará más adelante en otro archivo de configuración referente a este paquete, para ser preciso en el archivo chap-secrets.

Los valores de mtu y mru deben ser inferiores a 1500, esto para evitar fragmentación de paquetes en los clientes Windows.

### 2.1.5 Archivo chap-secrets

Ubicado en la ruta ***"/etc/ppp/chap-secrets"***, en este archivo se almacena las credenciales de autenticación para cada usuario y si se desea asignarle una ip fija, o asignar una ip del rango de direcciones, en el ejemplo se observa primero dos asignaciones de forma estática y la última a partir de un rango que se asignó en el archivo */etc/xl2tpd/xl2tpd.conf*.

```
# client   server     secret          IP addresses
cristian   l2tpd      cristian        192.168.3.3
franklin   l2tpd      franklin        192.168.3.4
test       l2tpd      test            192.168.3.128/25
```

El nombre que se utiliza para los clientes son: "cristian", "franklin", además la contraseña que utilizan para realizar la autenticación es el mismo nombre de usuario.

### 2.1.6 Configuraciones adicionales

Para que el servicio de ipsec funcione correctamente hay que editar el archivo ***/etc/systcl.conf***, agregar al final los siguientes parámetros, que se observan en la figura 104, garantizando así una correcta comunicación entre cliente-servidor:

```
#Desactivamos lo que solicita la verificación de "ipsec verify"
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.eth0.send_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
```

Figura 104: Archivo sysctl.conf

Si no se agregan los parámetros que se indican en la figura anterior, el resultado sería como el que se muestra en la figura 105, luego se ejecutar el comando:

# **ipsec verify**,

```
root@debian7:/home/cristian/Descargas/ipsec_con_certs# ipsec verify
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                                 [OK]
Linux Openswan U2.6.37/K3.2.0-4-686-pae (netkey)
Checking for IPsec support in kernel                            [OK]
 SAref kernel support                                           [N/A]
 NETKEY:  Testing XFRM related proc values                      [FAILED]

  Please disable /proc/sys/net/ipv4/conf/*/send_redirects
  or NETKEY will cause the sending of bogus ICMP redirects!

        [FAILED]

  Please disable /proc/sys/net/ipv4/conf/*/accept_redirects
  or NETKEY will accept bogus ICMP redirects!

        [OK]
Checking that pluto is running                                  [OK]
 Pluto listening for IKE on udp 500                             [OK]
 Pluto listening for NAT-T on udp 4500                          [OK]
Checking for 'ip' command                                       [OK]
Checking /bin/sh is not /bin/dash                               [WARNING]
Checking for 'iptables' command                                 [OK]
Opportunistic Encryption Support                                [DISABLED]
```

Figura 105: Resultado de comando “ipsec verify” antes de cambios en el archivo sysctl.conf

Una vez agregados las líneas en “sysctl.conf”, ejecutar el comando “sysctl -p”, en la consola, y al momento de ejecutar el comando de verificación de ipsec, no dará ningún, tal como se observa en la figura 106.

```
root@debian7:/home/cristian/Descargas/ipsec_con_certs# ipsec verify
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                                 [OK]
Linux Openswan U2.6.37/K3.2.0-4-686-pae (netkey)
Checking for IPsec support in kernel                            [OK]
 SAref kernel support                                           [N/A]
 NETKEY:  Testing XFRM related proc values                      [OK]
        [OK]
        [OK]
Checking that pluto is running                                  [OK]
 Pluto listening for IKE on udp 500                             [OK]
 Pluto listening for NAT-T on udp 4500                          [OK]
Checking for 'ip' command                                       [OK]
Checking /bin/sh is not /bin/dash                               [WARNING]
Checking for 'iptables' command                                 [OK]
Opportunistic Encryption Support                                [DISABLED]
```

Figura 106: Resultado de comando “ipsec verify” luego de aplicar cambios en el archivo sysctl.conf

### 2.1.7 Tipo de autenticación mediante Certificado Digital (RSA)

Con todo lo detallado anteriormente, se puede realizar una conexión utilizando el servicio de ipsec, mediante el uso de llave pre-compartida, o mediante el uso de

certificados digitales, para eso ubicarse en donde se encuentra el archivo ipsec.conf, y al final del mismo colocar las siguientes líneas:

```
conn L2TP-PSK-NAT2
rightsubnet=vhost:%priv
also=L2TP-PSK-noNAT
conn L2TP-PSK-noNAT2
authby=rsasig
pfs=no
auto=add
keyingtries=3
rekey=no
ikelifetime=8h
keylife=1h
type=transport
left=192.168.1.12
leftnexthop=192.168.1.1
leftrsasigkey=%cert
leftcert=/etc/ipsec.d/certs/tesisgad.com.pem
leftprotoport=17/1701
right=%any
rightprotoport=17/%any
dpddelay=10
dpdtimeout=90
dpdaction=clear
```

Los valores de los parámetros se describen a continuación:

**authby=rsasig**, el valor “rsasig”, corresponde al uso de certificados.

**pfs=no**, como sucedió con el caso de PSK, el valor continua siendo el mismo.

**auto=add**, indica a openswan que la conexión este activa al iniciar el servicio.

**keyingtries=3**, el valor “3”, indica el número de reconexiones en caso de fallo.

**rekey=no**, indica si una conexión debe ser renegociada o no.

**ikelifetime=8h**, tiempo máximo hasta de realizar una renegociación.

**keylife=1h**, indica el tiempo que una conexión debe durar, desde el momento de una negociación exitosa hasta su momento de expiración.

**type=transport**, tipo de funcionamiento de IPSec.

**left=192.168.1.12**, dirección ip del servidor.

**leftnexthop=192.168.1.1**, indica el siguiente salto que se debe dar para establecer la comunicación con el cliente, por tratarse de una prueba en la que tanto el cliente como el servidor se encuentran detrás de dispositivos NAT.

**leftrsasigkey=%cert**, define el tipo de certificado que desea utilizar.

**leftcert=/etc/ipsec.d/certs/tesisgad.com.pem**, especifica la ruta completa del certificado.

**leftprotoport=17/1701**, puerto de escucha para el servicio

**right=%any**, el valor de "%any", se establece para indicar que acepte conexiones de cualquier dirección.

**rightprotoport=17/%any**, indica el puerto que va a usar el cliente.

**dpddelay=10**, indica el tiempo de retardo en segundos, para recuperar recursos perdidos de un cliente (dead peer detection).

**dpdtimeout=90**, indica el tiempo que debe transcurrir para revisar si hay respuesta por parte del cliente, una vez transcurrido este periodo sin respuesta y ningún tráfico, se declara por muerto la comunicación.

**dpdaction=clear**, el valor de "clear", es utilizada para borrar los rastros cuando un cliente ha muerto en el intento de conexión.

## 2.2 Configuración del cliente.

El equipo cliente que hará uso de este servicio debe configurar los siguientes tres aspectos: creación del perfil de conexión (figura 107), importación de los certificados tanto del usuario como del CA (figura 108 – 109), configuración de políticas de conexión en el firewall para el servicio de IPSec.

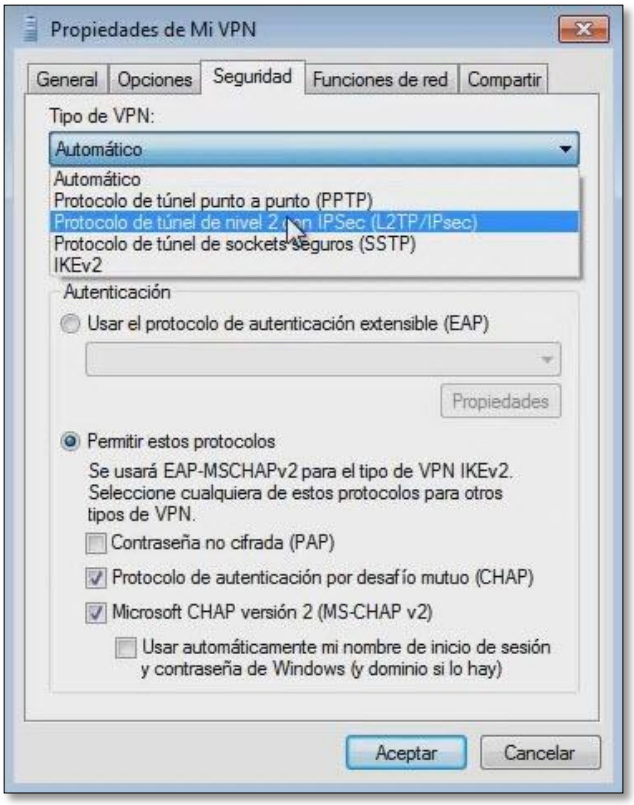



Figura 107: Propiedades de conexión VPN

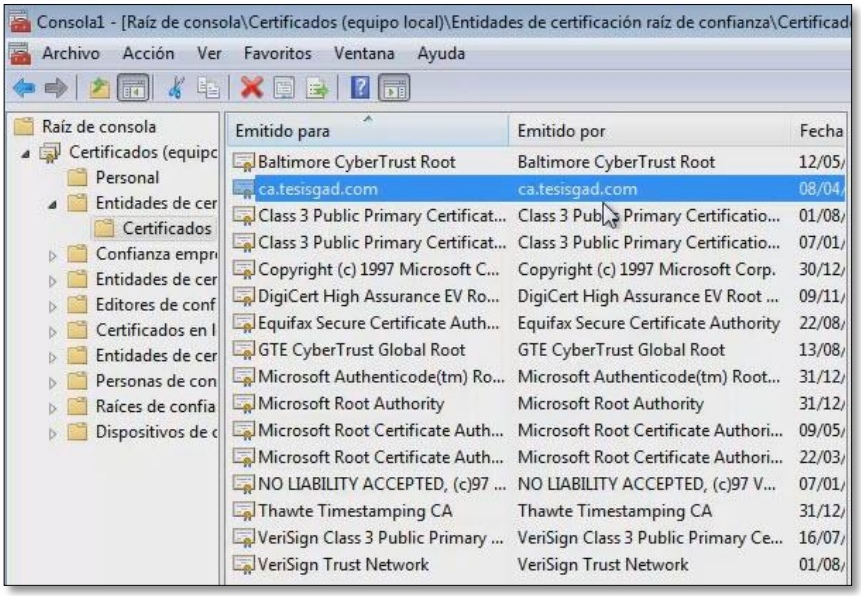



Figura 108: Ubicación de certificado de la Autoridad Certificadora

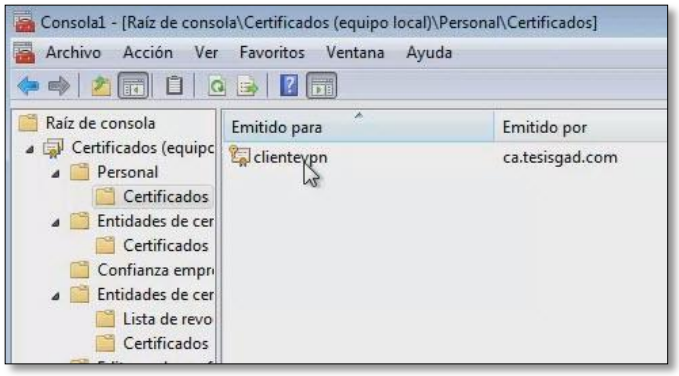



Figura 109: Nombre del usuario del certificado digital

## 3. Servidor de monitoreo Nagios.

En lo que respecta a la implementación de la herramienta de monitoreo Nagios, la documentación detallada en la fase 2 facilitó al administrador de la red configurar esta herramienta en uno de los servidores internos.

La figura 110 muestra el proceso de nagios iniciado correctamente, visto desde el navegador, una vez instalado en el servidor de pruebas.

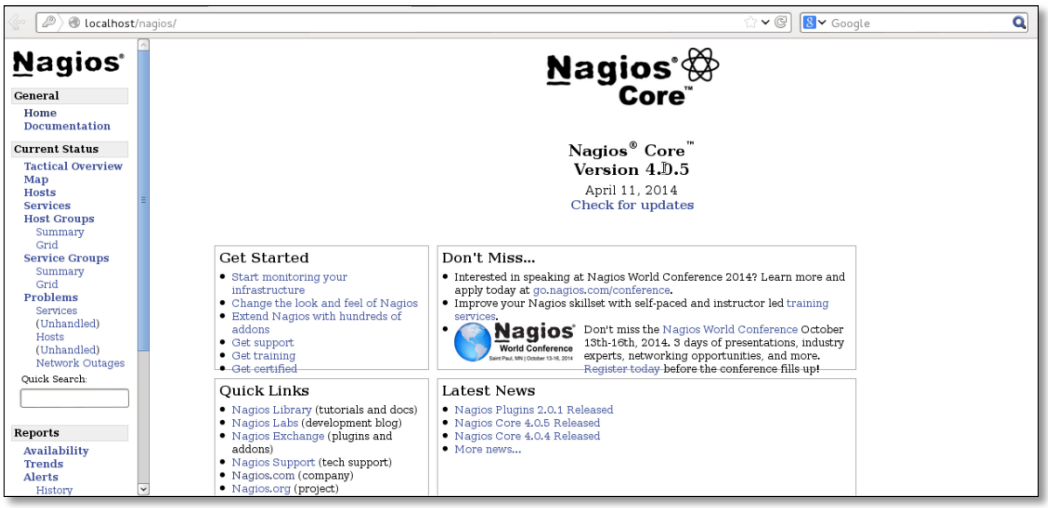
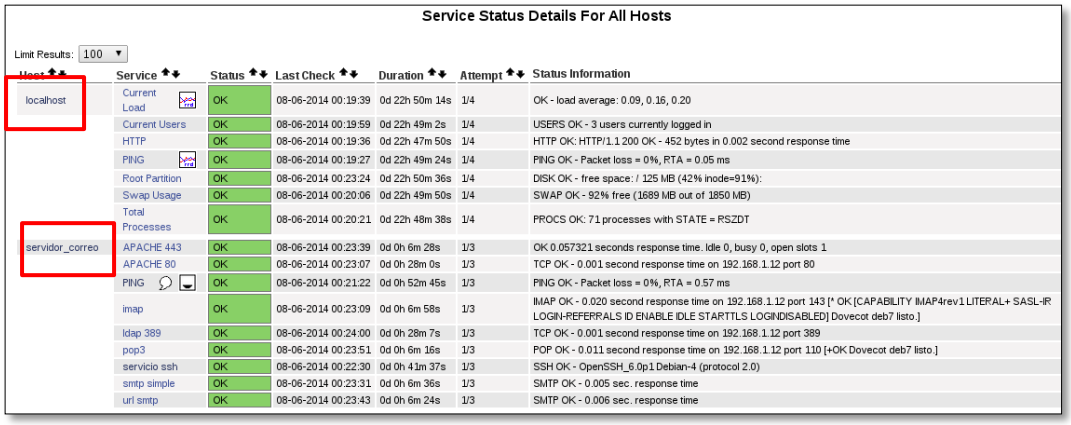



Figura 110: Interfaz de Nagios v4.0.5

Para comprobar que Nagios monitorea los servicios se agregaron dos equipos correspondientes al equipo donde está instalado Nagios (localhost) y al servidor de correo seguro (servidor_correo) los mismos que se pueden observar en la figura 111:



Service Status Details For All Hosts

Limit Results: 100

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| localhost | Current Load | OK | 08-06-2014 00:19:39 | 0d 22h 50m 14s | 1/4 | OK - load average: 0.09, 0.16, 0.20 |
| | Current Users | OK | 08-06-2014 00:19:59 | 0d 22h 49m 2s | 1/4 | USERS OK - 3 users currently logged in |
| | HTTP | OK | 08-06-2014 00:19:36 | 0d 22h 47m 50s | 1/4 | HTTP OK: HTTP/1.1 200 OK - 452 bytes in 0.002 second response time |
| | PING | OK | 08-06-2014 00:19:27 | 0d 22h 49m 24s | 1/4 | PING OK - Packet loss = 0%, RTA = 0.05 ms |
| | Root Partition | OK | 08-06-2014 00:23:24 | 0d 22h 50m 36s | 1/4 | DISK OK - free space: / 125 MB (42% inode=91%): |
| | Swap Usage | OK | 08-06-2014 00:20:06 | 0d 22h 49m 50s | 1/4 | SWAP OK - 92% free (1689 MB out of 1850 MB) |
| | Total Processes | OK | 08-06-2014 00:20:21 | 0d 22h 48m 38s | 1/4 | PROCS OK: 71 processes with STATE = RSZDT |
| servidor_correo | APACHE 443 | OK | 08-06-2014 00:23:39 | 0d 0h 6m 28s | 1/3 | OK 0.057321 seconds response time. Idle 0, busy 0, open slots 1 |
| | APACHE 80 | OK | 08-06-2014 00:23:07 | 0d 0h 28m 0s | 1/3 | TCP OK - 0.001 second response time on 192.168.1.12 port 80 |
| | PING | OK | 08-06-2014 00:21:22 | 0d 0h 52m 45s | 1/3 | PING OK - Packet loss = 0%, RTA = 0.57 ms |
| | imap | OK | 08-06-2014 00:23:09 | 0d 0h 6m 58s | 1/3 | IMAP OK - 0.020 second response time on 192.168.1.12 port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot deb7 listo.] |
| | ldap 389 | OK | 08-06-2014 00:24:00 | 0d 0h 28m 7s | 1/3 | TCP OK - 0.001 second response time on 192.168.1.12 port 389 |
| | pop3 | OK | 08-06-2014 00:23:51 | 0d 0h 6m 16s | 1/3 | POP OK - 0.011 second response time on 192.168.1.12 port 110 [+OK Dovecot deb7 listo.] |
| | servicio ssh | OK | 08-06-2014 00:22:30 | 0d 0h 41m 37s | 1/3 | SSH OK - OpenSSH_6.0p1 Debian-4 (protocol 2.0) |
| | smtp simple | OK | 08-06-2014 00:23:31 | 0d 0h 6m 36s | 1/3 | SMTP OK - 0.005 sec. response time |
| | url smtp | OK | 08-06-2014 00:23:43 | 0d 0h 6m 24s | 1/3 | SMTP OK - 0.006 sec. response time |

Figura 111: Equipos monitoreados por Nagios

Así mismo se instaló el front-end Check_mk, para visualizar de una manera más amigable tanto los equipos que se están monitoreando, la figura 112 muestra la ventana principal de Check_mk.

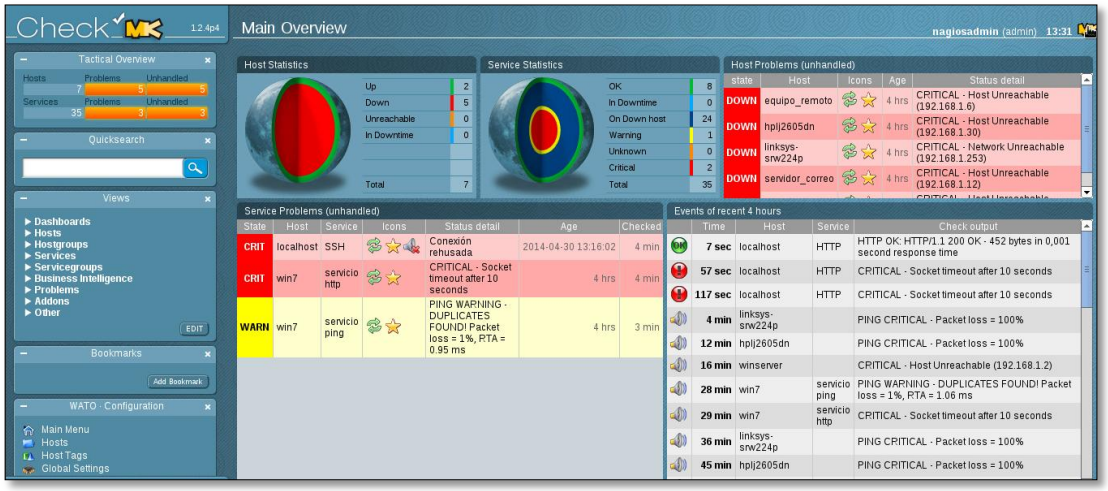



Figura 112: Ventana principal del addon check_mk

# g. Discusión

El presente trabajo es de carácter investigativo, cuyo propósito es la implementación de los protocolos seguros SSL/TLS mediante el empleo de los certificados digitales. Lo que garantiza que las comunicaciones cliente – servidor sean seguras y disminuir el nivel de vulnerabilidad que se presenta si no se utilizan estas implementaciones.

Además con la herramienta de monitoreo se tiene un control del estado de los servicios que se ejecutan dentro de la red de datos de la Institución.

## 1. Desarrollo de la propuesta alternativa.

**Objetivo 1: Analizar la infraestructura de la red en lo que refiere a equipamiento actual de la Institución.**

El cumplimiento de este objetivo se llevó a cabo en base a información proporcionada por el administrador de la red, para determinar cómo se realiza la comunicación y la disposición de los servidores dentro de la red de datos de la Institución.

De la información recolectada se pudo concluir que la red de datos de la Institución no cuenta con un dispositivo cortafuego tanto a nivel físico como lógico, lo que implica que cada servidor posea sus propias políticas para gestionar conexiones a los servicios que se considera de carácter público, como muestra la topología de la red.

**Objetivo 2: Realizar las pruebas de vulnerabilidades que presenta la red de datos de la Institución, para generar un informe del estado actual de la misma.**

Antes de realizar las pruebas de vulnerabilidades, se tuvo que realizar lo que se conoce como ***pentest***, en donde se recolecto información relevante de la Institución mediante el empleo de herramientas tales como: domainstools, netcraft y whois, que permitió reconocer datos esenciales de la Institución, obtener el bloque de direcciones e identificar la dirección IP del portal.

Aplicando Nmap al bloque de direcciones se obtuvo las direcciones IP activas de la Institución que se listan en la Tabla XII y finalmente utilizando nuevamente Nmap sobre cada una de las direcciones IP activas se conoció los puertos que están a la escucha, como se muestra en la Tabla XIII.

Además sobre estas mismas direcciones IP se realizó pruebas de vulnerabilidades utilizando Nessus, con el fin de determinar el nivel de amenaza de cada riesgo encontrado, esto se detalla en el Anexo 4.

Por último se generó un informe en donde constan las principales amenazas que tienen un gran impacto en la seguridad de la red de datos, como el robo de información personal (usuario – contraseña), estos resultados se pueden apreciar en la Tabla XXIX.

**Objetivo 3: Analizar las posibles soluciones encaminadas al proyecto planteado, tanto para el uso de protocolos seguros como herramienta de monitoreo.**

Una de las soluciones a la que se llegó luego de analizar las vulnerabilidades más críticas como se detalla en el informe de la Tabla XXIX, consistió en la creación de certificados digitales usando openssl y firmarlos localmente actuando como autoridad de certificación local. Esto permitió establecer conexiones SSL/TLS usando el estándar TLS v1.2 para el servicio de correo, es decir demostrar la autenticidad del servidor y proveer acceso seguro mediante HTTPS (Hypertext Transfer Protocol Secure).

Luego de analizar las posibles soluciones como alternativa a OpenVPN que se detallan en el punto 5 de la fase 1, se optó por utilizar el estándar VPN L2TP/IPSEC a nivel lógico, puesto que a nivel físico la Institución no tiene la necesidad de invertir en equipos para las dependencias rurales, que en algunos de los casos solo cuenta con un equipo y no demanda mayor inversión.

Para determinar qué tipo de herramienta cumple con las mejores condiciones para el monitoreo de servicios en tiempo real se realizó una comparativa entre: Nagios, Cacti, Zabbix, Zenoss y Pandora FMS; la misma que se detalla en el punto 6 de la fase 1 se pudo concluir que Nagios brinda las facilidades para realizar dichas funciones, además porque se pueden instalar complementos adicionales como es el caso de Check_mk, que permite visualizar de una amigable tanto los equipos como sus servicios.

Cabe recalcar que la solución a implementar estará al mismo nivel que funcionan los servidores de la Institución, tal como se muestra en la figura 113.

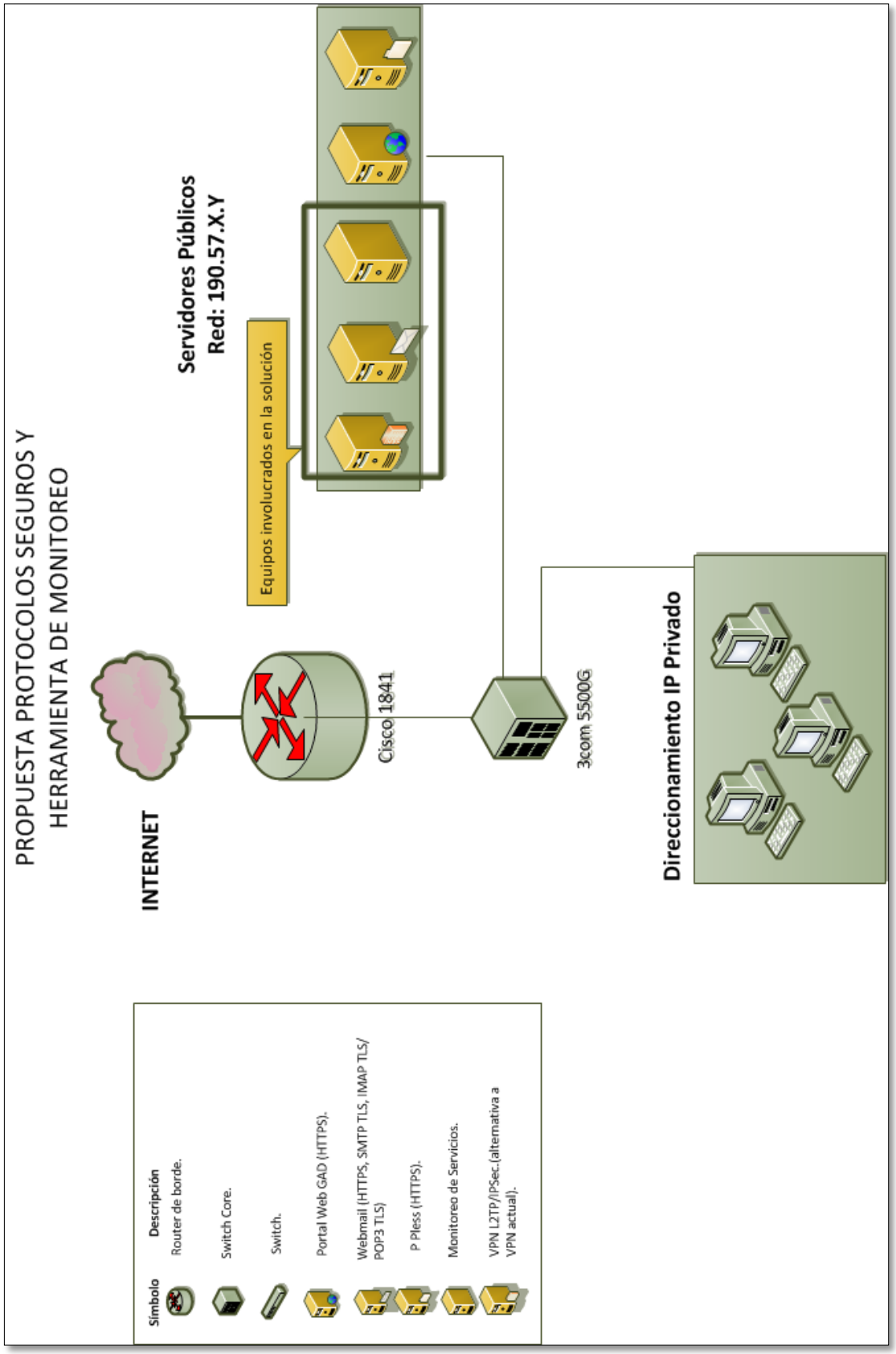



Figura 113: Topología de red con la solución a implementar

**Objetivo 4: Configuración y pruebas en un entorno controlado de los protocolos seguros y herramienta de monitoreo, para la red de datos de la Institución.**

**1. Configuraciones.**

**1.1. Servidor de correo.**

En el entorno controlado se utilizó software libre concretamente la distribución Linux Debian Wheezy como sistema base para las configuraciones del servicio de correo, ipsec y la herramienta de monitoreo Nagios. Las configuraciones empezaron con la creación de los certificados firmados localmente, los que se utilizaron en la configuración de servicio de correo seguro y acceso mediante HTTPS usando el estándar TLS v1.2. Además estos certificados fueron utilizados en la solución VPN propuesta en este proyecto.

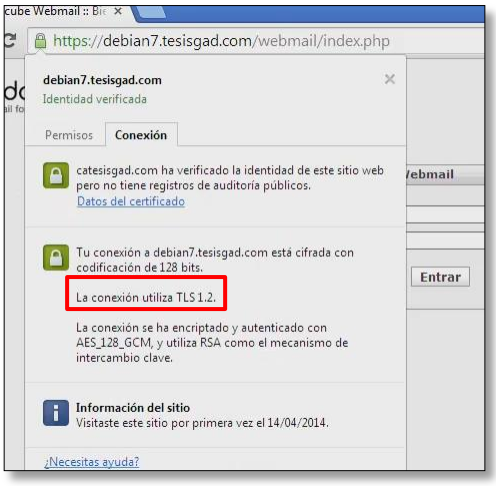



Figura 114: Detalles de la conexión HTTPS al sitio web de correo

Para realizar las configuraciones fue necesario realizar una réplica de las aplicaciones que maneja el servicio de correo, partiendo con la configuración del DNS utilizando como dominio local *"tesisgad.com"*.

Luego se realizó la configuración del agente de envío de correo Postfix, tomando como dominio el creado anteriormente. Este agente será el encargado de hacer llegar el correo a cada una de las cuentas de usuario que se creen en el directorio LDAP, pero para facilitar el manejo de LDAP se configuró la aplicación web "PHAMM" como gestor de cuenta de correo virtuales. Este front-end ayuda a gestionar de una mejor manera todas las cuentas de correo que se creen a partir de un dominio (tesisgad.com) en específico.

Para poder hacer uso del protocolo SSL/TLS es necesario activar ciertos parámetros en Postfix como se muestra en la figura 115, los mismos que permiten realizar una comunicación segura.

```
####Configuración de Postfix para trabajar con cuentas virtuales LDAP
myhostname = debian7.tesisgad.com
alias_maps = hash:/etc/aliases, ldap:/etc/postfix/ldap-aliases.cf
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = localhost
mynetworks = 127.0.0.0/8, 192.168.1.0/24
home_mailbox = Maildir/

####Sección de parámetros TLS####
#En esta sección se especifica los parámetros para establecer comunicaciones TLS (conexiones #cifradas)
smtpd_tls_cert_file=/etc/ssl/certificados/tesisgad.com.crt
smtpd_tls_key_file=/etc/ssl/certificados/tesisgad.com.key
smtpd_use_tls=yes
#smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache
#smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_scache

##Sección para usuario virtuales ldap
virtual_mailbox_base = /home/vmail/domains
virtual_mailbox_maps = ldap:/etc/postfix/ldap-users.cf
virtual_mailbox_domains = tesisgad.com
virtual_minimum_uid = 100
virtual_uid_maps = static:5000
virtual_gid_maps = static:5000
virtual_transport = virtual

##Sección para interactuar con SASL
#smtpd_sasl_local_domain = tesisgad.com
#smtpd_sasl_auth_enable = yes
#smtpd_sasl_security_options = noanonymous,noactive
#smtpd_sasl_type = dovecot
#smtpd_sasl_path = private/auth
#broken_sasl_auth_clients = yes

#Visualización de registros logs de Postfix
debug_peer_list=tesisgad.com
debug_peer_level=2
```

Figura 115: Resumen de configuración del archivo /etc/postfix/main.cf para conexiones seguras

Luego se configuró en agente de entrega de correo Dovecot para que interactúe tanto con Postfix así como con el directorio LDAP donde se encuentran las cuentas virtuales de correo.

En el servicio de apache se realizó la configuración que permite las conexiones SSL, este servicio se lo configuró para poder instalar un cliente web que facilite la interacción de los usuarios al servicio de correo mediante el acceso web.

Por último para terminar con la configuración del correo seguro se instaló el cliente web Roundcube, que permite el uso de los certificados digitales; al tratarse de una aplicación web el acceso será mediante HTTPS, como se muestra en la figura 116.

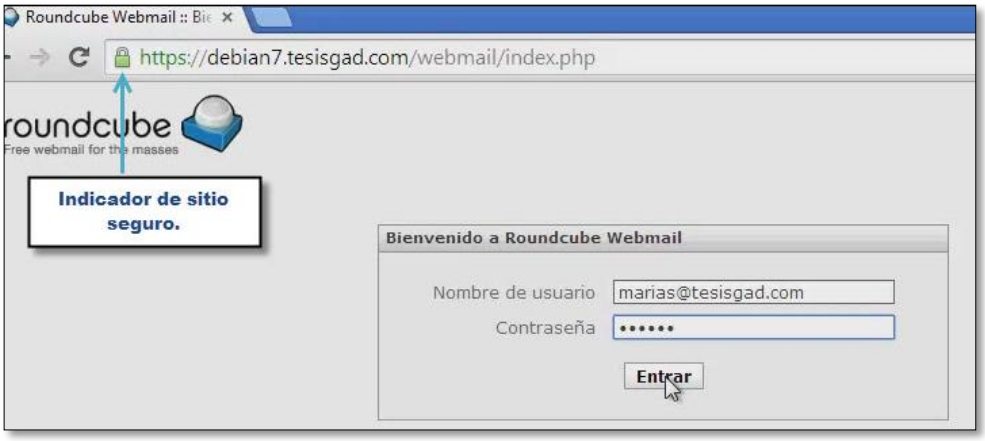



Figura 116: Acceso al servicio de correo local mediante HTTPS

### 1.2 Servidor VPN L2TP/IPSEC

En lo que respecta al uso de la tecnología L2TP/IPSEC, está divida en los partes:

- Primero: Configuración en el equipo que brindará el servicio de conexión segura a los clientes mediante el uso de L2TP/IPSEC, se instalaron y configuraron los paquetes OpenSwan y Xl2tpd.

- Segundo: Configuración del cliente Windows, para que pueda hacer uso del tipo de conexión L2TP/IPSEC, en el que se creó un perfil de conexión, se importó los certificados necesarios para autenticar al equipo como al usuario y por último de modificó el firewall para permitir la conexión al servicio IPSec.


Figura 117: Detalle de una conexión L2TP/IPSEC desde el cliente

### 1.3 Servidor de monitoreo Nagios.

Las últimas configuraciones realizadas corresponden a la herramienta de monitoreo Nagios; que comprende las siguientes etapas:

- **Configuración del equipo en donde se instalará Nagios:** Que permite monitorear los servicios públicos (todos aquellos que se pueden acceder directamente desde la red como: http, smtp, imap, pop, ssh, etc.) como privados. Mientras que para monitorear los servicios privados se integró Check_mk (front-end) con Nagios para visualizar los servicios de los equipos remotos que se agreguen.

- **Configuración del equipo a ser monitoreado:** Cada equipo del cual se requiera monitorear los servicios privados (aquellos recursos que no pueden ser accedidos directamente desde la red como procesos en ejecución, carga de CPU, espacio de las particiones, etc.), necesita tener instalado dos tipos de agentes (check-mk-agent, check-mk-agent-logwatch) que recolecten la información solicitada y la enviar al front-end Check_mk para su visualización.

## 2. Pruebas

Para constatar que el uso de SSL/TLS mediante certificados digitales reduce el riesgo de que atacantes puedan obtener información en las comunicaciones, se realizaron pruebas sin el uso de certificados, en dos escenarios distintos (Prueba 1 y Prueba 3) como se detalla en el punto 1 en la fase 3, donde quedó evidenciado que el uso de estas configuraciones son fácilmente aprovechadas por un atacante, que podría obtener información legible del usuario como: usuario – contraseña, además de poder leer los correos enviados.

Mientras que las Pruebas 2 y 4 del punto 1 en la fase 3, correspondes al uso de SSL/TLS mediante el uso de certificados digitales, en estas pruebas se pudo evidenciar que la información entre los dos extremos de la comunicación viaja cifrada, haciendo ilegible la información si un atacante interceptará dicha comunicación.

También se realizaron pruebas en una comunicación L2TP/IPSEC, como se detalla en el punto 2 en la fase 3, en donde al igual que con el servicio de correo (SSL/TLS), la información que se genera en la comunicación viaja cifrada, de esta manera el usuario

puede estar convencido de que lo que envía llega al destinatario correspondiente sin sufrir modificaciones.

Por último se realizó una prueba a la herramienta de monitoreo Nagios, para verificar si registra el estado de los servicios, por lo general el estado por defecto es el *"OK"*, si por algún motivo pasa a uno de los siguientes estados: *critical*, *warning*, *unknown* automáticamente se le hará llegar al responsable la notificación, indicando que un servicio ha cambiado de estado.

Esta notificación contiene información del servicio que cambio de estado, el nombre y dirección IP del equipo, y la hora en la que se registró la alerta.

**Objetivo 5: Implantar la solución que mejor se adapte a las necesidades de la Institución, en cuanto a protocolos seguros y herramienta de monitoreo.**

Luego de analizar las pruebas de la fase 3 en el entorno controlado, se presentó los resultados al encargado de la red y al jefe del departamento, para dar a conocer el funcionamiento de: correo seguro, l2tp/ipsec y herramienta de monitoreo Nagios; anteriormente configurados.

Para cumplir con el desarrollo de este objetivo se aportó con la respectiva documentación de cómo realizar las configuraciones relacionado con: servicio de correo seguro, VPN L2TP/IPSEC y herramienta de monitoreo Nagios.

Las configuraciones de los servicios antes mencionados se realizaron en el equipo de pruebas que posee la Institución, en donde se analizan las nuevas versiones de paquetes para determinar el desempeño de los servicios antes de pasar a producción.

**Objetivo 6: Evaluar el rendimiento de la solución.**

Para cumplir este objetivo se partió de los resultados obtenidos de las pruebas de los servicios de: correo seguro, l2tp/ipsec y herramienta de monitoreo Nagios.

En estos resultados se pudo evidenciar en el caso del servidor de correo como es su comportamiento cuando se establecen comunicaciones seguras y su contraparte cuando establece comunicaciones simples.

Al contar con una autoridad certificadora local se está contando con un tercero que valide los certificados para el servicio requerido, pero esto solo aplica a nivel de intranet. Cuando se trata de asegurar un servicio a nivel de internet es necesario

adquirir un certificado de una Autoridad Certificadora reconocida, entre ellas están: DigiCert, Symantec, Thawte, etc.

**Objetivo 7: Capacitar en el uso de las herramientas implantadas, así como la correcta gestión de las mismas, a los encargados del departamento de redes del GAD Municipal de Loja.**

Se realizó una exposición de los resultados que se obtuvieron durante el desarrollo del tema al Jefe del departamento de informática y administrador de la red de datos, en el departamento de informática.

**Objetivo 8: Elaboración del manual de usuario de las soluciones implantadas.**

Los manuales corresponden a las configuraciones tanto del servidor de correo, VPN de acceso remoto L2TP/IPSEC y herramienta de monitoreo Nagios a implantar en el departamento de informática del GAD Municipal de Loja.

## 2. Valoración técnica económica ambiental.

Dentro de la valoración técnica en el desarrollo del trabajo investigativo se recurrió a gastos necesarios para poder alcanzar los objetivos propuestos, todos estos gastos se materializaron en un plan lógico que se detalla a continuación:

TABLA XXXI: RECURSOS HUMANOS

| ROL | Equipo de trabajo | Horas | Precio/hora $ | Valor total $ |
|---|---|---|---|---|
| Tesista | Henry Cristian Cuesta Vega | 400 | 5,00 | 2.000,00 |
| Tesista | Franklin Rolando Mingo Morocho | 400 | 5,00 | 2.000,00 |
| Administrador de la red de datos del GAD | Ing. Darwin Betancourt | 38 | 10,00 | 380,00 |
| Director de tesis | Ing. Gabriela Viñán Rueda | 28 | 15,00 | 420,00 |
| | | | **Subtotal** | **4.800,00** |

TABLA XXXII: RECURSOS MATERIALES

| Descripción | Cantidad | Depreciación | | | Valor total $ |
|---|---|---|---|---|---|
| | | V. real $ | T. de util./año | V. Rec. $ | |
| **Hardware** | | | | | |
| Portátil HP Core i5 | 1 | 1.300,00 | 5 | 300 | 200,00 |
| Equipo de sobremesa Clon Core 2 Quad | 1 | 1.000,00 | 5 | 230 | 153 |
| Impresora Epson | 1 | 90 | 5 | 18 | 14,4 |
| | | | | **Subtotal** | **367,4** |
| **Software** | | | | | |
| Distribución Debian Wheezy | 2 | - | - | - | 0,00 |
| Sistema operativo Windows 7 | 2 | - | - | - | 298,00 |
| Actualización VMware Workstation | 2 | - | - | - | 238,00 |
| Openssl | - | - | - | - | 0,00 |
| Postfix | - | - | - | - | 0,00 |
| LDAP | 1 | - | - | - | 0,00 |
| Phamm | 1 | - | - | - | 0,00 |
| Roundcube | 1 | - | - | - | 0,00 |
| OpenSwan | 1 | - | - | - | 0,00 |
| Nagios | 1 | - | - | - | 0,00 |
| | | | | **Subtotal** | **536,00** |
| | | | | **Total** | **903,4** |

TABLA XXXIII: RECURSOS DE SERVICIOS

| **Descripción** | **Cantidad (horas)** | **Valor unitario $** | **Valor total $** |
|---|---|---|---|
| Internet | 600 h | 0,50 x hora | 300,00 |
| Llamadas celular | 5 h | 0,18 x min | 54,00 |
| Gastos de transporte | 200 | 0,25 | 50,00 |
| Taxi | 10 | 1,00 | 10,00 |
| | | **Subtotal** | **414,00** |

TABLA XXXIV: COSTE GENERAL DE RECURSOS

| **Descripción** | **Total $** |
|---|---|
| Recurso humano | 4.800,00 |
| Recursos materiales | 903,4 |
| Recursos de servicios | 414,00 |
| **Subtotal** | 6.117,4 |
| **Imprevistos (10 %)** | 611,74 |
| **Total** | **6.729,14** |

El desarrollo del presenta trabajo se considera factible, pues al utilizar herramientas de software libre en el desarrollo de la solución, se reduce considerablemente el coste de los recursos materiales, así mismo cabe mencionar que el coste económico se adjudicó por los autores del trabajo, debido a que la investigación se considera de carácter formativo y permitirá la obtención del título profesional, exceptuando el costo del recurso humano del director del proyecto que fue adjudicado por la universidad.

# h. Conclusiones

- El desarrollo de este proyecto permitió adquirir el conocimiento necesario para administrar servidores GNU/Linux como Debian Wheezy y de esta manera familiarizarse con el uso de software libre para el entorno de trabajo.

- Por medio de herramientas destinadas a la búsqueda e identificación de vulnerabilidades se desprende que los riesgos en los sistemas de información de las organizaciones pueden ser identificables y prevenibles, si se tiene claramente definido cuáles son los activos informáticos que requieren mayor seguridad.

- Se evidenció que la red de datos de la Institución proporciona un nivel medio/alto de seguridad en los equipos analizados con Nessus, al momento de medir los fallos en los servidores principales, desde fuera de la red, se encontraron vulnerabilidades significativas como el envío de información en texto plano que en manos equivocadas puede convertirse en una vulnerabilidad.

- El sistema de monitoreo configurado proporciona una interfaz web amigable parar el usuario, a través del front-end Check_mk que permite visualizar de manera detallada los servicios tanto públicos como los privados de los equipos que pertenece a la red de datos de la Institución, además de hacer más fácil la gestión de los servicios que se están monitoreando.

- El sistema de monitoreo implementado en la red de datos de la Institución monitorea continuamente el estado de los servicios y realiza él envió oportuno de notificaciones vía e-mail al personal de soporte técnico cuando alguno de estos servicios pasa a un estado inesperado.

- La implementación de protocolos seguros exigió dominar la gestión de certificados digitales locales a través de una Autoridad Certificadora en la Intranet, que valide los certificados emitidos para el servicio de correo y VPN de acceso remoto L2TP/IPSEC. Estos certificados interviene en el proceso de cifrado de comunicaciones garantizando disponibilidad, autenticidad, integridad y no repudio de la información.

- Al usar protocolos seguros basados en la tecnología SSL/TLS se brindó una mayor seguridad en la comunicaciones mitigando uno de los mayores riesgos que posee la Institución, específicamente el enviar información en texto plano.
- La socialización del proyecto del investigación con el personal del departamento de informática de la Institución, permitió reconocer la importancia que se obtuvo al aplicar los protocolos seguros y la herramienta de monitoreo para la red de datos.

# i. Recomendaciones

- Se recomienda usar comunicaciones seguras para cualquier tipo de servicio, pues garantiza que la información no será interceptada por intrusos en la red de comunicación, ni alterada en el proceso.
- Es necesario realizar periódicamente la búsqueda de vulnerabilidades en los sistemas, para corregir a tiempo cualquier riesgo que permita la ejecución de ataques informáticos.
- Si desea establecer un servicio VPN de acceso remoto que ofrezca una autenticación más robusta, la mejor alternativa es usar L2TP/IPSec ya que requiere validar el equipo y el usuario para cada conexión.
- La adquisición de certificados digitales emitidos por autoridades certificadoras reconocidas a nivel internacional facilitan la validación y correcta autenticidad de los sitios web que usan dichos certificados, esta es la razón por la que el GAD Municipal de Loja debería de realizar esta adquisición y usarla en servicios web públicos y así garantizar la seguridad en este tipo de conexiones.
- Se debe actualizar periódicamente los sistemas operativos, para evitar fallos de seguridad que puedan comprometer información crítica, así como la versión de los paquetes debe ser la más actual y estable en lo posible.
- Se recomienda siempre que sea factible, el disponer de un equipo cortafuego que realice el filtrado de tráfico y bloquee el acceso no autorizado a los servicios, de esta manera se controla las conexiones entrantes y salientes de la red de datos de la Institución.
- Es necesario contar con un sistema de detección y prevención de intrusiones que ayude a evitar ataques informáticos antes de que los sistemas sean vulnerados.

# j. Bibliografía

## Referencias Bibliográficas.


[1] Nmap.org. *Guía de referencia de Nmap (Página de manual)*. [En línea]. Disponible en: http://nmap.org/man/es/. Accedido el: 12-Mar-2013.

[2] Fixme. *Herramienta de exploración de redes y de sondeo de seguridad/puertos*. [En línea]. Disponible en: https://www.nmap.org/nmap-releases/nmap-6.01.DARPA1/docs/man-xlate/nmap-es.1. Accedido el: 12-Mar-2013.

[3] Hispasec.com. *Una al día: 12 años de seguridad informática – Hispasec*. [En línea]. Disponible en: www.hispasec.com/resources/UADv2.0.pdf. Accedido el: 19-Mar-2013.

[4] Secpedia. *OpenVAS*. [En línea]. Disponible en: http://secpedia.net/wiki/OpenVAS. Accedido el: 22-Mar-2013.

[5] Adastra. *Seguridad en Sistemas y Técnicas de Hacking*. [En línea]. Disponible en: http://thehackerway.com/2011/03/23/nexpose-con-metasploit/. Accedido el: 25-Mar-2013.

[6] Ohka. *NEXPOSE.* [En línea]. Disponible en: http://www.ohkasystems.com/Nexpose.html. Accedido el: 25-Mar-2013.

[7] Jsitech. *Escaneo web con Nikto. SEGURIDAD*. [En línea]. Disponible en: http://www.jsitech.com/seguridad/escaneo-web-con-nikto-seguridad/. Accedido el: 28-Mar-2013.

[8] Laboratorio de redes y seguridad, UNAM. *Seguridad Informática.* [En línea]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Integridad.php. Accedido el: 28-Mar-2013.

[9] Alejandro Eguía. *w3af, herramienta para detectar vulnerabilidades web*. [En línea]. Disponible en: http://www.spamloco.net/2012/04/w3af-detectar-vulnerabilidades-web.html. Accedido el: 31-Mar-2013.

[10] M. Morillo. *El Sistema de Nombres de Dominio (DNS).* [En línea]. Disponible en: http://www.dns-sec.es/index.php/sistema-de-nombres-de-dominio-dns/el-proposito-de-dns/. Accedido el: 9-Jun-2014.

[11] Universidad del Azuay. *El Sistema de Nombres de Dominio DNS.* [En línea]. Disponible en: http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/dns.htm. Accedido el: 9-Jun-2014.

[12] Ubuntu es. *Postfix.* [En línea]. Disponible en: http://doc.ubuntu-es.org/Postfix. Accedido el: 10-Jun-2014.

[13] M. Rouse. *SMTP (Simple Mail Transfer Protocol)*. [En línea]. Disponible en: http://searchexchange.techtarget.com/definition/SMTP. Accedido el: 10-Jun-2014.

[14] Dovecot.org. *Secure IMAP server.* [En línea]. Disponible en: http://www.dovecot.org/. Accedido el: 11-Jun-2014.

[15] UNICAN. *Configurar Correo IMAP.* [En línea]. Disponible en: https://sdei.unican.es/Paginas/servicios/correo/manual_imap.aspx. Accedido el: 11-Jun-2014.

[16] M. Donelly. *Una Introducción a LDAP.* [En línea]. Disponible en: http://ldapman.org/articles/sp_intro.html. Accedido el: 12-Jun-2014.

[17] S. Montoiro Peinado. *Instalación y configuración de un servidor GROUPWARE.* [En línea]. Disponible en: http://e-archivo.uc3m.es/bitstream/handle/10016/17892/PFC-Sergio%20Montoiro.pdf?sequence=1. Accedido el: 12-Jun-2014.

[18] MIT. *Capítulo 13. Protocolo ligero de acceso a directorios (LDAP)*. [En línea]. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-ldap-terminology.html. Accedido el: 12-Jun-2014.

[19] Nagios Chile Community Site. *Que es…. Nagios.* [En línea]. Disponible en: http://www.nagios-cl.org/que-es-nagios. Accedido el: 10-Jun-2013.

[20] E. M. González Pérez. *Sistema de Monitorización de la infraestructura CCTV en la UC3M con Zabbix.* [En línea]. Disponible en: http://e-

archivo.uc3m.es/bitstream/handle/10016/10533/MemoriaPFC_EmilioManuel_Gonzalez_Perez.pdf?sequence=1. Accedido el: 10-Jun-2013.

[21] The Cacti Group, Inc. *What is Cacti?* [En línea]. Disponible en: http://www.cacti.net/what_is_cacti.php. Accedido el: 11-Jun-2013.

[22] Ártica Soluciones Tecnológicas. *¿Qué es Pandora FMS?* [En línea]. Disponible en: http://pandorafms.com/Producto/what-is-pandorafms/. Accedido el: 11-Jun-2013.

[23] J. Herrera Acebey, D. Fernández Terrazas. *Certificados digitales.* Departamento de Ciencias Exactas e Ingeniería, Universidad Católica Boliviana. [En línea]. Disponible en: http://ucbconocimiento.ucbcba.edu.bo/index.php/ran/article/download/112/107. Accedido el: 17-Jun-2014.

[24] S. Talens-Oliag. *Introducción a los certificados digitales.* [En línea]. Disponible en: http://www.accv.es/noticias/certificadosdigitales.pdf. Accedido el: 17-Jun-2014.

[25] G. G. Brollo. *Redes Virtuales Privada.* [En línea]. Disponible en: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/VPN_Gerardo_Brollo.pdf. Accedido el: 19-Jun-2014.

[26] E. V. B. Esteban, *Redes privadas virtuales (VPN).* [En línea]. Disponible en: http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/VPN.pdf. Accedido el: 19-Jun-2014.

[27] M. L. *Seguridad en la capa de Red. IPSec*. [En línea]. Disponible en: http://www.laminfo.com/blog/archivos/__5_unidad_V_IP_sec.pdf. Accedido el: 19-Jun-2014.

[28] S. de la B. de I. U. de Sevilla. *Seguridad en la Red*. [En línea]. Disponible en: http://bibing.us.es/proyectos/abreproy/11499/fichero/05+-+Seguridad+en+la+red+en+GNU-Linux.pdf. Accedido el: 19-Jun-2014.

# k. Anexos

## Anexo 1: Aprobación del tema por parte del GAD Municipal de Loja

GAD Municipal de Loja

*Fomentemos las artes, la industria;*
*el saber tenga aquí su morada;*
*y la frente en sudor empapada,*
*sólo sepa inclinarse ante Dios.*

*Himno a Loja*

Loja enero 28, 2013

Ing.Mg.Sc.
ROBERTO JÁCOME GALARZA
**Director de Informática**
**Gobierno Autónomo Descentralizado Municipal de Loja**

**C E R T I F I C A :**

Que, fue aceptado el proyecto de tesis denominado "Implementación de Protocolos, Seguros y Herramienta de Monitoreo para la red de datos del Gobierno Autónomos Descentralizado Municipal de Loja", presentada por los señores Henry Cristian Cuesta Vega, con número de cédula 1104225865 y Franklin Rolando Mingo Morocho, con número de cédula 1104879380, alumnos de la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, Área de la Energía, la Industria y Recursos no Renovables, razón por la cual se autoriza iniciar con el proyecto antes señalado.

Lo certifico en honor a la verdad

**DIRECTOR DE INFORMÁTICA**

DIRECCIÓN DE INFORMÁTICA MUNICIPIO DE LOJA

Bolívar y José Antonio Eguiguren (esq.) | Télf. (593-7) 2570 407
Código Postal: 11-01-1028 | E-mail: info@loja.gob.ec
Loja - Ecuador

www.loja.gob.ec

Trabajamos con sentido social y profundamente humano

## Anexo 2: Listado de los servidores de la red de datos del GAD

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**1** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ing. Darwin Betancourt. | |
| **Cargo:** | Administrador de la Red. | |
| **Departamento:** | Informática | |

| **FICHA TECNICA DE SERVIDORES** | |
|---|---|
| **Función:** | Servidor Web 1.1 |
| **Código/Serie:** | KQFTAXW |
| **Marca:** | IBM |
| **Modelo:** | System X3650 |
| **Sistema Operativo:** | Debian Lenny GNU/Linux |
| **Descripción:** | Servidor que aloja el portal web del Gobierno Autónomo Descentralizado Municipal de Loja. |
| **Servicios:** | • WEB (Apache)<br>• Base de datos (Mysql)<br>• Ldap<br>• WEB (PHP)<br>• Email (Postfix)<br>• PHP |

| Información de componentes | | | | |
|---|---|---|---|---|
| Cant. | Nombre | Marca | Modelo | Características |
| 4 | Procesadores | Intel | Xeon | 2.66 Ghz |
| 1 | Disco duro | | SAS | 500 GB |
| | Memoria RAM | | | 18 GB |
| | | | | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**2** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ing. Darwin Betancourt | |
| **Cargo:** | Administrador de la Red. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | Servidor Proxy |
| **Código/Serie:** | KQDB9P |
| **Marca:** | IBM |
| **Modelo:** | X Series 226 |
| **Sistema Operativo:** | Debian Lenny GNU/Linux |
| **Descripción:** | Servidor Proxy, sirve para realizar el control de acceso a sitios web para el servicio de internet de la red interna del Gobierno Autónomo Descentralizado Municipal de Loja. |

**Servicios:**

- Proxy Transparente (Squid)
- Firewall (IPtables)
- DHCP
- DNS (Bind)
- _____
- _____
- _____
- _____

Información de componentes

| Cant. | Nombre | Marca | Modelo | Características |
|---|---|---|---|---|
| 2 | Procesadores | Intel | Xeon | 3.00 Ghz |
| 2 | Disco duro | | SCSI | SCSI de 75 GB |
| | Memoria RAM | | | 1 GB |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**3** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ing. Darwin Betancourt | |
| **Cargo:** | Administrador de la Red. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | Servidor de aplicaciones |
| **Código/Serie:** | KQADM0G |
| **Marca:** | IBM |
| **Modelo:** | X Series 226 |
| **Sistema Operativo:** | Suse 10.1 GNU/Linux |
| **Descripción:** | Autentica el registro del personal.<br>Roles de Pago. |

**Servicios:**

- Oracle 10.1
- Java SE
- _____
- _____
- _____
- _____

| Información de componentes | | | | |
|---|---|---|---|---|
| Cant. | Nombre | Marca | Modelo | Características |
| 4 | Procesadores | Intel | Xeon | 2.66 Ghz |
| 2 | Disco duro | | SCSI | SCSI de 75 GB Nivel de RAID 1 |
| | Memoria RAM | | | 1 GB |
| | | | | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**4** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 14 de Febrero 2013 | |
| **Responsable:** | Milton Canusa | |
| **Cargo:** | Analista de Red. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | QUIPUX |
| **Código/Serie:** | KQ03717 |
| **Marca:** | IBM |
| **Modelo:** | X Series 226 |
| **Sistema Operativo:** | Debian Lenny GNU/Linux |
| **Descripción:** | Servidor para la gestión documental del Gobierno Autónomo Descentralizado Municipal de Loja.<br>Almacena la base de datos para QUIPUX. |

**Servicios:**

- BD (Postgres )
- PHP
- _____
- _____
- QUIPUX
- _____
- _____
- _____

Información de componentes

| Cant. | Nombre | Marca | Modelo | Características |
|---|---|---|---|---|
| 4 | Procesadores | Intel | Xeon | 3.20 Ghz |
| 2 | Disco duro | | SCSI | SCSI de 75 GB |
| | Memoria RAM | | | 8 GB |
| | | | | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**5** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | | |
| **Responsable:** | Roberto Jácome | |
| **Cargo:** | Jefe del departamento de informática. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | Base de Datos |
| **Código/Serie:** | KQDB9M |
| **Marca:** | IBM |
| **Modelo:** | X Series 226 |
| **Sistema Operativo:** | Suse 10.1 GNU/Linux |
| **Descripción:** | Servidor de Base de datos. |

**Servicios:**

- BD Oracle 10.1
- _____
- _____
- _____
- _____
- _____
- _____
- _____

Información de componentes

| Cant. | Nombre | Marca | Modelo | Características |
|---|---|---|---|---|
| 4 | Procesadores | Intel | Xeon | 2.66 Ghz |
| 2 | Disco duro | | SCSI | 75 GB Nivel de RAID 1 |
| | Memoria RAM | | | 2 GB |
| | | | | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**6** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ronald Paladines | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | Catastros |
| **Código/Serie:** | MXQ029025F |
| **Marca:** | HP |
| **Modelo:** | Proliant DL 160G6 |
| **Sistema Operativo:** | - |
| **Descripción:** | Servidor de base de datos.<br>Dispone Geo data base para la Institución |

**Servicios:**

- BD (Postgress).
- Map Server
- _____
- _____
- CMS (Drupal)
- Apache
- _____
- _____

| Información de componentes | | | | |
|---|---|---|---|---|
| Cant. | Nombre | Marca | Modelo | Características |
| 1 | Procesadores | Intel | Xeon | 2.00 Ghz, posee 4 núcleos |
| 2 | Disco duro | | SCSI | 250 GB |
| | Memoria RAM | | | 4 GB |
| | | | | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**7** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ing. Darwin Betancourt | |
| **Cargo:** | Administrador de la Red. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | SIGAME |
| **Código/Serie:** | K0ADB8Z |
| **Marca:** | IBM |
| **Modelo:** | X Series 226 |
| **Sistema Operativo:** | Debian Lenny GNU/Linux |
| **Descripción:** | Servidor de Base de datos.<br>Gestiona procesos contables.<br>Presupuesto. |

**Servicios:**

- SQL Server
- Java
- _____
- _____
- Antivirus Update
- _____
- _____
- _____

Información de componentes

| Cant. | Nombre | Marca | Modelo | Características |
|---|---|---|---|---|
| 4 | Procesadores | Intel | Xeon | 3.20 Ghz |
| 1 | Disco duro | | SCSI | 300 GB |
| | Memoria RAM | | | 1 GB |
| | | | | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**8** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ing. Darwin Betancourt | |
| **Cargo:** | Administrador de la Red. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | Gestión Impuesto Municipales |
| **Código/Serie:** | |
| **Marca:** | HP |
| **Modelo:** | BL 460C G7 X 5670 |
| **Sistema Operativo:** | Debian 6.0 GNU/Linux 64 bits |
| **Descripción:** | Servidor de Gestión de Impuestos.<br>Recaudación de Impuestos. |

**Servicios:**

- JBoss
- _____
- _____
- _____
- Postgress
- _____
- _____
- _____

Información de componentes

| Cant. | Nombre | Marca | Modelo | Características |
|---|---|---|---|---|
| 4 | Procesadores | Intel | Xeon | 2.93 Ghz |
| 1 | Disco duro | | SAS | 500 GB |
| | Memoria RAM | | | 12 GB |
| | | | | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**9** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ing. Darwin Betancourt | |
| **Cargo:** | Administrador de la Red. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | Base de Datos |
| **Código/Serie:** | |
| **Marca:** | HP |
| **Modelo:** | BL 460C G7 X 5670 |
| **Sistema Operativo:** | Debian 6.0 GNU/Linux 64 bits |
| **Descripción:** | Base de Datos para la gestión de procesos. |

**Servicios:**

- Postgress
- _____
- _____
- _____
- S.I.G.
- _____
- _____
- _____

Información de componentes

| Cant. | Nombre | Marca | Modelo | Características |
|---|---|---|---|---|
| 4 | Procesadores | Intel | Xeon X5670 | 2.93 Ghz |
| 1 | Disco duro | | SATA | 500 GB 10000rpm |
| | Memoria RAM | | | 16 GB |
| | | | | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**10** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ing. Darwin Betancourt | |
| **Cargo:** | Administrador de la Red. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | P Pless (Sin papeles) |
| **Código/Serie:** | |
| **Marca:** | HP |
| **Modelo:** | BL 460C G7 X 5670 |
| **Sistema Operativo:** | Debian 6.0 GNU/Linux 64 bits |
| **Descripción:** | Sin papeles.<br>Seguimiento de trámites y documentos legales. |

**Servicios:**

- Alfresco
- _____
- _____
- Autenticación para seguimiento de trámites
- _____
- _____

Información de componentes

| Cant. | Nombre | Marca | Modelo | Características |
|---|---|---|---|---|
| 4 | Procesadores | Intel | Xeon | 2.93 Ghz |
| 1 | Disco duro | | SAS | 500 GB |
| | Memoria RAM | | | 12 GB |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | N° ficha<br>**11** |
| **Caso de estudio:** | Red de datos del GAD Municipal de Loja | |
| | | |
| **Fecha:** | 27 de Mayo 2013 | |
| **Responsable:** | Ing. Darwin Betancourt | |
| **Cargo:** | Administrador de la Red. | |
| **Departamento:** | Informática | |

## FICHA TECNICA DE SERVIDORES

| | |
|---|---|
| **Función:** | Sistema de Pruebas |
| **Código/Serie:** | |
| **Marca:** | HP |
| **Modelo:** | BL 460C G7 X 5670 |
| **Sistema Operativo:** | Debian 6.0 GNU/Linux 64 bits |
| **Descripción:** | Sistema con aplicaciones en pruebas, antes de pasar a servidor de impuestos municipales. |

**Servicios:**

- JBoss
- _____
- _____
- _____
- _____
- _____

Información de componentes

| Cant. | Nombre | Marca | Modelo | Características |
|---|---|---|---|---|
| 4 | Procesadores | Intel | Xeon | 2.93 Ghz |
| 1 | Disco duro | | SAS | 500 GB |
| | Memoria RAM | | | 12 GB |
| | | | | |

## Anexo 3: Amenazas encontradas en los servidores aplicando Nessus a cada una de las direcciones.

En este apartado de detalla los aspectos más reverentes, resumidos en sus respectivas fichas, luego de aplicar Nessus sobre cada una de las direcciones activas de la Institución.

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>1 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-05-21 | |
| **Departamento:** | Informática | |
| **PRUEBAS DE VULNERABILIDADES** | | |
| **Herramienta** | Nessus | |
| **OS** | Linux | |
| **Dirección IP** | 190.57.X.Y | |
| **Escenario** | Servidor | |
| **Total de amenazas** | 10 | |
| **Clasificación según Nessus** | • Críticos: 0<br>• Alto: 0<br>• Medio: 0<br>• Bajo: 1<br>• Solo se tiene información: 9 | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>2 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-05-21 | |
| **Departamento:** | Informática | |

| **PRUEBAS DE VULNERABILIDADES** | |
|---|---|
| **Herramienta** | Nessus |
| **OS** | Linux |
| **Dirección IP** | 190.57.X.Y |
| **Escenario** | Servidor |
| **Total de amenazas** | 23 |
| **Clasificación según Nessus** | • Críticos: 1<br>• Alto: 0<br>• Medio: 0<br>• Bajo: 0<br>• Solo se tiene información: 22 |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>3 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-04-23 | |
| **Departamento:** | Informática | |

| **PRUEBAS DE VULNERABILIDADES** | |
|---|---|
| **Herramienta** | Nessus |
| **OS** | Linux |
| **Dirección IP** | 190.57.X.Y |
| **Escenario** | Portal del GAD Municipal de Loja |
| **Total de amenazas** | 29 |
| **Clasificación según Nessus** | • Críticos: 0<br>• Alto: 0<br>• Medio: 3<br>• Bajo: 2<br>• Solo se tiene información: 24 |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>4 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-05-21 | |
| **Departamento:** | Informática | |
| **PRUEBAS DE VULNERABILIDADES** | | |
| **Herramienta** | Nessus | |
| **OS** | Linux | |
| **Dirección IP** | 190.57.X.Y | |
| **Escenario** | Servidor | |
| **Total de amenazas** | 36 | |
| **Clasificación según Nessus** | • Críticos: 0<br>• Alto: 0<br>• Medio: 3<br>• Bajo: 2<br>• Solo se tiene información: 31 | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>5 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-05-21 | |
| **Departamento:** | Informática | |
| **PRUEBAS DE VULNERABILIDADES** | | |
| **Herramienta** | Nessus | |
| **OS** | Linux | |
| **Dirección IP** | 190.57.X.Y | |
| **Escenario** | Servidor | |
| **Total de amenazas** | 54 | |
| **Clasificación según Nessus** | • Críticos: 0<br>• Alto: 1<br>• Medio: 3<br>• Bajo: 3<br>• Solo se tiene información: 47 | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>6 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-05-13 | |
| **Departamento:** | Informática | |
| **PRUEBAS DE VULNERABILIDADES** | | |
| **Herramienta** | Nessus | |
| **OS** | Linux | |
| **Dirección IP** | 190.57.X.Y | |
| **Escenario** | Servidor | |
| **Total de amenazas** | 51 | |
| **Clasificación según Nessus** | • Críticos: 0<br>• Alto: 1<br>• Medio: 5<br>• Bajo: 3<br>• Solo se tiene información: 42 | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>7 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-05-13 | |
| **Departamento:** | Informática | |
| **PRUEBAS DE VULNERABILIDADES** | | |
| **Herramienta** | Nessus | |
| **OS** | Linux | |
| **Dirección IP** | 190.57.X.Y | |
| **Escenario** | Servidor | |
| **Total de amenazas** | 19 | |
| **Clasificación según Nessus** | • Críticos: 0<br>• Alto: 0<br>• Medio: 0<br>• Bajo: 0<br>• Solo se tiene información: 19 | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>8 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-05-13 | |
| **Departamento:** | Informática | |
| **PRUEBAS DE VULNERABILIDADES** | | |
| **Herramienta** | Nessus | |
| **OS** | Linux | |
| **Dirección IP** | 190.57.X.Y | |
| **Escenario** | Servidor | |
| **Total de amenazas** | 16 | |
| **Clasificación según Nessus** | • Críticos: 0<br>• Alto: 0<br>• Medio: 0<br>• Bajo: 0<br>• Solo se tiene información: 16 | |

| | | |
|---|---|---|
| | **UNIVERSIDAD NACIONAL DE LOJA**<br>**A.E.I.R.N.N.R**<br>**Carrera de Ingeniería en Sistemas** | Tabla de resultados N°<br>9 |
| **Caso de estudio:** | GAD Municipal de Loja | |
| | | |
| **Fecha:** | 2013-05-13 | |
| **Departamento:** | Informática | |
| **PRUEBAS DE VULNERABILIDADES** | | |
| **Herramienta** | Nessus | |
| **OS** | Linux | |
| **Dirección IP** | 190.57.X.Y | |
| **Escenario** | Servidor | |
| **Total de amenazas** | 23 | |
| **Clasificación según Nessus** | • Críticos: 0<br>• Alto: 0<br>• Medio: 1<br>• Bajo: 0<br>• Solo se tiene información: 22 | |

## Anexo 4: Escaneos realizados a la red de datos del GAD con Nessus.

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Tue May 21 11:15:26 2013 |
| End time: | Tue May 21 11:33:50 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-193-uio.puntonet.ec |
| IP: | 190.57.[redacted] |
| OS: | CISCO PIX 7.0 |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 29 | 30 |

Figura 118: Escaneo realizado a la dirección IP 190.57.X.Y

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Tue May 21 11:43:27 2013 |
| End time: | Tue May 21 11:46:07 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-194-uio.puntonet.ec |
| IP: | 190.57.[redacted] |
| MAC Address: | [redacted] |
| OS: | Linux Kernel 2.6.32-5-amd64 |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 31 | 32 |

Figura 119: Escaneo realizado a la dirección IP 190.57.X.Y

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Tue Apr 16 11:22:02 2013 |
| End time: | Tue Apr 16 11:47:44 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-196-uio.puntonet.ec |
| IP: | 190.57.[redacted] |
| OS: | Linux Kernel 2.6 |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 0 | 3 | 2 | 26 | 31 |

Figura 120: Escaneo realizado a la dirección IP 190.57.X.Y

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Sun Apr 21 11:28:19 2013 |
| End time: | Sun Apr 21 11:45:34 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-197-uio.puntonet.ec |
| IP: | 190.57.[redacted] |
| OS: | Linux Kernel 2.6 on Debian 6.0 (squeeze) |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 0 | 3 | 2 | 38 | 43 |

Figura 121: Escaneo realizado a la dirección IP 190.57.X.Y

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Tue May 21 12:00:12 2013 |
| End time: | Tue May 21 13:49:33 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-198-uio.puntonet.ec |
| Netbios Name: | GADML-SJB1A |
| IP: | 190.57.[redacted] |
| OS: | Linux Kernel 2.6 on Debian 6.0 (squeeze) |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 1 | 3 | 4 | 137 | 145 |

Figura 122: Escaneo realizado a la dirección IP 190.57.X.Y

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Mon May 13 11:30:16 2013 |
| End time: | Mon May 13 12:39:13 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-200-uio.puntonet.ec |
| Netbios Name: | EVAGADMLA |
| IP: | 190.57.[redacted] |
| OS: | Linux Kernel 2.6 on Debian 6.0 (squeeze) |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 1 | 5 | 5 | 140 | 151 |

Figura 123: Escaneo realizado a la dirección IP 190.57.X.Y

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Mon May 13 20:54:17 2013 |
| End time: | Mon May 13 21:14:46 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-201-uio.puntonet.ec |
| IP: | 190.57.[redacted] |
| OS: | Linux Kernel 2.6 |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 45 | 45 |

Figura 124: Escaneo realizado a la dirección IP 190.57.X.Y

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Mon May 13 21:16:45 2013 |
| End time: | Mon May 13 21:24:33 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-202-uio.puntonet.ec |
| IP: | 190.57.[redacted] |
| OS: | Linux Kernel 2.6 on Debian 6.0 (squeeze) |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 21 | 21 |

Figura 125: Escaneo realizado a la dirección IP 190.57.X.Y

**190.57.[redacted]**

**Scan Information**

| | |
|---|---|
| Start time: | Mon May 13 21:32:06 2013 |
| End time: | Mon May 13 21:40:52 2013 |

**Host Information**

| | |
|---|---|
| DNS Name: | corp-190-57-168-203-uio.puntonet.ec |
| IP: | 190.57.[redacted] |
| OS: | Linux Kernel 2.6 on Debian 6.0 (squeeze) |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 30 | 31 |

Figura 126: Escaneo realizado a la dirección IP 190.57.X.Y

## Anexo 5: Glosario de términos.

**Auditoria:** Es un control selectivo, efectuado por un grupo independiente del sistema a auditar, con el objetivo de obtener información suficiente para evaluar el funcionamiento del sistema bajo análisis.

**Autenticación:** Procedimiento informático que permite asegurar que un usuario de un sitio web u otro servicio similar es auténtico o quien dice ser.

**CHAP:** Es el protocolo de autentificación periódica del cliente de L2F, sirve para mantener la comunicación continua o cancelar en base a una función hash.

**Cliente/servidor:** Este término define la relación entre dos programas de computación en el cual uno, el cliente, solicita un servicio al otro, el servidor, que satisface el pedido.

**Cortafuegos o Firewall.** Dispositivo para filtrar conexiones entrantes o salientes hacia un equipo.

**Dominio:** Conjunto de caracteres que identifica la dirección de un sitio web.

**DNI:** Documento Nacional de Identidad para la identificación de los ciudadanos.

**DN base:** Siglas de Distinguished Name, utilizado comúnmente en LDAP para la creación del nivel superior del directorio que por lo general es el nombre de la empresa.

**Escaneo:** Llevar a cabo un análisis mediante una herramienta.

**Exploit:** Programa o método concreto que saca provecho de una falla o agujero de seguridad de una aplicación o sistema, generalmente para un uso malicioso de dicha vulnerabilidad.

**Fingerprinting**: Procedimiento para identificación de sistema operativo, mediante información de software, considerada huella digital.

**Framework**: Es un conjunto estandarizado de conceptos, prácticas y criterios para hacer frente a un tipo común de problema, que puede ser usado para ayudarnos a resolverlo de forma rápida y eficaz.

**GPL:** Son las siglas de GNU General Public License (Licencia Pública General) es usada comúnmente en software y garantiza a los usuarios finales (personas,

organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar el software.

**Hacker**: Persona que tiene un conocimiento profundo acerca del funcionamiento de redes de forma que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

**HMAC:** Es un mecanismo de autenticación de mensaje usando funciones hash criptográficas. HMAC se puede utilizar con cualquier función de hash criptográfica iterativa, por ejemplo, MD5, SHA-1, en combinación con una clave secreta compartida.

**Host:** Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas (ssh, FTP, www, email, etc.). Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

**Hosting:** Es un término empleado al servicio que provee a los usuarios de internet un sistema para almacenar información de cualquier tipo y que se puede acceder vía web.

**IMAP:** Son las siglas de Internet Message Access Protocol, significa protocolo de acceso a mensajes de internet, que permite el acceso a los mensajes almacenados en un servidor de Internet.

**IP:** Es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única.

**L2F:** Son las siglas de Layer 2 Forwarding, este protocolo fue desarrollado por Cisco, no depende de IP, permitiéndolo trabajar sobre otros protocolos haciendo uso del servicio de enlace Virtual Dial-Up.

**Log**: Registro de las actividades que ocurren en un sistema de computación o programa. Se almacena en un fichero al efecto.

**LDAP:** Son la siglas de Lightweight Directory Access Protocol, en español Protocolo Ligero de Acceso a Directorios, permite el acceso a un servicio de directorio ordenado y distribuido para buscar información en un entorno de red.

**Mapeador:** Realiza un mapa o traza de procesos.

**NNTP:** Son la siglas de Network News Transport Protocol, es un protocolo utilizado para la transferencia de artículos y noticias en red.

**PAP:** Es el protocolo de autenticación de password de L2F, empleado para verificar el nombre – usuario y establecer la conexión.

**Paquete:** La parte de un mensaje que se transmite por una red. Antes de ser enviada a través de Internet, la información se divide en paquetes.

**Ping:** En el ámbito informático, el concepto de ping es considerado un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red.

**Plug-in:** Programa que puede ser instalado y usado como parte del navegador. Un ejemplo es Macromedia's Shockwave, que permite reproducir sonidos y animaciones.

**PPTP:** Son las siglas de Point to Point Tunneling Protocol, es un protocolo de red desarrollado por Microsoft, que permite el tráfico seguro de datos desde un cliente remoto a un servidor privado, estableciéndose así una Red Privada Virtual.

**Puertos:** (puertos lógicos) Son puntos de acceso entre equipos para el uso de servicios y flujo de datos entre ellos, ejemplos el puerto 21 correspondiente al servicio FTP.

**RFC:** Son la siglas de Request for Comments, cuya traducción literal es “Petición de Comentarios”, son publicaciones del IETF (Internet Engineering Task Force – Grupo de Trabajo de Ingeniería de Internet) que contienen una serie de documentos con notas técnicas y organizativas sobre Internet.

**RRDTool:** Son las siglas de Round Robin Database Tool, es una herramienta de trabaja con base de datos donde se aplica el algoritmo de planificación Round-Robin.

**RSA:** Es un algoritmo criptográfico de clave pública empleado para cifrar y firmar digitalmente.

**Shell:** Es el intérprete de comandos de las distribuciones de GNU/Linux para invocar programas, así como herramientas disponibles en el computador.

**TLS:** Son las siglas de Transport Layer Security o en español Seguridad en la Capa de Transporte, es un protocolo criptográfico que facilita comunicaciones seguras sobre una red.

**TACACS**: Son las siglas de Terminal Access Controller Access Control System, en español Sistema de Control de Acceso mediante Control del Acceso desde Terminales, es un protocolo de autenticación usado para comunicarse con un servidor de autenticación para determinar si un usuario tiene acceso a la red.

**X.500:** Es una forma estándar para desarrollar un directorio electrónico de las personas en una organización para que pueda formar parte de un directorio global disponible para cualquier persona en el mundo con acceso a Internet

**Anexo 6: Certificación de la traducción del resumen de la tesis.**

FINE-TUNED ENGLISH
LANGUAGE INSTITUTE

Lic. Henry Gómez López
PROFESOR DEL INSTITUTO
"FINE-TUNED ENGLISH"

CERTIFICA:

Que el documento aquí compuesto es fiel traducción del idioma español al idioma inglés del resumen para el artículo científico de la tesis titulada ***"IMPLEMENTACIÓN DE PROTOCOLOS SEGUROS Y HERRAMIENTA DE MONITOREO PARA LA RED DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LOJA"***, de los señores HENRY CRISTIAN CUESTA VEGA y FRANKLIN ROLANDO MINGO MOROCHO, egresados de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja.

Lo certifica en honor a la verdad y autoriza al interesado hacer uso del presente en lo que a sus intereses convenga.

Loja, 19 de septiembre de 2014

FINE-TUNED ENGLISH CIA. LTDA. LOJA - ECUADOR

Lic. Henry Gómez López
PROFESOR DE F.T.E.

Fine-Tuned English Cía. Ltda.
LOJA: Macará entre Miguel Riofrío y Rocafuerte * 2578899 * 2563224 * 2574702
CATAMAYO: Av. 24 de Mayo 08-21 y Juan Montalvo * 2678442
ZAMORA: García Moreno y Pasaje 12 de Febrero * 2608169
www.finetunedenglish.edu.ec

## Anexo 7: Declaración de confidencialidad.

**DECLARACIÓN DE CONFIDENCIALIDAD**

Los autores de este proyecto: **Henry Cristian Cuesta Vega** con cédula de identidad 1104225865 y **Franklin Rolando Mingo Morocho** con cédula de identidad 1104879380, declaran lo siguiente:

**PRIMERO: Antecedentes.**

1) Los autores participan o han participado en el proyecto de fin de carrera denominado *"Implementación de protocolos seguros y herramienta de monitoreo para la red de datos del Gobierno Autónomo Descentralizado Municipal de Loja"*, utilizando la distribución GNU/Linux Debian Wheezy como sistema base, dirigido en un inicio por el Ing. Hernán Leonardo Torres, que por motivos de relación contractual con la Universidad fue cesado de sus funciones, después de dicho cambio el coordinador de la carrera Ing. Roberto Jácome asigno a nuestro proyecto a la Ing. Gabriela Viñan Rueda en calidad de director.

2) Por el presente documento se regula el tratamiento que los autores han de dar a la información a la que pueden tener acceso en el desarrollo de las tareas de investigación que se realicen en dicho proyecto, el cual se regulará por las disposiciones contenidas en las siguientes clausulas.

**SEGUNDO: Información Confidencial.**

La información referida a materiales, métodos y resultados científicos, técnicos y comerciales utilizados u obtenidos durante la realización del proyecto de investigación o una vez realizado el mismo, se considerará siempre Información Confidencial.

**TERCERO: Excepciones.**

No será considerado como información confidencial:

a) La información que los autores puedan probar que tenían en su legítima posesión con anterioridad al conocimiento de la Información Confidencial.

b) La información que los autores puedan probar que era de dominio público en la fecha de la divulgación o pase a serlo con posterioridad, por haberse publicado o por otro medio, sin intervención ni negligencia de los autores.

c) La información que los autores puede probar que corresponda en esencia a información facilitada por terceros, sin restricción alguna sobre su divulgación, en virtud de un derecho de los autores a recibirla.

**CUARTO: Secreto de la Información Confidencial.**

Los autores se comprometen a mantener totalmente en secreto la Información Confidencial recibida en relación con el proyecto referido anteriormente y no se divulgará a terceros durante la vigencia de esta Declaración de Confidencialidad.

Asimismo los autores se comprometen a emplear la Información Confidencial, exclusivamente, en el desempeño de las tareas que tenga encomendadas en dicho proyecto.

**QUINTO: Duración.**

La obligación de los autores respecto al mantenimiento del compromiso de secreto de la Información Confidencial, será de un tiempo no mayor a 180 días para fines de investigación a partir de la fecha de recepción de la Información Confidencial.

Loja, 08 de octubre de 2014

Atentamente:

| | |
|---|---|
| Henry Cristian Cuesta Vega<br>C.I.: 1104225865 | Franklin Rolando Mingo Morocho<br>C.I.: 1104879380 |

## Anexo 8: Certificados Digitales para el GAD Municipal de Loja.

### CERTIFICADOS PARA SITIO SEGURO (PORTAL WEB)

| Certificado SSL para sitio Seguro 1 | | |
|---|---|---|
| **Autoridad de Certificación** | **Digicert** | **Symantec(Antes de Verisign)** |
| **Costo 1 año** | $ 175 | $ 399 |
| **Costo 2 años** | $ 315 | $ 695 |
| **Costo 3 años** | $ 419 | $ 995 |
| **Tiempo de emisión de certificado** | Menos de 1 hora | Menos de 4 días |
| **Longitud de cifrado en comunicaciones** | 128 a 256 bits | 128 a 256 bits |
| **Garantía** | $ 1 000 000 | $ 1 500 000 |
| **Ítem** | SSL Plus | Sitio seguro |

| Certificado SSL para sitio Seguro 2 (EV) | | |
|---|---|---|
| **Autoridad de Certificación** | **Digicert** | **Symantec(Antes de Verisign)** |
| **Costo 1 año** | $ 295 | $ 995 |
| **Costo 2 años** | $ 469 | $ 1790 |
| **Tiempo de emisión de certificado** | Menos de 1 hora | Menos de 4 días |
| **Longitud de cifrado en comunicaciones** | 128 a 256 bits | 128 a 256 bits |
| **Garantía** | $ 1 000 000 | $ 1 500 000 |
| **Ítem** | SSL EV | Sitio seguro con EV |

**Ofertas individuales de cada Autoridad certificadora:**

**Digicert:** EL certificado emitido puede instalarse un sin número de veces (no está orientado a un solo servicio o equipo). El certificado es válido tanto para https://www.sitio.com como para https://sitio.com.

**Symantec:** Ofrece escaneos en busca de malware en los equipos que se instaló los certificados digitales adquiridos. Además de la búsqueda gratuita de vulnerabilidades.

**Certificados para usar varios dominios/subdominios**

| Certificado SSL para varios dominios. | | |
|---|---|---|
| **Autoridad de Certificación** | **Digicert** | **Symantec(Antes de Verisign)** |
| **Costo 1 año** | $ 299 | $ 1999 |
| **Costo 2 años** | $ 538 | $ 3595 |
| **Costo 3 años** | $ 717 | $ 5095 |
| **Tiempo de emisión de certificado** | Menos de 1 hora | Menos de 7 días |

| | | |
|---|---|---|
| **Longitud de cifrado en comunicaciones** | 128 a 256 bits | 128 a 256 bits |
| **Garantía** | $ 1 000 000 | $ 1 500 000 |
| **ítem** | (UC) comunicaciones unificadas. | Secure Site Wildcard (comodín). |

**Ofertas individuales de cada Autoridad certificadora:**

**Digicert:** El certificado para comunicaciones unificadas tiene un soporte para 4 dominios, sitios, subdominios distintos: www.ejemplo.com, autodiscover.ejemplo.com, correo.ejemplo.com, otro.ejemplo.com. Si se desea agregar un dominio adicional el costo por esto es $39 usd. adicionales por cada dominio añadido para la compra de 1 año; para la compra por 2 años es de $69 usd; y $89 por el período de 3 años.

También existe el tipo de certificado llamado Multidominio con EV, el que brinda la validación extendida (barra verde), con este puede asegurar un máximo de 3 dominios, sitios, subdominios con un solo certificado, esto cubierto en el precio base.

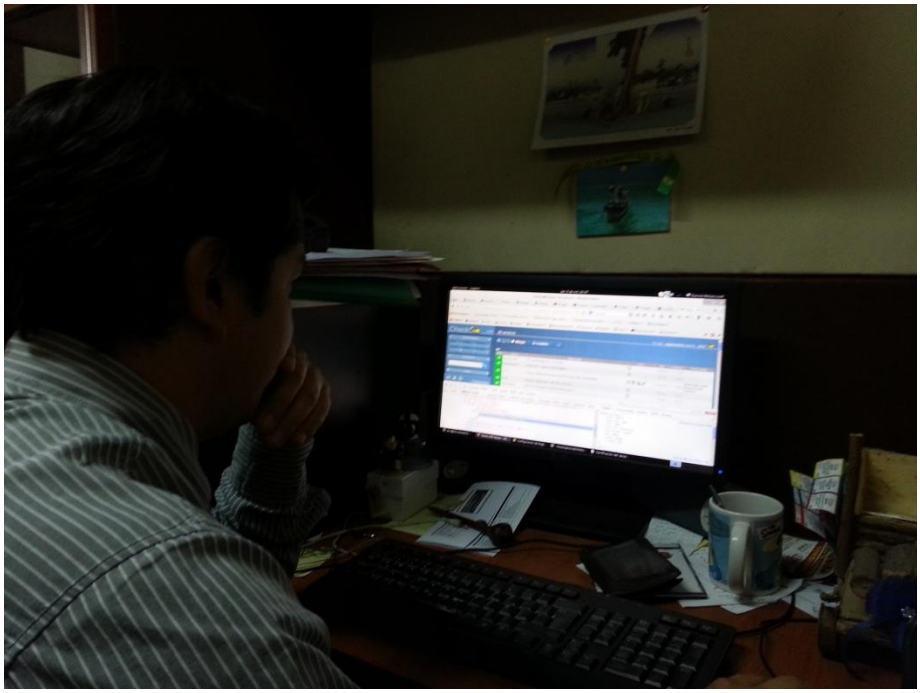
Costo de certificado 1 año: $489, y por cada nombre adicional $99

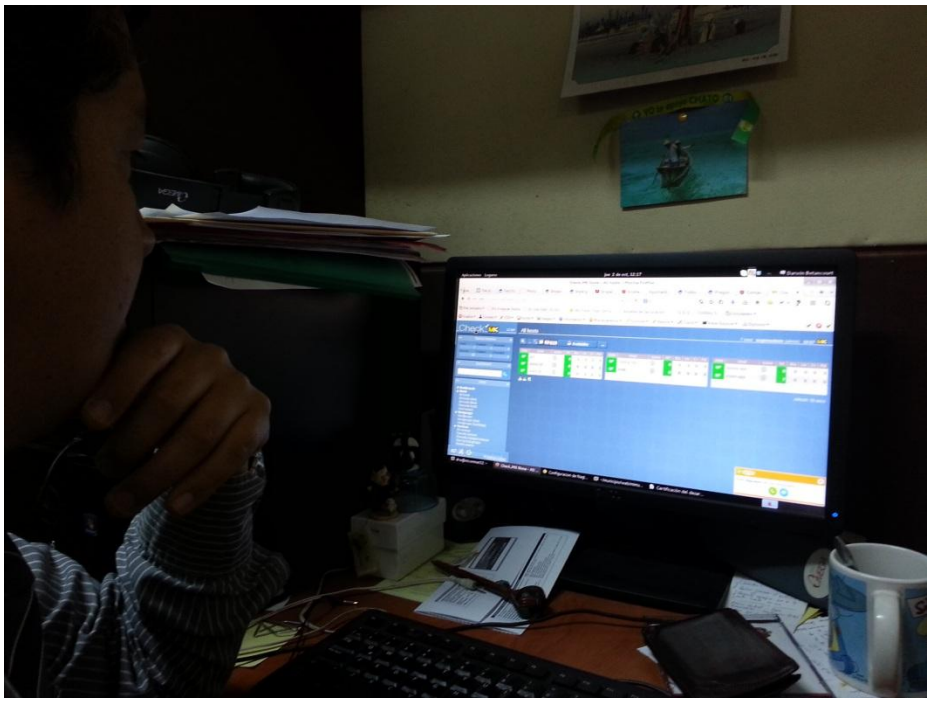
Costo de certificado 2 años: $489, y por cada nombre adicional $169

**Symantec:** El certificado Secure Site con Wildcard brinda soporte para múltiples subdominios (no se especifica un número fijado). Análisis de vulnerabilidades y malware en el equipo que se instalara el certificado.

**Anexo 9: Socialización de los resultados del proyecto con el jefe del departamento de informática y con el administrador de la red de datos de la Institución.**

**Anexo 10: Configuración de los servicios configurados en el servidor de pruebas de la Institución.**





**Anexo 11: Licencia Creative Commons.**

**Anexo 12: Anteproyecto de tesis.**

# Universidad Nacional de Loja

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

**CARRERA DE INGENIERIA EN SISTEMAS**

# "Implementación de protocolos seguros y herramienta de monitoreo para la red de datos del Gobierno Autónomo Descentralizado Municipal de Loja"


Integrantes:

- Henry Cristian Cuesta Vega
- Franklin Rolando Mingo Morocho


Loja -Ecuador

**2013**

**ÍNDICE GENERAL**

## ÍNDICE DE FIGURAS



## ÍNDICE DE TABLAS

## A. TEMA:

IMPLEMENTACIÓN DE PROTOCOLOS SEGUROS Y HERRAMIENTA DE MONITOREO, PARA LA RED DE DATOS DEL GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE LOJA.

## B. PROBLEMÁTICA

### 1. Antecedentes.

La seguridad es un tema fundamental en redes informáticas y en el ámbito de los servicios de red es indispensable proporcionar mecanismos que permitan identificar que tanto servidores como clientes sean quienes dicen ser y además que las comunicaciones y la información se encuentre debidamente cifrada. Actualmente los servicios de la red de datos del GAD Municipal de Loja se encuentran expuestos a ciertos riesgos ya que no se maneja autenticación, confidencialidad e integridad de las conexiones y de los datos que fluyen por éstas; lo cual permitiría que cualquier intruso a la red pueda capturar la información, realizar suplantaciones de equipos y servicios web, modificar información importante, acceder a servidores.

Todos estas aplicaciones y servicios se los gestiona a través de redes informáticas, es por este motivo que la seguridad de la misma debe ser un aspecto debidamente atendido, para esto existen mecanismos de seguridad variados como implementar SSL al protocolo HTTP a los servicios que se presentan mediante aplicaciones web, pero así mismo estos se hayan vulnerables a serie de ataques como robo de información, suplantaciones de equipos y daños relacionados a la información de servidores, que lo hacen vulnerable al mismo.

Muchos de los sistemas están expuestos a tener vulnerabilidades de seguridad que son explotadas para acceder archivos, obtener privilegios o realizar manipulación de información valiosa. Estas vulnerabilidades ocurren por varias razones, y miles de puertas invisibles son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, navegadores de Internet, correo electrónico y toda clase de servicios informáticos disponibles.

### 2. Situación Problemática

Actualmente los servicios de la institución se encuentran expuestos, ya que no se maneja autenticación, confidencialidad e integridad de las conexiones y de los datos que fluyen por éstas; lo cual permitiría que cualquier intruso a la red pueda capturar la información, realizar suplantaciones de equipos y servicios web, modificar información importante, y acceder a servidores. El control de acceso a los sistemas web que se

emplean dentro de la institución se lo realiza mediante configuraciones correspondientes a cada sistema.

Por esta razón nace la necesidad de añadir a la seguridad existente en la red de datos otros mecanismos de protección de la información.

Es una necesidad también el obtener un informe detallado acerca del tráfico de la red, para constatar el correcto funcionamiento de los servidores y para identificar rápidamente el equipo que necesite algún tipo de soporte.

Luego del análisis realizado sobre la red dela Institución, hemos podido determinar las siguientes problemáticas:

- En base a la encuesta realizada al encargado del departamento de informática se determinó que no hay un control del ancho de banda en los equipos usados por el personal que labora en la institución, esto no garantiza el correcto desempeño de los sistemas que dependan de este servicio, como por ejemplo al servicio de internet el cual está dentro de los 10 Mb y en ocasiones éste es excedido por usuarios de la red.
- No existe un equipo que realice la función de cortafuego que se encargue de controlar el tráfico de datos que fluye desde y hacia la red de datos del GAD Municipal.
- Cada servidor tiene una configuración específica de seguridad, es decir no existe un equipo cuya finalidad sea brindar la seguridad a la intranet.
- Falta de un proceso de autenticación para los equipos; al no existir tal mecanismo se puede llegar a tener un grado de desconfianza de que el equipo al cual se está accediendo sea el auténtico.
- El servicio de resolución de nombres o DNS no cuenta con mecanismos que permitan la validación de sus registros y punteros, lo que beneficiaria haciendo más confiable el acceso a los servidores.
- La institución cuenta con un sistema de monitoreo de servicios de red básico el cual ayuda a identificar donde se realiza el mayor consumo de ancho de banda, pero no a identificar el estado actual de cada equipos en la red, por ejemplo si se presenta una baja de servicio, si está conectado a la red, entre otros.

Por tal motivo nosotros como egresados de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja hemos visto conveniente presentar el siguiente tema:

***"IMPLEMENTACIÓN DE PROTOCOLOS SEGUROS Y HERRAMIENTA DE MONITOREO PARA LA RED DE DATOS DEL GAD MUNICIPAL DE LOJA".***

## 3. Problema de Investigación

Una vez realizado el análisis de los problemas ya mencionados hemos concluido que el problema general de investigación a solucionar es:

***La seguridad lógica existente dentro de la institución no permite establecer comunicaciones seguras, es decir comprobar la integridad de la información desde los servidores a los clientes autorizados y verificar la autenticidad de los equipos, el sistema de monitoreo es básico, no brinda información en tiempo real tanto de los servicios como de los equipos correspondientes***.

## 4. Delimitación

### 4.1 Espacio

Una vez realizado los trámites legales y obtenidos su aprobación se podrá acceder al espacio destinado para realizar la investigación en el Centro de Datos del GAD Municipal de Loja.

### 4.2 Tiempo

El desarrollo del proyecto de investigación, tiene una planificación de acuerdo a los parámetros a realizarse que se detallan en el cronograma de actividades con duración de 14 meses tomando en cuenta los días laborables de la institución, en el período comprendido entre Febrero 2013 a Abril 2014.

### 4.3 Unidades de Observación

Dentro del marco de contexto de la elaboración de un proyecto investigativo y de desarrollo existen actividades que ameritan un seguimiento detallado sobre su funcionamiento y desempeño para su implantación, el mismo que debe ser el deseado para garantizar la seguridad.

El presente trabajo investigativo tiene las siguientes unidades de observación:

- Testeo de herramientas libres para el desarrollo del proyecto.
- Protocolos de red orientados a seguridad: SSL, TLS, IPSec, DNSSec.
- Métodos de autenticación como certificados SSL, pares de llaves.
- Herramientas de monitoreo.

Así mismo se ha desarrollado las siguientes fases para ayudarnos a alcanzar los objetivos propuestos:

- **Fase 1: Diagnóstico de la situación actual.**

Una de las metas de esta fase es conocer la infraestructura de la red de datos de la institución eso nos ayudará a estimar la carga de datos de la institución. Mediante el uso de herramientas libres determinaremos las vulnerabilidades encontradas en los distintos servidores y respectivos servicios. Al final de esta fase el respectivo informe nos dará la perspectiva de la situación real de la red de datos.

- **Fase 2: Desarrollo de la solución planteada.**

En esta etapa del proyecto, se configurará equipos para simular la red de datos de la institución para ello usaremos herramientas de virtualización, distribuciones Linux como Debian, se probará los distintos protocolos seguros como SSL, TLS, IPSec y DNSSec para determinar cuáles se adaptan a las necesidades de la institución. Por otra parte se evaluará las herramientas de monitoreo para establecer la más apta para la institución.

- **Fase 3: Implantación de la solución.**

Luego de las configuraciones y pruebas realizadas en la fase anterior, se procederá a realizar las configuraciones en los equipos reales de la red de datos de la institución con el propósito de controlar el óptimo rendimiento de la solución en los equipos involucrados.

- **Fase 4: Evaluación y Pruebas de la solución.**

En esta fase se realizará las pruebas concernientes con la solución ya implantada a fin de mitigar las amenazas, luego de esto realizaremos una nueva búsqueda de vulnerabilidades para realizar un informe de la situación antes y después de implantada la solución.

## C. Justificación

La Universidad Nacional de Loja busca dar solución a problemas reales que afectan a nuestra sociedad en el ámbito tecnológico mediante los conocimientos adquiridos en los talleres concernientes a los tópicos de redes y comunicación de la malla curricular de la carrera de Ingeniería en sistemas, entre otros. En el presente proyecto se busca dar solución a problemas de seguridad en la red de datos del GAD Municipal de Loja, mediante el uso de herramientas de software libre de acuerdo al decreto 1014 estipulado en la constitución ecuatoriana. Además, este proyecto está encaminado a afianzar aspectos como, conocimientos académicos, formación tanto profesional como intelectual y obtener experiencia en el campo laboral, y de esta manera contribuir directamente al desarrollo de una sociedad académica, productiva y profesional.

El presente proyecto se justifica económicamente porque la institución brindará los equipos necesarios para la implementación de la solución planteada, y en cuestión de herramientas de software se utilizará aplicaciones bajo licencia GPL y de código abierto. Así mismo este proyecto será de gran aporte a la solución de los problemas de seguridad en la red de datos del GAD Municipal de Loja, además la institución brinda el apoyo necesario para el desarrollo del proyecto en sus instalaciones.

Se cuenta con el apoyo concerniente a equipos informáticos y de red que nos brinda la institución y asesoría del administrador de la red, se cuenta con la experiencia y asesoramiento de los docentes de la carrera de Ingeniería en Sistemas de nuestra prestigiosa institución de educación superior.

Para la realización del presente proyecto el grupo de investigación cuenta con los medios técnicos en material de estudio (computadoras, impresora, etc.) y herramientas basadas en software libre necesarias, que se usarán a lo largo del desarrollo del proyecto. Además es factible de realizar porque se accederá a diversos medios de consultas bibliográficas como libros, recursos de internet, etc. con la finalidad de obtener la información necesaria que permita sustentar este proyecto.

**Viabilidad**

El presente proyecto de investigación se lo considera viable porque se cuenta con los medios técnicos, tecnológicos y recursos económicos, que se requiere para la realización. Así mismo se cuenta con la guía de los docentes de la carrera y del director del proyecto.

De la misma manera se habló con los responsables de la red de datos del GAD Municipal de Loja, se obtuvo el permiso respectivo para la realización del proyecto dentro de sus instalaciones.

## D. OBJETIVOS

### 1. Objetivo General:

Implementar el Sistema de Monitoreo y el establecimiento de protocolos para mejorar la seguridad de las comunicaciones en la de red de datos del GAD Municipal de Loja.

### 2. Objetivo Específicos:

- Analizar la infraestructura de la red en lo que refiere a equipamiento actual de la institución.
- Realizar las pruebas de vulnerabilidades que presenta la red de datos de la institución, para generar un informe del estado actual de la misma.
- Analizar las posibles soluciones encaminadas al proyecto planteado, tanto para el uso de protocolos seguros como herramienta de monitoreo.
- Configuración y pruebas en un entorno controlado de los protocolos seguros y herramienta de monitoreo en la red de datos de la institución.
- Implantar la solución que mejor se adapte a las necesidades de la institución, en cuanto a protocolos seguros y herramienta de monitoreo.
- Evaluar el rendimiento de la solución.
- Capacitar en el uso de las herramientas implantadas, así como la correcta gestión de las mismas, a los encargados del departamento de redes del GAD Municipal de Loja.
- Elaboración del manual de usuario de las soluciones implantadas.

## E. METODOLOGÍA

### 1. Métodos

El desarrollo del proyecto requiere seguir los lineamientos de ciertos métodos, así como de técnicas e instrumentos que permitan la recopilación y análisis de la información necesaria para la presentación del proyecto de tesis, tales como:

- **Método Inductivo.-**Con base al análisis de los problemas encontrados y con la ayuda de este método se pudo determinar cuál es el problema general de investigación.
- **Método Deductivo.-**Una vez determinado el problema general de investigación. Este método nos ayudó a definir los objetivos específicos a obtenerse para dar solución a los problemas encontrados en la red de datos.
- **Método Analítico.-**Al momento de obtener información de la situación actual de la red de datos de la institución se elaboró un listado de los problemas que ésta presenta, este método nos ayudó a determinar cuáles son las posibles causas de los problemas y las consecuencias que se darían al no realizar las correcciones debidas del problema general de investigación.

### 2. Metodología de Desarrollo

Para la implantación del presente proyecto no se cuenta con una metodología previamente establecida es por esto que hemos creído conveniente la elaboración de las siguientes fases para el desarrollo del proyecto.

- **Fase 1: Diagnóstico de la situación actual.**

En esta fase se obtendrá toda la información necesaria para determinar la situación real de la red de datos de la institución.

- **Fase 2: Desarrollo de la solución planteada.**

En esta fase se realizará las configuraciones y pruebas necesarias tanto de los protocolos seguros como la herramienta de monitoreo en un entorno controlado en el Centro de Datos del GAD Municipal de Loja, para su posterior implantación.

- **Fase 3: Implantación de la solución.**

En esta fase final se implanta la solución obtenida en la fase anterior, en la red de datos del GAD Municipal de Loja.

- **Fase 4: Evaluación y Pruebas de la solución.**

En esta fase se realizará las pruebas necesarias a fin de determinar el correcto funcionamiento de la solución.

**3. Técnicas e instrumentos.**

Los métodos e instrumentos que se utilizarán para la recopilación de la información son los siguientes:

- **Lectura comprensiva:** Consiste en obtener un conocimiento ordenado y sistemático de un aspecto de la realidad o de los acontecimientos hecho o ideas relacionadas con el tema específico.

- **Entrevista:** Esta técnica nos permitió obtener información en detalle del software que se está utilizando para la administración de la red de datos, así mismo permitió elaborar un análisis preliminar, a través de preguntas a los encargados de la red de datos del GAD Municipal de Loja.

## F. MARCO TEÓRICO.

## Capítulo 1

### 1. Conceptos de seguridad.

#### 1.1. Definición de seguridad informática.

La seguridad es una característica de cualquier sistema, la cual nos indica que el sistema está libre de todo peligro, daño o riesgo. En el caso de redes de computadoras y los sistemas operativos, esta seguridad es difícil de conseguir, es por cuanto se adopta el término de fiabilidad, el cual expresa probabilidad de que un sistema se comporte tal como se espera.

Mantener un sistema fiable, debe contemplar aspectos básicos como: confidencialidad, integridad y disponibilidad. La confidencialidad indica que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ellos, y que los mismos no han de convertir dicha información en disponible para otras entidades, mientras que dentro de la integridad los objetos solo pueden ser modificados por elementos autorizados, en tanto que la disponibilidad nos dice que los objetos tienen permanecer accesibles a elementos autorizados.

#### 1.2. Importancia de la seguridad lógica.

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cuál será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa específico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno. [1]

### 1.3. Impacto en la organización.

La seguridad informática juega un papel importante dentro de las organizaciones, así mismo experimentan dificultades para lograr una adecuada gestión de seguridad, entre ellas podemos mencionar.

**a. Limitación en los programas de seguridad.**

A la hora de diseñar e implementar soluciones de negocios y dar soporte a los procesos de negocio, las organizaciones no cuentan con un enfoque sistemático dirigido a la administración de los riesgos de seguridad. [2]

**b. Desconexión entre las expectativas y la solución implementada.**

El interés en la seguridad de la alta gerencia está enfocado en mejorar el cumplimiento, mejorar el control, sin embargo, las soluciones de seguridad siguen enfocadas a la tecnología, son puntuales y reactivas al negocio. [2]

c. **Un programa de seguridad “Corporativo” requiere un enfoque verdaderamente integrado.**

Que vincule los aspectos técnicos, organizacionales, administrativos y medidas físicas en forma estratégica para responder a los distintos escenarios de riesgos. [2]

### 1.4. Vulnerabilidades en la red de datos.

Las vulnerabilidades son riesgos asociados con el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

#### 1.4.1. Ataques informáticos.

Los ataques son perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas [3], tales como:

a. **Ingeniería Social**

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente, puede engañar fácilmente a un usuario (que desconoce las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords.

Por ejemplo, suele llamarse a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. O bien, podría enviarse un mail (falsificando la dirección origen a nombre del administrador) pidiendo al usuario que modifique su password a una palabra que el atacante suministra.

Para evitar situaciones de IS es conveniente tener en cuenta estas recomendaciones:

- Tener servicio técnico propio o de confianza.
- Instruir a los usuarios para que no respondan ninguna pregunta sobre cualquier característica del sistema y deriven la inquietud a los responsables que tenga competencia para dar esa información. [3]

**b. Ingeniería Social Inversa.**

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en Ingeniería Social.

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechara esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).

La ISI es más difícil de llevar acabo y por lo general se aplica cuando los usuarios están alertados de las técnicas de IS. Puede usarse en algunas situaciones específicas y después de mucha preparación e investigación por parte del intruso:

- Generación de una falla en el funcionamiento normal del sistema. Generalmente esta falla es fácil de solucionar pero puede ser difícil de encontrar por los usuarios inexpertos (sabotaje). Requiere que el intruso tenga un mínimo contacto con el sistema.
- Comunicación a los usuarios de que la solución es brindada por el intruso (publicidad).
- Provisión de ayuda por parte del intruso encubierto como servicio técnico. [3]

### 1.4.2. Cambiando la petición de dirección

Es una práctica común para los clientes hacer uso de un servidor de almacenamiento en caché de nombres de dominio, que hace todo el trabajo de resolver ya que mantiene las respuestas en un sistema de cache para que puedan ser reutilizados por otros clientes. Este servidor DNS está en contacto con los clientes que están realizando consultas de manera frecuente, por lo que su caché es una herramienta ideal para reducir los accesos y peticiones a los servidores DNS principales, con lo que los clientes obtienen sus resultados más rápidamente, y los servidores DNS tienen menos carga de trabajo.

Pero imagina que fuese posible engañar al servidor de almacenamiento falsificando esa caché de nombres de dominio haciéndole al servidor aceptar una respuesta incorrecta, esta respuesta incorrecta, podría terminar en su caché y la serviría a todos los clientes que soliciten la misma dirección hasta que el tiempo de vida (TTL) de la respuesta incorrecta se agote. Como resultado, los usuarios podrían ser enviados a una dirección equivocada, a un sitio web con malware, sus e-mails pueden ser enviados a la dirección equivocada y hasta sus llamadas telefónicas pueden ser interceptadas, y si se hace correctamente, lo peor es que los usuarios no pueden percibir la diferencia entre la dirección correcta o incorrecta. [4]

Esta posible infección de la cache es posible en los actuales sistemas de nombres de dominio, cuando una resolución de un nombre de dominio envía una solicitud, es posible que un atacante envíe una respuesta errónea a dicha resolución. Si el atacante ofrece una respuesta aceptable con la suficiente rapidez, la resolución va a aceptar la respuesta. Ahora bien, este ataque sólo es posible si el atacante intercepta la solicitud original o genera la solicitud él mismo y solo tendrá éxito en ofrecer la respuesta falsa en la resolución si la envía antes de que lo realice el servidor autorizado, en la figura 1 se ilustra el proceso de suplantación.

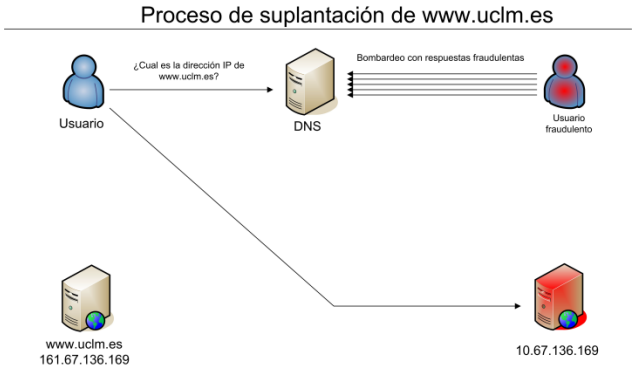



**Figura 127: Proceso de suplantación**

### 1.4.3. Ataque Kaminsky

El secuestro o falsificación de un dominio se conoce como el ataque Kaminsky. La vulnerabilidad descubierta por Dan Kaminsky da una vuelta de tuerca más al procedimiento anterior creando una respuesta fraudulenta que nos permite secuestrar el Authoritative nameserver y por tanto todo el dominio, no solo una entrada en la cache del servidor tal como lo muestra la figura 2.

El primer paso consiste en configurar un servidor de DNS que realice las funciones de Authoritative nameserver del dominio a secuestrar, obviamente en este DNS fraudulento tendremos configurados todos los registros (RR) de forma que se resuelvan a direcciones IP incorrectas deseadas que contienen webs o servicios que queremos secuestrar.

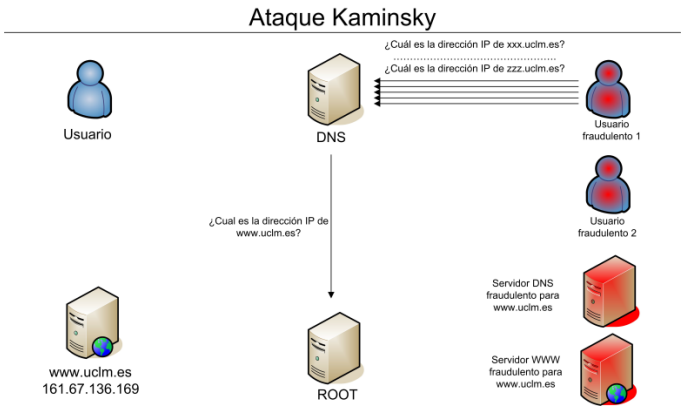



**Figura 128: Ataque Kaminsky**

En este proceso, los servidores de nombres pueden responder a un cliente que no saben la respuesta con lo que envían al cliente a realizar la consulta a otro servidor. La

información que es proporcionada por el servidor de nombres es la información llamada "autoridad". El servidor de nombres indica "No estoy autorizado para el dominio que estás buscando, pero este es otro servidor que si está autorizado", a continuación, indica el nombre y la dirección de este servidor de nombres autorizado como parte de la respuesta a la consulta. La respuesta a cada consulta consta de tres partes:

- La respuesta a la consulta (puede estar en blanco si la consulta no puede ser respondida).
- Autoridad de la información (que está autorizada para el dominio que se consulta).
- Información adicional (la información de la dirección de los servidores autorizados).

Es fácil ver cómo esto puede ser objeto de abuso: el atacante puede intentar responder antes de que el servidor pueda responder a los clientes que enviaron la solicitud. Si el atacante tiene éxito, se pueden suministrar servidores falsos, a todas las solicitudes que recibe (es decir, sustituye la "información adicional" de la respuesta con información falsa sobre su servidor).

Acerca de este ataque indicamos tres características importantes:

- El atacante puede llevar a cabo este ataque en cualquier momento. El atacante se limita a realizar consultas, al servidor de almacenamiento de caché del servidor de nombres que quiere falsear con nombres de host (inexistentes) en la memoria caché. El servidor de nombres atacado al no tener estos nombres en memoria cache enviará esta solicitud de resolución, dando al atacante la oportunidad de insertar sus propias respuestas incorrectas que luego serán almacenadas automáticamente en la memoria caché.
- Este ataque secuestra o falsea todo un dominio en vez de un nombre de host solamente.

Además el atacante normalmente establecerá en la respuesta falsa un tiempo de vida largo, para asegurarse de que permanece en la memoria caché durante mucho tiempo. Una vez que todo el dominio ha sido secuestrado todo el tráfico puede ser redireccionado, páginas web, servicios, correo electrónico, etc.

Este ataque no puede ser mitigado mediante la protección de su sitio web usando SSL (https) con lo que es trivial para un atacante redirigir a los usuarios a un sitio seguro SSL que puede parecer completamente válido desde el punto de vista del usuario. [5]

### 1.4.4. Agujeros de Seguridad.

Los agujeros de seguridad a nivel de software se dan cuando el problema está causado por una mala escritura de partes "privilegiadas" de software (daemons, cronjobs) que pueden estar comprometidos a realizar tareas que no deberían.

Nuevos agujeros aparecen todo el tiempo, y las mejores alternativas son:

- Tratar de estructurar tu sistema de forma que el menor software posible con privilegios root/daemon/bin corra en tu máquina.
- Suscribirse a una lista de mail para poder tener lo antes posible información con detalles acerca de problemas relacionados con la seguridad.
- Cuando se instale o actualiza un sistema dado, trata de instalar/habilitar solo aquellos paquetes de software por los que tengas una necesidad inmediata o previsible. Muchos paquetes incluyen daemons o utilidades que pueden revelar información a extraños.

Una administración del sistema cuidadosa es la solución. Muchos de estos programas son inicializados en el arranque; para ello se cambia los scripts de arranque (normalmente en los directorios /etc, /etc/rc) para prevenir su ejecución. Así mismo se debe eliminar algunas utilidades completamente.

### 1.4.5. Exploits y Payloads.

Un **exploit** es un programa o código que "explota" una vulnerabilidad del sistema o una parte de él para aprovechar esta deficiencia en beneficio.

Si bien el código que explota la vulnerabilidad no es un código malicioso en sí mismo, generalmente se lo utiliza para otros fines como permitir el acceso a un sistema o como parte de otros malware como gusanos y troyanos.

Es decir que actualmente, los exploits son utilizados como "componente" de otro malware ya que al explotar vulnerabilidades del sistema permite hacer uso de funciones que no estarían permitidas en caso normal.

Existen diversos tipos de exploits dependiendo las vulnerabilidades utilizadas y son publicados cientos de ellos por día para cualquier sistema y programa existente pero sólo una gran minoría son utilizados como parte de otros malware [6].

Un **payload** se refiere a los efectos destructivos, nocivos o molestos que cualquier virus puede producir cuando ya ha tenido lugar su infección, además de los efectos secundarios de dicha infección (cambios en la configuración del sistema, reenvío de e-mail, ejecución del virus en el arranque del sistema o de Windows, etc).

### 1.5. Test de Penetración.

Un Penetration Testing o Test de Penetración, es un procedimiento metodológico y sistemático en el que se simula un ataque real a una red o sistema, con el fin de descubrir y reparar sus problemas de seguridad.

Existen diferentes metodologías para realizar un test de penetración, una de las más famosas por ser gratuita y abierta es la OSSTMM (Open Source Security Testing Methodology Manual) del instituto para la seguridad y las metodologías abiertas ISECOM, también están herramientas como la guía de pruebas OWASP, que está enfocada a la auditoria de aplicaciones web o ISSAF (Information Systems Security Assassment Framework) o el Penetration Testing Framework de Vulnerability Assessment que además de mostrarnos la metodología a seguir, nos sugieren herramientas para realizar cada una de las etapas del Pentest. [7]

## Capítulo 2

## 2. Conceptos básicos de protocolos de red.

### 2.1. Modelo OSI.

A la hora de describir la estructura y función de los protocolos de comunicaciones se suele recurrir a un modelo de arquitectura desarrollado por la ISO (International Standards Organization). Este modelo se denomina Modelo de Referencia OSI (Open Systems Interconnect).

El modelo OSI está constituido por 7 capas que definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia, la figura 3 ilustra las capas del modelo OSI. [8]

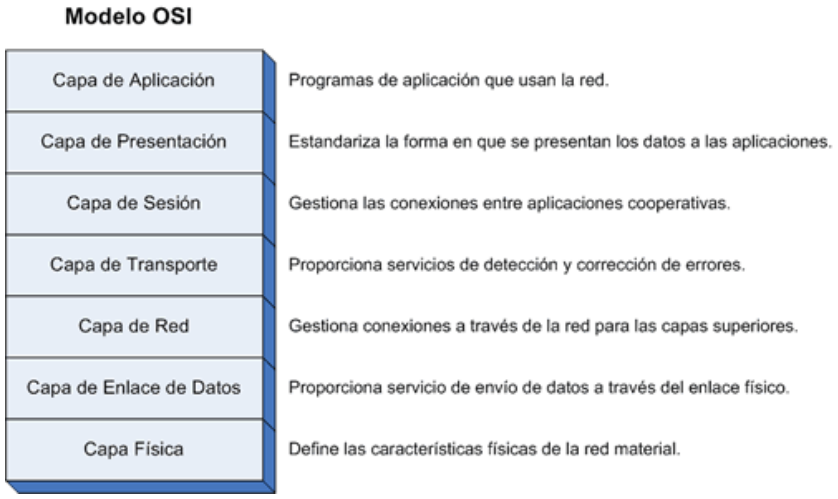



**Figura 129: Modelo OSI**

Las capas se pueden dividir en dos grupos:

a. Servicios de transporte (niveles 1, 2, 3 y 4).S
b. Servicios de soporte al usuario (niveles 5, 6 y 7).

El modelo OSI está pensado para las grandes redes de telecomunicaciones de tipo WAN.

No es un estándar de comunicaciones ya que es un lineamiento funcional para las tareas de comunicaciones, sin embargo muchos estándares y protocolos cumplen con los lineamientos del modelo. [9]

### 2.1.1. Descripción de las capas

**Aplicación:** Es la capa más cercana al usuario, no provee servicios a ninguna otra capa del modelo OSI, lo que hace es proporcionar servicios de red a las aplicaciones de usuario.

**Presentación:** Está a cargo de la presentación de los datos en una forma que el dispositivo receptor pueda comprender. Define el formato en que se intercambia la información entre aplicaciones.

**Sesión:** Se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos. Permite asegurar la sesión establecida, reanudándolas en caso de interrupción y también se haya a cargo de la transmisión ordenada de los datos.

**Transporte:** Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino. La unidad de dato de protocolo es el Segmento o Datagrama.

**Red:** Se encarga de identificar el enrutamiento existente entre una o más redes. El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino. Las unidades de información se denominan paquetes. [10]

**Enlace de datos:** Toma la información la filtra de errores y luego la divide en tramas y la dirige de forma secuencial para la capa de red.

Se encarga también de:

**a.** Direccionamiento físico
**b.** Topología de la red
**c.** Acceso al medio
**d.** Detección de errores
**e.** Distribución ordenada de tramas
**f.** Control del flujo.

**Física**

Es la que se encarga de:

**a.** Las conexiones físicas de la computadora hacia la red.

**b.** Definir el medio o medios físicos por los que va a viajar la comunicación.

**c.** Definir las características materiales y componentes para la transmisión de datos.

**d.** Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

**e.** Transmitir el flujo de bits a través del medio.

**f.** Manejar las señales eléctricas del medio de transmisión.

**g.** Garantizar la conexión.

El diseño de la arquitectura de comunicaciones del modelo OSI se muestra en la siguiente figura 4.

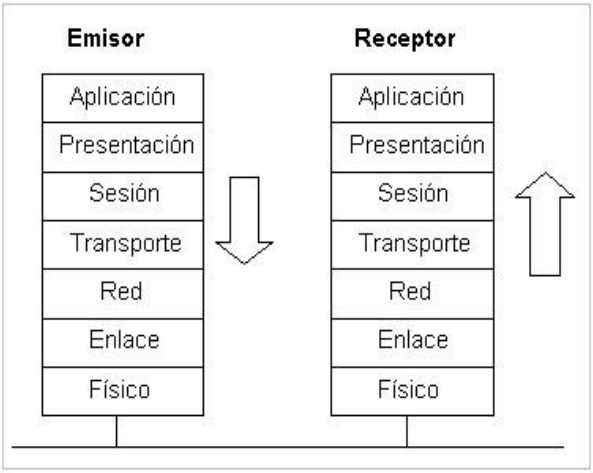



**Figura 130: Arquitectura de Comunicación del Modelo OSI**

### 2.2. Aproximación al modelo de arquitectura de los protocolos TCP/IP.

El modelo de arquitectura de estos protocolos es más simple que el modelo OSI, como resultado de la agrupación de diversas capas en una sola o bien por no usar alguna de las capas propuestas en dicho modelo de referencia.

Así, por ejemplo, la capa de presentación desaparece pues las funciones a definir en ellas se incluyen en las propias aplicaciones. Lo mismo sucede con la capa de sesión, cuyas funciones son incorporadas a la capa de transporte en los protocolos TCP/IP. Finalmente la capa de enlace de datos no suele usarse en dicho paquete de protocolos.

De esta forma nos quedamos con una modelo en cuatro capas, tal y como se ve en la figura 5:

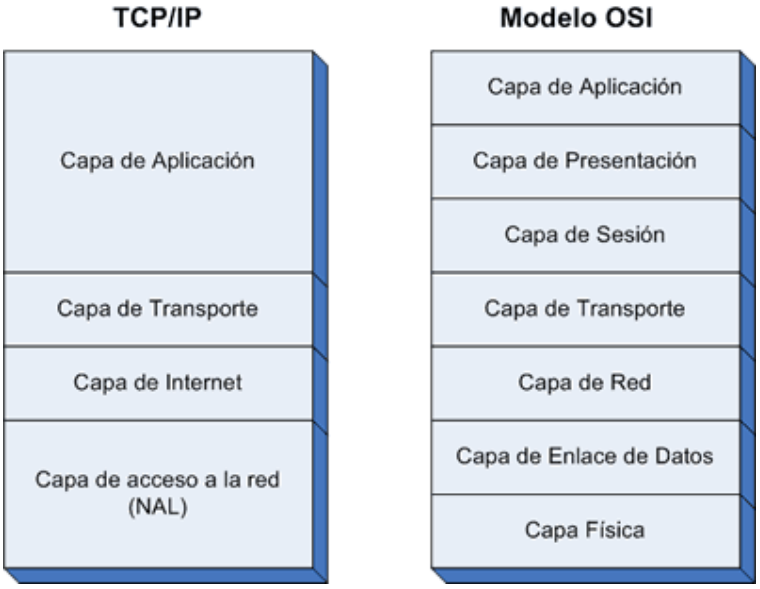



**Figura 131: Modelo TCP/IP y Modelo OSI**

Al igual que en el modelo OSI, los datos descienden por la pila de protocolos en el sistema emisor y la escalan en el extremo receptor. Cada capa de la pila añade a los datos a enviar a la capa inferior, información de control para que el envío sea correcto. Esta información de control se denomina cabecera, pues se coloca precediendo a los datos. A la adición de esta información en cada capa se le denomina encapsulación. Cuando los datos se reciben tiene lugar el proceso inverso, es decir, según los datos ascienden por la pila, se van eliminando las cabeceras correspondientes, tal como se muestra en la figura 6.

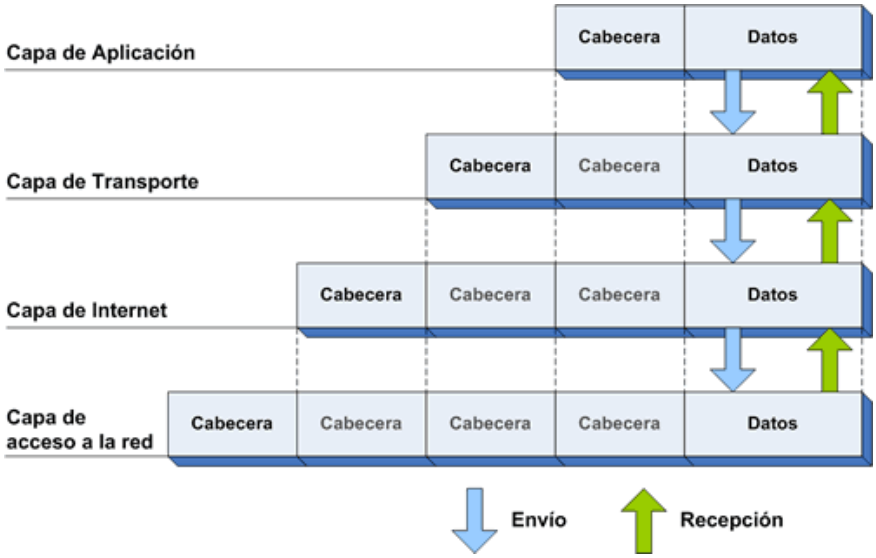



**Figura 132: Envío y Recepción según el Modelo TPC/IP**

Cada capa de la pila tiene su propia forma de entender los datos y, normalmente, una denominación específica que podemos ver en la figura 7. Sin embargo, todos son datos a transmitir, y los términos solo nos indican la interpretación que cada capa hace de los datos. [8]

| | TCP | UDP |
|---|---|---|
| Capa de Aplicación | Flujo | Mensaje |
| Capa de Transporte | Segmento | Paquete |
| Capa de Internet | Datagrama | Datagrama |
| Capa de Acceso a la Red | Trama | Trama |

**Figura 133: Datos asociados con cada Capa y según el Modelo**

### 2.3. Protocolo IP.

Internet Protocol (en español Protocolo de Internet) o IP es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados no fiable y de mejor entrega posible sin garantías.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de

que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

IP provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (best effort), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de cómo estén de congestionadas las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

El IP es el elemento común en la Internet de hoy. El actual y más popular protocolo de red es IPv4. IPv6 es el sucesor propuesto de IPv4; poco a poco Internet está agotando las direcciones disponibles por lo que IPv6 utiliza direcciones de fuente y destino de 128 bits (lo cual asigna a cada milímetro cuadrado de la superficie de la Tierra la colosal cifra de 670.000 millones de direcciones IP), muchas más direcciones que las que provee IPv4 con 32 bits. Las versiones de la 0 a la 3 están reservadas o no fueron usadas. La versión 5 fue usada para un protocolo experimental. Otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos. [11]

## 2.4. Sistema de Nombre de Dominio DNS.

### 2.4.1. Historia

Cuando Internet fue creado cada nodo de la red necesitaba tener su propia dirección, por ese motivo se definió la dirección IP.

Quienes comenzaron a trabajar en Internet pronto se encontraron con el problema de una falta de estructura lógica entre los sistemas informáticos con las direcciones IP y se optó por una solución simple: crear un archivo que asigne una dirección IP a un nombre lógico. Este archivo se llama 'hosts' archivo que contenía una lista de hosts conectados a la red [12]. Un ejemplo de un archivo hosts se muestra en la figura 8.

| | |
|---|---|
| 161.67.136.169 | www.uclm.es |
| 161.67.136.47 | webmail.alu.uclm.es |
| 161.67.136.150 | campusvirtual.uclm.es |
| ... | ... |

**Figura 134: Archivo host de nombres de Dominio**

### 2.4.2. El propósito de DNS

Internet es la red más grande del mundo, desde la perspectiva de un usuario, cada nodo o recurso en la red se identifica por un nombre único: el nombre de dominio.

Para alcanzar un ordenador o cualquier otro recurso de una red, es necesaria alguna forma de indicar el destino, esto se consigue asignando direcciones de red. La dirección de red debe de ser única para poder encaminar correctamente los paquetes de un host o router a otro. Esta dirección está formada por un identificador numérico el cual los routers o cualquier dispositivo de red puedan entender y procesar. Desde la perspectiva de los dispositivos de red (por ejemplo, routers) que solo encaminan paquetes a través de Internet, son solo transacciones de paquetes. Pero desde la perspectiva del usuario para acceder a los recursos de internet se utilizan los nombres de dominio, los usuarios necesitan un sistema que traduzca los nombres de dominio a direcciones IP y viceversa. Esta traducción es la tarea principal del Domain Name System (DNS). [13]

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

En respuesta a la rápida expansión de Internet, incrementando cada día el número de direcciones IP del espectro normalizado, se introdujo el servicio de nombres de dominio DNS en 1983 para poder gestionar de manera eficiente el direccionamiento.

El sistema de nombres de dominio es un sistema jerarquizado, es decir, existe un dominio raíz (representado por un solo punto "."), un conjunto de dominios de primer

nivel, como .com o .es, y cualquier número de niveles debajo de estos dominios. La figura 9 muestra un ejemplo de la jerarquía de nombres de dominio.

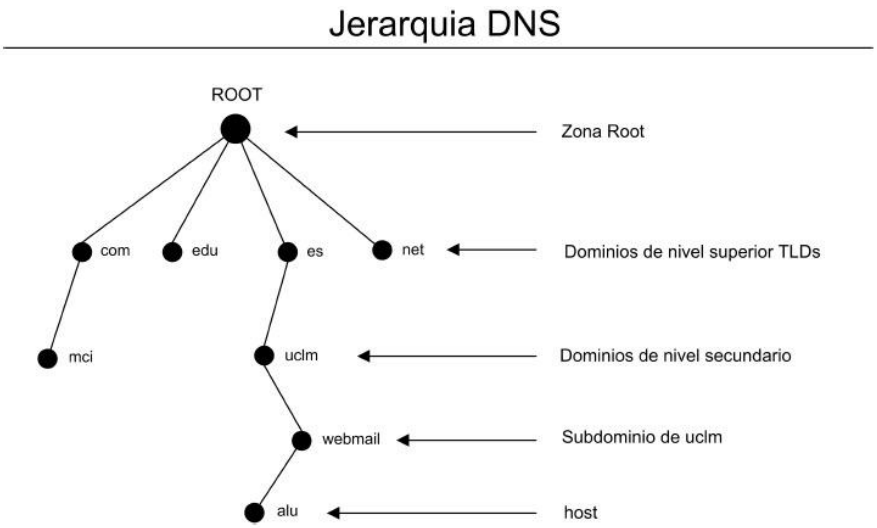



**Figura 135: Jerarquía DNS**

La zona de la parte superior de la jerarquía (el dominio ".") se llama la zona root o zona raíz. Las entradas de esta zona son los dominios de nivel superior (Top Level Domains, TLDs). Existen dominios de primer nivel como .com para empresas, .edu para instituciones educativas y dominios genéricos de nivel superior formado por el código de país.

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

DNS convierte nombres de máquina a las direcciones IP que tienen todas las máquinas de la red y traduce o relaciona nombres con direcciones y direcciones con nombres. [14]

## Capítulo 3

### 3. Tecnologías de cifrado de comunicaciones.

#### 3.1. Tecnología SSL.

**Secure Sockets Layer (SSL)** es el estándar mundial de la seguridad en Internet, SSL se convirtió en el estándar hace una década para garantizar la privacidad de las comunicaciones en línea. El proceso consiste en crear un archivo de datos especial llamado certificado SSL para un servidor específico en un dominio y para una entidad concreta. De forma similar a un pasaporte o un permiso de conducir, los certificados SSL son emitidos por entidades de confianza como VeriSign. Todas las entidades que reciben un certificado SSL se deben someter a algún tipo de autenticación que permita comprobar que son quienes dicen ser.

Con el aumento considerable del phishing y otras actividades fraudulentas en Internet, la autenticación de la identidad se convierte en un aspecto más importante que nunca. El nivel de autenticación de la identidad de un certificado SSL varía según el tipo de certificado SSL y la autoridad de certificación (CA).

Con SSL, un sistema de claves privadas o públicas cifra la conexión entre dos partes como, por ejemplo un usuario y un sitio Web con un certificado SSL. Si el explorador del cliente señala un sitio Web con SSL, un protocolo de enlace seguro entre ambos sistemas autentica ambas partes. En cada sesión se usa una clave de sesión única para el cifrado (cuanto más larga sea la clave, mayor será el nivel de cifrado). Una vez establecida la conexión, ambas partes pueden iniciar una sesión segura a la vez que garantizan la privacidad e integridad de sus comunicaciones. Esta seguridad es especialmente importante si los usuarios comparten información confidencial en Internet, una extranet o incluso en una intranet. En el caso del comercio electrónico, una conexión SSL segura es fundamental para hacer negocios, ya que la mayoría de los usuarios de Internet temen compartir la información con un sitio Web que no ofrezca protección SSL. [15]

#### 3.2. Tecnología IPSec

IPSec (Internet Protocol Security), es una extensión del protocolo IP y un conjunto de protocolos cuya función es asegurar las comunicaciones sobre IP. Fue diseñado en un

principio para IPv6, pero luego fue portado a IPv4, pudiendo se utilizar en ambas versiones del protocolo IP.

IPSec tiene la capacidad de proporcionar seguridad a protocolos de capas superiores dentro del modelo OSI/ISO. Otros protocolos como SSH, SSL, TLS operarán en capas superiores a la capa 3 del modelo OSI de ISO. Como también es el caso de TCP y UDP, protocolos de transporte, ya que estos son encapsulados por la capa tres donde actúa IPSec. Para entender mejor esto veamos un detalle del modelo de referencia OSI de ISO y el modelo TCP/IP [16], tal como lo muestra la figura 10.


**Figura 136: Modelo OSI y Modelo TCP/IP**

En cualquier escenario en el que haya una red, el concepto de enrutador está implícito, como en Huésped-a-Enrutador (y este enrutador controla y cifra el tráfico para una Red particular).

Como puede ver, IPSec se puede usar como túnel de tráfico para conexiones de «Redes Privadas Virtuales» (VPN, "Virtual Private Networks"). Sin embargo, su utilidad va más allá de las VPNs. Con un registro central de «Intercambio de Claves de Internet» (IKE, "Internet Key Exchange"), cada máquina en internet podría comunicarse con otra y usar cifrado y autenticación fuerte.

### 3.2.1. Propósito de IPSec

El protocolo de internet, IP, también conocido como IPv4, no provee por sí mismo de ninguna protección a sus transferencias de datos. Ni siquiera puede garantizar que el remitente sea quien dice ser. IPSec intenta remediarlo. Estos servicios vienen tratados

como dos servicios distintos, pero IPSec ofrece soporte para ambos de un modo uniforme.

- **Confidencialidad**

Asegura de que sea difícil para todos comprender qué datos se han comunicado, excepto para el receptor. No querrá que nadie vea sus contraseñas cuando ingrese en una máquina remota a través de Internet.

- **Integridad**

Garantiza que los datos no puedan ser cambiados en el camino. Si se encuentra en una línea que lleve datos sobre facturación, seguro que querrá estar seguro de que las cantidades y cifras de contabilidad son las correctas, y que no han podido ser alteradas durante el tránsito.

- **Autenticidad**

Firma sus datos de modo que otros puedan verificar que es realmente Vd. quien los envió. Es agradable saber que los documentos no son falsos.

- **Protección a la réplica**

Necesitamos modos para asegurarnos de que una transacción sólo se puede llevar a cabo una vez, a menos que autoricemos que la repitan. Nadie debería poder grabar una transacción, y luego replicarla al pie de la letra, con el propósito que pareciera como si se hubieran recibido múltiples transacciones del remitente original. Imagine que el atacante deba conocer cuál es el motivo del tráfico por medios distintos al de poder descifrarlo, y que el tráfico causara sucesos favorables para él, como depositar dinero en su cuenta. Tendríamos que asegurarnos que no pudiera replicar ese tráfico más tarde. [17]

### 3.2.2. Protocolos detrás de IPSec

IPSec está formado por un conjunto de protocolos:

**a. AH**

AH provee autenticación, integridad, y protección a la réplica (pero no confidencialidad). Su principal diferencia con ESP es que AH también asegura partes de la cabecera IP del paquete (como las direcciones de origen o destino).

- Para la autenticación y protección de integridad se basa en algoritmos de cifrado con clave, siendo requeridos en todas las implementaciones HMAC-MD5 y HMAC-SHA1.
- En las cabeceras añadidas para AH, se incluyen el SPI, un número de secuencia antirrepetición de 4 bytes y los datos de autenticación obtenidos mediante el algoritmo de hash de cifrado.
- AH usa el número de protocolo IP 51, no obstante, si además incluye ESP usaría el 50.
- Puede ser interesante usar sólo AH para evitar la modificación de datos sin añadir sobrecarga por la encriptación de todo el payload.

**b. ESP**

ESP puede proveer autenticación, integridad, protección a la réplica, y confidencialidad de los datos (asegura todo lo que sigue a la cabecera en el paquete). La protección a la réplica requiere autenticación e integridad (éstas dos van siempre juntas). La confidencialidad (cifrado) se puede usar con o sin autenticación y/o integridad. Del mismo modo, puede usar la autenticación y/o la integridad con o sin la confidencialidad.

- En la cabecera ESP se incluyen el SPI, en número de secuencia antirrepetición y los datos de autenticación si se incluyen.
- Al menos se debe proporcionar cifrados DES-CBC de 56 bits.
- Nótese que ESP no cifra la cabecera del paquete IP, sólo el payload.
- El número de protocolo usado por ESP es el 50.

**c. IP payload compresión (IPcomp)**

Realiza la compresión antes de llevar a cabo la autenticación o cifrado antes de la autenticación o cifrado. No se debe comprimir en capas inferiores de nuevo los datos, ya que generalmente no reportará beneficios de tamaño, y sí degradación de rendimiento.

### d. Internet Key Exchange (IKE)

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las asociaciones de seguridad y rellena la SAD. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

El protocolo IKE funciona en dos fases. La primera fase establece un ISAKMP SA (Internet Security Association Key Management Security Association – Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPSec.

La autenticación de los participantes en la primera fase suele basarse en claves compartidas con anterioridad (PSK – Pre-shared keys), claves RSA y certificados X.509 (racoon puede realizar esta autenticación incluso mediante Kerberos).

La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque man-in-the-middle (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La ISAKMP SA proporciona autenticación para protegerse de ataques man-in-the-middle. Esta segunda fase emplea el modo rápido. [16]

### 3.2.3. Modos IPSec

El **modo transporte** es el que usa un anfitrión que genera los paquetes. En modo transporte, las cabeceras de seguridad se añaden antes que las cabeceras de la capa de transporte (v.g., TCP, UDP), antes de que la cabecera IP sea añadida al paquete. En otras palabras, un AH añadido al paquete cubrirá el resumen criptográfico de la cabecera TCP y algunos campos de la cabecera IP extremo-a-extremo, y una cabecera ESP cubrirá el cifrado de la cabecera TCP y los datos, pero no la cabecera IP extremo-a-extremo.

El **modo Túnel** se usa cuando la cabecera IP extremo-a-extremo ya ha sido adjuntada al paquete, y uno de los extremos de la conexión segura es solamente una pasarela. En este modo, las cabeceras AH y ESP se usan para cubrir todo el paquete, incluida la cabecera extremo-a-extremo, y se añade una nueva cabecera IP al paquete que cubre sólo el salto al otro extremo de la conexión segura (aunque eso puedan ser varios saltos de distancia), en la figura 11 se muestra de manera gráfica como es este proceso.

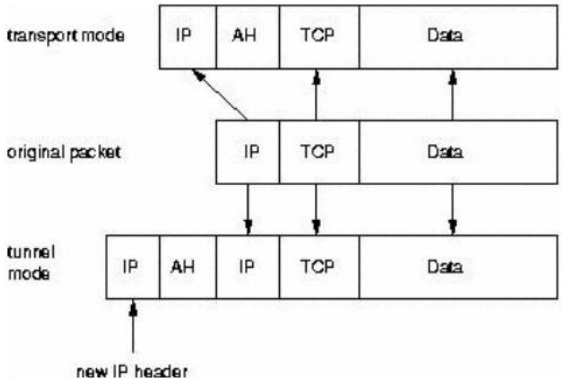



**Figura 137: Modo Túnel**

### 3.2.4. Security Associations (SA)

Los enlaces seguros de IPSec se definen en términos de «Asociaciones de Seguridad» (SAs). Cada SA viene definida por un único flujo unidireccional de datos, y por regla general (ignorando multicast) desde un único punto hasta otro, cubriendo el tráfico que se distingue por algún «selector único». Todo el flujo de tráfico sobre un único SA se trata del mismo modo. Algo del tráfico pueden estar sujetos a varios SAs, cada uno de los cuales aplica algún tipo de transformación criptográfica. Un grupo de

SAs se conoce como un «Haz» ("SA Bundle"). Los paquetes entrantes se pueden asignar a un SA particular por medio de los tres campos de definición:

«Dirección IP de destino» ("destination IP address").

«Índice del Parámetro de Seguridad» (SPI, "Security Parameter Index").

«Protocolo de seguridad» ("security protocol").

SPI se puede considerar como un "cookie" manejado por el receptor del SA, cuando se negocian los parámetros de la conexión. El protocolo de seguridad debe ser AH o ESP. Debido a que la dirección IP del receptor es parte del trío, ésta es un valor único garantizado. Se pueden encontrar desde la cabecera IP exterior y la primera cabecera de seguridad (que contiene el SPI y el protocolo de seguridad). [17]

**Security Policies**

- Las Security Policies almacenan información que determina que tráfico proteger y cuando; permitiendo tomar decisiones (descartar, pasar o aplicar IPSec) a paquetes específicos.
- Los SP se almacenan en la SP Database (SPD).
- La SPD almacena la política de protección, mientras que la SAD suministra los parámetros necesarios para establecerla.

**Procesado del Tráfico entrante y saliente**

- En el tráfico saliente, se utilizará primero la SPD para determinar qué hacer con el paquete. Luego si es necesario se consultará la SAD.
- En el tráfico entrante, IPSec consultará primero la SAD para verificar la identidad del remitente. Luego se accederá al SPD una vez verificada la identidad.

### 3.2.5. Intercambio de Claves

Podemos utilizar configuraciones estáticas, pero en implementaciones escalables, se suele usar el protocolo IKE para realizar un negociado dinámico de las claves, el cual consta de dos fases:

- Una primera fase donde se autentifican los extremos a través de ISAKMP (Internet Security Association Key Management Protocol), para poder realizar la segunda fase en un entorno seguro. Se pueden utilizar claves pre compartidas (PSK), algoritmos de clave pública o mediante firmas digitales.
- Una segunda fase, donde se negocian las SA de IPSec utilizadas para proteger el tráfico IP. Mientras que la primera fase se negocia con menos frecuencia (usualmente una vez a la hora o al día), la segunda fase se negocia frecuentemente (del orden de un minuto o cada 1024K datos cifrados).

Generalmente el negociado de IKE se realiza generalmente mediante protocolo UDP y el puerto 500, por lo que debemos permitir este tráfico en nuestro cortafuego.

### 3.2.6. Algoritmos de autentificación

AH lleva un campo (Integrity Check Value) para comprobar la integridad del paquete y que nadie lo ha manipulado durante el trayecto. El valor de ese campo está dado por algoritmos de encriptación tales como MD5 o SHA-1.

Más que usar un checksum convencional, el cual podría no proveer una seguridad real contra una manipulación intencional, esta usa una Hashed Message Authentication Code (HMAC), que incorpora una clave secreta mientras se crea el hash. Aunque un atacante puede recalcular un hash fácilmente, sin la clave secreta no sería capaz de crear el ICV apropiado.

HMAC está descrito por el RCF 2104 y se ilustra en la figura 12:

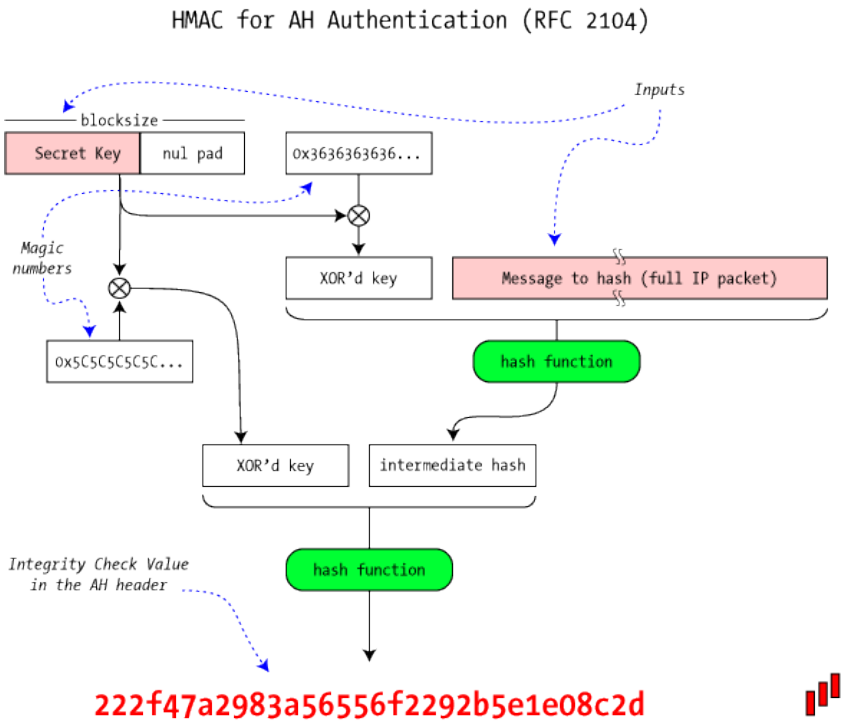



**Figura 138:** HMAC y RCF 2104

IPSec no define ni obliga como debe hacerse la autentificación, simplemente ofrece un marco de seguridad en la que los dos hosts que realizan la comunicación se ponen de acuerdo sobre qué sistema usar. Pueden usarse firmas digitales o funciones de encriptación, pero es obligatorio que ambos los conozcan y sepan cómo usarlos.

### 3.2.7. Otras características de IPSec

- IPSec soporta road warriors, donde no se especifican la ip de ciertos nodos con los que nos conectaremos, ya que éstos usan IP's dinámicas. Para ello las políticas se deben establecer para permitir direcciones desconocidas y usar un sistema de autenticación pre acordado.
- También se puede usar cifrado oportunista, donde aunque la autenticación no ha sido pre acordada, esta puede ser obtenida del servidor DNS. No obstante hasta la implantación de DNSSEC, esta solución no puede asegurar niveles de seguridad altos, debido a que se basa en confiar en los datos obtenidos del servidor DNS. [18]

### 3.2.8. Cuadro comparativo entre IPSec y SSL.

La siguiente tabla muestra algunos criterios importantes a ser tomados en cuenta a la hora de elegir tal a cual tecnología, dependiendo de las funcionalidades de la empresa.

| | SSL/TLS | IPSec |
|---|---|---|
| **Control de accesos** | | |
| **e.** Conexiones permanentes | | ✓ |
| **f.** Conexiones efímeras o puestos móviles | ✓ | |
| **g.** Ambos Tipos de acceso | ✓ | ✓ |
| **Usuarios** | | |
| **h.** Todos los usuarios son empleados de la compañía | | ✓ |
| **i.** No todos los usuarios son empleados de la compañía | ✓ | |
| **j.** No todos los usuarios son empleados de la compañía, además algunos trabajan con sus propios sistemas | ✓ | ✓ |
| **Software Cliente** | | |
| **k.** Todos los usuarios tienen acceso a todos los recursos de la red | | ✓ |
| **l.** Deseamos controlar el acceso a determinadas aplicaciones | ✓ | |
| **m.** Necesitamos niveles variables de control de acceso en las diferentes aplicaciones | ✓ | ✓ |
| **Confidencialidad y autenticidad** | | |
| **n.** Precisamos de un alto nivel de seguridad en el cifrado y autentificación | | ✓ |
| **o.** La confidencialidad y la autenticidad no son especialmente críticas en nuestros sistemas | ✓ | |
| **p.** Precisamos de niveles moderados de confidencialidad e integridad | ✓ | |

| Implantación, flexibilidad y escalabilidad | | |
|---|---|---|
| **q.** Deseamos una implantación rápida y de facilidad mantenimiento | ✓ | |
| **r.** Deseamos flexibilidad en las modificaciones futuras | | ✓ |
| **s.** Ambas consideraciones son importantes | ✓ | ✓ |

**Tabla 35: Cuadro Comparativo entre SSL/TLS e IPSec [19]**

### 3.3. Tecnología DNSSec.

El DNS fue diseñado durante los primeros años de Internet y durante esta época todos los usuarios pertenecían el sector académico, organizaciones militares y entusiastas de la informática, en los cuales, en general, se podía confiar. Todo aquello implicó que la seguridad no fuese uno de los principales objetivos de diseño del sistema de nombres de dominio. Como consecuencia, existen vulnerabilidades en el sistema (algunas de los cuales son incluso errores de diseño). La más importante vulnerabilidad se debe a que los servidores de nombres realizan consultas entre sí, sin un método seguro de verificación de los resultados obtenidos. Esto permite un tipo de ataque llamado “envenenamiento de cache”. [20]

#### 3.3.1. Resolver el problema DNSSec

La principal característica de DNSSec es la introducción de autenticación en las respuestas a consultas DNS. Esto se implementa mediante el uso de certificados digitales en la gestión de los dominios y subdominios.

Cada registro DNS es firmado usando algoritmos criptográficos, con lo que las resoluciones a consultas pueden comprobar estas firmas y así verificar la autenticación de la información facilitada. El algoritmo criptográfico deber ser suficientemente fuerte para prevenir un ataque que intente falsear un registro de DNS.

#### 3.3.2. DNSSec

DNSSec responde a “Domain Name System Security Extensions”. DNSSec es una extensión del protocolo DNS (RFCs 1034 y 1035) y es definido en varias especificaciones por la Internet Engineering Task Force (IETF).

En primer lugar, vamos a comentar lo que DNSSec no es. DNSSec no es una panacea de seguridad. No es una defensa sólida para parar todas las formas de ataque contra los servidores DNS. DNSSec no es una implementación que realice cifrado de datos DNS.

DNSSec es una especificación de una extensión de DNS a través de la definición de nuevos registros de recursos DNS que pueden ser utilizados por los clientes DNS para validar la autenticidad de una respuesta. La integridad de los datos de la respuesta DNS, donde la respuesta indica que no hay dominio o que el tipo de recurso existe o no, también se puede autenticar. En otras palabras, si un atacante intenta crear una respuesta DNS en la que ha alterado la respuesta original de alguna manera, mediante DNSSec se debe ser capaz de detectar esta acción, que la respuesta ha sido alterada y que la respuesta no corresponde a la información del DNS autorizado para dicha zona. En otras palabras, DNSSec se destina a proteger a los clientes de una posible falsificación de datos DNS. Esta protección no elimina la posibilidad de inyectar datos falsos en una operación de resolución de DNS, pero añade información adicional a las respuestas DNS para permitir a un cliente comprobar que la respuesta es auténtica y completa.

En reconocimiento de la urgente necesidad de una mayor seguridad para el actual sistema de nombres de dominio de Internet y el sistema de direcciones, las entidades que gestionan el sistema de nombres desean seguir adelante con la implementación de DNSSec tanto en la zona raíz como en el resto de dominios. Desde el 15 de Julio de 2010 a las 2050 UTC, entró en producción la primera zona firmada con el serial SOA 2010071501. Para facilitar un despliegue rápido de la manera más segura, es necesario coordinar el proceso de implementación con el proceso de gestión de la zona raíz existente y el resto de zonas secundarias, reduciendo al mínimo la introducción de nuevas medidas y cambios de responsabilidades entre las partes involucradas.

### 3.3.3. Seguridad basada en cifrado

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

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

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

### 3.3.4. Cadenas de confianza

La figura 13 muestra cada una de las calves de firma para cada nivel empezando por la raíz y los niveles del TLD.

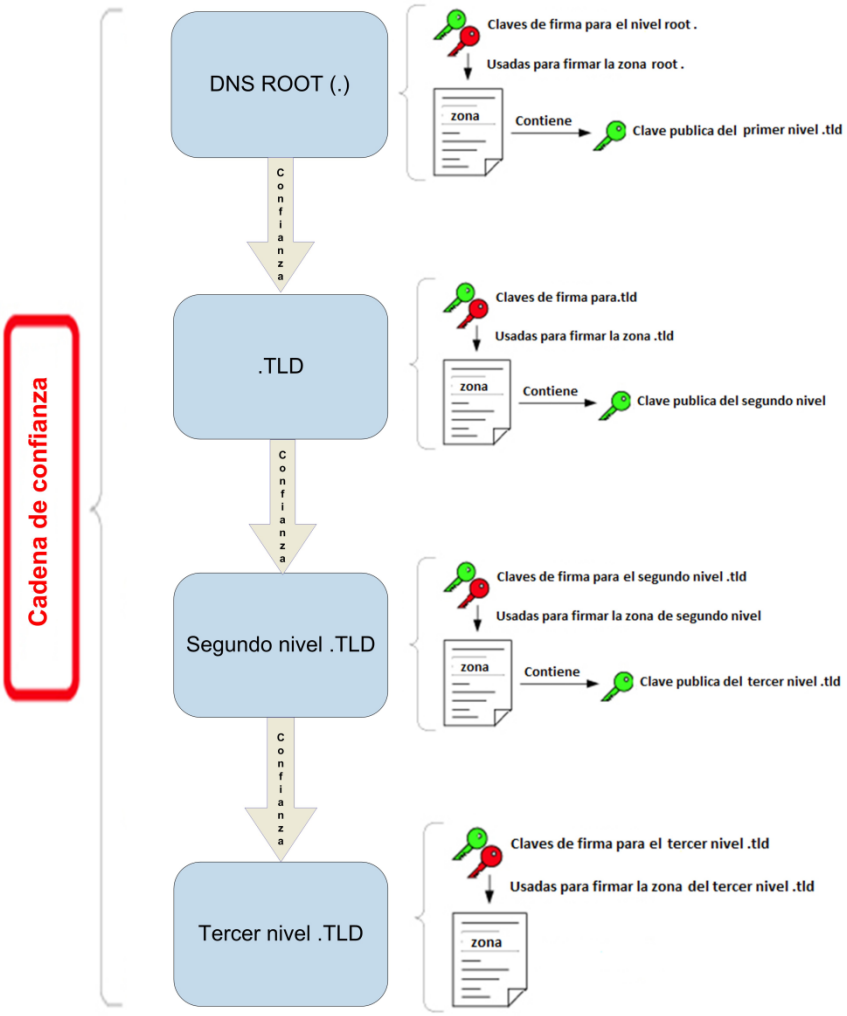



**Figura 139: Cadena de Confianza**

### 3.3.5. La Función de DNSSec

DNSSec es una tecnología que se ha desarrollado, entre otras cosas, para brindar protección contra este tipo de ataques mediante la firma digital de los datos a fin de tener la seguridad de que son válidos. Es importante destacar que este método no cifra los datos, tan solo certifica la validez de la dirección del sitio que se visita. La implementación de la DNSSec asegura que el usuario final se conecte al sitio web real que corresponde a un nombre de dominio en particular. Sin embargo, para eliminar

esta vulnerabilidad de Internet, esta tecnología se debe implementar en cada uno de los pasos del proceso de búsqueda, desde la zona raíz hasta el nombre de dominio final (por ejemplo, www.acens.com). La firma de la raíz (implementar la DNSSec en la zona raíz) es un paso necesario de este proceso. Es importante destacar que no cifra los datos, tan solo certifica la validez de la dirección del sitio que se visita, para evitar suplantación de direcciones que pueda causar los problemas.

Cuando se utiliza DNSSec, el sistema valida los datos de regreso (únicamente lo que corresponde a la resolución del dominio) con la firma digital. De forma se puede tener certeza que el sistema de DNS no ha enviado una IP equivocada y la computadora puede establecer la comunicación con el hosting confiadamente.

### 3.3.6. Confianzas

Necesitamos tener un punto de partida para realizar la comprobación de la cadena de confianza cuando se quiere validar una respuesta de DNS. Normalmente, la cadena de confianza comienza en la raíz del sistema de nombres de dominio. Desde el 15 de Julio de 2010 la zona raíz implementa DNSSec con lo que es posible comenzar esta cadena de confianza desde la raíz. Otra cuestión es que no puede haber lagunas en una cadena de confianza; DNSSec fue diseñado expresamente para ser desplegado de manera que la cadena de confianza puede y debe iniciarse y terminarse en cualquier punto de la rama.

Esto significa que un cliente tendrá que decidir en qué cadenas de confianza que va a confiar. Una vez que se ha decidido esto, es necesario confiar explícitamente en las claves públicas que forman la raíz de estas cadenas de confianza. Estos son llamados coloquialmente "anclas de confianza" o puntos de entrada de seguridad. Por ejemplo: si el dominio de nivel superior .es no está firmado pero uclm.es si y todos los subdominios a continuación también están firmados, un ancla de confianza para una respuesta sería la clave pública utilizada para firmar la zona uclm.es.

Actualmente sólo un pequeño número de dominios de primer nivel ofrecen soporte DNSSec y un gran número de administradores de dominios de nivel superior han anunciado que van a implementar DNSSec en el futuro.

### 3.3.7. Islas de confianza

Debido a que algunas zonas raíz no están aún firmadas, cualquier dominio en la actualidad que quiera desplegar DNSSec formara una isla de confianza. La gran desventaja de esta situación es que es difícil decidir en quién confiar, es decir, en que islas. Se tendrá que negociar alguna forma de establecer una confianza, la figura 14 ilustra cual podría ser considerada una isla de confianza.

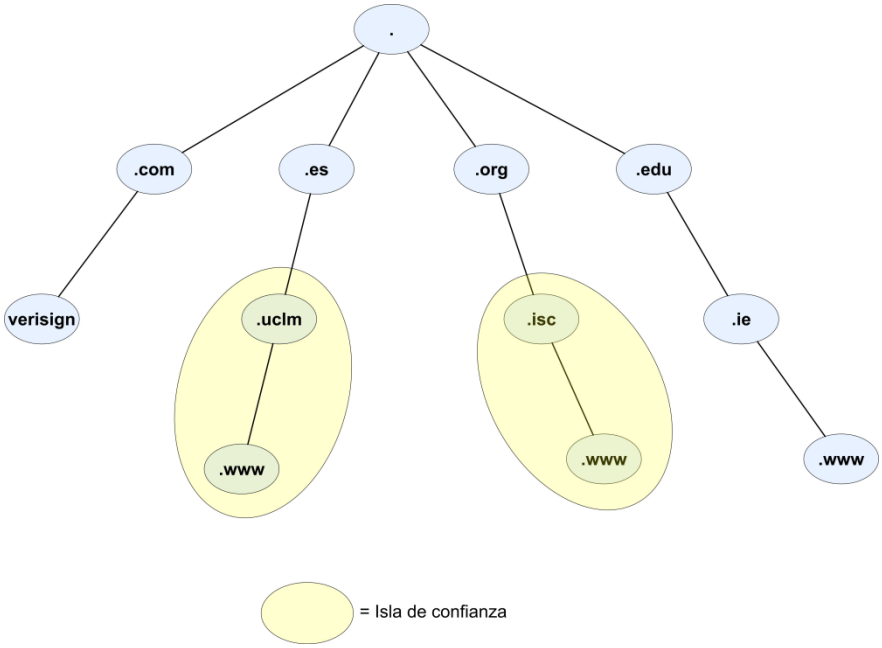



**Figura 140: Isla de Confianza**

Como puede pasar algún tiempo antes de que las zonas raíz se firmen, debido al modelo de implementación que existe actualmente es posible encontrar islas de confianza estableciendo "archipiélagos" de confianza. Un archipiélago sería una entidad externa a las anclas de confianza para un grupo de islas en que los resolvedores puedan decidir en confiar y por lo tanto confiar en todas las islas que forman parte del archipiélago. Existe un mecanismo para lograr esto, llamado DNSSec Look-a-side Validation (DLV).

### 3.3.8. DNSSEC Look-aside Validation

DLV (DNSSEC Look-aside Validación) es una extensión al protocolo DNSSECbis. Está diseñado para ayudar en la implementación de DNSSec simplificando la configuración de los servidores recursivos. DLV proporciona un punto de entrada adicional (además de la zona raíz) de la que obtener información DNSSec para su

validación. Sin DLV, en ausencia de una cadena de confianza completa firmada por la raíz a una zona, los usuarios que deseen habilitar resolvedores DNSSec tendrían que configurar y mantener varias claves de confianza.

El mantenimiento de varias claves de confianza es una tarea difícil de gestionar. DLV elimina esta necesidad ya que actúa como un repositorio de confianza en el que las claves se pueden recuperar de forma segura.

DLV está implementado en BIND 9.4.3-P2 y versiones posteriores. Para obtener más información sobre DNSSECbis y DLV, consulte las RFC que define las extensiones de protocolo.

### 3.3.9. DNSSec Resource Records (RR)

DNSSEC introduce cuatro registros de recursos adicionales para poder procesar la información de seguridad implementada en la extensión DNSSEC. Estos registros de recursos son:

- **DNSKEY**

Cada zona DNSSEC tiene un par de claves privada y pública asociadas, generadas por el administrador de la zona. La clave privada debe ser almacenada con seguridad y en lugar protegido por el administrador de la zona. La clave pública asociada a la zona se publica en el archivo de zona como un registro de recursos DNSKEY.

Un ejemplo de un registro DNSKEY para la zona uclm.net [RFC4034]:

```
uclm.net. 86400 IN DNSKEY 256 3 5 ( AQPSKmynfzW4kyBv015MUG2DeIQ3
Cbl+BBZH4b/0PY1kxkmvHjcZc8no
kfzj31GajIQKY+5CptLr3buXA10h
WqTkF7H6RfoRqXQeogmMHfpftf6z
Mv1LyBUgia7za6ZEzOJBOztyvhjL
742iU/TpPSEDhm2SNKLijfUppn1U
    aNvv4w== )
```

El (TTL) es de 1 día (86400 segundos). El valor de 256 indica que se trata de una zona que contiene una clave. El valor del protocolo es 3. El siguiente campo es el algoritmo de clave pública, 5 indica RSA/SHA1. El valor del RR es la codificación en Base64 del valor de clave pública.

- **RRSIG**

Un "conjunto de registros de recursos" (RRset) es una colección de registros de recursos en una zona DNS que comparten un nombre común, clase y tipo. En DNSSEC los RRsets son firmados por el administrador de la zona. Esta firma se genera mediante la generación de un hash de la Rrset y después cifrando el hash con la clave privada del administrador de la zona. Para una zona que contiene SOA, NS, A, MX y registros de recursos DNSKEY, hay como mínimo cinco RRsets distintos, y cada RRset tendría su propio registro de recursos RRSIG.

Un ejemplo de registro RRSIG para la zona uclm.net [RFC4034]:

host.uclm.net. 86400 IN RRSIG A 5 3 86400 20101122173103 (
20101020173103 2642 uclm.net.
oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTr
PYGv07h108dUKGMeDPKijVCHX3DDKdfb+v6o
B9wfuh3DTJXUAfI/M0zmO/zz8bW0Rznl8O3t
GNazPwQKkRN20XPXV6nwwfoXmJQbsLNrLfkG
J5D6fwFm8nN+6pBzeDQfsS3Ap3o

Los primeros cuatro campos especifican el nombre del propietario, TTL, clase y tipo RR (RRSIG). El siguiente campo es el tipo y tiene el valor "A" que indica que se trata de una firma de los RR A para "host.uclm.net". El siguiente campo es el algoritmo de firma, y el valor de 5 indica que se trata de RSA/SHA1. El valor 3 es el número de etiquetas en el nombre del propietario. El valor de 86400 en el RRSIG RDATA es el valor original TTL del RRset. 20030322173103 y 20030220173103 son las fechas de vencimiento y creación, lo que indica que la firma RRset fue creada el 20/10/2010 17:31:03, y la firma expira a 22/11/2010 17:31:03. La etiqueta con clave 2642 es el nombre del firmante es "uclm.net". El resto del valor del RR es el hash cifrado del RRset.

- **NSEC**

El DNSKEY y los registros RRSIG se pueden utilizar para comprobar la autenticidad de una respuesta DNS, pero donde no haya datos autorizados en la respuesta, la autenticación requiere información adicional.

El archivo de toda la zona se ordena en una forma canónica y el RR NSEC se añade para incrementar la firma en la zona. El registro NSEC define el conjunto de los tipos

de RR para el nombre de dominio entero. En respuesta a una consulta, si el nombre no existe en el archivo de zona, o no existe el tipo RR para el nombre en cuestión, el registro NSEC es devuelto como prueba autenticada de que el nombre, o el tipo de RR no existe.

Un ejemplo de registro NSEC para la zona uclm.net [RFC4034]:

alfa.uclm.net. 86400 IN NSEC host.uclm.net. (A MX RRSIG NSEC TYPE1234)

Los primeros cuatro campos especifican el nombre, TTL, clase y tipo RR (NSEC). La entrada host.uclm.net es el nombre de la siguiente autoridad después de alfa.uclm.net. Los nemotécnicos A, MX, RRSIG, NSEC, y TYPE1234 indican que son registros RRsets (A, MX, RRSIG, NSEC, y TYPE1234) asociados con el nombre alfa.uclm.net. Los registros NSEC se pueden utilizar para enumerar el contenido completo de un archivo de zona. Mientras los datos DNS son ofrecidos como información pública, hay cierta preocupación por la publicación implícita de toda la zona de esta manera.

- **DS**

La validación de la clave pública de la zona sigue sin abordarse con los tres primeros tipos de registros de recursos. Un atacante simplemente tendría que suministrar el DNSKEY y los datos RRSIG para que hacer coincidir con los datos RRset falsos con el fin de hacer que la respuesta parezca "auténtica”. La solución adoptada por DNSSEC es usar una cadena de confianza dentro de la estructura jerárquica del propio DNS. Aparte de la zona de la raíz, cada zona DNS tiene una zona principal. La Delegación Firmante (DS) RR contiene el hash de la clave pública de la zona secundaria. Esta entrada es firmada por la clave privada de la zona principal con RRSIG. Para validar una zona DNSKEY, el DS asociado, RRSIG (DS) y DNSKEY de la zona principal debe ser recuperado. El registro DS se valida mediante el DNSKEY para cifrar el registro RRSIG (DS) y luego comprobar que el resultado coincide con el registro DS. Esta es la clave pública de la zona, que puede ser comparada con el registro DNSKEY de la zona en cuestión.

El proceso de validación se detiene cuando el cliente DNSSEC se encuentra con una clave "de confianza". La clave de confianza ideal sería el DNSKEY de la zona root, pero en ausencia de dicha clave de confianza, cada cliente DNSSEC tiene que configurar su sistema de validación de confianza con los dominios de confianza en los que no existe una validación de un dominio superior.

Un ejemplo de registro DS para la zona uclm.net [RFC4034]:

dskey.uclm.net. 86400 IN DS 60485 5 1 ( 2BB183AF5F22588179A53B0A98631FAD1A292118 )

Los primeros cuatro campos de texto especifican el nombre, TTL, clase y tipo RR (DS). Valor 60485 es la clave para "dskey.uclm.net". El RR DNSKEY y el valor 5 indican el algoritmo utilizado por "dskey.uclm.net" RR DNSKEY. El valor 1 es el algoritmo utilizado para la construcción del resumen, y el resto del texto RDATA es el resumen en formato hexadecimal.

## Capítulo 4

# 4. Monitoreo de la red de datos.

### 4.1. Introducción.

El monitoreo es un proceso eminentemente pasivo, el cual se encarga de observar el estado y comportamiento de la configuración de red y sus componentes. También se encarga de agrupar todas las operaciones para la obtención de datos acerca del estado de los recursos de la red.

Monitoreo es la realización del estudio del estado de los recursos. Las funciones del monitoreo de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas. [21]

El monitoreo de una red abarca 4 fases:

- Definición de la información de administración que se monitorea.
- Acceso a la información.
- Diseño de políticas de administración.
- Procesamiento de la información.

Los tipos de monitoreo son:

- Automático.
- Manual.

Los elementos monitoreados pueden ser:

- En su totalidad.
- En Segmentos.

El monitoreo puede ser realizado en forma:

- Continua.
- Eventual.

### 4.2. Propósito del Monitoreo.

Dentro de los propósitos del monitoreo están las siguientes:

- Identificar la información a monitorear.
- Diseñar mecanismos para obtener la información necesaria.
- Tomar nuevas medidas sobre aspectos de los protocolos, colisiones, fallas, paquetes, etc.

- Almacenar la información obtenida en bases de información de gestión para su posterior análisis.
- Del análisis, obtener conclusiones para resolver problemas concretos o bien para optimizar la utilización de la red.

Dentro del monitoreo de la actividad de la red, los eventos típicos que son monitoreados suelen ser:

- Ejecución de tareas como la realización de copias de seguridad o búsqueda de virus.
- Registro del estado de finalización de los procesos que se ejecutan en la red.
- Registro de las entradas y salidas de los usuarios en la red.
- Registro del arranque de determinadas aplicaciones.
- Errores en el arranque de las aplicaciones, etc.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención, se pueden utilizar diferentes métodos de notificación o alerta tales como:

- Mensajes en la consola: método en el que se suele codificar en función de su importancia.
- Mensajes por correo electrónico: método mediante el cual se envía contenido el nivel de prioridad y el nombre del evento ocurrido.
- Mensajes a móviles: método utilizado cuando el evento necesita intervención inmediata del administrador de red. [21]

### 4.3. Monitoreo activo.

Este tipo de monitoreo se realiza inyectando paquetes de prueba a determinadas aplicaciones para medir sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red. [22]

Entre algunas de las técnicas de este tipo de monitoreo están:

- Basado en ICMP.
    - Diagnosticar problemas en la red
    - Detectar retardo, pérdida de paquetes.
    - RTT

    - Disponibilidad de host y redes.
- Basado en TCP
    - Tasa de transferencia.
    - Diagnosticar problemas a nivel aplicación.
- Basado en UDP
    - Pérdida de paquetes en un sentido (one-way)
    - RTT (traceroute)

### 4.4. Monitoreo pasivo.

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como sniffers, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para snmp, rmon y netflow. Este enfoque no agrega tráfico en la red como lo hace el activo. Es utilizado para caracterizar el tráfico en la red y para contabilizar su uso. [21]. Entre algunas de las técnicas de monitoreo pasivo tenemos:

- **Solicitudes remotas.**

Mediante SNMP, esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados traps que indican que un evento inusual se ha producido.

- **Captura de tráfico**

Se puede llevar a cabo de dos formas: 1) Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura; y 2) Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

- **Análisis de Tráfico**

Se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivos *probe* que envíen información mediante RMON o a través de un

dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

- **Flujos**

También utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes mediante:

  - La misma IP origen y destino
  - El mismo puerto TCP origen y destino
  - El mismo tipo de aplicación.

Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos.

### 4.5. Estrategias de Monitoreo.

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitoreo así como las herramientas que se utilizarán para esta tarea.

- **Qué monitorear**

Una consideración muy importante es delimitar el espectro sobre el cual se va a trabajar. Existen muchos aspectos que pueden ser monitoreados, los más comunes son los siguientes:

  - Utilización de ancho de banda
  - Consumo de CPU
  - Consumo de memoria
  - Estado Físico de las conexiones
  - Tipo de tráfico
  - Alarmas
  - Servicios (Web, correo, base de datos)

- **Métricas**

La definición de métricas permitirá establecer patrones de comportamiento para los dispositivos que serán monitoreados. También hay diversos tipos de métricas que pueden ser declarados, dependerán de las necesidades particulares de cada red. Las

métricas deben ser congruentes con los objetos a monitorear que fueron señalados en el punto anterior. Algunos ejemplos son:

- Métricas de tráfico de entrada y salida
- Métricas de utilización de procesador y memoria
- Métrica de estado de las interfaces
- Métrica de conexiones lógicas

### 4.6. Elección de herramientas para monitoreo de la red.

La elección de la mejor herramienta depende de diversos factores tales como: funcionalidad, desempeño, fácil manejo, infraestructura, económicos, que se adapte a la red de datos de la organización, entre algunas de ellas se describen a continuación.

**Cacti:** Es una completa solución para el monitoreo de redes. Utiliza RRDTool para almacenar la información de los dispositivos y aprovecha sus funcionalidades de graficación. Proporciona un esquema rápido de obtención de datos remotos, múltiples métodos de obtención de datos (snmp, scripts), un manejo avanzado de templates, y características de administración de usuarios. Además, ofrece un servicio de alarmas mediante el manejo de umbrales. Todo ello en una sola consola de administración, fácil de configurar. [22]

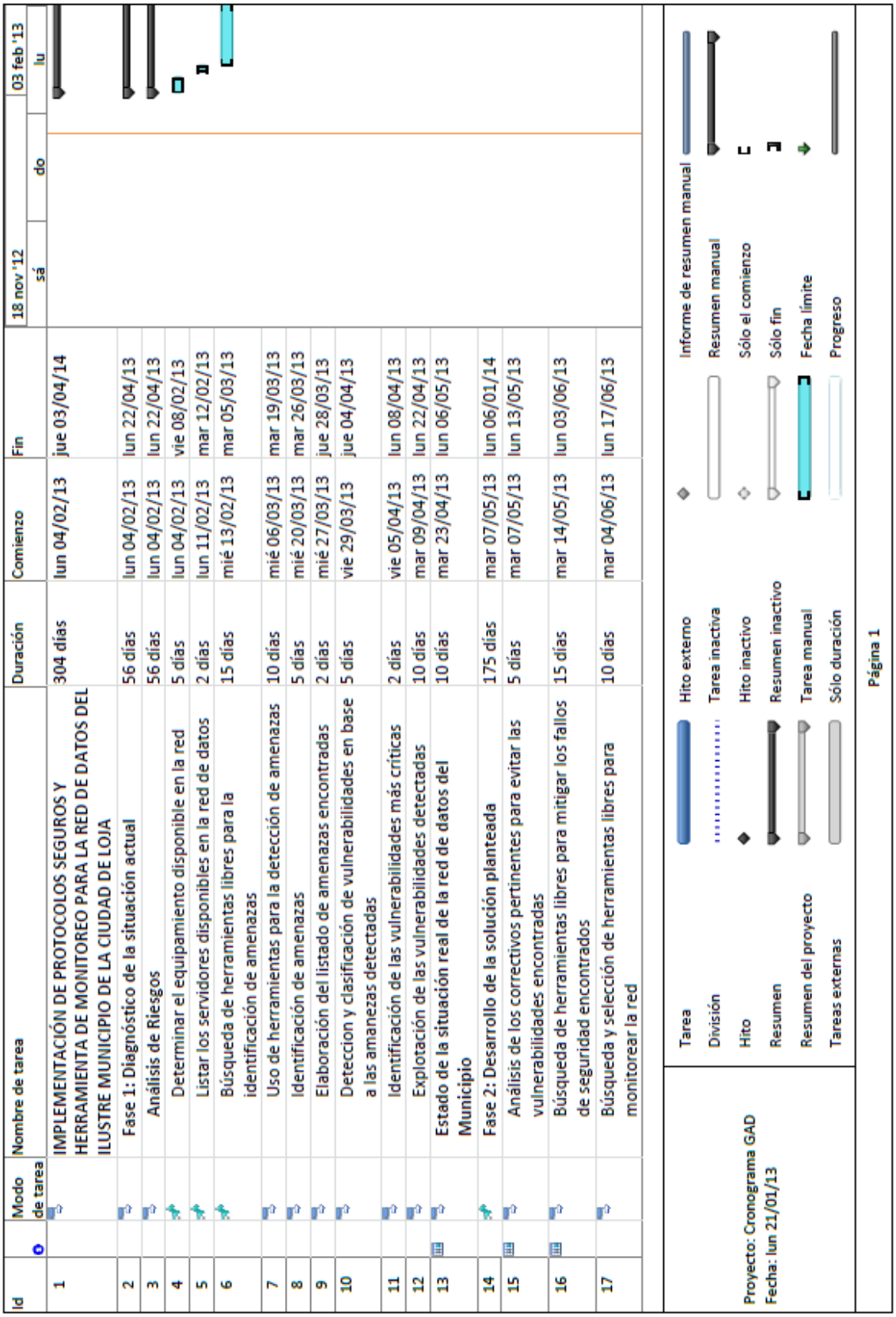
**Net-SNMP:** Conjunto de aplicaciones para obtener información vía snmp de los equipos de interconexión. Soporta la versión 3 del protocolo la cual ofrece mecanismos de seguridad tanto de confidencialidad como de autenticación. Provee de manejo de traps para la notificación de eventos. [22]

**Nagios:** Aplicación para el monitoreo de servicios, hosts que pertenecen a una red. Es capaz de monitorear si un servicio se encuentra activo o no, o si un hosts se encuentra operacional o no.

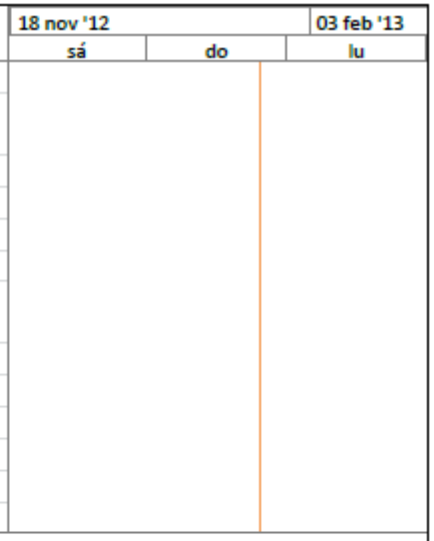
Muestra el estadio operacional de todos los servicios y hosts en un ambiente Web. Envía notificaciones mediante mail o pager cuando el estado operacional de un elemento a monitorear cambia. [22]

## G. CRONOGRAMA

| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|---|---|
| 1 | | IMPLEMENTACIÓN DE PROTOCOLOS SEGUROS Y HERRAMIENTA DE MONITOREO PARA LA RED DE DATOS DEL ILUSTRE MUNICIPIO DE LA CIUDAD DE LOJA | 304 días | lun 04/02/13 | jue 03/04/14 |
| 2 | | Fase 1: Diagnóstico de la situación actual | 56 días | lun 04/02/13 | lun 22/04/13 |
| 3 | | Análisis de Riesgos | 56 días | lun 04/02/13 | lun 22/04/13 |
| 4 | | Determinar el equipamiento disponible en la red | 5 días | lun 04/02/13 | vie 08/02/13 |
| 5 | | Listar los servidores disponibles en la red de datos | 2 días | lun 11/02/13 | mar 12/02/13 |
| 6 | | Búsqueda de herramientas libres para la identificación de amenazas | 15 días | mié 13/02/13 | mar 05/03/13 |
| 7 | | Uso de herramientas para la detección de amenazas | 10 días | mié 06/03/13 | mar 19/03/13 |
| 8 | | Identificación de amenazas | 5 días | mié 20/03/13 | mar 26/03/13 |
| 9 | | Elaboración del listado de amenazas encontradas | 2 días | mié 27/03/13 | jue 28/03/13 |
| 10 | | Detección y clasificación de vulnerabilidades en base a las amanezas detectadas | 5 días | vie 29/03/13 | jue 04/04/13 |
| 11 | | Identificación de las vulnerabilidades más críticas | 2 días | vie 05/04/13 | lun 08/04/13 |
| 12 | | Explotación de las vulnerabilidades detectadas | 10 días | mar 09/04/13 | lun 22/04/13 |
| 13 | | Estado de la situación real de la red de datos del Municipio | 10 días | mar 23/04/13 | lun 06/05/13 |
| 14 | | Fase 2: Desarrollo de la solución planteada | 175 días | mar 07/05/13 | lun 06/01/14 |
| 15 | | Análisis de los correctivos pertinentes para evitar las vulnerabilidades encontradas | 5 días | mar 07/05/13 | lun 13/05/13 |
| 16 | | Búsqueda de herramientas libres para mitigar los fallos de seguridad encontrados | 15 días | mar 14/05/13 | lun 03/06/13 |
| 17 | | Búsqueda y selección de herramientas libres para monitorear la red | 10 días | mar 04/06/13 | lun 17/06/13 |



| Id | | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|---|---|---|
| 18 | | | **Etapa de configuración** | 135 días | mar 18/06/13 | lun 23/12/13 |
| 19 | | | Configuración y pruebas de protocolos seguros SSL, TLS | 20 días | mar 18/06/13 | lun 15/07/13 |
| 20 | | | Configuración y pruebas IPSec | 40 días | mar 16/07/13 | lun 09/09/13 |
| 21 | | | Configuración y pruebas DNSSec | 45 días | mar 10/09/13 | lun 11/11/13 |
| 22 | | | Configuración de la herramienta de monitoreo | 30 días | mar 12/11/13 | lun 23/12/13 |
| 23 | | | **Fase 3: Implantación de la solución** | 28 días | mar 24/12/13 | jue 30/01/14 |
| 24 | | | Elaboración del informe de las medidas correctivas para los servidores expuestos | 3 días | mar 24/12/13 | jue 26/12/13 |
| 25 | | | Implantación de los servidores correspondientes | 25 días | vie 27/12/13 | jue 30/01/14 |
| 26 | | | **Fase 4: Evaluación y pruebas de la solución** | **45 días** | **vie 31/01/14** | **jue 03/04/14** |
| 27 | | | Pruebas de validación | 10 días | vie 31/01/14 | jue 13/02/14 |
| 28 | | | Control de vulnerabilidades | 20 días | vie 14/02/14 | jue 13/03/14 |
| 29 | | | Elaboración del informe de amenazas corregidas | 5 días | vie 14/03/14 | jue 20/03/14 |
| 30 | | | Elaboración de manuales de las soluciones | 10 días | vie 21/03/14 | jue 03/04/14 |




Proyecto: Cronograma GAD
Fecha: lun 21/01/13

| | | | | | |
|---|---|---|---|---|---|
| Tarea | | Hito externo | | Informe de resumen manual | |
| División | | Tarea inactiva | | Resumen manual | |
| Hito | | Hito inactivo | | Sólo el comienzo | |
| Resumen | | Resumen inactivo | | Sólo fin | |
| Resumen del proyecto | | Tarea manual | | Fecha límite | |
| Tareas externas | | Sólo duración | | Progreso | |

Página 2

## H. PRESUPUESTO Y FINANCIAMIENTO

Los materiales que vamos a utilizar para desarrollar este proyecto, son los siguientes:

### 8.1 Recursos Humanos

| Descripción | Cantidad | Horas | Valor/unit. | Valor/Total |
|---|---|---|---|---|
| Aspirantes | 2 | 600 | $ 5.00 | $6000.00 |
| Coordinador | 1 | 128 | $ 10.00 | $1280.00 |
| **Director del Proyecto** | 1 | 90 | $ 10.00 | $ 900.00 |
| Transporte | 2 | | $ 3.00 | $ 6.00 |
| Visitas a la Institución | 2 | 3 | $ 10.00 | $60.00 |

**Tabla 36:** Recursos Humanos

### 8.2 Recursos Técnicos y Tecnológicos

| Descripción | Cantidad | Valor/unit. | Valor/Total |
|---|---|---|---|
| **Hardware** | | | |
| Computador Portátil HP Pavilion g4-1085 | 100 horas | $ 0.70 | $ 70.00 |
| Computador Portátil Dell Studio XPS 15Z | 100 horas | $ 0.70 | $ 70.00 |
| Impresora | 300 hojas | $ 0.05 | $ 15.00 |
| Servidor IPSec/DNSSec | 1 | $ 1200,00 | $ 1200,00 |
| Servidor para monitoreo | 1 | $ 1600,00 | $ 1600,00 |
| **Software** | | | |
| BackTrack 5 | 1 | $ 0.00 | $ 0.00 |
| Debian 6.0.6 | 1 | $ 0.00 | $ 0.00 |
| IPSec + DNSSec | 1 | $ 0.00 | $ 0.00 |

**Tabla 37:** Recursos Técnicos y Tecnológicos

### 8.3 Recursos Materiales

| Descripción | Cantidad | Valor/unit. | Valor/Total |
|---|---|---|---|
| Paquete de Hojas A4 (resma) | 2 | $ 4,50 | $ 9.00 |
| Anillado | 3 | $ 1.80 | $ 5.40 |
| Materiales de oficina | varios | $ 0,00 | $ 35.00 |
| Borde o Perfil | 5 | $ 0.50 | $ 2.50 |
| DVD's | 5 | $ 0.45 | $ 2.25 |

**Tabla 38:** Recursos Materiales

## 8.4 Resumen del Presupuesto

| Resumen del Presupuesto | Costo Total |
|---|---|
| Recursos Humanos | $ 8246.00 |
| Recursos Técnicos y Tecnológicos | $2955.00 |
| Recursos Materiales | $54.15 |
| **SUBTOTAL** | $11255.15 |
| Imprevistos 10 % | $ 1125,515 |
| **TOTAL** | **$12354,065** |

**Tabla 39:** Resumen de Presupuesto

# I. BIBLIOGRAFÍA

[1] Cristian Borghello, Seguridad Lógica - Administración de Seguridad [online], Argentina, 2000-2009, Disponible en: http://www.segu-info.com.ar/logica/administracion.htm

[2] Martín M. Carmuega, Andrés L. Gil, La seguridad de la información y su impacto en las organizaciones [online], Argentina, 2006, Disponible en: http://www.deloitte.com/assets/Dcom-Argentina/Local%20Assets/Documents/arg_aud_deloitte-workshop-gobierno-corporativo_20061101.pdf

[3] Cristian Borghello, Amenazas Lógicas - Tipos de Ataques [online], Argentina 2000-2009, Disponible en: http://www.segu-info.com.ar/ataques/tipos.htm

[4] Miguel, DNSSEC DNS Security Extensions + Sec, "Cambiando la petición de dirección", [online]. dns-sec.es, Disponible en: http://www.dns-sec.es/index.php/inseguridad-en-dns/cambiando-la-peticion-de-direccion/

[5] Miguel, DNSSEC DNS Security Extensions + Sec, "Secuestrando un dominio: El ataque Kaminsky", [online]. dns-sec.es Disponible en: http://www.dns-sec.es/index.php/inseguridad-en-dns/secuestrando-un-dominio-el-ataque-kaminsky/

[6] Cristian Borghello, Exploit [online], Argentina, 2000-2009, Disponible en: http://www.segu-info.com.ar/malware/exploit.html

[7] DragoN, ¿Cómo se realiza un Pentest?[online], Manizales, julio de 2010, Disponible en: http://www.dragonjar.org/como-realizar-un-pentest.xhtml

[8] TextosCientificos.com, "TCP/IP y el modelo OSI", [online], Disponible en:

http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

[9] Jorge Della Gaspera, Mario Navarro, Daniel Rey. MODELO DE REFERENCIA OSI [online]. Disponible en: http://www.frm.utn.edu.ar/comunicaciones/modelo_osi.html

[10] Edgardo Alexis Rojas Cardona, "Capas del modelo osi" [online] slideshare.net Disponible en: http://www.slideshare.net/alxcdn/modelo-osi-10138985

[11] genus23, "Conceptos de protocolos de red", [online]. Wordpress. Marzo 2011 Disponible en:http://genus23.files.wordpress.com/2011/03/conceptos-de-protocolos-de-red.pptx

[12] Miguel, DNSSEC DNS Security Extensions + Sec, "Historia", [online]. dns-sec.es. Disponible en: http://www.dns-sec.es/index.php/sistema-de-nombres-de-dominio-dns/historia/

[13] Miguel, DNSSEC DNS Security Extensions + Sec, “El propósito de DNS”, [online]. dns-sec.es Disponible en: http://www.dns-sec.es/index.php/sistema-de-nombres-de-dominio-dns/el-proposito-de-dns/

[14] Miguel, DNSSEC DNS Security Extensions + Sec, “El Sistema de Nombres de Dominio (DNS)”, [online]. dns-sec.es Disponible en: http://www.dns-sec.es/index.php/sistema-de-nombres-de-dominio-dns/el-sistema-de-nombres-de-dominio-dns/

[15] VeriSign Spain S.L., Los últimos avances de la tecnología SSL [online], España, 2007, Disponible en: http://www.verisign.es/static/038828.pdfCapitulo1

[16] facuzdelacruz, “IPSec, seguridad en layer 3”, [online]. Wordpress. Noviembre 16 del 2008. Disponible en: http://facusdelacruz.wordpress.com/2008/11/16/ipsec-seguridad-en-layer-3/

[17] OpenBSD, “Está bien pero, ¿para qué querría usar IPSec?”. [online]. Diciembre 2000. Disponible en: http://openbsd.appli.se/faq/es/faq13.html

[18] Julio López Albín, “Tema 4. Medidas de seguridad en red Administración de Sistemas y Redes II”. [online]. xulio@dec.usc.es. Febrero 28 del 2008, Disponible en: www.ac.usc.es/docencia/ASRII/Tema_4print.pdf

[19] Juan Espinosa Vélez, Conclusiones y establecimiento de diferencias entre el IPSec y SSL [online].Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/202/4/Capitulo%203.pdf

[20] Miguel, DNSSEC DNS Security Extensions + Sec, “Por qué DNS es inseguro”, [online]. dns-sec.es Disponible en: http://www.dns-sec.es/index.php/inseguridad-en-dns/

[21] Naranjo Villacrés Diego Ricardo, Desarrollo de una aplicación gráfica, basado en el sistema operativo LINUX para el monitoreo y administración del tráfico de datos en redes LAN. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/2353/1/CD-0006.pdf

[22] Carlos A. Vicente Altamirano, Monitoreo de recursos de red, [online], Universidad Nacional Autónoma de México, Dirección de Telecomunicaciones, Departamento de Redes, 2005, Disponible en: http://juliorestrepo.files.wordpress.com/2011/04/monitoreo.pdf