UNIVERSIDAD NACIONAL DE LOJA

TT-CIS

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

---

CARRERA DE INGENIERÍA EN SISTEMAS

Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja.

TESIS PREVIA A OBTENER EL TÍTULO DE INGENIERO EN SISTEMAS.

Autor:

Henry Daniel Quezada Lozano.

Director:

Ing. Mario Andrés Palma Jaramillo, Mg. Sc.

LOJA - ECUADOR

2016

CERTIFICACIÓN DEL DIRECTOR

Ing. Mario Andrés Palma Jaramillo, Mg. Sc.
DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS

CERTIFICA:

Que el Sr. Henry Daniel Quezada Lozano ha trabajado bajo mi tutoría el presente trabajo de titulación (TT), previo a la obtención del título de Ingeniero en Sistemas, cuyo tema versa sobre **"Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja"**, el mismo que ha sido dirigido, orientado y discutido bajo mi asesoramiento y cumple con la reglamentación pertinente, razones por las cuales reúne la suficiente validez técnica y práctica, por consiguiente autorizo su certificación para su posterior presentación y sustentación.

Loja, 22 de marzo de 2016.

Ing. Mario Andrés Palma Jaramillo, Mg. Sc.
DIRECTOR DE TESIS

AUTORÍA

Yo, **HENRY DANIEL QUEZADA LOZANO**, declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido del mismo.

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

Firma: 

Cédula: 1104872815.

Fecha: 25-10-2016.

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

Yo, **HENRY DANIEL QUEZADA LOZANO**, declaro ser autor de la tesis titulada: **DISEÑO DE UNA VPN PARA EL ACCESO A LAS BASES DE DATOS CIENTÍFICAS DE LA UNIVERSIDAD NACIONAL DE LOJA**, como requisito para optar al grado de **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

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

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

Para constancia de esta autorización, en la ciudad de Loja, a los veinticinco días del mes de octubre del dos mil dieciséis.

Firma: 

Autor: Henry Daniel Quezada Lozano.
Cédula: 1104872815.
Dirección: Loja, (Av. 8 de Diciembre: entrada colegio militar).
Correo Electrónico: hdquezadal@unl.edu.ec.
Teléfono: 2540374. **Celular:** 0990205116.

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Mario Andrés Palma Jaramillo, Mg. Sc.
Tribunal de Grado: Ing. Hernán Leonardo Torres Carrión, Mg. Sc.
Ing. Mario Enrique Cueva Hurtado, Mg. Sc.
Ing. Gastón René Chamba Romero, Mg. Sc.

DEDICATORIA

Dedico el presente trabajo de titulación a mis padres, quienes han sido el pilar fundamental de mi vida, me han cuidado, me han brindado todas las facilidades económicas para realizar mis estudios y me han dado su apoyo incondicional.

A Dios, quien me ha permitido seguir alcanzando éxitos, por protegerme, por darme salud y estar presente en el transcurso de los años que llevo con vida.

A mis amigos, quienes han estado presentes durante estos años de universidad, me han ayudado, aconsejado y han sido un aporte esencial para este logro.

Henry Quezada

AGRADECIMIENTO

Agradezco a Dios por darme la oportunidad de tener vida y lograr culminar la meta propuesta desde que inicie la universidad, por permitirme contar con mis padres y hermanas quienes han sido un baluarte en mi desarrollo personal y profesional.

A la Universidad Nacional de Loja por haberme cobijado durante estos seis años de estudio y haberme capacitado tanto en el campo profesional como en valores éticos y morales. A mi director de tesis Ing. Mario Palma quien sin su ayuda y guía no hubiera logrado culminar con éxito el presente trabajo de titulación.

Agradezco a mis compañeros y amigos quienes me han brindado su apoyo incondicional durante los años de estudio y han sido uno de los pilares fundamentales para el presente logro académico.

Henry Quezada

Índice de Contenidos

Índice General

Índice de Figuras

Índice de Tablas

1. Título

DISEÑO DE UNA VPN PARA EL ACCESO A LAS BASES DE DATOS CIENTÍFICAS DE LA UNIVERSIDAD NACIONAL DE LOJA.

2. Resumen

El presente trabajo de titulación está orientado al Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja, con la finalidad de obtener un servicio que permita a los miembros de la comunidad universitaria acceder remotamente a los recursos de la red interna del campus universitario, desde una red externa a la institución.

Para el desarrollo del presente proyecto de titulación, se utilizó una metodología propia, la cual consta de cuatro fases: En la primera fase se analizó casos de éxito de herramientas Open Source para el diseño de la red privada virtual, los cuales permitieron obtener información de las herramientas VPN que se utilizaron para solventar las necesidades institucionales en cada uno de los casos de éxito expuestos. Además, se analizó y seleccionó la herramienta VPN que se utilizó en el desarrollo del presente trabajo de titulación. En la segunda fase se diseñó la red privada virtual basada en una tecnología y protocolos de seguridad para permitir la transmisión de datos, en la cual se analizó y seleccionó el tipo de VPN, la arquitectura de la red privada virtual y el protocolo de túnel. En la tercera fase se creó un escenario de una red privada virtual para acceder a las bases de datos científicas de la Universidad Nacional de Loja. La creación del escenario permitió configurar un servidor VPN para la conexión de usuarios remotos con la red interna de la Universidad Nacional de Loja.

Finalmente, en la cuarta fase se evaluó el escenario de la red privada virtual mediante la aplicación de cinco pruebas. La primera prueba se encargó de comprobar la conectividad tanto del cliente hacia el servidor VPN, y desde el servidor VPN hacia el cliente. En la segunda prueba se comprobó el acceso a las bases de datos científicas de la Universidad Nacional de Loja mediante la conexión a la red privada virtual. La tercera prueba evaluó la accesibilidad del servidor VPN, mediante el empleo de la prueba de carga y cantidad de accesos simultáneos. En la cuarta prueba se verificó el rendimiento del servidor VPN. Y finalmente se realizó la prueba de implementación con una muestra de usuarios de acuerdo con cada perfil establecido.

Summary

The present titration's work is oriented to the design of a VPN for access to databases scientific of the Universidad Nacional de Loja, in order to obtain a service that allows members of the University community to remotely access resources on the internal network of the University campus, from a foreign institution network.

For the development the present titration's work, is used a methodology own, which consists of four phases: in the first phase is analyzed cases of success of tools Open Source for the design of the network private virtual, which allowed get information of them tools VPN that is used to solve them needs institutional in each one of them cases of success exposed. In addition, is analyzed and selected the tool VPN that is used in the development of the present titration's work. In the second phase is designed the network private virtual based in a technology and protocols of security to allow the transmission of data, in which is analyzed and selected the type of VPN, the architecture of the network private virtual and the Protocol of tunnel. In the third phase was created a scenario of a virtual private network to access scientific databases of the Universidad Nacional de Loja. The creation of the stage allowed configuring a VPN server for connecting remote users to the internal network of the Universidad Nacional de Loja.

Finally, in the fourth phase is evaluated the scenario of the network private virtual by the application of five tests. The first test was responsible for check the connectivity of the client to the VPN server, and from the VPN server to the client. In the second test is found the access to them databases scientific of the Universidad Nacional de Loja by the connection to the network private virtual. The third test evaluated the accessibility of the server VPN, through the employment of the test of load and amount of access simultaneous. In the fourth test was verified the performance of the VPN server. And finally is made it test of implementation with a sample of users in accordance with each profile established.

3. Introducción

En la actualidad el Internet se ha convertido en uno de los adelantos tecnológicos de mayor impacto y desarrollo, produciendo cambios y avances espectaculares en el campo de la ciencia y de la tecnología [1], debido a esto las Redes Privadas Virtuales se han convertido en una alternativa práctica y segura de las empresas, instituciones u organismos para intercomunicar sus redes centrales con equipos de acceso remoto. Y de esta manera brindar acceso a los recursos internos de la red a sus trabajadores y estudiantes.

El presente Trabajo de Titulación tiene como objetivo general diseñar una red privada virtual que permita acceder de forma remota a las bases de datos científicas que dispone la Universidad Nacional de Loja.

El desarrollo del trabajo de titulación se encuentra estructurado en 9 secciones. Las tres primeras secciones corresponden a la parte introductoria: Titulo, Resumen e Introducción. La cuarta sección corresponde a la "Revisión de Literatura", en la que se describió la información recolectada para el desarrollado del trabajo de titulación. Esta sección está divida en 4 capítulos:

En el primer capítulo denominado "Redes privadas virtuales", se revisó la teoría necesaria para el entendimiento y desarrollo de cada una de las fases (objetivos planteados), también se especificó 3 casos de éxito internacionales y 2 casos de éxito nacionales, relacionados con el uso de herramientas VPN Open Source para el diseño de redes privadas virtuales; y finalmente se describieron varias herramientas Open Source que se emplean para el diseño de las redes privadas virtuales.

En el segundo capítulo denominado "Arquitecturas, Tipos y Protocolos de túnel de las redes privadas virtuales", se revisó sobre los diferentes tipos de redes privadas virtuales, las diferentes arquitecturas que utilizan las VPN y los protocolos de seguridad que las mismas emplean.

En el tercer capítulo denominado "Sistemas Operativos para Servidores", se revisó los principales sistemas operativos que existen para la instalación de servidores. Y

finalmente en el cuarto capítulo denominado “Análisis de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de servicios y recursos tecnológicos implementados actualmente”, se analizó como se encuentra la infraestructura de red de datos de la Universidad Nacional de Loja, y cuáles son los servicios que ofrece en la actualidad.

La quinta sección corresponde al apartado de “Materiales y Métodos”, en donde se describió en su totalidad los métodos, técnicas y metodología que se emplearon en el desarrollo del trabajo de titulación.

En la sexta sección se encuentra el apartado de “Resultados”, en el cual se indicó los resultados obtenidos en el desarrollo del trabajo de titulación, esta sección se compone de 4 fases. En la primera fase se analizó estados de arte y casos de éxito de herramientas Open Source para el diseño de la VPN. En la segunda fase se diseñó la VPN basada en una tecnología y protocolos de seguridad para permitir la transmisión de datos. En la tercera fase se creó un escenario de una VPN para acceder a las bases de datos científicas de la Universidad Nacional de Loja. Y finalmente en la cuarta fase se aplicó pruebas para evaluar el correcto funcionamiento del escenario de la VPN.

La séptima sección corresponde al apartado de “Discusión”, en el que se presenta una descripción breve de cómo se logró el cumplimiento de cada uno de los objetivos planteados, estos a su vez se contrastan con el apartado anterior sobre los resultados obtenidos. Además, también se detalló el presupuesto económico empleado en el desarrollo del Trabajo de Titulación.

En la octava sección se encuentra el apartado de “Conclusiones”, en el cual se detalló cómo se evidencia los resultados, en base a la experiencia obtenida en el desarrollo del trabajo de titulación. Y finalmente la novena sección corresponde al apartado de “Recomendaciones”, en el cual se presentó una lista de sugerencias en base a la experiencia que se obtuvo en el desarrollo del trabajo de titulación.

Una red privada virtual diseñada para acceder a las bases de datos científicas de la institución, facilitará el acceso de cualquier usuario a través de un amplio número de dispositivos, permitiendo la búsqueda de información científica en el ámbito académico.

4. Revisión de Literatura

4.1. CAPÍTULO I: REDES PRIVADAS VIRTUALES.

4.1.1. Definiciones Generales.

Para el desarrollo del presente Trabajo de Titulación, es necesario conocer definiciones relacionadas con el diseño y uso de las redes privadas virtuales, las mismas que ayudan a la comprensión de cada una de las actividades planificadas para el cumplimiento de los objetivos planteados.

4.1.1.1. Glosario de Términos.

- **LEAP:** Lightweight Extensible Authentication Protocol, Protocolo Ligero de Autenticación Extensible.
- **L2F:** Layer 2 Forwarding, Protocolo de Túnel de Capa 2 de Cisco.
- **L2TP:** Layer 2 Tunneling Protocol, Protocolo de Túnel de Capa 2.
- **MAC:** Message Authentication Code, Código de Autenticación del Mensaje.
- **MPLS:** MultiProtocol Label Switching, Protocolo Basado en Etiquetas.
- **NAT:** Network Address Translation, Traducción de Direcciones de Red.
- **CA:** Certificate Authority, Autoridad Certificadora.
- **CoS:** Class of Service, Clase de Servicio.
- **CRL:** Certificate Revocation List, Lista de Revocación de Certificados.
- **CSR:** Certificate Signing Request, Petición de Firma de Certificados.
- **DHCP:** Dynamic Host Configuration Protocol, Protocolo Dinámico de Configuración de Anfitrión.
- **DES:** Data Encryption Standard, Cifrado de Datos Estándar.
- **DoS:** Denial of Service, Ataque de Denegación de Servicio.
- **FTP:** File Transfer Protocol, Protocolo de Transferencia de Ficheros.
- **GPL:** GNU General Public License, Licencia Pública General de GNU.
- **GUI:** Graphical User Interface, Interfaz Gráfica de Usuario para Programas.
- **HTTP:** HyperText Transfer Protocol, Protocolo de Transferencia de Hipertexto.
- **IETF:** Internet Engineering Task Force, Grupo de Trabajo en Ingeniería de Internet.

- **IKE:** Internet Key Exchange, Protocolo para Establecer Asociaciones de Seguridad en IPSec.
- **IP:** Internet Protocol, Protocolo de Internet.
- **IPSec:** Internet Protocol Security, Seguridad para el Protocolo de Internet.
- **IPv4:** Internet Protocol versión 4, Versión 4 del Protocolo de Internet.
- **IPv6:** Internet Protocol versión 6, Versión 6 del Protocolo de Internet.
- **ISP:** Internet Service Provider, Proveedor de Servicios de Internet.
- **LAN:** Local Área Network, Red de Área Local.
- **LDAP:** Lightweight Directory Access, Protocolo Ligero de Acceso a Directorios.
- **OSI:** Open System Interconnection, Modelo de Referencia de Interconexión de Sistemas Abiertos.
- **PAM:** Pluggable Authentication Module, Modulo de Autenticación Reemplazable.
- **PAP:** Password Authentication Protocol, Protocolo Simple de Autenticación.
- **POP3:** Post Office Protocol, versión actual del Protocolo de Correo Electrónico.
- **PPP:** Point to Point Protocol, Protocolo Punto a Punto.
- **PPTP:** Point-to-Point Tunneling Protocol, Protocolo de Túnel Punto a Punto.
- **QoS:** Quality of Service, Calidad de Servicio.
- **RADIUS:** Remote Authentication Dial-In User Server, Protocolo de Autenticación y Autorización para Aplicaciones de Acceso a la Red.
- **RPM:** Red Hat Package Manager, Herramienta de Administración de Paquetes para Linux.
- **SSH:** Secure Shell, Protocolo de Acceso Seguro a Máquinas Remotas.
- **SSL:** Secure Socket Layer, Protocolo de Acceso Seguro a Máquinas Remotas.
- **TCP:** Transmission Control Protocol, Protocolo de Control de Transmisión.
- **TELNET:** Telecommunication Network, Protocolo de Acceso a Máquinas Remotas.
- **TLS:** Transport Layer Security, Seguridad de la Capa de Transporte.
- **UDP:** User Datagram Protocol, Protocolo de Capa de Transporte Basado en Datagramas.
- **VPN:** Virtual Private Network, Red Privada Virtual.

4.1.1.2. Concepto de una VPN.

Una red privada virtual (VPN), es una red privada construida dentro de una infraestructura de red pública [2]. Se usan las redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet proporcionados por terceros, en vez de costosos enlaces WAN dedicados o enlaces de marcación remota de larga distancia.

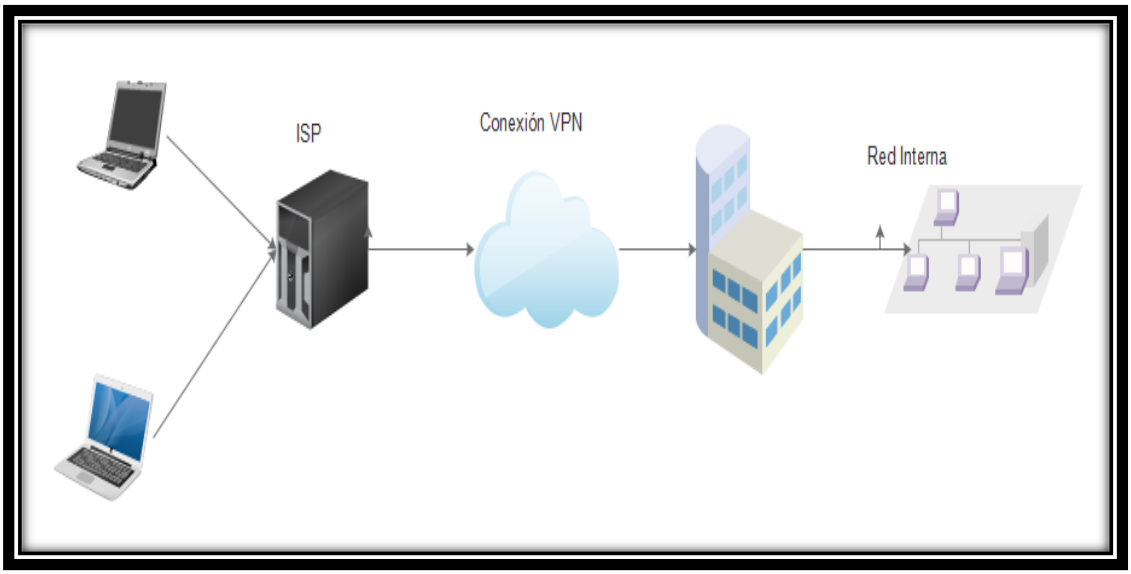


Figura 1: Ejemplo de una Red Privada Virtual.
Fuente: Autor.

El objetivo de una red privada virtual, es permitir la conexión para transportar los paquetes de datos de la red privada por medio de un túnel definido en la red pública [3], y de esta manera intercomunicar oficinas centrales con usuarios de acceso remoto.

4.1.1.3. Funcionamiento de una VPN.

Una red privada virtual se basa en un protocolo denominado protocolo de túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro lado de la misma [4].

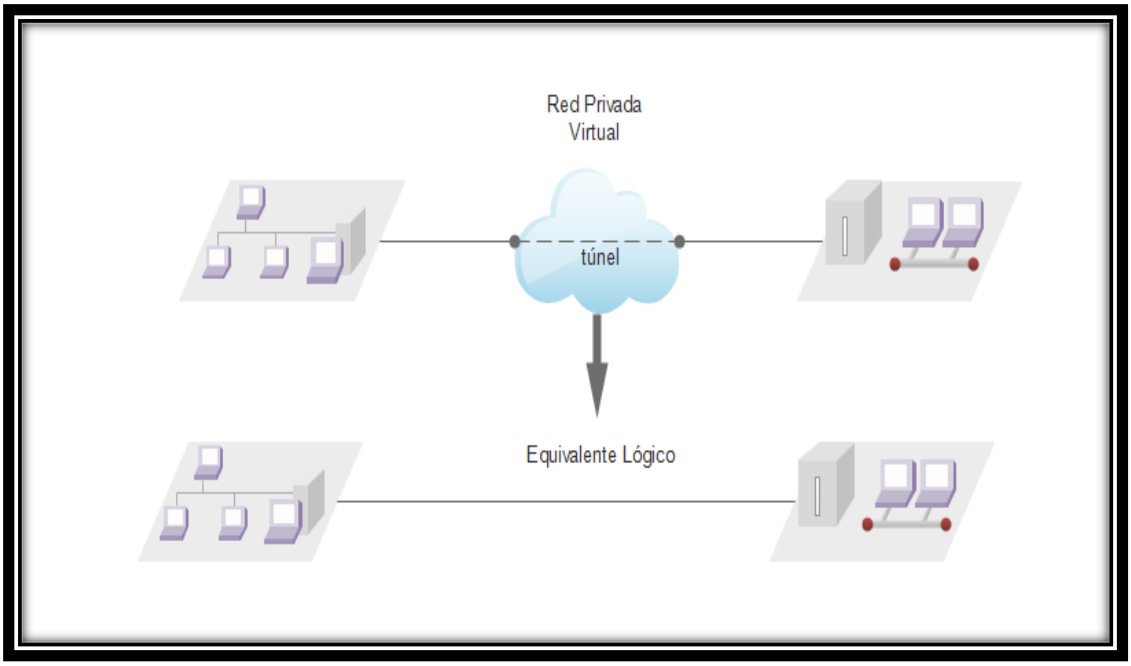


Figura 2: Funcionamiento de una Red Privada Virtual.

Fuente: Autor.

La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella [5].

4.1.1.4. Seguridad de una VPN.

Según Mario Galarza [6], manifiesta que al momento de implementar una red privada virtual hay que asegurarse que la misma proporcione los siguientes mecanismos de seguridad:

- **Autenticación del usuario:** debe verificarse la identidad de los clientes de la VPN, permitiendo el acceso únicamente a los usuarios autorizados. En ocasiones se crean unos registros que muestran quién se conectó y por cuánto tiempo.
- **Gestión de direcciones:** deben asignarse direcciones en la red local a los clientes VPN, asegurándose de que no sean visibles fuera de dicha red. También debe darse cierta información a los clientes, para que puedan acceder a los recursos protegidos de la red.
- **Cifrado de datos:** los datos que atraviesen las redes públicas deben ser ilegibles para todos, excepto para los clientes VPN y su servidor. Esto se consigue mediante tecnologías de cifrado de la información.

- **Gestión de claves:** para cifrar los datos, la solución VPN debe utilizar algún mecanismo de cifrado (basado en claves) que permita crear el túnel. Deben por tanto generarse, y renovarse cada cierto tiempo, las claves de cifrado, de modo que se mantengan la seguridad y la privacidad en las conexiones VPN.

4.1.1.5. Ventajas y Desventajas de una VPN.

Según Mario Galarza [6], manifiesta que existen varias ventajas y desventajas al momento de utilizar las redes privadas virtuales, las mismas que dependen del tipo de tecnología VPN que se utilice.

Las principales ventajas son:

- El costo de acceso remoto es económico.
- La tecnología VPN es una de las más seguras.
- Fácil accesibilidad a la información.
- Simplicidad.

Las principales desventajas son:

- Dependencia de la estabilidad de conexión.
- Desconocimiento y descuidos de parte del usuario final.
- Los equipos de los clientes están sin control de Administrador.

Existen además otras ventajas que ofrecen las redes privadas virtuales, cuya principal motivación de uso y difusión de esta tecnología, es la reducción de los costos de comunicaciones directos, tanto en costos de llamados de larga distancia como en vínculos dedicados [7]. Estas ventajas son:

- ✓ Permiten conectar redes físicamente separadas sin necesidad de usar una red dedicada, si no que a través de internet.
- ✓ Permiten asegurar la conexión entre usuarios móviles y la red fija.
- ✓ Una VPN puede crecer para adaptarse a más usuarios y diferentes lugares mucho más fácil que las líneas dedicadas.

4.1.2. Casos de Éxito Internacionales.

En esta sección se han recopilado casos de éxito internacionales orientados a la utilización de herramientas Open Source para el diseño de redes privadas virtuales. Estos casos de éxito se encuentran enfocados en dar soluciones prácticas a problemáticas de accesibilidad a los recursos internos de las universidades.

Además, estos casos de éxito, contribuyen de manera positiva con valiosa información para el desarrollo del presente trabajo de titulación, después de un análisis respectivo.

4.1.2.1. Caso de éxito 1: Servicio de Red Privada Virtual para la Universidad de Cádiz, España.

Figura 3: Guía de Instalación de VPN de la Universidad de Cádiz.

Fuente: Universidad de Cádiz (2016).

El Área de Informática y la Oficina del Software Libre (OSLUCA) diseñó una red privada virtual (VPN) [8] para la Universidad de Cádiz, la cual es una universidad española que se dedica a la educación, formación y capacitación de los miembros de la comunidad autónoma de Andalucía. Cuenta con cuatro campus universitarios distribuidos en la región de Cádiz, Bahía de Algeciras, Jerez de la Frontera y Puerto Real [9]. Todas las

sedes deben de tener conectividad, ya que necesitan acceder a los recursos internos que se encuentran albergados en la sede principal en Cádiz.

a) Problemas a solucionar.

El Área de Informática y la Oficina del Software Libre (OSLUCA) de la Universidad de Cádiz tenían que solucionar diferentes problemas expuestos por las autoridades, estudiantes y personal administrativo de la institución, de los cuales los principales eran:

- ✓ No se contaba con un servicio que logre acceder a la red interna de la universidad desde fuera del campus universitario en Cádiz.
- ✓ Falta de acceso a los recursos electrónicos de la Universidad.
- ✓ No se podía acceder a las revistas, libros electrónicos, bases de datos en línea y documentos a texto completo desde fuera del campus universitario.

b) Solución planteada.

La solución que generó el Área de Informática y la Oficina del Software Libre (OSLUCA) de la Universidad de Cádiz fue la de crear una VPN, la cual permita a sus miembros (PAS, PDI, becarios), debidamente autenticados, acceder a la red de la Universidad de Cádiz (UCA) desde fuera de ella (Internet) como si se estuviera dentro, mediante el establecimiento de un túnel de datos cifrado.

Para ello se utilizó el software OpenVPN, el motivo fue su fácil implantación y gran versatilidad. La topología escogida fue HOST TO LAN, es decir, los equipos de los estudiantes, administrativos y becarios que se encuentran fuera del campus universitario se conectan al campus central de la Universidad de Cádiz usando el software cliente OpenVPN.

c) Resultados obtenidos.

El resultado fue la creación del servicio de VPN para la Universidad de Cádiz, destacando los siguientes puntos:

- ✓ Se logró que los miembros universitarios, debidamente autenticados, accedan a la red de la Universidad de Cádiz (UCA) desde fuera de ella como si se estuviera dentro de la misma.

- ✓ Acceso a los recursos electrónicos de la Universidad de Cádiz.
- ✓ Acceso a las revistas, libros electrónicos, bases de datos en línea y documentos a texto completo desde fuera del campus universitario.

4.1.2.2. Caso de éxito 2: Red Privada Virtual de la Universidad de Valencia, España.

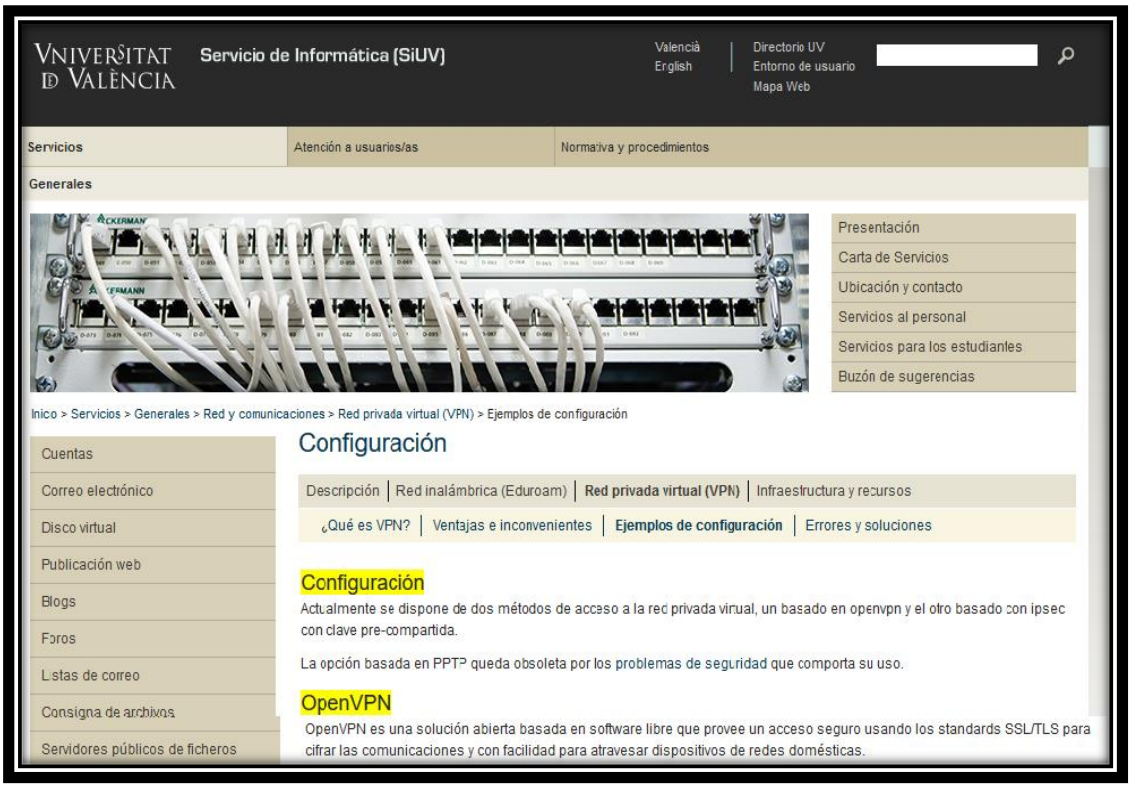


Figura 4: Configuración de VPN de la Universidad de Valencia.
Fuente: Universidad de Valencia (2015).

El Servicio de Informática (SiUV) diseñó una red privada virtual para la Universidad de Valencia [10], la cual es una universidad española que se dedica a la educación y capacitación de los miembros de la provincia de Valencia, España. Como toda sede universitaria cuenta con recursos electrónicos, revistas digitales y bases de datos en línea que se encuentran albergadas únicamente dentro de la red interna de la universidad.

a) Problema a solucionar.

El Servicio de Informática (SiUV) de la Universidad de Valencia tenía que solucionar los problemas de los diferentes estudiantes y personal administrativo de la institución, de los cuales los principales eran:

- ✓ Necesidad de un servicio que logre acceder a la red interna de la Universidad de Valencia desde fuera del campus universitario.
- ✓ Necesidad de acceder al catálogo bibliotecario, diccionarios, enciclopedias y películas electrónicas desde la casa u otro lugar externo a la universidad.
- ✓ No se podía acceder a las revistas, libros electrónicos, bases de datos en línea y documentos a texto completo desde fuera del campus universitario.

b) Solución planteada.

La solución que generó el Servicio de Informática (SiUV) de la Universidad de Valencia fue la de crear una VPN, la cual permita a los miembros de la comunidad universitaria, debidamente autenticados, acceder a la red de la Universidad de Valencia desde fuera de ella como si se estuviera dentro de la misma, mediante el establecimiento de un túnel de datos cifrado.

El Servicio de Informática de la Universidad de Valencia configuró una conexión VPN, para ello se utilizó el software OpenVPN, debido a que OpenVPN es una solución abierta basada en software libre que provee un acceso seguro usando los estándares SSL/TLS para cifrar las comunicaciones y con facilidad atravesar dispositivos de redes domésticas.

La topología escogida fue HOST TO LAN, es decir los equipos de los estudiantes y administrativos que se ubican fuera del campus universitario, se conectan a la red interna de la Universidad de Valencia usando el software cliente OpenVPN.

c) Resultados obtenidos.

El resultado que se obtuvo fue la creación del servicio de VPN para la Universidad de Valencia por parte del Servicio de Informática (SiUV), destacando los siguientes puntos:

- ✓ Se logró que los miembros de la comunidad universitaria logren acceder a la red interna de la Universidad de Valencia desde fuera del campus universitario.
- ✓ Acceso al catálogo bibliotecario, diccionarios, enciclopedias y películas electrónicas desde la casa u otro lugar externo a la universidad.
- ✓ Acceso a las revistas, libros electrónicos, bases de datos en línea y a documentos a texto completo desde fuera del campus universitario.

4.1.2.3. Caso de éxito 3: Acceso externo a los recursos electrónicos de la Universidad de Sevilla vía VPN.

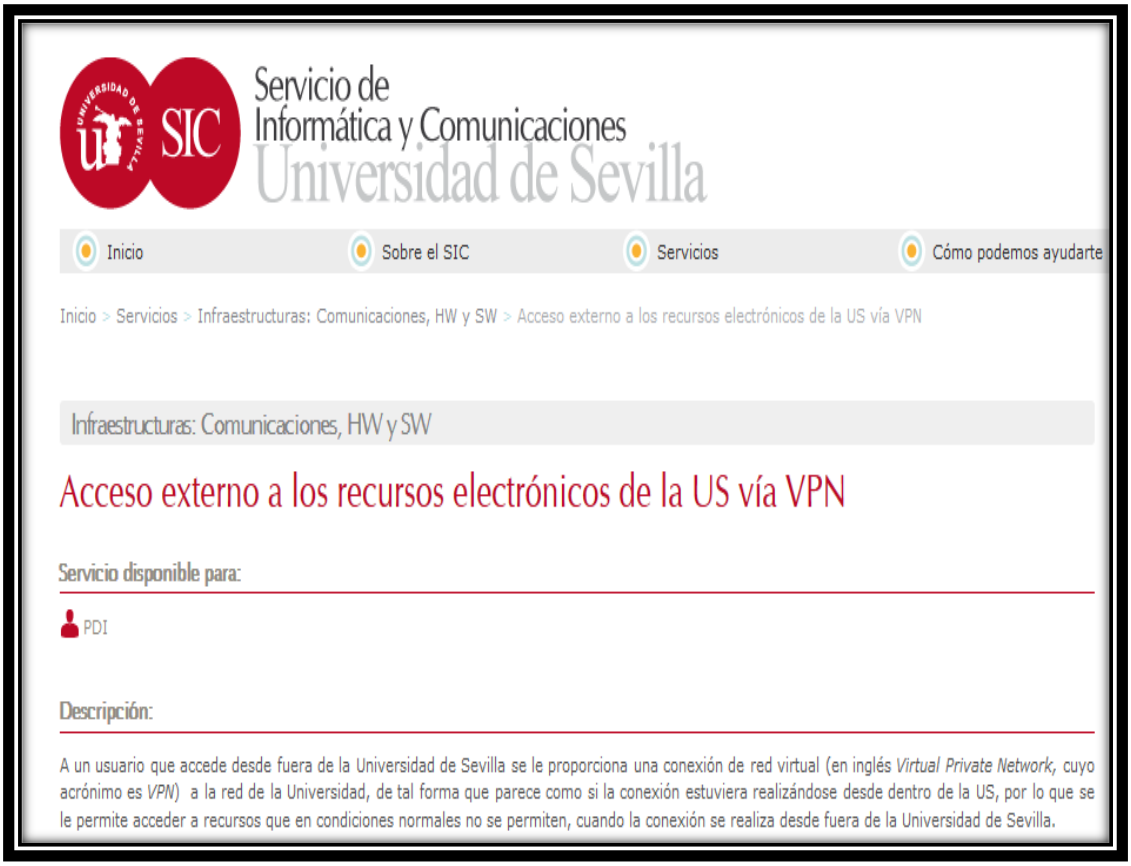


Figura 5: Acceso externo VPN de la Universidad de Sevilla.

Fuente: Universidad de Sevilla (2016).

El Servicio de Informática y Comunicaciones (SIC) diseñó una red privada virtual para la Universidad de Sevilla [11], la misma que es una Universidad Pública con sede en Sevilla, España. Como toda universidad cuenta con recursos electrónicos, revistas digitales, bases de datos y catálogos en línea que se encuentran albergados únicamente dentro de la red interna de la universidad. Surgiendo de ésta manera la necesidad de

acceder a los recursos internos que se encuentran únicamente albergados dentro de la Universidad de Sevilla.

a) Problema a solucionar.

El Servicio de Informática y Comunicaciones (SIC) de la Universidad de Sevilla tenía que solucionar el problema de la falta de un acceso a la red interna de la universidad desde un punto externo a la misma. Además de otros problemas expuestos por las autoridades, estudiantes y personal administrativo de la institución, de los cuales los principales eran:

- ✓ La falta de un servicio que permita acceder a los recursos de la Intranet de la Universidad de Sevilla, los mismos que sólo estaban disponibles dentro de la universidad.
- ✓ No se podía acceder a las revistas, libros electrónicos, bases de datos y documentos que únicamente se encontraban en la red interna de la Universidad de Sevilla.

b) Solución planteada.

La solución que planteó el Servicio de Informática y Comunicaciones (SIC) de la Universidad de Sevilla fue la de crear una VPN, la cual permita a sus miembros (PAS, PDI), debidamente autenticados, acceder a la red de la Universidad de Sevilla desde un punto externo, como si se estuviera dentro de la misma, mediante el establecimiento de un túnel de datos cifrados.

Para ello el Servicio de Informática y Comunicación de la Universidad de Sevilla utilizó el software OpenVPN, debido a su seguridad y fácil implementación. Lo que permitió que los equipos de los estudiantes y administrativos que se ubican fuera del campus universitario se conecten a la red interna de la Universidad de Sevilla, usando el cliente OpenVPN.

c) Resultados obtenidos.

El resultado que se obtuvo fue la creación del servicio de VPN para la Universidad de Sevilla por parte del Servicio de Informática y Comunicación (SIC), destacando los siguientes puntos:

- ✓ La creación de un servicio, que permitió a los miembros de la comunidad universitaria lograr acceder a la red interna de la Universidad de Sevilla desde fuera del campus universitario.
- ✓ Acceso a las revistas, libros electrónicos, bases de datos y a documentos desde fuera del campus universitario de Sevilla.

4.1.3. Casos de Éxito Nacionales.

En esta sección se detallan dos casos de éxito nacionales de implementación de redes privadas virtuales en las Universidades del Ecuador.

4.1.3.1. Caso de éxito 1: Servicio de Red Privada Virtual (VPN) Institucional de la Universidad Católica de Cuenca (UCACUE).

Figura 6: Servicio de VPN de la Universidad Católica de Cuenca.
Fuente: Universidad Católica de Cuenca (2016).

El Departamento de Tecnologías de la Información y Comunicación diseñó una red privada virtual para la Universidad Católica de Cuenca [12], la cual es una Universidad Ecuatoriana fundada el 7 de septiembre de 1970, en la ciudad de Cuenca, con

extensiones en Quito, Azogues, y la Amazonía. Como toda sede universitaria cuenta con revistas digitales y bases de datos científicas en línea que se encuentran albergadas únicamente dentro de la red interna de la universidad. Surgiendo de ésta manera la necesidad de acceder a los recursos internos que se encuentran únicamente albergados dentro de la Universidad Católica de Cuenca.

a) Problema a solucionar.

El Departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca tenía que solucionar los problemas de los diferentes estudiantes y personal administrativo de la institución, de los cuales los principales eran:

- ✓ Lograr acceder desde cualquier punto de Internet (desde casa, otra universidad, dispositivos móviles) a los servicios de red de la universidad, como si estuviese conectado físicamente dentro de la infraestructura de red propia de la Universidad Católica de Cuenca.
- ✓ La falta de un acceso remoto a los recursos de la Biblioteca Digital de la universidad (libros-e, bases de datos, revistas electrónicas).

b) Solución planteada.

La solución planteada por el Departamento de Tecnologías de la Información y Comunicación de la Universidad Católica de Cuenca fue la de crear un acceso remoto vía VPN a los recursos de la Biblioteca Digital (libros-e, bases de datos, revistas electrónicas) de la Universidad Católica de Cuenca.

Para ello el Departamento de Tecnologías de la Información y Comunicación utilizó el software OpenVPN. Lo que permitió que los equipos de los docentes, estudiantes y administrativos que se encuentran fuera del campus universitario tengan acceso remoto vía VPN a los recursos de la red interna de la Universidad Católica de Cuenca, usando el cliente OpenVPN.

c) Resultados obtenidos.

El resultado obtenido fue el diseño del servicio de VPN para la Universidad Católica de Cuenca por parte del Departamento de Tecnologías de la Información y Comunicación, destacando los siguientes puntos:

- ✓ Se logró obtener acceso remoto vía VPN a los servicios de red de la universidad, como si se estuviese conectado físicamente dentro de la infraestructura de red propia de la Universidad Católica de Cuenca.
- ✓ Se logró el acceso a los recursos de la Biblioteca Digital (libros-e, bases de datos, revistas electrónicas).

4.1.3.2. Caso de éxito 2: Sistema para Acceso Externo a Bases Digitales de la Universidad de Cuenca.

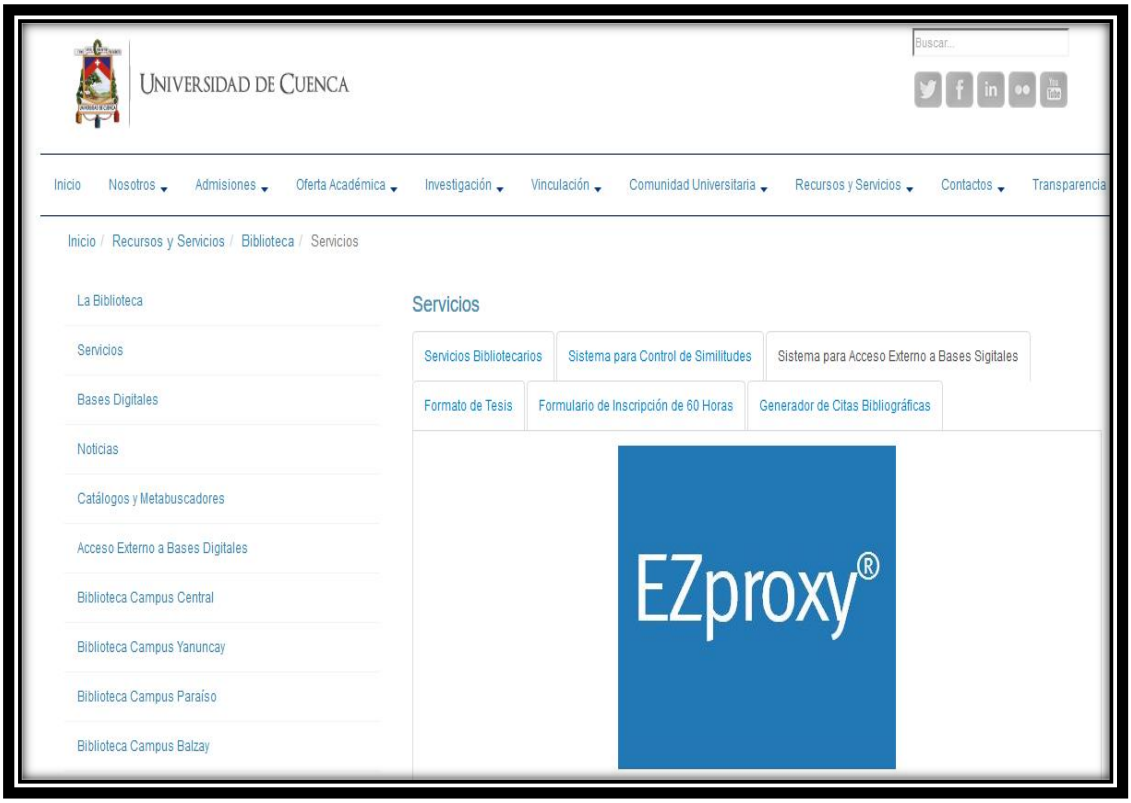


Figura 7: Servicio de Acceso Externo a Bases Digitales de la Universidad de Cuenca. Fuente: Universidad de Cuenca (2016).

La Dirección de Tecnologías de Información y Comunicación (DTIC) diseñó un sistema para el Acceso Externo a Bases Digitales en la Universidad de Cuenca [13], la cual es una universidad pública ecuatoriana situada en la ciudad de Cuenca, provincia del Azuay. La Universidad de Cuenca posee bases de datos científicas en línea que se encuentran albergadas únicamente dentro de la red interna de la universidad. Surgiendo de ésta manera la necesidad de contar con un sistema que permita acceder a los

recursos internos que se encuentran únicamente albergados dentro de la Universidad de Cuenca.

a) Problema a solucionar.

La Dirección de Tecnologías de Información y Comunicación (DTIC) de la Universidad de Cuenca tenía que solucionar el problema de la falta de acceso externo a las Bases Digitales de la universidad. Los principales problemas a solucionar eran:

- ✓ La falta de un acceso externo que permita acceder a los recursos internos de la Universidad de Cuenca.
- ✓ Necesidad de un servicio que logre acceder a las Bases Digitales que ofrecen material multidisciplinario a texto completo de las más importantes revistas y editoriales científicas: artículos académicos, reseñas, ebooks, tesis, videos, imágenes y estadísticas.

b) Solución planteada.

La solución planteada por la Dirección de Tecnologías de Información y Comunicación fue la de crear un sistema de acceso externo a las bases digitales de la Universidad de Cuenca.

Para ello la Dirección de Tecnologías de Información y Comunicación utilizó el software EZproxy. Lo que permitió que los equipos de los docentes, estudiantes y administrativos que se ubican fuera del campus universitario tengan acceso a los recursos de la red interna de la Universidad de Cuenca.

c) Resultados obtenidos.

El resultado obtenido fue el diseño del sistema de acceso externo a bases digitales para la Universidad de Cuenca por parte de la Dirección de Tecnologías de Información y Comunicación, destacando los siguientes puntos:

- ✓ Acceso a los servicios de red de la universidad como si se estuviese conectado físicamente dentro de la infraestructura de red propia de la Universidad.

- ✓ Acceso a las Bases Digitales que ofrecen material multidisciplinario a texto completo de las más importantes revistas y editoriales científicas: artículos académicos, reseñas, ebooks, tesis, videos, imágenes y estadísticas.

4.1.4. Herramientas VPN Open Source.

En la actualidad existen varias herramientas Open Source que permiten conectarse y diseñar redes privadas virtuales, a continuación se muestran las más importantes:

4.1.4.1. Herramienta LogMeIn Hamachi.

Figura 8: Herramienta LogMeIn Hamachi.

Fuente: Autor.

La herramienta LogMeIn Hamachi es una propuesta que apuesta por la facilidad de uso, además de ofrecer seguridad y opciones avanzadas para crear y acceder a redes VPN. Esta herramienta permite el acceso mediante un cliente de escritorio o directamente desde el navegador web, tanto para acceder a la red como para gestionar accesos, permisos y usuarios. Es gratuita para uso personal y de pago para uso profesional [14].

Esta herramienta permite la seguridad de las comunicaciones, gracias al cifrado SSL de 256 bits, a través de redes tanto públicas como privadas. Además controla el acceso y la utilización de la red, incluyendo la gestión de contraseñas, la autenticación, el bloqueo de red y la suscripción de red continua [15].

a) Características.

- Es una herramienta automática.
- Es un software multiplataforma: Windows, Mac OS, Linux, Android.
- Fácil uso y ofrece seguridad.
- Opciones avanzadas al crear y acceder a redes VPN.
- Acceso mediante cliente de escritorio o directamente desde el navegador.
- Gratuita para uso personal y de pago para uso profesional.

b) Ventajas.

- Ofrece una alternativa segura sobre las VPN's tradicionales.
- Ofrece comunicaciones cifradas.
- Permite que el equipo acceda de forma segura a los recursos de trabajo.

c) Desventajas.

- No funciona a través de proxys no transparentes.
- Vulnerabilidad de la red, ya que cualquiera puede entrar en la misma.
- Versión profesional pagada.

d) Demanda de la Herramienta.

Para determinar la demanda que tiene LogMeIn Hamachi, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de LogMeIn Hamachi son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 2. 9 millones de visitas.

- En la categoría de Internet y telecomunicaciones, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el ranking: 4690.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta LogMeIn Hamachi tiene una alta demanda.

4.1.4.2. Herramienta Itshidden VPN.

Figura 9: Herramienta Itshidden VPN.

Fuente: Autor.

La herramienta Itshidden es parte de Port 80 Limited (Seychelles), empresa holandesa reconocida por proporcionar VPN gratuito, así como también servicios de pago de VPN. Esta VPN crea una conexión segura para cifrar todos los datos con 128 bits que protegen la privacidad. No se necesita instalar ningún software. ItsHidden.com funciona en todas las plataformas, incluyendo Windows, Mac, Linux, iPhone, Android y no guarda log alguno de la actividad [17].

Itshidden proporciona un servicio de privacidad para navegar en Internet con gran capacidad, seguridad y sin complicación alguna [18].

a) Características.

- Es una herramienta automática.
- Software multiplataforma: Windows, Mac OS, Linux, Android.
- Conexión segura para cifrar datos con 128 bits.
- Maneja protocolos PPTP Y OpenVPN.
- La herramienta está en idioma Inglés.
- Es una versión online.

b) Ventajas.

- Es gratuita.
- Protege la privacidad.
- Evita detecciones Profundas.
- No se necesita instalar ningún software.
- No guarda historial alguno de la actividad realizada.
- Cuenta con servidores dedicados que son administrados por el propio equipo.

c) Desventajas.

- Únicamente sirve para navegar en internet.
- No permite administrar usuarios.
- No funciona como servidor VPN.

d) Demanda de la Herramienta.

Para determinar la demanda que tiene Itshidden VPN, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de Itshidden son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 142.1K visitas.

- En el ranking mundial, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el puesto: 541998.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta Itshidden tiene una baja demanda.

4.1.4.3. Herramienta TorVPN.

La herramienta TorVPN es la respuesta al anonimato a través del navegador, es simple y segura. TorVPN servirá especialmente para saltarse filtros de contenido, proteger una comunicación VoIP, acceder remotamente al ordenador de oficina y hogar a través de diferentes accesos como SSH, PPTP, Proxy TOR. La limitación es de 1GB mensual, pero funciona en Windows, Mac, iPhone e iPad [17].

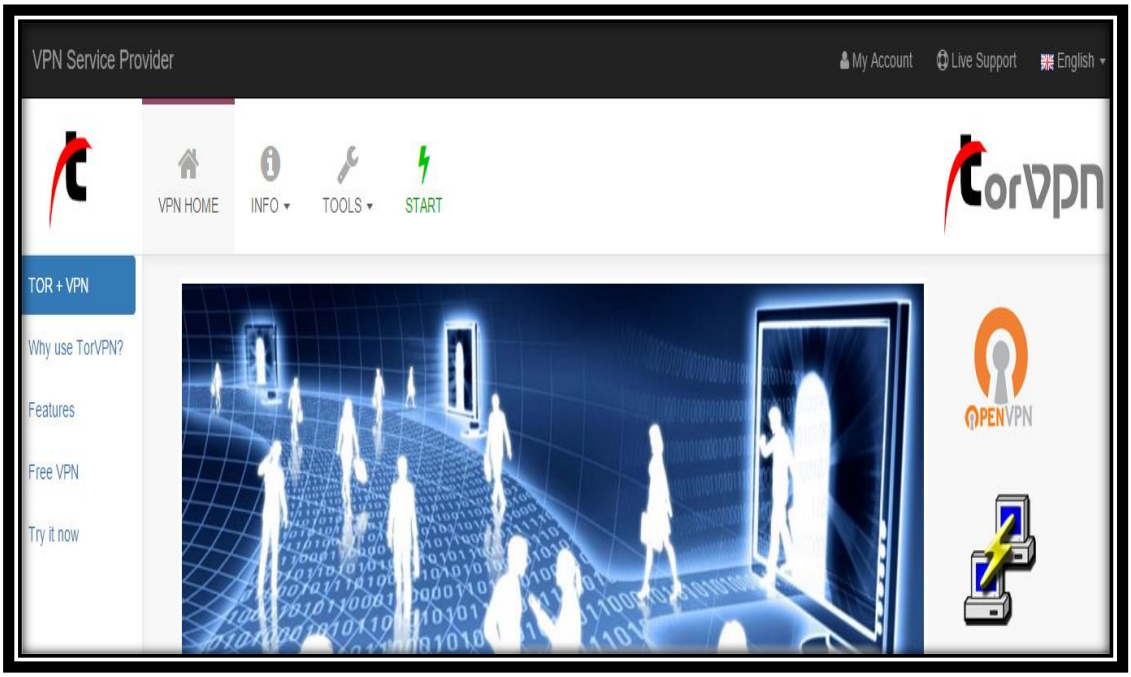


Figura 10: Herramienta TorVPN.

Fuente: Autor.

TorVPN es compatible con iPhone, Android, Windows, Linux, MacOS. Además con OpenVPN TCP + UDP, protocolos PPTP y SSH [19].

a) Características.

- Es una herramienta automática.
- Funciona en Windows, Mac, Android, Linux, IPhone e iPad.
- Maneja accesos SSH, PPTP y OpenVPN.
- Está en el idioma Inglés.
- Es una versión online.

b) Ventajas.

- Permite el anonimato a través del navegador.
- Es simple y segura.
- Sirve para saltarse filtros de contenido.
- Protege una comunicación VoIP.

c) Desventajas.

- No funciona como servidor VPN.
- No gestiona usuarios.
- No gestiona certificados.

d) Demanda de la Herramienta.

Para determinar la demanda que tiene TorVPN, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de TorVPN son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 306.5K visitas.
- En la categoría de Internet y telecomunicaciones, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el ranking: 18748.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta TorVPN tiene una baja demanda.

4.1.4.4. Herramienta The Securepoint TERRA

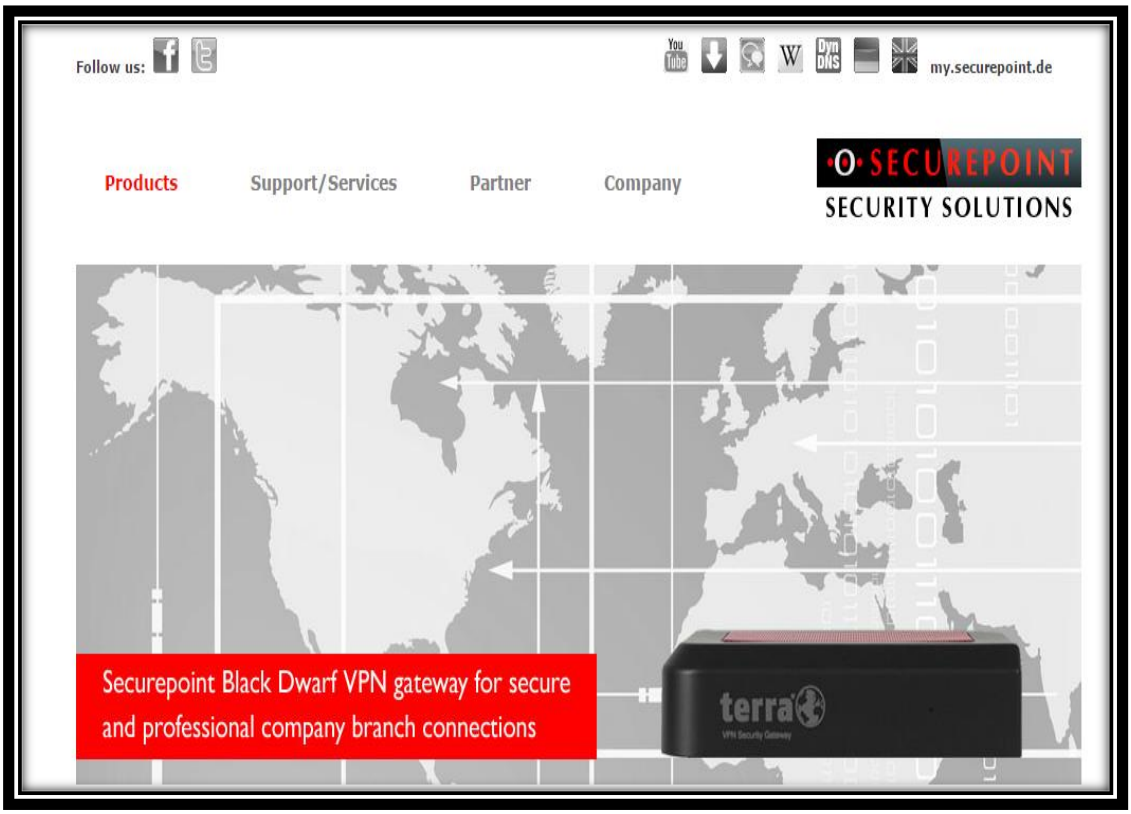


Figura 11: Herramienta The Securepoint TERRA.

Fuente: Autor.

The Securepoint TERRA es una puerta de enlace VPN, lo que la convierte en un servicio seguro para las pequeñas empresas que desean tener sus propias redes privadas. Esta herramienta permite el acceso remoto seguro mediante IPSEC, OpenVPN (SSL), L2TP y PPTP. Uno de los principales beneficios de Securepoint TERRA es su compatibilidad con otros sistemas VPN [20].

Esta herramienta permite una configuración extremadamente rápida, permite una configuración segura, inicio inmediato con la ayuda del asistente de configuración, el asistente de VPN permite ajustes rápidos y sencillos, y finalmente cuenta con una interfaz gráfica de usuario fácil [21].

a) Características.

- Es una herramienta manual.

- Se encuentra disponible en idioma Inglés.
- Es una puerta de enlace VPN.
- Permite el acceso remoto mediante IPSEC, OpenVPN, L2TP y PPTP.
- Cuenta con interfaz GUI.

b) Ventajas.

- Tiene compatibilidad con otros sistemas VPN.
- Su configuración es rápida y segura.
- Cuenta con una interfaz gráfica de usuario fácil.

c) Desventajas.

- Se necesita un equipo firewall para su configuración.
- Es una herramienta pagada.

d) Demanda de la Herramienta.

Para determinar la demanda que tiene The Securepoint TERRA, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de The Securepoint TERRA son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 192.9K visitas.
- En el ranking mundial, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el puesto: 394025.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta Securepoint TERRA tiene una baja demanda.

4.1.4.5. Herramienta Your – Freedom.

Figura 12: Herramienta Your - Freedom.

Fuente: Autor.

La herramienta Your – Freedom, también conocida con el nombre (tu libertad) da libertad de acción en casi cualquier servidor del mundo. Se puede descargar el software oficial o utilizar en un modo OpenVPN tanto en Windows, Mac o Linux. También como en otros casos, sus IPs empiezan a ser conocidas y a ser bloqueadas, pero por suerte se renuevan constantemente [17].

Los servicios de Freedom convierte la propia PC en una web que se maneja mediante un proxy sin censura que las aplicaciones pueden utilizar, incluso se puede estar conectado a Internet como si se estuviera utilizando un DSL o cable sin restricciones de conexión [22].

a) Características.

- Es una herramienta online y descargable.
- Funciona en plataforma Windows, Mac o Linux.
- Está en idioma Inglés.
- Soporta el protocolo OpenVPN.

b) Ventajas.

- Permite acceder a cualquier servidor del mundo.
- Sus direcciones IP se renuevan automáticamente.
- Se maneja mediante proxy.

c) Desventajas.

- No permite gestionar usuarios, ni contraseñas.
- No maneja cifrados.

d) Demanda de la Herramienta.

Para determinar la demanda que tiene Your – Freedom, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de Your – Freedom son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 999.2K visitas.
- En el ranking mundial, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el puesto: 119097.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta Your – Freedom tiene una demanda media.

4.1.4.6. Herramienta SoftEther VPN.

El proyecto VPN SoftEther es un programa de red privada virtual, de código abierto y libre, para plataformas de múltiples protocolos, este proyecto surge como un proyecto académico de la Universidad de Tsukuba [23].

Figura 13: Herramienta SoftEther VPN.

Fuente: Autor.

El Proyecto SoftEther VPN no es sólo una alternativa a los productos existentes VPN (OpenVPN, IPSec y MS-SSTP). SoftEther VPN tiene también un fuerte protocolo original SSL-VPN, el cual le permite penetrar cualquier tipo de cortafuegos. El protocolo SSL VPN tiene un buen rendimiento y baja latencia.

Además esta herramienta es libre y de código abierto, es fácil de establecer, funciona tanto como acceso remoto y de sitio a sitio, posee cifrado AES de 256 bits y RSA de 4096 bits, es compatible con Windows, Linux, Mac, Android, iPhone, iPad y Windows Mobile, los protocolos que soporta son SSL-VPN (HTTPS) y varios de los principales protocolos VPN (OpenVPN , IPSec , L2TP , MS-SSTP , L2TPv3 y EtherIP).

a) Características.

- Fue creada como proyecto académico de la Universidad de Tsukuba.
- Está disponible en idiomas múltiples.
- Es una herramienta descargable.
- Fácil de establecer, tanto como acceso remoto o de sitio a sitio.
- Maneja protocolos SSL-VPN, OpenVPN, IPSEC.
- Cuenta con cifrado AES de 256 bits.
- Multiplataforma: Windows, Linux, Mac, Android, iPhone e iPad.
- SoftEther VPN se basa en OpenVPN, adquiriendo sus funcionalidades.
- Tiene la funcionalidad de un servidor y cliente VPN.

b) Ventajas.

- Es una herramienta altamente segura y confiable.
- Permite penetrar cualquier tipo de cortafuegos.
- Es libre y de código abierto.

c) Demanda de la Herramienta.

Para determinar la demanda que tiene SoftEther VPN, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de SoftEther VPN son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 2.3 millones de visitas.
- En el ranking mundial, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el puesto: 62148.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta SoftEther VPN tiene una alta demanda.

4.1.4.7. Herramienta ExpressVPN.

Figura 14: Herramienta ExpressVPN.

Fuente: Autor.

ExpressVPN cuenta con seguridad SSL y maneja una encriptación de 256 bits. Su funcionalidad le permite ejecutarse en segundo plano para poder usar el Internet sin interrupciones [24].

La herramienta ExpressVPN, es compatible con múltiples plataformas de sistemas operativos (Windows, Mac, Linux, iOS y Android). Dentro de su funcionalidad, soporta todos los protocolos relacionados a redes privadas virtuales, de acuerdo al nivel de seguridad que se desee escoger para su uso.

a) Características.

- Es una herramienta automática.
- Es una aplicación online.
- Está disponible en un idioma multilenguaje.
- Cuenta con seguridad SSL.
- Maneja una encriptación de 256 bits.
- Es compatible con Windows, Mac, Linux, iOS y Android.
- Soporta los protocoles de túnel OpenVPN, L2TP, IPSEC y PPTP.

b) Ventajas.

- Posee una fuerte encriptación.
- Maneja un ancho de banda ilimitado.
- No deja rastro en su actividad de navegación.
- Cuenta con soporte las 24 horas.

c) Desventajas.

- Solo permite la conexión simultánea de un ordenador y un dispositivo de mano.
- No funciona como servidor VPN.
- Es gratis por tres meses y luego hay que adquirir licencia.

d) Demanda de la Herramienta.

Para determinar la demanda que tiene ExpressVPN, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de ExpressVPN son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 10.2 millones de visitas.
- En el ranking mundial, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el puesto: 11521.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta ExpressVPN tiene una alta demanda.

4.1.4.8. Herramienta OAST.

Figura 15: Herramienta OAST.

Fuente: Autor.

OAST es una herramienta multiplataforma (GUI) para OpenVPN-client, lo que permite gestionar múltiples usuarios. Es muy sencilla de utilizar y proporciona funcionalidad de base, tal como el estado de conexión de monitoreo. La aplicación está escrita en Java por lo que funciona tanto en Windows y Linux [25].

Esta herramienta es principalmente utilizada para sistemas Linux y soporta los protocolos OpenVPN, L2TP-IPsec, SSTP, PPTP.

Además esta herramienta es libre y de código abierto, es fácil de establecer, y permite obtener acceso remoto a servidores VPN mediante la configuración del archivo .ovpn.

Es una herramienta flexible, muy liviana y fácil de emplear, para utilizarla se necesita tener instalado OpenVPN.

a) Características.

- Está disponible en el idioma inglés.
- Funciona para los sistemas operativos Windows y Linux.
- Soporta los protocolos OpenVPN, L2TP, IPSEC, PPTP.
- Funciona como cliente para OpenVPN.

b) Ventajas.

- Permite gestionar múltiples usuarios.
- Es libre.
- Es de código abierto.
- Es flexible, liviana y fácil de usar.

c) Desventajas.

- Únicamente funciona como cliente VPN para realizar conexiones, y no como servidor.

d) Demanda de la Herramienta.

Para determinar la demanda que tiene OAST, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de OAST son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 96.8K visitas.
- En el ranking mundial, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el puesto: 933889.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta OAST tiene una baja demanda.

4.1.4.9. Herramienta VPNBOOK.

Figura 16: Herramienta VPNBOOK.

Fuente: Autor.

La herramienta VPNBOOK, es una red privada diseñada con las últimas tecnologías y técnicas criptográficas. Esta VPN realiza el enrutamiento de todo su tráfico de Internet a través de un túnel encriptado, y de esta manera eludir la censura del gobierno, la vigilancia y la supervisión corporativa.

VPNBOOK se esfuerza por mantener el internet como un lugar seguro y libre, proporcionando un protocolo PPTP libre y acceso a servicios de OpenVPN [26].

a) Características.

- Es una herramienta diseñada con las últimas tecnologías y técnicas criptográficas.
- Realiza un enrutamiento del tráfico de internet para no obtener censura.
- Maneja protocolos PPTP y acceso a servicios de OpenVPN.
- Se encuentra disponible en idioma Inglés.

b) Ventajas.

- Es una herramienta con tecnología de punta.
- Utiliza técnicas criptográficas avanzadas.
- Es segura.
- Es libre y totalmente gratis.

c) Desventajas.

- Sirve únicamente como acceso seguro a Internet, más no como un servidor VPN para gestionar usuarios

d) Demanda de la Herramienta.

Para determinar la demanda que tiene VPNBOOK, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de VPNBOOK son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 8.6 millones de visitas.
- En el ranking mundial, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el puesto: 15151.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta VPNBOOK tiene una alta demanda.

4.1.4.10. Herramienta OpenVPN Access Server.

La herramienta OpenVPN Access Server (OpenVPN-AS), es una solución libre para la implementación de Redes Privadas Virtuales y esta liberada bajo la licencia Pública General GPL versión 2.

OpenVPN Access Server incluye características que le permiten realizar configuraciones simples para redes privadas virtuales de Sitio a Sitio y de Acceso

Remoto. Además, incluye funcionalidades a nivel empresarial para proveer balanceo de cargas, failover, y controles de acceso refinados. Iniciando así con su premisa fundamental de que la complejidad es enemiga de la seguridad, OpenVPN-AS ofrece una alternativa ligera y económica a otras tecnologías VPN [27].

Figura 17: Herramienta OpenVPN Access Server.

Fuente: Autor.

El modelo de seguridad de OpenVPN-AS está basado en SSL; el estándar de la industria para comunicaciones seguras vía Internet. OpenVPN-AS implementa las extensiones dos o tres del modelo OSI usando los protocolos SSL/TLS, soporta métodos flexibles de autenticación para los clientes basados en certificados, Smart cards, y autenticación de doble factor, y permite políticas de control de acceso para usuarios o grupos en específico; usando reglas de firewall aplicadas a la interfaz virtual VPN.

- El Servidor de Acceso OpenVPN consta de tres componentes principales:

- Servidor OpenVPN.
- Interfaz del administrador.
- Cliente OpenVPN.

OpenVPN-AS es un software para la creación de redes privadas virtuales basadas en la tecnología SSL, lo cual permite conectar las oficinas remotas de una forma segura.

La tecnología que utiliza OpenVPN, se encuentra basada en estándares abiertos SSL/TLS y en la utilización de software libre. El Servidor de Acceso OpenVPN ofrece las siguientes características [27]:

- Genera una solución VPN de clase empresarial, basada en Software libre y GNU/Linux.
- Permite la creación de túneles VPN para conexiones Punto a Punto, Sitio a Sitio y usuarios móviles (Road Warriors).
- Utiliza como medio de transporte los protocolos TCP o UDP.
- Permite múltiples conexiones a una misma instancia sobre un único puerto TCP o UDP.
- Los túneles VPN funcionan sobre conexiones NAT (Network Address Translation) y direcciones IP dinámicas.
- Basada en los estándares de la industria SSL/TLS para comunicaciones seguras y autenticación, usa todas las características de OpenSSL para el cifrado, autenticación y certificación para proteger el tráfico privado de la red mientras transita por el Internet.
- Interfaz gráfica de usuario web, que permite disponer de todos los clientes, acorde al sistema operativo que se use.

a) Características.

- Es una herramienta que se encuentra online y también es descargable.
- Es una herramienta en idioma inglés.
- Se basa en la tecnología SSL.
- Permite conexiones sitio a sitio y de acceso remoto.
- Maneja 2 licencia gratis, si se desean más hay que adquirirlas.
- Maneja los protocolos SSL/TLS.
- Utiliza reglas firewall.
- Permite conexión de usuarios móviles (Road Warriors).
- Utiliza los protocolos 943 TCP y 1194 UDP como medio de transporte.
- Cuenta con un cifrado de 256 bits.

- Permite múltiples conexiones.
- Permite gestionar grupos de usuario.
- Maneja una autenticación PAM, LDAP, Active Directory y autenticación Radius,
- Cuenta con soporte nativo de cliente para los sistemas operativos GNU/Linux, Android, IOS, Windows y Mac OSX.

b) Ventajas.

- Es rápida y flexible.
- Permite la conexión de múltiples usuarios a la vez.
- Maneja comunicaciones seguras y posee autenticación.
- Es la herramienta más utilizada para el diseño Redes Privadas Virtuales.
- Utiliza certificaciones de seguridad.
- Utiliza NAT y direcciones IP dinámicas.
- Ofrece una alternativa ligera y económica respecto a otras tecnologías.
- Es una solución OpenSource, pero maneja licencias.
- Esta liberado bajo la licencia GPL.
- Permite gestionar grupos de usuarios.

c) Desventajas.

- Posee dos licencias gratis de prueba, si se desea más hay que adquirirlas a un precio de 10 dólares por cada licencia.
- No es compatible con IPSec.

d) Demanda de la Herramienta.

Para determinar la demanda que tiene OpenVPN Access Server, se ha utilizado la herramienta SimilarWeb PRO [16]. SimilarWeb PRO es una plataforma de conocimientos digitales que proporciona información analítica para cualquier sitio, herramienta o aplicación web.

Los datos obtenidos de OpenVPN-AS son los siguientes:

- Total de Visitas a la página web de la herramienta, en los meses de Mayo 2016 - Julio 2016: 11.3 millones de visitas.

- En el ranking mundial, en los meses de Mayo 2016 - Julio 2016 se encuentra ubicada en el puesto: 9303.

Lo que se puede deducir con los datos obtenidos anteriormente, es que la herramienta OpenVPN Access Server tiene una alta demanda.

4.2. CAPÍTULO II: ARQUITECTURAS, TIPOS Y PROTOCOLOS DE TÚNEL DE LAS REDES PRIVADAS VIRTUALES.

En la actualidad existen diferentes arquitecturas, tipos y protocolos de túnel que se emplean en el diseño de las redes privadas virtuales, algunas basadas en distintos métodos de seguridad y otras por su composición en hardware y software. Todas representan ventajas y desventajas a la hora de su aplicación, de tal manera, que se debe elegir la manera más adecuada y sobre todo, de menor riesgo y costo para la institución donde se desea implementar. Uno de los puntos más importantes en el diseño de redes privadas virtuales, es el protocolo de túnel que se utiliza para la implementación y seguridad de la misma.

En esta sección se detalla las diferentes arquitecturas, tipos y protocolos de seguridad que se toman en cuenta al momento de diseñar redes privadas virtuales como solución a un problema determinado.

4.2.1. Tipos de Redes Privadas Virtuales.

En la actualidad existen diferentes formas en que una institución puede implementar una red privada virtual. Los proveedores ofrecen diferentes tipos de soluciones VPN dependiendo del problema a solucionar. Las instituciones tendrán que decidir la opción que más les convenga acorde a su presupuesto, capacidad y requerimientos. Los principales tipos de VPN son:

- VPN basada en hardware.
- VPN basada en firewall.
- VPN basada en software.

4.2.1.1. VPN basada en hardware.

Las redes privadas virtuales basadas en hardware utilizan básicamente equipos dedicados, por ejemplo los routers, los cuales son seguros y fáciles de usar, ofreciendo un gran rendimiento, ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo, el cual utiliza muchos recursos del procesador para brindar otros servicios [28].

Estos sistemas están basados en routers que encriptan la información, son seguros y fáciles de usar, pero requieren de una configuración correcta y definida. Ofrecen un gran rendimiento, ya que no malgastan los ciclos del procesador, haciendo funcionar un Sistema Operativo.

Los sistemas basados en hardware son equipos dedicados, muy rápidos y de fácil instalación; aunque de un costo económico elevado. Estos sistemas proveen de la capacidad de asegurar un paquete en una parte de la red, a través del tunneling de paquetes [29].

4.2.1.2. VPN basada en firewall.

Este tipo de redes privadas virtuales aprovecha los mecanismos de seguridad del servidor, incluyendo la restricción de acceso a la red interna, y realiza la traducción de direcciones, satisfaciendo los requisitos de autenticación.

La mayoría de los firewalls comerciales también optimizan al núcleo del sistema operativo, al despojar a los servicios innecesarios o peligrosos, proporcionando de esta manera una seguridad adicional para el servidor VPN.

La desventaja de este tipo de tecnología es poder optimizar su desempeño de manera eficiente sin mermar las aplicaciones del sistema operativo [30]. El rendimiento en este tipo de VPN decrece, ya que no se tiene hardware especializado de encriptación.

4.2.1.3. VPN basada en software.

Este tipo de redes privadas virtuales son ideales en casos, donde ambos extremos de la VPN no están controlados por la misma organización o cuando diferentes firewalls y enrutadores se implementan dentro de la misma.

Estas redes privadas virtuales son independientes y ofrecen mayor flexibilidad en cómo se gestiona el tráfico de red. Muchos productos basados en software permiten que el tráfico de túnel dependa de la dirección o protocolo, a diferencia de los productos basados en hardware, que en general encapsulan el tráfico que manejan, independientemente del protocolo [30].

4.2.2. Arquitecturas de Redes Privadas Virtuales.

Dentro de las redes privadas virtuales existen arquitecturas con características muy particulares, dependiendo de su implementación. Para comprender esta situación, a continuación se explica las características más relevantes de las redes privadas virtuales más utilizadas.

4.2.2.1. Red Privada Virtual de Acceso Remoto.

Una VPN de acceso remoto consiste en usuarios que se conectan a la red de datos interna de una institución u organización, desde sitios remotos, utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso similar a estar dentro de la red local de la institución u organización [31].

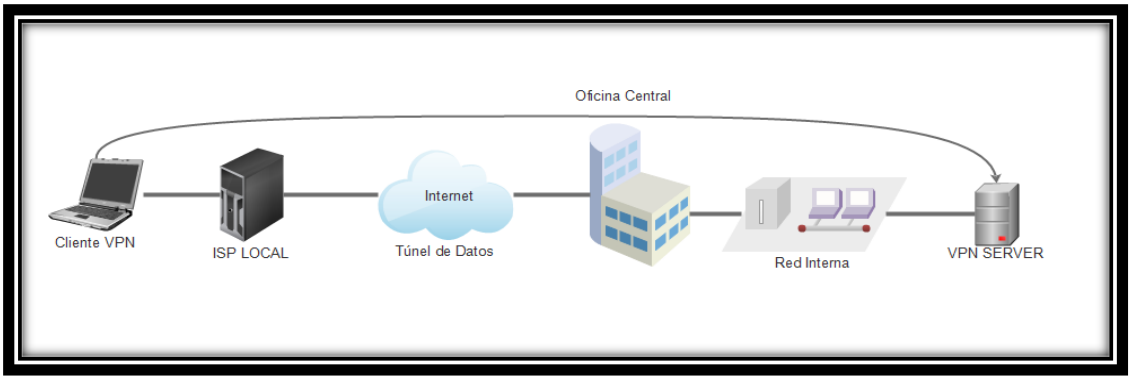


Figura 18: VPN de Acceso Remoto.

Fuente: Autor.

Con una VPN de acceso remoto, cualquier trabajador o cliente que se haya desplazado a otro país o se encuentre fuera de la red interna de la organización y que desee acceder a la base de datos de su organización, correo interno o cualquier otro recurso de su red institucional, solo tiene que conectarse a Internet y ejecutar el servicio de VPN.

4.2.2.2. Red Privada Virtual Sitio a Sitio.

Una VPN Sitio a Sitio, se trata de una conexión permanente y segura entre dos redes locales diferentes, utilizando Internet como vínculo de acceso. Los usuarios estarán permanentemente conectados a los recursos de las redes remotas [32].

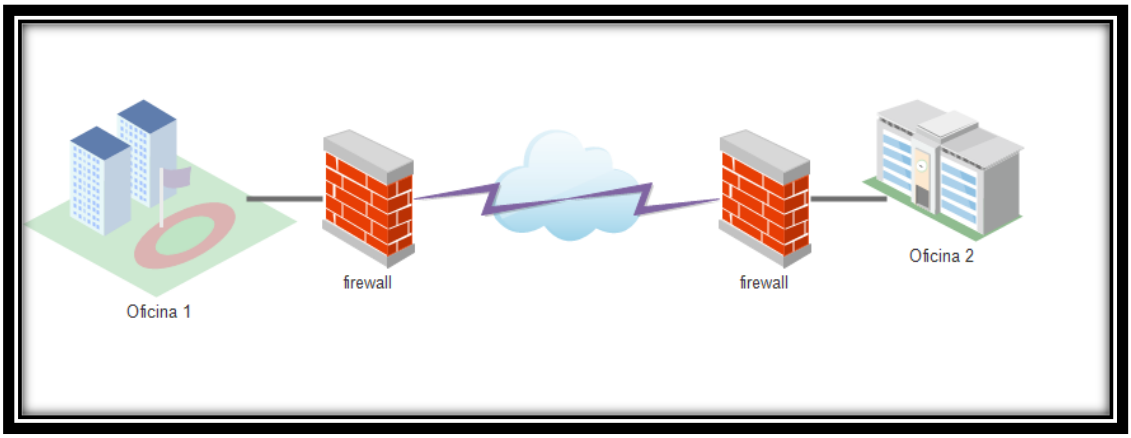


Figura 19: VPN Sitio a Sitio.

Fuente: Autor.

Esta arquitectura se utiliza para conectar oficinas remotas con la sede central de la organización. El equipo central VPN, que posee un vínculo a Internet, permanente acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, normalmente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto, sobre todo en las comunicaciones internacionales [30].

En este tipo de arquitectura, existen dos escenarios que se pueden presentar para su implementación, los cuales son:

- Tipo Intranet.
- Tipo Extranet.

a) Tipo Intranet.

Este tipo de red se define cuando una institución tiene una o más sucursales y se las desea unir en una sola red privada. Esto se logra creando una VPN para conectar ambas redes locales.

b) Tipo Extranet.

Este tipo de red se da cuando una institución tiene una asociación con otra y se desea conectar sus redes para permitir a estas instituciones trabajar en un ambiente compartido. Con esta arquitectura cada empresa tiene que controlar muy meticulosamente el acceso a los recursos de su red corporativa y a los datos que van a intercambiar con sus socios de negocios.

4.2.2.3. Red Privada Virtual Interna (over LAN).

Una VPN interna (over LAN) funciona como una VPN normal, salvo que dentro de la misma red local LAN de la institución. Sirve para aislar zonas y servicios de la misma red interna. Sirve también para mejorar las características de seguridad de una red inalámbrica WiFi [31].

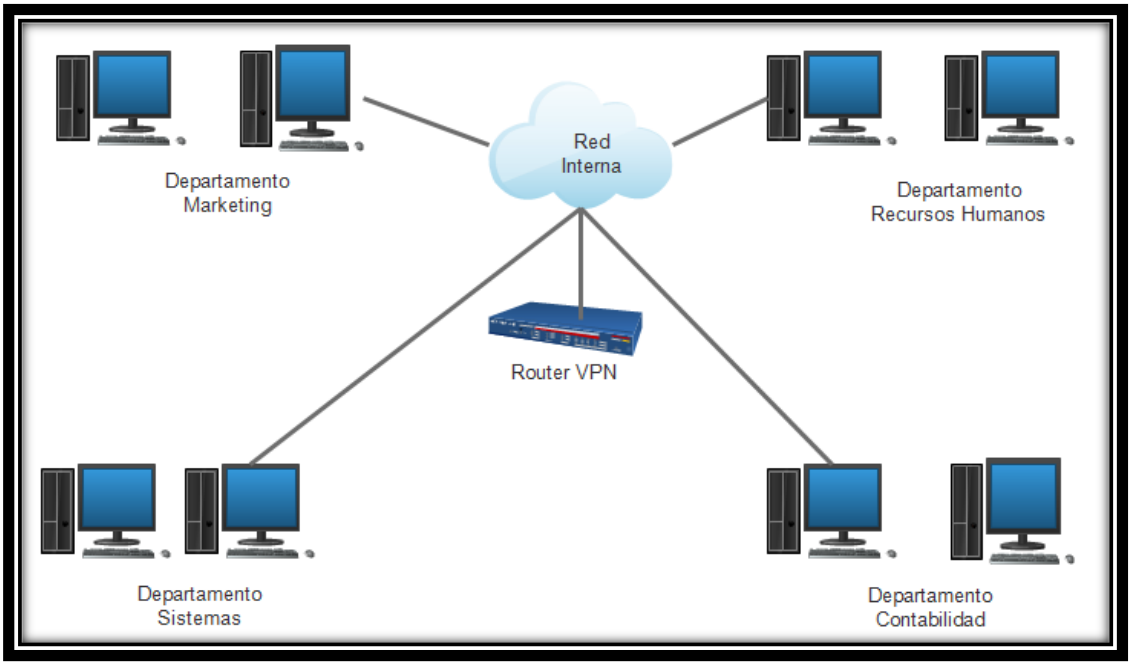


Figura 20: VPN Interna.

Fuente: Autor.

Esta red privada virtual es la menos difundida, pero una de las más poderosas para utilizarse dentro de una organización. Es una variante del tipo "acceso remoto", pero en vez de utilizar Internet como medio de conexión, se emplea la misma red LAN de la empresa. Sirve para aislar zonas y servicios de la red LAN interna.

Las Redes Privadas Virtuales Internas son una aplicación realmente desconocida, pero muy útil y potente, las mismas que consisten en establecer redes privadas virtuales dentro de una misma red local. El objetivo último de estas, es aislar partes de la red y sus servicios entre sí, aumentando la seguridad. Una aplicación muy típica de este modelo se utiliza para aumentar la seguridad en redes de acceso inalámbrico, separándolas así de la red física para evitar posibles fugas de información o accesos no autorizados [33].

4.2.3. Protocolos de Túnel de Redes Privadas Virtuales.

En la actualidad existen varios protocolos de túnel que permiten diseñar redes privadas virtuales, cada uno de estos protocolos se implementan con técnicas y seguridades diferentes. Una característica común de estos protocolos de VPN es que modifican el portal de defecto en el ordenador/dispositivo para desviar todo el tráfico de Internet a través de la VPN. A continuación se explicará los protocolos más importantes y de mayor uso al momento de implementar una red privada virtual.

4.2.3.1. Protocolo PPTP.

El protocolo PPTP (Point to Point Tunneling Protocol), permite el intercambio seguro de datos de un cliente a un servidor, formando así una red privada virtual basada en el Protocolo de Control de Transmisión / Protocolo de Internet (TCP/IP).

PPTP permite que el tráfico multiprotocolo se cifre y se encapsule en un encabezado IP para que, de este modo, se envíe a través de una red IP o una red IP pública, como Internet. PPTP puede utilizarse para el acceso remoto y las conexiones VPN entre sitios. Cuando se usa Internet como la red pública de una VPN, el servidor PPTP es un servidor VPN habilitado para PPTP con una interfaz en Internet y una segunda interfaz en la intranet [34].

PPTP puede utilizarse con diversos clientes de Microsoft. Al contrario que L2TP/IPSec, PPTP no requiere el uso de una infraestructura de clave pública (PKI). Gracias al cifrado, las conexiones VPN basadas en PPTP proporcionan confidencialidad de datos (los paquetes capturados no pueden interpretarse sin la clave de cifrado). Sin embargo, las conexiones VPN basadas en PPTP no ofrecen integridad de datos (pruebas de que los datos no se modificaron durante su tránsito), ni autenticación del origen de datos (pruebas de que los datos fueron enviados por un usuario autorizado) [34].

La seguridad de PPTP está totalmente rota y los sistemas con PPTP deberían ser sustituidos por otra tecnología de VPN. Existen incluso herramientas para romper las claves de las sesiones PPTP y descifrar el tráfico de una VPN [35].

En la TABLA I se muestran las principales características que se manejan en el protocolo PPTP según la empresa Giganews [36].

TABLA I: CARACTERÍSTICAS DEL PROTOCOLO PPTP

Características	Protocolo PPTP
Fuerza de Cifrado.	✓ 128 bits con protocolo MPPE.
Nivel de Seguridad.	✓ Normal.
Plataformas Soportadas.	✓ Windows, Linux, Mac, Android, iPhone/iPad.
Software adicional requerido.	✓ No.
Rendimiento.	✓ Muy Bueno.
Compatible con IP dedicada.	✓ Si.
Puerto VPN aleatorio.	✓ No.
Peligro de filtración.	✓ Si.
Seguridad VPN.	✓ Encriptación básica.
Velocidad de VPN.	✓ Rápido debido a la encriptación más baja.
Estabilidad.	✓ Funciona bien en la mayoría de puntos de acceso Wi-Fi, muy estable.
Compatibilidad.	✓ Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.

PPTP es una extensión de PPP, el cual es utilizado tradicionalmente para las conexiones dial-up. PPTP fue diseñado principalmente para las VPN de acceso remoto, sin embargo también puede trabajar en las VPN de sitio a sitio. PPTP opera en la capa 2 del modelo OSI [37].

Una desventaja que tiene PPTP es que no posee un estándar para la encriptación y la autenticación, ya que PPTP se ocupa únicamente de crear un túnel. Además, PPTP es el protocolo VPN menos seguro. L2TP e IPSec ofrecen mejores alternativas para garantizar la seguridad en una VPN.

4.2.3.2. Protocolo L2TP.

El protocolo L2TP (Layer 2 Tunneling Protocol) fue diseñado por un grupo de trabajo del IETF como el heredero aparente de los protocolos PPTP, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar [38].

L2TP permite cifrar el tráfico multiprotocolo y enviarlo a través de cualquier medio compatible con la entrega de datagramas punto a punto, como IP o ATM (modo de transferencia asincrónico). L2TP es una combinación de PPTP y L2F, una tecnología desarrollada por Cisco Systems, Inc. L2TP presenta las mejores características de PPTP y L2F.

A diferencia de PPTP, la implementación de Microsoft de L2TP no usa MPPE para cifrar los datagramas PPP. L2TP se basa en IPsec (protocolo de seguridad de Internet) en modo de transporte para los servicios de cifrado. La combinación de L2TP e IPsec se denomina L2TP/IPsec.

Tanto el cliente como el servidor VPN deben ser compatibles con L2TP e IPsec. La compatibilidad del cliente con L2TP está integrada en los clientes de acceso remoto de Windows Vista y Windows XP y la compatibilidad del servidor VPN con L2TP está integrada en los miembros de las familias de Windows Server® 2008 y Windows Server 2003. L2TP se instala con el protocolo TCP/IP [34].

El Protocolo de Túnel de Capa 2 (L2TP, Layer 2 Tunneling Protocol), es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de

Internet. Es aceptado ya por la mayoría de firmas y vendedores de productos de conectividad [39].

4.2.3.3. Protocolo IPSec.

El protocolo IPsec (abreviatura de Internet Protocol security), es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado [40].

Está basado en dos tipos de funcionamiento, el primero es el modo transporte de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSEC son el que envía y el que recibe; cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro. El segundo es el modo túnel, en el cual la encriptación se produce solo entre los routers de cada red.

IPSec es un protocolo definido por el IETF que se usa para transferir datos de manera segura en la capa de red. En realidad es un protocolo que mejora la seguridad del protocolo IP para garantizar la privacidad, integridad y autenticación de los datos enviados [4].

IPSec se basa en tres módulos:

- Encabezado de autenticación IP (AH), que incluye integridad, autenticación y protección contra ataques de REPLAY a los paquetes.

- Carga útil de seguridad encapsulada (ESP), que define el cifrado del paquete. ESP brinda privacidad, integridad, autenticación y protección contra ataques de REPLAY.

- Asociación de seguridad (SA) que define configuraciones de seguridad e intercambio de clave. Las SA incluyen toda la información acerca de cómo procesar paquetes IP.

En la TABLA II se muestran las principales características que se manejan en el protocolo L2TP junto a IPSec [36].

TABLA II: CARACTERÍSTICAS DEL PROTOCOLO L2TP/IPSec

Características	Protocolo L2TP/IPSec
Fuerza de Cifrado.	✓ 256 bits con cifrado AES.
Nivel de Seguridad.	✓ Bueno.
Plataformas Soportadas.	✓ Windows, Linux, Mac, Android, iPhone/iPad.
Software adicional requerido.	✓ No.
Rendimiento.	✓ Muy Bueno.
Compatible con IP dedicada.	✓ Si.
Puerto VPN aleatorio.	✓ No.
Peligro de filtración.	✓ Si.
Seguridad VPN.	✓ La máxima encriptación. Comprueba la integridad de los datos y encapsula los datos dos veces.
Velocidad de VPN.	✓ Necesita más proceso de la CPU para encapsular los datos dos veces.
Estabilidad.	✓ Compatible con dispositivos NAT.
Compatibilidad.	✓ Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.

4.2.3.4. Protocolo OpenVPN SSL/TLS.

Los protocolos SSL (Secure Socket Layer) y TLS (Transport Layer Security) son protocolos de la capa de transporte que proporcionan comunicaciones seguras en Internet. Los protocolos SSL versión 3.0 y TLS versión 1.0 son idénticos, una de las diferencias, son sus diseñadores.

SSL/TLS permite la autenticación tanto del cliente como del servidor, usando claves públicas y certificados digitales, y proporciona comunicación segura mediante el cifrado de la información entre emisor y receptor. SSL/TLS funciona por encima del protocolo de transporte (normalmente TCP) y por debajo de los protocolos de aplicación. Este protocolo está muy extendido para realizar actividades de comercio electrónico de tal manera que Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet [35].

OpenVPN utiliza el cifrado SSL. Este es el mismo método usado para asegurar los datos cuando se visita un sitio web que comienza con "https", como todos los sitios web bancarios. De hecho OpenVPN envía los datos sobre el mismo puerto que utilizan sitios https. Por lo tanto, es difícil para un ISP bloquear OpenVPN, porque si bloqueara el puerto https también acabarían bloqueando la mayoría de los sitios importantes y útiles en Internet. Para conectar a un servidor OpenVPN es necesario un conjunto de archivos de certificados. Estos certificados en medio de una llave, en donde la mitad de la llave debe estar en el ordenador del cliente y la otra mitad de la llave se almacena en el servidor y se necesita ambas partes si se quiere descifrar los datos. Por lo tanto, únicamente el servidor puede descifrar los datos.

Por esta razón de todos los protocolos VPN existentes en la actualidad, OpenVPN es el más seguro, incluso si un hacker está escuchando los datos y si de alguna manera roba certificados del ordenador, todavía no puede descifrar los datos que salen de la computadora porque aún faltaría la segunda mitad de la llave [41].

OpenVPN le permite verificar la autenticidad de su identidad, utilizando contraseñas previamente compartidas y certificados de usuario y contraseña. Al utilizar una configuración de servidores para múltiples clientes, le permite al servidor liberar certificados de autentificación para cada uno, utilizando una firma y la autoridad del certificado. Utiliza la biblioteca de encriptación de OpenSSL extensivamente, así como el protocolo SSLv3/TLSv1 y contiene muchas características adicionales de control y seguridad [42].

En la TABLA III se muestran las principales características que se manejan en el protocolo OpenVPN SSL/TLS [36].

TABLA III: CARACTERÍSTICAS DEL PROTOCOLO OpenVPN SSL/TLS

Características	Protocolo OpenVPN SSL/TLS
Fuerza de Cifrado.	✓ 256 bits con cifrado AES.
Nivel de Seguridad.	✓ Muy Bueno.
Plataformas Soportadas.	✓ Windows, Linux, Mac, Android, iPhone/iPad.
Software adicional requerido.	✓ Si.
Rendimiento.	✓ Excelente.
Compatible con IP dedicada.	✓ Si.
Puerto VPN aleatorio.	✓ Si 443/TCP.
Peligro de filtración.	✓ No.
Seguridad VPN.	✓ La máxima encriptación. Autenticación de los datos con certificados digitales.
Velocidad de VPN.	✓ Protocolo con mejor rendimiento. Velocidades elevadas, incluso en conexiones con alta latencia y a grandes distancias.
Estabilidad.	✓ La más fiable y estable, incluso tras routers inalámbricos, en redes no fiables, y en puntos de acceso Wi-Fi.
Compatibilidad.	✓ Compatible con la mayoría de los sistemas operativos de ordenadores de sobremesa y dispositivos Android móviles y tablets.

4.3. CAPÍTULO III: SISTEMAS OPERATIVOS PARA SERVIDORES.

En la actualidad existen diferentes tipos de sistemas operativos dedicados para servidores, algunos basados en software privativo y otros basados mediante el software libre. Todos representan ventajas y desventajas a la hora de su aplicación, de tal manera, que se debe elegir el más adecuado y sobre todo, el de menor riesgo y costo para la institución donde se desea implementar, lo más importante es la seguridad del mismo.

En esta sección se detalla los principales tipos de sistemas operativos para servidores que se encuentran disponibles en la actualidad.

4.3.1. Sistemas Operativos basados en Software Libre.

Existen diferentes tipos de sistemas operativos basados en Linux para la implementación de servidores. Los principales tipos de sistemas operativos libres son:

- CentOS.
- Debian.
- Ubuntu Server.
- Red Hat Enterprise Linux.

4.3.1.1. Sistema Operativo Centos.

Figura 21: Logo Sistema Operativo Centos.

Fuente: Autor.

CentOS o Community Enterprise Operating System es un sistema operativo de código libre basado enteramente en Red Hat Enterprise Linux con el objetivo de ser 100% compatible con el mismo. Centos es básicamente Red Hat pero sin el logotipo, marcas y soporte oficial de la compañía. Es el sistema operativo por excelencia para empresas y servidores [43].

CentOS es una distribución mantenida por la comunidad y derivada de los paquetes fuentes de Red Hat Enterprise Linux (RHEL). De tal forma, CentOS está enfocado en ser operacionalmente compatible con RHEL. La redistribución de CentOS Linux es libre y no hay que pagarlo. Cada versión de CentOS es mantenida por 10 años y es periódicamente actualizada (cada 6 meses) para incorporar un nuevo hardware. Esto

da como resultado un entorno seguro, de bajo mantenimiento, confiable, predecible y reproducible [44].

a) Características.

- Centos es un sistema operativo de fácil mantenimiento.
- Es idóneo para el uso a largo plazo en entornos de producción.
- Entorno favorable para los usuarios y mantenedores de paquetes.
- Apoyo a largo plazo de las principales aplicaciones para el servidor.
- Desarrollo activo de módulos y aplicaciones.
- Diseñado para trabajar con servidores.
- Presenta seguridad y estabilidad.
- En las actualizaciones se enfoca únicamente a los paquetes obsoletos y no actualiza a los demás módulos, permitiendo rapidez y solvencia.
- Administra la gestión de paquetes mediante el comando yum y rpm.

Además la última distribución la CentOS 7 presenta nuevas modalidades y características, las cuales son [45]:

- ✓ Actualización del núcleo del sistema: Kernel 3.10.0.
- ✓ Soporte para Linux Containers.
- ✓ Inclusión de VMware Tools y controladores de gráficos 3D.
- ✓ OpenJDK-7 como JDK por defecto.
- ✓ Contempla actualización de CentOS 6.5 a CentOS 7.0.
- ✓ Cambio a systemd, firewalld y GRUB2.
- ✓ XFS es el sistema de archivos por defecto y permite escalar la capacidad de almacenamiento del sistema hasta 500 terabytes. XFS es un sistema de archivos de 64 bits con journaling de alto rendimiento, y está especialmente indicado para discos grandes (superiores a 1 TB). No obstante y para necesidades menos exigentes se pueden emplear otros sistemas de archivos, como Ext4.
- ✓ iSCSI y FCoE (Fibre Channel over Ethernet) en el espacio del Kernel.
- ✓ Soporte para PPTv2 (Precisión Time Protocol).
- ✓ Soporte para tarjetas Ethernet 40G.
- ✓ Soporte UEFI.

b) Requerimientos del Sistema.

Los requerimientos mínimos del sistema para operar son:

- Memoria RAM: 512 MB (Mínimo), 1 GB (Recomendado).
- Disco Duro: 1 GB (Mínimo), 2 GB (Recomendado).
- Con entorno de escritorio: Disco Duro: 20 GB (mínimo), 40 GB (recomendado).
- Procesador: Intel x86-compatible (32 bit), (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/II/III, AMD Duron, Athlon/XP/MP). Intel Itanium (64 bit). Advanced Micro Devices AMD64 (Athlon 64, etc) e Intel EM64T (64 bit). IBM Mainframe (e Server zSeries y S/390).

c) Desventajas.

- Para escalar hay que añadir servidores.
- Limitaciones para audio y video sincronizado.
- Si falla el servidor falla todo.

4.3.1.2. Sistema Operativo Debian.

Figura 22: Logo Sistema Operativo Debian.

Fuente: Autor.

El Proyecto Debian surge como una asociación de personas que han hecho una causa común para crear un sistema operativo libre. Este sistema operativo creado se denomina Debian.

Debian o Proyecto Debian es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. Este

sistema se encuentra precompilado, empaquetado y en un formato sencillo para múltiples arquitecturas y varios núcleos [46].

a) Características.

El sistema operativo Debian al estar compuesto por software libre presenta ciertas características, las cuales son [47]:

- La disponibilidad en varias plataformas hardware. Es compatible con 11 plataformas.
- Posee una amplia colección de software disponible.
- Tiene un grupo de herramientas para facilitar el proceso de instalación y actualización del software.
- Mantiene un compromiso con los principios y valores involucrados en el movimiento del Software Libre.
- Posee un entorno gráfico, ya sea GNOME, KDE u otro.
- Maneja el formato de paquetes DEB y su ciclo de vida no es estable, manteniendo 1 año hasta su próxima versión.

b) Requerimientos del Sistema.

Los requerimientos básicos que debe poseer el sistema en donde se desee instalar Debian son los siguientes [48]:

- Memoria RAM: 128 MB (Mínimo).
- Memoria RAM: 512 MB (Recomendado).
- Disco Duro: 1024 MB (Mínimo).
- Disco Duro: 2 GB (Recomendado).
- Procesador: Basada en Intel x86, AMD64 e Intel 64, ARM con hardware FPU, MIPS (big endian), IBM/Motorola PowerPC, IBM S/390 64bit.

c) Desventajas.

- Se necesita tener conocimiento en Linux para poder utilizar y configurar el Sistema Operativo.
- El lanzamiento de versiones estables es largo. Los lanzamientos de versiones son casi de 1 año.

- La instalación es difícil para un usuario sin conocimiento en Linux.
- Resulta incómodo el uso de Debian para los usuarios de Windows, ya que en Debian la mayoría de las aplicaciones se realizan a través de la Shell de comando.

4.3.1.3. Sistema Operativo Ubuntu Server.

Figura 23: Logo Sistema Operativo Ubuntu Server.
Fuente: Autor.

El sistema operativo Ubuntu Server está dedicado especialmente para su uso en servidores. El uso de Ubuntu como servidor se ha extendido mucho en los últimos años, sobre todo para el uso de servidores web.

Ubuntu Server es un Sistema Operativo en donde se trabaja mediante consola, y normalmente ni si quiera a través del propio servidor, sino desde una conexión remota. El manejo de Ubuntu Server es muy similar al de cualquier otro Sistema Linux, pero con las particularidades de Ubuntu (como el sudo) [49].

a) Características.

El sistema operativo Ubuntu Server cuenta con algunas características que le permiten mejorar su rendimiento y competir en el ámbito de los servidores con software libre. Estas características son las siguientes [50]:

- Posee una cobertura de cinco años por parte de la empresa de Reino Unido Canonical.
- Se ejecuta en todas las arquitecturas - x86, x86-64, v7 ARM, ARM64, POWER8 e IBM s390x (LinuxONE).
- Tiene una ZFS estable, sistema de archivos rica en características con capacidades instantáneas.

- Cuenta con LXD Linux, mejoras del hipervisor de contenedores incluyendo calidad de servicio y los controles de recursos (CPU, memoria, bloque de E / S, almacenamiento).
- Permite instalar Ubuntu Core Snaps.
- Cuenta con una primera versión de producción del DPDK - línea de redes de núcleo de alta velocidad.
- Cuenta con Linux 4.4 Kernel e integra el servicio systemd.
- Posee certificación como invitado en AWS, Microsoft Azure, Joyent, IBM y HP Cloud.
- Cuenta con actualizaciones de Tomcat (v8), PostgreSQL (v9.5), acoplable v (1.10), de marionetas (v3.8.5), Qemu (v2.5), Libvirt (v1.3.1), LXC (v2.0), y MySQL (v5.6).
- Maneja el formato de paquetes DEB y mantiene un ciclo de vida de 5 años hasta su próxima versión.

b) Requerimientos del Sistema.

Los requerimientos básicos que debe poseer el sistema en donde se desee instalar el sistema operativo Ubuntu Server son los siguientes [51]:

- Memoria RAM: 128 MB (Mínimo), 512 MB (Recomendado).
- Disco Duro: 1 GB (Mínimo), 2 GB (Recomendado).
- Procesador: procesadores con arquitecturas x86, AMD64 o ARM.

c) Desventaja.

La principal desventaja que tiene Ubuntu Server es que no cuenta con soporte para los controladores privativos; la única alternativa son los libres.

4.3.1.4. Sistema Operativo Red Hat Enterprise Linux.

Figura 24: Logo Sistema Operativo Red Hat Enterprise Linux.

Fuente: Autor.

Red Hat Enterprise Linux (RHEL) es la distribución de Linux más conocida y popular en cuanto a servidores, además de ser uno de los más veteranos en el mundo de sistemas operativos. Ha contribuido con un gran número de aplicaciones para la comunidad Open Source en los últimos años, incluyendo Red Hat GFS y su sistema de archivos en clúster. Para el acceso a soporte y actualizaciones de seguridad se requiere que los clientes paguen una cierta cantidad de dinero [52].

El Sistema Operativo Red Hat Enterprise Linux se anticipa a los cambios en el ámbito de las Tecnologías de la Información que disipan los límites entre la informática física, virtual y cloud computing. Red Hat ha sido creada para un entorno de centros de datos moderno, con [53]:

- ✓ Virtualización y trabajo en red generalizado.
- ✓ Seguridad integral.
- ✓ Avances en hardware multinúcleo.

Red Hat Enterprise Linux puede facilitar una transición flexible y sin contratiempos de una organización al modelo de centro de datos de la nueva generación. Además soporta todas las arquitecturas de hardware, tiene compatibilidad en las distintas versiones y cuenta con un ciclo de vida de 10 años.

a) Características.

El sistema operativo Red Hat Enterprise Linux dispone de algunas características que le permiten alcanzar un grado de estabilidad, control y seguridad dentro del mercado actual. Estas características son las siguientes [53]:

- Es optimizado para sistemas multinúcleo altamente escalables.
- Gestiona la complejidad subyacente del sistema.
- Reduce los cuellos de botella de datos.
- Mejora el rendimiento de la aplicación.
- Reduce el consumo de energía.
- Garantiza una integridad total de los datos.
- Implantación sencilla de aplicaciones nuevas.
- Soporte y mantenimiento para todos los paquetes suministrados por Red Hat.
- Utiliza el formato de paquetes RPM.

b) Requerimientos del Sistema.

Los requerimientos básicos que debe poseer el sistema en donde se desee instalar Red Hat Enterprise Linux son los siguientes [54]:

- Memoria RAM: 512 MB (Mínimo), 2 GB (Recomendado).
- Disco Duro: 5 GB (Mínimo), 6 GB (Recomendado).
- Procesador: procesadores con arquitecturas AMD64 e Intel 64, IBM Power Systems (big endian), IBM Power Systems (Little endian), IBM System z.

c) Desventaja.

La principal desventaja que tiene Red Hat Enterprise Linux es que para acceder al soporte y actualizaciones del sistema operativo se debe realizar un determinado pago.

4.3.2. Sistemas Operativos basados en Software Privativo.

En la actualidad existen diferentes tipos de sistemas operativos basados en software privativo, pero el principal sistema operativo para la implementación de servidores es Windows Server. A continuación se detalla las principales características y desventajas que posee la última versión de Windows Server; el Sistema Operativo Windows Server 2012 R2.

4.3.2.1. Sistema Operativo Windows Server 2012 R2.

Figura 25: Logo Sistema Operativo Windows Server 2012.
Fuente: Autor.

Windows Server 2012 R2 es la versión de Windows Server actual y mejorada. Las ediciones de Windows Server 2012 R2 son optimizadas y simplificadas para que los

administradores puedan elegir fácilmente la edición que más les convenga de acuerdo a sus necesidades. Windows Server 2012 R2 cuenta con mejoras en virtualización, administración, almacenamiento, redes, infraestructura de escritorio virtual, protección de la información y del acceso, plataforma de aplicaciones y web [55].

Windows Server 2012 R2, en conjunto con System Center y Windows Azure, son las tres plataformas que forman parte de la visión hacia el sistema operativo en la nube de Microsoft [56]. Windows Server 2012 R2 es la versión para servidores de Windows 8.1 y es el sucesor de Windows Server 2008 R2.

a) Características.

El sistema operativo Windows Server 2012 R2 dispone de ciertas características que le permiten alcanzar un grado de control y seguridad, haciendo de este uno de los mejores sistemas operativos privativos para servidores. A continuación se detallan las principales características que posee [57]:

- El Administrador de Servidores se ha rediseñado buscando una gestión más sencilla de múltiples servidores.
- La característica Hyper-V Replica permite replicar una máquina virtual de una locación a otra con Hyper-V y una conexión de red sin ningún tipo de almacenamiento compartido.
- Una línea de comandos primero, una segunda mentalidad de interfaces gráficas.
- Nuevo Server Manager: Para crear Manage Server Groups.
- Compatibilidad con las APIs y tecnologías existentes.
- Ampliación de las capacidades de PowerShell.
- Posee gestión de direcciones IP fuera de la caja.
- Mejora de la fiabilidad de las estructuras en disco.
- Tiene capacidad de resiliencia incorporada.
- Mejor edición, selección SKU.
- Posee DirectAccess que permite un túnel seguro tipo VPN desde cualquier extremo de vuelta a la red corporativa, sin la sobrecarga y el impacto en el rendimiento de una VPN verdadera.
- Es un sistema operativo flexible, seguro, confiable y estable. Además posee soporte de documentación y actualizaciones.

b) Requerimientos del Sistema.

Los requerimientos básicos que debe poseer el sistema en donde se desee instalar Windows Server 2012 R2 son los siguientes:

- Memoria RAM: 512 MB (Mínimo).
- Disco Duro: 32 GB (más si hay 16 GB o más de RAM).
- Procesador: Windows Server 2012 sólo se ejecuta en procesadores x64 que cuenten con 1,4 GHz.

c) Desventaja.

La principal desventaja que posee Windows Server 2012 R2 es que al ser un sistema operativo privativo tiene un elevado costo para acceder al soporte y actualizaciones.

4.4. CAPÍTULO IV: ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD NACIONAL DE LOJA, A NIVEL DE SERVICIOS Y RECURSOS TECNOLÓGICOS IMPLEMENTADOS ACTUALMENTE.

En la actualidad, la Universidad Nacional de Loja cuenta con diferentes recursos tecnológicos implementados en la red institucional. Estos recursos tecnológicos se emplean para generar servicios que cubran las necesidades de todos los integrantes del campus universitario.

En esta sección se analiza la infraestructura de red, servicios y recursos tecnológicos que posee la Universidad Nacional de Loja.

4.4.1. Universidad Nacional de Loja.

La Universidad Nacional de Loja se encuentra ubicada, en la provincia y ciudad de Loja, en la ciudadela universitaria Guillermo Falconí Espinoza (La Argelia).

La Universidad Nacional de Loja, es una Institución de Educación Superior, laica, autónoma, de derecho público, con personería jurídica y sin fines de lucro, de alta calidad académica y humanística, que ofrece formación en los niveles: técnico y tecnológico superior; profesional o de tercer nivel; y, de postgrado o cuarto nivel; que realiza investigación científico-técnica sobre los problemas del entorno, con calidad, pertinencia y equidad, a fin de coadyuvar al desarrollo sustentable de la región y del país, interactuando con la comunidad, generando propuestas alternativas a los problemas nacionales, con responsabilidad social; reconociendo y promoviendo la diversidad cultural y étnica y la sabiduría popular, apoyándose en el avance científico y tecnológico, en procura de mejorar la calidad de vida del pueblo ecuatoriano [58].

Figura 26: Portada Universidad Nacional de Loja.
Fuente: Página de la Universidad Nacional de Loja (2016).

a) Misión.

Es misión de la Universidad Nacional de Loja, la formación académica y profesional, con sólidas bases científicas y técnicas, pertinencia social y valores; la generación y aplicación de conocimientos científicos, tecnológicos y técnicos, que aporten al desarrollo integral del entorno y al avance de la ciencia; el fortalecimiento del

pensamiento, la promoción, desarrollo y difusión de los saberes y culturas; y, la prestación de servicios especializados [58].

b) Visión.

La Universidad Nacional de Loja tiene como visión, consolidarse como una Comunidad Educativa, con excelencia académica, humanista y democrática, líder en el desarrollo de la cultura, la ciencia y la tecnología [58].

c) Área de Influencia.

Región Sur del Ecuador, ubicada en el extremo meridional del territorio ecuatoriano, conformada por las provincias de El Oro, Loja y Zamora Chinchipe. Comprende tres grandes zonas con clara diferenciación de clima, fisiografía, suelos y vegetación: la zona litoral o costera, que corresponde a la parte baja de la provincia de El Oro, conformada por la llanura costera, la llanura aluvial y el pie de monte occidental; la zona serraniega o andina, que corresponde a la parte alta de la provincia de El Oro y toda la provincia de Loja, típicamente montañosa, con prevalencia de terrenos de ladera y escasas áreas planas, onduladas y ligeramente inclinadas; y, la zona oriental o amazónica, que pertenece enteramente a la provincia de Zamora Chinchipe, constituida por la estribación oriental, los valles estrechos y alargados de la subcuenca del río Nangaritza y del curso medio del río Zamora, y, las vertientes de la cordillera Subandina, predominantemente montañosa con pocas áreas planas, onduladas y ligeramente inclinadas que conforman los valles estrechos [58].

4.4.1.1. Oferta Académica.

En la actualidad la Universidad Nacional de Loja oferta 35 carreras, distribuidas en cinco áreas Académico-Administrativas, las cuales son [59]:

- Área Agropecuaria de Recursos Naturales Renovables.

  - Carrera de Ingeniería Forestal.
  - Carrera de Ingeniería Agrícola.
  - Carrera en Manejo y Conservación del Medio Ambiente.
  - Carrera de Ingeniería Agronómica.

- Carrera de Medicina veterinaria y Zootecnia.

- Área de la Educación el Arte y la Comunicación.

- Carrera de Artes Plásticas.
- Carrera de Educación Básica.
- Carrera de Físico – Matemáticas.
- Carrera de Informática Educativa.
- Carrera de Psicología Educativa y Orientación.
- Carrera de Psicorehabilitación y Educación Especial.
- Carrera en Ciencias de la Comunicación Social.
- Carrera de Cultura Física.
- Carrera de Educación Musical.
- Carrera de Idioma Inglés.
- Carrera de lengua Castellana y Literatura.
- Carrera de Psicología Infantil y Educación Parvularia.
- Carrera de Químico – Biológicas.

- Área de la Energía, Las Industrias y los Recursos Naturales No Renovables.

- Carrera de Electromecánica.
- Carrera de Ingeniería en Sistemas.
- Carrera de Electrónica y Telecomunicaciones.
- Carrera de Geología Ambiental y Ordenamiento Territorial.

- Área Jurídica, Social y Administrativa.

- Carrera de Administración de Empresas.
- Carrera de Banca y Finanzas.
- Carrera de Derecho.
- Carrera de Trabajo Social.
- Carrera de Administración Pública.
- Carrera de Contabilidad y Auditoría.
- Carrera de Economía.
- Carrera de Turismo.

- Área de la Salud Humana.

  - Carrera de Enfermería.
  - Carrera de Medicina Humana.
  - Carrera de Psicología Clínica.
  - Carrera de Laboratorio Clínico.
  - Carrera de Odontología.

La Universidad Nacional de Loja cuenta también con un Área Administrativa en donde funcionan varios departamentos, los principales son:

- Administración Central.

  - Rectorado.
  - Vicerrectorado.
  - Dirección de Comunicación.
  - Departamento de Recursos Humanos.
  - Dirección de Telecomunicaciones e Información.

Además, la Universidad Nacional de Loja cuenta con la Modalidad de Estudios a Distancia (MED), la cual oferta actualmente diez carreras. Estas carreras son:

  - Carrera de Administración de Empresas.
  - Carrera de Bibliotecología e Información Científico – Técnica.
  - Carrera de Ingeniería en Contabilidad y Auditoría.
  - Carrera de Derecho.
  - Carrera de Psicorrehabilitacion y Educación Especial.
  - Carrera de Comunicación Social.
  - Carrera de Administración y Producción Agropecuaria.
  - Carrera de Psicología Infantil y Educación Parvularia.
  - Carrera de Informática Educativa.
  - Carrera de Trabajo Social.

La Universidad Nacional de Loja oferta también un Plan de Contingencia con diez carreras para garantizar la continuidad de los estudios de las y los estudiantes de las

Universidades y Escuelas Politécnicas que fueron suspendidas definitivamente por el CEAACES. Estas carreras son:

- Carrera de Enfermería.
- Carrera de Manejo y Conservación del Medio Ambiente.
- Carrera de Mecánica Automotriz.
- Carrera de Cultura Física.
- Carrera de Administración de Empresas.
- Carrera de Derecho.
- Carrera de Administración y Producción Agropecuaria.
- Carrera de Contabilidad y Auditoría.
- Carrera de Administración Turística.
- Carrera de Informática Educativa.

En el ámbito de los estudios de cuarto nivel, la Universidad Nacional de Loja con la finalidad de promover profesionales que generen y apliquen conocimientos innovadores y científico - técnicos, oferta los siguientes programas de postgrado:

- Área Jurídica, Social y Administrativa.

- Especialidad en Proyectos de Consultoría.
- Maestría en Derecho y Auditoria Ambiental.
- Maestría en Derecho Laboral y Medio Ambiente de Trabajo.
- Maestría en Derecho e Investigación Jurídica.
- Maestría en Administración de Empresas.
- Maestría en Gerencia Contable Financiera.
- Maestría en Administración Bancaria y Finanzas.
- Maestría en Derecho Empresarial.
- Maestría en Ciencias Penales.
- Maestría en Desarrollo Comunitario.
- Maestría en Derecho Procesal.
- Maestría en Gestión del Desarrollo del Turismo.

- Área de la Salud Humana.

- Medicina: Especialización de Medicina Familiar y Comunitaria.

- Medicina: Especialización en Cirugía General.
- Medicina: Especialización en Anestesiología.
- Medicina: Especialización en Pediatría.
- Medicina: Especialización en Medicina Interna.
- Medicina: Especialización en Ginecología y Obstetricia.
- Medicina: Especialización en Ortopedia y Traumatología.
- Medicina: Especialización en Radiología e Imagen.

4.4.1.2. Servicios de la Universidad Nacional de Loja.

La Universidad Nacional de Loja proporciona algunos servicios a la comunidad universitaria, los cuales se ofrecen con la finalidad de mejorar la calidad de vida de los estudiantes, docentes y administrativos de la institución. Estos servicios son de carácter gratuito y se puede acceder a ellos estando dentro de la institución. A continuación se detallan los servicios que brinda la Universidad Nacional de Loja.

a) Servicio de Bienestar Estudiantil.

La Unidad de Bienestar Estudiantil de la Universidad Nacional de Loja, pretende generar un medio que permita el progresivo desarrollo integral de toda la comunidad universitaria para implementar herramientas y ejecutar planes, programas y proyectos que promuevan el bienestar de todos los estudiantes, docentes y administrativos de la institución [60].

- **Servicios.**

Actualmente la Unidad viene funcionando como Proyecto de Bienestar Universitario aprobado por el H. Junta Universitaria en el año 2002 con los siguientes servicios:

- Infocentro Universitario.
- Servicio de la Defensoría de los Derechos Estudiantiles.
- Servicio de Trabajo Social.
- Servicio de Trabajo Social: Proyecto para las Estudiantes - Madres Embarazadas de la Universidad Nacional de Loja.
- Servicio de Trabajo Social: Programa para Estudiantes con Discapacidad.
- Servicio de Becas.

- Servicio de Salud.
- Servicio Psicopedagógico y Asistencia Psicológica.

b) Servicio de Radio Universitaria.

Radio Universitaria 98.5 es un medio de comunicación público de la Universidad Nacional de Loja, dispuesto para comunicarse con la comunidad a través de la coordinación, cooperación, consulta, intercambio y promoción del arte, la ciencia, la cultura y el desarrollo de Loja y la Región Sur. Se constituye en un laboratorio para las prácticas pre-profesionales de los estudiantes de la Carrera en Ciencias de la Comunicación Social; funciona las 24 horas al día. La radio tiene equipos que permiten a la institución producir y emitir todo tipo de información enmarcada en programas científicos, académicos, de orientación, entretenimiento y otros, de acuerdo a las necesidades institucionales y sociales [61].

- **Servicios.**

Actualmente la Radio Universitaria de la Universidad Nacional de Loja brinda los siguientes servicios:

- Apoyo Interinstitucional.
- Medio Académico.
- Servicios Sociales.
- Laboratorio de Prácticas Pre-Profesionales.
- Producción de Productos Radiofónicos.

c) Servicio de Unidad de Proyectos SENESCYT.

La Unidad de Proyectos SENESCYT de la Universidad Nacional de Loja se crea como un actor del Sistema Nacional de Nivelación y Admisión, amparada en los convenios u otros instrumentos jurídicos suscritos entre la UNL y la SENESCYT para la ejecución de los componentes de: Nivelación General, Nivelación de Carreras y Examen de Exoneración. La Unidad de Proyectos SENESCYT- UNL es una unidad de excelencia académica administrativa, pertinente y permanente, que contribuye con la admisión, la nivelación de conocimientos; y, el desarrollo de aptitudes de lógica y razonamiento de los aspirantes a ingresar en la Universidad Nacional de Loja [62].

- **Servicios.**

Actualmente la Unidad de Proyectos SENESCYT de la Universidad Nacional de Loja brinda los siguientes servicios:

- Coordinar con la SENESCYT-SNNA los cursos de nivelación a desarrollarse en la Universidad Nacional de Loja.
- Coordinar con la SENESCYT-SNNA los exámenes de exoneración aplicados a los aspirantes a ingresar en la Universidad Nacional de Loja.
- Coordinar con la SENESCYT-SNNA la habilitación de docentes del curso de nivelación.

d) Servicio de Sistema Bibliotecario.

El Sistema Bibliotecario de la Universidad Nacional de Loja, es un centro de información, estudio e investigación. Está inmerso en la generación del conocimiento, mediante el apoyo permanente en el desarrollo de los programas académicos, investigativos, de extensión y de vinculación con la colectividad. Es coordinado por la Jefatura General de Bibliotecas y lo integran las bibliotecas de las Áreas [63]:

- ✓ Área de la Educación, el Arte y la Comunicación.
- ✓ Área Jurídica, Social y Administrativa.
- ✓ Área Agropecuaria y de Recursos Naturales Renovables.
- ✓ Área de la Energía, las Industrias y los Recursos Naturales no Renovables.
- ✓ Área de la Salud Humana.
- ✓ Centro Histórico “Pío Jaramillo Alvarado”.

El campo de acción que maneja el Sistema Bibliotecario de la Universidad Nacional de Loja es establecer las políticas sobre el uso y manejo de la información científica y técnica. Además planifica, norma, supervisa y evalúa el desarrollo y funcionamiento del Sistema Bibliotecario. Coordina la vinculación con las unidades, redes y bibliotecas virtuales, para proveer a la comunidad universitaria y al público en general servicios de alta calidad, especializados y multidisciplinarios que estimulen la investigación y que amplíen la cobertura informativa disponible en diversidad de formatos y soportes, apoyándose en tecnologías de punta, liderando un plan de capacitación en la cultura informática [63].

Actualmente el Sistema Bibliotecario de la Universidad Nacional de Loja brinda los siguientes servicios:

- ✓ Préstamo de Libros.
- ✓ Préstamo de revistas y artículos Científicos.
- ✓ Préstamo de Tesis.
- ✓ Acceso a Biblioteca Virtual.

- ➢ **Servicio de Acceso a Biblioteca Virtual.**

La Universidad Nacional de Loja cuenta con el servicio de acceso a Biblioteca Virtual. Este servicio se utiliza para acceder al catálogo del Sistema Bibliotecario, Descubridores EDS, Red Universia y a las Bases de Datos Científicas que dispone la universidad.

Las Bases de Datos Científicas que dispone la Universidad Nacional de Loja, son las siguientes:

- o Base de Datos Academic OneFile.
- o Base de Datos BiblioMedex.
- o Base de Datos Colección LWW.
- o Base de Datos EBRARY.
- o Base de Datos E-LIBRO.
- o Base de Datos IEEE.
- o Base de Datos Informe Académico.
- o Base de Datos OvidSP.
- o Base de Datos Springer.
- o SCOPUS.
- o Base de Datos THOMSON & GALE.
- o Base de Datos Alexander.
- o Base de Datos Biblitechnia.
- o Base de Datos EBL.
- o Base de Datos EBSCO.
- o Base de Datos EQUAL.
- o Base de Datos InformaWorld.
- o Base de Datos Lexis Inteligencia Jurídica.
- o Base de Datos PROQUEST.

- Base de Datos Taylor Francis Online.
- Base de Datos WILEY.

Para lograr acceder a las Bases de Datos Científicas, que dispone la Universidad Nacional de Loja, únicamente se lo puede realizar desde el campus universitario, caso contrario no se puede acceder a las mismas (ver Figura 27).

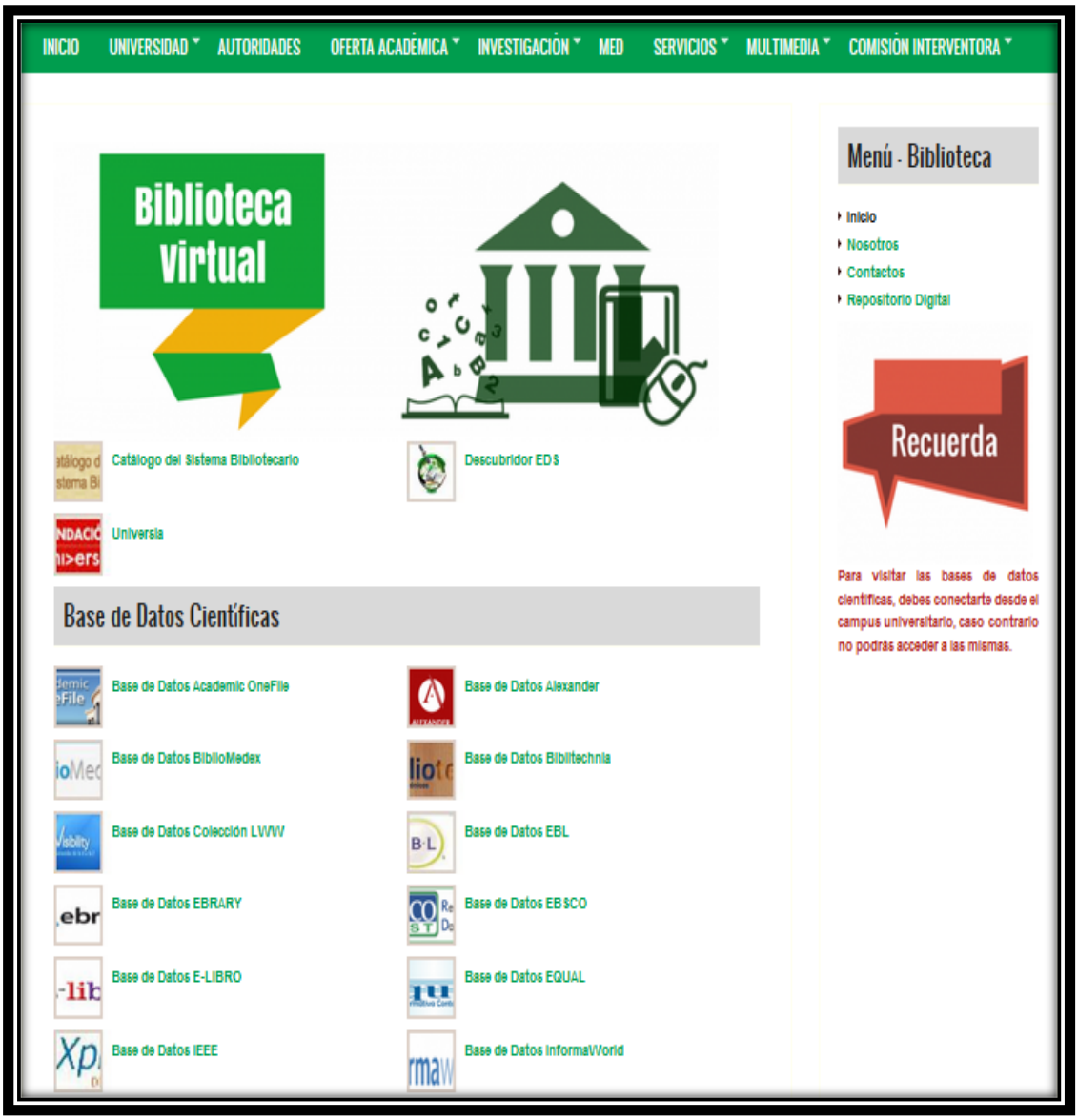


Figura 27: Biblioteca Virtual de la Universidad Nacional de Loja.
Fuente: Sistema Bibliotecario de la Universidad Nacional de Loja (2016).

4.4.1.3. Organigrama Estructural de la Universidad Nacional de Loja.

La Universidad Nacional de Loja, cuenta con una estructura organizativa que se encarga del manejo de la institución. En la Figura 28 se puede apreciar el organigrama estructural de la Universidad Nacional de Loja.

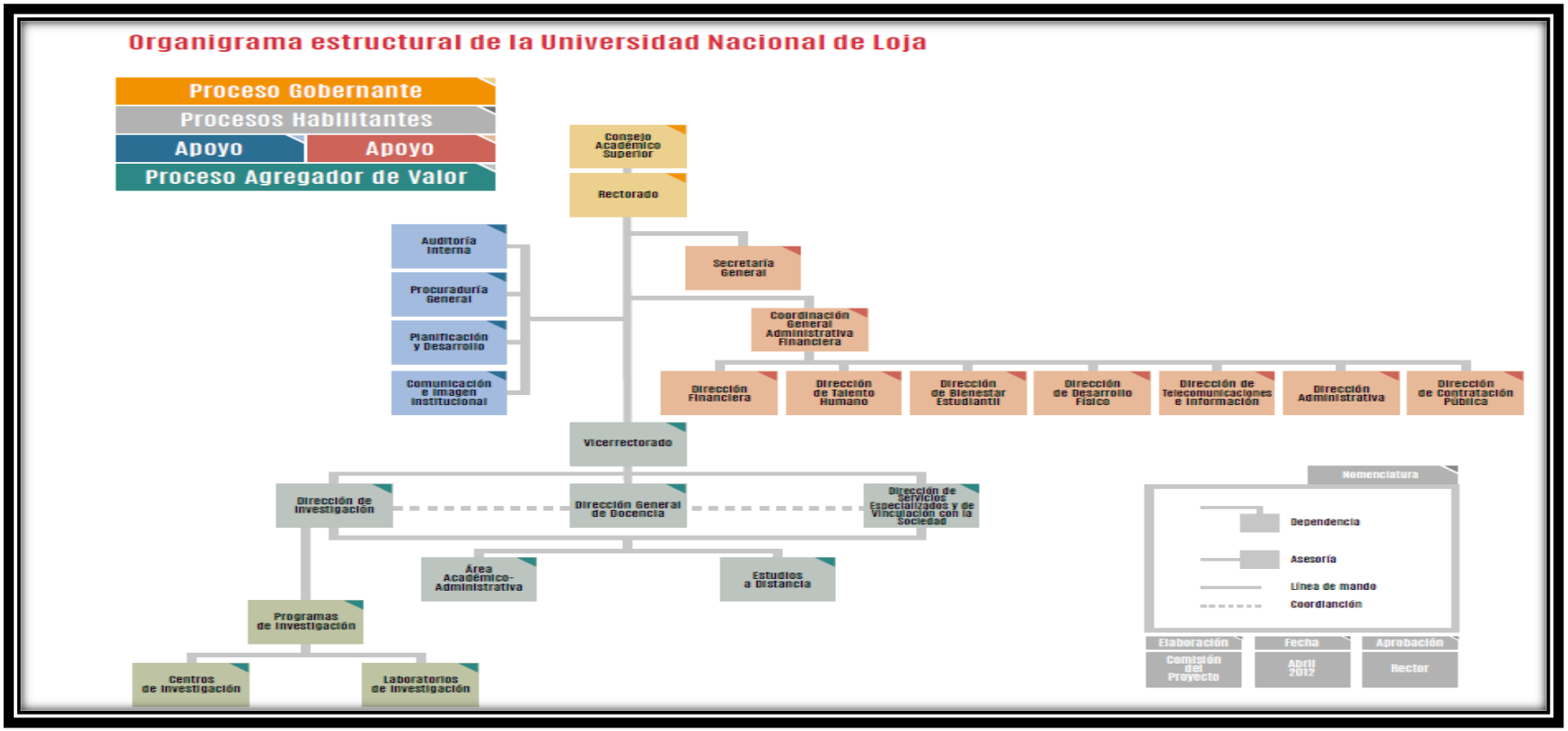


Figura 28: Organigrama estructural de la Universidad Nacional de Loja.

Fuente: Universidad Nacional de Loja (2016).

4.4.2. Dirección de Telecomunicaciones e Información de la Universidad Nacional de Loja.

La Dirección de Telecomunicaciones e Información de la Universidad Nacional de Loja, se encuentra ubicada en el organigrama estructural universitario, como dependencia de Coordinación General Administrativa Financiera. Sus instalaciones se encuentran ubicadas en el tercer piso del edificio dos de Administración Central.

La Dirección de Telecomunicaciones e Información de la Universidad Nacional de Loja, se la define como la unidad de servicios que tiene a su cargo a todas las áreas de la institución. La función que desempeña es fundamental para la comunidad universitaria, ya que se encarga de la administración e instalación de software, actualizaciones de antivirus, administración de accesos, y configuración de equipos de red y de computación, tanto para el sector administrativo y académico de toda la universidad.

4.4.2.1. Organigrama Estructural de la Dirección de Telecomunicaciones e Información de la Universidad Nacional de Loja.

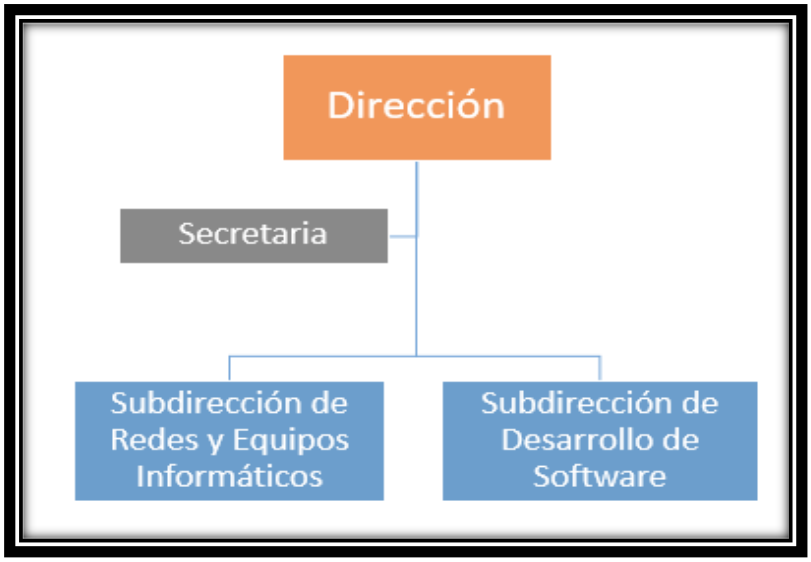


Figura 29: Organigrama estructural Dirección de Telecomunicaciones e Información.
Fuente: Autor.

La Dirección de Telecomunicaciones e Información de la Universidad Nacional de Loja, se encuentra liderada por el Ing. Milton Leonardo Labanda Jaramillo, quien funge como director de dicha entidad. La Subdirección de Redes y Equipos Informáticos, se

encuentra a cargo del Ing. John Calderón, mientras que la Subdirección de Desarrollo de Software, se encuentra a cargo del Ing. Edison Coronel. En la Figura 29 se puede apreciar el organigrama estructural de la Dirección de Telecomunicaciones e Información de la Universidad Nacional de Loja.

4.4.2.2. Subdirección de Redes y Equipos Informáticos de la Universidad Nacional de Loja.

a) Misión.

Planificar, coordinar y controlar la implementación y mantenimiento de redes informáticas; así como la renovación y mantenimiento de los equipos informáticos; para el efectivo cumplimiento de las actividades académicas y administrativas de la Universidad Nacional de Loja [64].

b) Funciones que desempeña.

La Subdirección de Redes y Equipos Informáticos de la Universidad Nacional de Loja, cumple con diversas actividades para administrar, controlar y gestionar los recursos de la red interna de la universidad. Las actividades que realizan son las siguientes [64]:

- Planifica, coordina, controla y evalúa los estudios, diseños, implementación, construcción y mantenimiento de redes informáticas, según los requerimientos académicos e institucionales.

- Planifica, coordina y evalúa la adquisición y/o renovación de los equipos informáticos de propiedad de la Universidad Nacional de Loja.

- Planifica, organiza, coordina y controla el apoyo técnico a los centros de cómputo y laboratorios informáticos de las áreas académicas y centros especializados, para garantizar el funcionamiento adecuado de sus redes y equipos informáticos.

- Planifica, organiza y coordina el soporte técnico, mantenimiento preventivo y correctivo a las redes y equipos de los sistemas informáticos de la Universidad Nacional de Loja.

- Coordina la elaboración de los términos de referencia de los pliegos para la adquisición de equipos informáticos y materiales para su mantenimiento.

- Coordina la capacitación a los usuarios internos en la operación de los equipos informáticos y TIC's, en coordinación con los responsables de las otras secciones de la unidad administrativa.

4.4.3. Infraestructura de la Red de Datos de la Universidad Nacional de Loja.

La Universidad Nacional de Loja posee una red de datos interna con topología de estrella, la cual permite la distribución y acceso a los servicios en red que se ofrece a toda la comunidad universitaria que se encuentra dentro y fuera del campus universitario.

El servicio de internet que posee la Universidad Nacional de Loja, es suministrado por la empresa TELCONET - CEDIA. Este servicio se suministra a través de fibra óptica, y el ancho de banda actual es de 300 megas.

La Universidad Nacional de Loja, cuenta con un Data Center (cuarto frío), en el cual están alojados algunos equipos de red. Este Data Center se encuentra ubicado en la Subdirección de Redes y Equipos Informáticos de la Dirección de Telecomunicaciones e Información, desde esta unidad se administra y distribuye los servicios de red a las diferentes áreas que conforman la universidad.

Actualmente la Universidad Nacional de Loja cuenta una red de datos tanto inalámbrica como cableada, cualquier miembro de la Comunidad Universitaria puede acceder a ellas sin restricción alguna. Las principales redes inalámbricas con que cuenta la universidad son:

- INVITADOS UNL.
- CAMPUS UNL.
- UNL.
- EDUROAM.

4.4.3.1. Servicios en Red de la Universidad Nacional de Loja.

La Subdirección de Redes y Equipos Informáticos de la Universidad Nacional de Loja, proporciona de varios servicios en red a todos los miembros de la comunidad universitaria. Existen servicios en red que únicamente pueden ser accedidos dentro del campus universitario, y servicios en red que se pueden acceder desde una red externa a la institución.

a) Servicios en red que pueden ser accedidos únicamente dentro de la red interna de la Universidad.

- Servicio de Conexión a Internet.

Para acceder al servicio de internet de la Universidad Nacional de Loja, se lo puede realizar de dos formas:

- Infraestructura de red cableada: Proporciona conectividad a los equipos de sobremesa ubicados en los puestos de trabajo, aulas, laboratorios, impresoras y equipos multifunción dotados con capacidad de conexión a red, así como servidores, NAS, teléfonos IP.
- Infraestructura de red inalámbrica: Ofrece los servicios de conexión Wi-Fi a través de las redes Eduroam, UNL, Invitados UNL, Campus UNL, y todos los puntos de acceso Wi-Fi de las áreas académicas y administrativas de la institución.

- Servicio de Telefonía IP (VoIP).

Para acceder al servicio de telefonía VoIP, únicamente se lo puede realizar desde la red interna de la Universidad Nacional de Loja.

- Servicio de Acceso a Biblioteca Virtual.

La Biblioteca Virtual de la Universidad Nacional de Loja, ofrece los servicios de acceso al catálogo del Sistema Bibliotecario, Descubridores EDS, Red Universia, y Bases de Datos Científicas que dispone la universidad.

Para acceder a los servicios de Biblioteca Virtual de la Universidad Nacional de Loja, únicamente se lo puede realizar desde el campus universitario; ya que no existe un servicio que permita acceder a ellos desde fuera del campus de la universidad.

b) Servicios en red que pueden ser accedidos dentro y fuera del campus universitario.

Los servicios en red a los que se pueden acceder desde dentro y fuera del campus universitario, son los siguientes:

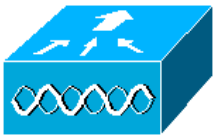
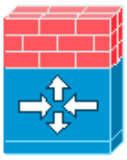
- ✓ Servicio de Acceso a la Página Web de la Universidad Nacional de Loja.
- ✓ Servicio de Acceso al SGA Estudiantes.
- ✓ Servicio de Acceso al SGA Docentes.
- ✓ Servicio de Acceso al Entorno Virtual de Aprendizaje (EVA).
- ✓ Servicio de Acceso al Correo Institucional.
- ✓ Servicio de Acceso a Moodle.
- ✓ Servicio de Acceso a la Radio Universitaria.
- ✓ Servicio de Acceso a la Modalidad de Estudios a Distancia (MED).
- ✓ Servicio de Acceso a Cursos Virtuales.

4.4.3.2. Diagrama de Red de Datos de la Universidad Nacional de Loja.

La estructura de red de la Universidad Nacional de Loja, se encuentra compuesta por un modelo jerárquico de tres capas: núcleo, distribución y acceso (ver Figura 30).

Para facilitar la comprensión del diagrama de red de datos indicado en la Figura 30, es necesario conocer los símbolos que se emplean en él, para ello se ha elaborado una tabla en donde se representa la simbología y significado de cada elemento del diagrama de red de datos de la Universidad Nacional de Loja (ver TABLA IV).

TABLA IV: SIMBOLOGÍA DEL DIAGRAMA DE RED DE DATOS

SÍMBOLO	SIGNIFICADO
	*Cisco – Cloud White*
	*Cisco – NAT*
	*Cisco – WLAN controller*
	*Cisco – Workgroup switch*
	*Cisco - Router*
	*Cisco – IOS Firewall*
	*Cisco – Multilayer switch*
	*Cisco – ATM Tag Sw Gigabit Router*

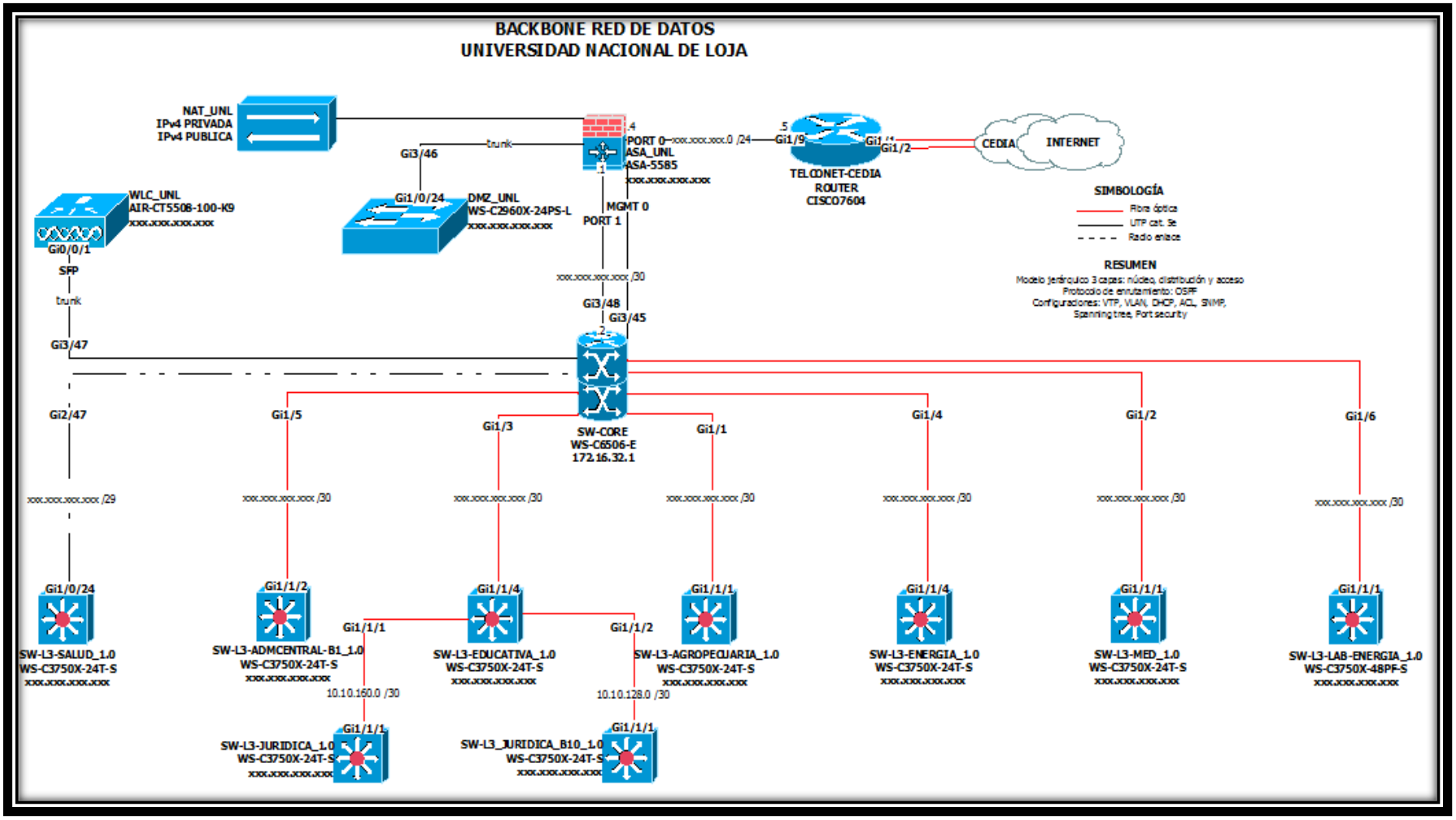


Figura 30: Diagrama Red de Datos de la Universidad Nacional de Loja.

Fuente: Subdirección de Redes y Equipos Informáticos (2016).

4.4.3.3. Recursos Físicos de la Infraestructura de Red de Datos de la Universidad Nacional de Loja.

La infraestructura de red de la Universidad Nacional de Loja, está conformada por varios equipos de redes, los cuales permiten la administración y gestión de los servicios en red dentro del campus universitario.

En el Data Center de la Universidad Nacional de Loja, se encuentran alojados tres Racks (armarios de equipos de red), de los cuales, dos de ellos se encuentran destinados para el alojamiento de servidores. Mientras que en el tercer Rack, se encuentran instalados diferentes equipos de red; quienes son los encargados de brindar servicios tecnológicos a la comunidad universitaria. Los equipos de red que se encuentran instalados son:

a) Sistema de Alimentación Ininterrumpida (SAI).

En el Rack de equipos de red, se encuentran alojados dos equipos de alimentación ininterrumpida o mejor conocidos como (UPS), la marca de estos equipos es POWERCOM. Además, estos equipos son los encargados de almacenar y controlar la energía de los equipos de red conectados en el Data Center al momento de presentarse fallas eléctricas, escases de energía, sobretensión o caídas de tensión en la universidad; evitando así la pérdida de los servicios que se estén ejecutando en ese preciso momento.

b) Cisco Switch.

En el Rack, se encuentran alojados tres switch de la marca Cisco, los cuales cumplen con funciones importantes dentro de la red de datos de la Universidad Nacional de Loja.

- En el primer Switch, se encuentran conectados los servidores internos de la Dirección de Telecomunicaciones.
- En el segundo equipo, se encuentran conectados los servidores públicos de la Universidad Nacional de Loja; estos son: servidor DNS, servidor para la Radio Universitaria y servidor Web de la UNL.
- El tercer equipo de red, se encuentra destinado al funcionamiento del Firewall que maneja la Universidad Nacional de Loja.

c) Cisco Router.

Uno de los equipos de mayor importancia que se encuentra alojado en el tercer Rack es el Router de interconexión con el servicio de internet. La marca de este equipo es Cisco y el uso del mismo, es por parte de la empresa TELCONET – CEDIA; proveedor de internet para la Universidad Nacional de Loja.

d) Cisco ATM Tag Sw Gigabit Router.

Otro de los equipos principales de la infraestructura de red de la Universidad Nacional de Loja, es el Switch Core, quien es el equipo encargado de proveer de internet a todo el campus universitario. Mediante la utilización de Switch de distribución (Multilayer Switch).

e) Cisco WLAN Controller.

Uno de los equipos de red, que se encuentra alojado en el tercer Rack, es el WLAN Controller; quien es el equipo encargado de controlar la interconexión de las redes inalámbricas de la institución.

4.4.3.4. Recursos Físicos de la Infraestructura de Red de Datos de la Universidad Nacional de Loja, a nivel de Servidores.

En el Data Center de la Universidad Nacional de Loja, se encuentran alojados tres Racks (armarios de equipos de red). De los cuales, el rack uno y dos se encuentran destinados para el alojamiento de los servidores.

En el primer Rack, se encuentran alojados algunos CPU's, que cumplen la función de servidores. Mientras, que en el segundo Rack, se encuentra alojado el Servidor BLADE (o con cuchillas); que actualmente tiene el 30% de su capacidad ocupada.

El Servidor BLADE, se encuentra distribuido físicamente de la siguiente manera:

- 24 Cuchillas de 450 Gb.
- 8 Cuchillas de 146 Gb.
- 4 Cuchillas de 306 Gb.

- **Sistema Operativo que utilizan los Servidores.**

Los servidores alojados en los rack del Data Center de la Universidad Nacional de Loja, trabajan con sistemas operativos libres, debido a su capacidad de seguridad, actualización, gestión y administración en tema de servidores.

Las distribuciones Linux que se utilizan en los servidores de la Universidad Nacional de Loja, son: Centos y Debian. Aunque en la actualidad la mayoría de servidores que se encuentran implementados en la Universidad Nacional de Loja, trabajan con el Sistema Operativo Linux Centos; debido a las características que posee. Estas características son:

- Centos es un sistema operativo de fácil mantenimiento.
- Es idóneo para el uso a largo plazo en entornos de producción.
- Diseñado para trabajar con servidores.
- Presenta seguridad y estabilidad.

Según versión del Subdirector de Redes y Equipos Informáticos de la Universidad Nacional de Loja, Ingeniero Jhon Calderón, una de las principales características por lo que se utiliza Centos en los Servidores de la Universidad Nacional de Loja, es debido a que permite que las actualizaciones se enfoquen únicamente en los paquetes obsoletos y no en la actualización de los demás módulos, permitiendo de esta manera rapidez y solvencia.

La Universidad Nacional de Loja, recientemente también adquirió la licencia del Sistema Operativo Windows Server 2012, el mismo que tiene un espacio en el Servidor BLADE, con las siguientes características:

- Sistema Operativo Windows Server 2012 Standard.
- Procesador Intel(R) Pentium (r) D CPU 3.4GHz.
- Memoria 2 GB.

Los Servidores que en la actualidad se encuentran alojados en el Servidor BLADE del Data Center de la Universidad Nacional de Loja son [65]:

a) Servidor Web.

La Universidad Nacional de Loja, posee un servidor web, el cual es el encargado de administrar los sistemas de gestión académica (SGA), matriculación, desempeño docente y pagina web de la universidad.
Las características principales del servidor son:

- Sistema Operativo Linux.
- Intel(R) Xeon (TM) CPU 3.2GHz.
- Memoria 1 Gb.
- Disco 160 Gb.

b) Servidor de Correo Institucional.

El Servidor de Correo Institucional de la Universidad Nacional de Loja, se encuentra administrado por Google; empresa que utiliza el servicio de correo electrónico Gmail.

El servicio de correo electrónico Gmail, permite contar con direcciones de correo electrónico bajo un dominio de la universidad (@unl.edu.ec), pero asociadas a Gmail.

Las características principales del servidor son:

- Sistema Operativo Linux.
- Intel(R) Xeon (TM) CPU 3.2GHz.
- Memoria 1 Gb.
- Disco 160 Gb.

c) Servidor Firewall.

El Servidor Firewall de la Universidad Nacional de Loja, es el encargado de bloquear el acceso no permitido que se genere entre la red pública (Internet) y la red privada de la universidad. Además, en el Servidor Firewall de encuentran las reglas para el uso del Internet en la Universidad Nacional de Loja.

Las características principales del servidor son:

- Sistema Operativo Linux.
- Intel(R) Xeon (TM) CPU 3.2GHz.
- Memoria 1 Gb.
- Disco 160 Gb.

d) Servidor DHCP.

La Universidad Nacional de Loja, cuenta con un servidor DHCP, el cual permite asignar dinámicamente direcciones de red a los equipos que se conecten dentro del campus universitario.

Las características principales del servidor son:

- Sistema Operativo Linux.
- Intel(R) Pentium (r) D CPU 3.4GHz.
- Memoria 1 Gb.
- Disco 160 Gb.

e) Servidor Radio Universitaria.

El Servidor de la Radio Universitaria, se encarga de transmitir la señal de "Radio Universitaria", a través de internet, transmitiendo en vivo todos los programas que se generan.

Las características principales del servidor son:

- Sistema Operativo Linux.
- Intel(R) Pentium (r) D CPU 3.4GHz.
- Memoria 1Gb.
- Disco 160Gb.

5. Materiales y Métodos

5.1. Métodos.

El presente Trabajo de Titulación se desarrolló utilizando distintos métodos, los cuales permitieron obtener la información necesaria y así cumplir con los objetivos planteados. Los métodos aplicados en el desarrollo del presente trabajo de titulación fueron los siguientes:

5.1.1. Método Científico.

Este método sirvió como guía principal de todo el trabajo de titulación, ya que permitió determinar la situación problemática, el planteamiento del problema, el objetivo general y los objetivos específicos. Además, permitió el análisis e interpretación de la información obtenida de las diversas fuentes bibliográficas.

5.1.2. Método Deductivo.

El método deductivo permitió determinar la causa principal del problema, desde lo general hasta lo específico, también permitió determinar los objetivos del proyecto de titulación.

5.1.3. Método Inductivo.

El método inductivo permitió, a partir desde la causa encontrada: ¿La falta de una VPN para la transmisión de datos en la Universidad Nacional de Loja, provoca la limitación de acceso a los servicios de la universidad?, y con la ayuda del análisis de herramientas, arquitecturas y protocolos sobre redes privadas virtuales, diseñar una red privada virtual que permitió acceder a las bases de datos científicas de la Universidad Nacional de Loja desde fuera del campus universitario.

5.1.4. Estudios Descriptivos.

Este método se lo usó en el desarrollo del primer objetivo, para recolectar información de los casos de éxito más recientes sobre el uso de herramientas Open Source para el diseño de redes privadas virtuales.

5.2. Técnicas.

Las técnicas usadas para el desarrollo del presente trabajo de titulación fueron las siguientes:

5.2.1. Observación.

Mediante la técnica de la observación, se constató la situación actual del acceso a las bases de datos científicas de la Universidad Nacional de Loja, identificando los problemas que se presentan al momento de acceder desde fuera del campus universitario.

5.2.2. Entrevista.

Se utilizó está técnica para la obtención de mayor información sobre la situación actual del acceso a las bases de datos científicas de la Universidad Nacional de Loja, realizando dicha entrevista al Ing. Miltón Palacios, Director de la Unidad de Telecomunicaciones e Información.

5.2.3. Análisis de Información.

Se utilizó está técnica para realizar el análisis de la información recolectada, necesaria para el cumplimiento de los objetivos planteados en el presente Trabajo de Titulación.

5.3. Metodología.

Para el presente trabajo de titulación realizado, no existe una metodología fija para su desarrollo, debido a esto el trabajo de titulación se desarrolló bajo las siguientes fases:

5.3.1. FASE 1: Analizar estados de arte y casos de éxito de herramientas Open Source para el diseño de la VPN.

Se detallan las actividades iniciales que se llevaron a cabo para el cumplimiento de esta fase.

- Actividad 1: Análisis de Casos de éxito relacionados con herramientas Open Source para el diseño de redes privadas virtuales a nivel internacional.
- Actividad 2: Análisis de Casos de éxito realizados con herramientas Open Source a nivel nacional sobre el diseño de redes privadas virtuales.
- Actividad 3: Análisis de las herramientas Open Source a utilizar para diseñar la red privada virtual.

5.3.2. FASE 2: Diseñar la VPN basada en una tecnología y protocolos de seguridad para permitir la transmisión de datos.

Se detallan las actividades que se llevaron a cabo para el cumplimiento de esta fase.

- Actividad 1: Análisis de los principales tipos de redes privadas virtuales.
- Actividad 2: Análisis de las principales arquitecturas que poseen las redes privadas virtuales.
- Actividad 3: Análisis de los principales protocolos de túnel que emplean las redes privadas virtuales.
- Actividad 4: Análisis de los principales sistemas operativos que se emplean para servidores.
- Actividad 5: Selección y determinación de la alternativa para la red privada virtual acorde al problema planteado.
- Actividad 6: Diseño de la red privada virtual para el acceso a las bases de datos científicas de la UNL.

5.3.3. FASE 3: Crear un escenario de una VPN para acceder a las bases de datos científicas de la Universidad Nacional de Loja.

Se detallan las actividades que se llevaron a cabo para el cumplimiento de esta fase.

- Actividad 1: Instalación del servidor OpenVPN para la integración de la red privada virtual con el campus universitario.
- Actividad 2: Configuración del Servidor de Acceso OpenVPN.
- Actividad 3: Configuración de los clientes en el Servidor OpenVPN.
- Actividad 4: Conexión de los clientes a la Red Privada Virtual.

5.3.4. FASE 4: Aplicar pruebas para evaluar el correcto funcionamiento del escenario de la VPN.

Se detallan las actividades que se llevaron a cabo para el cumplimiento de esta fase.

- Actividad 1: Pruebas de Conectividad.
- Actividad 2: Pruebas de Conexión.
- Actividad 3: Pruebas de Accesibilidad.
- Actividad 4: Pruebas de Implementación.
- Actividad 5: Pruebas del Rendimiento del Servidor.

6. Resultados

En esta sección se describen los resultados de cada uno de los objetivos planteados para el desarrollo del presente trabajo de titulación.

Problema: La falta de una Red Privada Virtual para la transmisión de datos en la Universidad Nacional de Loja, provoca la limitación de acceso a los servicios de la universidad.

A continuación se detallan de manera esquematizada las fases y actividades que engloban los objetivos del presente trabajo de titulación:

6.1. FASE I: Analizar estados de arte y casos de éxito de herramientas Open Source para el diseño de la VPN.

En esta fase se detallan las actividades iniciales que se llevaron a cabo para el cumplimiento de este objetivo.

6.1.1. Actividad 1: Análisis de Casos de éxito relacionados con herramientas Open Source para el diseño de redes privadas virtuales a nivel internacional.

Las redes privadas virtuales son el mecanismo ideal para conectarse a la red interna de las instituciones, empresas u organizaciones, y de esta manera lograr desde un punto externo acceder a los diferentes servicios internos que se ofrecen en las mismas.

Se han recopilado 3 casos de éxito orientados al uso de las redes privadas virtuales en el ámbito institucional, los mismos que demuestran el impacto de la aplicación de las redes privadas virtuales para acceder a los recursos internos (bases de datos científicas) de las universidades, desde una red externa a la institución.

Los casos de éxito recopilados son los siguientes:

- **Caso de éxito 1:** Servicio de Red Privada Virtual para la Universidad de Cádiz, España.
- **Caso de éxito 2:** Red Privada Virtual de la Universidad de Valencia, España.
- **Caso de éxito 3:** Acceso externo a los recursos electrónicos de la Universidad de Sevilla vía VPN.

Estos casos de éxito se encuentran detallados en el apartado Revisión de Literatura, CAPÍTULO I: REDES PRIVADAS VIRTUALES.

- **Análisis Final de los Casos Expuestos.**

Para una mejor comprensión de los casos de éxito analizados en esta actividad, se elaboró una tabla comparativa donde se especificó la solución, herramienta utilizada y los resultados obtenidos al emplear herramientas VPN Open Source como solución al problema de acceso a los recursos internos (bases de datos científicas) de una universidad, desde un punto externo a la red interna de la institución (ver TABLA V).

Este análisis se lo realizó para sustentar el tema objeto de estudio y para obtener un breve conocimiento sobre herramientas VPN Open Source que han sido aplicadas en universidades internacionales, y en base a los resultados determinar cuál es la herramienta VPN que se va a utilizar en el presente trabajo de titulación.

TABLA V: COMPARATIVA DE LOS CASOS DE ÉXITO INTERNACIONALES

Caso de Éxito	Problema a Solucionar	Solución Planteada	Resultados Obtenidos	Herramienta VPN
Servicio de Red Privada Virtual para la Universidad de Cádiz, España.	✓ No se contaba con un servicio que logre acceder a la red interna de la universidad desde fuera del campus universitario. ✓ Falta de acceso a los recursos electrónicos de la Universidad. ✓ No se podía acceder a las revistas, libros electrónicos, bases de datos en línea y documentos a texto completo desde fuera del campus universitario.	✓ La creación de una VPN, la cual permita a sus miembros debidamente autenticados, acceder a la red de la Universidad de Cádiz desde fuera de ella, mediante el establecimiento de un túnel de datos cifrado.	✓ Se logró que los miembros universitarios, accedan a la red de la Universidad de Cádiz desde fuera de ella. ✓ Acceso a las revistas, libros electrónicos, bases de datos en línea y documentos a texto completo desde fuera del campus universitario.	✓ Software OpenVPN, debido a su fácil implementación y gran versatilidad.
Red Privada Virtual de la Universidad de Valencia, España.	✓ Necesidad de un servicio que logre acceder a la red interna de la Universidad de Valencia desde fuera del campus universitario.	✓ Creación de una VPN, la cual permita a los miembros de la comunidad universitaria, acceder a la red de	✓ Acceder a la red interna de la Universidad de Valencia desde fuera del campus universitario.	✓ Software OpenVPN, debido a que es una solución abierta basada en software libre que provee un acceso seguro

	✓ Necesidad de acceder al catálogo bibliotecario, diccionarios, enciclopedias y películas electrónicas desde la casa u otro lugar externo a la universidad. ✓ No se podía acceder a las revistas, libros electrónicos, bases de datos en línea y documentos a texto completo desde fuera del campus universitario.	la Universidad de Valencia desde una red externa a la institución.	✓ Acceso al catálogo bibliotecario, diccionarios, enciclopedias y películas electrónicas desde un lugar externo a la universidad. ✓ Acceso a las revistas, libros electrónicos, bases de datos en línea y a documentos a texto completo desde fuera del campus universitario.	usando los estándares SSL/TLS para cifrar las comunicaciones.
Acceso externo a los recursos electrónicos de la Universidad de Sevilla vía VPN.	✓ La falta de un servicio que permita acceder a los recursos de la Intranet de la Universidad de Sevilla, los mismos que sólo estaban disponibles dentro de la universidad.	✓ Diseño de una red privada virtual, la cual permita a sus miembros, debidamente autenticados, acceder a la red de	✓ Lograr acceder a la red interna de la Universidad de Sevilla desde fuera del campus universitario. ✓ Acceso a las revistas, libros electrónicos,	✓ Software OpenVPN, debido a su seguridad y fácil implementación.

	✓ No se podía acceder a las revistas, libros electrónicos, bases de datos científicas y documentos que únicamente se encontraban disponibles en la red interna de la Universidad de Sevilla.	la Universidad de Sevilla desde un punto externo.	bases de datos y a documentos desde fuera del campus universitario de Sevilla.	

- **Conclusión.**

Después de que se realizó la comparación de los casos de éxito internacionales relacionados con el uso de herramientas Open Source para el diseño de redes privadas virtuales (ver TABLA V), se logró deducir que:

La herramienta Open Source que utilizaron las Universidades de Cádiz, Valencia y Sevilla para el diseño de redes privadas virtuales fue OpenVPN.

La herramienta OpenVPN permitió acceder a la red interna de las universidades y de esta manera ingresar a las bases de datos científicas de las mismas, desde un punto externo a la institución.

El diseño de una red privada virtual, es la solución más efectiva para acceder desde una red externa a los servicios de la red interna de las universidades, mediante el establecimiento de un túnel de datos cifrado.

6.1.2. Actividad 2: Análisis de Casos de éxito realizados con herramientas Open Source a nivel nacional sobre el diseño de redes privadas virtuales.

En esta actividad se han recopilado 2 casos de éxito orientados al uso de las redes privadas virtuales en las Universidades del Ecuador, los mismos que demuestran el impacto de la aplicación de las redes privadas virtuales para acceder a los recursos internos (bases de datos científicas) de las universidades, desde una red externa a la institución.

Los casos de éxito recopilados son los siguientes:

- **Caso de éxito 1:** Servicio de Red Privada Virtual (VPN) Institucional de la Universidad Católica de Cuenca (UCACUE).
- **Caso de éxito 2:** Sistema para Acceso Externo a Bases Digitales de la Universidad de Cuenca.

Estos casos de éxito se encuentran detallados en el apartado revisión de literatura, CAPÍTULO I: REDES PRIVADAS VIRTUALES.

- **Análisis Final de los Casos de Éxito Nacionales.**

Para una mejor comprensión de los casos de éxito nacionales analizados en esta actividad, se elaboró una tabla comparativa donde se especificó la solución, herramienta utilizada y los resultados obtenidos al emplear herramientas VPN Open Source como solución al problema de acceso a los recursos internos (bases de datos científicas) de una universidad, desde un punto externo a la red interna de la institución (ver TABLA VI).

Este análisis se lo realizó para obtener un breve conocimiento sobre herramientas VPN Open Source que han sido aplicadas en universidades de nuestro medio, y en base a los resultados determinar cuál es la herramienta VPN que se va a utilizar en el presente trabajo de titulación.

TABLA VI: COMPARATIVA DE LOS CASOS DE ÉXITO NACIONALES

Caso de Éxito	Problema a Solucionar	Solución Planteada	Resultados Obtenidos	Herramienta VPN
Servicio de Red Privada Virtual (VPN) Institucional de la Universidad Católica de Cuenca (UCACUE).	✓ Lograr acceder desde cualquier punto de Internet a los servicios de red de la universidad, como si estuviese conectado físicamente dentro de la infraestructura de red propia de la Universidad Católica de Cuenca. ✓ La falta de un acceso remoto a los recursos de la Biblioteca Digital de la universidad (libros-e, bases de datos, revistas electrónicas).	✓ La creación de un acceso remoto vía VPN a los recursos de la Biblioteca Digital (libros-e, bases de datos, revistas electrónicas) de la Universidad Católica de Cuenca.	✓ Se logró obtener acceso remoto vía VPN a los servicios de red de la universidad, como si se estuviese conectado físicamente dentro de la infraestructura de red propia de la Universidad Católica de Cuenca. ✓ Se logró el acceso a los recursos de la Biblioteca Digital.	✓ Software OpenVPN, debido a su forma de implementación .
Sistema para Acceso Externo a Bases Digitales de la Universidad de Cuenca.	✓ La falta de un acceso externo que permita acceder a los recursos internos de la Universidad de Cuenca.	✓ La creación de un sistema de acceso externo a las bases digitales de la Universidad de Cuenca.	✓ Acceso a los servicios de red de la universidad como si se estuviese conectado	✓ Software EZproxy, debido a su vinculación con

	✓ Necesidad de un servicio que logre acceder a las Bases Digitales: bases de datos científicas, artículos académicos, reseñas, ebooks, tesis, videos, imágenes y estadísticas.		físicamente dentro de la infraestructura de red propia de la Universidad. ✓ Acceso a las Bases Digitales que ofrecen material multidisciplinario a texto completo de las más importantes revistas y editoriales científicas.	bases de datos científicas.

- **Conclusión.**

Luego de que se realizó la comparación de los casos de éxito nacionales relacionados con el uso de herramientas Open Source para el diseño de redes privadas virtuales (ver TABLA VI), se logró deducir que:

La creación de una red privada virtual es la solución más utilizada para acceder desde una red externa a los servicios de la red interna (bases de datos científicas) de las universidades.

Las herramientas Open Source que utilizaron la Universidad Católica de Cuenca y la Universidad Estatal de Cuenca fueron OpenVPN y EZproxy respectivamente.

6.1.3. Actividad 3: Análisis de las herramientas Open Source a utilizar para diseñar la red privada virtual.

En base al análisis de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de servicios y recursos tecnológicos implementados actualmente, que se realizó en el apartado revisión de literatura, CAPÍTULO IV. Se evidencia la siguiente necesidad institucional respecto a los servicios en red que ofrece la universidad:

- Servicio de Acceso a Biblioteca Virtual.

La Biblioteca Virtual de la Universidad Nacional de Loja, ofrece los servicios de acceso al catálogo del Sistema Bibliotecario, Descubridores EDS, Red Universia, y Bases de Datos Científicas.

Para acceder a los servicios de Biblioteca Virtual de la Universidad Nacional de Loja, únicamente se lo puede realizar desde el campus universitario; ya que no existe un servicio que permita acceder a ellos desde fuera del campus de la universidad.

Debido a la necesidad de un servicio que permita ingresar a las bases de datos científicas de la institución desde un punto externo a la red interna de la universidad, a continuación se han recopilado 10 herramientas Open Source que se emplean para el acceso a los recursos internos de una institución desde una red externa, mediante el diseño de redes privadas virtuales.

Las herramientas analizadas son las siguientes:

- Herramienta LogMeIn Hamachi.
- Herramienta Itshidden VPN.
- Herramienta TorVPN.
- Herramienta The Securepoint TERRA.
- Herramienta Your – Freedom.
- Herramienta SoftEther VPN.
- Herramienta ExpressVPN.
- Herramienta OAST.

- Herramienta VPNBOOK.
- Herramienta OpenVPN Access Server.

Estas herramientas se encuentran detalladas en el apartado revisión de literatura, CAPÍTULO I: REDES PRIVADAS VIRTUALES.

- **Análisis Final de las Herramientas VPN Open Source.**

Para una mejor comprensión de las herramientas VPN Open Source analizadas en esta actividad, se elaboró una tabla comparativa donde se especificó las características, ventajas, desventajas, demanda y si la herramienta sirve para solventar las necesidades de la Universidad Nacional de Loja (ver TABLA VII).

Este análisis se lo realizó para determinar cuál es la herramienta VPN Open Source que se va a utilizar en el presente trabajo de titulación, sirviendo como base para la selección y determinación de la alternativa para el diseño de una red privada virtual en la Universidad Nacional de Loja, realizado en la Actividad 5 - Fase II de Resultados.

TABLA VII : HERRAMIENTAS OPEN SOURCE PARA EL DISEÑO DE REDES PRIVADAS VIRTUALES

Herramienta	Características	Ventajas	Desventajas	Demanda	Aplica
LogMeIn Hamachi	▪ Es una herramienta automática. ▪ Es un software multiplataforma: Windows, Mac OS, Linux, Android. ▪ Fácil uso y ofrece seguridad. ▪ Opciones avanzadas al crear y acceder a redes VPN. ▪ Acceso mediante cliente de escritorio o directamente desde el navegador. ▪ Gratuita para uso personal y de pago para uso profesional.	▪ Ofrece una alternativa segura sobre las VPN's tradicionales. ▪ Ofrece comunicaciones cifradas. ▪ Permite que el equipo acceda a los recursos de trabajo.	▪ No funciona a través de proxys no transparentes. ▪ Vulnerabilidad de la red, ya que cualquiera puede entrar en la misma. ▪ Versión profesional pagada.	▪ Alta	SI
Itshidden VPN	▪ Es una herramienta automática. ▪ Software multiplataforma: Windows, Mac OS, Linux, Android. ▪ Conexión segura para cifrar datos con 128 bits. ▪ Maneja protocolos PPTP Y OpenVPN.	▪ Es gratuita. ▪ Protege la privacidad. ▪ Evita detecciones Profundas. ▪ No se necesita instalar ningún software.	▪ Únicamente sirve para navegar en internet. ▪ No permite administrar usuarios. ▪ No funciona como servidor VPN.	▪ Baja	NO

	▪ La herramienta está en idioma Inglés. ▪ Es una versión online.	▪ No guarda historial alguno de la actividad realizada. ▪ Cuenta con servidores dedicados que son administrados por el propio equipo.			
TorVPN	▪ Es una herramienta automática. ▪ Funciona en Windows, Mac, Android, Linux, IPhone e iPad. ▪ Maneja accesos SSH, PPTP y OpenVPN. ▪ Está en el idioma Inglés. ▪ Es una versión online.	▪ Permite el anonimato a través del navegador. ▪ Es simple y segura. ▪ Sirve para saltarse filtros de contenido. ▪ Protege una comunicación VoIP.	▪ No funciona como servidor VPN. ▪ No gestiona usuarios. ▪ No gestiona certificados.	▪ Baja	NO
The Securepoint TERRA	▪ Es una herramienta manual. ▪ Se encuentra disponible en idioma Inglés. ▪ Es una puerta de enlace VPN. ▪ Permite el acceso remoto mediante IPSEC, OpenVPN, L2TP y PPTP. ▪ Cuenta con interfaz GUI.	▪ Tiene compatibilidad con otros sistemas VPN. ▪ Su configuración es rápida y segura. ▪ Cuenta con una interfaz gráfica de usuario fácil.	▪ Se necesita un equipo firewall para su configuración. ▪ Es una herramienta pagada.	▪ Baja	SI

Your Freedom	▪ Es una herramienta online y descargable. ▪ Funciona en plataforma Windows, Mac o Linux. ▪ Está en idioma Inglés. ▪ Soporta el protocolo OpenVPN.	▪ Permite acceder a cualquier servidor del mundo. ▪ Sus direcciones IP se renuevan automáticamente. ▪ Se maneja mediante proxy.	▪ No permite gestionar usuarios, ni contraseñas. ▪ No maneja cifrados.	▪ Media	NO
VPN SoftEther	▪ Está disponible en idiomas múltiples. ▪ Fácil de establecer, tanto como acceso remoto o de sitio a sitio. ▪ Maneja protocolos SSL-VPN, OpenVPN, IPSEC. ▪ Cuenta con cifrado AES de 256 bits. ▪ Multiplataforma: Windows, Linux, Mac, Android, iPhone e iPad. ▪ SoftEther VPN se basa en OpenVPN, adquiriendo sus funcionalidades.	▪ Es una herramienta altamente segura y confiable. ▪ Permite penetrar cualquier tipo de cortafuegos. ▪ Es libre y de código abierto.	▪ No dispone de demasiada documentación y soporte.	▪ Alta	SI

ExpressVPN	▪ Es una herramienta automática. ▪ Es una aplicación online. ▪ Está disponible en idioma multilenguaje. ▪ Cuenta con seguridad SSL. ▪ Maneja una encriptación de 256 bits. ▪ Es compatible con Windows, Mac, Linux, iOS y Android. ▪ Soporta los protocoles de túnel OpenVPN, L2TP, IPSEC y PPTP.	▪ Posee una fuerte encriptación. ▪ Maneja un ancho de banda ilimitado. ▪ No deja rastro en su actividad de navegación. ▪ Cuenta con soporte las 24 horas.	▪ Solo permite la conexión simultánea de un ordenador y un dispositivo de mano. ▪ No funciona como servidor VPN. ▪ Es gratis por tres meses y luego hay que adquirir licencia.	▪ Alta	NO
Herramienta OAST	▪ Está disponible en el idioma inglés. ▪ Funciona para los sistemas operativos Windows y Linux. ▪ Soporta los protocolos OpenVPN, L2TP, IPSEC, PPTP. ▪ Funciona como cliente para OpenVPN.	▪ Permite gestionar múltiples usuarios. ▪ Es libre. ▪ Es de código abierto. ▪ Es flexible, liviana y fácil de usar.	▪ Únicamente funciona como cliente VPN para realizar conexiones, y no como servidor.	▪ Baja	NO

VPNBOOK	▪ Es una herramienta diseñada con las últimas tecnologías y técnicas criptográficas. ▪ Realiza un enrutamiento del tráfico de internet para no obtener censura. ▪ Maneja protocolos PPTP y acceso a servicios de OpenVPN.	▪ Es una herramienta con tecnología de punta. ▪ Utiliza técnicas criptográficas avanzadas. ▪ Es segura. ▪ Es libre y totalmente gratis.	▪ Sirve únicamente como acceso seguro a Internet, más no como un servidor VPN para gestionar usuarios	▪ Alta	NO
OpenVPN-AS	▪ Permite conexiones sitio a sitio y de acceso remoto. ▪ Maneja 2 licencia gratis, si se desean más hay que adquirirlas. ▪ Maneja los protocolos SSL/TLS. ▪ Utiliza reglas firewall. ▪ Permite conexión de usuarios móviles (Road Warriors). ▪ Utiliza los protocolos 943 TCP y 1194 UDP como medio de transporte.	▪ Es rápida y flexible. ▪ Permite la conexión de múltiples usuarios a la vez. ▪ Maneja comunicaciones seguras y posee autenticación. ▪ Es la herramienta más utilizada para el diseño Redes Privadas Virtuales. ▪ Utiliza certificaciones de seguridad.	▪ Posee dos licencias gratis de prueba, si se desea más hay que adquirirlas a un precio de 10 dólares por cada licencia. ▪ No es compatible con IPSec.	▪ Alta	SI

	▪ Cuenta con un cifrado de 256 bits. ▪ Permite gestionar grupos de usuario. ▪ Cuenta con soporte nativo de cliente para los sistemas operativos GNU/Linux, Android, IOS, Windows y Mac OSX.	▪ Utiliza NAT y direcciones IP dinámicas. ▪ Ofrece una alternativa ligera y económica respecto a otras tecnologías. ▪ Permite gestionar grupos de usuarios.			

- **Conclusión.**

Luego de que se realizó la comparación de las herramientas Open Source relacionadas para el diseño de redes privadas virtuales (ver TABLA VII), se logró deducir que la herramienta LogMeIn Hamachi es un software multiplataforma, permite solucionar la necesidad de acceder a las bases de datos científicas de la Universidad Nacional de Loja, posee una alta demanda, pero debido a su vulnerabilidad en la red se descarta. La herramienta The Securepoint Terra es rápida, segura, sirve para solucionar la necesidad de acceso a las bases de datos científicas de la universidad, pero debido a que necesita un equipo firewall para su configuración y a su baja demanda se descarta. La herramienta VPN SoftEther es segura, es un software multiplataforma, permite realizar conexiones de acceso remoto, posee una alta demanda, sirve para solucionar la necesidad de la universidad, pero debido a su escasa documentación y soporte se descarta. Mientras que la herramienta OpenVPN-AS maneja los protocolos SSL/TLS, permite la conexión de usuarios móviles (Road Warriors), cuenta con un cifrado de 256 bits, posee una alta demanda y permite solventar la necesidad de acceder a las bases de datos científicas de la institución; debido a estas razones se seleccionó la herramienta OpenVPN-AS para el diseño de la red privada virtual de la Universidad Nacional de Loja.

6.2. FASE II: Diseñar la VPN basada en una tecnología y protocolos de seguridad para permitir la transmisión de datos.

En esta fase se realizó el diseño de la red privada virtual para la Universidad Nacional de Loja. Para el diseño de la VPN primeramente se realizó el análisis de los principales tipos, arquitecturas y protocolos de túnel que emplean las redes privadas virtuales. Además, se analizó el sistema operativo donde va a funcionar la VPN y se realizó la selección de la alternativa para el diseño de la red privada virtual de la Universidad Nacional de Loja.

A continuación se detallan cada una de las actividades que se llevaron a cabo para el cumplimiento de este objetivo.

6.2.1. Actividad 1: Análisis de los principales tipos de redes privadas virtuales.

En esta actividad se han detallado los principales tipos de VPN que se emplean para el diseño de las redes privadas virtuales, acorde a sus características y funcionalidades.

Los principales tipos de redes privadas virtuales son los siguientes:

- VPN basada en hardware.
- VPN basada en firewall.
- VPN basada en software.

Estos tipos de redes privadas virtuales se encuentran detallados en el apartado revisión de literatura, CAPÍTULO II: ARQUITECTURAS, TIPOS Y PROTOCOLOS DE TÚNEL DE LAS REDES PRIVADAS VIRTUALES.

- **Análisis Final de los Principales Tipos de Redes Privadas Virtuales.**

Para una mejor comprensión de los principales tipos de redes privadas virtuales analizados en esta actividad, se elaboró una tabla comparativa donde se especificó las características que poseen. Lo cual permitió obtener un mejor entendimiento de las diferencias que existen entre cada uno de ellos (ver TABLA VIII).

Este análisis se lo realizó para determinar cuál es el tipo de red privada virtual que se va a utilizar en el presente trabajo de titulación, sirviendo como base para la selección y determinación de la alternativa para el diseño de una red privada virtual en la Universidad Nacional de Loja, realizado en la Actividad 5 - Fase II de Resultados.

TABLA VIII: DIFERENCIA DE LOS PRINCIPALES TIPOS DE REDES PRIVADAS VIRTUALES

Tipo de Red Privada Virtual	Características
▪ VPN basada en hardware.	✓ Utilizan básicamente equipos dedicados (routers). ✓ Son seguras y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red. ✓ Son redes privadas virtuales de alto costo económico. ✓ Requieren de una configuración correcta y definida.
▪ VPN basada en firewall.	✓ Aprovecha los mecanismos de seguridad del servidor, incluyendo la restricción del acceso a la red interna. ✓ El rendimiento en este tipo de VPN decrece, ya que no se tiene hardware especializado de encriptación. ✓ Utilizan equipos firewall dedicados. ✓ Tienen un alto costo económico.
▪ VPN basada en software.	✓ Permiten que el tráfico de túnel sea dependiendo de la dirección o protocolo, a diferencia de los productos basados en hardware. ✓ Son Independientes. ✓ Ofrecen mayor flexibilidad en cómo se gestiona el tráfico de red. ✓ No se necesita equipos especializados. ✓ Tienen un bajo costo económico.

- **Conclusión.**

Luego de que se realizó la comparación de los principales tipos de redes privadas virtuales (ver TABLA VIII), se seleccionó la VPN basada en software. Se realizó la elección de este tipo de red privada virtual debido a que no se necesita hardware especializado para su implementación y a su bajo costo económico.

Además, en base al análisis de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de servicios y recursos tecnológicos implementados actualmente, que se realizó en el apartado revisión de literatura, CAPÍTULO IV. Se evidencia que no existe ningún equipo de red especializado para redes privadas virtuales, por lo que la selección de la VPN basada en software es la adecuada.

6.2.2. Actividad 2: Análisis de las principales arquitecturas que poseen las redes privadas virtuales.

En esta actividad se han detallado las principales arquitecturas VPN que se emplean para el diseño de las redes privadas virtuales, acorde a sus características y necesidades.

Las principales arquitecturas de redes privadas virtuales son las siguientes:

- Red Privada Virtual de Acceso Remoto.
- Red Privada Virtual Sitio a Sitio.
- Red Privada Virtual Interna.

Estas arquitecturas de redes privadas virtuales se encuentran detalladas en el apartado revisión de literatura, CAPÍTULO II: ARQUITECTURAS, TIPOS Y PROTOCOLOS DE TÚNEL DE LAS REDES PRIVADAS VIRTUALES.

- **Análisis Final de las Principales Arquitecturas de Redes Privadas Virtuales.**

Para una mejor comprensión de las principales arquitecturas de las redes privadas virtuales analizadas en esta actividad, se elaboró una tabla comparativa donde se especificó las características que poseen. Lo cual permitió obtener un mejor entendimiento de las diferencias que existen entre cada una de ellas (ver TABLA IX).

Este análisis se lo realizó para determinar cuál es la arquitectura de red privada virtual que se va a utilizar en el presente trabajo de titulación, sirviendo como base para la selección y determinación de la alternativa para el diseño de una red privada virtual en la Universidad Nacional de Loja, realizado en la Actividad 5 - Fase II de Resultados.

TABLA IX: DIFERENCIA DE LAS PRINCIPALES ARQUITECTURAS DE REDES PRIVADAS VIRTUALES

Arquitectura de Red Privada Virtual	Características
Red Privada Virtual de Acceso Remoto.	✓ Usuarios se conectan a una institución desde sitios remotos utilizando Internet como vínculo de acceso. ✓ Al conectarse tienen un nivel de acceso similar a estar dentro de la red local. ✓ Se necesita un cliente vpn para la conexión.
Red Privada Virtual Sitio a Sitio.	✓ Poseen una conexión permanente y segura entre dos redes locales diferentes, utilizando Internet como vínculo de acceso. ✓ Esta arquitectura se utiliza para conectar oficinas remotas con la sede central de la organización. ✓ Pueden ser intranet o extranet.
Red Privada Virtual Interna.	✓ Funciona como una red VPN normal, salvo que dentro de la misma red local LAN en lugar de a través de Internet. ✓ Sirve para aislar zonas y servicios de la misma red interna.

- **Conclusión.**

Luego de que se realizó la comparación de las principales arquitecturas de redes privadas virtuales (ver TABLA IX), se seleccionó la arquitectura de Red Privada Virtual de Acceso Remoto. Se realizó la elección de este tipo de arquitectura de red privada virtual debido a que los usuarios se conectarán a la red interna de la Universidad Nacional de Loja desde varios sitios remotos, utilizando Internet como vínculo de acceso.

Además, en base al análisis de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de servicios y recursos tecnológicos implementados actualmente, que se realizó en el apartado revisión de literatura, CAPÍTULO IV. Se evidencia mediante el diagrama de red interna de la Universidad Nacional de Loja (ver Figura 30) que la selección de la Arquitectura de Red Privada

Virtual de Acceso Remoto es la correcta debido a la infraestructura de red que posee la universidad.

6.2.3. Actividad 3: Análisis de los principales protocolos de túnel que emplean las redes privadas virtuales.

En esta actividad se han detallado los principales protocolos de túnel VPN que se emplean para el diseño de las redes privadas virtuales, acorde a sus características y funcionalidades.

Los principales protocolos de túnel que poseen las redes privadas virtuales son los siguientes:

- Protocolo PPTP.
- Protocolo L2TP/IPSec.
- Protocolo OpenVPN SSL/TLS.

Estos protocolos de túnel se encuentran detallados en el apartado revisión de literatura, CAPÍTULO II: ARQUITECTURAS, TIPOS Y PROTOCOLOS DE TÚNEL DE LAS REDES PRIVADAS VIRTUALES.

- **Análisis Final de los Principales Protocolos de Túnel que emplean las Redes Privadas Virtuales.**

Para una mejor comprensión de los principales protocolos de túnel de redes privadas virtuales analizados en esta actividad, se elaboró una tabla comparativa donde se especificó las características que poseen. Lo cual permitió obtener un mejor entendimiento de las diferencias y ventajas que existen entre cada uno de ellos (ver TABLA X).

Este análisis se lo realizó para determinar cuál es el protocolo de túnel de la red privada virtual que se va a utilizar en el presente trabajo de titulación, sirviendo como base para la selección y determinación de la alternativa para el diseño de una red privada virtual en la Universidad Nacional de Loja, realizado en la Actividad 5 - Fase II de Resultados.

TABLA X: TABLA COMPARATIVA DE LOS PRINCIPALES PROTOCOLOS DE TÚNEL DE LAS REDES PRIVADAS VIRTUALES

Características	Protocolo PPTP	Protocolo L2TP/IPSec	Protocolo OpenVPN SSL/TLS
Fuerza de Cifrado.	✓ 128 bits con protocolo MPPE.	✓ 256 bits con cifrado AES.	✓ 256 bits con cifrado AES.
Nivel de Seguridad.	✓ Normal.	✓ Bueno.	✓ Muy Bueno.
Plataformas Soportadas.	✓ Windows, Linux, Mac, Android, iPhone/iPad.	✓ Windows, Linux, Mac, Android, iPhone/iPad.	✓ Windows, Linux, Mac, Android, iPhone/iPad.
Software adicional requerido.	✓ No.	✓ No.	✓ Si.
Rendimiento.	✓ Muy Bueno.	✓ Muy Bueno.	✓ Excelente.
Compatible con IP dedicada.	✓ Si.	✓ Si.	✓ Si.
Puerto VPN aleatorio.	✓ No.	✓ No.	✓ Si 443/TCP.
Peligro de filtración.	✓ Si.	✓ Si.	✓ No.
Seguridad VPN.	✓ Encriptación básica.	✓ La máxima encriptación. Comprueba la integridad de los datos y encapsula los datos dos veces.	✓ La máxima encriptación. Autentifica los datos con certificados digitales.
Velocidad de VPN.	✓ Rápido debido a la encriptación más baja.	✓ Necesita más proceso de la CPU para encapsular los datos dos veces.	✓ Protocolo con mejor rendimiento. Velocidades elevadas, incluso en

	✓ Su velocidad no es acorde a la seguridad que brinda.		conexiones con alta latencia y a grandes distancias.
Estabilidad.	✓ Funciona bien en la mayoría de puntos de acceso Wi-Fi, muy estable.	✓ Compatible con dispositivos NAT.	✓ La más fiable y estable, incluso tras routers inalámbricos, en redes no fiables, y en puntos de acceso Wi-Fi.
Compatibilidad.	✓ Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.	✓ Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.	✓ Compatible con la mayoría de los sistemas operativos de ordenadores de sobremesa y dispositivos Android móviles y tablets.

- **Conclusión.**

Luego de que se realizó la comparación de los principales protocolos de túnel que emplean las redes privadas virtuales (ver TABLA X), se seleccionó el protocolo de túnel OpenVPN SSL/TLS. Se realizó la elección de este protocolo de túnel debido a que cuenta con una fuerza de cifrado de 256 bits con cifrado AES, su nivel de seguridad es muy bueno, su rendimiento es excelente y cuenta con la máxima encriptación mediante la autenticación con certificados digitales.

Además, en base a la selección de la herramienta OpenVPN-AS que se realizó en el análisis para determinar cuál es la herramienta VPN Open Source a utilizarse para el diseño de la red privada virtual en la Universidad Nacional de Loja (ver Actividad 3 – Fase I de Resultados), se logró deducir que la herramienta OpenVPN-AS tiene incorporado en su funcionamiento al protocolo de túnel OpenVPN SSL/TLS, debido a esto la elección del protocolo de túnel OpenVPN SSL/TLS es el correcto.

6.2.4. Actividad 4: Análisis de los principales sistemas operativos que se emplean para servidores.

En esta actividad se han detallado los principales sistemas operativos que se emplean en la instalación de servidores, acorde a sus características y funcionalidades.

Los principales sistemas operativos dedicados para la instalación de servidores son los siguientes:

- Sistema Operativo Centos.
- Sistema Operativo Debian.
- Sistema Operativo Red Hat Enterprise.
- Sistema Operativo Ubuntu Server.
- Sistema Operativo Windows Server 2012 R2.

Estos sistemas operativos se encuentran detallados en el apartado revisión de literatura, CAPÍTULO III: SISTEMAS OPERATIVOS PARA SERVIDORES.

- **Análisis Final de los Principales Sistemas Operativos que se emplean para Servidores.**

Para una mejor comprensión de los principales sistemas operativos analizados en esta actividad, se elaboró una tabla comparativa donde se especificó las características que poseen. Lo cual permitió obtener un mejor entendimiento de las diferencias y ventajas que existen entre cada uno de ellos (ver TABLA XI).

Este análisis se lo realizó para determinar cuál es el sistema operativo que se va a utilizar en el presente trabajo de titulación, sirviendo como base para la selección y determinación de la alternativa para el diseño de una red privada virtual en la Universidad Nacional de Loja, realizado en la Actividad 5 - Fase II de Resultados.

TABLA XI: TABLA COMPARATIVA DE LOS PRINCIPALES SISTEMAS OPERATIVOS EMPLEADOS PARA SERVIDORES

Sistema Operativo	Licencia	Uso	Ciclo Vida	Soporte	Basado	Formato
Centos.	Gratuita.	▪ Servidores. ▪ Estaciones de Trabajo. ▪ Producción.	10 años.	Si de forma gratuita.	Red Hat.	Rpm.
Debian.	Gratuita.	▪ Servidores. ▪ Producción.	1 año.	Si de forma gratuita.	-	Deb.
Ubuntu Server.	Gratuita.	▪ Servidores. ▪ Producción.	5 años.	Si de forma gratuita.	Debian.	Deb.
Red Hat.	Pagada.	▪ Servidores. ▪ Estaciones de Trabajo. ▪ Producción.	10 años.	Si pero de forma pagada.	-	Rpm.
Windows Server 2012 R2.	Pagada.	▪ Servidores. ▪ Producción.	4 años.	Si pero de forma pagada.	Windows Server 2008.	ReFS

- **Conclusión.**

Luego de que se realizó la comparación de los principales sistemas operativos que se emplean en la instalación de servidores (ver TABLA XI), se seleccionó el Sistema Operativo Centos. Se realizó la elección de este sistema operativo debido a que posee una estabilidad de 10 años sin necesidad de más actualizaciones, está dedicado para servidores en producción, es gratuito y está basado en Red Hat el sistema operativo número uno dedicado para servidores.

Además, en base al análisis de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de servicios y recursos tecnológicos implementados actualmente, que se realizó en el apartado revisión de literatura,

CAPÍTULO IV. Se logró deducir que la Universidad Nacional de Loja emplea al Sistema Operativo Centos en sus servidores, debido a esto la elección del Sistema Operativo Centos es el adecuado.

6.2.5. Actividad 5: Selección y determinación de la alternativa para la red privada virtual acorde al problema planteado.

En base al problema planteado que enmarca al presente Trabajo de Titulación "La falta de una Red Privada Virtual para la transmisión de datos en la Universidad Nacional de Loja provoca la limitación de acceso a los servicios de la universidad" y al análisis de la situación actual de la infraestructura de red de la Universidad Nacional de Loja, a nivel de servicios y recursos tecnológicos implementados actualmente, que se realizó en el apartado revisión de literatura, CAPÍTULO IV. Se evidencia la siguiente necesidad institucional respecto a los servicios en red que ofrece la universidad:

- Servicio de Acceso a Biblioteca Virtual.

La Biblioteca Virtual de la Universidad Nacional de Loja, ofrece los servicios de acceso al catálogo del Sistema Bibliotecario, Descubridores EDS, Red Universia, y Bases de Datos Científicas. Para acceder a los servicios de Biblioteca Virtual de la Universidad Nacional de Loja, únicamente se lo puede realizar desde el campus universitario; ya que no existe un servicio que permita acceder a ellos desde fuera del campus de la universidad. Debido a ello se presenta la necesidad de contar con un acceso que permita acceder a los servicios que ofrece la Biblioteca Virtual de la Universidad Nacional de Loja desde un punto externo a la red de la universidad.

En base a la necesidad mencionada anteriormente, en esta actividad se seleccionó la alternativa que permitió el diseño de una red privada virtual para el acceso a los servicios de Biblioteca Virtual de la institución desde un punto externo a la red interna de la universidad.

A continuación se detalla la alternativa que se seleccionó para el diseño de la Red Privada Virtual en la Universidad Nacional de Loja.

- **Herramienta VPN.**

En base al análisis que se realizó en la Actividad 3 – Fase I de Resultados sobre las diferentes herramientas VPN Open Source relacionadas para el diseño de redes privadas virtuales, la herramienta VPN que se escogió para el diseño de la red privada virtual en la Universidad Nacional de Loja es OpenVPN-AS.

- **Tipo de Red Privada Virtual a utilizar.**

En base al análisis que se realizó en la Actividad 1 – Fase II de Resultados sobre los principales tipos de redes privadas virtuales, el tipo de VPN que se escogió para el diseño de la red privada virtual en la Universidad Nacional de Loja es una VPN basada en software.

- **Arquitectura de Red Privada Virtual a utilizar.**

En base al análisis que se realizó en la Actividad 2 – Fase II de Resultados sobre las principales arquitecturas que emplean las redes privadas virtuales, la arquitectura que se escogió para el diseño de la red privada virtual en la Universidad Nacional de Loja es una VPN de Acceso Remoto.

- **Protocolo de Túnel a utilizar.**

En base al análisis que se realizó en la Actividad 3 – Fase II de Resultados sobre los principales protocolos de túnel que emplean las redes privadas virtuales, el protocolo de túnel que se escogió para el diseño de la red privada virtual en la Universidad Nacional de Loja es OpenVPN SSL/TLS.

- **Sistema Operativo a utilizar.**

En base al análisis que se realizó en la Actividad 4 – Fase II de Resultados sobre los principales sistemas operativos que se emplean en la instalación de servidores, el sistema operativo que se escogió para el diseño de la red privada virtual en la Universidad Nacional de Loja es Centos.

6.2.6. Actividad 6: Diseño de la red privada virtual para el acceso a las bases de datos científicas de la UNL.

En base a la selección y determinación de la alternativa para la red privada virtual que se realizó en la Actividad 5 – Fase II de Resultados, se elaboró el diseño de la VPN que permitió la conexión de usuarios remotos a las bases de datos científicas de la UNL desde una red externa a la institución (ver Figura 31).

A continuación se detallan los componentes básicos que se utilizaron para el diseño de la red privada virtual dentro de la Universidad Nacional de Loja (ver TABLA XII).

TABLA XII: COMPONENTES DE LA RED PRIVADA VIRTUAL

Herramienta VPN	Tipo VPN	Arquitectura VPN	Protocolo Túnel	Sistema Operativo
▪ Software OpenVPN.	▪ VPN basada en Software.	▪ VPN de Acceso Remoto.	▪ OpenVPN SSL/TLS.	▪ Centos.

- **Determinar los perfiles de usuarios para la autenticación en la VPN.**

Los perfiles de usuarios para la autenticación en la VPN se los estableció acorde a los usuarios de la red de datos de la Universidad. La Universidad Nacional de Loja cuenta con diferentes áreas tanto académicas como administrativas. En cada una de estas áreas existe un número significativo de usuarios de la red de datos. Los principales tipos de usuarios que hacen uso de la red de datos de la institución son los siguientes:

- **Docentes:** Son los profesionales encargados de impartir conocimientos a los estudiantes y de generar investigación.
- **Administrativos:** Son aquellas personas que trabajan en la institución, pero sin el cargo de docencia.
- **Estudiantes:** Especifica a cada una de las personas que se hallan adquiriendo conocimiento dentro de la Institución.

Los principales procesos que son llevados a cabo por cada uno de los usuarios de la red de datos de la institución son los siguientes:

a) Docentes.

- Generación de conocimientos para impartir a los estudiantes de la institución
- Generación de investigaciones a través de la elaboración de proyectos investigativos.
- Acceso al Sistema de Gestión Académica (SGA) de la Universidad Nacional de Loja.
- Consultas a las bases de datos científicas que ofrece la Universidad Nacional de Loja.

b) Estudiantes.

- Investigación personal, accediendo a las bases de datos científicas que ofrece la Universidad Nacional de Loja.
- Acceso al SGA, para consultas respecto a calificaciones y asistencias en el transcurso del periodo académico.

c) Administrativos.

Los procesos que ejecutan los administrativos depende del cargo que ocupe cada funcionario, entre los principales tenemos los siguientes:

- Admisión y Matriculación de estudiantes.
- Mantenimiento y acceso a las bases de datos científicas, repositorio de datos institucional y acceso al catálogo de biblioteca.
- Expedición de títulos y certificaciones.
- Autorizaciones, acreditaciones e inscripciones.
- Ayudas, becas y convenios.
- Procedimientos en Tesorería.
- Selección, Contratación de Personal y Provisión de puestos.

Dentro del grupo de administrativos se encuentra el personal del departamento de la Unidad de Telecomunicaciones e Información, los mismos que son los encargados de diseñar y dar mantenimiento a los servicios de software, hardware y red de datos de la Universidad Nacional de Loja.

En base a los usuarios de la red de datos de la Universidad y a las indicaciones recibidas por parte de la Unidad de Telecomunicaciones e Información, se estableció los perfiles de usuarios para la autenticación en la red privada virtual de la Universidad Nacional de Loja, los mismos que son:

- **uTI:** El perfil uTI le corresponde al Director de la Unidad de Telecomunicaciones e Información.
- **Administrador**: El perfil de usuario le corresponde a la persona que va a manejar el servicio de VPN.
- **Docentes:** Son todos los docentes pertenecientes a la Universidad Nacional de Loja.
- **Estudiantes:** Son todos los estudiantes que pertenecen a la Universidad Nacional de Loja.
- **Administrativos:** Es todo el personal administrativo de la Universidad, excepto el personal de la Unidad de Telecomunicaciones e Información.
- **srei.uti:** Es el personal de mantenimiento y redes de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.
- **sdsw.uti:** Es el personal de software de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

En la TABLA XIII, se muestran los perfiles de usuarios que se estableció para la autenticación en la red privada virtual de la Universidad Nacional de Loja.

TABLA XIII: PERFILES DE USUARIOS PARA LA AUTENTICACIÓN

Perfiles de Usuarios
uTI
administrador
docentes
estudiantes
administrativos
srei.uti
sdsw.uti

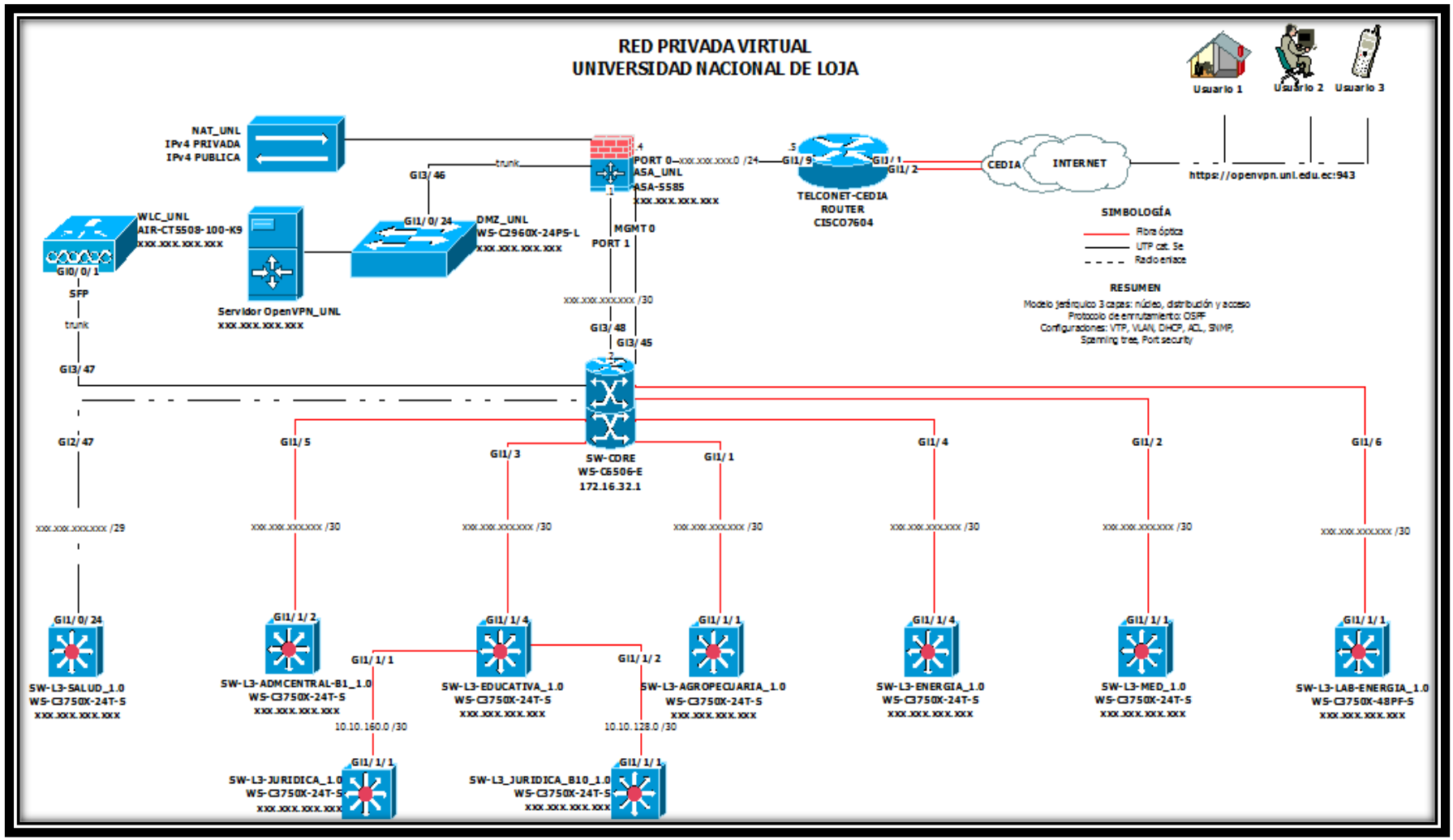


Figura 31: Diseño Red Privada Virtual de la Universidad Nacional de Loja.

Fuente: Autor.

6.3. FASE III. Crear un escenario de una VPN para acceder a las bases de datos científicas de la Universidad Nacional de Loja.

En base al diseño de la red privada virtual para el acceso a las bases de datos científicas de la Universidad Nacional de Loja que se realizó en la Actividad 6 – Fase II de Resultados, se realizó la instalación y configuración del servidor OpenVPN para la integración de la red privada virtual con el campus universitario. Además, en esta fase se realizó la configuración de los usuarios de la VPN acorde a los perfiles de usuarios establecidos y se realizó la conexión de los usuarios a la red privada virtual de la Universidad Nacional de Loja.

A continuación se detallan cada una de las actividades que se llevaron a cabo para el cumplimiento de este objetivo.

6.3.1. Actividad 1: Instalación del servidor OpenVPN para la integración de la red privada virtual con el campus universitario.

En esta actividad se realizó la instalación del servidor de acceso OpenVPN para la integración de la red privada virtual con el campus de la Universidad Nacional de Loja.

6.3.1.1. Instalación del Sistema Operativo GNU/Linux Centos 7.

Antes de instalar OpenVPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja, se instaló el sistema operativo GNU/Linux Centos 7 (ver Figura 32), con las siguientes características:

- Procesador: arquitectura x86_64 GNU/Linux.
- Disco Duro: 20 GB.
- Memoria RAM: 1 GB.
- CPU: 1 QEMU VIRTUAL CPU.

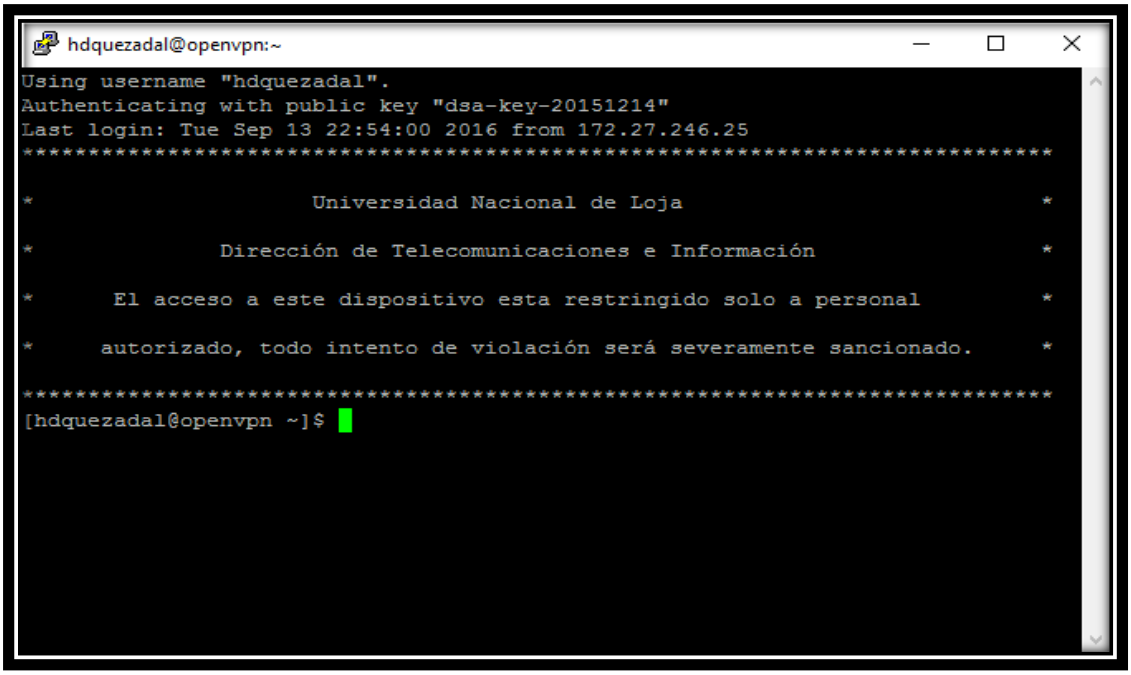


Figura 32: Vista del Sistema Operativo Centos 7 instalado.

Fuente: Autor.

Una vez instalado el Sistema Operativo Centos 7, se comprobó que el servidor cuenta con una dirección IP perteneciente a la red interna de la institución (ver Figura 33). Esto se lo realizó mediante el comando:

- **Ifconfig**

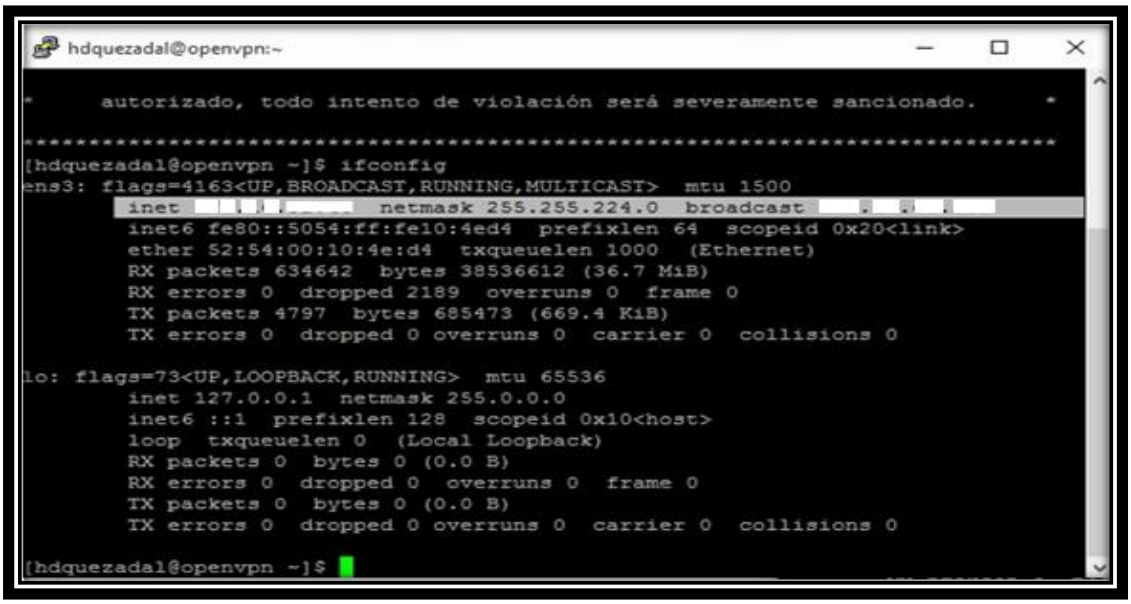


Figura 33: Comprobación de la asignación de una dirección IP interna.

Fuente: Autor.

Luego de comprobar que el servidor tiene asignada una dirección IP de la red interna de la Universidad Nacional de Loja, se comprobó que los repositorios de Centos se encuentren actualizados. Esto se lo realizó mediante el comando:

- **sudo yum update**

6.3.1.2. Instalación del Servidor de Acceso OpenVPN.

Una vez que se comprobó que los repositorios de Centos se encuentran actualizados, se instaló el Servidor de Acceso OpenVPN. Para ello se accedió como super usuario "root" y se instaló el software OpenVPN (ver Figura 34). Esto se lo realizó mediante el comando:

- **sudo rpm –Uvh http://swupdate.openvpn.org/as/openvpn-as-2.0.21-CentOS7.x86_64.rpm**

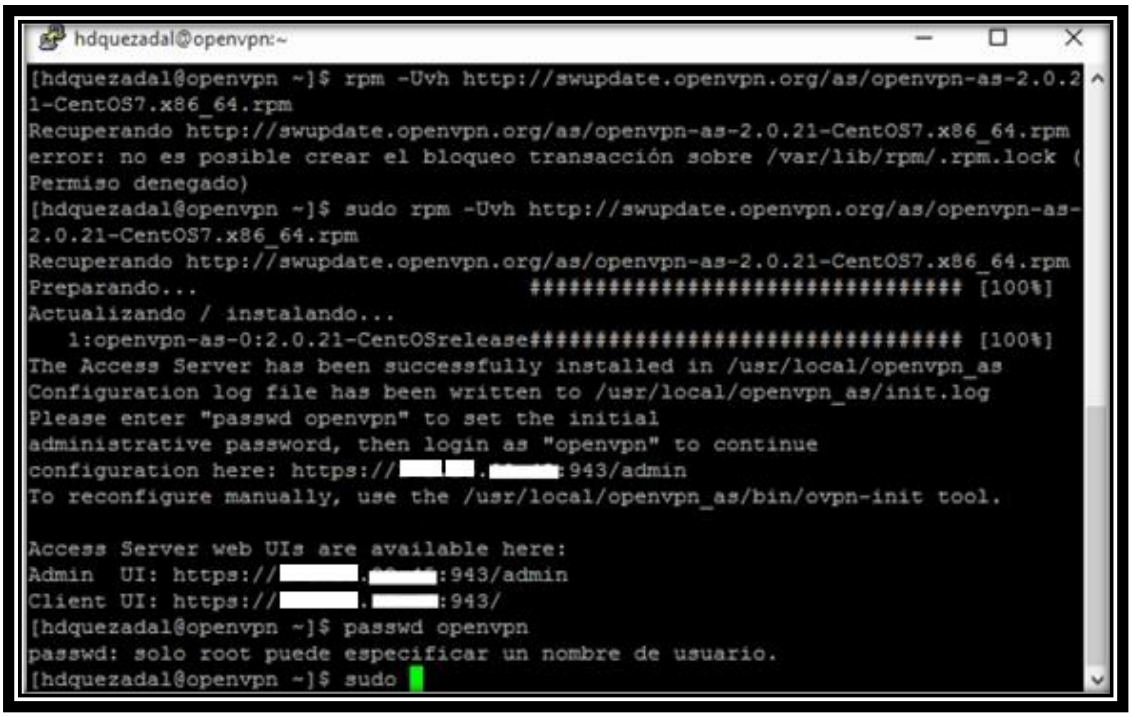


Figura 34: Instalación del Servidor de Acceso OpenVPN.

Fuente: Autor.

Una vez instalado el Servidor de Acceso OpenVPN, se estableció la contraseña del usuario administrador (ver Figura 35). Para la asignación de la contraseña del usuario administrador se utilizó el comando:

- **sudo passwd openvpn**

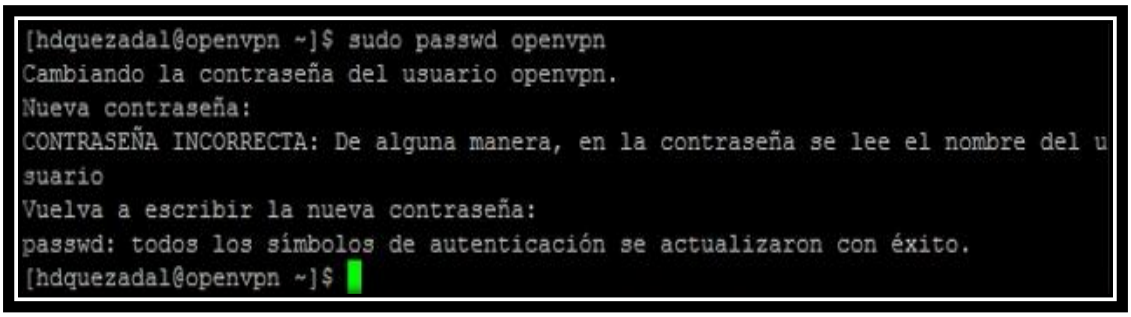


Figura 35: Asignación de contraseña al usuario administrador.

Fuente: Autor.

6.3.2. Actividad 2: Configuración del Servidor de Acceso OpenVPN.

En esta actividad se realizó la configuración del Servidor de Acceso OpenVPN para la Universidad Nacional de Loja.

6.3.2.1. Inicialización del Servidor de Acceso OpenVPN mediante la Interfaz de Usuario de Administración Web.

Después de que se realizó la instalación del Servidor de Acceso OpenVPN y se estableció la contraseña para el usuario administrador, se inicializó el Servidor de Acceso OpenVPN. Para ello, en primer lugar se abrió un navegador web (se puede abrir desde cualquier equipo de la red LAN donde se encuentra el servidor OpenVPN) y se colocó la siguiente dirección URL: **https://openvpn.unl.edu.ec:943/admin**

El navegador informó que la conexión no es segura, aun así se continuó. Esto se debe a que el certificado fue generado por el propio servidor en el momento de la instalación. Se hizo clic en "Opciones Avanzadas" y se presentó el detalle del mensaje de aviso (ver Figura 36).

Figura 36: Mensaje de Conexión no Segura.

Fuente: Autor.

Una vez que se realizó clic en "Opciones avanzadas", se mostró el detalle del mensaje y se marcó la opción "Acceder a openvpn.unl.edu.ec (sitio no seguro)" (ver Figura 37).

Figura 37: Añadir excepción de seguridad del sitio web.

Fuente: Autor.

Después de hacer clic en “Acceder a openvpn.unl.edu.ec (sitio no seguro)”, se presentó la pantalla de inicio de sesión de OpenVPN (ver Figura 38). Se inició sesión utilizando el usuario “uti” y la contraseña que se la estableció anteriormente durante la instalación del Servidor de Acceso OpenVPN.

Figura 38: Pantalla de inicio de sesión OpenVPN.

Fuente: Autor.

La primera vez que se accedió a la Interfaz de Usuario de Administración Web de OpenVPN, se presentó un formulario de aceptación de la licencia. Se lo leyó y se realizó clic en "Agree" para continuar (ver Figura 39).

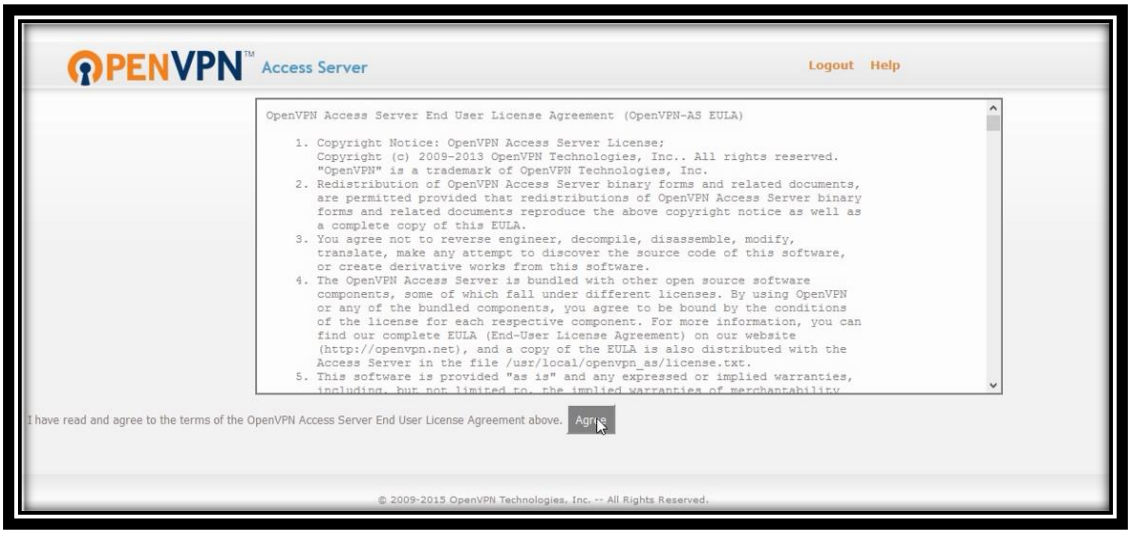


Figura 39: Aceptación de la Licencia OpenVPN.

Fuente: Autor.

Después de que se aceptó la licencia, se muestra la página principal de la Interfaz de Usuario de Administración Web de OpenVPN (ver Figura 40).

La página de la Interfaz de Usuario de Administración de OpenVPN contiene el estado del servidor “Status Overview”, con un vínculo para iniciar o detener el servidor VPN. Además, contiene dos barras laterales que cuentan con enlaces de configuración para el Servidor de Acceso OpenVPN.

Figura 40: Página Principal de la Interfaz de Usuario de Administración Web de OpenVPN. Fuente: Autor.

La barra lateral derecha (ver Figura 41) muestra el estado del servidor VPN (encendido o apagado), con un vínculo para iniciar o detener el servidor VPN, dependiendo de su condición. Además, contiene el número de usuarios de VPN simultáneos permitidos por la licencia instalada, con un vínculo a la página de licencias para información de usuarios conectados, con un enlace a la página de descripción de estado (que contiene una tabla con una lista de todos los usuarios conectados actualmente).

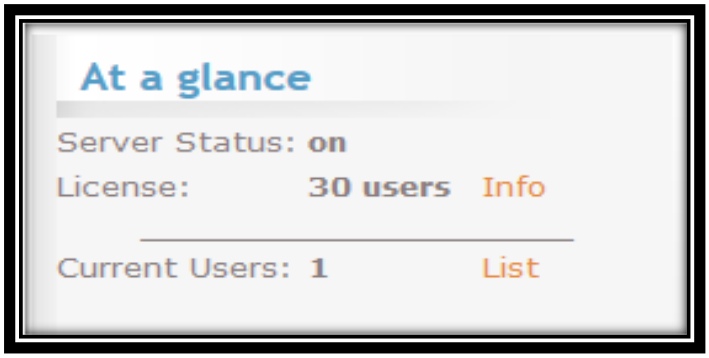


Figura 41: Barra lateral Derecha de Administración.

Fuente: Autor.

La barra lateral izquierda (ver Figura 42) contiene los enlaces de configuración del servidor OpenVPN (texto naranja), cada uno de ellos agrupados con los enlaces de sección de la página de interfaz de usuario de administración web (texto azul).

Figura 42: Barra lateral Izquierda de Administración.

Fuente: Autor.

6.3.2.2. Configuración del Servidor de Acceso OpenVPN mediante la Interfaz de Usuario de Administración Web.

Luego de que se realizó la inicialización del Servidor de Acceso OpenVPN, se inició con la configuración del servidor OpenVPN.

a) Server Network Settings (Configuración de Red del Servidor).

Dentro de la sección "Configuration" de la página de interfaz de usuario de administración web, se encuentra la página "Server Network Settings", la cual está compuesta por diferentes subsecciones para las configuraciones en red del servidor VPN, el Administrador de interfaz de usuario Web, y el servidor Web de clientes (ver Figura 43).

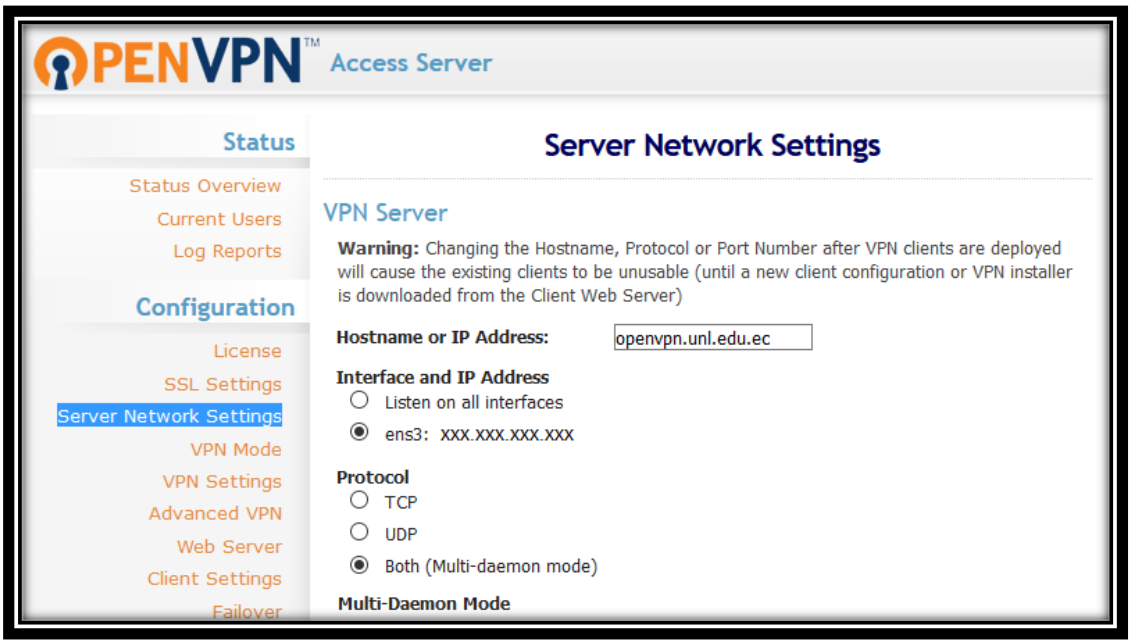


Figura 43: Configuración de Red del Servidor.

Fuente: Autor.

- **VPN Server (Servidor VPN).**

Una vez que se accedió a la sección "Server Network Settings", se encuentra la subsección "VPN Server", en la cual se realizó varias configuraciones de red para el servidor OpenVPN (ver Figura 44).

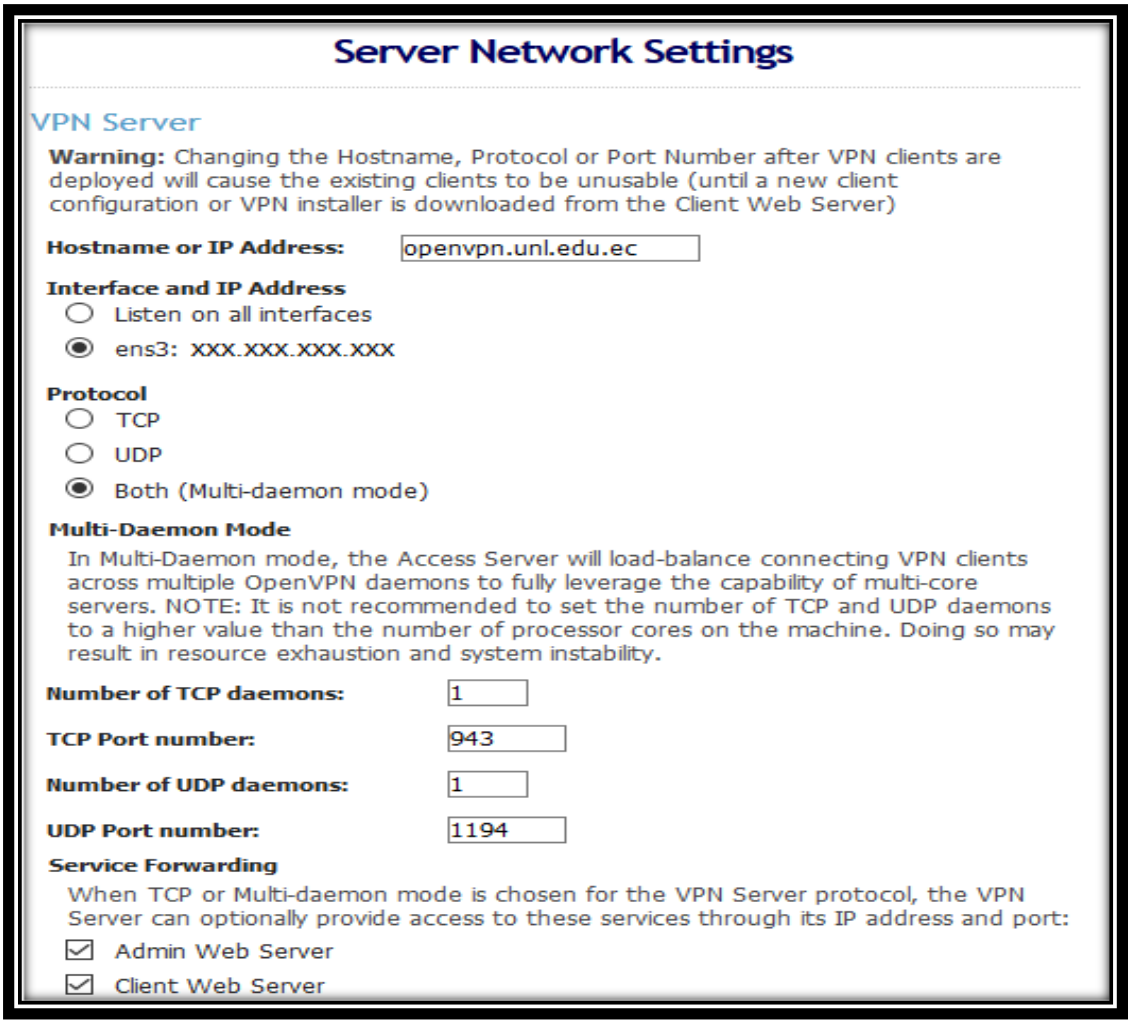


Figura 44: Configuración de la Subsección VPN Server.

Fuente: Autor.

En esta subsección se establecieron los siguientes valores:

Hostname or IP Address: en este campo se colocó el **hostname: openvpn.unl.edu.ec**, mediante el cual se logró acceder a la VPN desde fuera de la red interna de la institución.

Además, se marcó la casilla por donde se va a escuchar las peticiones hacia el servidor, en este caso se marcó la opción: "ens3 xxx.xxx.xxx.xxx", la cual contiene la dirección IP del servidor dentro de la red interna de la Universidad Nacional de Loja.

Posteriormente se seleccionó el protocolo por donde se va a realizar la comunicación del cliente y servidor. Se seleccionó "Multi Daemon-Mode", para tener la opción de comunicarse tanto por el protocolo TCP o UDP.

Finalmente se asignó los puertos por donde se va a establecer la comunicación con la red privada virtual, estos son: TCP 943 y UDP 1194.

- **Admin Web UI (Interfaz de usuario Web de administración).**

En esta subsección se especificó la dirección IP y número de puerto para la comunicación con el servidor Web de administración de OpenVPN (ver Figura 45).

Figura 45: Configuración de la Subsección Admin Web UI.

Fuente: Autor.

- **Client Web Server (Servidor Web Cliente).**

En esta subsección se seleccionó la forma en que los clientes se van a comunicar con el Servidor de Acceso OpenVPN para iniciar sesión en el servidor Web de clientes y obtener la configuración VPN generada automáticamente (ver Figura 46). Se seleccionó la opción para utilizar la misma dirección y puerto que posee el servidor Web de administración.

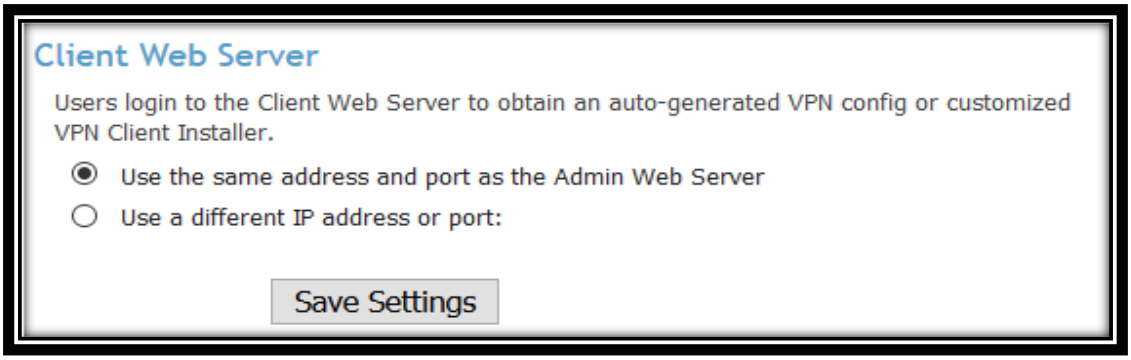


Figura 46: Configuración de la Subsección Client Web Server.

Fuente: Autor.

Una vez que se terminó con las configuraciones en la página “Server Network Settings”, se hizo clic en “Save Settings” para guardar las configuraciones establecidas.

b) VPN Mode (Modo VPN).

Luego de que se realizó las configuraciones en la página “Server Network Settings”, se ingresó a la página de configuración “VPN Mode” en la sección “Configuration”.

Dentro de esta página de configuración se encuentra la subsección “VPN Topology”, en la cual se configuró la topología de túneles VPN para el Servidor de Acceso OpenVPN (ver Figura 47). Se seleccionó la Capa 3 (Routing / NAT) del modelo OSI para el túnel VPN.

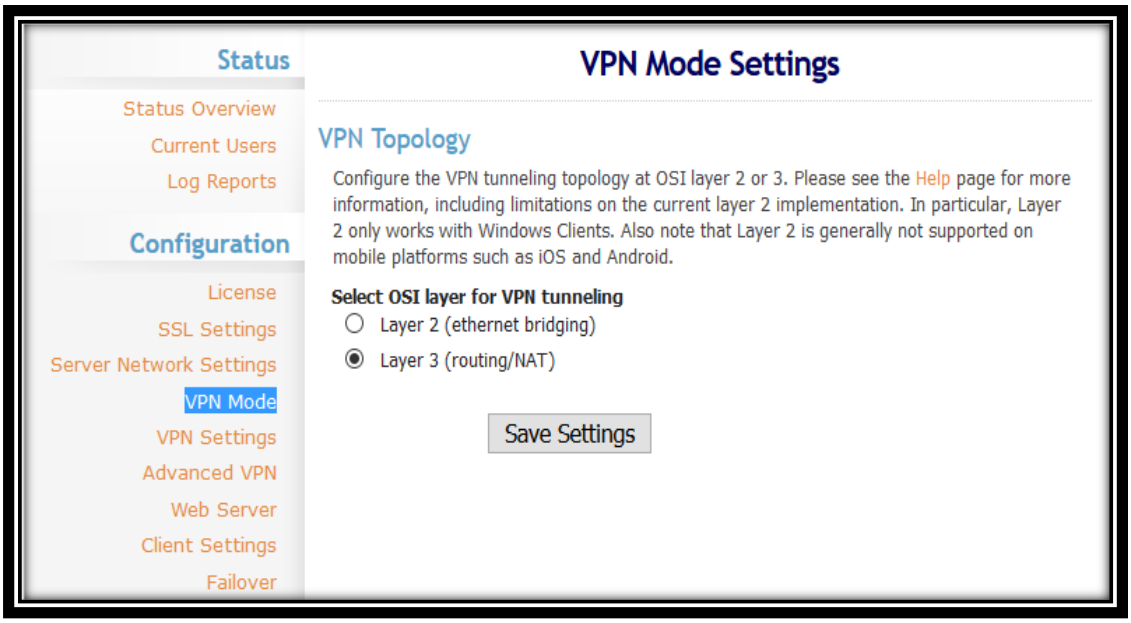


Figura 47: Configuración de la Topología de la VPN.

Fuente: Autor.

Una vez que se terminó con las configuraciones en la página “VPN Mode”, se hizo clic en “Save Settings” para guardar las configuraciones realizadas.

c) VPN Settings (Configuración de la VPN).

Después de que se realizó las configuraciones en la página “VPN Mode”, se ingresó a la página de configuración “VPN Settings” en la sección “Configuration” (ver Figura 48).

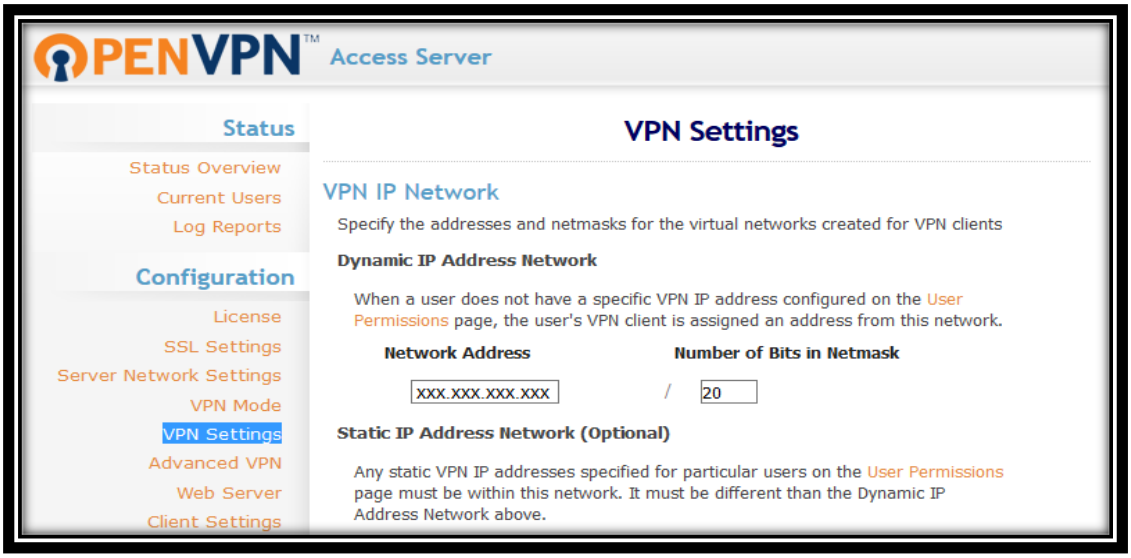


Figura 48: Configuración de la Página VPN Settings.

Fuente: Autor.

- **VPN IP Network (Red IP de la VPN).**

Una vez que se accedió a la página de configuración "VPN Settings", se encuentra la subsección "VPN IP Network", en la cual se realizó algunas configuraciones de red para el Servidor de Acceso OpenVPN (ver Figura 49).

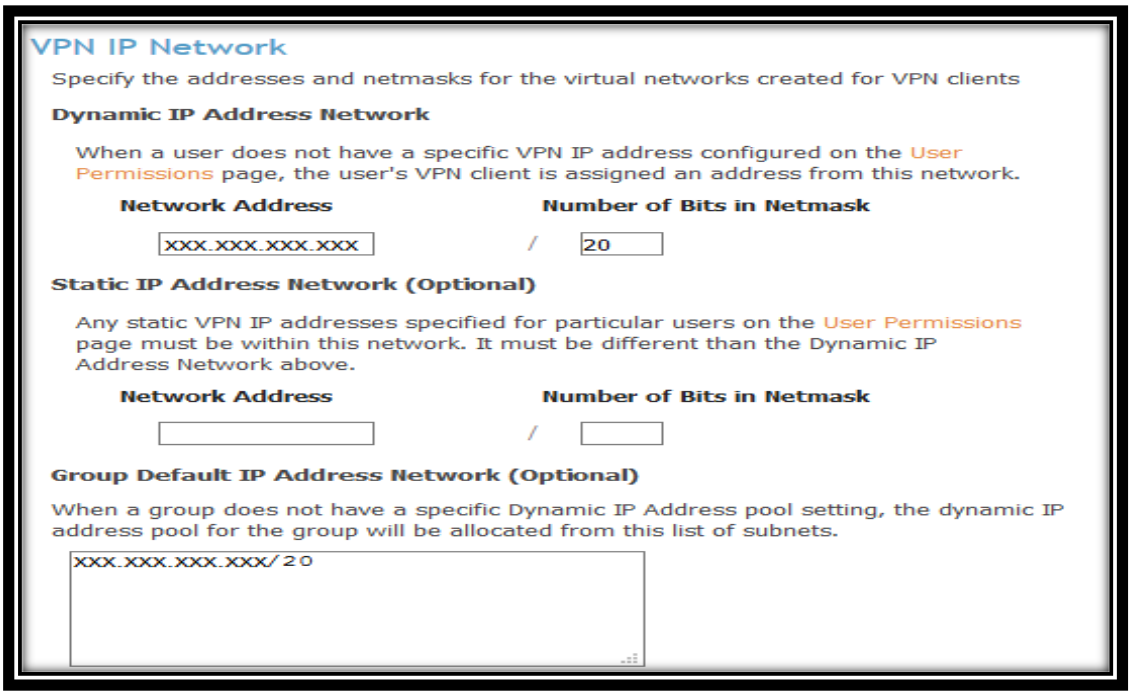


Figura 49: Configuración de la Subsección VPN IP Network.

Fuente: Autor.

En esta subsección se especificó las direcciones y máscaras de red, para la asignación de las redes virtuales creadas para los clientes VPN. En esta subsección se establecieron las siguientes configuraciones:

Se seleccionó el uso de direcciones de red IP Dinámicas, en donde se especificó una dirección IP y una máscara de red para la asignación de direcciones para los clientes VPN que se conecten a la red privada virtual. Además, se estableció un grupo predeterminado de direcciones de red IP mediante la asignación de una subred (ver Figura 49).

- **Routing (Enrutamiento).**

En esta subsección se estableció las subredes privadas a las que los clientes VPN podrán acceder desde el Servidor de Acceso OpenVPN. Esto se lo realizó a través de la especificación de subredes privadas (ver Figura 50).

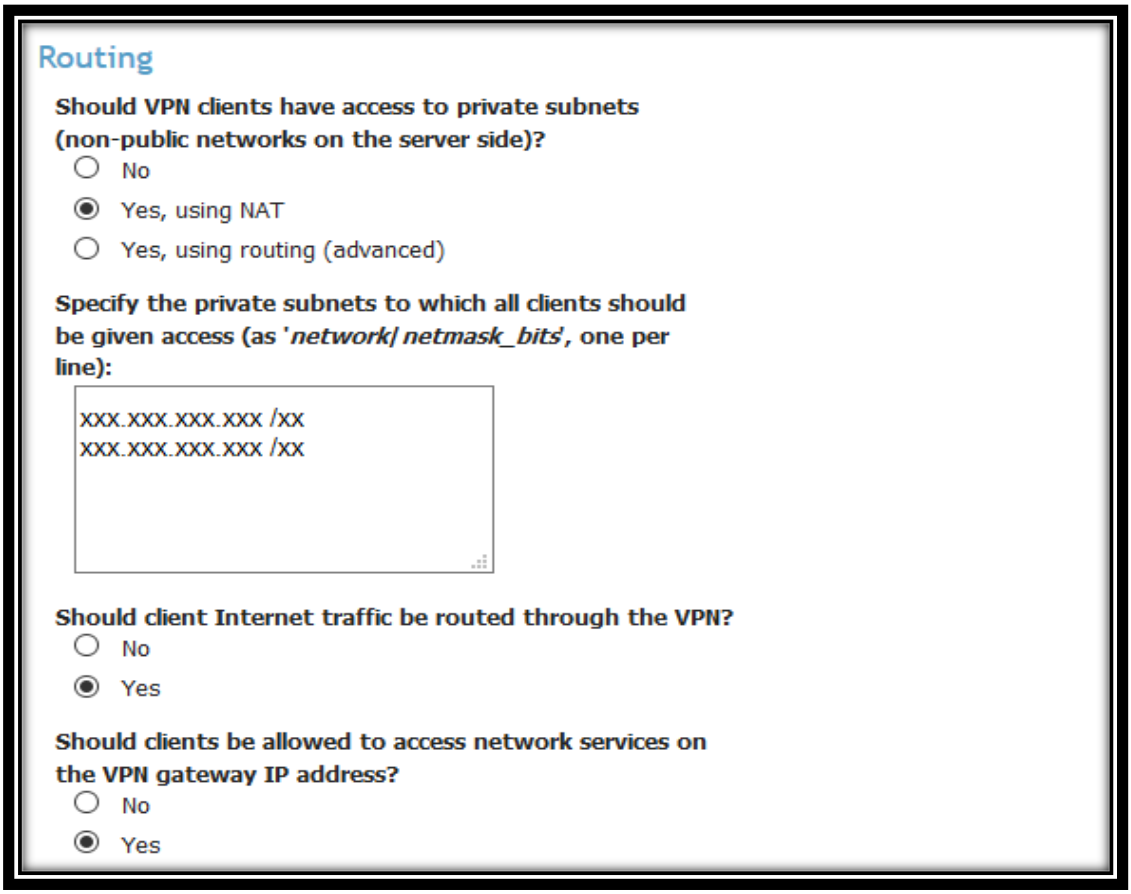


Figura 50: Configuración de la Subsección Routing.

Fuente: Autor.

En esta subsección se realizaron las siguientes configuraciones:

Se seleccionó la opción “Yes, using NAT” para permitir que los clientes VPN tengan acceso a las subredes privadas de la institución, a través de la traducción de direcciones de red (NAT).

Se especificó las subredes privadas a las que todos los clientes de la red privada virtual podrán acceder. En este caso las subredes privadas únicamente serán para las bases de datos científicas: xxx.xxx.xxx/xx – xxx.xxx.xxx/xx.

Se estableció que el tráfico de red del cliente sea dirigido a través de la VPN y se pueda obtener comunicación con la red interna de la Universidad. Y finalmente se seleccionó la opción “Yes” para permitir que los clientes tengan acceso a los servicios de la red interna.

Se utilizó NAT para permitir el acceso de los clientes de la VPN a las subredes privadas, debido a que el enrutamiento es más complicado de configurar, ya que se requiere cambios de enrutamiento en la infraestructura de red.

- **DNS Settings (Ajustes DNS).**

En esta subsección se especificó los servidores DNS para que el tráfico de Internet de los clientes se encamine a través de la VPN. Se seleccionó la opción “Have clients use these DNS servers” para que los clientes utilicen los servidores DNS de la institución (ver Figura 51).

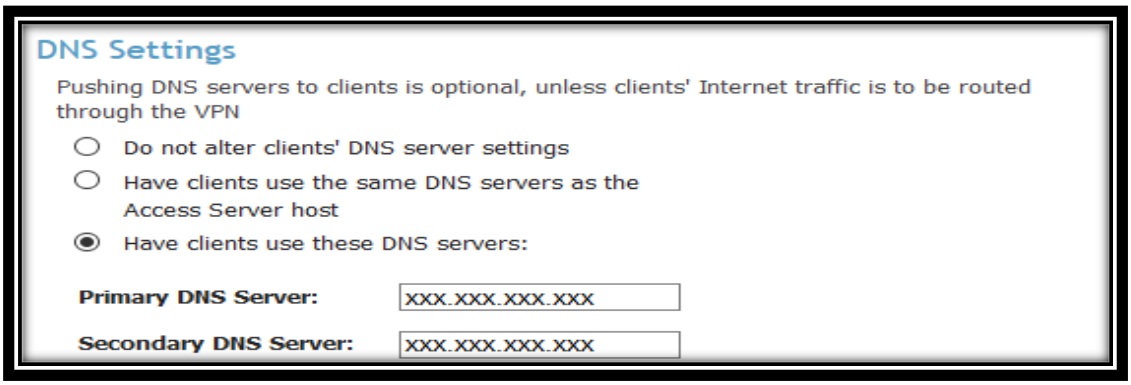


Figura 51: Configuración de la Subsección DNS Settings.

Fuente: Autor.

Una vez que se terminó con las configuraciones en la página “DNS Settings”, se realizó clic en “Save Settings” para guardar las configuraciones realizadas.

d) Advanced VPN (VPN Avanzada).

Después de que se realizó las configuraciones en la página “VPN Settings”, se ingresó a la página de configuración “Advanced VPN” en la sección “Configuration” (ver Figura 52).

Figura 52: Configuración de la Página Advanced VPN.

Fuente: Autor.

- **Inter-Client Communication (Comunicación entre Clientes).**

Una vez que se ingresó a la página de configuración “Advanced VPN”, se encuentra la subsección “Inter-Client Communication”, en la cual se realizó algunas configuraciones para el Servidor de Acceso OpenVPN (ver Figura 53).

Figura 53: Configuración de la Subsección Inter-Client Communication.

Fuente: Autor.

En esta subsección se seleccionó la opción "No (unless explicitly allowed by User Permissions)", la misma que permitió establecer que los clientes de la VPN no puedan comunicarse entre sí dentro de la Red Privada Virtual.

- **Multiple Sessions per User (Múltiples Sesiones por Usuario).**

En esta subsección se seleccionó la opción "Allow multiple concurrent VPN connections", la cual permitió que se realicen múltiples conexiones simultáneas para cada usuario (ver Figura 54).

Figura 54: Configuración de la Subsección Multiple Sessions per User.

Fuente: Autor.

- **Connection Security Refresh (Actualizar Seguridad de Conexión).**

En esta subsección se estableció el intervalo de tiempo para la actualización de la conexión de los clientes dentro de la Red Privada Virtual. Esto se lo realizó para preservar la seguridad de la conexión del cliente VPN, cada sesión TLS se renegocia en el intervalo de tiempo especificado (ver Figura 55).

Figura 55: Configuración de la Subsección Connection Security Refresh.

Fuente: Autor.

- **Default Compression Settings (Ajustes de Compresión por Defecto).**

En esta subsección se estableció el soporte de compresión para las conexiones de los clientes VPN (ver Figura 56). Se seleccionó la opción "Support compression on client VPN connections", la cual permitió los ajustes de compresión por defecto para cada una de las conexiones de los clientes VPN.

Figura 56: Configuración de la Subsección Default Compression Settings.

Fuente: Autor.

- **Private Routed Subnets (Enrutamiento de Subredes Privadas).**

En esta subsección se establecen las listas de subredes privadas que deben ser accesibles a través del método de enrutamiento en lugar de NAT (ver Figura 57).

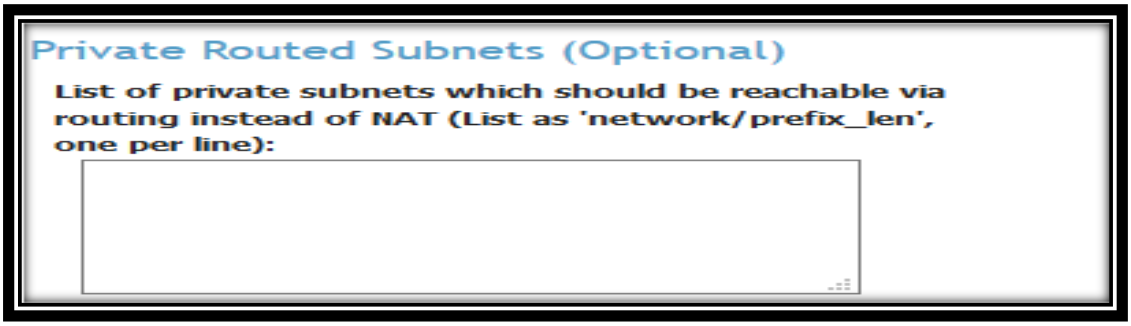


Figura 57: Configuración de la Subsección Private Routed Subnets.

Fuente: Autor.

- **Windows Networking (Red de Windows).**

En esta subsección se seleccionó la opción “Don’t alter Windows Networking Settings on clients” para no alterar la configuración de red de los clientes VPN que se conecten a través del Sistema Operativo Windows (ver Figura 58).

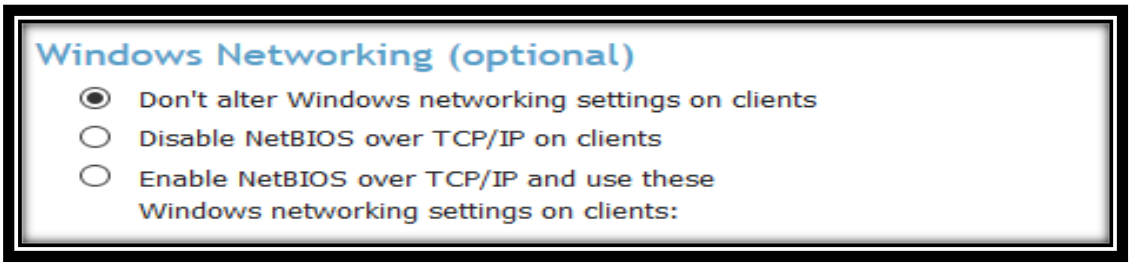


Figura 58: Configuración de la Subsección Windows Networking.

Fuente: Autor.

- **Additional OpenVPN Config Directives (Directivas de Configuración Adicionales de OpenVPN).**

En esta subsección se especifican las directivas de configuración adicionales que se añaden al cliente VPN y a los archivos de configuración del Servidor de Acceso OpenVPN (ver Figura 59).

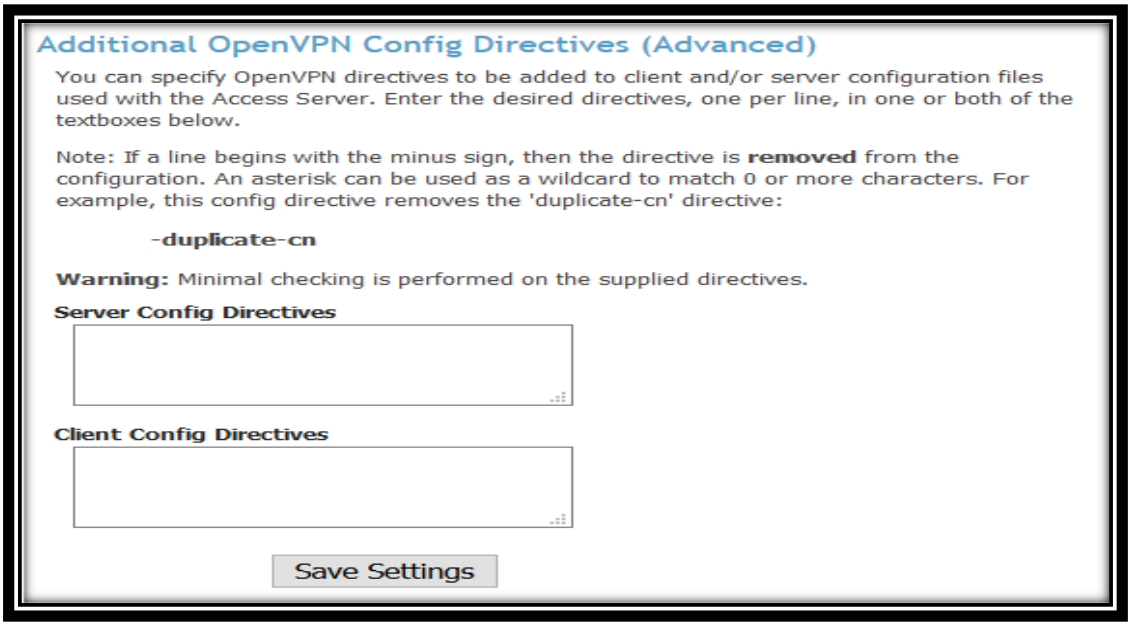


Figura 59: Configuración de la Subsección Additional OpenVPN Config Directives.

Fuente: Autor.

Una vez que se terminó con las configuraciones en la página “Advanced VPN”, se realizó clic en “Save Settings” para guardar las configuraciones realizadas.

e) Web Server (Configuración del Servidor Web).

Después de que se realizó las configuraciones en la página “Advanced VPN”, se ingresó a la página de configuración “Web Server” en la sección “Configuration” (ver Figura 60).

Figura 60: Configuración de la Página Web Server.

Fuente: Autor.

- **Web Server Certificates (Certificados de Servidor Web).**

Una vez que se ingresó a la página de configuración “Web Server”, se encuentra la subsección “Web Server Certificates” (ver Figura 61).

En esta subsección se cargan los certificados del servidor web y las claves de validación de los mismos. Los certificados y claves deben estar en formato PEM (Formato de archivo empleado para almacenar certificados digitales).

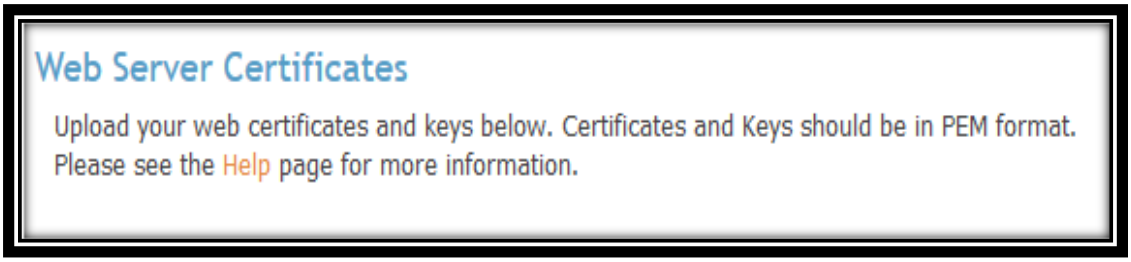


Figura 61: Configuración de la Subsección Web Server Certificates.

Fuente: Autor.

- **Validation Results (Resultados de validación).**

En esta subsección se encuentran los certificados digitales asignados al Servidor de Acceso OpenVPN, al igual que las claves de validación para cada uno de ellos (ver Figura 62).

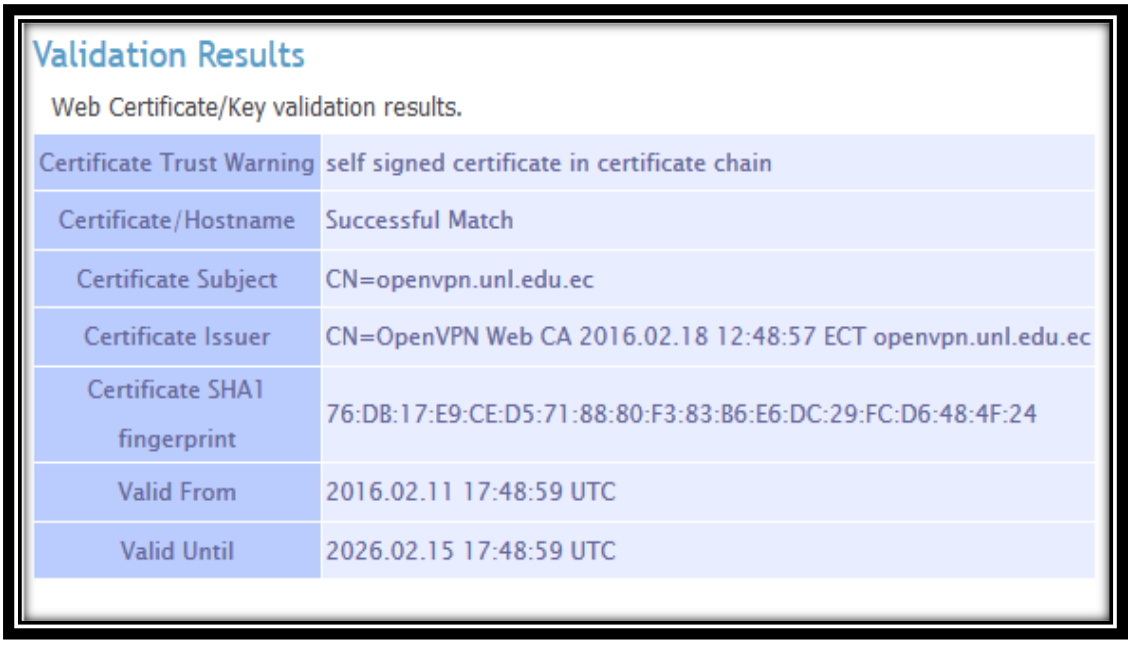


Figura 62: Configuración de la Subsección Validation Results.

Fuente: Autor.

- **CA Bundle (Paquete de Autoridad de Certificación).**

En esta subsección se proporciona una lista concatenada de certificados de CA (Autoridad de Certificación), que valida al certificado del Servidor Web (ver Figura 63).

Figura 63: Configuración de la Subsección CA Bundle.

Fuente: Autor.

- **Certificate (Certificado).**

Esta subsección se emplea para seleccionar y cargar los archivos del certificado Web del Servidor de Acceso OpenVPN (ver Figura 64).

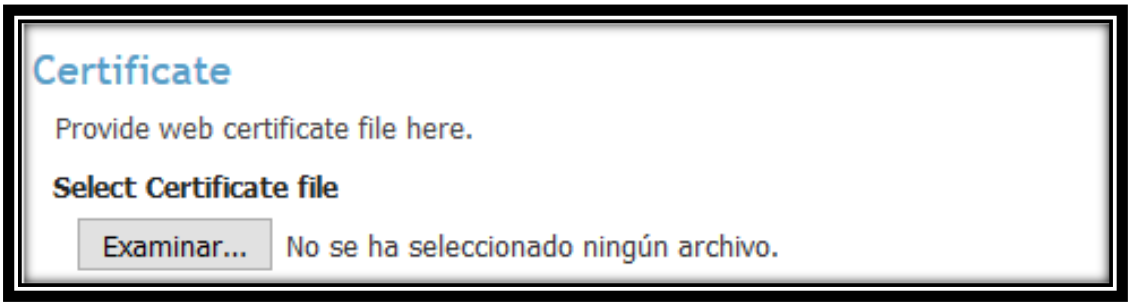


Figura 64: Configuración de la Subsección Certificate.

Fuente: Autor.

- **Private Key (Llave Privada).**

Esta subsección se emplea para proporcionar las claves privadas al certificado Web del Servidor OpenVPN (ver Figura 65).

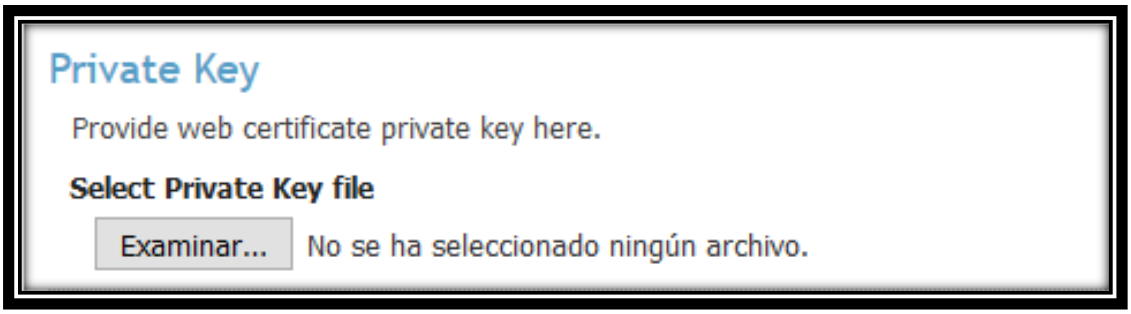


Figura 65: Configuración de la Subsección Private Key.

Fuente: Autor.

- **Validate (Validar).**

En esta subsección se validan los certificados y las claves seleccionadas anteriormente. Para ello, se realiza clic en “Validate”. Además, permite volver al certificado activo actual mediante la opción “Revert” (ver Figura 66).

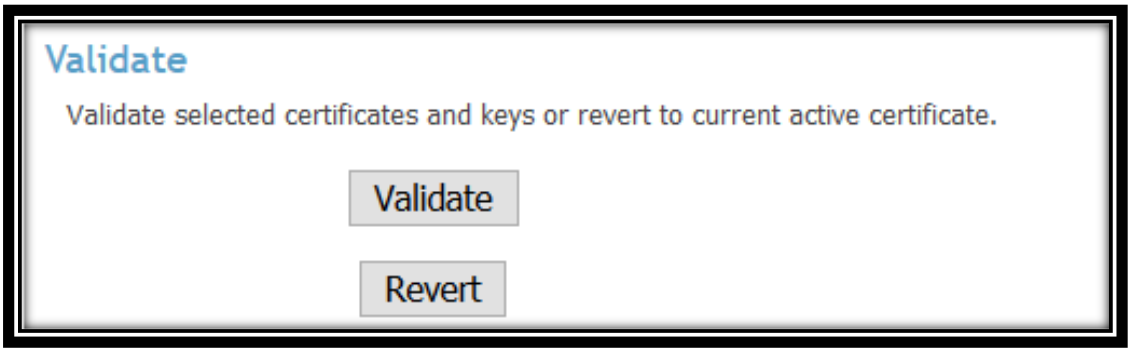


Figura 66: Configuración de la Subsección Validate.

Fuente: Autor.

- **Finish (Finalizar).**

En esta subsección se guardan los certificados y claves después de a ver realizado la validación. Para guardar las opciones validadas se realiza clic en la opción “Save” (ver Figura 67).

Figura 67: Configuración de la Subsección Finish.

Fuente: Autor.

f) SSL Settings (Configuraciones de SSL).

Después de que se realizó las configuraciones en la página “Web Server”, se ingresó a la página de configuración “SSL Settings” en la sección “Configuration” (ver Figura 68).

Figura 68: Configuración de la Página SSL Settings.

Fuente: Autor.

- **SSL Library (Biblioteca SSL).**

En esta subsección se configuró la biblioteca SSL, la misma que se utilizó para las comunicaciones seguras en el Servidor Web y para la asignación del protocolo de túnel OpenVPN. Se escogió la opción de OpenSSL para el Servidor de Acceso OpenVPN (ver Figura 69).

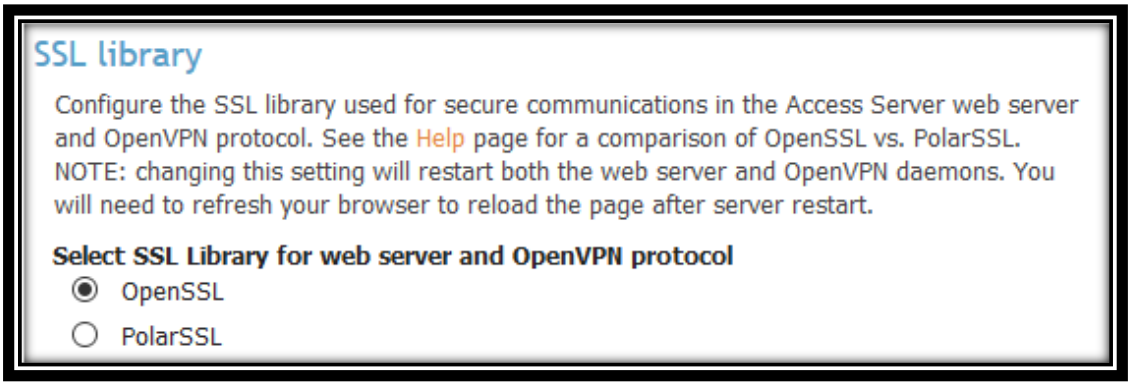


Figura 69: Configuración de la Subsección SSL Library.

Fuente: Autor.

- **SSL/TLS options for OpenVPN (SSL/TLS opciones para OpenVPN).**

En esta subsección se seleccionó la opción “Default”. La misma que sirvió para configurar la versión del protocolo de túnel asignado al Servidor de Acceso OpenVPN (ver Figura 70).

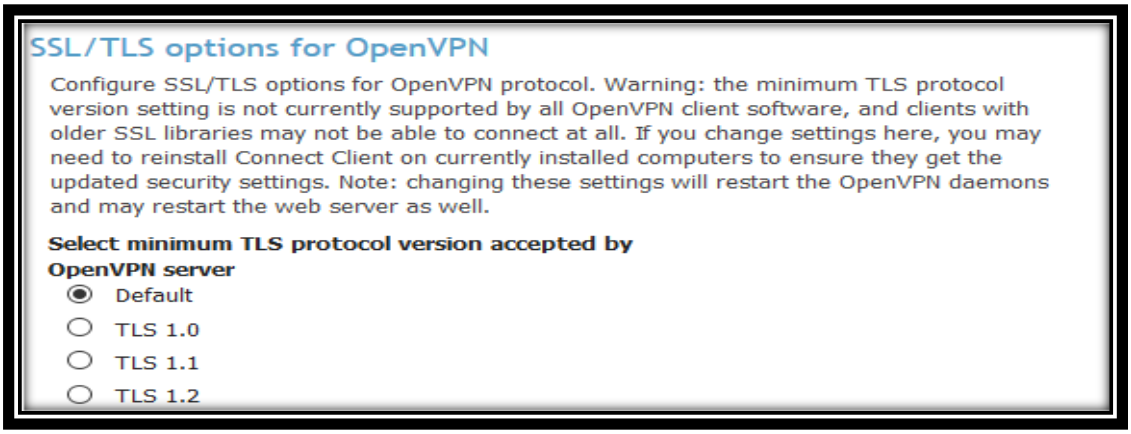


Figura 70: Configuración de la Subsección SSL/TLS options for OpenVPN.

Fuente: Autor.

- **SSL/TLS options for Web Server (SSL/TLS opciones para el Servidor Web).**

En esta subsección se seleccionó la opción “TLS 1.0”, la cual permitió configurar las opciones de SSL / TLS para el servidor web del Servidor de Acceso OpenVPN (ver Figura 71).

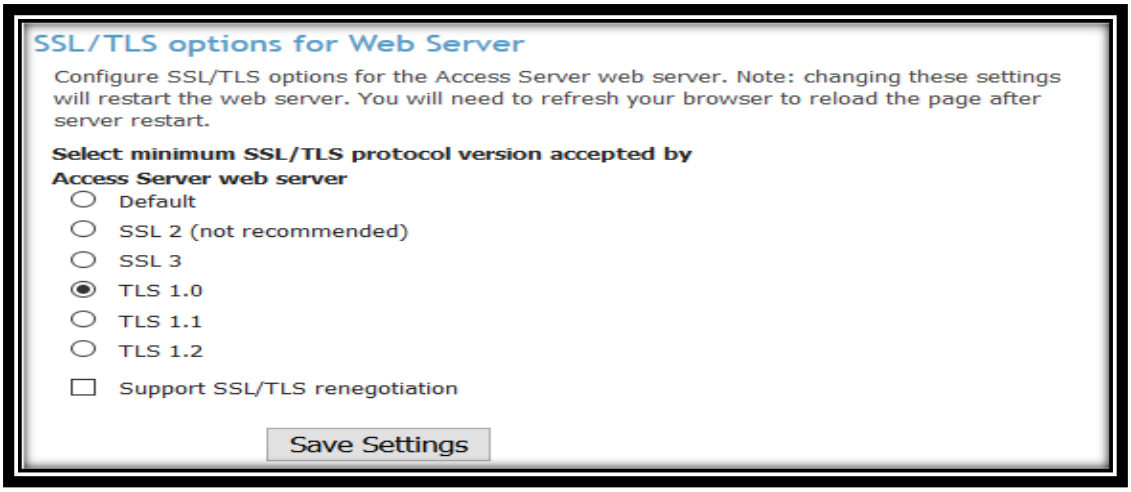


Figura 71: Configuración de la Subsección SSL/TLS options for Web Server.

Fuente: Autor.

g) Client Settings (Configuraciones del Cliente).

Una vez que se realizó las configuraciones en la página “SSL Settings”, se ingresó a la página de configuración “Client Settings” en la sección “Configuration” (ver Figura 72).

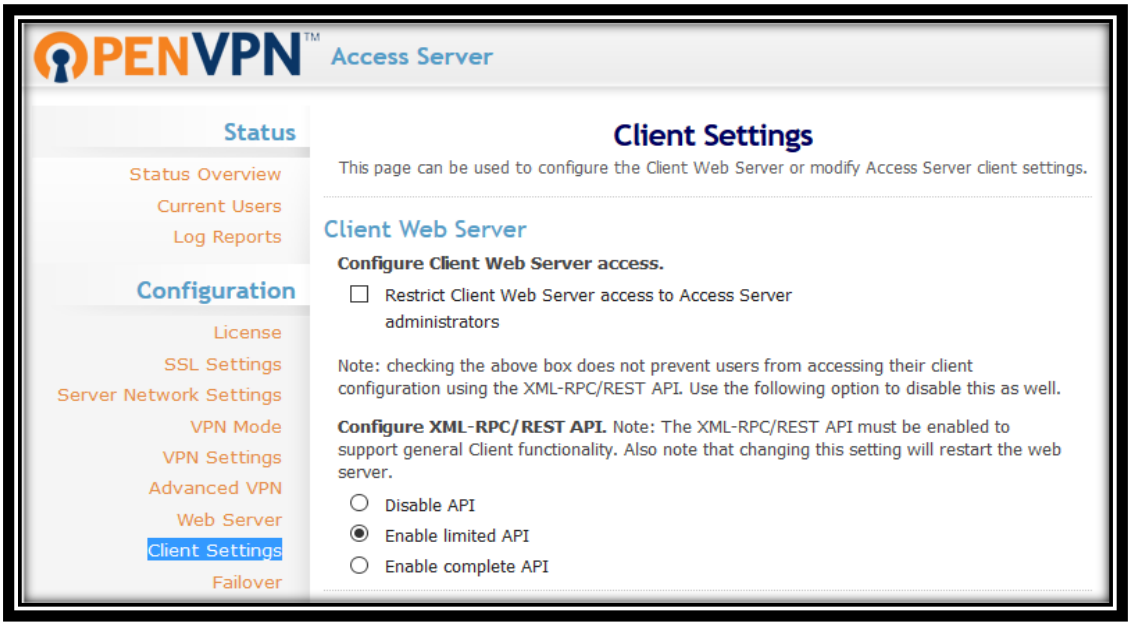


Figura 72: Configuración de la Página Client Settings.

Fuente: Autor.

- **Client Web Server (Servidor Web Cliente).**

En esta subsección se marcó la opción “Enable Limited API” para configurar XML-RPC/API REST, la cual permitió apoyar las funcionalidades generales del cliente dentro del servidor Web (ver Figura 73).

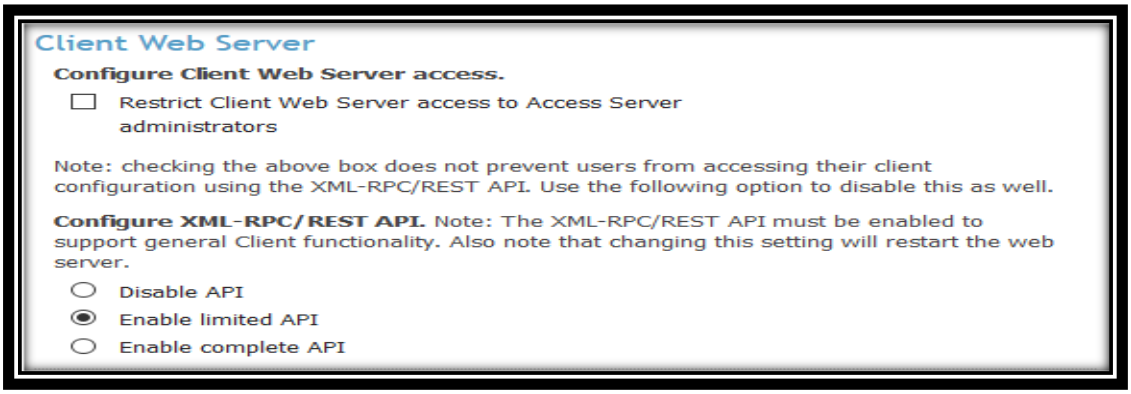


Figura 73: Configuración de la Subsección Client Web Server.

Fuente: Autor.

- **Configure Google Authenticator support (Configurar Soporte Autenticador de Google).**

Esta subsección se emplea para configurar “Google Authenticator”, el cual es un sistema de autenticación de contraseña única basada en el tiempo (ver Figura 74). Cuando se activa la opción para su uso, los usuarios tendrán que proporcionar las contraseñas de un solo uso, además de otras credenciales de acceso al conectarse a la VPN. Los usuarios tendrán que ejecutar la aplicación Google Authenticator en su teléfono móvil e introducirlos mediante el escaneo de un código QR desde el servidor Web Cliente.

Figura 74: Configuración de la Subsección Configure Google Authenticator support.

Fuente: Autor.

- **Customize Client Web Server UI (Cliente Personalizado de Interfaz de Usuario del Servidor Web).**

En esta subsección se seleccionó las opciones para controlar la visibilidad de los enlaces proporcionados a los usuarios del servidor Web al momento de acceder a la página principal de autenticación del cliente OpenVPN (ver Figura 75).

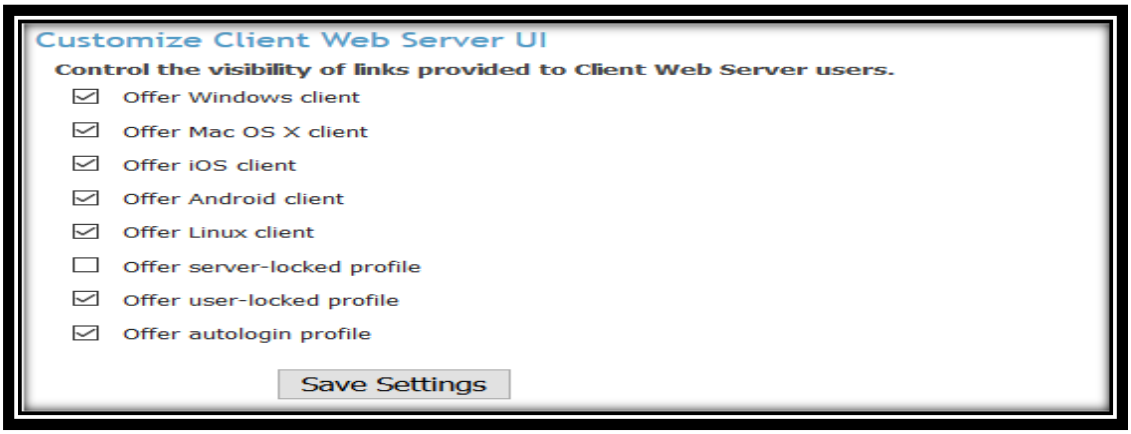


Figura 75: Configuración de la Subsección Customize Client Web Server UI.

Fuente: Autor.

Una vez que se terminó con las configuraciones en la página “Client Settings”, se realizó clic en la opción “Save Settings” para guardar las configuraciones realizadas.

h) License (Licencia).

Luego de que se realizó las configuraciones en la página “Client Settings”, se ingresó a la página de configuración “License” en la sección “Configuration” (ver Figura 76).

Figura 76: Configuración de la Página License.
Fuente: Autor.

El licenciamiento para el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se lo adquirió de forma personal. Se adquirió una licencia para 30 usuarios concurrentes debido a que el Servidor de Acceso OpenVPN únicamente otorga 2 conexiones de usuarios concurrentes.

La adquisición de las 30 licencias para el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja se la realizó por parte del Tesista. Se seleccionó 30 licencias debido a su costo económico y a las reuniones efectuadas con el Ingeniero Jhon Calderón; Subdirector de Redes y Telecomunicaciones y con el Director del

Departamento de Telecomunicaciones e Información; Ing. Milton Labanda. En donde se manifestó que el Tesista adquirirá por sus propios medios económicos la cantidad de 30 licencias y en la nueva planificación presupuestaria de la Universidad Nacional de Loja se irá adquiriendo nuevas licencias acorde a la necesidad institucional.

El valor de cada licencia adquirida para el Servidor de Acceso OpenVPN fue de 10.00 dólares, sumando un total de 200 dólares por las 30 licencias que se adquirió.

- **Installed License Keys (Claves de Licencia Instaladas).**

En esta subsección se instaló la licencia que se adquirió para el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja (ver Figura 77).

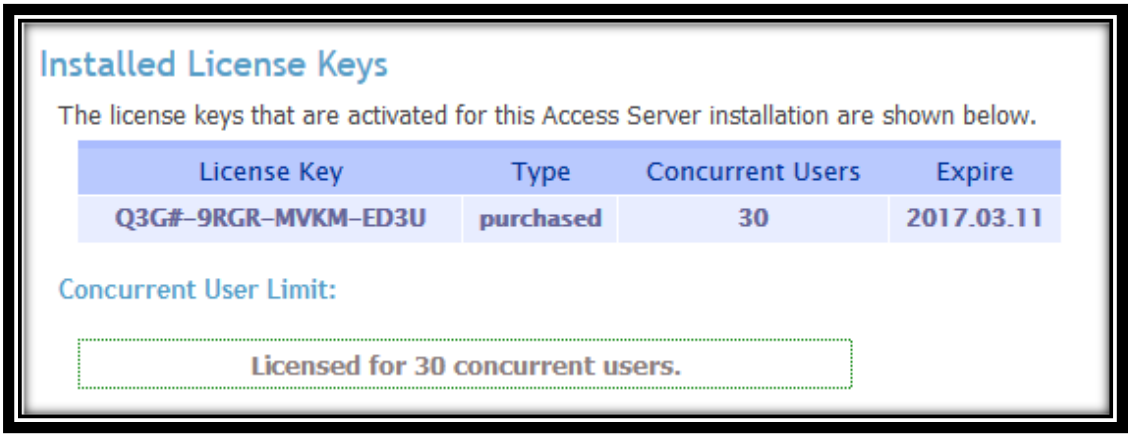


Figura 77: Configuración de la Subsección Installed License Keys.
Fuente: Autor.

La clave de la licencia que se activó para el Servidor OpenVPN fue: Q3G#-9RGR-MVKM-ED3U. La misma que permitió la conexión simultanea de 30 usuarios concurrentes.

- **Add A New License Key (Agregar una nueva Clave de Licencia).**

En esta subsección se agregó la clave de la licencia que se adquirió para el Servidor OpenVPN desde la página oficial del Servidor de Acceso (ver Figura 78). Para ello, se ingresó la clave de la licencia y se seleccionó la opción “Add A New License Key”.

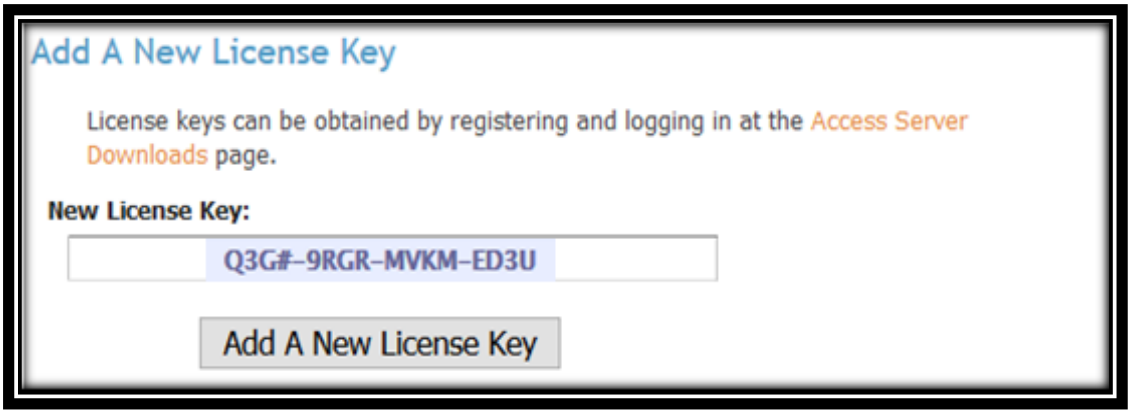


Figura 78: Configuración de la Subsección Add A New License Key.

Fuente: Autor.

- **Download Renewal Keys (Descargar Claves de Renovación).**

En esta subsección se descargan las claves de las licencias en caso de que se las haya renovado (ver Figura 79).

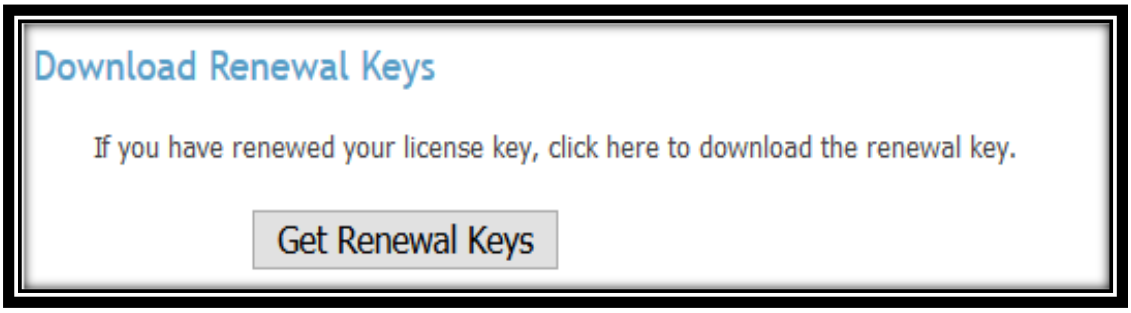


Figura 79: Configuración de la Subsección Download Renewal Keys.

Fuente: Autor.

i) Log Reports (Informes de Registro).

Después de que se realizó las configuraciones en la página “License”, se ingresó a la página de informes de registro “Log Reports” en la sección “Status” (ver Figura 80).

En esta subsección se encuentra la página de Informes de Registro, en la cual se muestra de una forma detallada los informes de los accesos a la Red Privada Virtual de la Universidad Nacional de Loja.

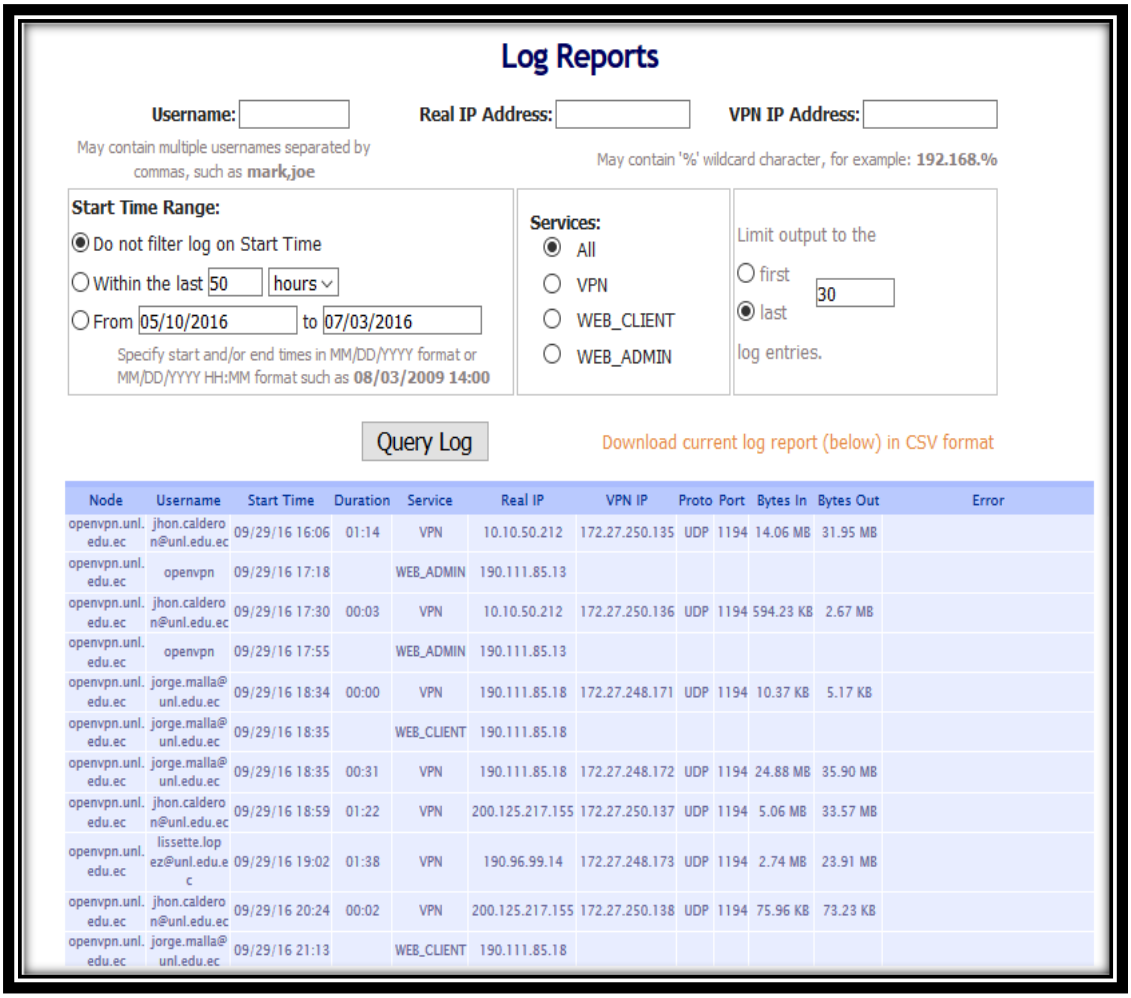


Figura 80: Configuración de la Página de Informes Log Reports.

Fuente: Autor.

Para realizar las consultas en la página de informes de registro se deben especificar las restricciones de entrada (ver Figura 81):

- **Nombre de usuario:** un nombre de usuario único o múltiples nombres de usuario separados por comas (en blanco para cualquier 'Username').
- **Dirección IP real:** una dirección IP pública, incluyendo posiblemente un carácter % como comodín (en blanco para 'Cualquier dirección IP real').
- **Dirección IP VPN:** una dirección IP pública, posiblemente incluyendo un carácter % como comodín (en blanco para 'Cualquier dirección IP VPN').
- **El rango de tiempo:** se realizan consultas estableciendo rangos de tiempo y fechas.
- **Acceso a los Servicios:** se realizan las consultas especificando el tipo de acceso que se realizó.

- **Número de entradas:** especificando las consultas por medio de un rango de los últimos accesos al Servidor VPN.

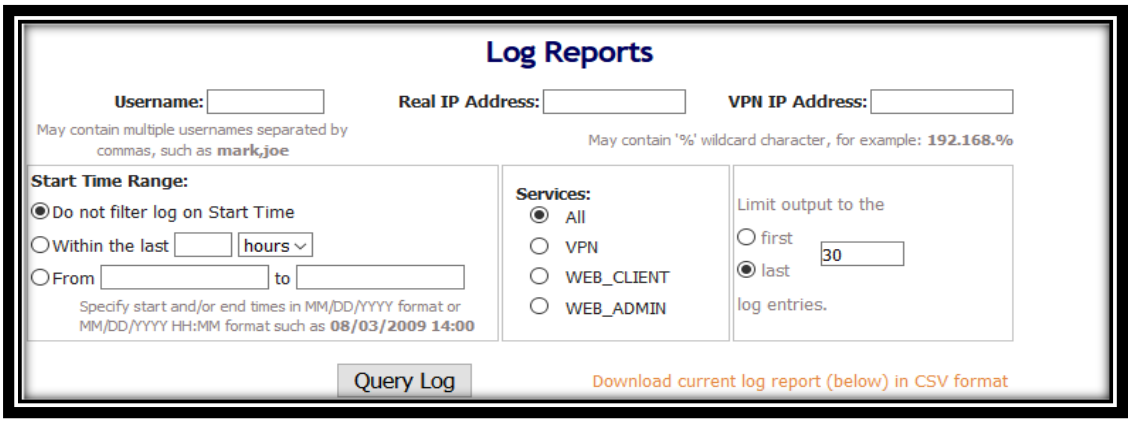
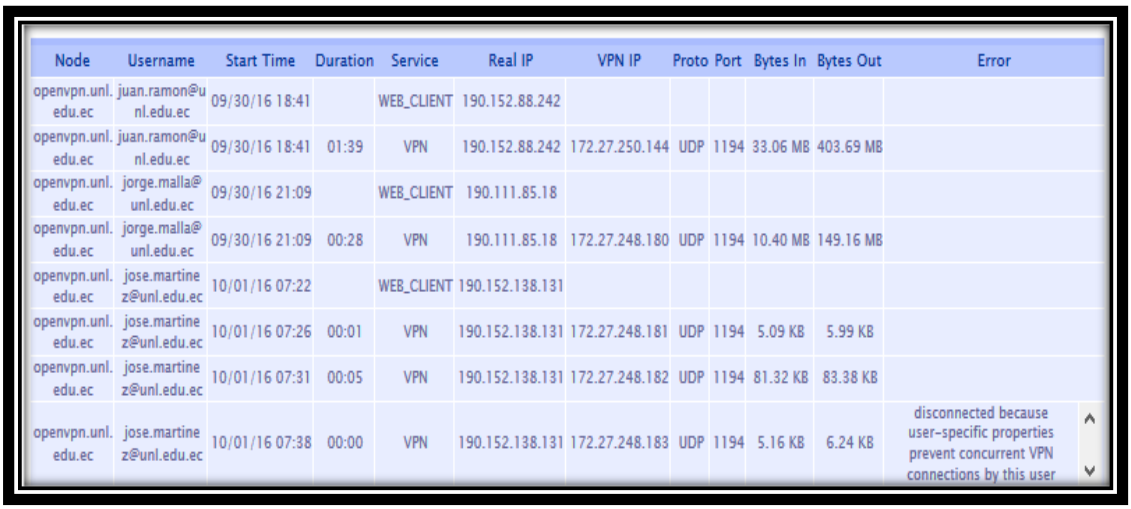


Figura 81: Consultas en la Página Log Reports.

Fuente: Autor.

El informe de registro presenta la siguiente información (ver Figura 82): Un nodo (nombre del hostname), el nombre del usuario, la hora de inicio de la conexión VPN, el tiempo de duración de la conexión VPN, el servicio por el cual se accedió, la dirección IP real del cliente OpenVPN, la dirección IP que el Servidor de Acceso OpenVPN le ha asignado al cliente, el protocolo que se está utilizando: TCP o UDP, el número de puerto por el cual se ha establecido la comunicación, la cantidad de datos enviados, la cantidad de datos recibidos y finalmente cualquier mensaje de error en caso de presentarse al momento de acceder al servidor OpenVPN.



Node	Username	Start Time	Duration	Service	Real IP	VPN IP	Proto	Port	Bytes In	Bytes Out	Error
openvpn.unl.edu.ec	juan.ramon@unl.edu.ec	09/30/16 18:41		WEB_CLIENT	190.152.88.242						
openvpn.unl.edu.ec	juan.ramon@unl.edu.ec	09/30/16 18:41	01:39	VPN	190.152.88.242	172.27.250.144	UDP	1194	33.06 MB	403.69 MB	
openvpn.unl.edu.ec	jorge.malla@unl.edu.ec	09/30/16 21:09		WEB_CLIENT	190.111.85.18						
openvpn.unl.edu.ec	jorge.malla@unl.edu.ec	09/30/16 21:09	00:28	VPN	190.111.85.18	172.27.248.180	UDP	1194	10.40 MB	149.16 MB	
openvpn.unl.edu.ec	jose.martinez@unl.edu.ec	10/01/16 07:22		WEB_CLIENT	190.152.138.131						
openvpn.unl.edu.ec	jose.martinez@unl.edu.ec	10/01/16 07:26	00:01	VPN	190.152.138.131	172.27.248.181	UDP	1194	5.09 KB	5.99 KB	
openvpn.unl.edu.ec	jose.martinez@unl.edu.ec	10/01/16 07:31	00:05	VPN	190.152.138.131	172.27.248.182	UDP	1194	81.32 KB	83.38 KB	
openvpn.unl.edu.ec	jose.martinez@unl.edu.ec	10/01/16 07:38	00:00	VPN	190.152.138.131	172.27.248.183	UDP	1194	5.16 KB	6.24 KB	disconnected because user-specific properties prevent concurrent VPN connections by this user

Figura 82: Elementos de la Página de Informes de Registro.

Fuente: Autor.

Los Informes de Registro se los puede exportar en formato CSV para su uso posterior con el software de la hoja de cálculo Excel.

6.3.3. Actividad 3: Configuración de los clientes en el Servidor OpenVPN.

En esta actividad se realizó la configuración de los usuarios dentro del Servidor de Acceso OpenVPN de la Universidad Nacional de Loja.

6.3.3.1. Autenticación de los Clientes VPN en el Servidor de Acceso OpenVPN.

Después de que se realizó la instalación y configuración del Servidor de Acceso OpenVPN, se seleccionó la autenticación que emplearan los usuarios OpenVPN dentro del Servidor de Acceso OpenVPN de la Universidad Nacional de Loja.

a) Autenticación General.

Dentro de la sección "Authentication" de la página de interfaz de usuario de administración web, se encuentra la página de configuración "General" (ver Figura 83).

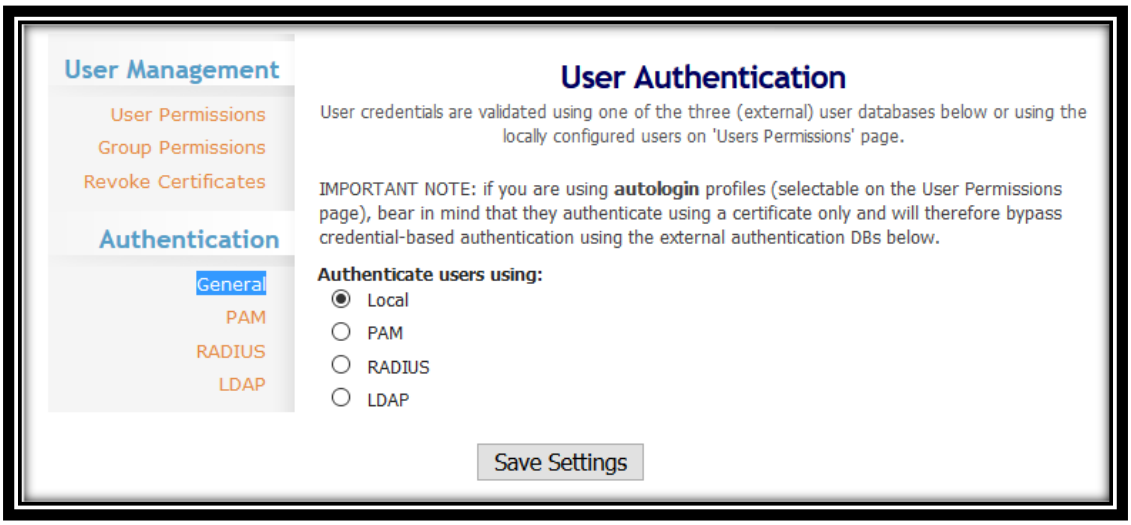


Figura 83: Configuración de la Página General.

Fuente: Autor.

Una vez que se accedió a la sección "General", se encuentra la subsección "User Authentication". En la cual se seleccionó el tipo de autenticación que emplearan los usuarios en el Servidor de Acceso OpenVPN (ver Figura 84).

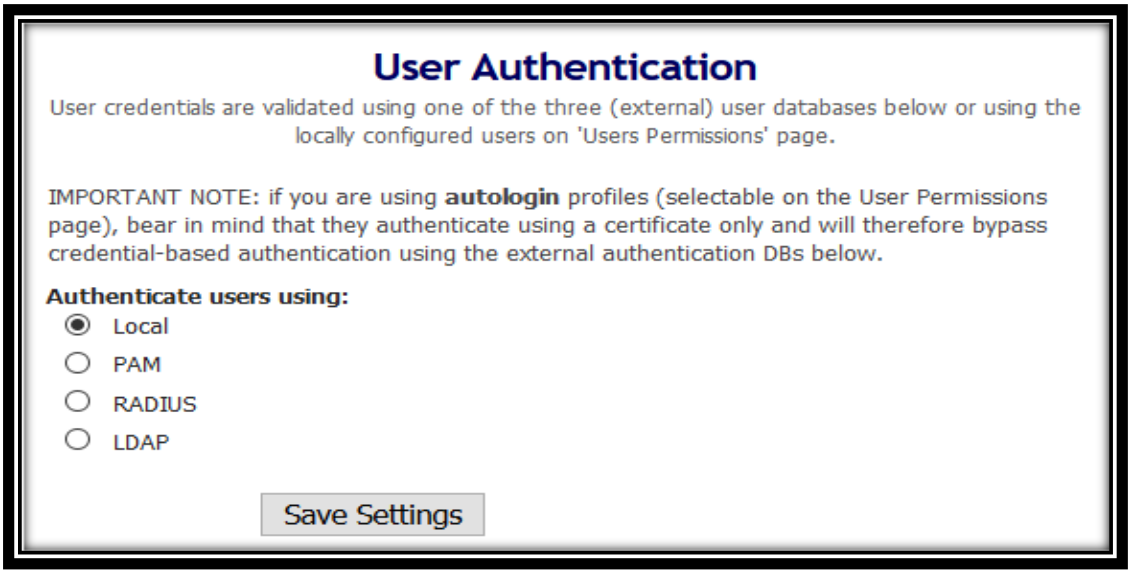


Figura 84: Configuración de la Subsección User Authentication.

Fuente: Autor.

El Servidor de Acceso OpenVPN posee los siguientes sistemas de autenticación de usuario:

- **Local:** Es un sistema de autenticación de usuario que está gestionado por el Servidor de Acceso OpenVPN. Mediante este tipo de autenticación se puede establecer la contraseña de los usuarios de la VPN en la página de permisos de usuario, cuando la autenticación local está activada.

- **PAM (Módulos de autenticación conectables):** Aunque no es un modelo de autenticación en sí, sino que se trata de un mecanismo que proporciona una interfaz entre las aplicaciones de usuario y diferentes métodos de autenticación. El sistema lo utiliza para autenticar a los usuarios de la máquina Unix que se ejecuta en el Servidor de Acceso OpenVPN.

- **RADIUS (Servicio Telefónico de autenticación remota de usuario):** El Servidor de Acceso OpenVPN puede establecer conexión entre uno y cinco servidores RADIUS. Los mismos que pueden ser contactados para la autenticación de usuarios y también para la contabilidad de usuarios.

- **LDAP (Protocolo Ligero/Simplificado de Acceso a Directorios):** Un controlador de dominio de Active Directory u otro servidor LDAP se utiliza para validar las credenciales de usuario.

En la página "General" de autenticación de usuario se seleccionó el método de autenticación "Local", ya que en la infraestructura de red de la Universidad Nacional de Loja no existe un servidor LDAP, ni tampoco un servidor RADIUS disponibles en la actualidad.

Además, se configuró los usuarios de la red privada virtual localmente, ya que en la actualidad se está estandarizando las tecnologías utilizadas en la infraestructura de red de la Universidad Nacional de Loja.

No se utilizó PAM (Módulo de autenticación conectable) debido a que no es un modelo de autenticación en sí, sino que se trata de un mecanismo que proporciona una interfaz entre las aplicaciones de usuario y diferentes métodos de autenticación.

Una vez que se terminó con las configuraciones en la página "General", se realizó clic en la opción "Save Settings" para guardar las configuraciones realizadas.

b) PAM (Módulo de Autenticación Conectable).

Dentro de la sección "Authentication" de la página de interfaz de usuario de administración web, se encuentra la página de configuración "PAM" (ver Figura 85).

Figura 85: Configuración de la Página PAM.

Fuente: Autor.

Una vez que se accedió a la sección “PAM”, se encuentra la subsección “PAM Authentication”. La cual contiene la opción “Use PAM” para configurar el sistema de autenticación de usuarios en el Servidor de Acceso OpenVPN (ver Figura 86).

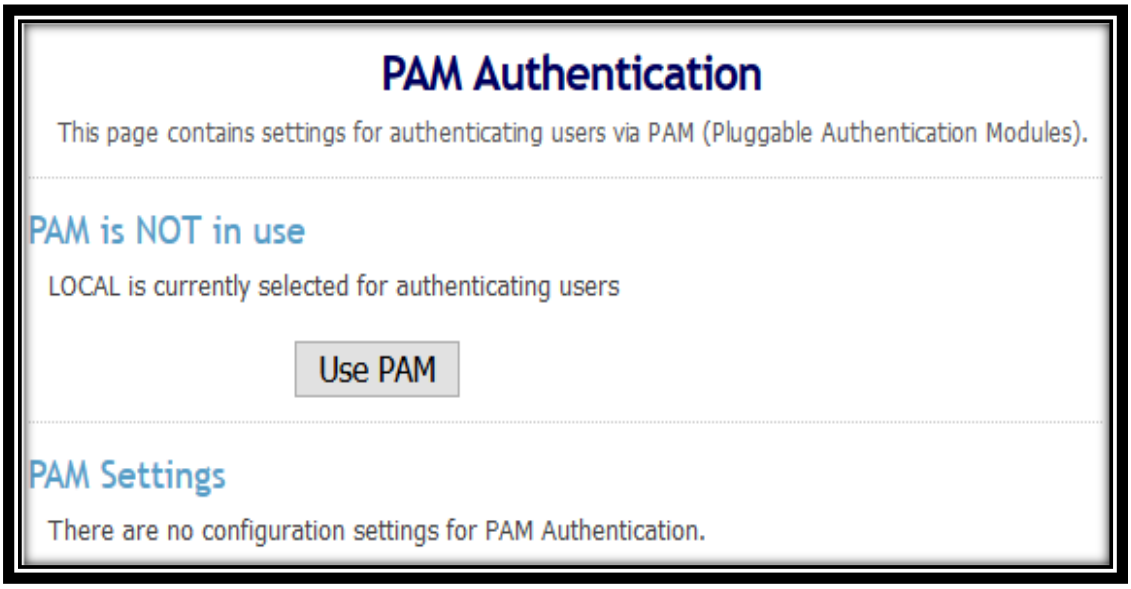


Figura 86: Configuración de la Subsección PAM Authentication.

Fuente: Autor.

El sistema de autenticación PAM, es el método estándar para la autenticación de usuarios en un sistema Unix. Si se selecciona la opción “Use PAM” para la autenticación de usuarios en el Servidor de Acceso OpenVPN, significa que los usuarios deben proporcionar las mismas credenciales de usuario y contraseña para el servidor de acceso como lo harían al autenticarse en el host Unix que ejecuta el Servidor de Acceso OpenVPN.

Internamente, el Servidor de Acceso OpenVPN utiliza un servicio de PAM llamado openvpn_as, que corresponde al archivo /etc/pam.d/openvpn_as (añadido durante la configuración inicial del Servidor de Acceso OpenVPN).

c) RADIUS (Servicio Telefónico de Autenticación Remota de Usuario).

Dentro de la sección “Authentication” de la página de interfaz de usuario de administración web, se encuentra la página de configuración “RADIUS” (ver Figura 87).

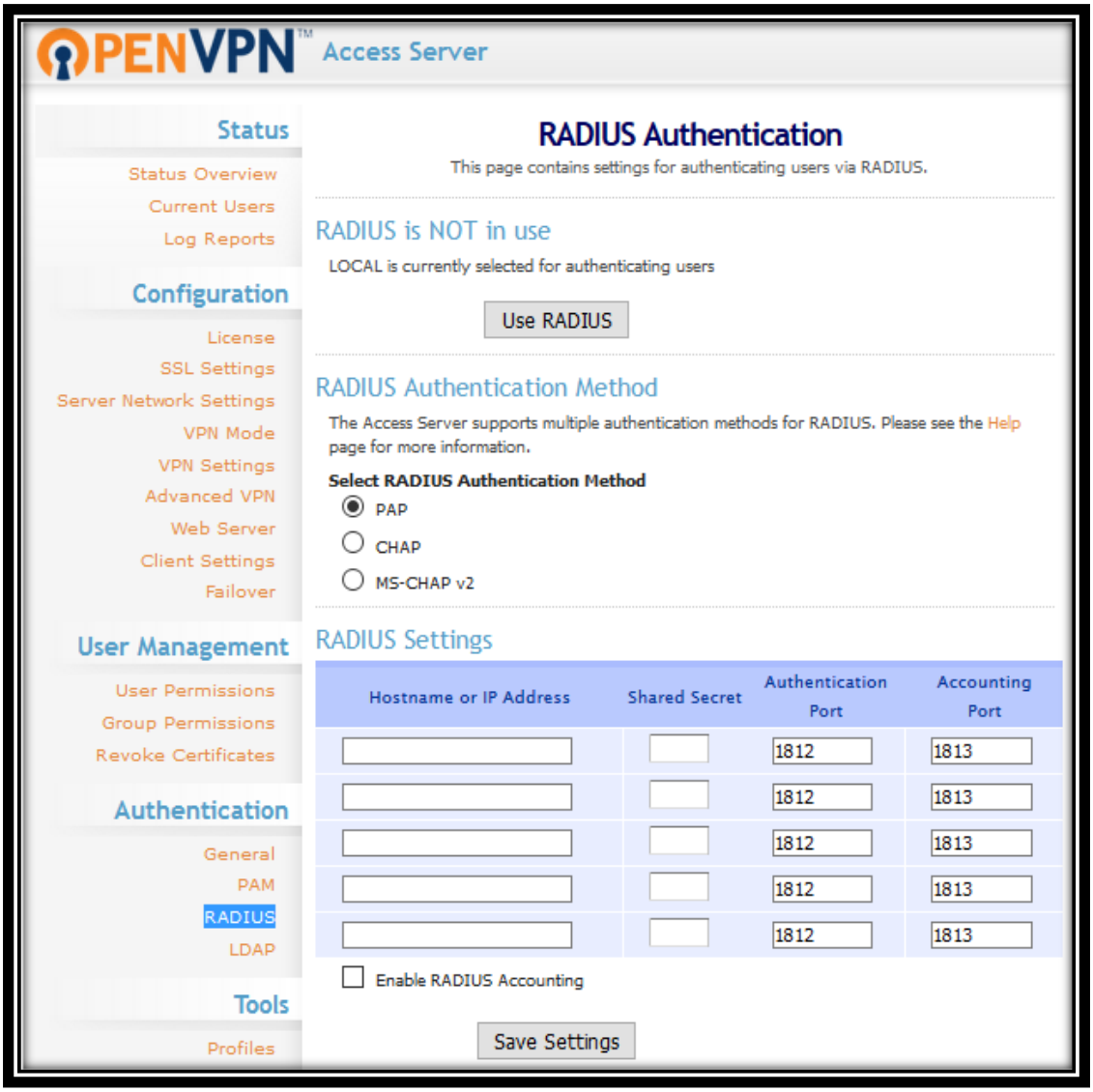


Figura 87: Configuración de la Página RADIUS.

Fuente: Autor.

Este sistema de autenticación permite que hasta cinco servidores RADIUS redundantes puedan ser configurados en el Servidor de Acceso OpenVPN. Para autenticar los usuarios a través de RADIUS, el Servidor de Acceso OpenVPN intenta comunicarse con uno de los servidores RADIUS configurados (elegidos al azar). Si los tiempos de comunicación (después de 5 segundos) no responden, el servidor de acceso vuelve a intentar la comunicación al mismo servidor una vez más.

A continuación se describe como se debería asociar el sistema de autenticación de usuarios RADIUS con el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja.

- **RADIUS is not in use (RADIUS no está en uso).**

En esta subsección se configura el uso del sistema de autenticación RADIUS para el Servidor de Acceso OpenVPN. Para ello, se selecciona la opción “Use RADIUS” (ver Figura 88).

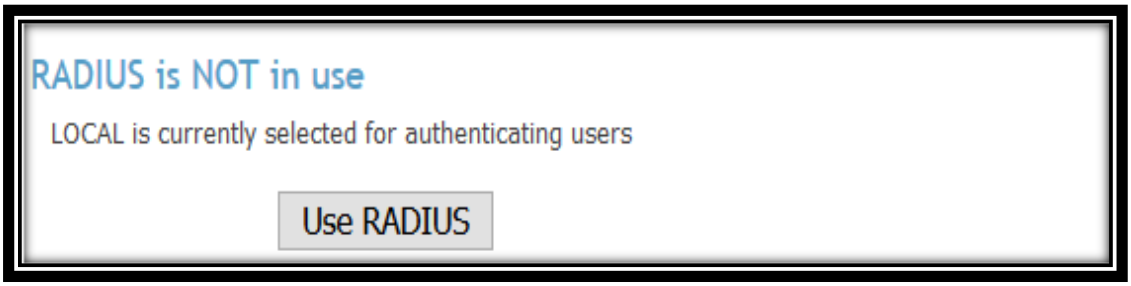


Figura 88: Configuración de la Subsección RADIUS is NOT in use.

Fuente: Autor.

- **RADIUS Authentication Method (Método de Autenticación RADIUS).**

En esta subsección se selecciona el método de autenticación que va a utilizar el sistema de autenticación RADIUS dentro del Servidor de Acceso OpenVPN (ver Figura 89).

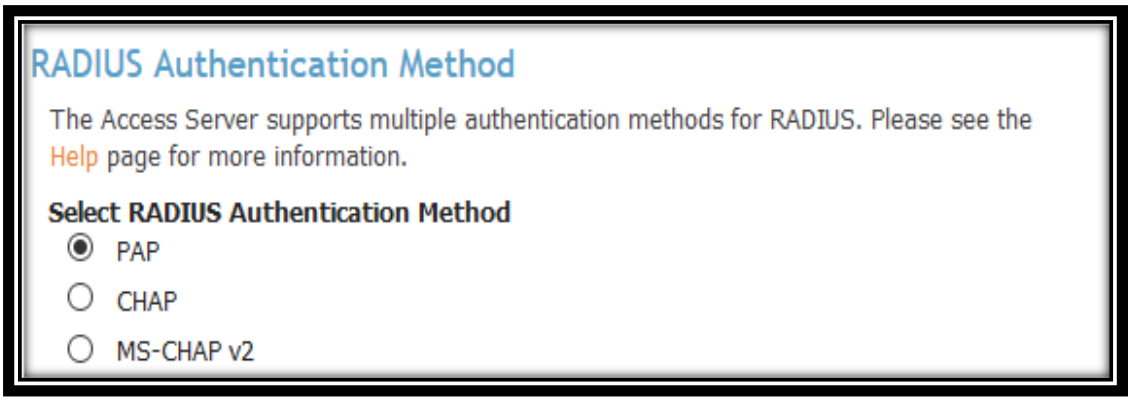


Figura 89: Configuración de la Subsección RADIUS Authentication Method.

Fuente: Autor.

- **RADIUS Settings (Configuraciones RADIUS).**

En esta subsección se realizan las configuraciones del sistema de autenticación RADIUS, para la conexión con el Servidor de Acceso OpenVPN (ver Figura 90).

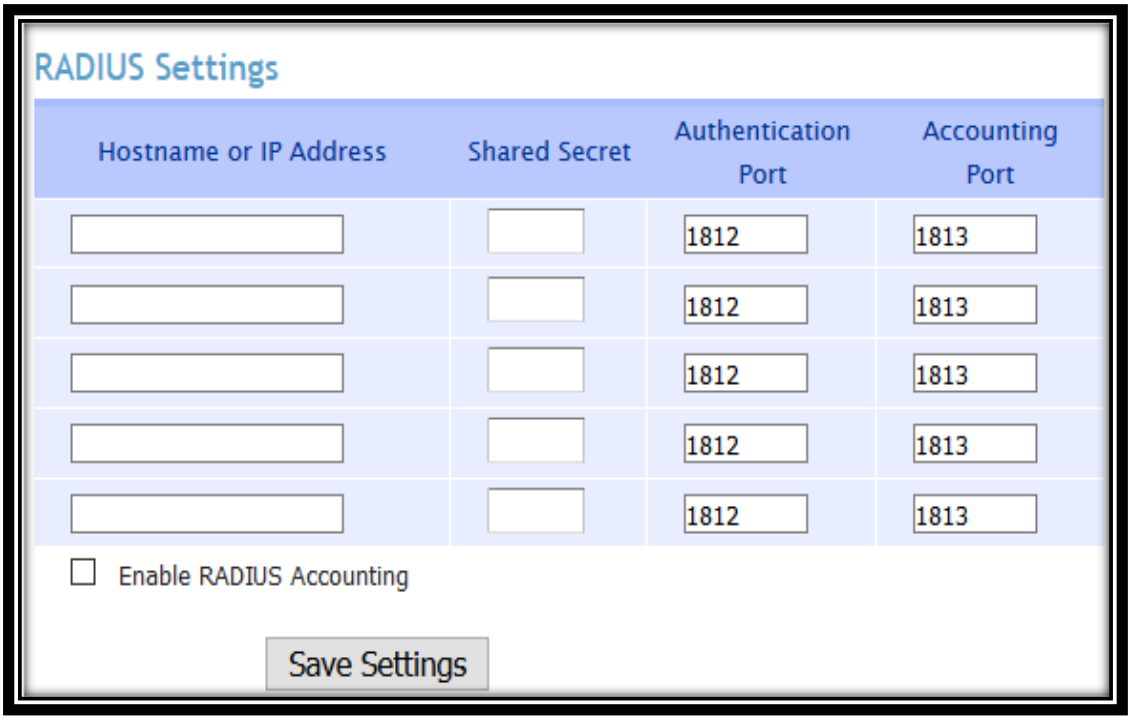


Figura 90: Configuración de la Subsección RADIUS Settings.

Fuente: Autor.

El sistema de autenticación de usuarios RADIUS permite que hasta cinco servidores RADIUS puedan ser configurados en el Servidor de Acceso OpenVPN. Para configurar cada Servidor RADIUS se debe especificar el nombre de host o dirección IP, el secreto compartido, el puerto de autenticación y el puerto de cuenta (RADIUS utiliza el puerto de autenticación: 1812 y el puerto de cuenta: 1813).

Una vez que se termina con las configuraciones en la página "RADIUS", se debe realizar clic en la opción "Save Settings" para guardar las configuraciones que se han realizado.

d) LDAP (Protocolo Ligero/Simplificado de Acceso a Directorios).

Dentro de la sección "Authentication" de la página de interfaz de usuario de administración web, se encuentra la página de configuración "LDAP" (ver Figura 91).

A continuación se describe como se debería configurar el sistema de autenticación de usuarios LDAP en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja.

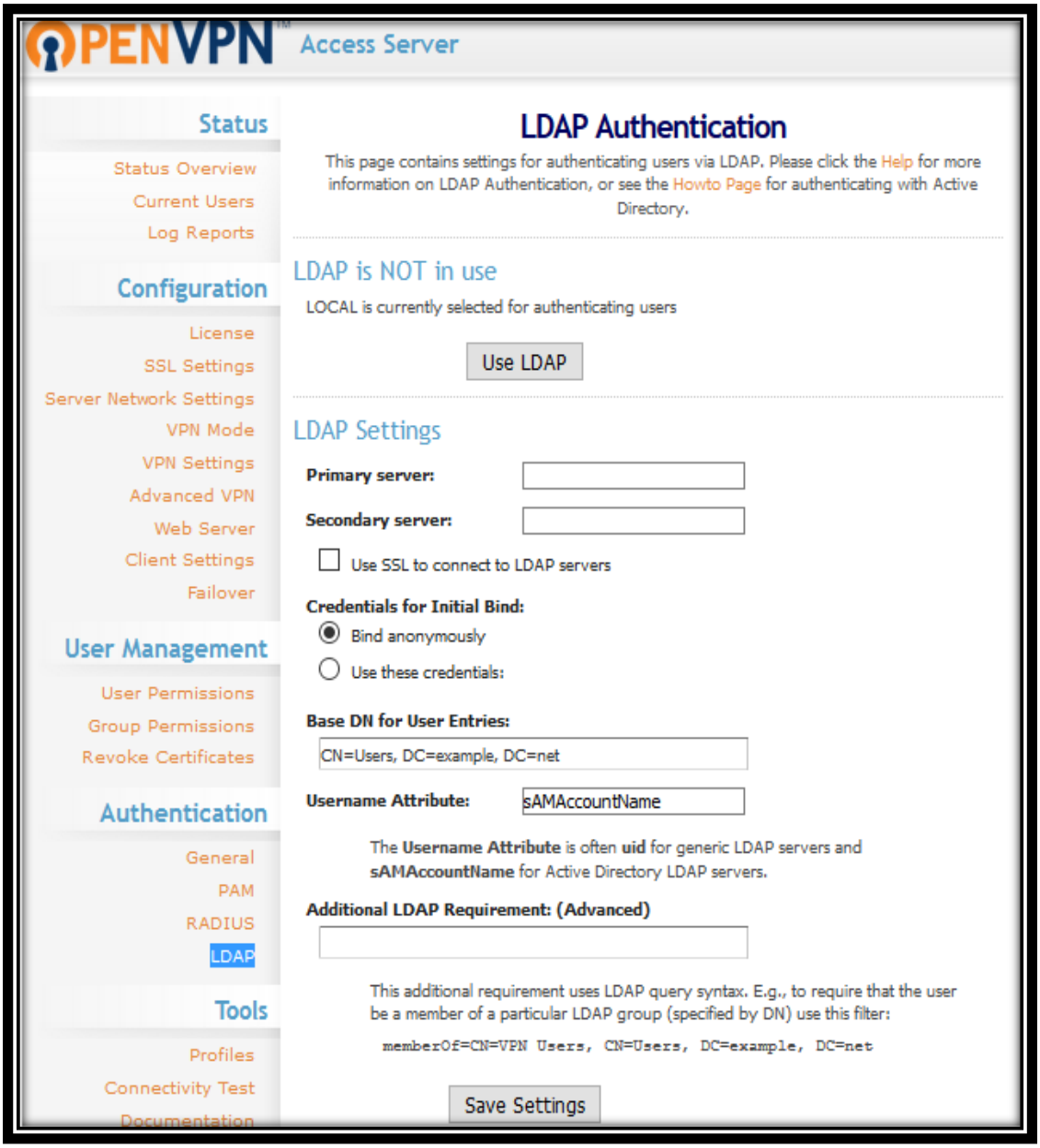


Figura 91: Configuración de la Página LDAP.

Fuente: Autor.

Para autenticar los usuarios a través de LDAP, el servidor de acceso lleva a cabo los siguientes pasos:

- **LDAP is NOT in use (LDAP no está en uso).**

En esta subsección se configura el sistema de autenticación LDAP para el Servidor de Acceso OpenVPN. Para ello, se selecciona la opción “Use LDAP” (ver Figura 92).

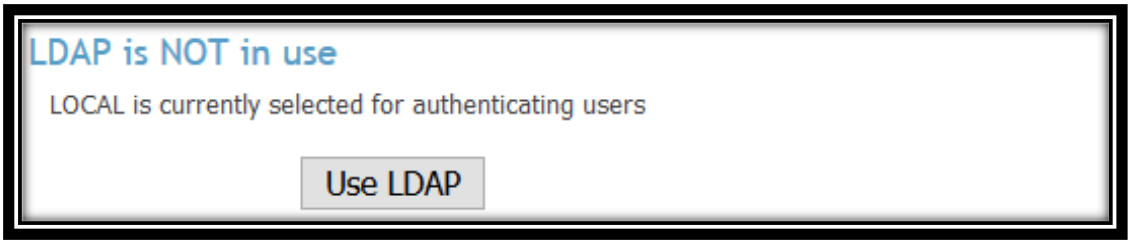


Figura 92: Configuración de la Subsección LDAP is NOT in use.

Fuente: Autor.

- **LDAP Settings (Configuraciones LDAP).**

En esta subsección se realizan las configuraciones del sistema de autenticación de usuarios LDAP, para la conexión con el Servidor de Acceso OpenVPN (ver Figura 93).

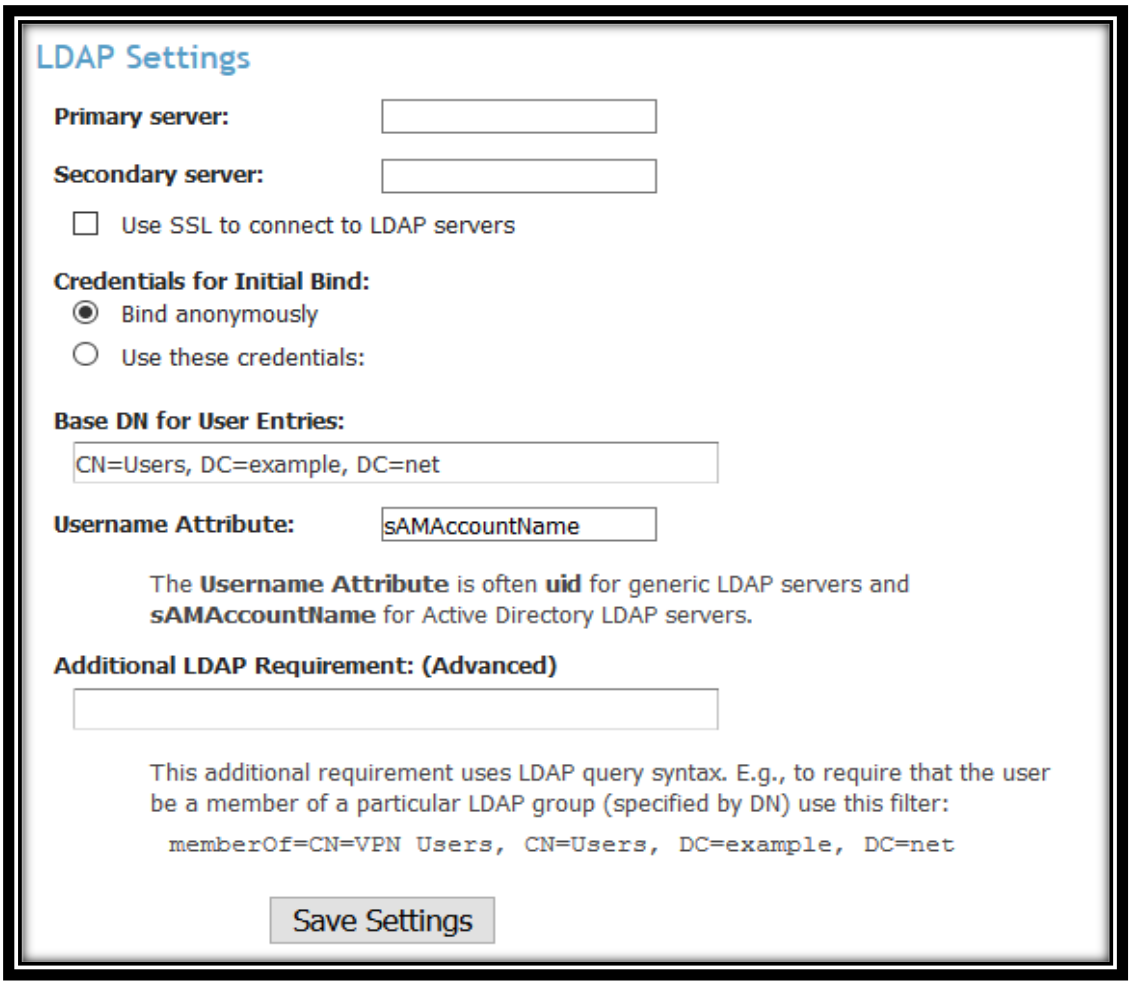


Figura 93: Configuración de la Subsección LDAP Settings.

Fuente: Autor.

Para asociar el sistema de autenticación de usuarios LDAP, con el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja. Primeramente se especifica en la opción "Primary Server" un servidor primario, ya sea con el nombre del host o la dirección IP del servidor. Además, en la opción "Secondary Server" se especifica un servidor secundario; si se encuentra especificado el servidor secundario, el Servidor de Acceso OpenVPN intentará comunicarse con el servidor secundario, si fallan los intentos de establecer comunicación con el servidor primario.

Una vez especificados los servidores LDAP (primario y secundario), se debe seleccionar la opción "Use SSL to Connect to LDAP servers" para establecer una conexión segura.

En la parte de "Credentials for Initial Bind" se debe seleccionar la opción "Bind anonymously" para unir de forma anónima al Servidor de Acceso OpenVPN.

Una vez realizada esta acción, en la parte de "Base DN for User Entries" se debe realizar una consulta LDAP para encontrar las entradas de usuarios; utilizando el DN (base para entradas de usuario). La entrada de un usuario es aquel cuyo valor de atributo coincide con el nombre de usuario introducido en la página de inicio de sesión.

Luego de realizar las consultas LDAP de las entradas de los usuarios, se coloca en la opción "Username Attribute" el nombre del usuario del Atributo para los servidores LDAP. En este caso el nombre es "sAMAccountName". Y finalmente en la opción "Additional LDAP Requirement" se puede especificar una restricción para la entrada de un usuario. Esto se lo utiliza, por ejemplo, para exigir la afiliación a un grupo LDAP en particular (especificado por su grupo DN).

Una vez que se termina con las configuraciones en la página "LDAP", se debe realizar clic en la opción "Save Settings" para guardar las configuraciones que se han realizado.

6.3.3.2. Configuración de los Clientes VPN en el Servidor de Acceso OpenVPN.

Después de que se realizó la configuración del sistema de autenticación de usuarios para el Servidor VPN, se inició con la configuración de los usuarios en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja.

a) Group Permissions (Permisos de Grupo).

Dentro de la sección “User Management” de la página de interfaz de usuario de administración web, se encuentra la página “Group Permissions” (ver Figura 94).

Figura 94: Configuración de la Página Group Permissions.

Fuente: Autor.

Una vez que se accedió a la página “Group Permissions”, se creó los grupos de usuarios para el Servidor de Acceso OpenVPN (ver Figura 95). Los grupos de usuarios que se crearon fueron definidos en base a los perfiles de usuario para la autenticación que se establecieron en el diseño de la Red Privada Virtual (ver Actividad 6 – Fase II de Resultados).

Los grupos de usuarios que se establecieron para la autenticación en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja fueron los siguientes:

- **uTI:** El grupo uTI le corresponde al Director de la Unidad de Telecomunicaciones e Información.
- **Administrador**: Corresponde a la persona que va a manejar el servicio de la VPN.

- **Docentes:** Son todos los docentes pertenecientes a la Universidad Nacional de Loja.
- **Estudiantes:** Son todos los estudiantes que pertenecen a la Universidad Nacional de Loja.
- **Administrativos:** Es todo el personal administrativo de la Universidad, excepto el personal de la Unidad de Telecomunicaciones e Información.
- **srei.uti:** Es el personal de mantenimiento y redes de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.
- **sdsw.uti:** Es el personal de software de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

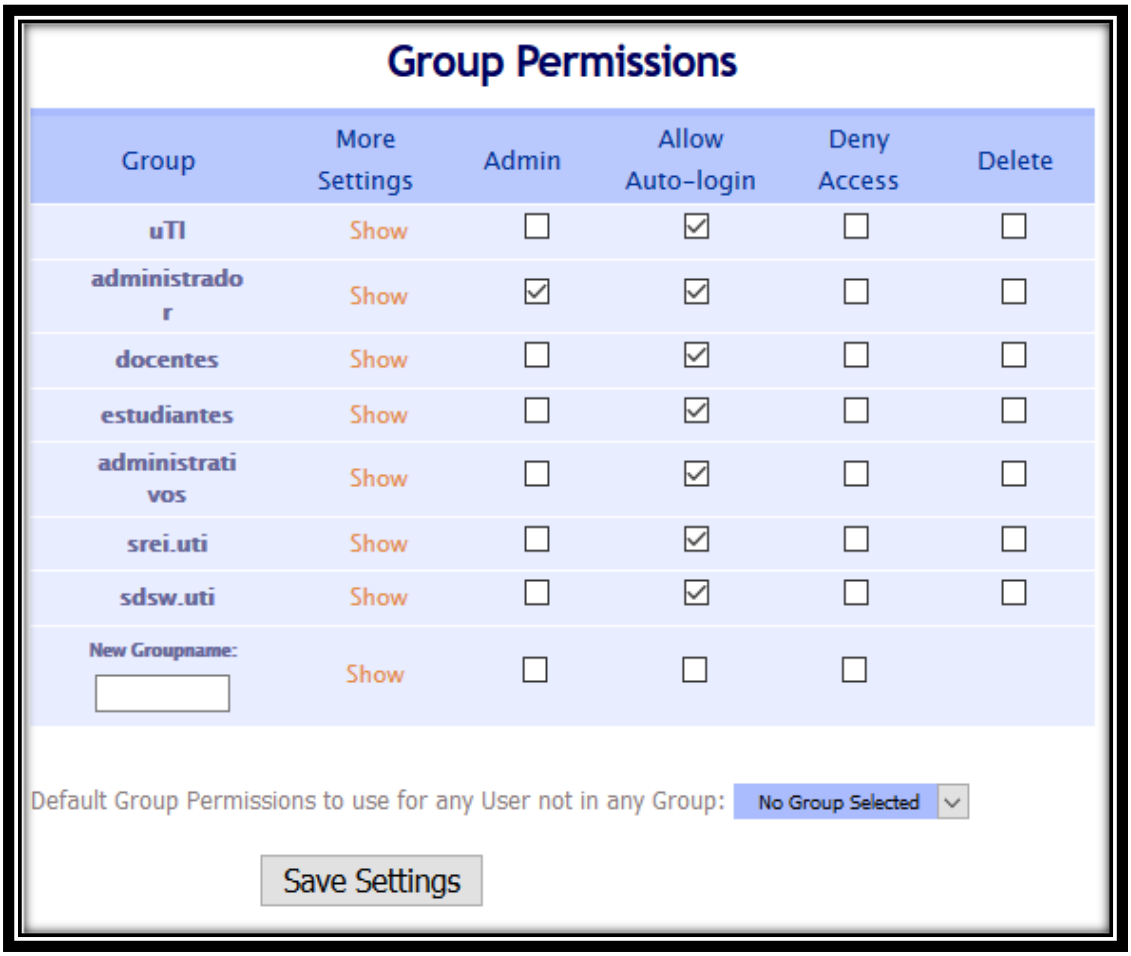


Figura 95: Creación de los Perfiles de usuarios.

Fuente: Autor.

Una vez que se crearon los grupos de usuarios para el acceso al Servidor OpenVPN, se establecieron los privilegios de acceso para cada uno de ellos.

A continuación se detallan los grupos de usuarios que se creó y los privilegios de acceso con que cuentan cada uno de ellos:

- **Grupo UTI.**

El grupo "uTI" se creó para asignarlo al Director de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja. Los privilegios de acceso que se le asignó a este grupo, se lo realizó a través de direccionamiento IP (ver Figura 96).

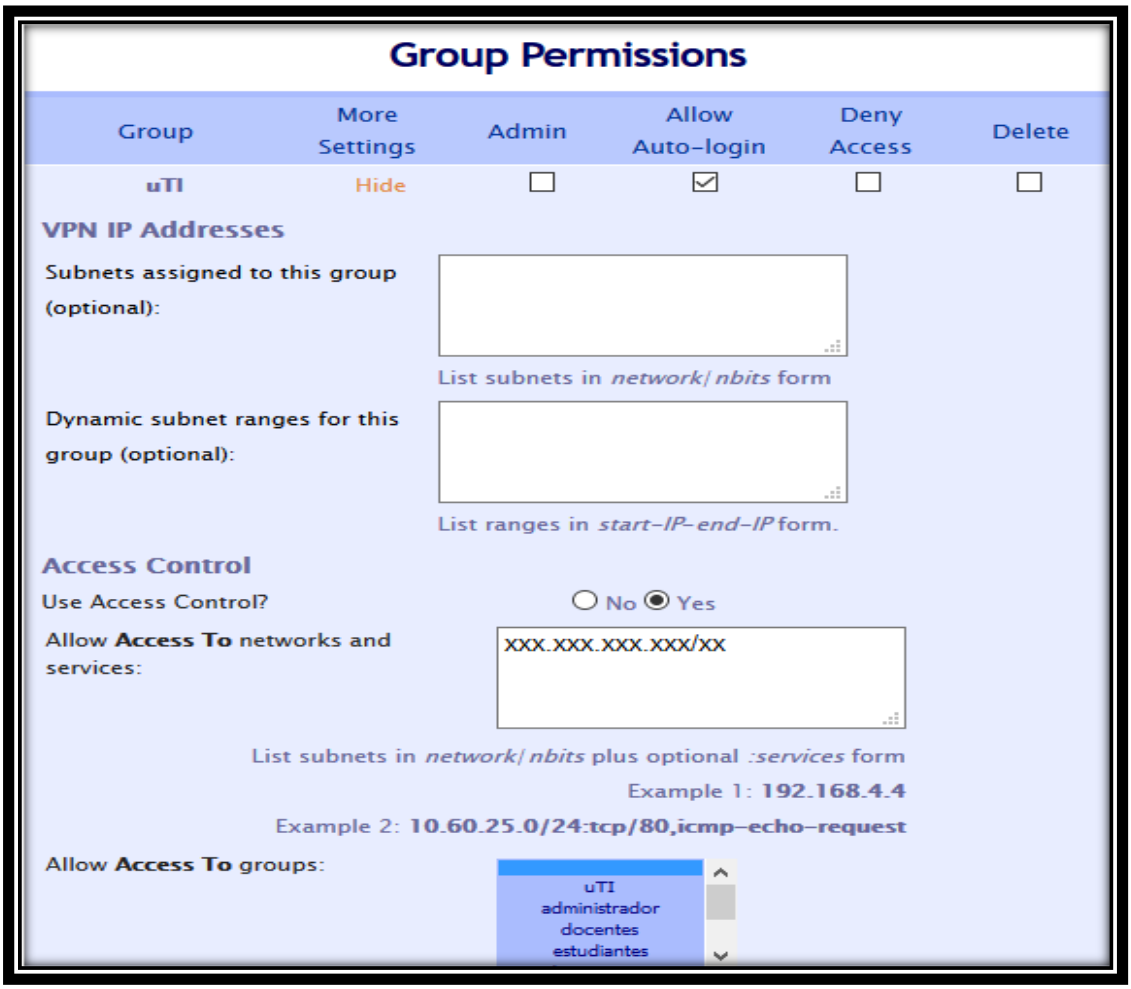


Figura 96: Configuración del Perfil de Usuario UTI.

Fuente: Autor.

Una vez que se accedió a la página "Group Permissions", se realizó clic en la opción "Show" del grupo "uTI" y se desplegó las opciones de configuración del grupo. Se accedió a la subsección "Access Control" y se seleccionó "Yes" para usar la opción de control de acceso.

Después de que se habilitó el control de acceso, en la opción "Allow Access To networks and services" se ingresó las subredes privadas adicionales a las que el grupo "uTI" va a tener los privilegios de acceso.

Luego de que se ingresó las subredes privadas para el grupo "uTI", se seleccionó la opción "Auto-login" para que se establezcan las conexiones automáticamente al momento de conectarse con el Servidor de Acceso OpenVPN. Además, se encuentran disponibles las opciones "Admin" que permite dar privilegios de administrador al grupo, la opción "Deny Access" que permite denegar el acceso del grupo al Servidor OpenVPN y la opción "Delete" que permite eliminar al grupo que se creó.

Cabe mencionar que el grupo "uTI", también posee el acceso a las bases de datos científicas de la institución, debido a la configuración de enrutamiento que se realizó en la Actividad 2 – Fase III de Resultados.

- **Grupo Administrador.**

El grupo "administrador" se creó para la administración del Servidor de Acceso OpenVPN de la Universidad Nacional de Loja (ver Figura 97).

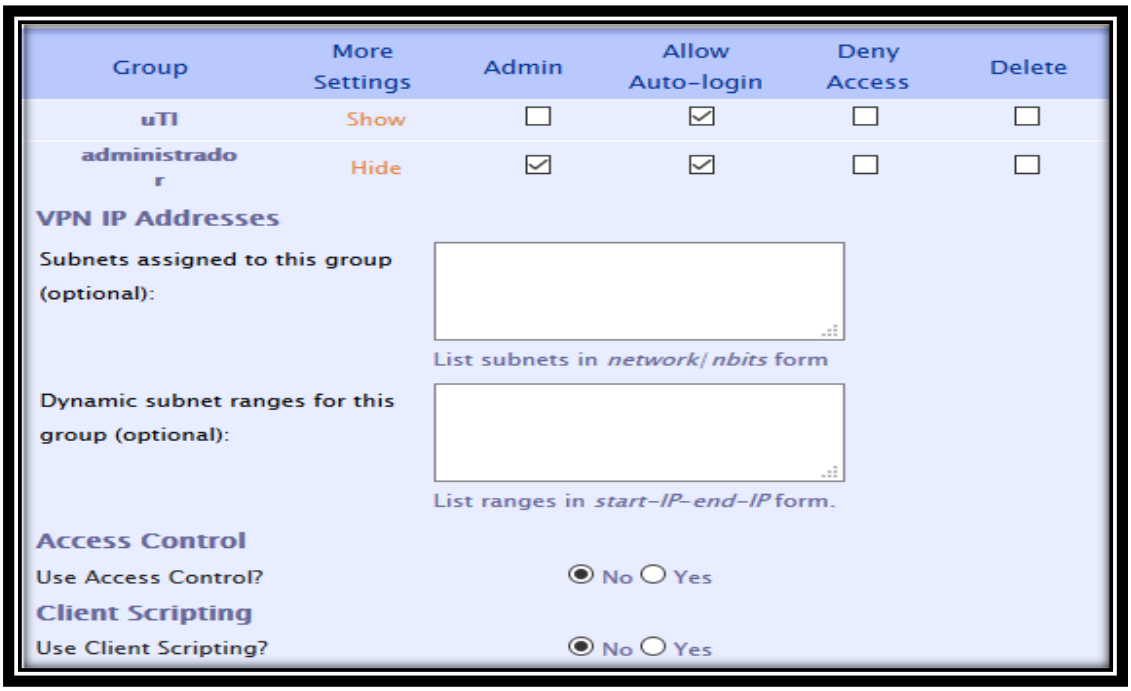


Figura 97: Configuración del Perfil de Usuario Administrador.

Fuente: Autor.

Una vez que se accedió a la página “Group Permissions”, se realizó clic en la opción “Show” del grupo “administrador” y se desplegó las opciones de configuración del grupo. Se accedió a la subsección “Admin” y se marcó la casilla. Esto se lo realizó para otorgar los privilegios como administrador del Servidor de Acceso OpenVPN.

Cabe mencionar que el grupo “administrador”, también posee el acceso a las bases de datos científicas de la institución, debido a la configuración de enrutamiento que se realizó en la Actividad 2 – Fase III de Resultados.

- **Grupo Docentes.**

El grupo “docentes” se creó para asignar a todos los docentes pertenecientes a la Universidad Nacional de Loja (ver Figura 98).

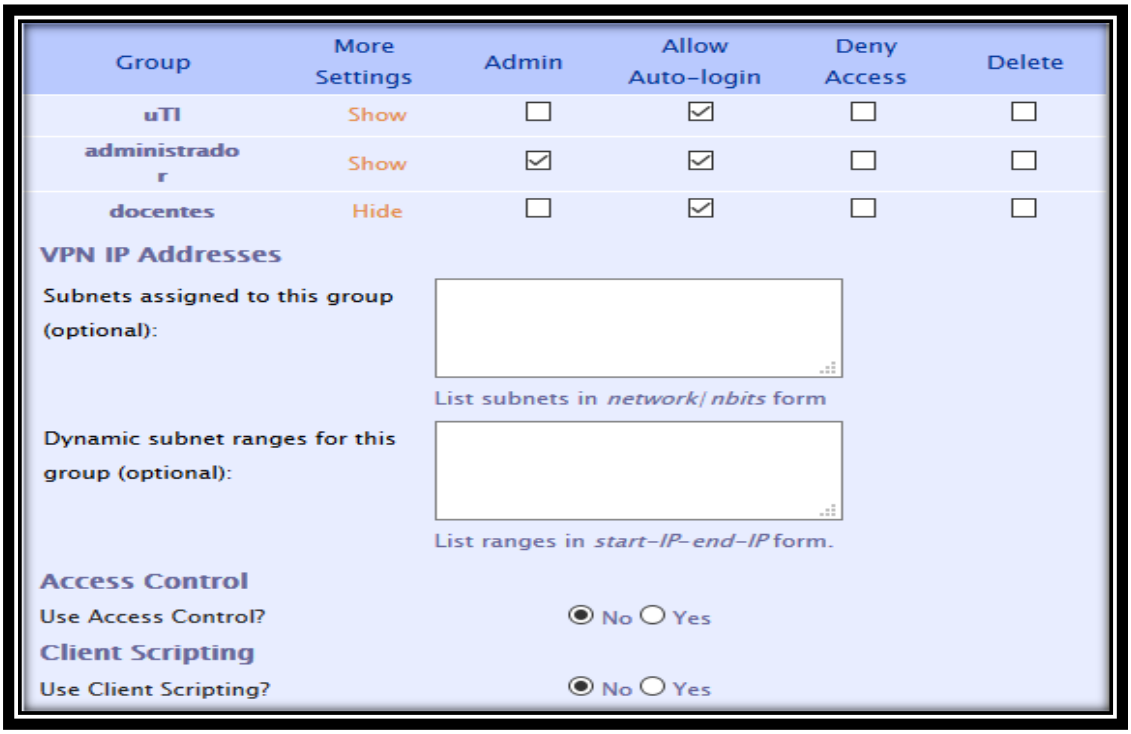


Figura 98: Configuración del Perfil de Usuario Docentes.

Fuente: Autor.

Una vez que se accedió a la página “Group Permissions”, se realizó clic en la opción “Show” del grupo “docentes” y se desplegó las opciones de configuración del grupo. En este caso no se asignó ningún privilegio de acceso a los docentes dentro del Servidor de Acceso OpenVPN.

Cabe mencionar que el grupo “docentes” posee el acceso a las bases de datos científicas de la Universidad Nacional de Loja, debido a la configuración de enrutamiento que se realizó en la Actividad 2 – Fase III de Resultados.

- **Grupo Estudiantes.**

El grupo “estudiantes” se creó para asignar a todos los estudiantes pertenecientes a la Universidad Nacional de Loja (ver Figura 99).

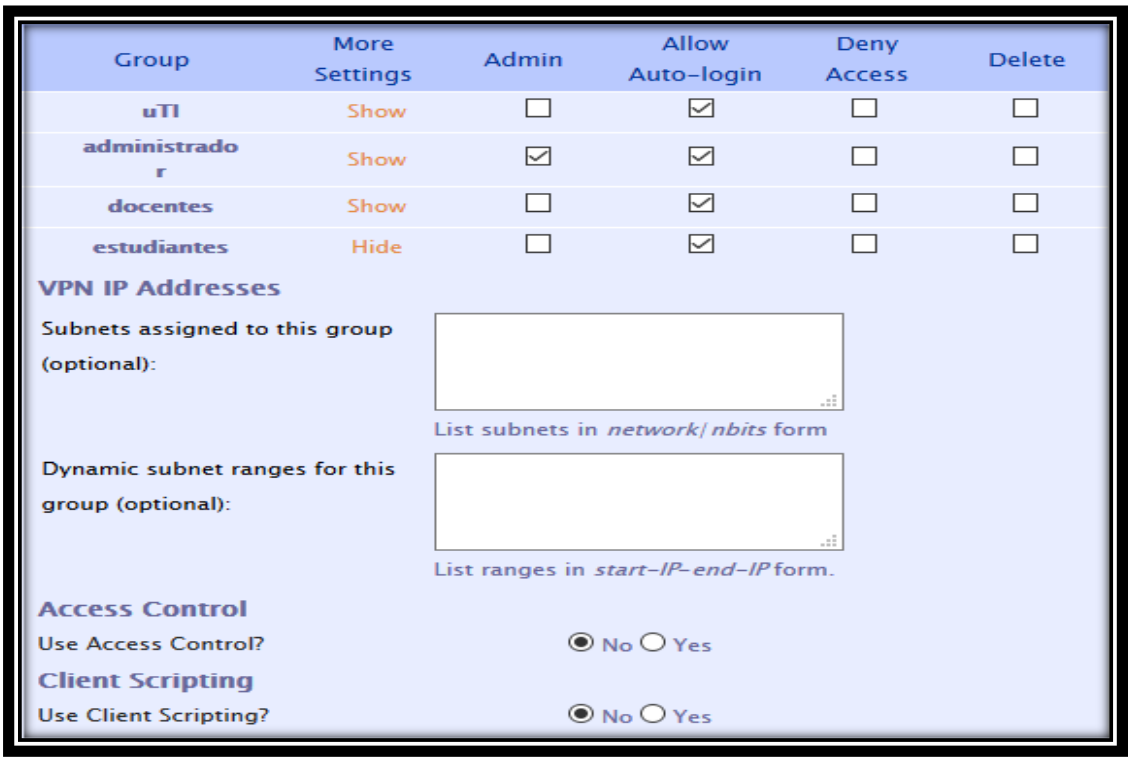


Figura 99: Configuración del Perfil de Usuario Estudiantes.

Fuente: Autor.

Una vez que se accedió a la página de gestión de usuarios “Group Permissions”, se realizó clic en la opción “Show” del grupo “estudiantes” y se desplegó las opciones de configuración del grupo. En este caso no se asignó ningún privilegio de acceso a los estudiantes dentro del Servidor de Acceso OpenVPN.

Cabe mencionar que el grupo “estudiantes” posee el privilegio de acceso a las bases de datos científicas de la Universidad Nacional de Loja, debido a la configuración de enrutamiento que se realizó en la Actividad 2 – Fase III de Resultados.

- **Grupo Administrativos.**

El grupo “administrativos” se creó para asignar a todo el personal administrativo de la Universidad Nacional de Loja; excepto al personal de la Unidad de Telecomunicaciones e Información (ver Figura 100).

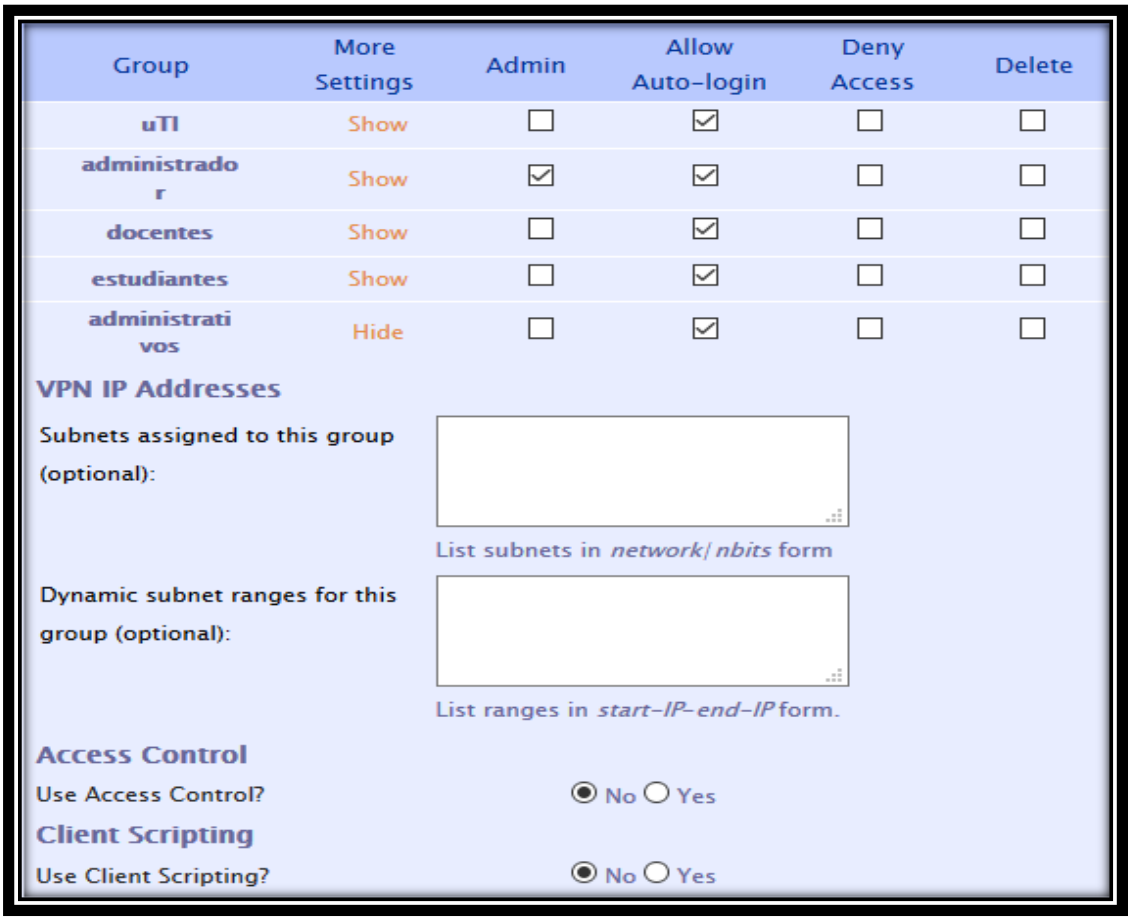


Figura 100: Configuración del Perfil de Usuario Administrativos.

Fuente: Autor.

Una vez que se accedió a la página “Group Permissions”, se realizó clic en la opción “Show” del grupo “administrativos” y se desplegó las opciones de configuración del grupo. En este caso no se asignó ningún privilegio de acceso al personal administrativo dentro del Servidor de Acceso OpenVPN.

Al igual que los otros grupos, el grupo “administrativos” posee el acceso a las bases de datos científicas de la Universidad Nacional de Loja, debido a la configuración de enrutamiento que se realizó en la Actividad 2 – Fase III de Resultados.

- **Grupo Srei.uti.**

El grupo “srei.uti” se creó para asignar a todo el personal de mantenimiento y redes de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja. Los privilegios de acceso que se le asignó a este grupo, se lo realizó a través de direccionamiento IP (ver Figura 101).

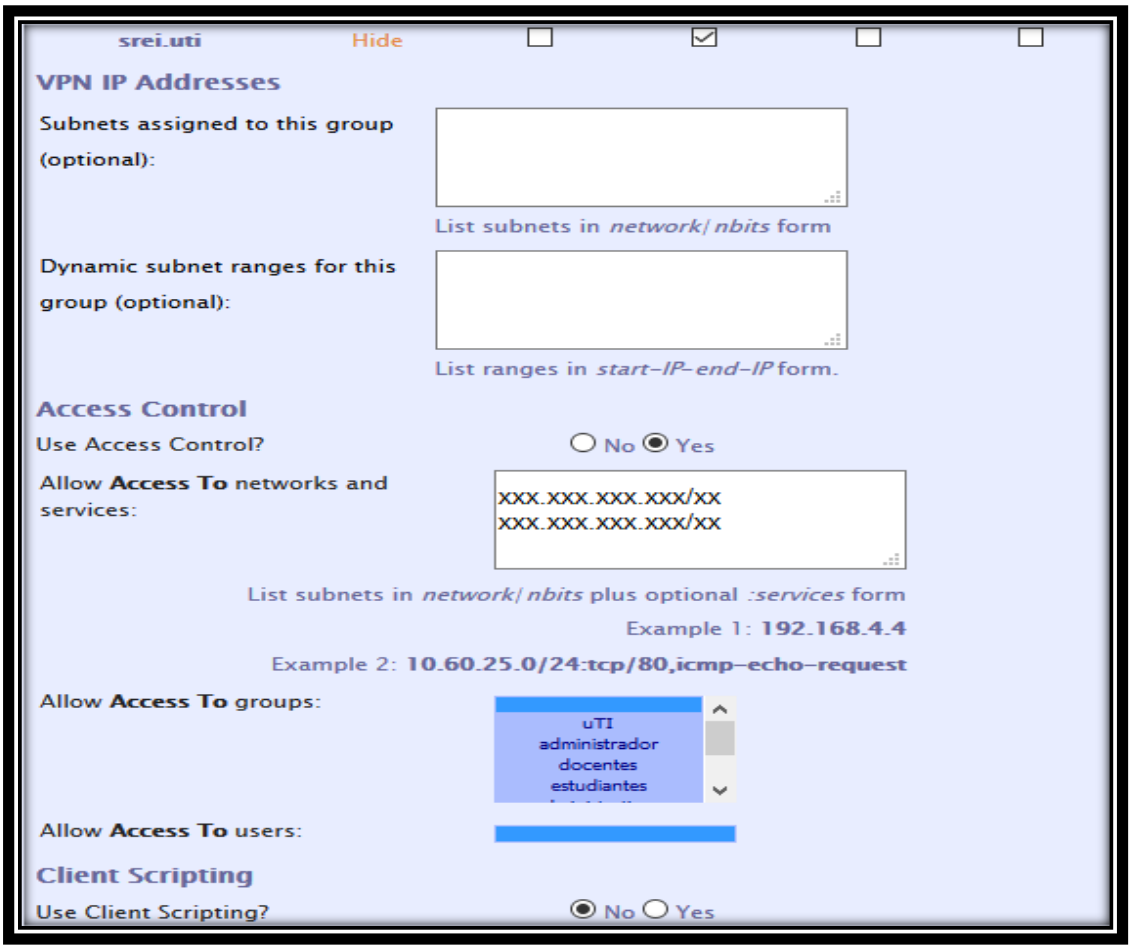


Figura 101: Configuración del Perfil de Usuario Srei.uti.

Fuente: Autor.

Una vez que se accedió a la página “Group Permissions”, se realizó clic en la opción “Show” del grupo “srei.uti” y se desplegó las opciones de configuración del grupo. Se accedió a la subsección “Access Control” y se seleccionó “Yes” para usar la opción de control de acceso. Luego de que se habilitó el control de acceso, en la opción “Allow Access To networks and services” se ingresó las subredes privadas adicionales a las que el grupo “srei.uti” va a tener los privilegios de acceso.

El grupo “srei.uti”, también posee el acceso a las bases de datos científicas de la institución, debido a la configuración de enrutamiento que se realizó en la Actividad 2 – Fase III de Resultados.

- **Grupo Sdsw.uti.**

El grupo “sdsw.uti” se creó para asignar a todo el personal de software de la Unidad de Telecomunicaciones e Información. Los privilegios de acceso que se le asignó a este grupo, se lo realizó a través de direccionamiento IP (ver Figura 102).

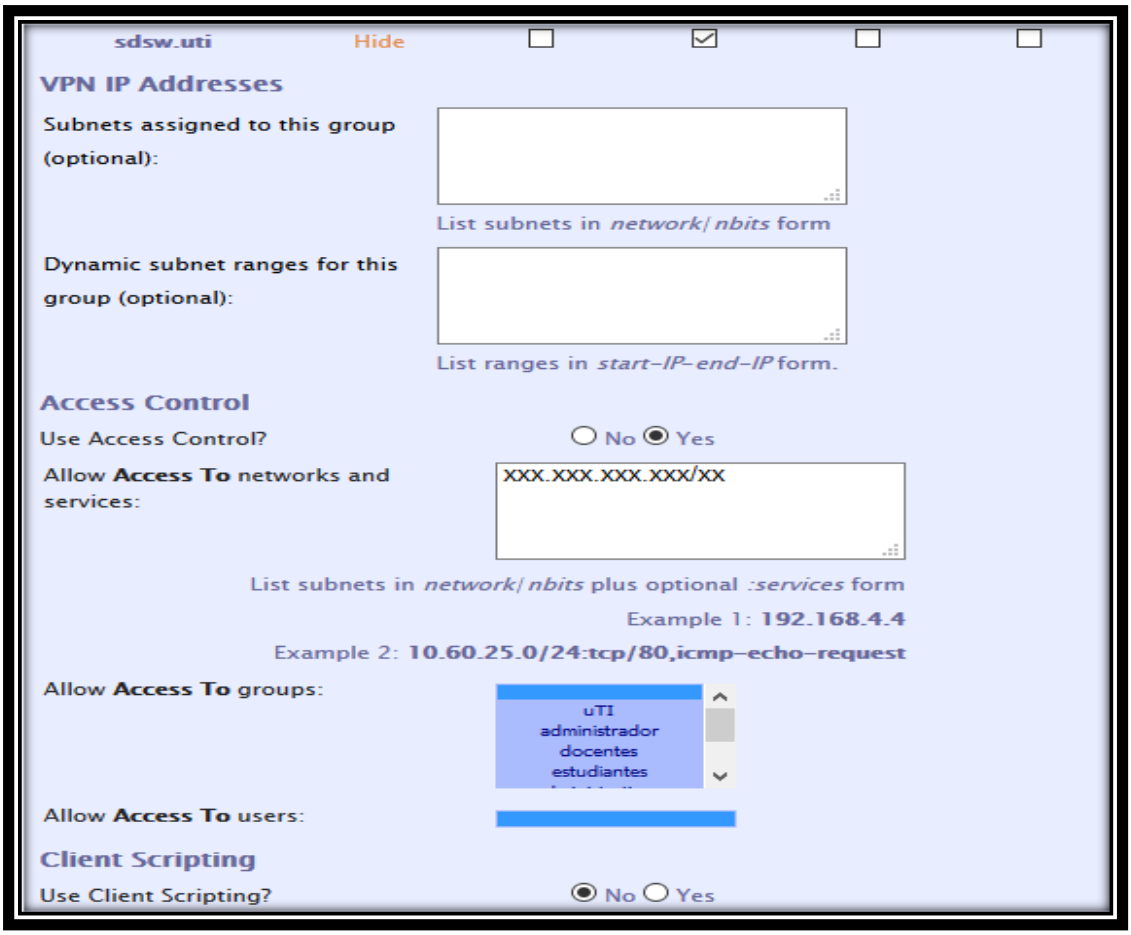


Figura 102: Configuración del Perfil de Usuario Sdsw.uti.

Fuente: Autor.

Una vez que se accedió a la página “Group Permissions”, se realizó clic en la opción “Show” del grupo “sdsw.uti” y se desplegó las opciones de configuración del grupo. Se accedió a la subsección “Access Control” y se seleccionó “Yes” para usar la opción de control de acceso.

Luego de que se habilitó el control de acceso, en la opción “Allow Access To networks and services” se ingresó las subredes privadas adicionales a las que el grupo “sdsw.uti” va a tener los privilegios de acceso.

Cabe mencionar que el grupo “sdsw.uti”, también cuenta con acceso a las bases de datos científicas de la institución, debido a la configuración de enrutamiento que se realizó en la Actividad 2 – Fase III de Resultados.

b) User Permissions (Permisos de Usuario).

Dentro de la sección “User Management” de la página de interfaz de usuario de administración web, se encuentra la página “User Permissions” (ver Figura 103).

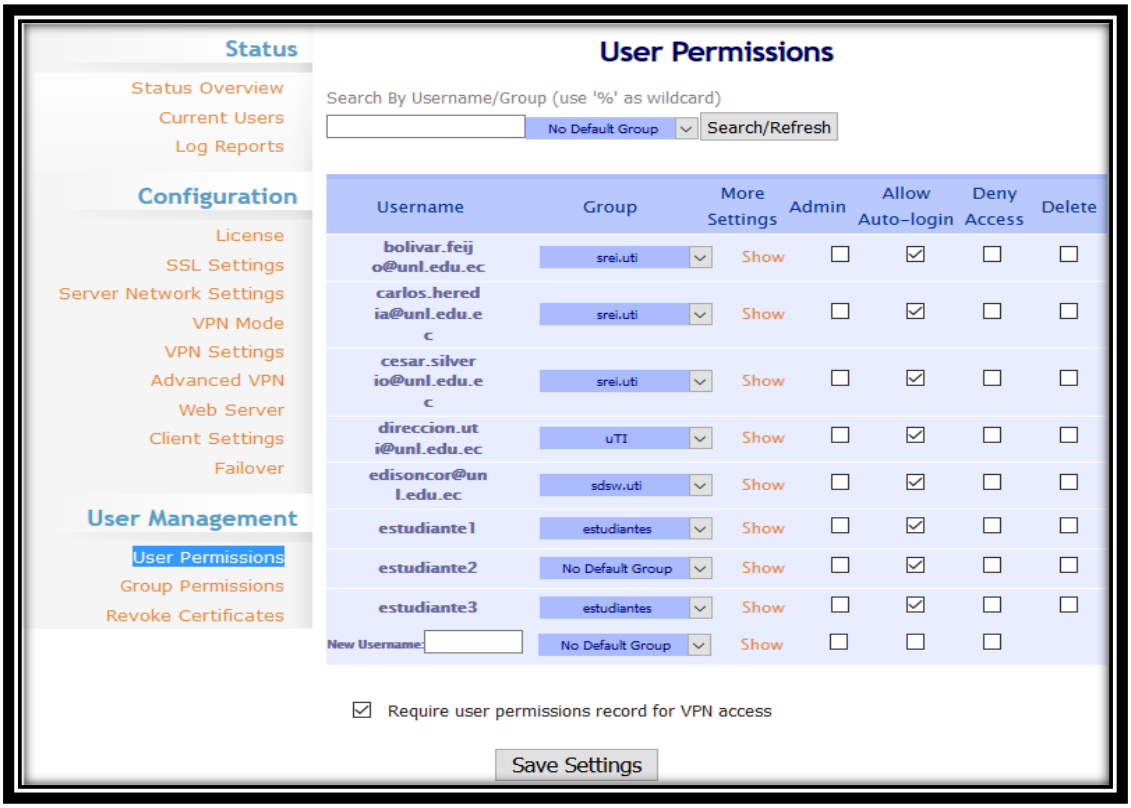


Figura 103: Configuración de la Página User Permissions.

Fuente: Autor.

Luego de que se ingresó a la página “User Permissions” se encuentran los usuarios creados en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja (ver Figura 104).

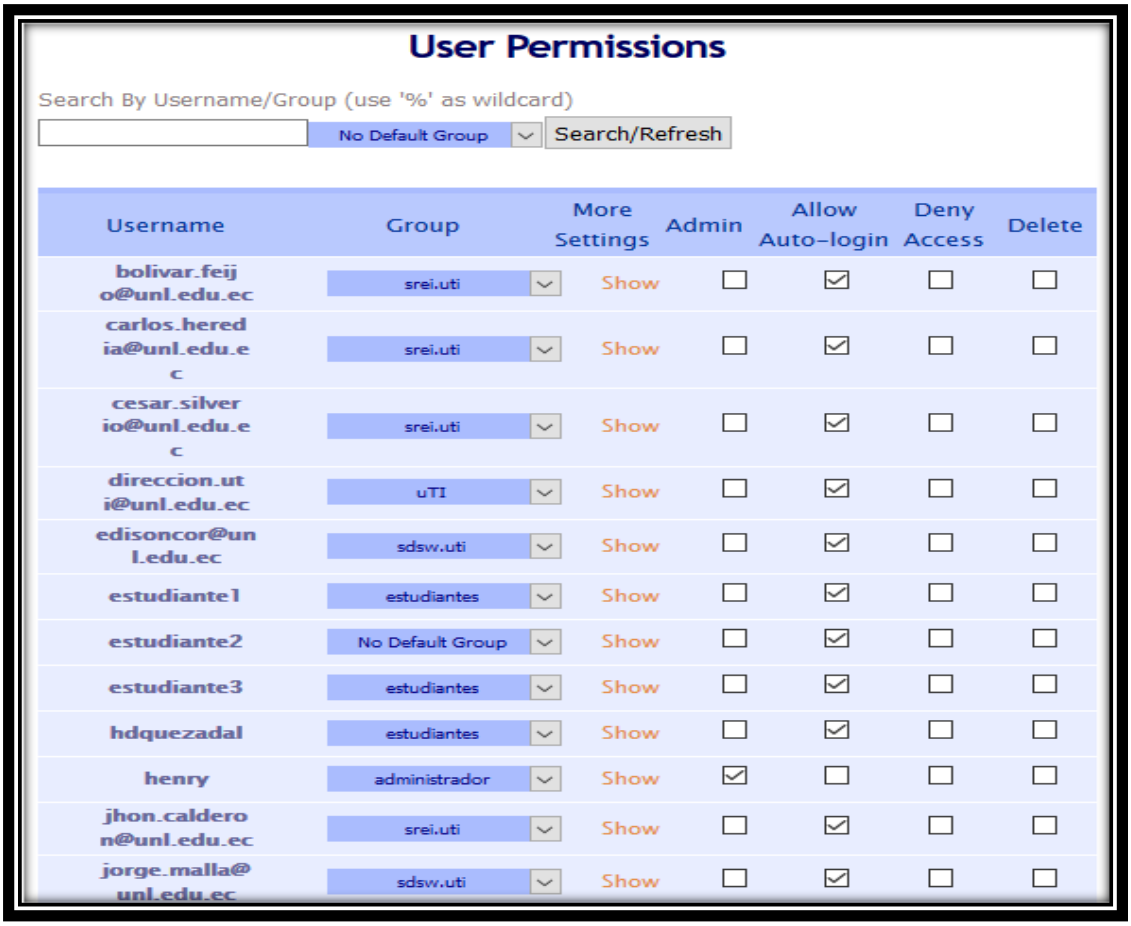


Figura 104: Usuarios Creados en el Servidor de Acceso OpenVPN.

Fuente: Autor.

Para crear un nuevo usuario en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se realizó clic en la opción “New Username” y se ingresó el nombre del usuario; en este caso se llamó “usuario”. Una vez que se ingresó el nombre del usuario, se realizó clic en la opción “Show” y se desplegó las opciones de configuración del usuario.

Luego de que se ingresó a la opción “show”, se seleccionó la opción “Auto-login” para que se establezcan las conexiones automáticamente al momento de conectarse con el Servidor de Acceso OpenVPN. Además, se encuentran disponibles las opciones “Admin” que permite dar privilegios de administrador al usuario VPN, “Deny Access” que permite denegar el acceso del usuario al Servidor OpenVPN y la opción “Delete” que permite eliminar el usuario que se creó.

Dentro de las opciones de configuración del usuario se accedió a la opción “Local Password” y se estableció su contraseña. Luego de que se le asignó la contraseña al nuevo usuario, se le asignó un grupo de usuario acorde a los privilegios de acceso que vaya a tener.

En la subsección “Access Control”, se seleccionó la opción “all server-side private Subnets” para permitir que el nuevo usuario tenga acceso a todas las subredes privadas que se configuró en el Servidor de Acceso OpenVPN (ver Figura 105).

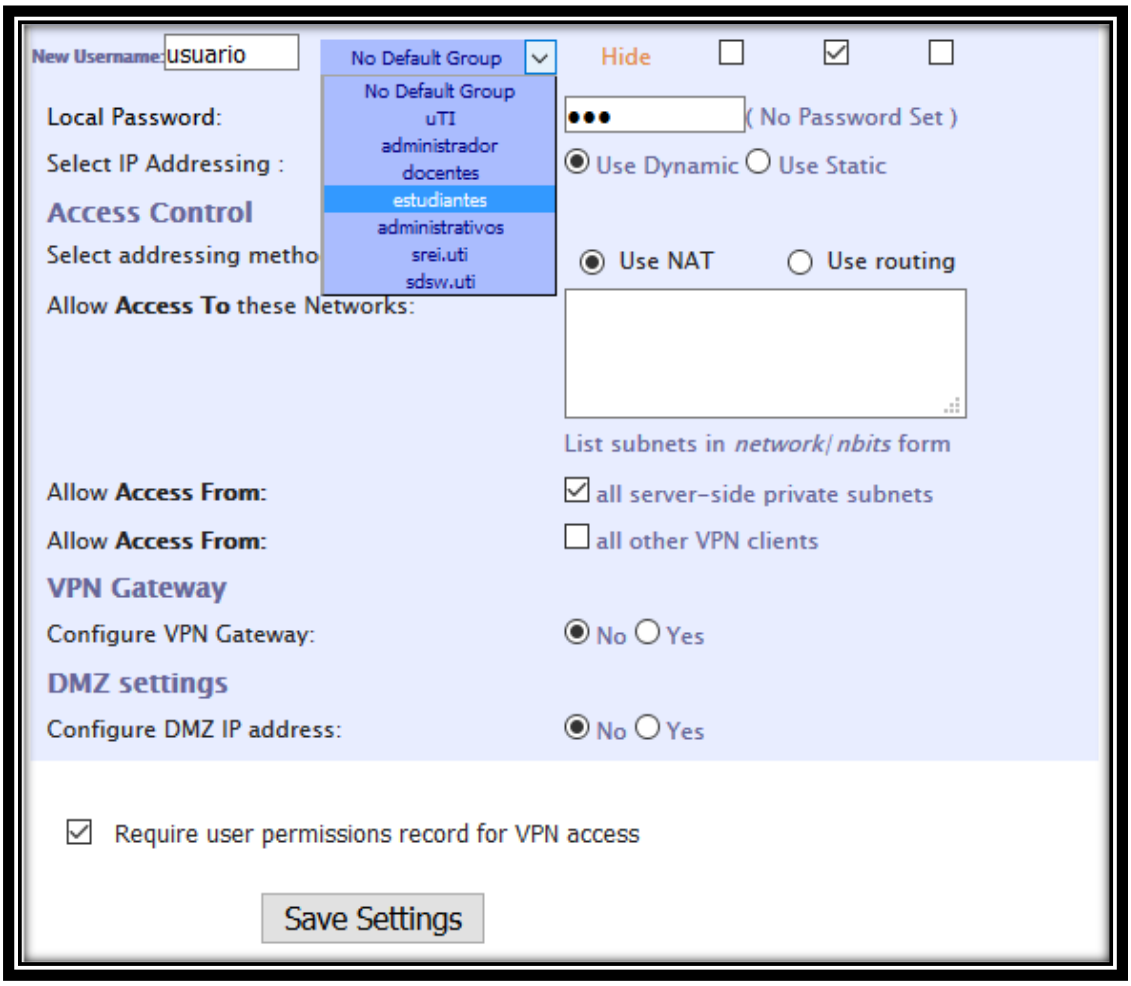


Figura 105: Creación de un Usuario en el Servidor de Acceso OpenVPN.

Fuente: Autor.

Una vez que se terminó con las configuraciones del nuevo usuario, se realizó clic en la opción “Save Settings” para guardar las configuraciones realizadas.

c) Revoke Certificates (Revocar Certificados).

Dentro de la sección “User Management” de la página de interfaz de usuario de administración web, se encuentra la página “Revoke Certificates” (ver Figura 106).

Figura 106: Revocar Certificados de Usuario en el Servidor de Acceso OpenVPN.
Fuente: Autor.

Una vez que se accedió a la página “Revoke Certificates”, se encuentra la subsección “Currently Issued VPN client Certificates”, la cual contiene todos los certificados de los clientes generados en el Servidor de Acceso OpenVPN. Para revocar el certificado de un cliente únicamente se selecciona el certificado y se realiza clic en la opción “Revoke”.

6.3.4. Actividad 4: Conexión de los clientes a la Red Privada Virtual.

En esta actividad se realizó la conexión de los clientes con el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja. Para realizar la conexión de los clientes a la VPN primeramente deberán estar registrados en el Servidor de Acceso OpenVPN.

6.3.4.1. Conexión de los Clientes en el Servidor de Acceso OpenVPN.

Para establecer la conexión de los clientes VPN con el Servidor de Acceso OpenVPN, se ingresó a la siguiente dirección URL: **https://openvpn.unl.edu.ec:943**

El acceso a la misma se lo realizó desde fuera de la red interna del campus universitario de la Universidad Nacional de Loja.

Luego de que se ingresó a la URL antes mencionada, el navegador web informó que la conexión no es segura, aun así se continuó. Esto se debe a que el certificado fue generado por el propio servidor al momento de la instalación. Se realizó clic en "Opciones Avanzadas" y se presentó el detalle del mensaje de aviso (ver Figura 107).

Figura 107: Mensaje de Conexión Insegura del Servidor.

Fuente: Autor.

Una vez que se realizó clic en la opción “Opciones avanzadas”, se presentó el detalle del mensaje y se hizo clic en la opción “Acceder a openvpn.unl.edu.ec (sitio no seguro)” (ver Figura 108).

Figura 108: Añadir Excepción de Seguridad para la conexión con el Servidor.

Fuente: Autor.

Luego de que se realizó clic en la opción “Acceder a openvpn.unl.edu.ec (sitio no seguro)”, se presentó la página de inicio de sesión para los usuarios de la VPN (ver Figura 109).

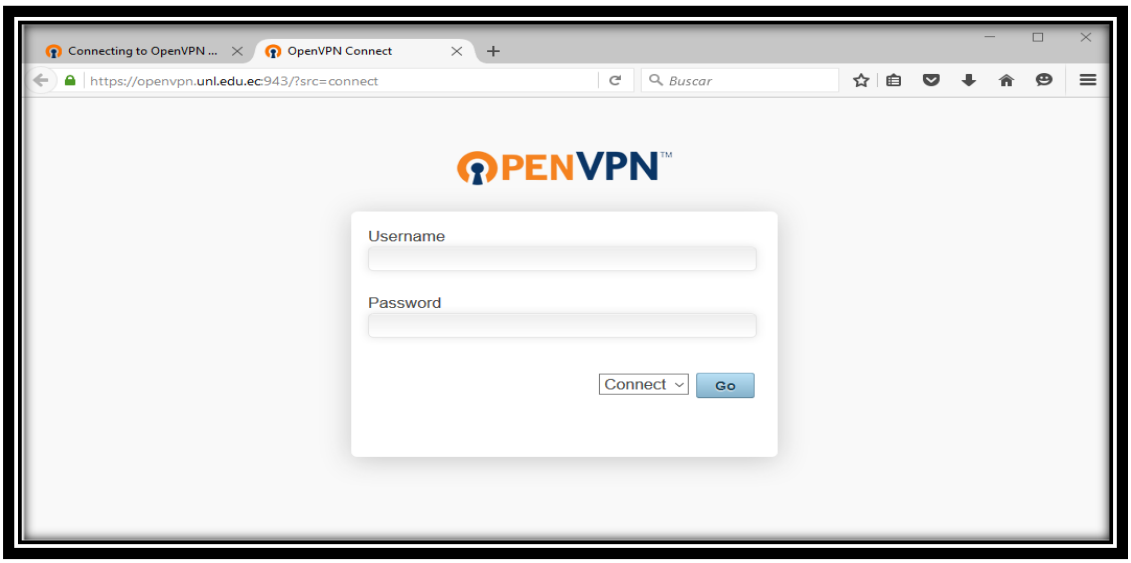


Figura 109: Página de Inicio de Sesión del Cliente VPN.

Fuente: Autor.

Una vez que se accedió a la página de inicio de sesión de los clientes VPN en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se ingresó el “Username” y “Password” del cliente VPN registrado. Después de que se ingresó el usuario y la contraseña, se realizó clic en la opción “Go” (ver Figura 110).

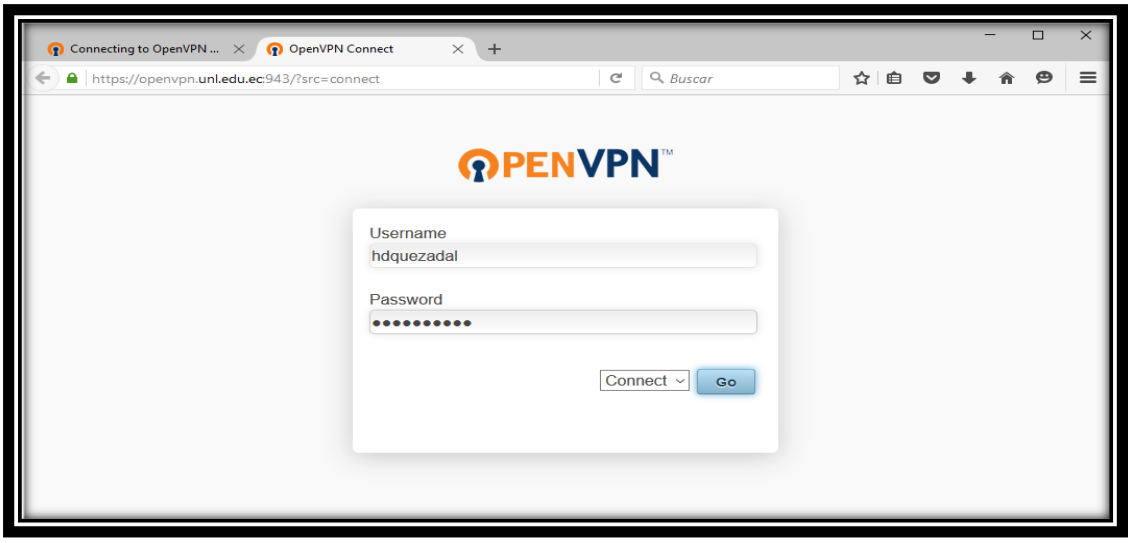


Figura 110: Autenticación del Cliente VPN en el Servidor de Acceso OpenVPN.

Fuente: Autor.

Luego de que se realizó clic en la opción “Go”, se muestran los diferentes clientes OpenVPN que se pueden elegir dependiendo del sistema operativo que se esté utilizando (ver Figura 111).

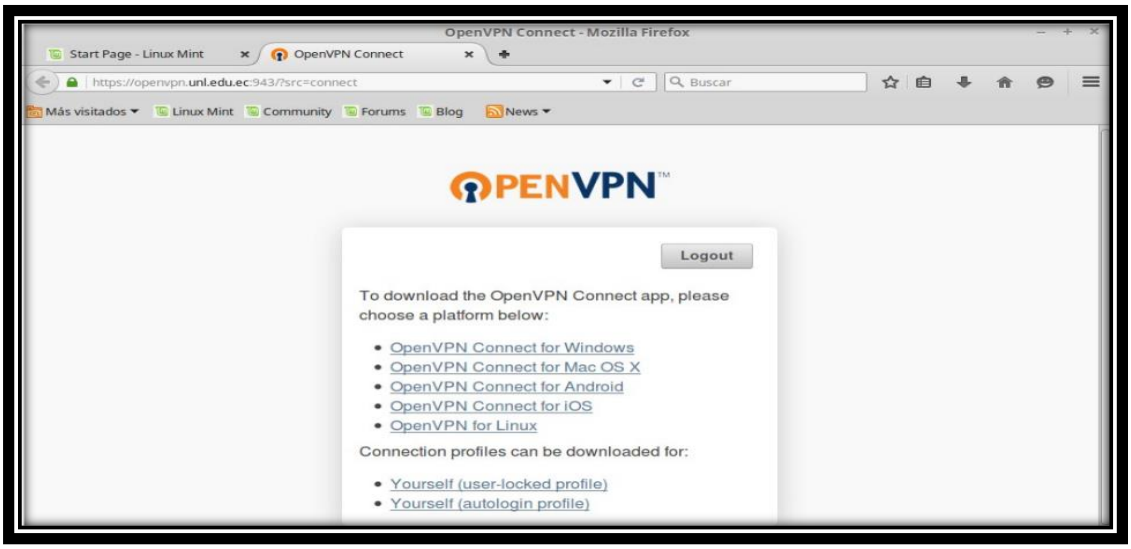


Figura 111: Página de selección de los diversos Clientes OpenVPN.

Fuente: Autor.

Una vez que se seleccionó el cliente OpenVPN (en este caso Windows), se realizó clic sobre la opción “OpenVPN Connect for Windows” y apareció un archivo ejecutable, al cual se realizó clic en la opción “Guardar archivo” (ver Figura 112).

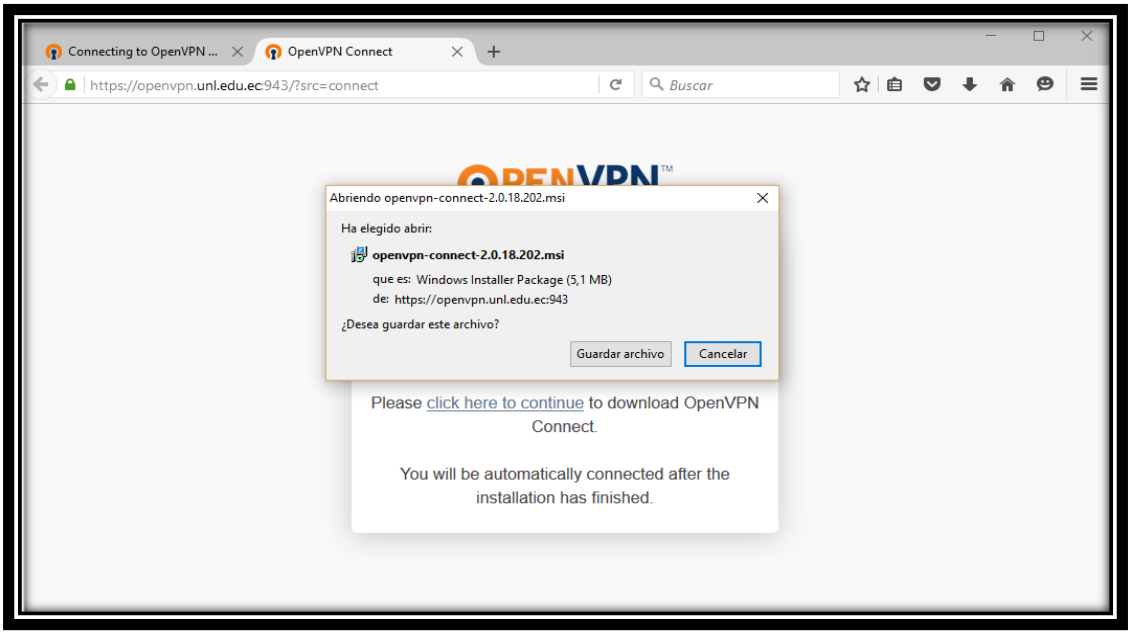


Figura 112: Selección y Descarga del Cliente OpenVPN para Windows.

Fuente: Autor.

Después de que se realizó clic en la opción “Guardar archivo”. El archivo ejecutable se comenzó a descargar y posteriormente se lo ejecutó (ver Figura 113).

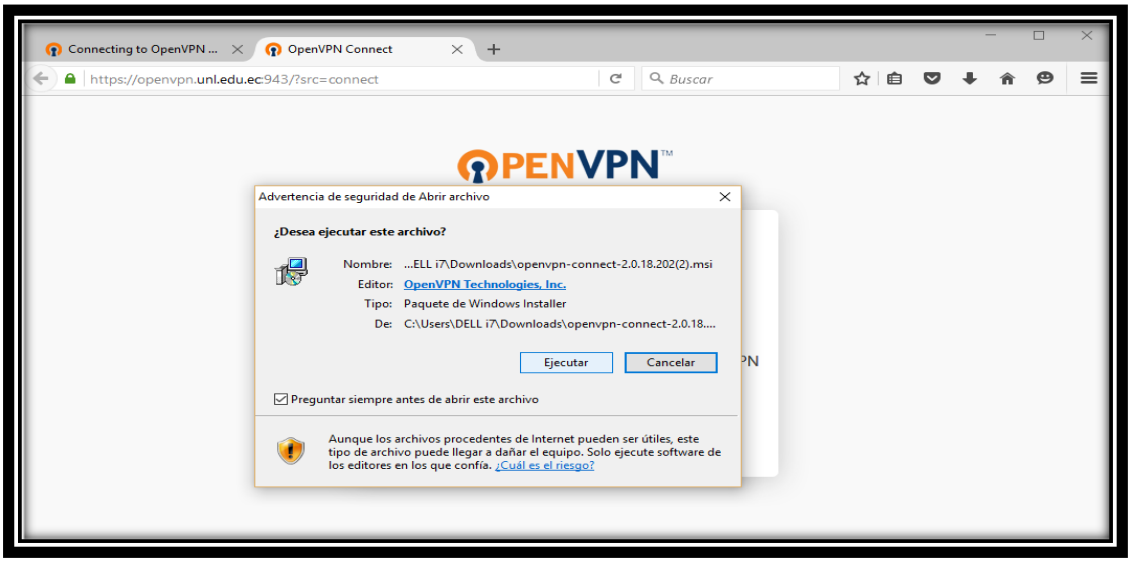


Figura 113: Ejecutar Archivo OpenVPN para el Cliente Windows.

Fuente: Autor.

Una vez que se ejecutó el archivo ejecutable, se instaló el cliente “OpenVPN Connect” y se ubicó en la parte inferior de la barra de tareas. Luego de que se instaló el cliente OpenVPN, se realizó clic sobre el icono del mismo y se seleccionó la opción “Connect to openvpn.unl.edu.ec” (ver Figura 114).

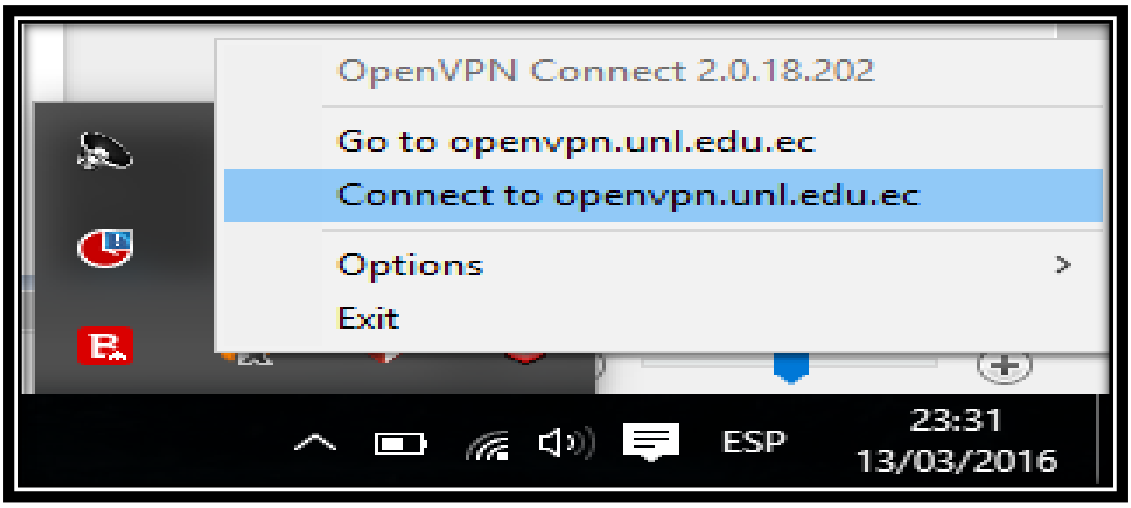


Figura 114: Cliente OpenVPN Instalado en el Sistema Operativo Windows.

Fuente: Autor.

Después de que se seleccionó la opción “Connect to openvpn.unl.edu.ec”, que es la dirección del Servidor de Acceso OpenVPN, la conexión se estableció y la VPN comenzó con su funcionamiento (ver Figura 115).

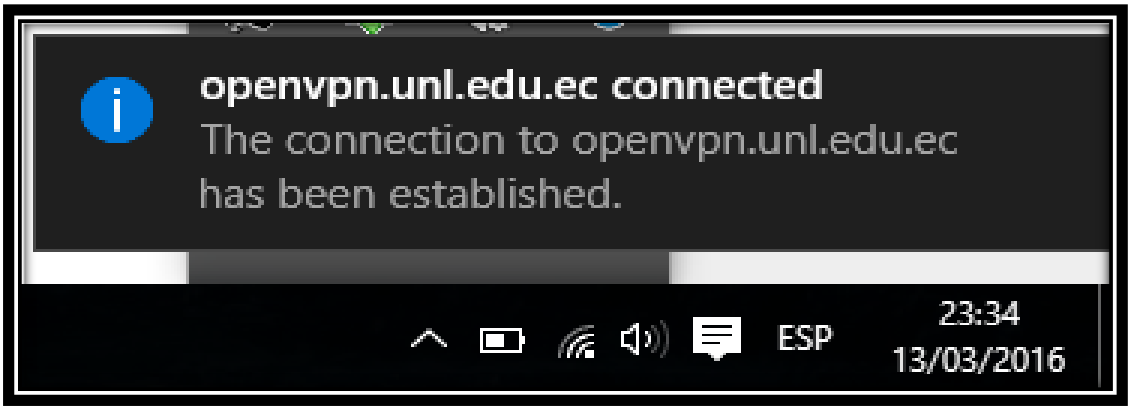


Figura 115: Conexión Establecida del Cliente OpenVPN en Windows.

Fuente: Autor.

Luego de que se utilizó el servicio de la VPN, se cerró la conexión con el Servidor de Acceso OpenVPN. Para ello se seleccionó el icono de OpenVPN que se encuentra en

la parte inferior de la barra de tareas. Una vez que se seleccionó el icono de OpenVPN, se realizó clic izquierdo sobre el mismo y se seleccionó la opción “Disconnect openvpn.unl.edu.ec” (ver Figura 116).

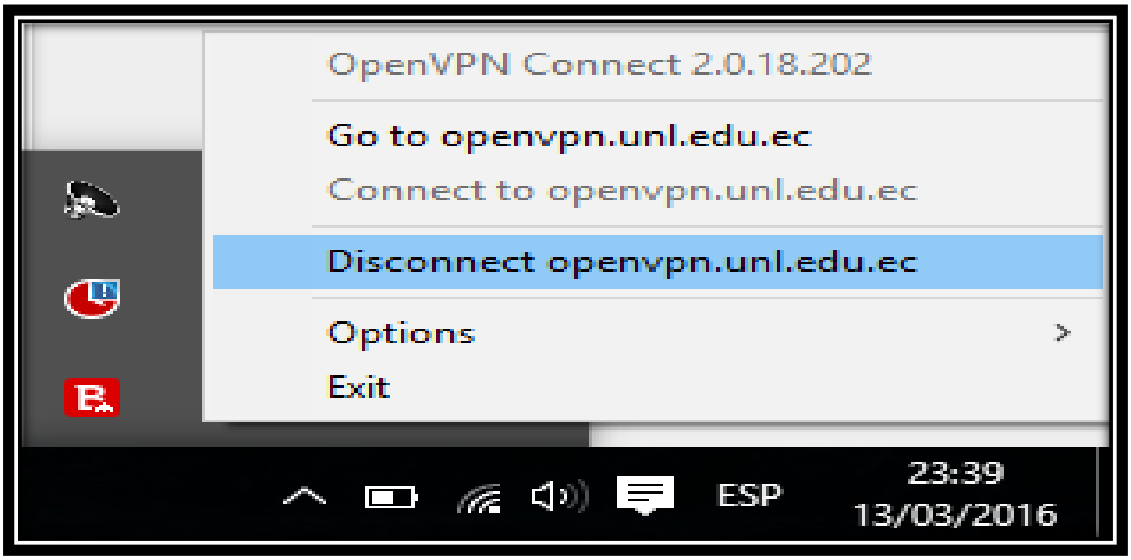


Figura 116: Desconectar Servicio VPN en Windows.

Fuente: Autor.

Después de que se seleccionó la opción “Disconnect openvpn.unl.edu.ec” que es la dirección del Servidor de Acceso OpenVPN, la conexión con el Servidor OpenVPN de la Universidad Nacional de Loja se desconectó (ver Figura 117).

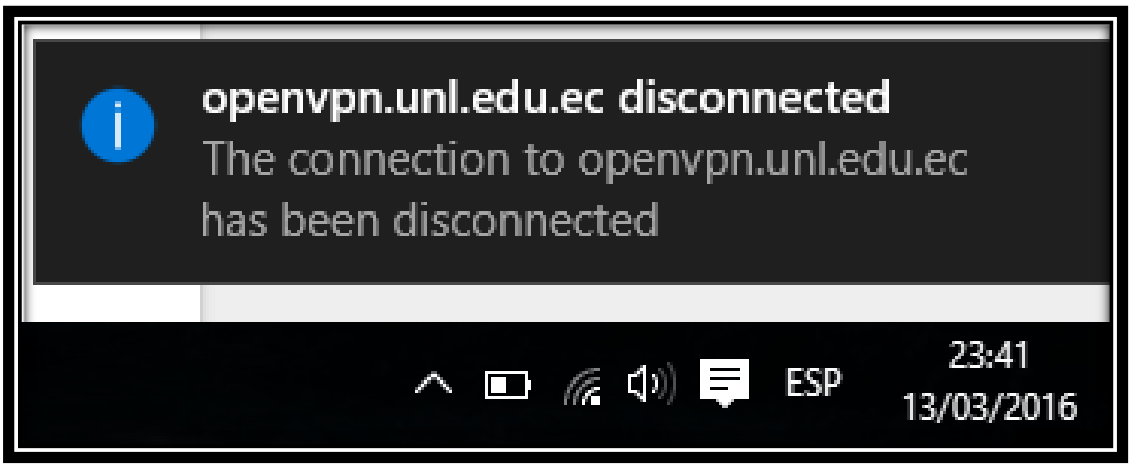


Figura 117: Conexión VPN Desconectada en Windows.

Fuente: Autor.

6.4. FASE IV: Aplicar pruebas para evaluar el correcto funcionamiento del escenario de la VPN.

En esta fase se realizó las pruebas para evaluar el correcto funcionamiento del escenario de la Red Privada Virtual que se creó en la Universidad Nacional de Loja.

A continuación se detallan cada una de las actividades que se llevó a cabo para el cumplimiento de este objetivo.

6.4.1. Actividad 1: Pruebas de Conectividad.

En esta actividad se realizó las pruebas de conectividad entre el cliente VPN y el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja. Para ello se realizó dos pruebas, la primera prueba se la realizó para comprobar la conectividad desde el cliente VPN hacia el Servidor de Acceso OpenVPN y la segunda prueba se la realizó desde el Servidor de Acceso OpenVPN hacia el cliente VPN.

6.4.1.1. Prueba de Conectividad desde el Cliente VPN hacia el Servidor de Acceso OpenVPN.

En esta prueba se realizó la comprobación de conectividad del cliente VPN hacia el Servidor de Acceso OpenVPN. Para ello, primeramente se estableció la conexión del cliente con el Servidor OpenVPN de la Universidad Nacional de Loja (ver Figura 118).

Figura 118: Conexión al Servidor de Acceso OpenVPN.

Fuente: Autor.

Una vez que se realizó la conexión del cliente al Servidor de Acceso OpenVPN, se ingresó a “Símbolo del Sistema” y se realizó “ping” a la dirección privada del Servidor OpenVPN de la Universidad Nacional de Loja (ver Figura 119).

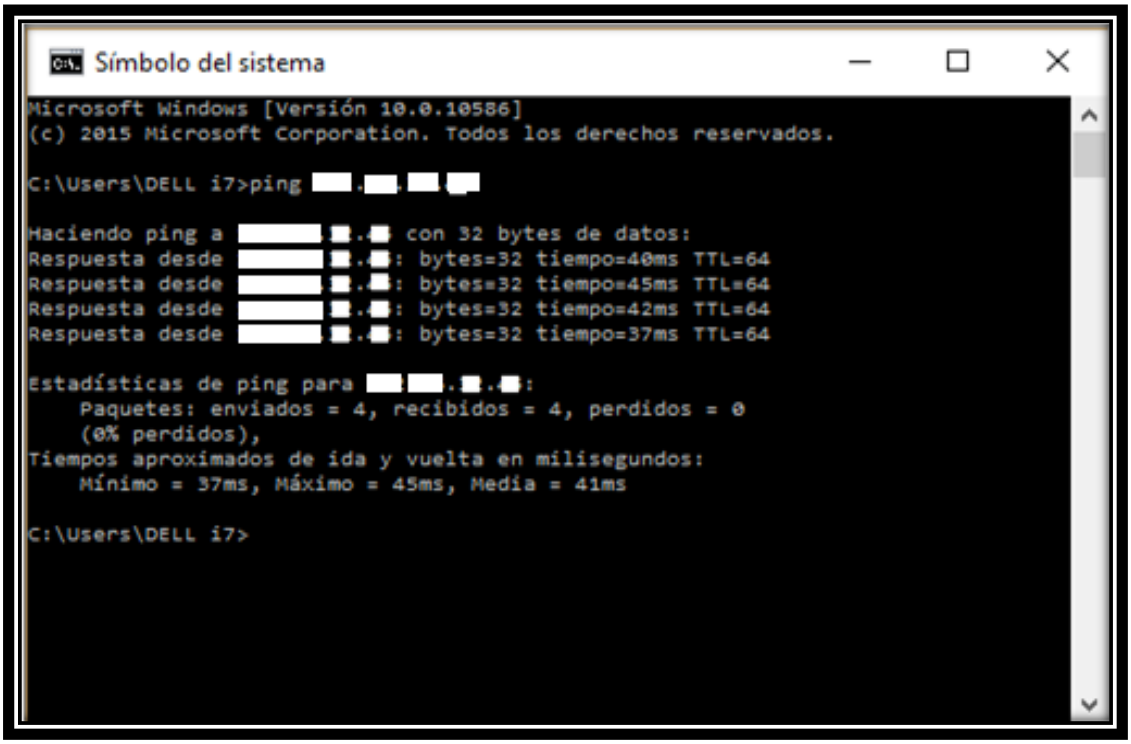


Figura 119: Realización de Ping al Servidor de Acceso OpenVPN.

Fuente: Autor.

Luego de que se realizó “ping” a la dirección privada del Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se evidenció que la conectividad fue exitosa.

6.4.1.2. Prueba de Conectividad desde el Servidor de Acceso OpenVPN hacia el Cliente VPN.

Para comprobar la conectividad desde el Servidor de Acceso OpenVPN hacia el cliente VPN, primeramente se necesitó que el cliente VPN se encuentre conectado al Servidor de Acceso OpenVPN (ver Figura 118). Luego de que se verificó que el cliente VPN se encuentra conectado al Servidor OpenVPN, se realizó un “ipconfig**”** para verificar la dirección IP que el Servidor de Acceso OpenVPN le asignó al cliente (ver Figura 120).

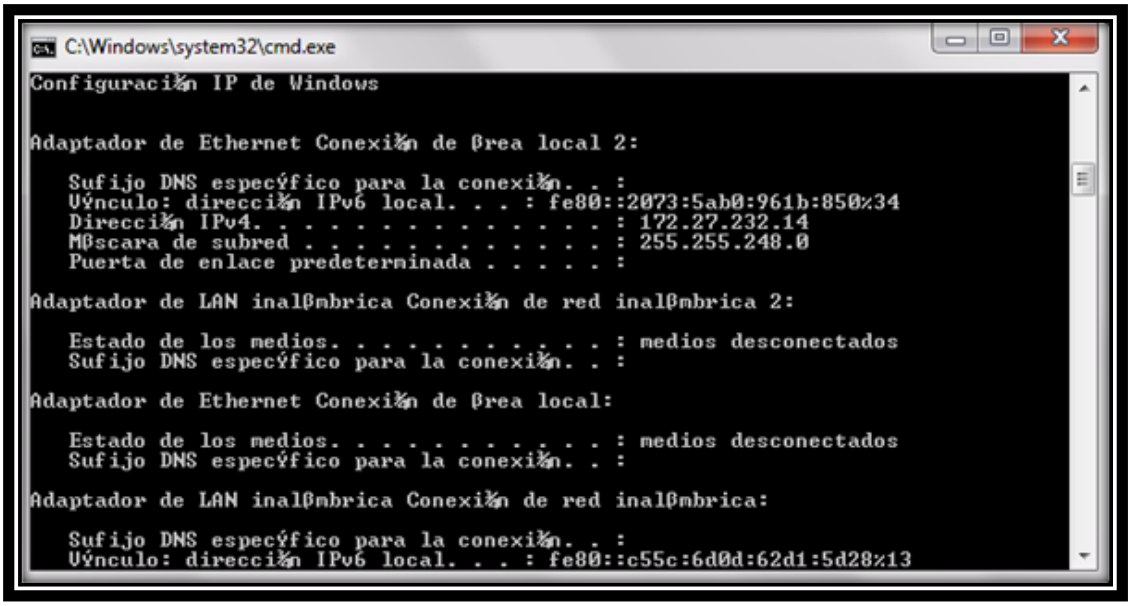


Figura 120: Asignación IP al Cliente VPN por parte del Servidor de Acceso OpenVPN.

Fuente: Autor.

La dirección IP que el Servidor de Acceso OpenVPN le asignó al cliente fue la 172.27.232.14. Una vez que se conoció la dirección IP asignada al cliente VPN, se realizó "ping" desde el Servidor de Acceso OpenVPN hacia la dirección IP del cliente VPN (ver Figura 121).

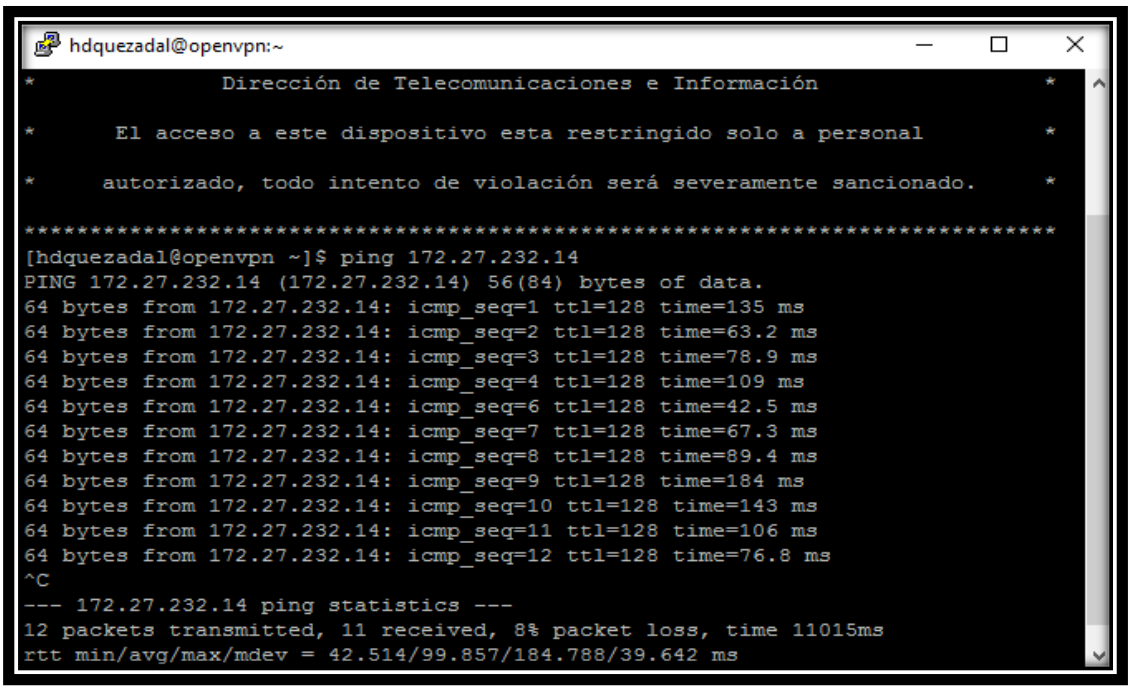


Figura 121: Realización de Ping al Cliente VPN desde el Servidor de Acceso OpenVPN.

Fuente: Autor.

Luego de que se realizó “ping” a la dirección IP del cliente VPN, se evidenció que la conectividad fue exitosa.

- **Resultados de las Pruebas de Conectividad.**

Una vez que se finalizó las pruebas de conectividad entre el cliente VPN y el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se constató que existe una conexión exitosa desde el cliente VPN hacia el Servidor de Acceso OpenVPN y desde el Servidor de Acceso OpenVPN hacia el cliente VPN.

6.4.2. Actividad 2: Pruebas de Conexión.

En esta actividad se realizó las pruebas de conexión a las bases de datos científicas de la Universidad Nacional de Loja, mediante el acceso a la Red Privada Virtual que se creó en la fase anterior (ver Fase III de Resultados).

Estas pruebas consistieron en acceder a las bases de datos científicas de la Universidad Nacional de Loja mediante la conexión a la Red Privada Virtual de la institución. Para ello se seleccionó dos pruebas, la primera prueba se realizó para acceder a las bases de datos científicas de la UNL desde un cliente VPN Windows y la segunda prueba se realizó para acceder a las bases de datos científicas de la UNL desde un cliente VPN Android.

6.4.2.1. Prueba de Conexión desde un Cliente VPN Windows.

Para acceder a las bases de datos científicas de la Universidad Nacional de Loja desde un cliente VPN Windows, primeramente se ingresó a la siguiente dirección URL: **https://openvpn.unl.edu.ec:943**

El acceso a la misma se lo realizó desde fuera de la red interna del campus universitario de la Universidad Nacional de Loja.

Luego de que se ingresó a la URL antes mencionada, el navegador web informó que la conexión no es segura. Esto se debe a que el certificado fue generado por el propio

servidor al momento de la instalación. Se realizó clic en "Opciones Avanzadas" y se presentó el detalle del mensaje de aviso (ver Figura 122).

Figura 122: Presentación del Mensaje de Conexión Insegura del Servidor OpenVPN.

Fuente: Autor.

Una vez que se realizó clic en “Opciones avanzadas” y se presentó el detalle del mensaje de aviso, se hizo clic en la opción “Acceder a openvpn.unl.edu.ec (sitio no seguro)” (ver Figura 123).

Figura 123: Añadir Excepción para el Certificado del Servidor de Acceso OpenVPN.

Fuente: Autor.

Luego de que se realizó clic en la opción “Acceder a openvpn.unl.edu.ec (sitio no seguro)”, se presentó la página de inicio de sesión para los clientes del Servidor de Acceso OpenVPN (ver Figura 124).

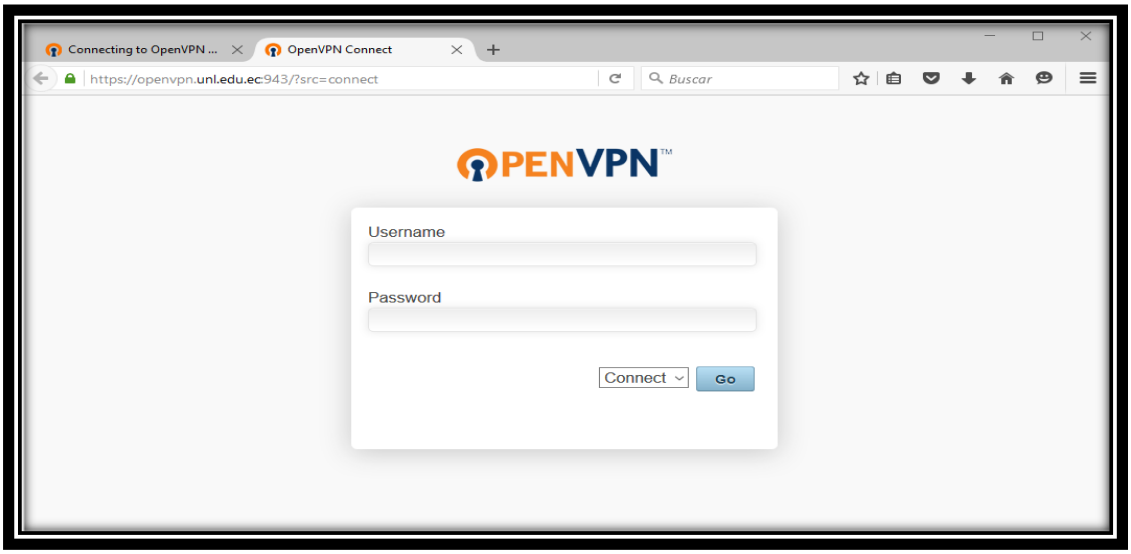


Figura 124: Página de Inicio de Sesión para los Clientes VPN.

Fuente: Autor.

Una vez que se accedió a la página de inicio de sesión de los clientes VPN en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se ingresó el “Username” y “Password” del cliente VPN registrado. Después de que se ingresó el usuario y la contraseña, se realizó clic en la opción “Go” (ver Figura 125).

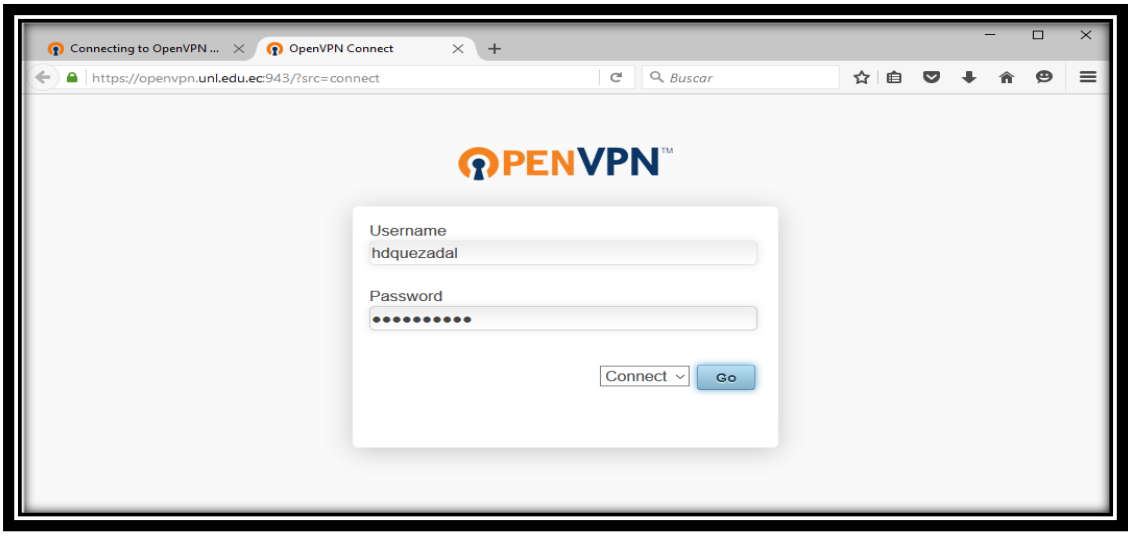


Figura 125: Autenticación del Cliente VPN dentro del Servidor de Acceso OpenVPN.

Fuente: Autor.

Luego de que se realizó clic en la opción “Go”, se muestran los diferentes clientes OpenVPN que se pueden elegir dependiendo del sistema operativo que se esté utilizando (ver Figura 126).

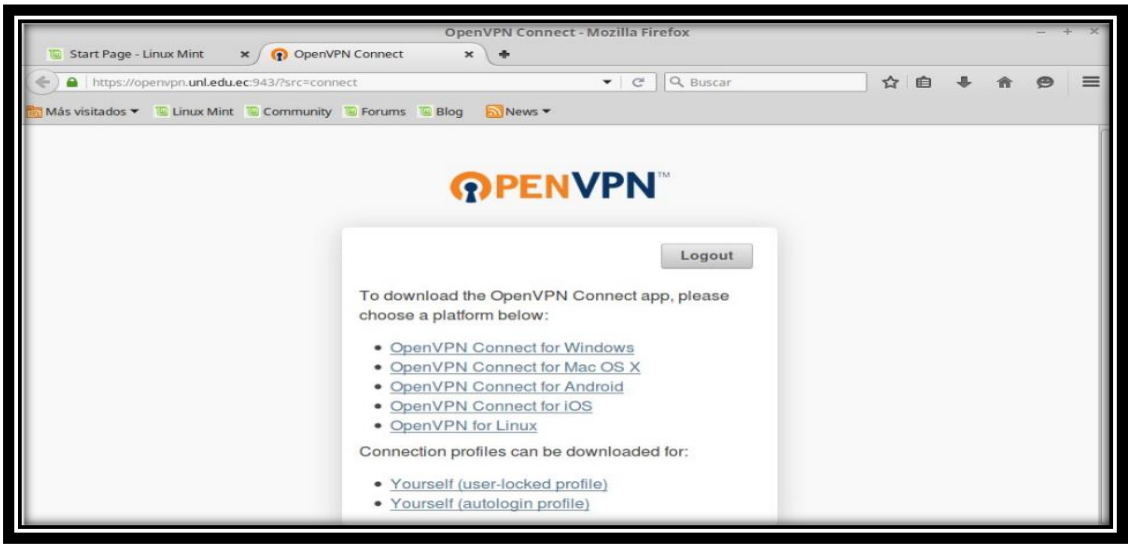


Figura 126: Página de selección de los Clientes OpenVPN.

Fuente: Autor.

Una vez que se seleccionó el cliente OpenVPN (en este caso Windows), se realizó clic sobre la opción “OpenVPN Connect for Windows” y apareció un archivo ejecutable, en el cual se realizó clic sobre la opción “Guardar archivo” (ver Figura 127).

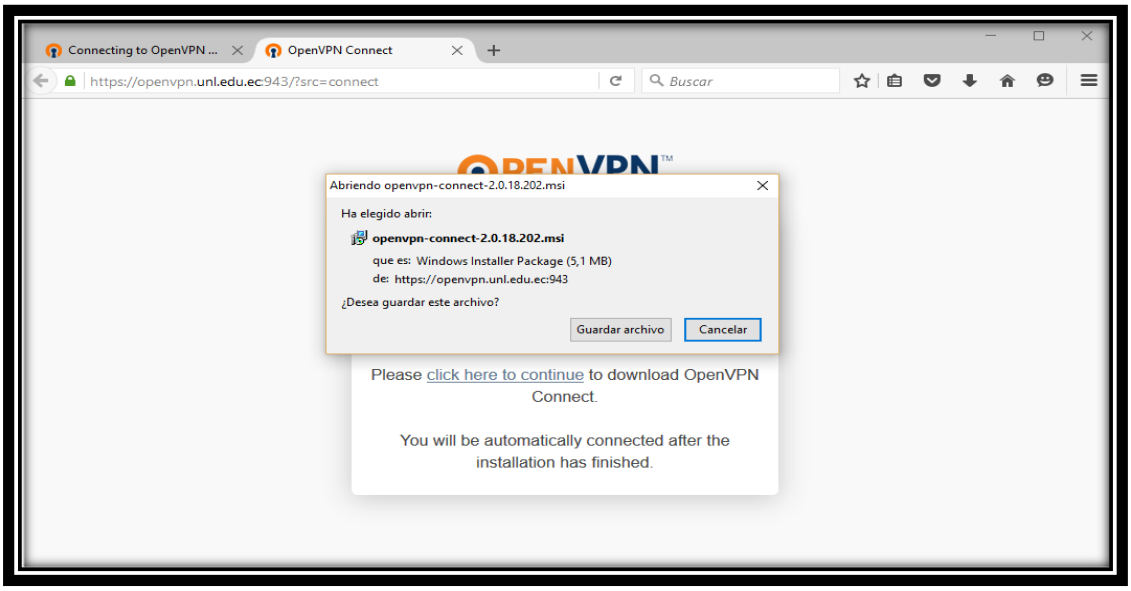


Figura 127: Archivo Ejecutable del Cliente OpenVPN para Windows.

Fuente: Autor.

Después de que se realizó clic en la opción “Guardar archivo”. El archivo ejecutable se comenzó a descargar y posteriormente se lo ejecutó (ver Figura 128).

Figura 128: Ejecutar Cliente OpenVPN para Windows.

Fuente: Autor.

Una vez que se ejecutó el archivo, se instaló el cliente “OpenVPN Connect” y se ubicó en la parte inferior de la barra de tareas. Luego de que se instaló el cliente "OpenVPN Connect”, se realizó clic sobre el icono del mismo y se seleccionó la opción “Connect to openvpn.unl.edu.ec” (ver Figura 129).

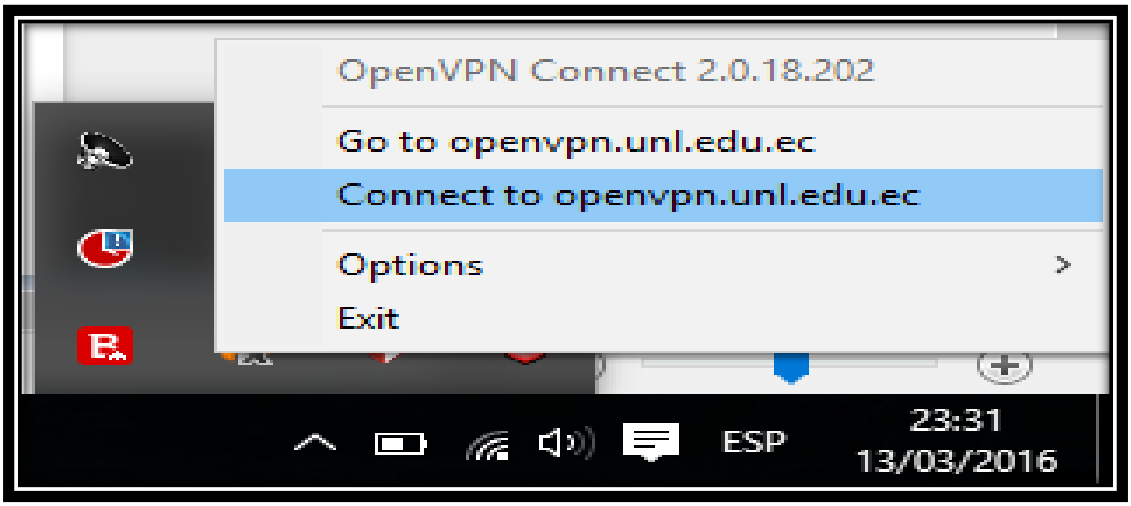


Figura 129: Conectarse al Servidor de Acceso OpenVPN.

Fuente: Autor.

Después de que se seleccionó la opción “Connect to openvpn.unl.edu.ec”, que es la dirección del Servidor de Acceso OpenVPN. Se estableció la conexión y la VPN comenzó a funcionar (ver Figura 130).

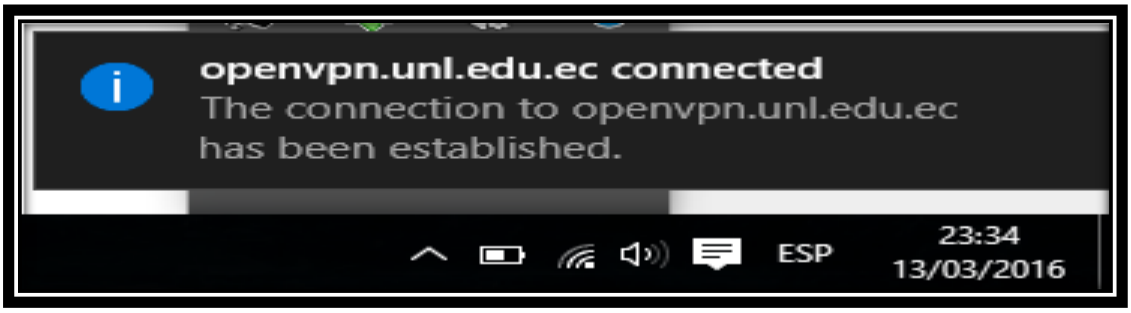


Figura 130: Conexión del Cliente OpenVPN en Windows.

Fuente: Autor.

Una vez que se estableció la conexión con el Servidor de Acceso OpenVPN, se abrió un navegador web y en la barra de navegación se ingresó la dirección de la Página de la Universidad Nacional de Loja, URL: https://unl.edu.ec (ver Figura 131).

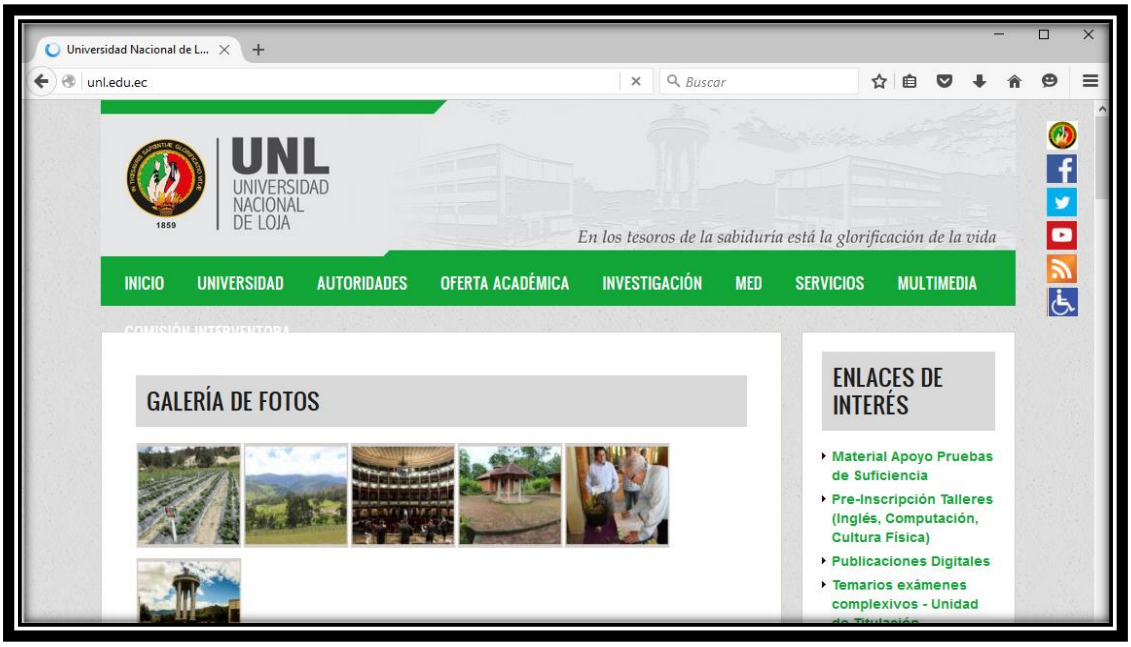


Figura 131: Conexión a la Página de la Universidad Nacional de Loja.

Fuente: Autor.

Luego de que se ingresó a la página de la Universidad Nacional de Loja, se buscó el enlace a Biblioteca y se realizó clic en la opción “Biblioteca Virtual” (ver Figura 132).

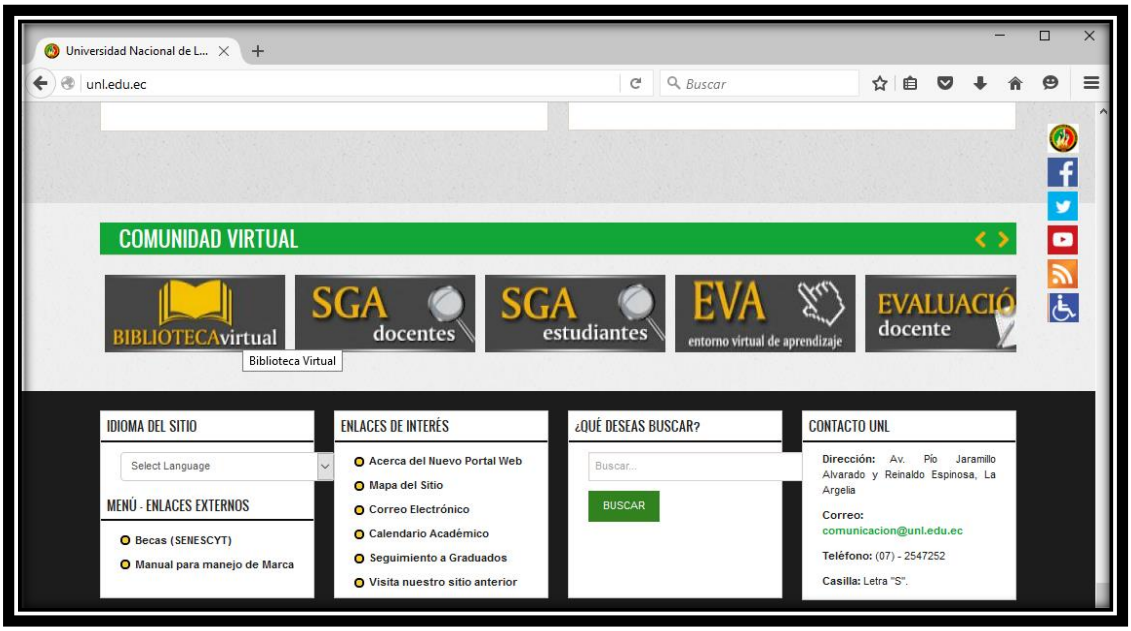


Figura 132: Ingresar a Biblioteca Virtual de la Universidad Nacional de Loja.

Fuente: Autor.

Después de que se realizó clic en la opción “Biblioteca Virtual”, se ingresó a la Biblioteca Virtual y se presentó el listado de Base de Datos Científicas con que cuenta la Universidad Nacional de Loja (ver Figura 133).

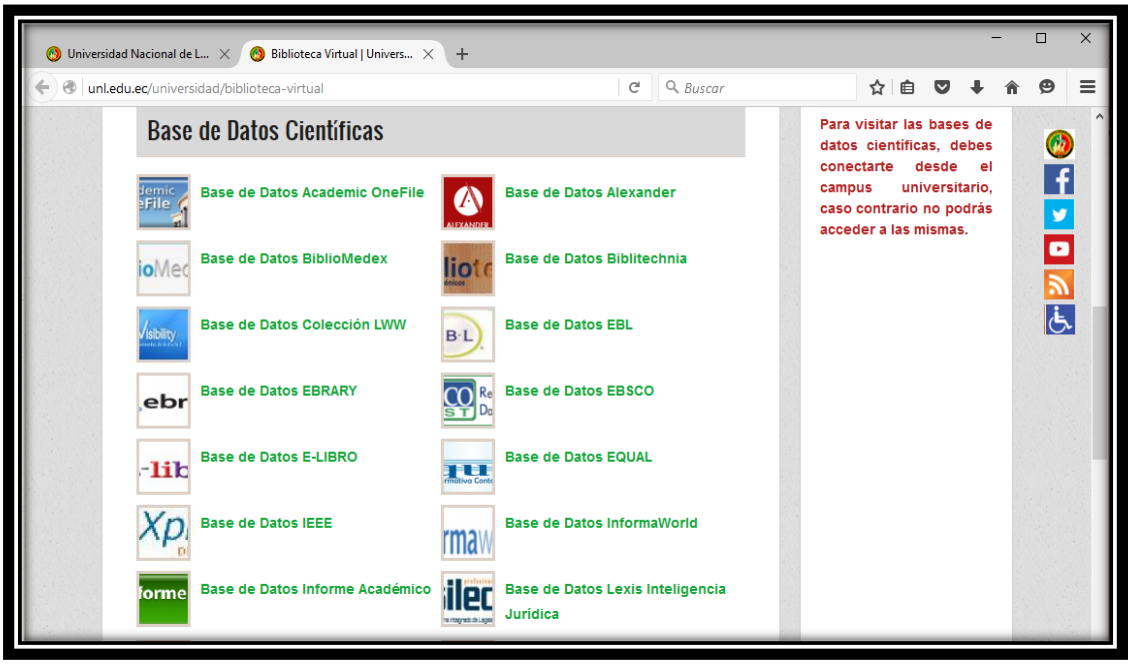


Figura 133: Lista de Base de Datos Científicas de la Universidad Nacional de Loja.

Fuente: Autor.

Luego de que se presentó el listado de Base de Datos Científicas de la Universidad Nacional de Loja, se eligió una Base de Datos para comprobar que se tiene acceso a la misma. En este caso se ingresó a la “Base de Datos IEEE” (ver Figura 134).

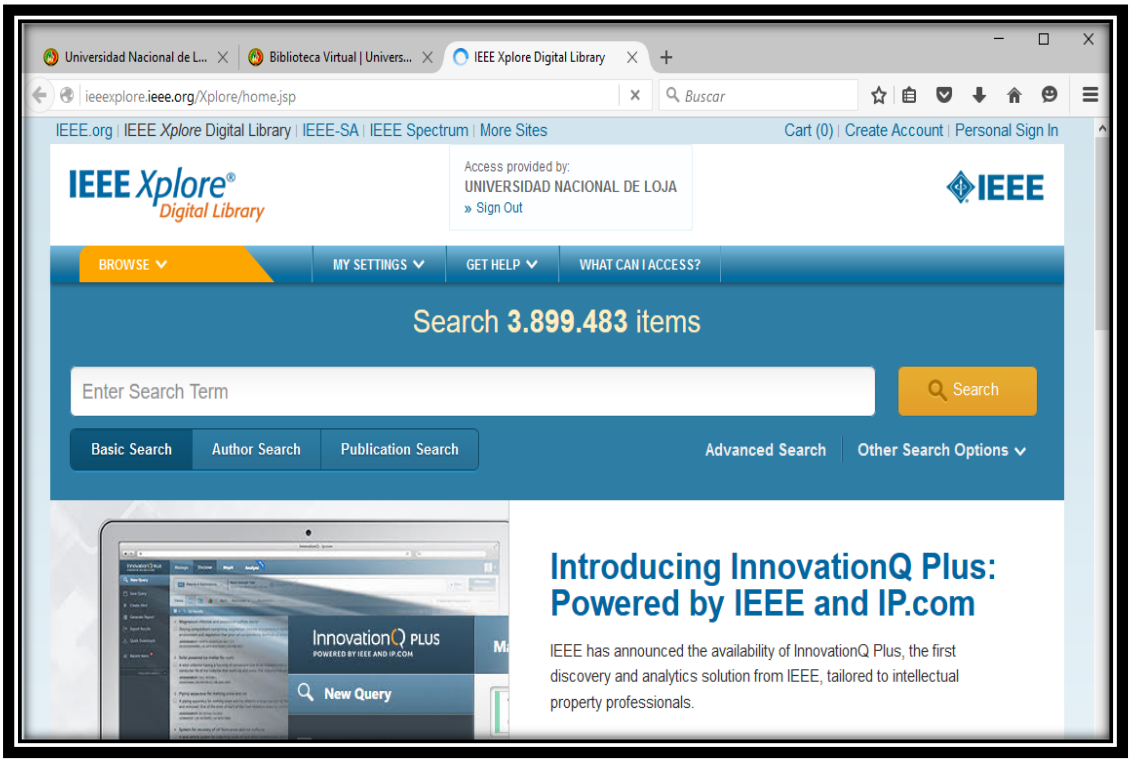


Figura 134: Ingreso a la Base de Datos Científica IEEE de la Universidad Nacional de Loja.
Fuente: Autor.

Una vez que se ingresó a la “Base de Datos IEEE”, se constató que se tiene acceso a la base de datos científica y el servicio es proporcionado por la Universidad Nacional de Loja (ver Figura 135).

Figura 135: Base de Datos IEEE Servicio Proporcionado por la UNL.
Fuente: Autor.

Luego de que se verificó que se tiene acceso a la “Base de Datos IEEE”, se seleccionó una nueva Base de Datos Científica. Esto se realizó para comprobar que se puede

acceder a la información que ofrece la misma. En este caso se seleccionó la “Base de Datos EBSCO” (ver Figura 136).

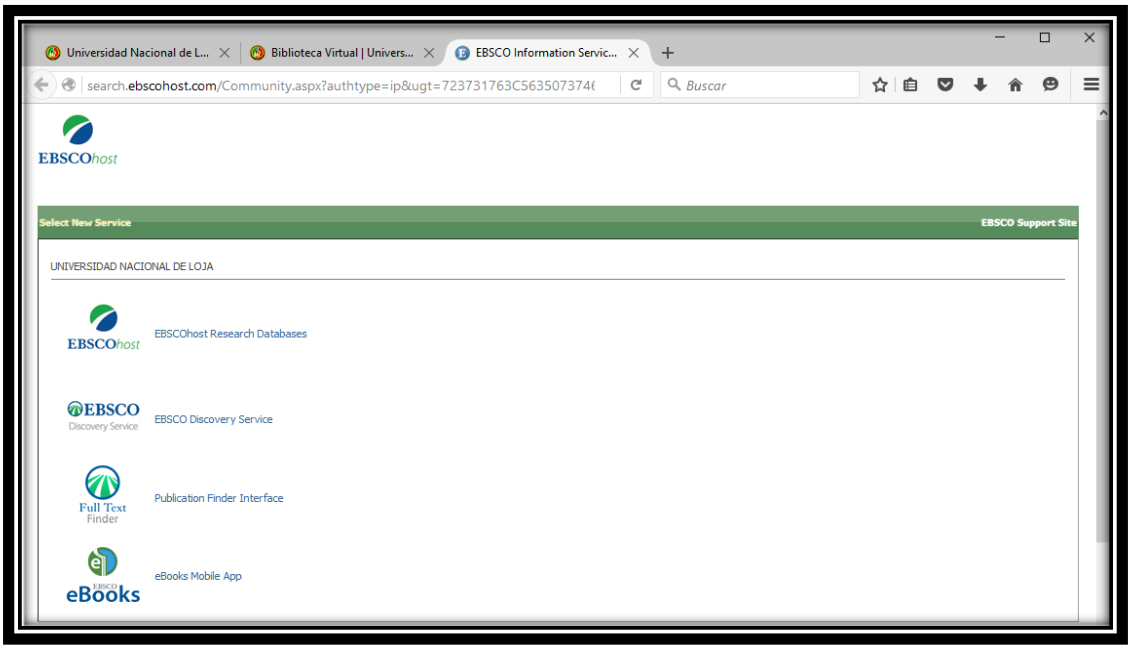


Figura 136: Ingreso a la Base de Datos EBSCO de la Universidad Nacional de Loja.
Fuente: Autor.

Una vez que se ingresó a la “Base de Datos EBSCO”, se constató que también se tiene acceso a la base de datos científica y el servicio es proporcionado por la Universidad Nacional de Loja (ver Figura 137).

Figura 137: Base de Datos EBSCO Servicio Proporcionado por la UNL.
Fuente: Autor.

Luego de que se verificó que se tiene acceso a las Bases de Datos Científicas de la Universidad Nacional de Loja, se cerró la conexión con el Servidor de Acceso OpenVPN. Para ello se seleccionó el icono de OpenVPN que se encuentra en la parte inferior de la barra de tareas. Una vez que se seleccionó el icono de OpenVPN, se realizó clic izquierdo sobre el mismo y se seleccionó la opción “Disconnect openvpn.unl.edu.ec” (ver Figura 138).

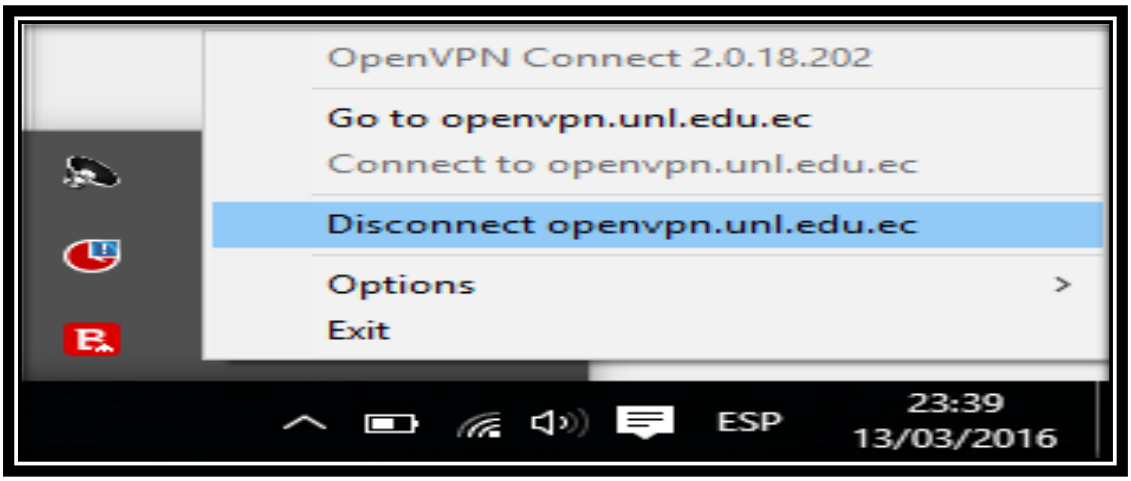


Figura 138: Desconectar el Servicio de OpenVPN en Windows.

Fuente: Autor.

Luego de que se realizó clic en la opción “Disconnect openvpn.unl.edu.ec”, la conexión con el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja se desconectó (ver Figura 139).

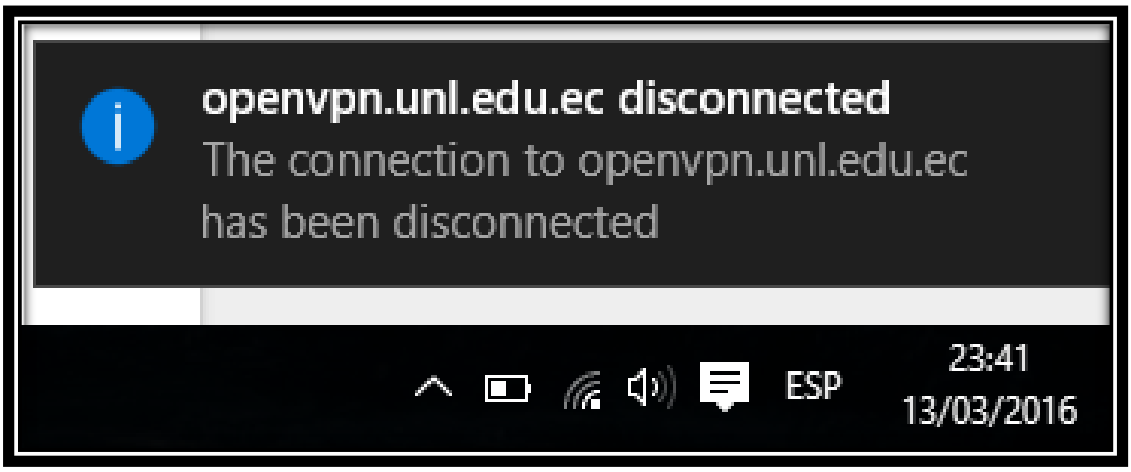


Figura 139: Conexión OpenVPN Desconectada desde el Cliente Windows.

Fuente: Autor.

6.4.2.2. Prueba de Conexión desde un Cliente VPN Android.

Para acceder a las bases de datos científicas de la Universidad Nacional de Loja desde un cliente VPN Android, se ingresó desde un navegador web del dispositivo a la siguiente dirección URL: https://openvpn.unl.edu.ec:943

Luego de que se ingresó a la dirección URL antes mencionada, el navegador web informó que el certificado de seguridad del sitio no es seguro, aun así se continuó y se realizó clic en la opción "Continuar de todos modos" (ver Figura 140).

Figura 140: Mensaje de Conexión no Segura del Servidor de Acceso OpenVPN.
Fuente: Autor.

Una vez que se realizó clic en la opción “Continuar de todos modos”, se presentó la página web de inicio de sesión para los clientes del Servidor de Acceso OpenVPN (ver Figura 141).

Figura 141: Página Inicio de Sesión de Clientes del Servidor de Acceso OpenVPN.
Fuente: Autor.

Luego de que se accedió a la página de inicio de sesión de los clientes VPN en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se ingresó el "Username" y "Password" del cliente VPN registrado. Una vez que se ingresó el usuario y la contraseña, se realizó clic en la opción "Go" (ver Figura 142).

Figura 142: Autenticación del Cliente VPN dentro del Servidor de Acceso OpenVPN.

Fuente: Autor.

Luego de que se realizó clic en la opción "Go", se muestran los diferentes clientes OpenVPN que se pueden elegir dependiendo del sistema operativo que se esté utilizando (ver Figura 143).

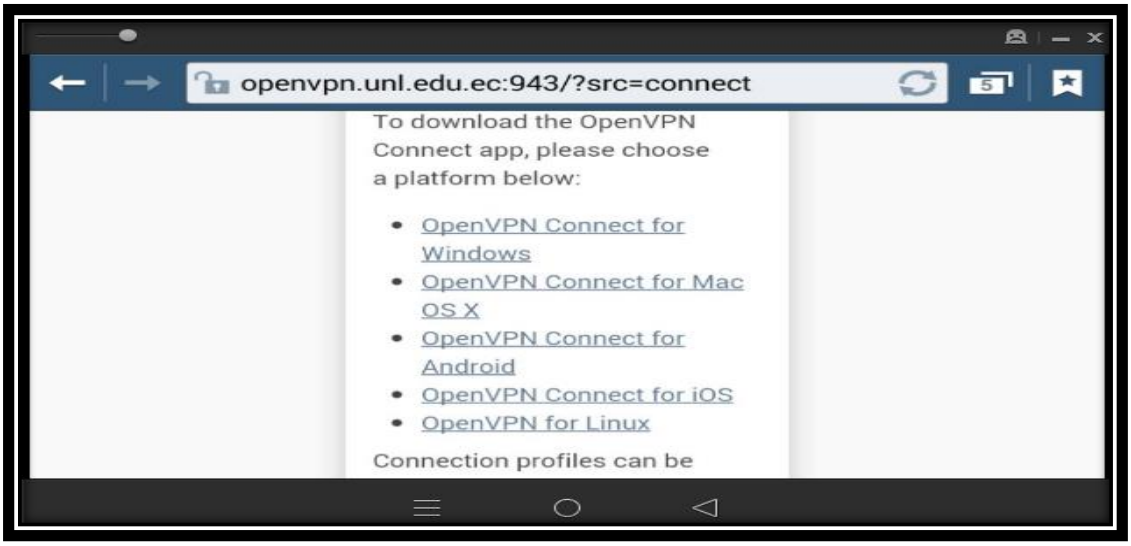


Figura 143: Página con los diferentes Clientes OpenVPN disponibles.

Fuente: Autor.

Una vez que se seleccionó el cliente OpenVPN (en este caso Android), se presentó una nueva pestaña para elegir por cual medio de navegación se desea instalar el cliente OpenVPN para Android. Se eligió la opción “Play Store” (ver Figura 144).

Figura 144: Selección del Medio de Instalación para el Cliente OpenVPN Android.

Fuente: Autor.

Después de que se realizó clic en la opción “Play Store”, apareció un archivo de instalación, en el cual se realizó clic sobre la opción “Instalar” (ver Figura 145).

Figura 145: Instalación del Cliente OpenVPN para Android.

Fuente: Autor.

Luego de que hizo clic en la opción “Instalar”, se comenzó a instalar el cliente OpenVPN para Android. Una vez que se instaló el cliente OpenVPN en Android, se realizó clic en la opción “Abrir” (ver Figura 146).

Figura 146: Cliente OpenVPN Android instalado en el dispositivo móvil

Fuente: Autor.

Luego de que se realizó clic en la opción “Abrir”, se ingresó a la configuración del cliente OpenVPN Connect para Android. Se presionó el botón menú del dispositivo y se eligió la opción “Import” (ver Figura 147).

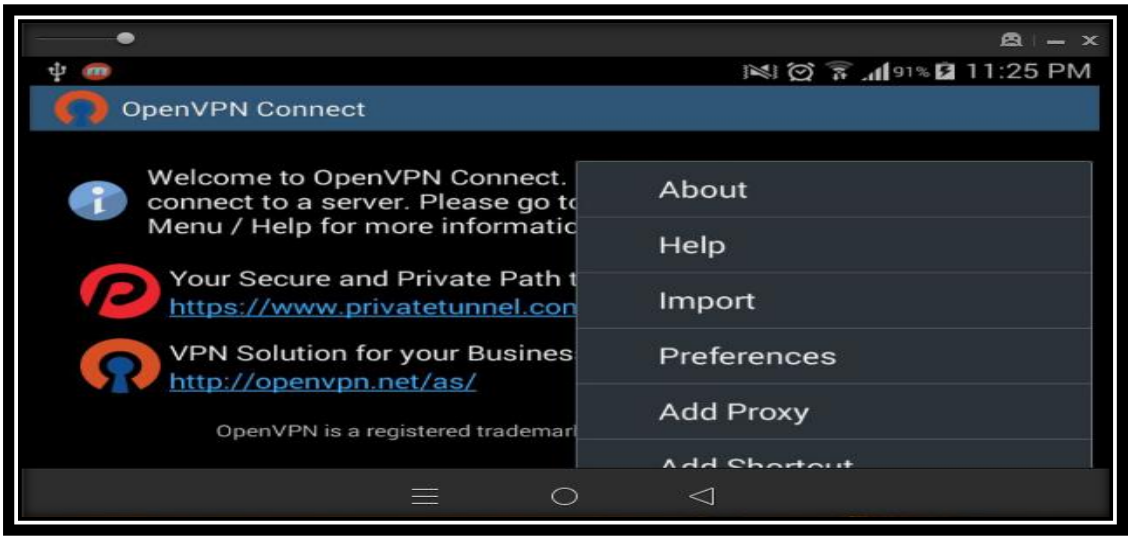


Figura 147: Opciones de Configuración del Cliente OpenVPN Connect en Android.

Fuente: Autor.

Una vez que se realizó clic en la opción “Import”, se presentó unas nuevas opciones de importación. En este caso se seleccionó la opción “Import Access Server Profile”. La cual permitió importar el perfil del Servidor de Acceso OpenVPN (ver Figura 148).

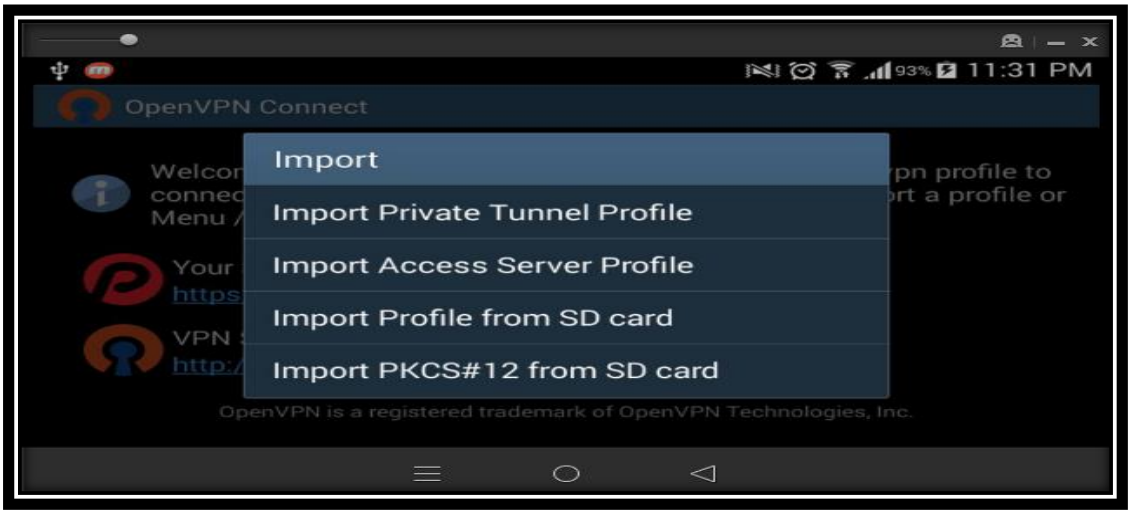


Figura 148: Selección de Import Access Server Profile.

Fuente: Autor.

Después de que se realizó clic en la opción “Import Access Server Profile”, se presentó un menú donde se ingresó la dirección pública del Servidor de Acceso OpenVPN, el usuario y la contraseña del cliente VPN registrado. Una vez que se ingresó los datos en el menú, se seleccionó la opción “Import autologin Profile” y se realizó clic en la opción “Import Profile” (ver Figura 149).

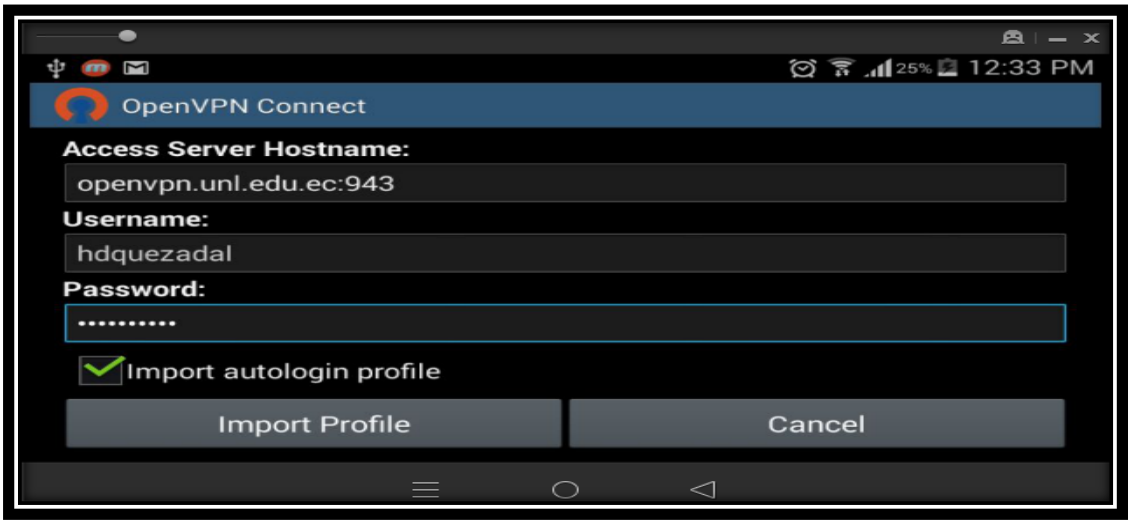


Figura 149: Importar Perfil del usuario para establecer la conexión.

Fuente: Autor.

Luego de que se realizó clic en la opción “Import Profile”, se presentó el mensaje de advertencia “Accept Invalid Certificate” y se realizó clic en la opción “Accept” del mismo (ver Figura 150).

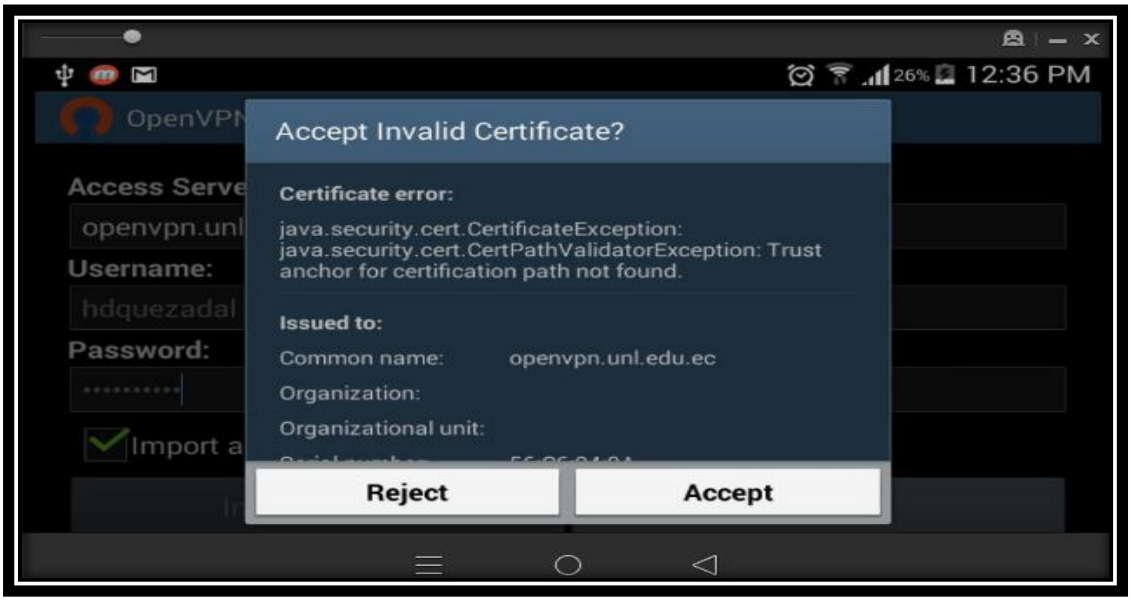


Figura 150: Aceptación del Certificado del Perfil de Usuario para el Cliente VPN.

Fuente: Autor.

Una vez que se realizó clic en la opción “Accept”, se importó el perfil del cliente VPN y se seleccionó la opción “Connect” (ver Figura 151).

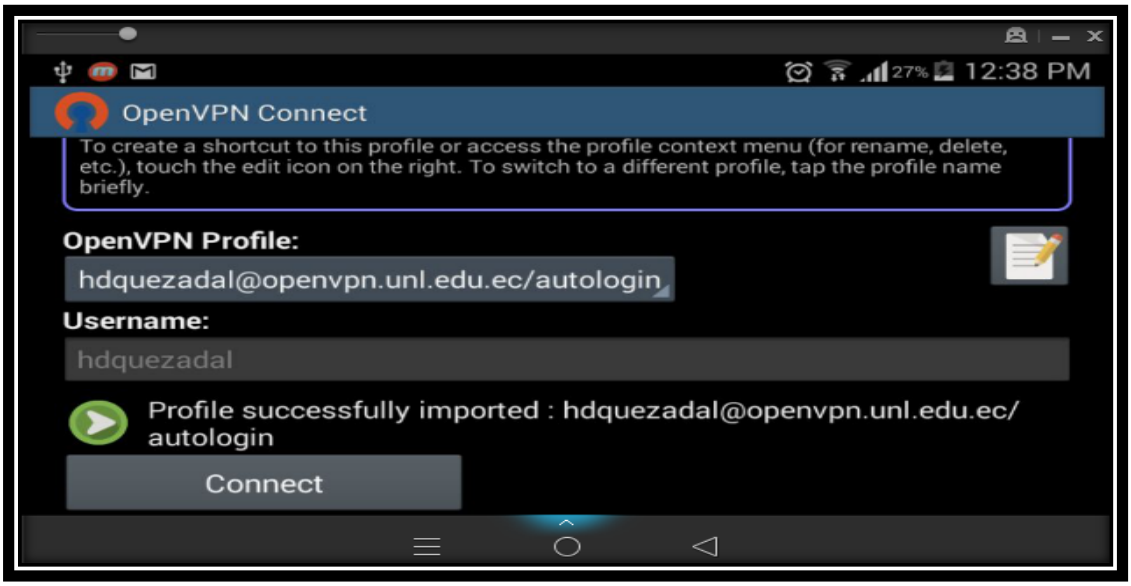


Figura 151: Conectarse al Servidor de Acceso OpenVPN.

Fuente: Autor.

Después de que se realizó clic en la opción “Connect”, se estableció la conexión entre el cliente VPN Android y el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja (ver Figura 152).

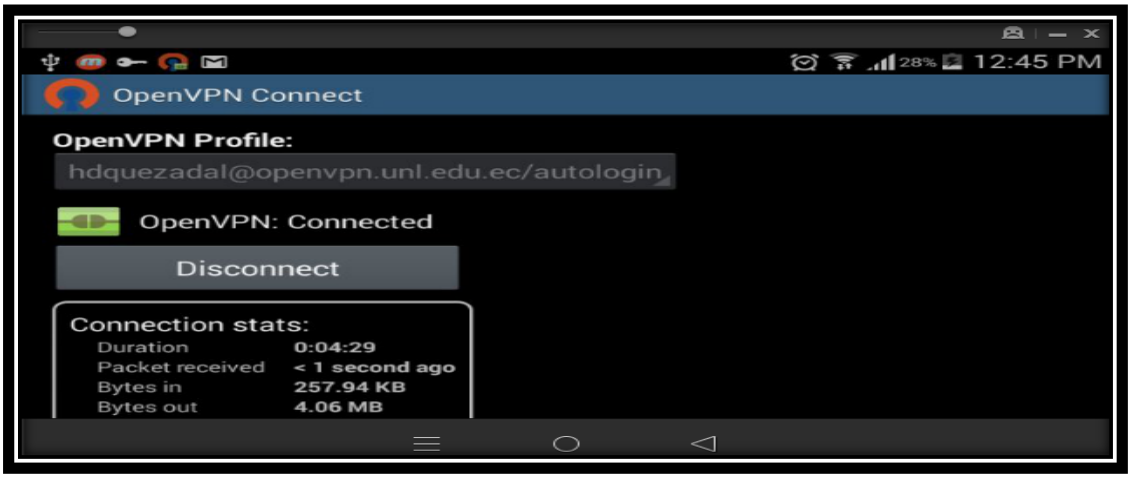


Figura 152: Conexión establecida entre el Cliente VPN Android y el Servidor OpenVPN.
Fuente: Autor.

Una vez que se estableció la conexión con el Servidor de Acceso OpenVPN, se abrió un navegador web y en la barra de navegación se ingresó la dirección de la Página de la Universidad Nacional de Loja, URL: https://unl.edu.ec. Luego de que se ingresó a la página de la Universidad Nacional de Loja, se buscó el enlace a Biblioteca y se realizó clic en la opción “Biblioteca Virtual” (ver Figura 153).

Figura 153: Acceso a Biblioteca Virtual de la Universidad Nacional de Loja.
Fuente: Autor.

Después de que se realizó clic en la opción “Biblioteca Virtual”, se ingresó a la Biblioteca Virtual y se presentó el listado de Base de Datos Científicas con que cuenta la Universidad Nacional de Loja (ver Figura 154).

Figura 154: Listado de Base de Datos Científicas de la Universidad Nacional de Loja.
Fuente: Autor.

Luego de que se presentó el listado de Base de Datos Científicas de la Universidad Nacional de Loja, se eligió una Base de Datos para comprobar que se tiene acceso a la misma. En este caso se ingresó a la “Base de Datos IEEE” (ver Figura 155).

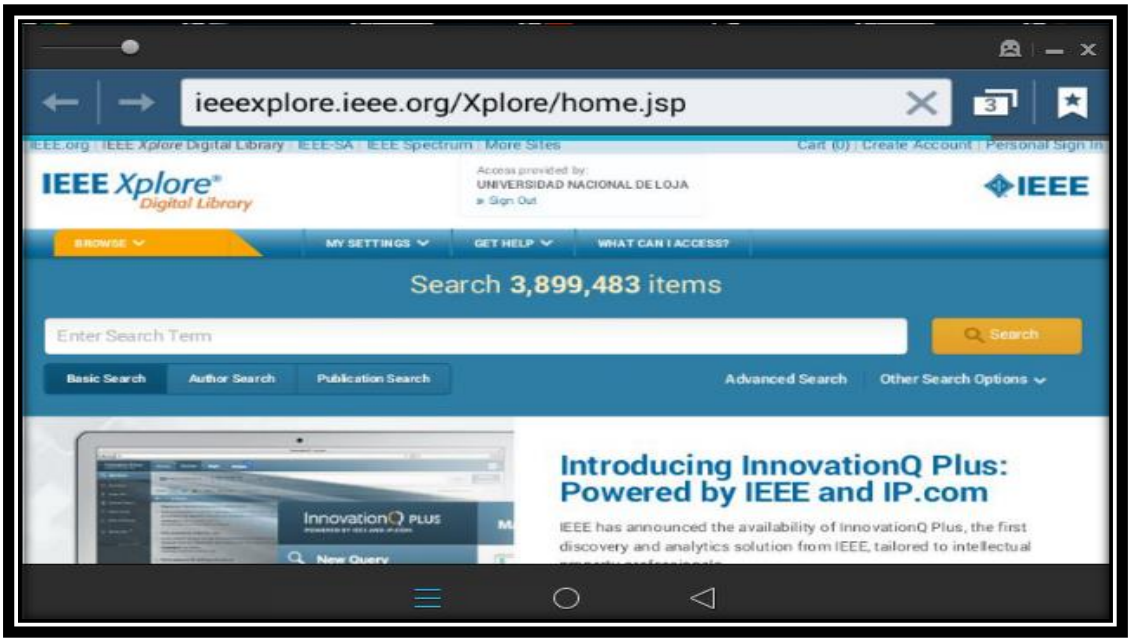


Figura 155: Ingreso a la Base de Datos IEEE de la Universidad Nacional de Loja.
Fuente: Autor.

Una vez que se ingresó a la “Base de Datos IEEE”, se constató que se tiene acceso a la base de datos científica y el servicio es proporcionado por la Universidad Nacional de Loja (ver Figura 156).

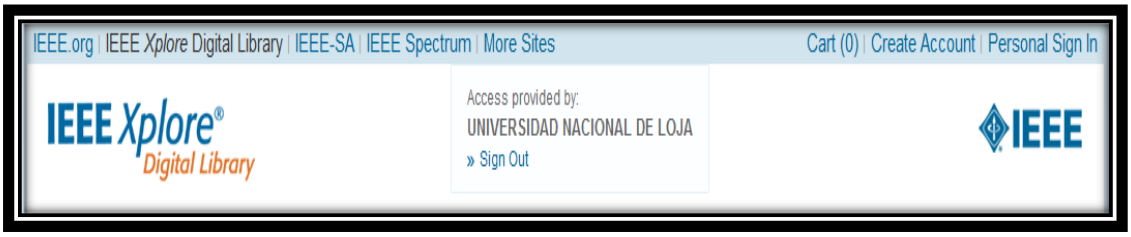


Figura 156: Acceso a la Base de Datos IEEE por parte de la UNL.

Fuente: Autor.

Luego de que se verificó que se tiene acceso a las Bases de Datos Científicas de la Universidad Nacional de Loja, se cerró la conexión con el Servidor de Acceso OpenVPN. Para ello se realizó clic en la opción “Disconnect” (ver Figura 157).

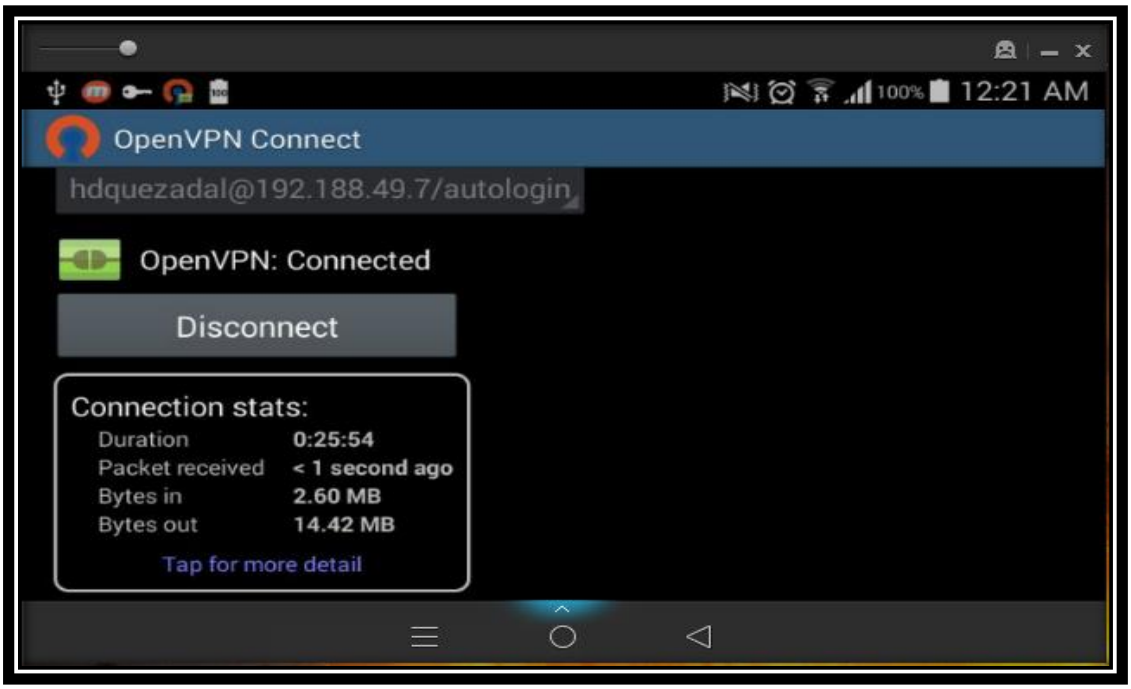


Figura 157: Desconectar el Servicio de OpenVPN en Android.

Fuente: Autor.

Una vez que se realizó clic en la opción “Disconnect”, la conexión con el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja se desconectó (ver Figura 158).

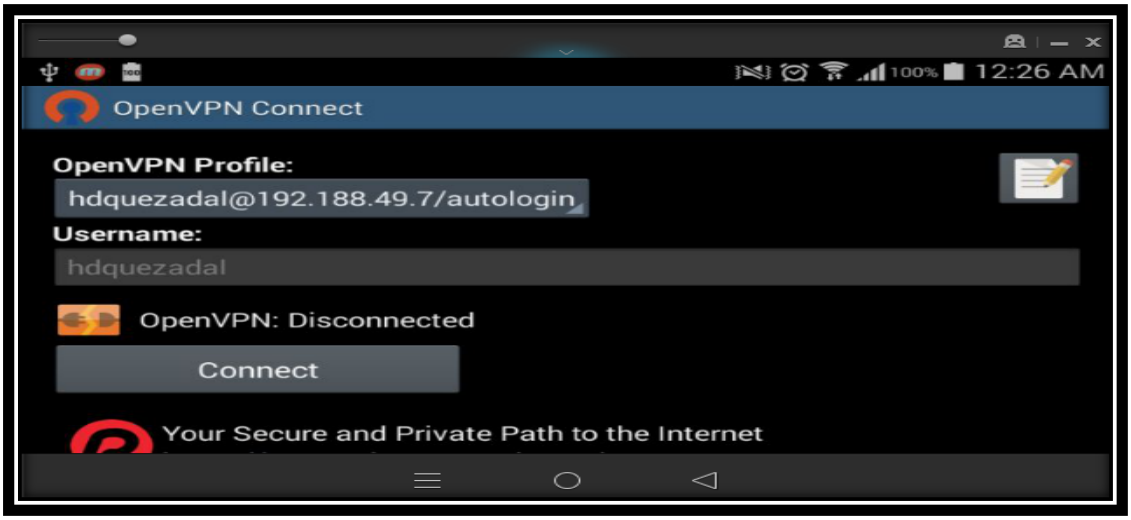


Figura 158: Conexión VPN Desconectada desde el Cliente Android.

Fuente: Autor.

- **Resultados de las Pruebas de Conexión.**

Una vez que se finalizó las pruebas de conexión a las bases de datos científicas de la Universidad Nacional de Loja a través de la Red Privada Virtual, se constató que el acceso a las bases de datos científicas de la Universidad Nacional de Loja desde un cliente VPN Windows y Android fue exitoso.

6.4.3. Actividad 3: Pruebas de Accesibilidad.

En esta actividad se realizó las pruebas de accesibilidad (carga y cantidad de accesos) en el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja.

Estas pruebas consistieron en crear un escenario normal de acceso al Servidor OpenVPN por parte de un usuario VPN registrado. La realización de esta prueba ayudó a verificar el uso del Servidor de Acceso OpenVPN cuando existen accesos simultáneos de usuarios.

Se usó la herramienta Apache JMeter para realizar las pruebas de carga al Servidor de Acceso OpenVPN, conjuntamente con la herramienta Badboy, la cual permitió crear el script del escenario de acceso al servidor y exportarlo a la herramienta JMeter, debido a que JMeter no soporta conexiones “https”. Estas herramientas son aplicaciones de escritorio y gratuitas.

El escenario de acceso al Servidor OpenVPN que se realizó en la herramienta Badboy fue el siguiente:

1. Primero se accedió a la página de inicio de sesión del Servidor de Acceso OpenVPN.
2. Luego se realizó la autenticación en el Servidor de Acceso OpenVPN empleando un usuario registrado en el Servidor de Acceso.
3. Se realizó la conexión del usuario con el Servidor de Acceso OpenVPN.
4. Y finalmente se desconectó la conexión del usuario con el Servidor de Acceso OpenVPN.

Una vez que se realizó el escenario para la prueba de carga, se exportó el script generado por la herramienta Badboy a JMeter (ver Figura 159).

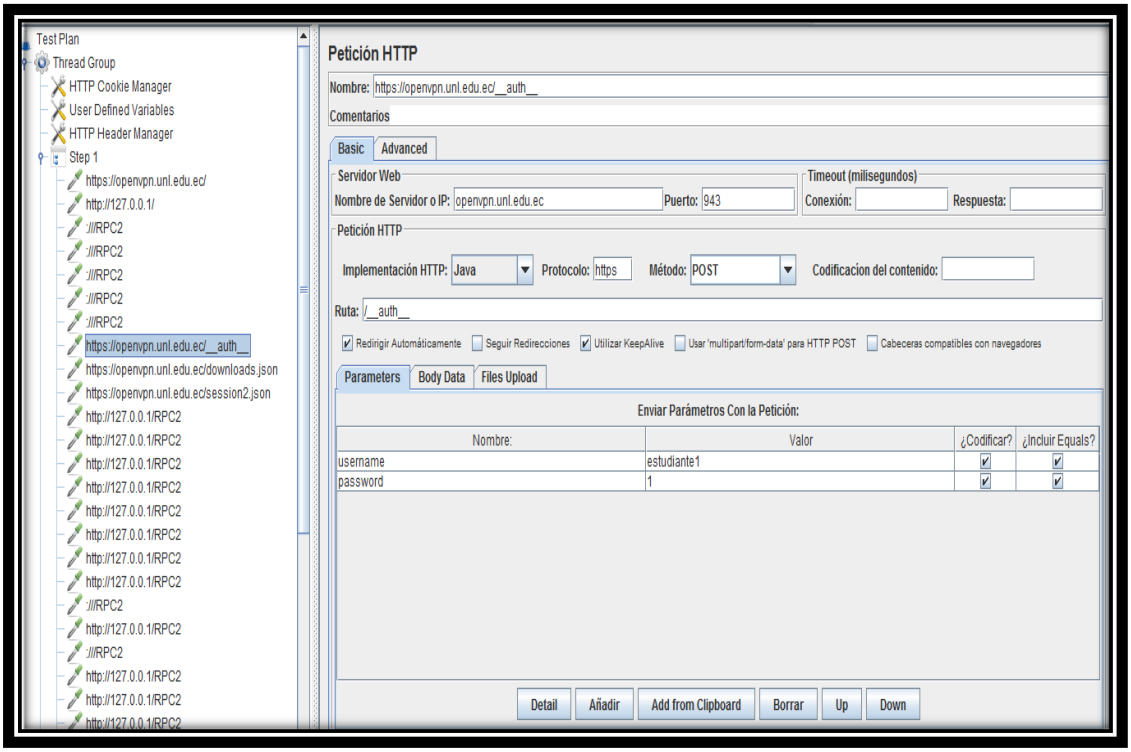
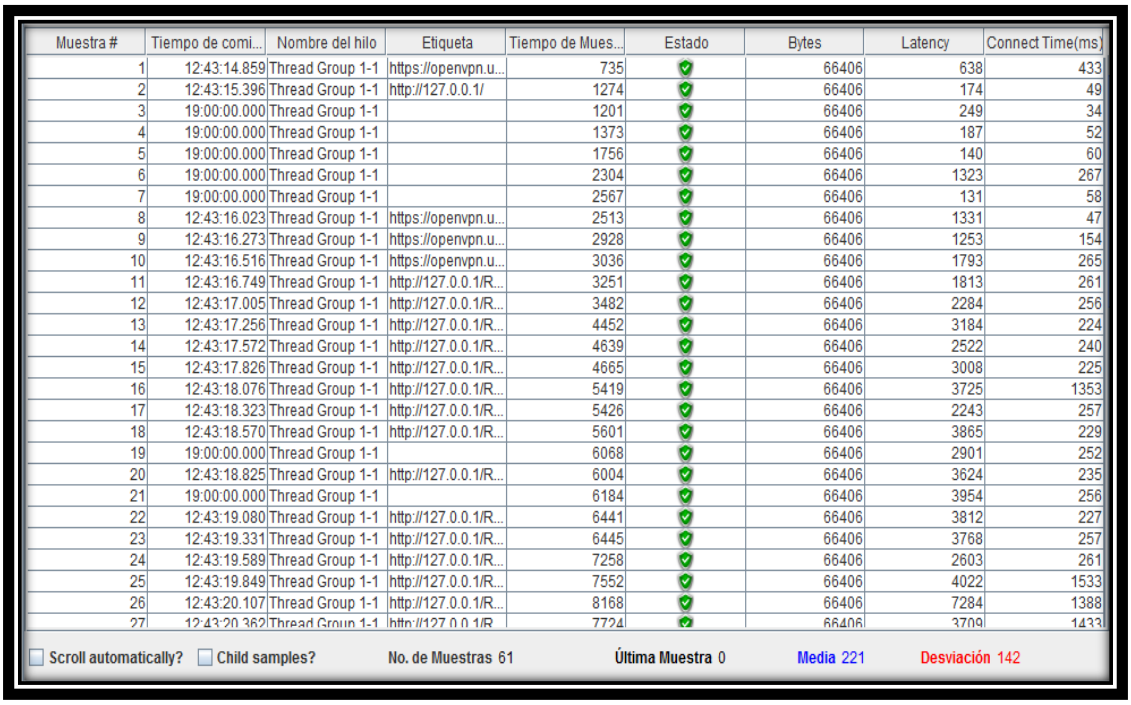


Figura 159: Script del escenario de acceso al Servidor OpenVPN.

Fuente: Autor.

Una vez que se exportó el script del escenario de Acceso a la herramienta JMeter se lo ejecutó. Se definió una carga de 2 usuarios que realizan diferentes peticiones (61 peticiones) en un segundo.

Luego de que se terminó su ejecución, como resultado se visualizó las peticiones que se realizaron para el Acceso al Servidor OpenVPN (ver Figura 160).



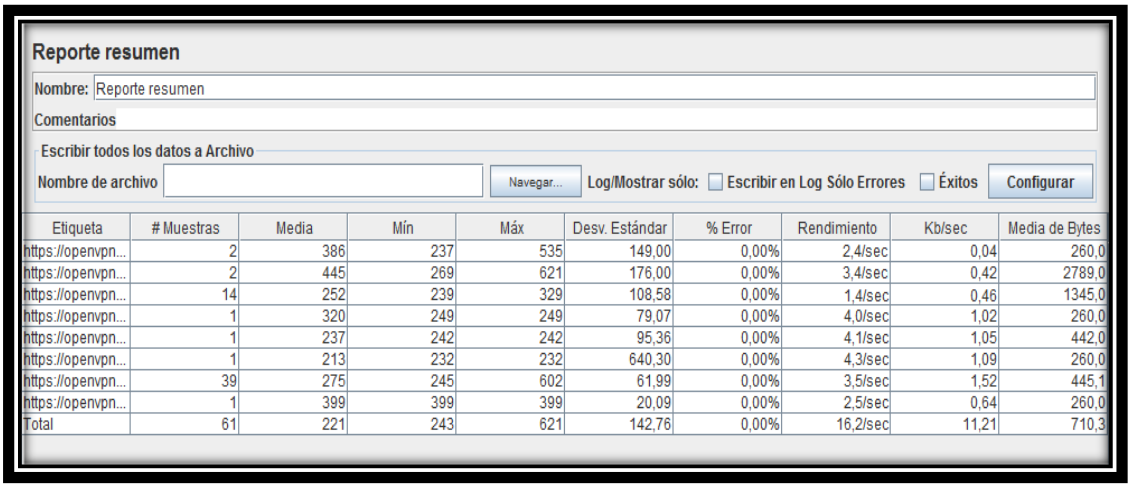
Muestra #	Tiempo de comi...	Nombre del hilo	Etiqueta	Tiempo de Mues...	Estado	Bytes	Latency	Connect Time(ms)
1	12:43:14.859	Thread Group 1-1	https://openvpn.u...	735		66406	638	433
2	12:43:15.396	Thread Group 1-1	http://127.0.0.1/	1274		66406	174	49
3	19:00:00.000	Thread Group 1-1		1201		66406	249	34
4	19:00:00.000	Thread Group 1-1		1373		66406	187	52
5	19:00:00.000	Thread Group 1-1		1756		66406	140	60
6	19:00:00.000	Thread Group 1-1		2304		66406	1323	267
7	19:00:00.000	Thread Group 1-1		2567		66406	131	58
8	12:43:16.023	Thread Group 1-1	https://openvpn.u...	2513		66406	1331	47
9	12:43:16.273	Thread Group 1-1	https://openvpn.u...	2928		66406	1253	154
10	12:43:16.516	Thread Group 1-1	https://openvpn.u...	3036		66406	1793	265
11	12:43:16.749	Thread Group 1-1	http://127.0.0.1/R...	3251		66406	1813	261
12	12:43:17.005	Thread Group 1-1	http://127.0.0.1/R...	3482		66406	2284	256
13	12:43:17.256	Thread Group 1-1	http://127.0.0.1/R...	4452		66406	3184	224
14	12:43:17.572	Thread Group 1-1	http://127.0.0.1/R...	4639		66406	2522	240
15	12:43:17.826	Thread Group 1-1	http://127.0.0.1/R...	4665		66406	3008	225
16	12:43:18.076	Thread Group 1-1	http://127.0.0.1/R...	5419		66406	3725	1353
17	12:43:18.323	Thread Group 1-1	http://127.0.0.1/R...	5426		66406	2243	257
18	12:43:18.570	Thread Group 1-1	http://127.0.0.1/R...	5601		66406	3865	229
19	19:00:00.000	Thread Group 1-1		6068		66406	2901	252
20	12:43:18.825	Thread Group 1-1	http://127.0.0.1/R...	6004		66406	3624	235
21	19:00:00.000	Thread Group 1-1		6184		66406	3954	256
22	12:43:19.080	Thread Group 1-1	http://127.0.0.1/R...	6441		66406	3812	227
23	12:43:19.331	Thread Group 1-1	http://127.0.0.1/R...	6445		66406	3768	257
24	12:43:19.589	Thread Group 1-1	http://127.0.0.1/R...	7258		66406	2603	261
25	12:43:19.849	Thread Group 1-1	http://127.0.0.1/R...	7552		66406	4022	1533
26	12:43:20.107	Thread Group 1-1	http://127.0.0.1/R...	8168		66406	7284	1388
27	12:43:20.362	Thread Group 1-1	http://127.0.0.1/R...	7724		66406	3709	1433

Scroll automatically? Child samples? No. de Muestras 61 Última Muestra 0 Media 221 Desviación 142

Figura 160: Reporte del escenario creado para el Acceso al Servidor OpenVPN.

Fuente: Autor.

Como se observa en la Figura 160, las peticiones se realizaron exitosamente sin ningún tipo de error. Para interpretar los datos de la prueba se generó el "Resumen de Reporte" de la ejecución del escenario en la herramienta JMeter (ver Figura 161).



Reporte resumen

Nombre: Reporte resumen

Comentarios

Escribir todos los datos a Archivo

Nombre de archivo Navegar... Log/Mostrar sólo: Escribir en Log Sólo Errores Éxitos Configurar

Etiqueta	# Muestras	Media	Mín	Máx	Desv. Estándar	% Error	Rendimiento	Kb/sec	Media de Bytes
https://openvpn...	2	386	237	535	149,00	0,00%	2,4/sec	0,04	260,0
https://openvpn...	2	445	269	621	176,00	0,00%	3,4/sec	0,42	2789,0
https://openvpn...	14	252	239	329	108,58	0,00%	1,4/sec	0,46	1345,0
https://openvpn...	1	320	249	249	79,07	0,00%	4,0/sec	1,02	260,0
https://openvpn...	1	237	242	242	95,36	0,00%	4,1/sec	1,05	442,0
https://openvpn...	1	213	232	232	640,30	0,00%	4,3/sec	1,09	260,0
https://openvpn...	39	275	245	602	61,99	0,00%	3,5/sec	1,52	445,1
https://openvpn...	1	399	399	399	20,09	0,00%	2,5/sec	0,64	260,0
Total	61	221	243	621	142,76	0,00%	16,2/sec	11,21	710,3

Figura 161: Resumen del Reporte generado en el escenario creado.

Fuente: Autor.

Una vez que se generó el resumen del reporte del escenario, se realizó la interpretación de los datos obtenidos:

- Muestra: Se ha utilizado 2 threads para cada acción. Teniendo 61 threads en total.
- Media: El tiempo promedio que se ha invertido en cada consulta es de 221 milisegundos (0.221 segundos).
- Min: El tiempo mínimo que ha demorado un thread en acceder a una página es de 243 milisegundos.
- Max: El tiempo máximo que ha demorado un thread en acceder a una página es de 621 milisegundos
- Desviación Estándar: 142,76.
- Error: Demuestra el porcentaje de peticiones con errores, como se observa no se ha obtenido ningún error en las peticiones.
- Rendimiento: el rendimiento es de 16,2 sec. Se ha obtenido un rendimiento de 11,21 Kb por segundo.
- Media Bytes: La media de la respuesta del servidor en bytes es de 710.3

6.4.4. Actividad 4: Pruebas de Implementación.

En esta actividad se realizó las pruebas de implementación del Servidor de Acceso OpenVPN de la Universidad Nacional de Loja. Para ello se tomó una muestra de 5 usuarios de acuerdo a cada perfil que se estableció para la autenticación en el servidor.

Estas pruebas consistieron en realizar la conexión de los usuarios al Servidor de Acceso OpenVPN de acuerdo a los perfiles de usuarios que se establecieron anteriormente (ver Actividad 3 – Fase III de Resultados).

6.4.4.1. Crear usuarios en el Servidor de Acceso OpenVPN.

Como paso inicial se creó los usuarios en el Servidor de Acceso OpenVPN. Los usuarios que se creó fueron definidos en base a los perfiles de usuarios para la autenticación que se establecieron en el diseño de la Red Privada Virtual (ver Actividad 6 – Fase II de Resultados).

Los usuarios que se establecieron para la conexión con el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja fueron los siguientes:

- **Usuarios "uti".**

En base al número de licencias (30 licencias) que se activó para el Servidor de Acceso OpenVPN, se creó 5 usuarios para el grupo "uTI" (ver Figura 162). Los nombres de usuario que se estableció para el grupo "uTI" fueron los siguientes: uti1, uti2, uti3, uti4 y uti5.

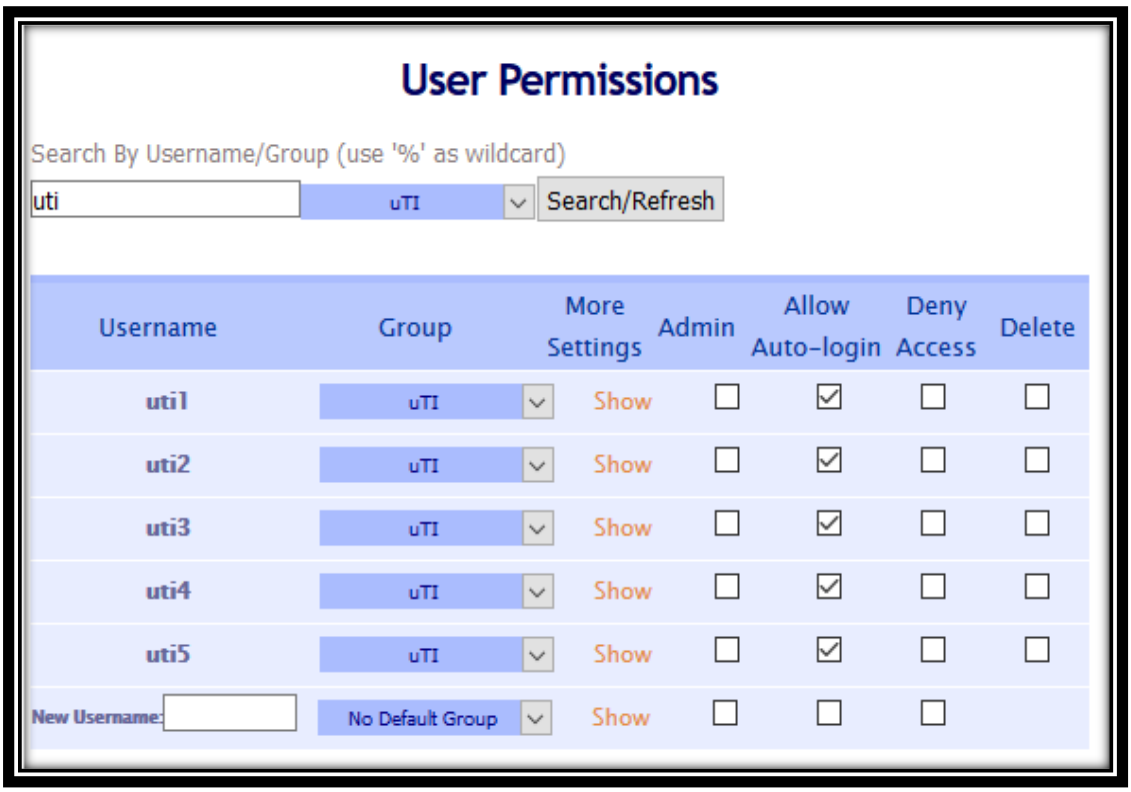


Figura 162: Creación de los usuarios para el Perfil de Usuario "uTI".

Fuente: Autor.

- **Usuarios "docentes".**

Luego de que se crearon los usuarios para el grupo "uTI", se creó 5 usuarios para el grupo "docentes" (ver Figura 163). Los nombres de usuario que se estableció para el grupo "docentes" fueron los siguientes: docente1, docente2, docente3, docente4 y docente5.

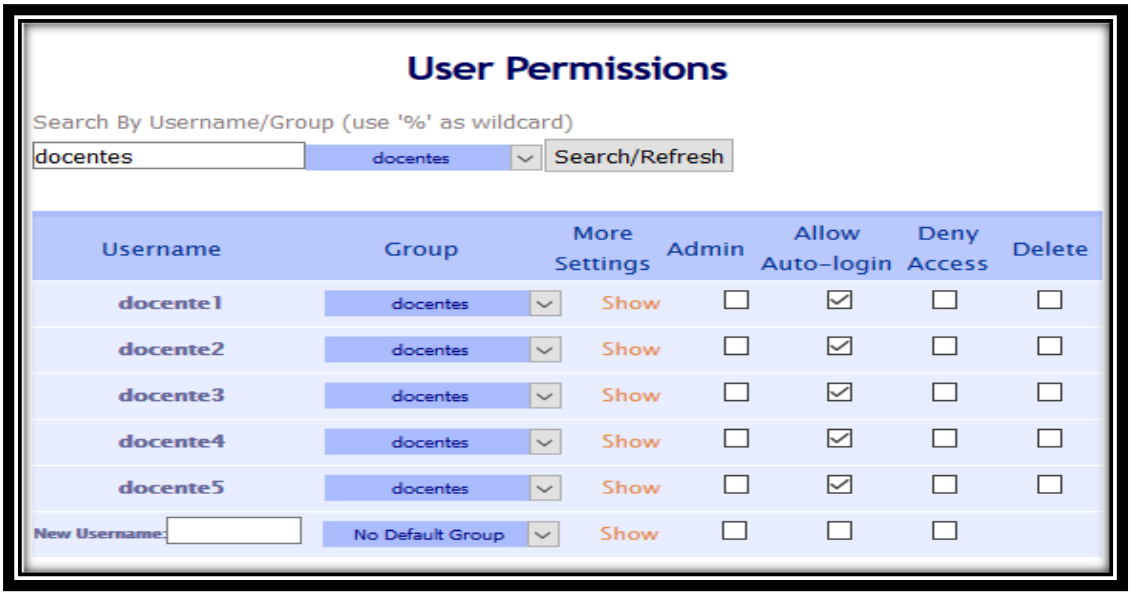


Figura 163: Creación de los usuarios para el Perfil de Usuario "docentes".

Fuente: Autor.

- **Usuarios "estudiantes".**

Una vez que se crearon los usuarios para el grupo "docentes", se creó 5 usuarios para el grupo "estudiantes" (ver Figura 164). Los nombres de usuario que se estableció para el grupo "estudiantes" fueron los siguientes: estudiante1, estudiante2, estudiante3, estudiante4 y estudiante5.

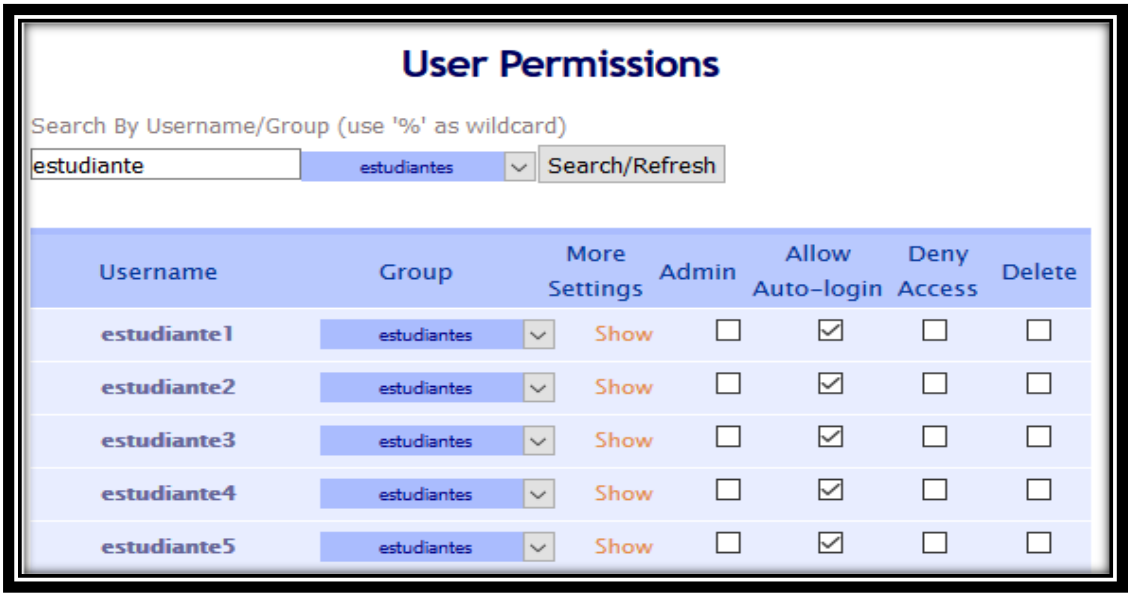


Figura 164: Creación de los usuarios para el Perfil de Usuario "estudiantes".

Fuente: Autor.

- **Usuarios “administrativos.**

Después de que se crearon los usuarios para el grupo “estudiantes”, se creó 5 usuarios para el grupo “administrativos” dentro del Servidor de Acceso OpenVPN (ver Figura 165). Los nombres de usuario que se estableció para el grupo “administrativos” fueron los siguientes: administrativo1, administrativo2, administrativo3, administrativo4 y administrativo5.

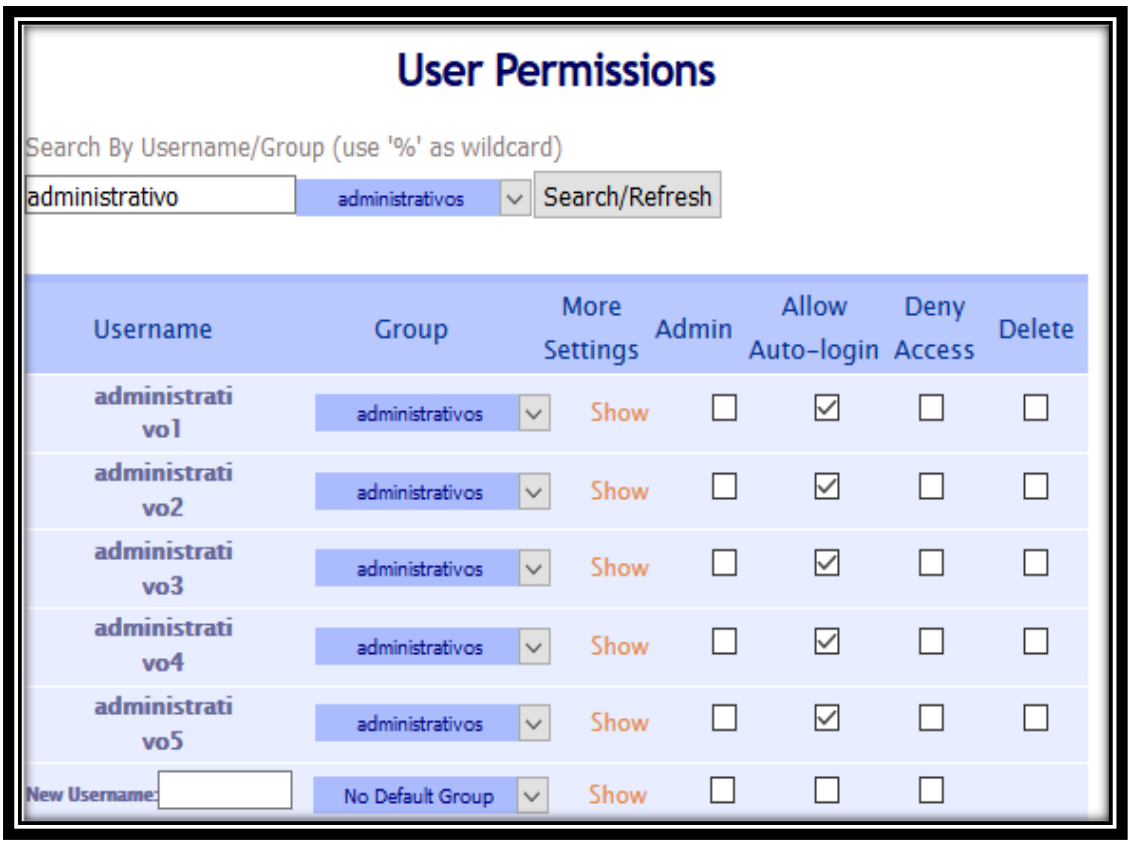


Figura 165: Creación de los usuarios para el Perfil de Usuario “administrativos”.

Fuente: Autor.

- **Usuarios “srei.uti”.**

Luego de que se crearon los usuarios para el grupo “administrativos”, se creó 5 usuarios para el grupo “srei.uti” dentro del Servidor de Acceso OpenVPN de la Universidad Nacional de Loja (ver Figura 166). Los nombres de usuario que se estableció para el grupo “srei.uti” fueron los siguientes: redes1, redes2, redes3, redes4 y redes5.

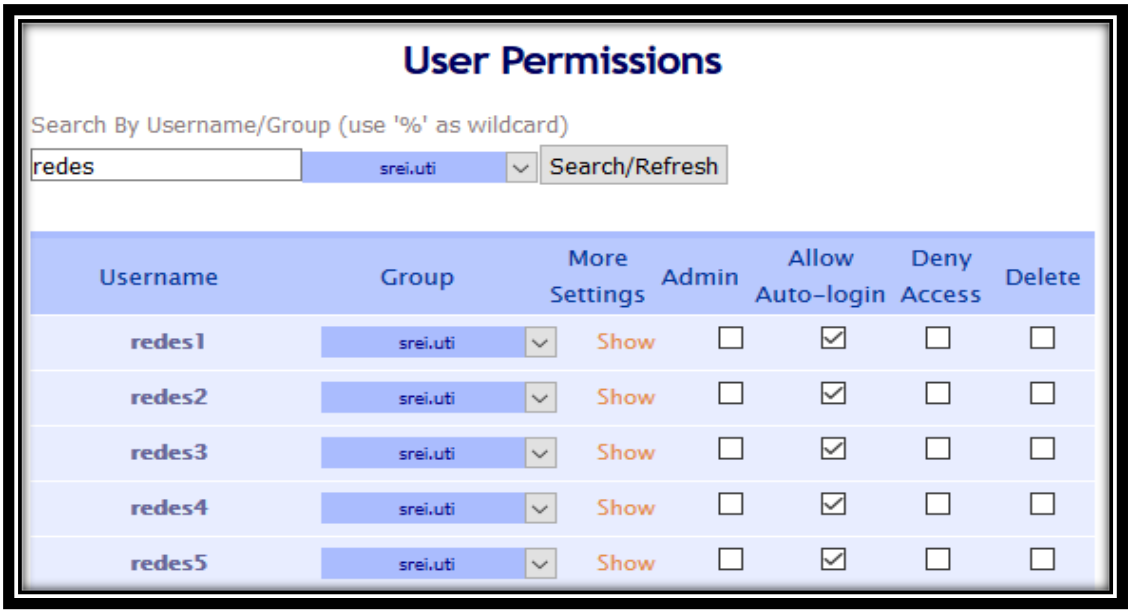


Figura 166: Creación de los usuarios para el Perfil de Usuario "srei.uti".

Fuente: Autor.

- **Usuarios "sdsw.uti".**

Una vez que se crearon los usuarios para el grupo "srei.uti", se creó 5 usuarios para el grupo "sdsw.uti" dentro del Servidor de Acceso OpenVPN de la Universidad Nacional de Loja (ver Figura 167). Los nombres de usuario que se estableció para el grupo "sdsw.uti" fueron los siguientes: software1, software2, software3, software4 y software5.

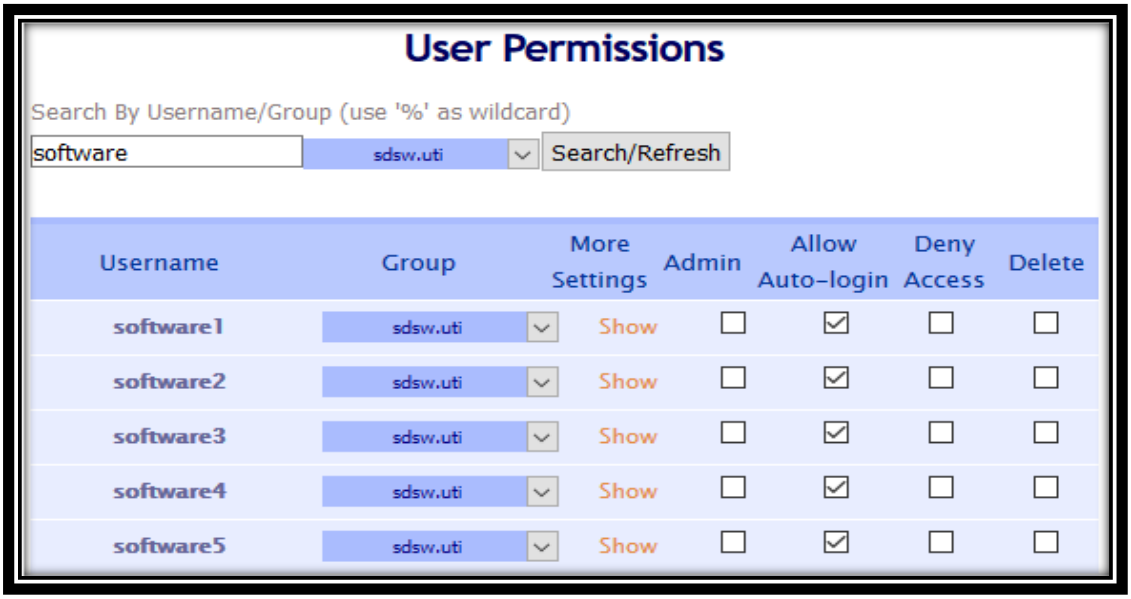


Figura 167: Creación de los usuarios para el Perfil de Usuario "sdsw.uti".

Fuente: Autor.

6.4.4.2. Conexión de los usuarios con el Servidor de Acceso OpenVPN.

Una vez que se crearon los usuarios para cada uno de los “perfiles de usuario”, se realizó la conexión de cada uno de ellos con el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja. Se utilizó VirtualBox para crear 30 máquinas virtuales con el sistema operativo “Linux Mint” y así realizar las conexiones al Servidor de Acceso OpenVPN con cada uno de los usuarios que se creó (ver Figura 168).

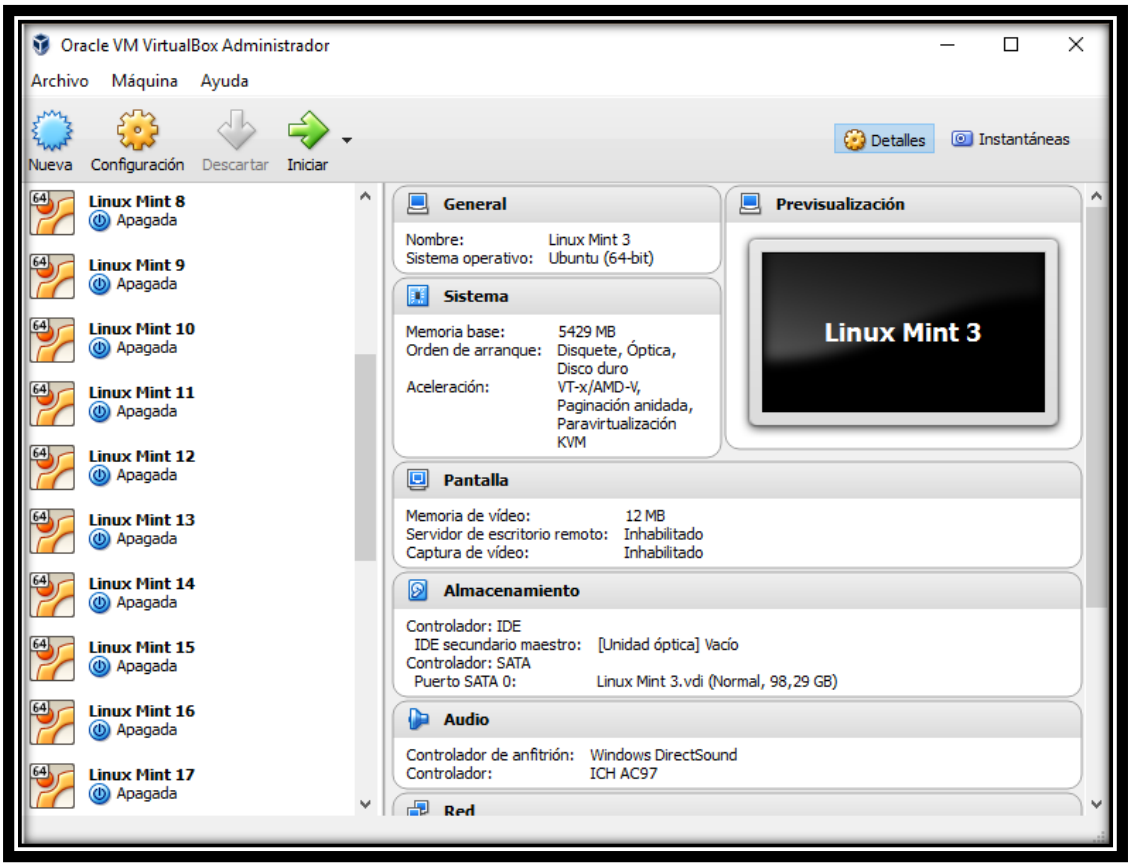


Figura 168: Máquinas creadas en VirtualBox para la conexión de los usuarios.
Fuente: Autor.

Luego de que se realizó la instalación de los usuarios VPN en las máquinas virtuales, se realizó las conexiones de cada uno de los usuarios al Servidor de Acceso OpenVPN.

Una vez que se realizó las conexiones de los usuarios con el Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se observa que en la página de administración web de OpenVPN se encuentran conectados los 30 usuarios concurrentes (ver Figura 169).

Figura 169: Visualización de los Usuarios Concurrentes conectados al Servidor OpenVPN. Fuente: Autor.

6.4.4.3. Comprobación de la conexión de los usuarios en el Servidor de Acceso OpenVPN.

Luego de que se realizó la conexión de cada uno de los usuarios al Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se comprobó que cada usuario se encuentre asociado al servidor y en funcionamiento.

A continuación se detallan las conexiones de cada uno de los usuarios al Servidor de Acceso OpenVPN de la Universidad Nacional de Loja.

- **Usuarios "estudiantes".**

Una vez que se realizó la conexión de los usuarios del grupo "estudiantes" al Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se evidencia que los usuarios del grupo se encuentran conectados al servidor y en funcionamiento (ver Figura 170).

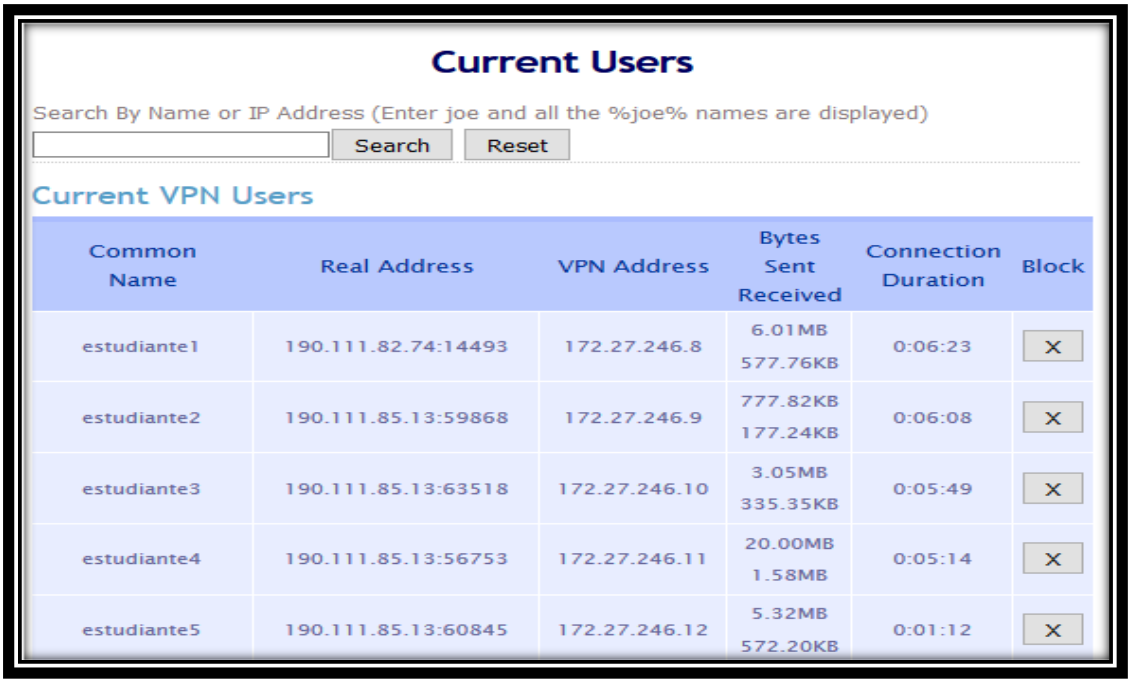


Figura 170: Comprobación de Conexión de los usuarios "estudiantes".

Fuente: Autor.

- **Usuarios "docentes".**

Después de que se realizó la conexión de los usuarios del grupo "docentes" al Servidor de Acceso OpenVPN, se evidencia que los usuarios del grupo se encuentran conectados al servidor y en funcionamiento (ver Figura 171).

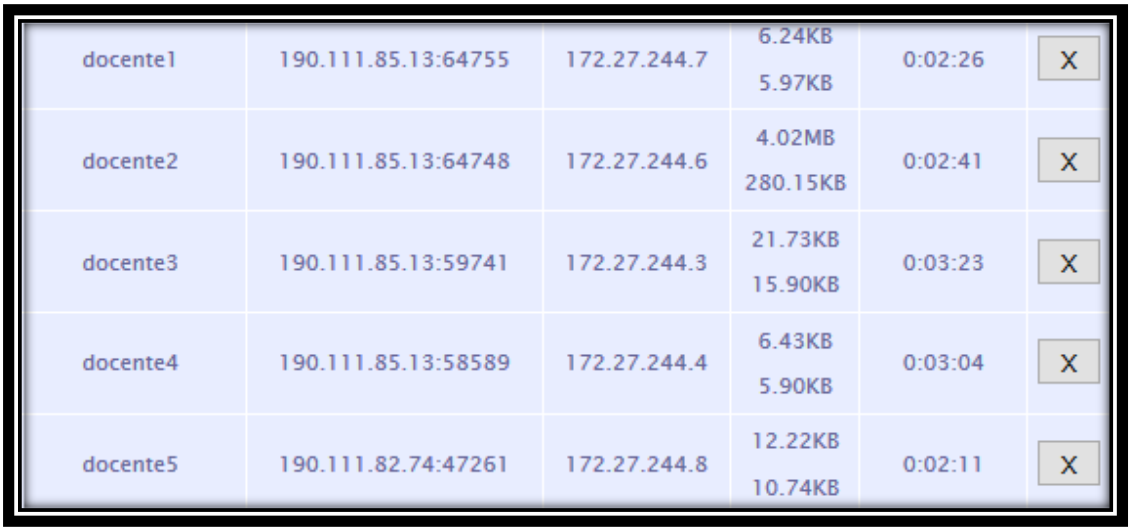


Figura 171: Comprobación de Conexión de los usuarios "docentes".

Fuente: Autor.

- **Usuarios “administrativos”.**

Una vez que se realizó la conexión de los usuarios del grupo “administrativos” al Servidor de Acceso OpenVPN, se evidencia que los usuarios del grupo se encuentran en funcionamiento y conectados (ver Figura 172).

administrativo1	190.111.85.13:64220	172.27.242.5	6.11KB 5.91KB	0:03:19	X
administrativo2	190.111.85.13:49269	172.27.242.3	6.32KB 6.48KB	0:03:50	X
administrativo3	190.111.85.13:64218	172.27.242.4	12.79KB 8.55KB	0:03:32	X
administrativo4	190.111.85.13:46211	172.27.242.2	13.34KB 23.30KB	0:04:31	X
administrativo5	190.111.82.74:25245	172.27.242.6	24.80KB 15.08KB	0:02:26	X

Figura 172: Comprobación de Conexión de los usuarios “administrativos”.

Fuente: Autor.

- **Usuarios “uTI”.**

Luego de que se realizó la conexión de los usuarios del grupo “uTI” al Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se evidencia que los usuarios del grupo se encuentran conectados al servidor OpenVPN y en funcionamiento (ver Figura 173).

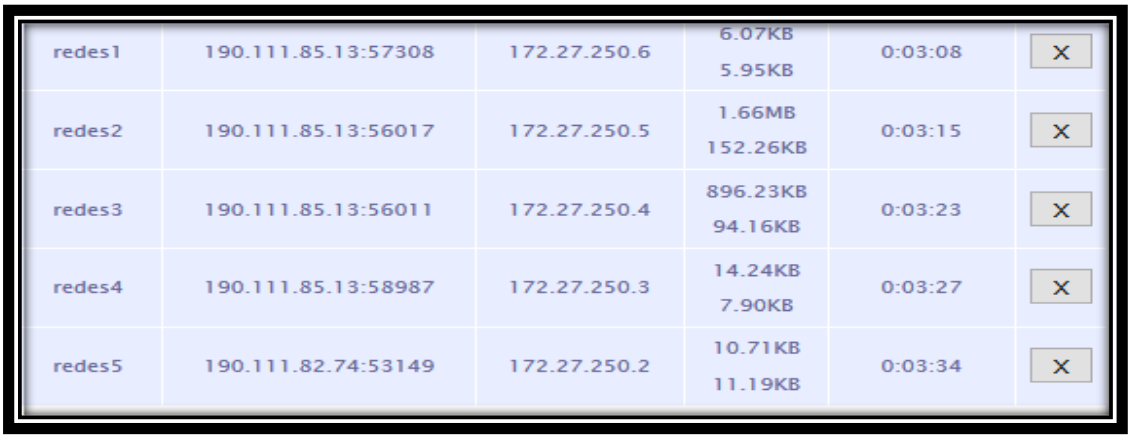
uti1	190.111.85.13:54986	172.27.252.5	6.02KB 8.81KB	0:03:06	X
uti2	190.111.85.13:54983	172.27.252.4	6.11KB 6.03KB	0:03:14	X
uti3	190.111.85.13:63776	172.27.252.3	6.26KB 6.04KB	0:03:33	X
uti4	190.111.85.13:38654	172.27.252.2	73.98KB 55.27KB	0:03:37	X
uti5	190.111.82.74:8349	172.27.252.6	8.06KB 8.50KB	0:02:27	X

Figura 173: Comprobación de Conexión de los usuarios “uTI”.

Fuente: Autor.

- **Usuarios “srei.uti”.**

Una vez que se realizó la conexión de los usuarios del grupo “srei.uti” al Servidor de Acceso OpenVPN, se evidencia que los usuarios del grupo se encuentran en funcionamiento y conectados (ver Figura 174).



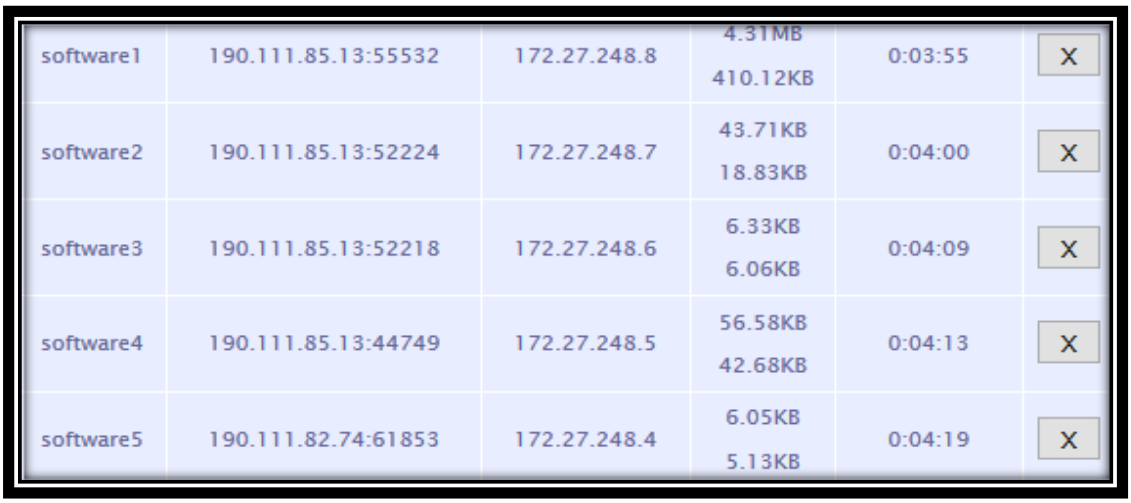
redes1	190.111.85.13:57308	172.27.250.6	6.07KB 5.95KB	0:03:08	X
redes2	190.111.85.13:56017	172.27.250.5	1.66MB 152.26KB	0:03:15	X
redes3	190.111.85.13:56011	172.27.250.4	896.23KB 94.16KB	0:03:23	X
redes4	190.111.85.13:58987	172.27.250.3	14.24KB 7.90KB	0:03:27	X
redes5	190.111.82.74:53149	172.27.250.2	10.71KB 11.19KB	0:03:34	X

Figura 174: Comprobación de Conexión de los usuarios “srei.uti”.

Fuente: Autor.

- **Usuarios “sdsw.uti”.**

Después de que se realizó la conexión de los usuarios del grupo “sdsw.uti” al Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se evidencia que los usuarios del grupo se encuentran en funcionamiento y conectados (ver Figura 175).



software1	190.111.85.13:55532	172.27.248.8	4.31MB 410.12KB	0:03:55	X
software2	190.111.85.13:52224	172.27.248.7	43.71KB 18.83KB	0:04:00	X
software3	190.111.85.13:52218	172.27.248.6	6.33KB 6.06KB	0:04:09	X
software4	190.111.85.13:44749	172.27.248.5	56.58KB 42.68KB	0:04:13	X
software5	190.111.82.74:61853	172.27.248.4	6.05KB 5.13KB	0:04:19	X

Figura 175: Comprobación de Conexión de los usuarios “sdsw.uti”.

Fuente: Autor.

- **Resultados de las Pruebas de Implementación.**

Una vez que se finalizó las pruebas de implementación del Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se verificó que las conexiones de las muestras de usuarios al Servidor de Acceso OpenVPN de acuerdo a los perfiles de usuarios que se definieron, se realizaron de manera exitosa.

6.4.5. Actividad 5: Prueba de Rendimiento.

En base a las pruebas de implementación que se realizaron en la Actividad 5 – Fase IV de Resultados, se realizó la prueba de rendimiento al Servidor OpenVPN de la Universidad Nacional de Loja, mediante la utilización de comandos Linux.

Esta prueba se la realizó para verificar el uso de los recursos del Servidor OpenVPN, al momento de encontrarse conectado con los 30 usuarios concurrentes. A continuación se detallan cada una de las capturas de pantalla que se realizó del rendimiento del servidor:

- **Ingreso al Servidor OpenVPN.**

Antes de realizar las capturas de pantalla del uso de los recursos del Servidor OpenVPN, se ingresó al Servidor (ver Figura 176).

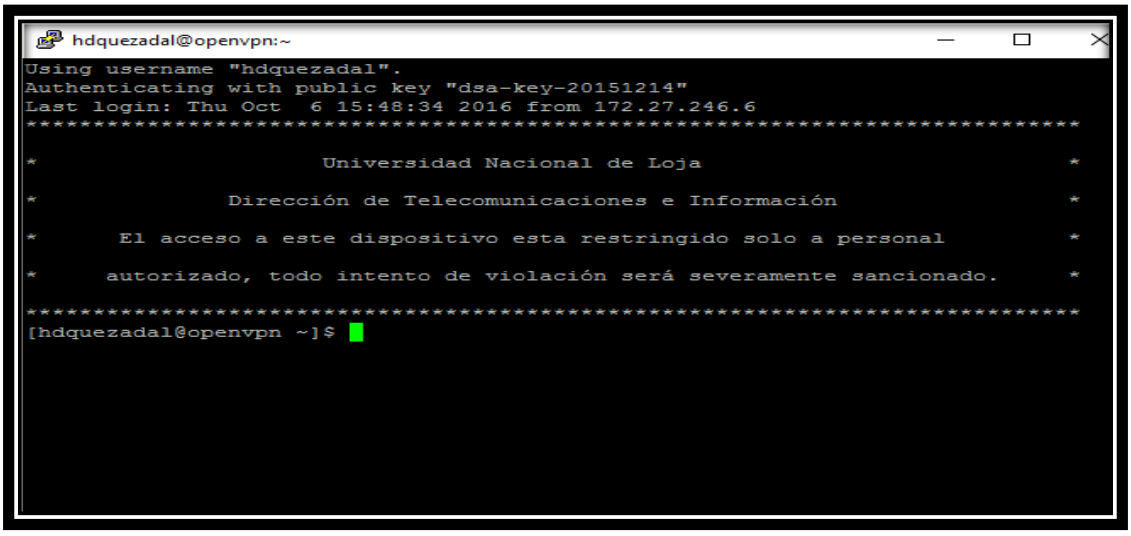


Figura 176: Ingreso al Servidor OpenVPN.

Fuente: Autor.

➢ **Capturas Rendimiento del Servidor.**

Luego de que se ingresó al Servidor OpenVPN, se realizó la captura con la información del sistema. Para ello se utilizó el comando: **uname –p**.

Una vez que se ingresó el comando "uname -p" en la terminal del servidor, se presentó la información del tipo de Kernel, el nombre del equipo, la versión del Kernel, la arquitectura del CPU, el procesador y el tipo del sistema operativo (GNU/Linux) (ver Figura 177).

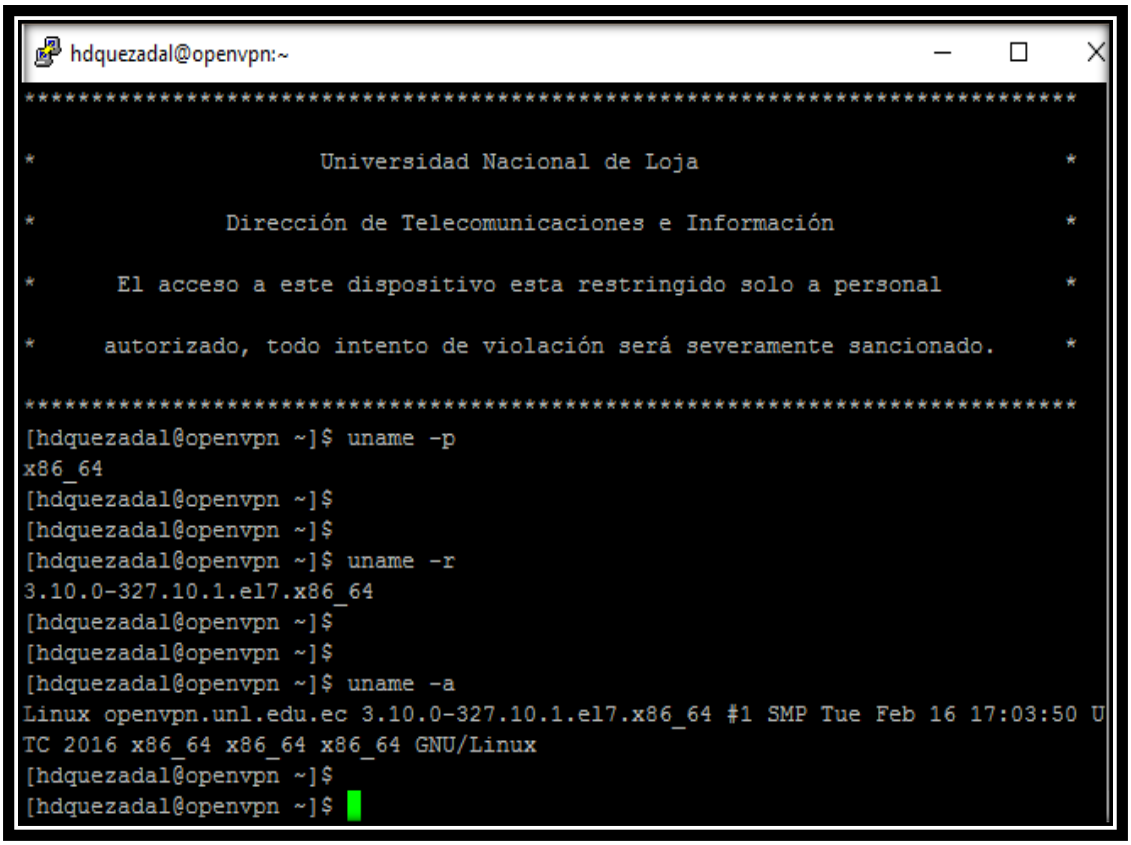


Figura 177: Captura de Pantalla Información de Sistema.

Fuente: Autor.

Después de que se obtuvo la información del sistema, se realizó la captura de pantalla del uso de espacio en los discos duros del servidor. Para ello se utilizó el comando: **df –h**.

Una vez que se ingresó el comando "df -h" en la terminal del servidor, se presentó la información del uso de espacio en los discos duros del servidor (ver Figura 178).

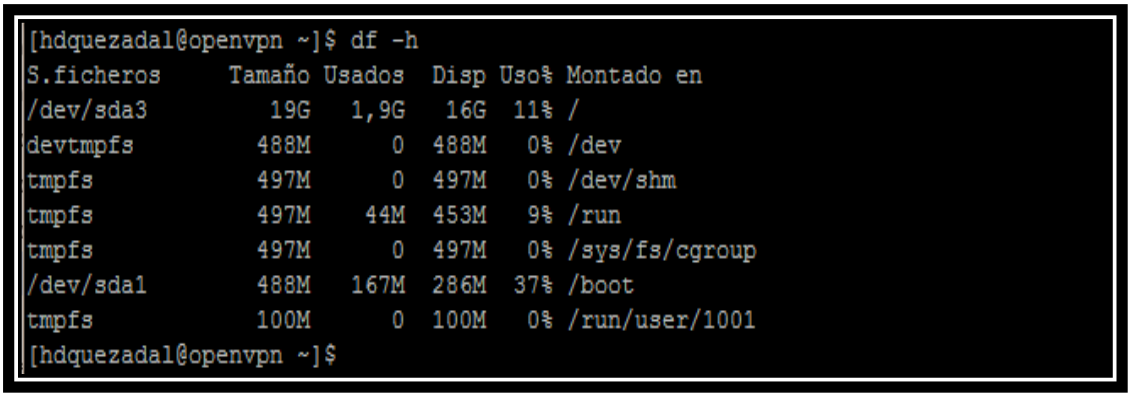


Figura 178: Información del Uso de Espacio en los Discos Duros del Servidor.
Fuente: Autor.

Después de que se obtuvo la información del uso de espacio en los discos duros del servidor, se realizó la captura de pantalla con el uso de memoria del servidor. Para ello se utilizó el comando: **watch –n 1 –d free**.

Una vez que se ingresó el comando "watch –n 1 –d free" en la terminal del servidor, se presentó la información del uso de memoria del servidor al momento de encontrarse conectados los 30 usuarios concurrentes (ver Figura 179).

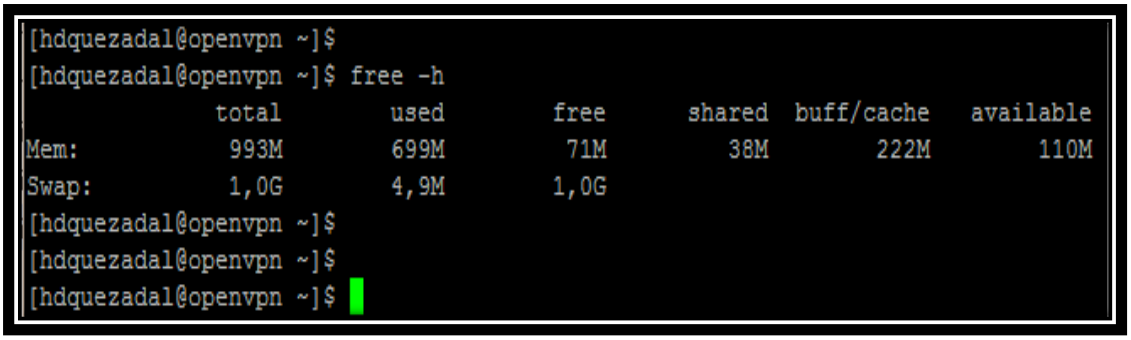


Figura 179: Información del Uso de Memoria en el Servidor.
Fuente: Autor.

- **Resultado de la Prueba.**

Una vez que se finalizó la prueba de rendimiento del Servidor OpenVPN de la Universidad Nacional de Loja, se evidenció que el uso de los recursos del sistema al momento de encontrarse los 30 usuarios concurrentes conectados al Servidor de Acceso OpenVPN fueron los siguientes (ver TABLA XIV):

TABLA XIV: RESULTADOS PRUEBA DE RENDIMIENTO

Resultados Prueba de Rendimiento del Servidor OpenVPN.		
Disco Duro		
Espacio Asignado: 19 GB	Espacio Usado: 1.9 GB	Espacio Disponible: 16 GB
Memoria RAM		
Memoria Asignada: 1 GB	Memoria Usada: 699 MB	Memoria Disponible: 71 MB
Memoria Swap		
Memoria Asignada: 1 GB	Memoria Usada: 4.9 MB	Memoria Disponible: 1 GB

- **Recomendación.**

Luego de que se verificó los recursos del sistema al momento de encontrarse los 30 usuarios concurrentes conectados al Servidor de Acceso OpenVPN de la Universidad Nacional de Loja, se recomienda ampliar la Memoria RAM asignada al servidor OpenVPN, acorde a las necesidades institucionales y a la integración de nuevas licencias OpenVPN de usuarios concurrentes.

7. Discusión

7.1. Desarrollo de la propuesta alternativa.

Para llevar a cabo la realización del presente trabajo de titulación se evaluaron cada uno de los objetivos planteados: general y específicos, indicando la forma en la que se fueron cumpliendo cada uno de ellos. Los cuales se detallan a continuación.

7.1.1. Objetivo Específico 1: Analizar estados de arte y casos de éxito de herramientas Open Source para el diseño de la VPN.

En esta primera etapa se realizó el análisis de casos de éxito orientados a la utilización de herramientas VPN Open Source para solucionar problemas de acceso a los recursos internos de las Universidades (base de datos científicas, libros electrónicos, videos, artículos, revistas). Se recopiló casos de éxitos nacionales e internacionales (ver Actividad 1 y 2 de la Fase I de Resultados), los cuales luego de su respectivo análisis permitieron obtener información relevante sobre las herramientas VPN Open Source que utilizaron para solucionar los problemas de acceso a la red interna desde un punto externo a la red.

Además, se revisó y analizó las diferentes herramientas VPN Open Source que se utilizan para el diseño de redes privadas virtuales (ver Actividad 3 – Fase I de Resultados). Lo cual permitió seleccionar la herramienta VPN más idónea para resolver el problema de acceso a las bases de datos científicas de la Universidad Nacional de Loja desde fuera del campus universitario.

7.1.2. Objetivo Específico 2: Diseñar la VPN basada en una tecnología y protocolos de seguridad para permitir la transmisión de datos.

Para el cumplimiento de este objetivo se realizó el análisis de las principales arquitecturas VPN (ver Actividad 2 – Fase II de Resultados), de los principales tipos de redes privadas virtuales (ver Actividad 1 – Fase II de Resultados), de los principales protocolos de túnel que se emplean en el diseño de las redes privadas virtuales (ver Actividad 3 – Fase II de Resultados) y de los principales Sistemas Operativos que se emplean en la instalación de servidores (ver Actividad 4 – Fase II de Resultados). Lo

cual permitió seleccionar los componentes más idóneos que se emplearon en el diseño de la red privada virtual de la Universidad Nacional de Loja. Además, se determinó los perfiles de usuario para la autenticación en la red privada virtual que se diseñó (ver Actividad 6 – Fase II de Resultados).

7.1.3. Objetivo Específico 3: Crear un escenario de una VPN para acceder a las bases de datos científicas de la Universidad Nacional de Loja.

Para el cumplimiento de este objetivo se utilizó el diseño de la red privada virtual que se realizó en el objetivo anterior (ver Actividad 6 – Fase II de Resultados). Lo cual permitió la integración de la red privada virtual con la red interna de la Universidad Nacional de Loja, mediante la instalación y configuración de un Servidor de Acceso OpenVPN para el acceso a las bases de datos científicas de la institución (ver Fase III de Resultados).

7.1.4. Objetivo Específico 4: Aplicar pruebas para evaluar el correcto funcionamiento del escenario de la VPN.

Para evaluar el correcto funcionamiento de la red privada virtual que se creó en el objetivo anterior (ver Fase III de Resultados). Se aplicó pruebas de conectividad, de conexión a las bases de datos científicas, de carga, de implementación y de rendimiento al Servidor de Acceso OpenVPN (ver Fase IV de Resultados). Lo cual permitió verificar que la red privada virtual que se creó en la Universidad Nacional de Loja, permitió el acceso a las bases de datos científicas desde una red externa a la institución.

7.2. Valoración Técnica Económica Ambiental.

En el presente Trabajo de Titulación se aplicó y reforzó los conocimientos adquiridos a lo largo de los años de preparación académica en la carrera de Ingeniería en Sistemas y se concluyó de manera satisfactoria porque se contó con todos los recursos humanos, económicos y tecnológicos.

En el ámbito económico se hizo una mayor inversión, ya que el software usado en su mayoría es libre, pero pagado en la adquisición de licencias, para el hardware se usaron los equipos de la Universidad Nacional de Loja de manera gratuita. En la parte de

recursos humanos se contó con la persona investigadora y el tutor del Trabajo de Titulación.

El resultado del presente Proyecto de Titulación es el diseño de una red privada virtual para el acceso a las bases de datos científicas de la Universidad Nacional de Loja, reduciendo la movilización constante a las bibliotecas de cada una de las áreas de la Universidad y reducción del uso de papel y tinta al momento de imprimir las consultas realizadas, lo cual representa un ahorro significativo de los recursos naturales.

Por las razones mencionadas fue factible el desarrollo del presente proyecto. Los materiales utilizados para el desarrollo del proyecto se detallan a continuación:

TABLA XV: RECURSOS HUMANOS

RECURSOS HUMANOS				
DESCRIPCIÓN	**UNIDAD**	**CANTIDAD**	**COSTO UNITARIO (USD)**	**SUBTOTAL**
Tesista	Hora	400	5.00	2000.00
Director de Tesis	Hora	100	----	----
			TOTAL	2000.00

TABLA XVI: RECURSOS MATERIALES

RECURSOS MATERIALES				
DESCRIPCIÓN	**UNIDAD**	**CANTIDAD**	**COSTO UNITARIO (USD)**	**SUBTOTAL**
Cartuchos de Tinta	Unidad	3	24.00	72.00
Copias	Unidad	100	0.02	2.00
Resma Papel	Unidad	2	5.00	10.00
Anillados	Unidad	3	3.00	9.00
CD´s	Unidad	3	1.00	3.00
Empastados	Unidad	3	10.00	30.00
Internet	Hora	200	0.40	80.00
Transporte	----	----	40.00	40.00
			TOTAL	246.00

TABLA XVII: RECURSOS TÉCNICOS/TECNOLÓGICOS

RECURSOS TECNICOS/TECNOLOGICOS				
DESCRIPCIÓN	**UNIDAD**	**CANTIDAD**	**COSTO UNITARIO (USD)**	**SUBTOTAL**
HARDWARE				
Computador	Unidad	1	200.00	200.00
Disco Externo	Unidad	1	100.00	100.00
Impresora	Unidad	1	80.00	80.00
Memorias	Unidad	1	10.00	10.00
Servidor	Unidad	1	----	----
SOFTWARE				
Editor Látex	Unidad	1	----	----
S.O Centos	Unidad	1	----	----
OpenVPN (licencias)	Unidad	30	10.00	300.00
			TOTAL	690.00

TABLA XVIII: IMPREVISTOS

IMPREVISTOS	
DESCRIPCIÓN	**SUBTOTAL**
Valores adicionales a los recursos necesarios	50.00
TOTAL	50.00

La TABLA XVII, presenta la suma total de todos los recursos: humanos, materiales, técnicos/tecnológicos e imprevistos asignados para el desarrollo del trabajo de titulación.

TABLA XIX: PRESUPUESTO UTILIZADO

DESCRIPCION	SUBTOTAL
HUMANOS	2000.00
MATERIALES	246.00
TÉCNICOS/TECNOLÓGICOS	690.00
IMPREVISTOS	50.00
TOTAL	2986.00

8. Conclusiones

- Mediante el respectivo análisis de los principales elementos que componen las redes privadas virtuales y casos de éxito orientados al diseño de redes privadas virtuales se determinó que las redes privadas virtuales son la mejor alternativa para permitir que los estudiantes accedan a las bases de datos científicas de la Universidad Nacional de Loja, debido a su alto grado de confidencialidad, seguridad, integridad y autenticidad.

- Con el uso del software OpenVPN se logró diseñar una red privada virtual basada en una tecnología y protocolos de seguridad SSL-TLS que permitió a los usuarios remotos acceder de una forma segura a las bases de datos científicas de la Universidad Nacional de Loja.

- La instalación y configuración del Servidor de Acceso OpenVPN permitió establecer un enlace de comunicación directo entre los servicios de la red interna de la Universidad Nacional de Loja y los usuarios remotos, sin preocuparse de la infraestructura física de la red ni de los equipos que la conforman.

- Con la implementación de la red privada virtual en la Universidad Nacional de Loja se creó un servicio de acceso a biblioteca virtual que permitió acceder a los recursos internos (base de datos científicas, libros electrónicos, revistas digitales) desde una red externa a la institución.

9. Recomendaciones

- Establecer las políticas de seguridad necesarias para evitar el acceso de usuarios no autorizados a los servicios de la red interna de la Universidad Nacional de Loja.

- Implementar nuevos servicios académicos externos para la comunidad universitaria (video conferencias, chats online, tutorías virtuales).

- Realizar un monitoreo continuo de los registros de acceso que genere la red privada virtual, para poder determinar las conexiones establecidas, el tiempo de duración de las conexiones y a que información accedieron en la red interna de la institución.

- Mejorar el servicio y mantenimiento de las bases de datos científicas de la Universidad Nacional de Loja para la realización de consultas por parte de los estudiantes y docentes, ya que la mayoría de ellas se encuentran deshabilitadas.

- Implementar el servicio de VoIP y video conferencia para la conexión de las extensiones universitarias y centros de investigación que posee la Universidad Nacional de Loja.

- Realizar un estudio sobre el acceso a las bases de datos científicas de la institución por parte de los estudiantes para adquirir una mayor cantidad de licencias que beneficien a la comunidad universitaria.

10. Bibliografía

[1] Claudia Isla Torres, «Uso de las Tecnologías,» Abril 2008. [En línea]. Available: http://www.eveliux.com/mx/Uso-de-Tecnologias-en-la-educacion.html. [Último acceso: 12 febrero 2016].

[2] Cisco, «Red Privada Virtual,» [En línea]. Available: http://www.cisco.com/web/LA/soluciones/la/vpn/index.html. [Último acceso: 12 febrero 2016].

[3] Universidad de Valencia, «Que es una Red Privada Virtual,» 2014. [En línea]. Available: http://www.uv.es/uvweb/servicio-informatica/es/servicios/generales/red-comunicaciones/red-privada-virtual-vpn-/-es-vpn-1285903202284.html. [Último acceso: 13 febrero 2016].

[4] CCM, «Funcionamiento de una VPN,» [En línea]. Available: http://es.ccm.net/contents/258-vpn-redes-privadas-virtuales. [Último acceso: 13 febrero 2016].

[5] Daysi Patricia Cansino Henao, «Diseño e Implementación de una Red Privada Virtual segura para las oficinas de Caminosca S.A. Basado en Plataforma GNU/Linux.,» Universidad Politécnica Salesiana, Quito, 2012.

[6] Luis Mario Galarza, «Fundamentos de la Computación,» ecotec, Guayaquil, 2002.

[7] Patricia Izarra, «Virtual Private Network,» 19 octubre 2012. [En línea]. Available: http://www.universaldesk.com/support/index.php?/Knowledgebase/Article/View/135. [Último acceso: 12 febrero 2016].

[8] Universidad de Cádiz, «Área de Informática de la Universidad de Cádiz, Oficina del Software Libre de la Universidad de Cádiz (OSLUCA),» 2016. [En línea]. Available: http://www2.uca.es/serv/ai/servicios/vpn/linux/openvpn.pdf. [Último acceso: 16 mayo 2016].

[9] Página Web de la Universidad de Cádiz, «Campus Universitarios,» 2016. [En línea]. Available: http://www.uca.es/es/nuestra-universidad/los-campus. [Último acceso: 14 Mayo 2016].

[10] Universidad de Valencia, «Servicio de Informática de la Universidad de Valencia,» 2016. [En línea]. Available: http://www.uv.es/uvweb/servicio-informatica/es/servicios/generales/red-comunicaciones/red-privada-virtual-vpn-/ventajas-inconvenientes-1285903202290.html. [Último acceso: 17 Mayo 2016].

[11] Universidad de Sevilla, «Servicio de Informática y Comunicación (SIC) de la Universidad de Sevilla,» 2016. [En línea]. Available: http://sic.us.es/servicios/infraestructuras-comunicaciones-hw-y-sw/acceso-externo-los-recursos-electronicos-de-la-us. [Último acceso: 15 Mayo 2016].

[12] Universidad Católica de Cuenca, «Servivio de Red Privada Virtual (VPN) Institucional (UCACUE),» 2016. [En línea]. Available: http://matriculas.ucacue.edu.ec/BasesCientificas/Inicio.aspx?ReturnUrl=%2fBasesCientificas%2f. [Último acceso: 05 Junio 2016].

[13] Universidad de Cuenca, «Sistema para Acceso Externo a Bases Digitales,» 2015. [En línea]. Available: http://www.ucuenca.edu.ec/recursos-servicios/biblioteca/servicios#sistema-para-acceso-externo-a-bases-sigitales. [Último acceso: 20 Mayo 2016].

[14] Hipertextual, «Las mejores herramientas para trabajar desde casa con VPN,» 28 octubre 2013. [En línea]. Available: http://hipertextual.com/archivo/2013/10/trabajar-casa-con-vpn/. [Último acceso: 12 febrero 2016].

[15] LogMeIn, «Hamachi,» [En línea]. Available: https://secure.logmein.com/products/hamachi/. [Último acceso: 13 febrero 2016].

[16] SimilarWeb, «SimilarWeb,» 2016. [En línea]. Available: https://www.similarweb.com/pro. [Último acceso: 15 julio 2016].

[17] Neoteo, «Las Mejores VPN Gratuitas,» [En línea]. Available: http://www.neoteo.com/los-mejores-vpn-gratuitos. [Último acceso: 15 febrero 2016].

[18] ItsHidden, «ItsHidden,» [En línea]. Available: www.itshidden.com. [Último acceso: 12 febrero 2016].

[19] torVPN, «torVPN,» [En línea]. Available: https://www.torvpn.com/en/vpn. [Último acceso: 12 febrero 2016].

[20] Frondev, «10 Best VPN,» [En línea]. Available: http://www.fromdev.com/2011/12/10-excellent-opensource-vpn-solutions.html#lilivpn. [Último acceso: 13 febrero 2016].

[21] SecurePoint, «Securepoint securyty solutions,» [En línea]. Available: http://www.securepoint.cc/products-terra-vpn-gateway.html. [Último acceso: 15 febreo 2016].

[22] Freedom, «Your - Freedom,» [En línea]. Available: http://www.your-freedom.net. [Último acceso: 12 febrero 2016].

[23] SoftEther, «VPN Project,» [En línea]. Available: https://www.softether.org. [Último acceso: 13 febrero 2016].

[24] ExpressVPN, «ExpressVPN,» [En línea]. Available: https://www.expressvpn.com/es. [Último acceso: 20 febrero 2016].

[25] Oast, «OAST VPN,» [En línea]. Available: https://sourceforge.net/projects/oast/. [Último acceso: 13 febrero 2016].

[26] VPNBOOK, «VPNBOOK,» [En línea]. Available: http://www.vpnbook.com. [Último acceso: 15 febrero 2016].

[27] tuxjm, «Introducción a OpenVPN,» [En línea]. Available: http://tuxjm.net/docs/Creacion_de_Redes_Privadas_Virtuales_en_GNU_Linux_con_OpenVPN/html-multiples/introduccion-a-openvpn.html. [Último acceso: 16 febrero 2016].

[28] LUGRO, «Introducción Redes Privadas Virtuales,» [En línea]. Available: http://www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html. [Último acceso: 16 febrero 2016].

[29] Andrés Montes de los Santos, «Propuesta Implementación de una VPN,» Instituto Politécnico Nacional, Mexico, 2012.

[30] UNAM, «Redes Privadas Virtuales,» México, 2013.

[31] Diego Álvarez Delgado, «Redes Privadas Virtuales,» Universidad Técnica Federico Santa María, Chile, 2014.

[32] CMR Networks, «Infraestructura IT,» [En línea]. Available: http://www.cmr-networks.com/?page=infraestructura_it. [Último acceso: 15 febrero 2016].

[33] Jaime Perez Crespo, «Redes Privadas Virtuales,» 09 febrero 2011. [En línea]. Available: http://blackspiral.org/docs/pfc/itis/node5.html. [Último acceso: 19 mayo 2016].

[34] Technet, «Protocolos VPN,» [En línea]. Available: https://technet.microsoft.com/es-es/library/cc771298%28v=ws.10%29.aspx. [Último acceso: 15 febrero 2016].

[35] Juan Jóse Tomas, «Servicio VPN de acceso remoto basado en SSL mediante OpenVPN,» Universidad Politécnica de Cartagena, España, 2008.

[36] GIGANEWS, «Compare los Protocolos de VPN,» 15 julio 2016. [En línea]. Available: http://es.giganews.com/vyprvpn/compare-vpn-protocols.html. [Último acceso: 09 agosto 2016].

[37] Bradley Mitchel, «PPTP - Point to Point Tunneling Protocol,» about Tech, 2016. [En línea]. Available: http://compnetworking.about.com/od/vpn/g/bldef_pptp.htm. [Último acceso: 15 mayo 2016].

[38] Jesús Fernandez Hernandez, «Redes Privadas Virtuales,» Departamento de Informática y Automática - Universidad de Salamanca, España, 2006.

[39] Alexandro Gonzalez Morales, «Redes Privadas Virtuales,» Universidad Autónoma del Estado de Hidalgo, Pachuca, 2011.

[40] Universidad Politécnica de Madrid, «Protocolo IPSEC,» [En línea]. Available: http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec. [Último acceso: 16 febrero 2016].

[41] ElephantVPN, «Mejores Protocolos VPN,» [En línea]. Available: http://www.elephantvpn.com/es/content/58-what-is-the-best-vpn-connection-method. [Último acceso: 22 febrero 2016].

[42] LeVPN, «OpenVPN,» [En línea]. Available: http://www.le-vpn.com/es/openvpn-protocolo-vpn/. [Último acceso: 14 febrero 2016].

[43] PYDOT, «Sistemas Operativos y software disponible,» Pydot, 2015. [En línea]. Available: https://www.pydot.com/servidores/software. [Último acceso: 15 mayo 2016].

[44] CentOS, «Community Enterprise Operating System,» CentOS, 18 Noviembre 2015. [En línea]. Available: https://wiki.centos.org/es. [Último acceso: 25 Junio 2016].

[45] Fernando Manuel, «CentOS 7.0,» Genbeta, 14 julio 2014. [En línea]. Available: http://www.genbeta.com/linux/centos-7-0-la-primera-version-de-la-nueva-era-ya-esta-aqui. [Último acceso: 21 julio 2016].

[46] Debian, «Acerca de Debian,» Proyecto Debian, 5 julio 2016. [En línea]. Available: https://www.debian.org/intro/about#what. [Último acceso: 12 junio 2016].

[47] Acerca de Guía Ubuntu, «Debian,» Debian, 05 mayo 2015. [En línea]. Available: http://guia-ubuntu.com/index.php?title=Debian. [Último acceso: 15 junio 2016].

[48] Debian, «Requerimientos del Sistema,» Debian, 15 julio 2015. [En línea]. Available: https://www.debian.org/releases/stable/i386/ch03s04.html.es. [Último acceso: 20 mayo 2016].

[49] Ubuntu Fácil, «Ubuntu Server,» 17 abril 2013. [En línea]. Available: http://www.ubuntufacil.com/2013/04/ubuntu-server/. [Último acceso: 20 mayo 2016].

[50] Canonical , «Ubuntu Server,» Canonical Ltd, 12 enero 2016. [En línea]. Available: http://www.ubuntu.com/server. [Último acceso: 25 marzo 2016].

[51] Recursos de CEPIndalo, «Sistema operativo servidor (Ubuntu Server),» CEPIndalo, 24 agosto 2016. [En línea]. Available:

http://recursos.cepindalo.es/mod/book/tool/print/index.php?id=548#ch154. [Último acceso: 26 agosto 2016].

[52] Alberto Hornero Luque, «Linux Hispano,» 16 febrero 2011. [En línea]. Available: http://www.linuxhispano.net/2010/02/16/distribuciones-linux-para-servidores/. [Último acceso: 20 junio 2016].

[53] Seaq, «Red Hat Enterprise Linux,» [En línea]. Available: http://www.seaq.co/rhels.html. [Último acceso: 21 junio 2016].

[54] Red Hat, «Requerimientos del Hardware,» 2016. [En línea]. Available: https://access.redhat.com/documentation/es-ES/Red_Hat_Network_Satellite/5.4/html/Proxy_Installation_Guide/s1-hardware-requirements.html. [Último acceso: 15 junio 2016].

[55] Microsoft, «Windows Server 2012 R2,» Microsoft, 2016. [En línea]. Available: https://www.microsoft.com/es-xl/server-cloud/products/windows-server-2012-r2/default.aspx. [Último acceso: 20 junio 2016].

[56] Joan Carles Roca, «Descubre las novedades en Windows Server 2012 R2,» Netmind, 26 junio 2014. [En línea]. Available: http://www.netmind.es/knowledge-center/novedades-en-windows-server-2012-r2/. [Último acceso: 15 julio 2016].

[57] Internet Ya Soluciones Web, «Ventajas y Características de Windows Server 2012 R2,» 07 mayo 2016. [En línea]. Available: http://www.internetya.co/versiones-y-caracteristicas-de-windows-server-2012-r2/. [Último acceso: 18 julio 2016].

[58] Universidad Nacional de Loja, «Universidad,» 2016. [En línea]. Available: http://unl.edu.ec/universidad/nosotros. [Último acceso: 24 julio 2016].

[59] Universidad Nacional de Loja, «Ofertas Académicas,» 2016. [En línea]. Available: http://unl.edu.ec/universidad/oferta-acad%C3%A9mica-carreras. [Último acceso: 15 julio 2016].

[60] Universidad Nacional de Loja, «Servicios. Bienestar Estudiantil,» 2016. [En línea]. Available: http://unl.edu.ec/bienestar/bienestar-nosotros. [Último acceso: 20 julio 2016].

[61] Universidad Nacional de Loja, «Radio Universitaria,» 2016. [En línea]. Available: http://unl.edu.ec/radio/radio-universitaria-nosotros. [Último acceso: 21 julio 2016].

[62] Universidad Nacional de Loja, «U.P.S Nivelación,» 2016. [En línea]. Available: http://unl.edu.ec/nivelacion/nivelaci%C3%B3n-nosotros. [Último acceso: 21 julio 2016].

[63] Universidad Nacional de Loja, «Sistema Bibliotecario,» 2016. [En línea]. Available: http://unl.edu.ec/universidad/biblioteca-nosotros. [Último acceso: 15 julio 2016].

[64] Universidad Nacional de Loja, «Redes y Equipos Informáticos,» 2014. [En línea]. Available: http://unl.edu.ec/universidad/noticia/convocatoria-p%C3%BAblica-para-puesto-de-subdirectora-de-redes-y-equipos-inform%C3%A1ticos. [Último acceso: 21 julio 2016].

[65] Jaramillo Castro Carlos Miguel, Ocampo Vélez Lenin Sebastián, Vivanco Encalada Henry Paúl, «Implementación Active Directory aplicando el estándar 802.1x, dentro de la red LAN y WLAN de la Universidad Nacional de Loja.,» 2016. [En línea]. Available: http://dspace.unl.edu.ec/jspui/handle/123456789/10942. [Último acceso: 20 julio 2016].

11. Anexos

Anexo 1: Mensaje de Advertencia sobre el Acceso a las Bases de Datos Científicas de la UNL.

Al momento de acceder a Biblioteca Virtual en la Universidad Nacional de Loja se observa un mensaje de advertencia sobre el acceso a las bases de datos científicas de la institución:

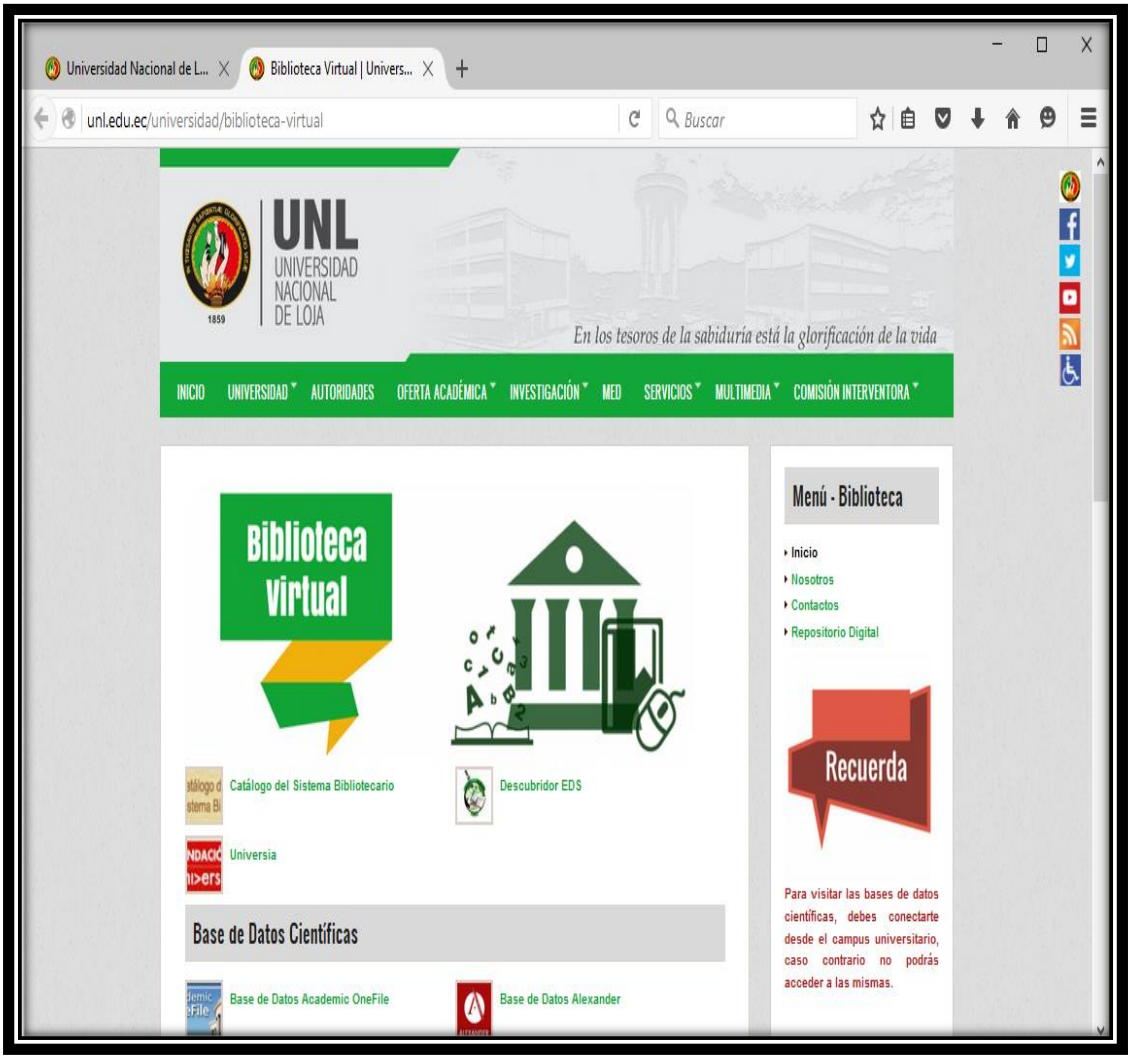


Figura 180: Mensaje de Advertencia para el Acceso a las Bases de Datos Científicas.
Fuente: Autor.

Anexo 2: Ingreso a las Bases de Datos Científicas desde fuera del Campus Universitario.

En este anexo se puede observar las restricciones que existen para acceder a las bases de datos científicas de la Universidad Nacional de Loja desde fuera del campus universitario:

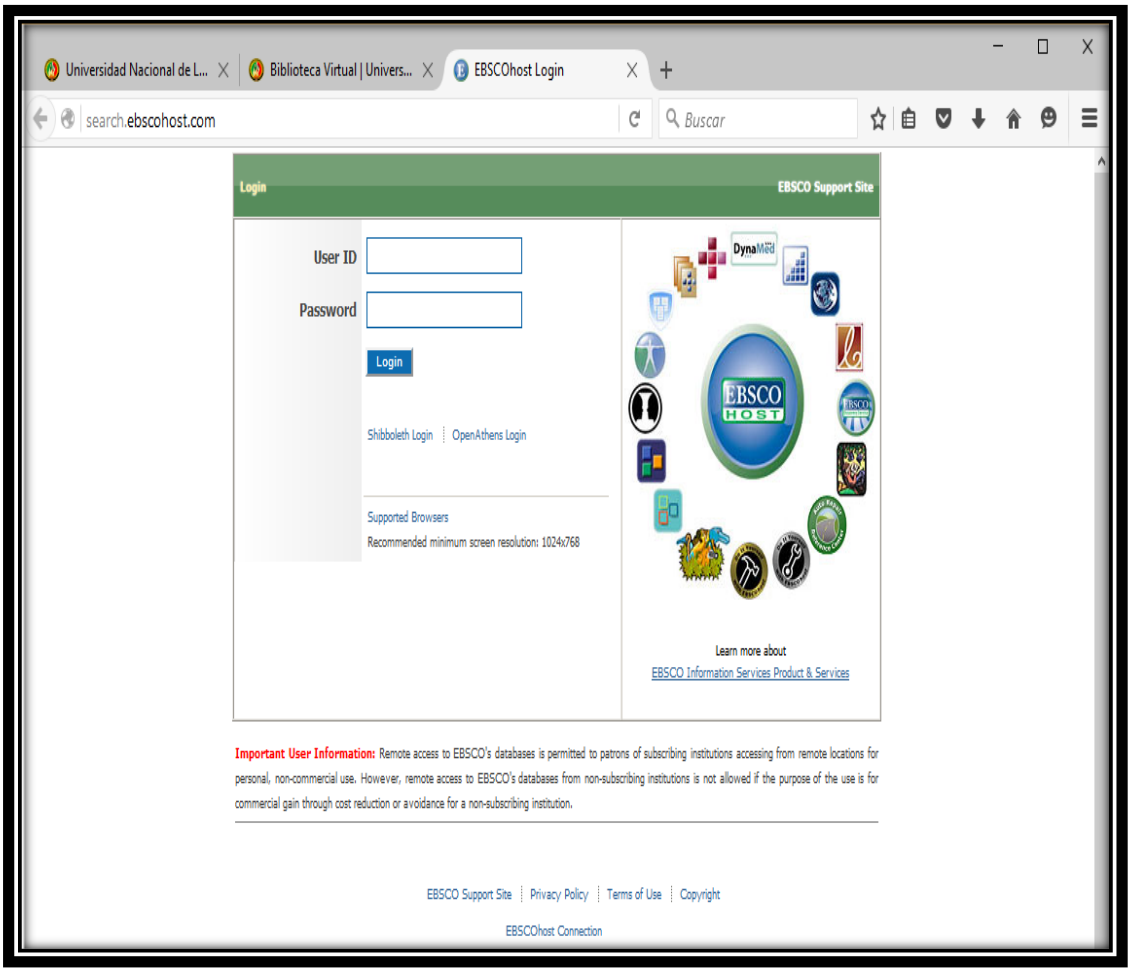


Figura 181: Acceso a la Base de Datos Científica EBSCO desde fuera de la Universidad.
Fuente: Autor.

Anexo 3: Convocatoria de reunión a los funcionarios de la Unidad de Telecomunicaciones e Información para la ostentación de los resultados del proyecto de titulación.

UNIVERSIDAD NACIONAL DE LOJA

CIS

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

CARRERA DE INGENIERÍA EN SISTEMAS

Loja, 15 de marzo del 2016

A los funcionarios de la Unidad de Telecomunicaciones e Información, se los convoca a una reunión el día Miércoles 16 de marzo del presente año, a las 9h00 a.m., en la sala de reuniones de la Unidad de Telecomunicaciones e Información, con el fin de realizar la Ostentación de los resultados del proyecto de titulación denominado: DISEÑO DE UNA VPN PARA EL ACCESO A LAS BASES DE DATOS CIENTÍFICAS DE LA UNIVERSIDAD NACIONAL DE LOJA.

Esperando contar con la presencia de todos, desde ya les anteio mis más sinceros agradecimientos.

Ing. Milton Labanda
DIRECTOR DE LA UTI

Ing. Edison Coronel
SUBDIRECTOR DE SOFTWARE

Ing. Mario Palma
DOCENTE DE LA CIS

Ing. Juan Pablo Ramón
FUNCIONARIO UTI

UNIVERSIDAD NACIONAL DE LOJA

Ing. Juan Calderón
SUBDIRECTOR DE REDES

Ing. Rodrigo Japón
FUNCIONARIO DE LA UTI

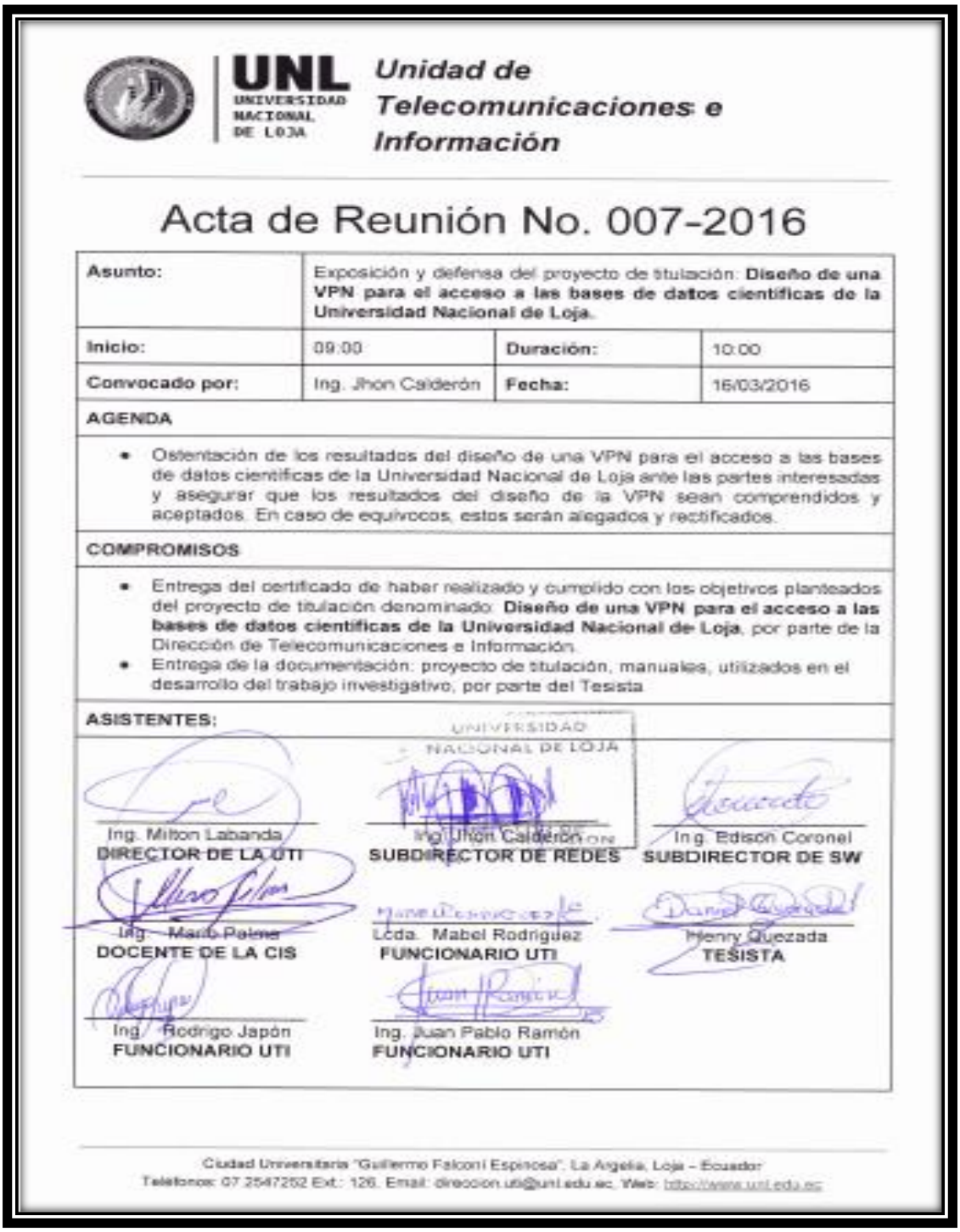
Lcda. Mabel Rodríguez
FUNCIONARIO DE LA UTI

Atentamente, Henry Quezada
TESISTA

Figura 182: Convocatoria Reunión para la Defensa de la Tesis en la UTI.

Fuente: Autor.

Anexo 4: Acta de Reunión de la defensa del proyecto de titulación en la Unidad de Telecomunicaciones e Información.



UNL
UNIVERSIDAD NACIONAL DE LOJA

Unidad de Telecomunicaciones e Información

Acta de Reunión No. 007-2016

Asunto:	Exposición y defensa del proyecto de titulación: **Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja.**		
Inicio:	09:00	**Duración:**	10:00
Convocado por:	Ing. Jhon Calderón	**Fecha:**	16/03/2016

AGENDA

- Ostentación de los resultados del diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja ante las partes interesadas y asegurar que los resultados del diseño de la VPN sean comprendidos y aceptados. En caso de equívocos, estos serán alegados y rectificados.

COMPROMISOS

- Entrega del certificado de haber realizado y cumplido con los objetivos planteados del proyecto de titulación denominado: **Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja**, por parte de la Dirección de Telecomunicaciones e Información.
- Entrega de la documentación: proyecto de titulación, manuales, utilizados en el desarrollo del trabajo investigativo, por parte del Tesista

ASISTENTES:

UNIVERSIDAD NACIONAL DE LOJA

Ing. Milton Labanda
DIRECTOR DE LA UTI

Ing. Jhon Calderón
SUBDIRECTOR DE REDES

Ing. Edison Coronel
SUBDIRECTOR DE SW

Ing. Mario Palma
DOCENTE DE LA CIS

Lcda. Mabel Rodriguez
FUNCIONARIO UTI

Henry Quezada
TESISTA

Ing. Rodrigo Japón
FUNCIONARIO UTI

Ing. Juan Pablo Ramón
FUNCIONARIO UTI

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja – Ecuador
Teléfonos: 07 2547252 Ext.: 126. Email: direccion.uti@unl.edu.ec. Web: http://www.unl.edu.ec

Figura 183: Acta de Reunión Defensa de la Tesis en la UTI.

Fuente: Autor.

Anexo 5: Certificado de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

UNL
UNIVERSIDAD NACIONAL DE LOJA

Unidad de Telecomunicaciones e Información

Milton L. Labanda Jaramillo Mg.
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

Certifica

Que el señor **Henry Daniel Quezada Lozano** con cédula de ciudadanía número **1104872815** y egresado de la Carrera de Ingeniería en Sistemas, ha finalizado lo referente a la ejecución práctica de su proyecto de titulación denominado **"Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja"** en la Unidad de Telecomunicaciones de Información, bajo los lineamientos y requerimientos establecidos por esta unidad administrativa de la Universidad Nacional de Loja.

Es cuanto puedo indicar en honor a la verdad, facultando al interesado hacer uso del presente documento.

Loja, 21 de Marzo del 2016.

Milton Labanda, Mg.
DIRECTOR DE TELECOMUNICACIONES E INFORMACIÓN

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 126, Email: direccion.uti@unl.edu.ec, Web: http://www.unl.edu.ec

Figura 184: Certificado Finalización de la Tesis en la UTI.

Fuente: Autor.

Anexo 6: Licencia del Trabajo de Titulación.